ISSN:1858-571X (يوليو 2011م) العدد الحادي عشر

دليل الإثبات الإلكتروني - Degital Evidence

سوسن سعيد شندي [1]

المقدمة:

لقد أحرز التقدم العلمي والتكنولوجي أنواعاً جديدة من الوسائل ، وأنماطاً حديثة لم تعرف إلا في المجتمعات المعاصرة؛ فقد أدى الاستخدام الواسع لأجهزة الحاسب الآلي [Computer] في المعاملات المدنية، والمعاملات التجارية ـ إلى وجود أنماط جديدة، وهي المعاملات الالكترونية، كما أدى التطور التقني إلى دفع بعض الأشخاص من الاستفادة غير القانونية من هذه التكنولوجيا المتقدمة؛ وذلك لتحقيق مكاسب غير مشروعة مستفيدين مما وصلت إليه التكنولوجيا من تقدم سعياً للوصول إلى أغراضهم.

بل أصبحت هذه المعلوماتية مصدراً مهماً لكثير من التطورات القانونية التي تحدث الآن في العالم، والسودان كجزءٍ من هذه العولمة [Globalization] حتماً قد تأثر بهذا التطور في مجال المعلوماتية ، ولكن بقي الوضع قانوناً كما كان إلى أن صدرت القوانين التي تحكمها في العام 2007م ؛ فقد أصدرت السلطة التشريعية قانونى المعاملات الالكترونية 2007م ، وقانون جرائم المعلوماتية 2007م لمقابلة التطور؛ لأنه ليس من المنطق، وفي ظل هذا التطور الهائل في مجال التكنولوجيا، ومجال المعلوماتية ـ أن تبقى القوانين كما هي دون مواكبة، ولا خلاف أن القاعدة القانونية قاعدة اجتماعية تعبر عن المجتمع، وتتطور بتطوره، كما تعبر بالفعل عن احتياجاته. ويحتل الإثبات مكانةً مهمة في التطبيق العملي؛ لأنه هو الوسيلة الأساسية للحصول على الحقوق، ومن ثم إلزام الأخريين بالوفاء بهذه الحقوق.

وقد أدى التقدم التكنولوجي إلى تغيير مفهوم الإثبات التقليدي؛ لأن الحقوق والالتزامات أصبحت تثبت بطرق الكترونية أيضاً، ولم يعد بالإمكان تجاهل هذا الوضع؛ إذ أصبحت غالبية

---

[1] قاضي الاستئناف إدارة المكتب الفني والبحث العلمي

الالتزامات، والعقود تتم بوسائل الكترونية؛ لما يوفره الإنترنت من وقت وجهد، بل أصبح الإنترنت وسيلة تستخدم للترويج، وتوزيع السلع والخدمات، وهو ما يعرف بالتجارة الإلكترونية، وتطبيقاتها أصبحت كثيرة تغطي شراء وبيع المنتجات، وهو ما يسمى بالسوق الالكتروني، وتسهيل وتسيير المعلومات والاتصالات والتعاون ما بين الشركات، وتوفير الخدمات لطالبي الخدمات. لذلك رأيت أن أتناول موضوع الإثبات الالكتروني بالمناقشة لمعرفة الوضع القانوني فى هذا المجال فى ظل افتقار المجتمع للتجارب العملية للحداثة، وعدم انتشار المعاملات الاكترونية، وعدم وجود قانون خاص بالإثبات الالكترونى، وعدم وجود سوابق قضائية فى هذا المجال تثير النقاش، ونسأل الله العلى العظيم أن أتمكن من لفت نظر الخبراء فى هذا المجال لتناول هذه الموضوعات بالمناقشة.

أولاً – الإثبات الالكتروني :

1– تعريف الإثبات في اللغة والاصطلاحين الفقهي والقانوني :

الإثبات لغةً : يعني ثبت الشيء يثبتُ ثباتاً فهو ثابت ، ويقال ثبت فلان في المكان يثبت فهو ثابت ، إذا إقام به .

وثبت في الأمر: تأنى ولم يتعجل . ويثبت إذا شاور وفحص عنه.

وقوله عز وجل: " ومثل الذين ينفقون أموالهم إبتغاء مرضاة الله وتثبيتاً من أنفسهم".

قال الزَجَّاج: أي ينفقونها مقرين بأنها مما يثبتُ الله عليها.

وقوله عز وجل: "وكلاً نقص عليك من أنباء الرسل ما نثبت به فؤادك"، قال: معنى نثبت الفؤاد تسكين القلب، وهنا ليس للشك، ولكن كلما كان البرهان والدلالة أكثر على القلب . كان القلب أسكن وأثبت أبداً. (1)

أما الإثبات بمعناه القانوني، فهو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتبت أثارها.(2)

وللإثبات أهمية من الناحية العملية، لأن الحق يفقد قيمته إذا عجز صاحبه أن يقيم الدليل على مصدر هذا الحق، وإذا لم يقم الدليل على الحق ضاع وفقد، وأصبح هو والعدم سواء؛

لأن الحق بتجرد من قوته إذا لم يقم الدليل على ثبوته؛ لذلك يتعين تقديم الدليل على كل واقعة قانونية يدعى بها مهما كانت هذه الواقعة.

ويقوم النظام القانوني للإثبات برسم الإجراءات المتعلقة بتقديم الأدلة إلى القضاء تاركاً تحديد ما يعتبر من الأدلة ووزن وقوة كل منهما في الإثبات إلى سلطة القاضي التقديرية والقاعدة الفقهية (**البينة على من ادعى واليمين على من أنكر**).

فالبينة يقصد بها أي وسيلة يتم بها إثبات أو نفي أي واقعة متعلقة بدعوى، أو نزاع أمام المحكمين، أو الموفقين وفقاً لقانون الإثبات لسنة 1993م (3)

ويعرف د. محمد محي الدين عوض البينه بأنها " كل ما يقود إلى صحة، أو عدم صحة الواقعة، أو الوقائع موضوع التحقيق "(4)

ويجب أن تكون البينة منتجة في الدعوى وجائز قبولها (المادة 6 من قانون الإثبات 1993م)، والدعوى تشمل إي إجراء تؤخذ فيه البينة أمام المحكمة.

أما الواقعة محل الإثبات فهي " أي فعل أو شيء أو حالة أو علاقة بين الأشياء مما يمكن تكييفه بالحواس أو بالفعل " (المادة 13 من القانون).

وعملياً لا يمكن أن نتكلم عن دليل إثبات الكتروني دون تبيان وتحديد لماهية المعاملة الالكترونية ، أو الجريمة الالكترونية ؛ فبالرجوع لقانون الإثبات لسنة 1993م، فقد عرف (**المعاملات**) في المادة (4) بأنها :-" يقصد بها العلاقات والتصرفات المالية والأحوال الشخصية وسائر المسائل القانونية غير الجنائية".

أما القانون الجنائي لسنة 1991م ، فقد عرف (**الجريمة**) في المادة الثالثة بأنها : " تشمل كل فعل معاقب عليه بموجب أحكام هذا القانون أو أي قانون آخر".

ومن تعريف المعاملة أو الجريمة؛ فإن المعاملة والجريمة الالكترونية تدخلان ضمن المنسوج القانوني، ولكن هذا المنسوج التقليدي لا يستطيع أن يستوعب كل أنواع المعاملات الالكترونية، أو الجرائم الالكترونية؛ إذ يستلزم هذا التطور المعلوماتي قواعد قانونية متطورة موضوعية وإجرائية وإثباتيه؛ لذلك صدر قانون المعاملات الالكترونية 2007م، وقانون

الجرائم الالكترونية 2007م، وفى انتظار تعديل بقية القوانين لمواكبة التطور كقانون الإثبات، والمعاملات المدنية، والإجراءات الجنائية والمدنية.

إن مستخدمي الإنترنت عادةً ما يجهلون الشرعية المقررة في التعامل مع الحاسوب، والعقد الذي يحكم استخدام مواقع الويب (Websites)؛ لذلك فإن الأمر يجعل ملايين من البشر مسؤولين جنائياً، ومدنياً عن طريقتهم في إرسال البريد الالكتروني، وتصفحهم الويب، والتعدى على حقوق الآخرين؛ لذلك لابد من الحماية لاستقرار المعاملات التجارية، وغيرها من المعاملات بين الناس، وكذلك هناك عبء على مزودي الخدمات للانترنت بوضع تفسير للعقد بين الملاك والمستخدمين.(5)، **وهناك ضرورة** بالرجوع للقوانين الخاصة لمعرفة الوضع القانوني.

وبدأت الدول في إصدار تشريعات خاصة لمعاملات، وجرائم الحاسوب في نهاية التسعينيات (وبداية القرن العشرين)؛ وذلك لعدم ملائمة التشريعات النافذة آنذاك للاستجابة للأفعال غير المشروعة على الحاسوب، وقد جاءت هذه القوانين استجابة حقيقية لمشكلة قائمة خاصة في الأفعال التي تعد جرائم. وقد نتج عن استعمال الحاسوب، أيضاً كثير من المعاملات المدنية (عقود ومعاملات الكترونية) استدعت وضع قواعد قانونية لحفظ حقوق المتعاملين مع الانترنت.

ولا يمكن أن نتحدث عن قبول دليل الكتروني دون الإشارة إلى النص الموضوعي الذي يفسر لنا كثيراً من المصطلحات الحاسوبية التي تكون نافذة على أفعال إساءة استخدام الحاسب؛ لأنه بتطبيق القوانين القديمة ينتج عن ذلك عدم رضا من حيث نتائج النظام القانوني، بل لابد من سن تشريعات لجرائم الحاسوب، ونصوص أخرى إثباتية توضح طرق إثبات هذه الجرائم؛ لأن الإبقاء على تشريع قديم غير مواكب سوف يترتب عليه استخدام تشريعات ليست ذات علاقة، وقد لا تؤدي إلى إثبات المعاملة أو الجريمة؛ لذلك كان لا بد من وجود تشريعات تعرف على سبيل المثال الدخول غير المصرح به للانترنت؛ لأن القيمة الاجتماعية للانترنت تعتمد على وجود خليط من النماذج القانونية والتقنية التي تسمح لمستخدمي الانترنت بناء محيط من الخصوصية، والأمن بعيداً عن تدخل الغير. (6)

بل وجود مثل هذه القوانين يؤمن لمستخدمي الانترنت كيفية الاستخدام، وزيارة المواقع، وإرسال المراسلات الالكترونية دون خشية من احتمال الوقوع في إطار القانون الجنائي، والذي يبرز حال انتهاك اتفاق الخدمات سواء أكان الاتفاق بالاستخدام نفسه، أم أي اتفاق عقدي أخر، إذ يصبح مستخدمو الانترنت خاضعين للتنظيم القانوني سواء وفق قانون العقد، أو القوانين الجنائية.

ولكل ذلك صدر قانون المعاملات الالكترونية لسنة 2007م، وقانون الجرائم المعلوماتية لسنة 2007م ؛ إذ عرّف قانون المعاملات الالكترونية لسنة 2007م.

المعاملات الالكترونية: "يقصد بها العلاقات، والتصرفات المالية، والأحوال الشخصية، وسائر المسائل القانونية غير الجنائية بما في ذلك التصرفات الفردية، أو العقود التي يتم إبرامها، أو تنفيذها كلياً، أو جزئياً عن طريق رسالة البيانات الإلكترونية." (المادة 2 من القانون)، وعرف السند الالكتروني بأنه " المستند الذي يتم إنشاءه، أو تخرينه، أو استخراجه، أو نسخه، أو إرساله، أو إبلاغه، أو استلامه بوسيلة الكترونية ".

أما قانون جرائم المعلوماتية 2007م فلم يعرف الجريمة المعلوماتية، وإنما عرف المعلوماتية بأنها :" يقصد بها نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والانترنت والأنشطة المتعلقة بها ". ولذلك نرجع لتعريف الجريمة في القانون العام وهي "كل فعل معاقب عليه بموجب أحكام القانون الجنائي، أو أي قانون آخر".

وتتعدد المعاملات القانونية التي تتم عبر السند الالكتروني، والذي تم تعريفه بأنه محتوى أي اتصال يفترض عملية الكترونية لمعلومات رقمية عبر شبكات الاتصال المفتوحة للعموم أو المغلقة ، أو عبر وسيلة اتصال الكترونية يمكن الوصول إليها، أي قابلة للاستعمال في مراجعات لاحقة (7).

ومثل هذه المعاملات على سبيل المثال تلك التي نلجأ فيها إلى استعمال السند الالكتروني فيها، الشبكات الالكترونية، المحفظة الالكترونية، الدفع بواسطة التحويل المصرفي السحوبات النقدية والمالية الآلية، والتحويل عبر الانترنت، الدفع بواسطة استعمال بطاقات الائتمان الالكترونية والممغنطة، والمعاملات المتعلقة بالنقد الالكتروني،

والمعاملات التي تتم بواسطة الكمبيوتر عرض السلع والخدمات وشرائها، والتعاقد عبر الانترنت، العقود المتعلقة بالتجارة الالكترونية التي تتم عن بعد. وقد أظهر التطور تحديات قانونية تستلزم التنظيم لعقود تقنية المعلومات.

وجاء أيضاً قانون الجرائم الالكترونية بأنواع مختلفة للجريمة الالكترونية، وهي جرائم خاصة بالدخول في المواقع، وأنظمة المعلومات المملوكة للغير، والجرائم الواقعة على الأموال والبيانات، والاتصالات بالتهديد والابتزاز ، وجرائم الإخلال بالنظام العام والآداب، وجرائم الإرهاب والملكية الفكرية، وجرائم الاتجار في الجنس البشري والمخدرات وغسيل الأموال.

وعليه وبصدور هذه التشريعات يمكن تتبع الجرائم الالكترونية، والتى نص عليها المشرع وإثباتها ، كما يمكن استخدام الوسائل الالكترونية فى تحرير وتبادل المستندات، والعقود، وكافة التصرفات القانونية؛ إذ أعطى المشرع حجية للكتابة الالكترونية ، والتوقيع الالكترونى فى الإثبات.

2- الجرائم الالكترونية :

إذا تناولنا . على سبيل المثال . جرائم الحاسوب والتي سببت الأرق لكثير من رجال المباحث، فنشاط الجاني المادي قد يتعدى حدوده المكانية ، ويحقق نتائجه في دول أخرى، وتثور هنا مشكلة الاختصاص المكاني للجريمة والقانون الواجب التطبيق، واختصاص المحاكم في نظر الدعوى؛ لأن حدود المسئولية الجنائية تنتهي في نطاق الدولة التي أصدرت التشريع عملاً بمبدأ إقليمية الجرائم، كما يبرز أيضاً مبدأ شرعية الجرائم (لا جريمة، ولا عقوبة إلا بنص) ويتفرع عن هذا المبدأ حظر القياس في مجال التجريم، وعدم جواز التوسع في تفسير النصوص الجنائية .

وتثور مشكلة أخرى فإن هذه الجريمة سريعة التنفيذ، ولا تتطلب وقتاً كبيراً؛ فضغطة واحده على لوحة المفاتيح **(Keyboard)** يمكن أن نتنقل ملايين الدولارات من مكان إلى آخر، وهي تُعد من الجرائم المخفية، ولكن يمكن أن تلاحظ أثارها والتخمين بموقعها **(8)**. وهناك صعوبة في معرفة الطريقة التي يقوم بموجبها بها مجرمو الحاسب بتنفيذ

جرائمهم، والكيفية التي يخططون بها لتنفيذ هذه الجرائم، وبيان مستواهم الفني؛ لأن هذه الجرائم قد يسبقها تخطيط بعناية، وقد تكون للصدفة فيها دور مهم. وفي هذا المقام نرجع إلى سابقة حكومة السودان ضد عبد العزيز محمد أحمد حسن/ م ع/ف ج/ 130/ 2007م؛ إذ جاء على لسان مولانا العالم عبد الرحمن محمد عبد الرحمن شرفي بأنه (ليس من الضرورة أن يكون من اخترق موقعاً في الحاسوب، أو كلمة سر خبيراً عالماً، وإنما يمكن أن يكون هاوياً، وقد يكون محترفاً، كما أن مستوى الخبرة فيهم مختلفة ومتباينة، بعضهم لديه الخبرة، والبعض الآخر قليل الخبرة).

صحيح أن هناك تبايناً في سلوكيات مجرمي الحاسب الآلي، ودوافع كل منهم ورغباتهم ومهاراتهم، وهذه الجرائم لا تتطلب استخدام أدوات وعنف كالجرائم التقليدية، فنقل بيانات من حاسب إلى آخر، أو السطو الالكتروني على أرصدة بنك لا يتطلب أي عنف، ولكنها في الوقت ذاته تُعد من الجرائم الصعبة الإثبات، عكس الجرائم التقليدية؛ وذلك لافتقار وجود الآثار التقليدية للجريمة، وغياب الدليل المادي الظاهر (بصمات، تخريب، شواهد مادية) مع سهولة محو الدليل، أو تدميره في زمن قصير، وكل ذلك مع نقص في خبرة النظام العدلي، وعدم كفاية القوانين المتاحة لضبط الجريمة الالكترونية، كقانون الإجراءات الجنائية الذي ينظم عملية التحري في هذه الجرائم، وقانون الإثبات الإلكتروني.

ويعد عدم التدريب، أو الخبرة أكبر مهدد لأمن الحاسب؛ لأن وجود شرطة، أو نيابة غير مدربة، أو قضاء غير مؤهل . قد يودي إلى تبديد أكبر في المعلومات، والعبث بأنظمة التشغيل والتعطيل.

وهناك صور وأنواع عديدة من جرائم الحاسب، ويمكن تصنيفها إلى أربع فئات على النحو الآتي:

أ- المجموعة الأولى: تشمل الجرائم التي تتمثل في استغلال البيانات المخزنة على الحاسوب بشكل قانوني، ومنها الدخول إلى شبكة الحاسوب التي تحمل أرقام بطاقات الائتمان البنكية من خلال استخدام الحاسوب الشخصي، فيطلب مرتكب الجريمة رقماً

معيناً، ويطلب من الحاسوب الحصول على مبلغ معين من النقود تحت هذا الرقم، ولا يمكن كشف هذه الجريمة إلا إذا كان هناك تشابه في أسماء أصحاب هذه الأرقام.

ب- المجوعة الثانية : الدخول في البرامج واختراقها لتدميرها، وتدمير البيانات الموجودة في الملفات المخزنة عليها . **مثال** : يقوم موظف في مشروع بوضع جملة معينة للبرنامج الحاسب، وعندها يتم تنفيذ هذه الجملة عبر تشغيل البرنامج، و يتم مسح كل الملفات المرتبطة بالبرنامج.

ج- المجموعة الثالثة: وبها يتم استخدام الحاسوب بشكل غير قانوني من قبل الأفراد المرخص لهم باستخدامه: **مثال** قيام بعض الموظفين في الشركات والمؤسسات باستخدام الحاسوب في بعض الأغراض الشخصية غير المرتبطة بالعمل الرسمي. ومثال آخر جرائم التعدي على حقوق الملكية الفكرية.

د- المجموعة الرابعة: تشمل الجرائم التي يتم فيها استخدام الحاسوب لارتكاب جرائم معينة، أو التخطيط لها، **مثال:** قيام أحد الموظفين في إحدى الشركات التي تجرى سحباً (يانصيب) بتوجيه الحاسوب اختيار أرقام معينة تمثل الأرقام الفائزه في السحب.(9)

وقسمت الجرائم أعلاه إلى:

أولاً- جرائم تقليدية ترتكب باستخدام الحاسوب، (كل نماذج الاحتيال عبر الانترنت)، هذه الجرائم تتم بسهولة، وأساس الجريمة يظل في حاله بصرف النظر أنها ارتكبت عبر الانترنت، **مثلاً:** فإن التهديد يظل تهديد بالفعل بصرف النظر عما إذا تم بإرسال مكالمة الكترونية بالتهديد الالكتروني، أو بمكالمة هاتفية.

ثانياً- القسم الأخر وهي جرائم إساءة استخدام الحاسوب التي تبرز نوعية جديدة من الجرائم تقوم بطرح تحديات جديدة أمام القانون الجنائي والإثباتى، وهذه الأفعال ترتكب عن علم وإدراك وطيش وإهمال بما تسبب عنه تداخل، أو تشويش على الوظيفة الصحيحة للحواسيب وشبكات الحاسوب، من الأمثلة اختراق الحواسيب، وبث الفيروسات، وإغراق الخوادم، **مثال:** في حالة قيام أحد الدخلاء بتخمين كلمة العبور التي تخص مالك الموقع، وقراءة مراسلاته الشخصية، فإن ذلك يعد انتهاكاً لحقوقه بحيث أنها لم تعد خاصة، ومؤمنة، وبهذا يعد انتهاكاً لحقوق وامتيازات تقرر ضمانها للمالك عندها يحصل على الموقع.**(10)**

وهذا النوع من الجرائم وغيرها تترتب عليه أضرار خطيره، وقد ينتج عنها انتهاك للخصوصية، بالإضافة إلى الخسائر الاقتصادية. وقد يتمكن الجاني من تغيير وإتلاف للمعلومات عن طريق اختراق غير مأذون فيه لبنوك المعلومات وقواعدها. وقد استخدم المجرمون أوجه التقدم العلمي والتكنولوجي في ارتكاب جرائمهم، واستغلوا معرفتهم بهذه التكنولوجيا؛ فتدخلوا بطرقهم غير المشروعة في العمليات المالية والمصرفية بهدف الإثراء الفاحش بطريق الغش بتحويل مبالغ ضخمة لمصلحتهم الشخصية؛ لذلك لابد من أن تواكب القاعدة الإثباتيه هذه الجرائم لإمكانية محاربة هذه الجرائم، وتطويق النشاط الإجرامى.

ولكن رغم ذلك فإن تكنولوجيا المعلومات أصبحت تشكل جزءاً أساسياً في الحياة اليومية، وأصبحت الحاسبات آداة منتشرة لا يمكن الاستغناء عنها في مختلف المؤسسات، كما أن تأثيرها واضحاً في محتوى، وشكل تلك النشاطات اليومية، وعلى تطوير العالم والصناعة ، وعلى عمل المنظومة الرسمية، وأنظمة الاتصالات، والبحث العلمي عموماً فهي تؤثر في شكل الحياة الحديثة، مع ضرورة التأكيد بفوائد هذه التكنولوجيا للحكومات، وقطاع الأعمال، والدراسيين، وللمواطن العام؛ لذلك لابد أن تفعل هذه القوانين المتعلقة بنظم الاتصال والتقنية؛ لمواكبة التطور والحداثة الرقمية. فالمعلومات المنسابة عبر وسائط أجهزة الكمبيوتر، وشبكات الانترنت أصحبت عرضة للانتهاك، ووسيلة تهديد لمستهلكي هذه الخدمات من قبل بعض أصحاب النفوس الضعيفة، وأصبح المستهلك لها عرضة في حياته، وماله، وسمعته للانتهاك. لذلك فإن عمليات كشف وتجميع الأدلة لإثبات وقوع الجرائم الالكترونية، والتعرف على مرتكبها. هو أحد أبرز المشكلات التي يمكن أن تواجه سلطات التحري؛ فعلى سبيل المثال: جرائم البريد الالكتروني حيث يكون من الصعب على سلطات التحري تحديد مصدر المرسل، أو المتهم الفعلي، والبحث عن دليل، أو أثر تقليدي، وكذلك جريمة التزوير الالكتروني فلا يمكن ضبط المحرر المزور كما يحدث في التزوير المادي التقليدى؛ فهناك صعوبة في ضبط المحرر المزور الالكتروني بجانب سهولة محو الدليل، أو تدميره.

وإليكم بعض الأمثلة للتأكيد على اختلاف في أنواع الجرائم، ومن ثم ضرورة استعداد سلطات التحري لإثبات هذه الجرائم:

مثال أول: تخمين كلمة العبور: أراد أحد الأشخاص ولخشيته من خداع صديقته، أو مخطوبته له ـ أراد أن يرى ما يوجد في حساب بريدها الالكتروني ؛ فقام بالدخول إلى مزود خدمات الانترنت الخاص بصديقته، ووضع اسم استخدام، وبدأ في تخمين كلمة العبور **(Password)** واستطاع في النهاية تخمين كلمة العبور الصحيحة ، ومن ثم قراءة المراسلات الالكترونية الخاصة بها. وقد قام هنا بالدخول باحتيال شخصية صديقته؛ إذ اعتقد الحاسوب أن صديقته هي التي قامت بإدخال كلمة العبور والتصريح ، وبذلك يكون مسئول عن الدخول غير المصرح به .

مثال ثاني : موظف في شركة أدوية ترك العمل، وأراد أن ينافس العمل السابق، وقبل رحيله قام بنسخ ملفات معينة من الشركة على قرص مرن **(CD)** وأخذها معه. هذا المسؤول عند دخوله على الحاسوب ، دخل بطريقة مشروعة؛ لأنه كان يعمل لدى الشركة، ولكنه عند النسخ كان في نيته الإضرار بالشركة ؛ فهو غير مسموح له بالنسخ إلا بعد إذن مشروع من صاحب الشركة.

مثال ثالث: قام موظف مبرمج حاسوب، ولغضبه من صاحب عمله لعدم منحه ترقية . بإلغاء بعض ملفات الشركة ذات الأهمية؛ وذلك بارتكاب هجوم إغراق الخادم لكي يغير خادم الويب بطلبات يتم أخذها خارج الخط **Offline** .

مثال رابع: قام شخص بكتابة فيروس **(Virus)** حاسوب بهدف توزيعه كملصقة بمراسلة الكترونية، وفيه يقوم المستقبل بالنقر على الملصق فينزلق البرنامج ، ويقوم بإرسال المراسلات الالكترونية خارج الحاسوب إلى كل عنوان بريد الكتروني من دفتر عناوين المستقبل، قام هذا الشخص بإرسال الفيروس، وأصاب عشرات الآلف من الأجهزة.

وفيما يتعلق بالممارسات الخاصة بنسخ برامج الحاسب الآلي المختلفة والتي لم تسقط في الدومين العام بعد، ونقلها إلى الغير دون إذن صاحبها يُعد هذا اعتداء على الملكية الأدبية والفكرية، ويشكل هذا الفعل جريمة؛ لأن من قام بالتقليد والنسخ غير ذي الصفة. **(11)**

وكل هذه الأشكال داخلة في الجريمة الالكترونية، وهي أعمال إجراميه يُعدُّ لها باستخدام أجهزة الحاسوب، وشبكات الحاسوب، وتقنيات الاتصالات بغرض إحداث دمار في البنية التحتية، أو السرقة، أو التهديد.....ألخ للحكومات والمواطنين **(12)**، وتحتاج إلى يقظة من سلطات التحري لإثبات هذه الجرائم.

أما فيما يتعلق بالتجارة الالكترونية **(E-Commerce)** فقد اتفق فقهاء القانون على أنها لا تختلف عن التجارة التقليدية سواء من حيث الوسيلة المستخدمة لإجراء المفاوضات، وإبرام العقود والتي يتم عبر شبكة الانترنت، سواء دولياً، أو محلياً، ولكن تواجه هذه التجارة مشكلات خاصة بحماية المواقع وصحف الانترنت من الاختراق والتبديل أو التعديل والاطلاع على المعلومات الخاصة والأسرار التجارية . ويتم الاختراق باستخدام أجهزة تصنت، أو الحصول على البيانات والمعلومات الموجودة عبر طريقة خطوط تحويلية ترسل إشارات الكترونية بواسطتها تُسرق المعلومات، أو يتم نسخ أو تدمير بعض المعلومات المتعلقة بالتجارة الالكترونية، أو سرقة المعلومات الخاصة في مجال الملكية الفكرية، والإعتداء على الأسماء التجارية والشركات، وعقد صفقات بأسمائها عن طرق الغش، وكل هذه التصرفات تلقى عبئاً كبيراً على اللجنة القومية لتصديق التوثيقات للكشف ومتابعة هذه الجرائم، وكذلك سلطات النيابة والمباحث لتتبع الدليل الإلكتروني.

3- المعاملات الالكترونية:

عرفت المعاملات الالكترونية بأنها: " العلاقات والتصرفات المالية والأحوال الشخصية ، وسائر المسائل القانونية غير الجنائية بما في ذلك التصرفات الفردية ، أو العقود التي يتم إبرامها ، أو تنفيذها كلياً ، و جزئياً عبر طريق رسائل البيانات الالكترونية". (13)

وقد انتشرت المعاملات الالكترونية فى الأونة الأخيرة على النطاق الدولى ، ومن هذه المعاملات التجارة الالكترونية ؛ حيث أسَست كثير من الشركات مواقع خاصة بها على شبكة الانترنت.

ومن أهم تطبيقات هذه المعاملات ـ أيضاً ـ ما يسمى بالحكومة الالكترونية، والتي تشمل جميع المعاملات الإدارية الحكومية ، وخدمات المواطنين بشكل عام، والتصاريح

المختلفة، والخدمات التي تقدمها الجمارك، والضرائب، والسجل المدني، والخدمات الاستثمارية والتى تتم عن طريق المحررات الالكترونية التي تصدرها هذه الجهات، ويتم توقيعها من قبل الموظفين العموميين ؛ مما يضفي على المحرر صفة المحرر الرسمي بسبب قيام الموظف العام بتوقيعها الكترونياً. (14)

كما يشمل التعريف جميع المعاملات التجارية الالكترونية، والتى هى كل معاملة ذات طابع تجاري في مختلف المعاملات، مثل عقودات البيع والإيجاره، وغيرها من العقود، والتصرفات القانونية التجارية، والاستيراد والتصدير، والتعامل مع وكالات السفر، وحجوزات الفنادق وجميع المعاملات المصرفية، وكل المعاملات التي تتم في شكل محرر الكتروني موقع توقيعاً الكترونياً، وعليه فإن هذه التعاملات بحاجة إلى قوانين وضعية وإجرائية و إثباتية لتنظيم هذه التصرفات، والعلاقات لحماية المتعاملين عبر شبكة الانترنت.

وقد جاء في دراسة أعدها الأستاذ حسن أحمد الحاج بابا بأن أنواع المعاملات الالكترونية هي:

أ- معاملات الشبكات الداخلية .

ب- معاملات قواعد البيانات ونظم المعلومات .

ج- معاملات الشبكات العامة المتشاركة .

د- المعاملات المصرفية الإلكترونية .

هـ- معاملات الإنترنت.

فالعقود الالكترونية هي العقود التي تتم عبر الوسائل والآلآت التي تعمل عن طريق الوسائل الالكترونية ، ويتم التعاقد عبر البريد الالكتروني ، أو شبكة المواقع ، والتعاقد عبر المحادثة والمشاهدة . ويُعد الانترنت وسيلة لتوصيل الكتابة .

ويُعد التوقيع الالكتروني حجز الزاوية في المعاملات الالكترونية ووسيلة إثبات ، سواء المعاملات الحكومية ، أم التجارية أم الإدارية ، ويمكن استخدام الوسائل الالكترونية في

تحرير وتبادل وحفظ المستندات ، مما يحفظ حقوق المتعاقدين ، ويضمن مصداقية وقانونية المعاملات الالكترونية وفق أحكام القانون .

ثانياً- الحجية :

1- حجية السجلات الالكترونية .

يتم استخدام الوسائل الالكترونية في تحرير وتبادل وحفظ المستندات؛ لتنظيم وإتمام العملية التبادلية بما يحفظ حقوق المتعاملين، ويضمن مصداقية السجل الالكتروني. وأصبحت العديد من العقودات ـ الآن . تتم عبر شبكة الانترنت فيما أصبح يعرف بالعقودات الالكترونية ، وكان لابد من وجود حجية، أو قيمة للكتابة الالكترونية. وكان قانون الإثبات لسنة 1993م قد عرَّف المعاملات بأنها "االعلاقات، والتصرفات المالية، والأحوال الشخصية، وسائر المسائل القانونية غير الجنائية "، ولكن لم يحدد القانون الوسيلة التي تتم بها المعاملة، ولأن البينة يقصد بها أي وسيلة يتم بها إثبات أو نفي أي واقعة متعلقة بدعوى، أو نزاع أمام المحكمين، أو الموفقين . فلا مجال للقول بعدم قبول البينة الالكترونية فى الإثبات .

ولكن بصدور قانون المعاملات الالكترونية لسنة 2007م، فقد نص هذا القانون . على سبيل المثال . في المادة الرابعة على حجية العقود الالكترونية ونفاذها عند ارتباط الإيجاب بالقبول عبر رسالة البيانات التي يتبادل فيها المتعاقدان التعبير عن إرادتين متطابقتين على وجه يثبت أثره في المعقود عليه، ويترتب عليه التزام كل منهما بما وجب عليه للأخر.

كما يجوز لطرفي العقد . وعلى الرغم من النص أعلاه . أن يتفقا على أن يكون العقد صحيحاً، ونافذاً، إذا تم التعبير عن الإرادة جزئياً عبر رسالة البيانات.

وقد أعطى المشرع السجلات الالكترونية الأثر القانوني، من حيث اعتماد الصحة وإمكان العمل بمقتضاها سواء صدرت في شكل كلي أو جزئي. وأعطى المشرع المعلومات في السجل الالكتروني نفس أثر المعلومة المتطلبة قانوناً إثباتها بالكتابة بشرط أن تكون

المعلومة قابلة للوصول إليها، واستخراجها لاحقاً عن طريق البث، أو الطباعة ، أو غير ذلك، ولقد اشترط للإيفاء بهذا الغرض :

أ- أن يتمكن المرسل إليه من الدخول على المعلومات، واستخراجها لاحقاً سواء عن طريق البث، أو الطباعة، أو غير ذلك.

ب- أن يتمكن المرسل إليه من حفظ هذه المعلومات بما يمكنه من التحقق من منشأ رسالة البيانات، وجهة وصولها، وتاريخ ووقت وصولها، وارسالها واستقبالها.

وعند تقدير حجية السجل الالكتروني في الإثبات، عند النزاع في سلامة ما يلي :

أ- مدى الثقة في الطريقة التي يتم بها إنشاء، أو حفظ، أو بث السجل الالكتروني.

ب- مدى الثقة في الطريقة التي يتم بها توقيع السجل الالكتروني

ج- مدى الثقة في الطريقة التي استعملت في المحافظة على سلامة المعلومة التي تضمنها السجل الالكتروني .

د- أية أمور أخرى ذات علاقة بسلامة السجل الالكتروني . (15)

وبهذا أصبح للسجل أو المستند الالكترونى حجية فى الإثبات ، الأمر الذى يتطلب تعديل المادة "36" من قانون الإثبات 1993م لتدخل الكتابة الالكترونية ضمن المستندات، ومن ثم يمكن تطبيق النصوص الخاصة بالمستندات كتعريف المستند الرسمى والعرفى، وحجية صور المستند علماً بأن جميع صور المستند الالكترونية تعد جزءاً من الأصل؛ إذ يمكن استخراج مئات من أصل المستند دون جهد، ولكن يبقى هناك ضرورة فى النص على طرق الطعن فى السجلات والمستندات الالكترونية. ونحن نرى ضرورة إعادة النظر فى جميع القوانين ذات العلاقة لمعرفة أوجه النقص فى التشريعات للتعديل، وإضافة نصوص جديدة تكفل الحماية القانونية للمتعاملين عبر الشبكة الالكترونية.

2- الدليل الرقمي (Degital Evidence):

إذا تكلمنا عن الدليل الرقمي فإنه الدليل الكامن في العالم الافتراضي؛ لذلك فإن هذا الدليل في حاجة إلى الاهتمام به وأساليب استنباطه و تأمينه؛ ففي الجريمة الالكترونية مسرح الجريمة هو جهاز أو أجهزة الحاسوب التي يتم فيها الفعل الذي يشكل جريمة بموجب القانون، أما المعاملة الالكترونية فهي مختلف التصرفات التي تتم عبر شبكة الانترنت .

ويُعد الدليل المستمد من مسرح الجريمة نوعاً من أنواع الأدلة الرقمية، بجانب الأدلة المتعارف عليها في المجال الجنائي.

وقد عرفت البينة الالكترونية قانوناً بأنها " المعلومات والبيانات ذات القيمة في أي تحقيقات جارية ومخزنة، أو المنقوله، أو المعالجة بواسطة الأجهزة الالكترونية ".**(16)** .

ويتكون الدليل الالكتروني من دوائر وحقول مغناطسية ، ونبضات كهربائية غير ملموسة؛ وللاستفادة من هذا الدليل الموجود في الحاسب على القرص الصلب، أو على القرص المرن، وحتى يصبح مستنداً الكترونياً متضمناً كافة المعلومات التي تم نشرها على الشبكة . يجب تعريفه، وتوثيقه، وطباعته، وتخزين نسخة منه، وتحريزه بالقدر الذي يوفر له المصداقيه، ويحمي الدليل من أي طعن بسبب سوء التعامل معه؛ لذلك من الضروري تدريب وكلاء النيابة، ورجال الشرطة تدريباً عالياً لمعرفة كيفية استنباط الأدلة القانونية التي يمكن قبولها أمام المحاكم، فهذا النوع من الأدلة يحتاج إلى دراية خاصة؛ لأنه قد لا تترك الجريمة المعلوماتية أثراً، ولكن هذا لا يمنع من معاينة مسرح الجريمة (بتصوير الحاسب وتصوير كل ما يمكن تصويره).

وتتمثل الأدلة الالكترونية في كلمات المرور، وأسماء المستخدمين، البصمة عبر الأجهزة الالكترونية ، المواد الإحيائية ، والتوقيع الالكتروني **(17)**.

وقد قسم الدليل الرقمي إلى ثلاث مجموعات وهي:

1- السجلات المحفوظة في الحاسوب، وهي الوثائق المكتوبة، والمحفوظة، مثل البريد الالكتروني، وملفات برامج معالجة الكلمات، ورسائل غرف المحادثة على الانترنت.

2- السجلات التي تم إنشائها بواسطة الحاسوب، وتُعد مخرجات برامج الحاسوب ، وبالتالي لم يمسها الإنسان، مثل Log Files، وسجلات الهاتف، وفواتير أجهزة السحب الآلي ATM .

3- السجلات التي جزء منها تم حفظه بالإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسوب، ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل، مثل Excel، ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها. **(18)**

ولا خلاف بأن الأدلة الكتابية كانت تحتل مركزاً مرموقاً بين وسائل الإثبات في التشريعات؛ إذ تعد من أقوى الوسائل؛ إذ يعد الدليل الكتابى، أو المحرر للإثبات منذ البدء، فتدون فيه دقائق التصرفات القانونية وتفصيلاتها؛ مما يقلل عناء القيام بعبء الإثبات عند حدوث النزاع، وهذا هو سبب عناية التشريعات بالكتابة والتوثيق **(19)**. بل نص قانون الإثبات 1983م فى المادة(2/38) على أنه: "لا تقبل الشهادة لتقديم ما يجاوز المستند، أو يعدل، أو يعارض ما اشتمل عليه المستند إلا استثناءً فى حالات محددة، وعليه يثور التساؤل . رغم النص أعلاه . عن قوة الكتابة الالكترونية فى الإثبات، ونجيب بأن قانون المعاملات الالكترونية أعطاها نفس قوة الكتابة التقليدية، بشرط التقيد بمتطلبات القانون، أى إن هناك شروط شكلية يجب توافرها لاكتساب نفس الحجية.

3- طرق جمع الأدلة:

من سمات هذا العصر هي التحولات الكبيرة في كل مجالات الحياة، وقد بدأ الإنسان باستخدام تقنيات حديثة؛ الغرض منها توفير الجهد والزمن، والاتقان في الجودة والنوعية.

والعالم يتطور كل يوم وتزيد التقنيات، وتزيد التعقيدات، وتتسارع التحولات من حولنا؛ فهناك تطور مستمر في مجال العلم، وهنا منافسة قوية لتصريف المنتجات وترويجها عن طريق الانترنت، وهناك أبحاث في مجالات مختلفة، وهنا حركة بشرية متنامية في مجال التطور، ويصاحب ذلك تعاقدات والتزامات.

وفي مقابل ذلك هناك أفعال تشكل تهديدات خطيرة لأمن هذا المجتمع لدقتها، وصعوبة كشفها، وحداثتها، وضعف الثقافة فيها، بل قد استغل البعض معطيات العصر لمصالحهم الأنانية المحضة، فظهرت مشكلات أمنية جديدة حملت الأجهزة العدلية أعباء جديدة لمكافحة مثل هذه الأفعال، وهي تحديات تواجه أجهزة العدالة في مرحلة تعاني فيها الدولة، وهذه الأجهزة من أمية معلوماتية؛ لأننا بحاجة حقيقة لإثبات هذه الجرائم،

وإلى الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها. وهذا الوضع يتطلب وجود قدر كبير من التعاون والثقة بين أجهزة تنفيذ القانون المختلفة والمؤسسات التي تقوم بتقديم خدمة المعلومات والاتصالات لتمكين الأجهزة العدلية من توثيق الدليل الرقمي لحفظه إلى حين انتهاء الإجراءات أمام المحكمة. و يتم التوثيق بعدة طرق : كالتصوير الفوتوغرافي، التصوير بالفيديو، والخرائط الكروكية، وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص.

وعند حفظ الأدلة الرقمية على الأقراص يجب تدوين البيانات الآتية :

أ- التاريخ والوقت.

ب- توقيع الشخص الذي قام بإعداد النسخة.

ج- اسم أو نوع نظام التشغيل.

د- اسم البرنامج أو الأوامر المستعملة لإعداد النسخ.

هـ- المعلومات المضمنة في الملف المحفوظ.

و- رسالة التصديق والتوقيعات الرقمية.

وبعد ذلك يتم تقييم للأشياء التي وجدت في مسرح الجريمة للبحث حول إيجاد علاقة بين الجاني، ومسرح الجريمة **(20)**.

وتُجمع جمع الأدلة على مرحلتين بواسطة سلطات المختبرات الجنائية:

* **القسم الميدانى:** أو ما يسمى بمسرح الجريمة، والذى منه تنبثق كافة الأدلة المادية، ومن خلالها يمكن الاستدلال، والاستنتاج، والاستنطاق.

* **القسم المخبرى:** وهنا يتم تحصيل الدليل، وكتابة التقرير حوله وتقديمه للمحاكم بدرجاتها المختلفة. **(21)**

وقد استقر الفقه والقانون بأن للقاضي سلطة واسعة في تقدير الأدلة، واستنباط القوانين، وما تحمله الوقائع من دلالات شريطة أن يكون الدليل ثابت على درجة اليقين، ومرتبطاً بالواقعة الرئيسة منسجماً مع التسلسل المنطقي للأحداث، وينسحب ذلك على

الأدلة الرقمية، والتي تعد من الأدلة المادية العلمية؛ لأنها محكمة بقواعد علمية، وحسابية قاطعة لا تقبل التأويل، وهي معالجة بوسائل تقنية معلوماتية؛ الأمر الذي يتطلب درجة عالية من المعرفة، والإلمام بتفاصيل عمليات تقنية المعلومات، والاتصالات في جميع المراحل ابتداءً بمرحلة تلقي البلاغ؛ حيث يتطلب الأمر الوقوف على مسرح الجريمة، والمحافظة عليه، والتحفظ المؤقت على الأدلة، ثم مرحلة التحري لإيجاد علاقة بين الجاني والجريمة، ثم مرحلة التأمين على الأدلة، بحفظ هذه الأدلة . ومرحلة الاتهام والادعاء حيث يقوم وكلاء النيابة في الجنايات بتقديم الأدلة لإحالتها إلى المحكمة، ثم مرحلة المحاكمة حيث يقوم القضاء بالوقوف على الأدلة لتقييم مدى كفايتها لإثبات التهمة بما لا يدع مجالاً للشك أو نفيها .

أما في مجال المعاملة الالكترونية فعلى الأطراف تقديم مستنداتهم الالكترونية سو أكانت عقداً، أم أى معاملة لإثبات الادعاء، أو نفيه وفق قواعد الإثبات في القانون المدني، ويفي التوقيع الرقمي بمتطلبات القانون، وفي حالة وجود أي إجراءات قانونية، فإن تقديم توقيع رقمي مقرون بشهادة معتمدة لأي شخص، فإن ذلك التوقيع يكون معادلاً لتوقيعه اليدوي وذلك بشرط:

أ- استخدام آلية لتحديد هوية الشخص، والتدليل على موافقته على المعلومات الواردة في رسالة البيانات الالكترونية.

ب- تكون تلك الآلية مما يعتمد عليه بالقدر المناسب للغرض الذي أنشئت من أجله رسالة البيانات الالكترونية، على ضوء الظروف بما في ذلك أي اتفاق آخر متصل بذلك الشخص.

وفي حالة عدم وضع التوقيع الالكتروني باستعمال شهادة معتمدة . فإن قرينة الصحة لا تلحق أياً من التوقيع، أو السجل الالكتروني. **(22)**

وتفقد أدلة الإثبات قوتها إذا تعرضت لأي من الأخطاء التي يمكن أن تحدث في قيمة العناصر الأولية عند إدخالها في الحاسب، أو تحديثها، أو عند تخزينها، و عند إجراء بعض التعديلات عليها.

ويجب وصف الحالة ووصف المواد دون نقلها إن كان نقلها يؤدي إلى محو البيانات التي تم تسجيلها، مع مراعاة اتباع كل القواعد الفنية المتعلقة بكيفية نقل الإحراز المعلوماتية، وحملها، وتأمين البرامج المضبوطة قبل تشغيلها، وعمل نسخ سليمة وكاملة منها، وأحكام ضبط هذه المادة بعلامات مادية لإمكان التعرف عليها، ومن ثم بعد ذلك تقديمها للمحاكم لإثبات الدعاوى. ولكن لا يمكن تفعيل هذه الحماية إلا إذا حدث تدريب كافي للنيابة والشرطة والسادة القضاة على أساليب التحقيق الحديثة، وتدريب رجال الشرطة على الأساليب الحديثة لجمع الأدلة، ومعرفة طرق التفتيش التي لا تضر بآثار جرائم الحاسب، مع كيفية تأمين البرامج المضبوطة قبل تشغيلها؛ لأن جرائم الحاسب هي جرائم معظمها مخفية، إلا أنه يمكن أن نلاحظ آثارها والتخمين بوقوعها أحياناً، ولكن غالباً ما تكون صعبة الإثبات لافتقار وجود الآثار التقليدية للجريمة، وغياب الدليل المادي، ولسهولة محو الدليل في زمن قصي . فتدريب الأجهزة العدلية يعد من عوامل مكافحة هذه الجرائم؛ لأن المجرم سوف يراجع نفسه كثيراً قبل الإقدام على الفعل غير المشروع. راجع سابقة محاكمة عبد العزيز محمد أحمد حسن /م ع/ف ح/ 2007/130م(غير منشورة)؛ إذ قضى ببراءة المتهم؛ لأن التحقيق لم يتم بالشكل العلمي حسب ما أورده القاضي العالم مولانا /عبد الرحمن محمد عبد الرحمن شرفي . كما ذكرنا سابقا– وكان المتهم قد أُتهم باستخدام الرقم السري للشاكي، وقام بأخذ أموال المشتركين مسبباً كسباً غير مشروع لنفسه، وخسارة للشاكي حيث كان المتهم يعمل لدى شركات الخدمات، ويقوم بتحصيل إيرادات الشركة، ويودعها في حساب الشركة عن طريق الحاسوب الذي هو تحت إشراف الشاكي ومسئوليته، وعن طريق الغش تحصل على كلمة السر **(Password)** الخاصة بالشاكي، وقام بتحويل مبلغ ثلاثة وثلاثين مليون جنيه إلى حساب وهمي؛ إذ حصل عليها ، وحولها لمصلحته. لم يستطع الاتهام، وهو المناط به عبء إثبات الدعوى تقديم البينة ؛ لذلك قضى ببراءته .

والمتفق عليه أن هذه الجرائم كانت آثاراً للتقنية الالكترونية، وهذه التقنية ذاتها قادرة على إيجاد الحلول على ما خلفته من مشكلات، لذلك يجب تشجيع البحث المستمر في هذا المجال.

وكمثال فإن تقنية الهاتف النقال (**Mobile Phone**) أوجدت مشكلة المعاكسات الهاتفية في محيط الشباب، ولم تفلح العقوبات في ردعها، إلا أن المشكلة قد حلت بإدخال خدمة إظهار الرقم.

لذلك علينا ألا نقف تجاه هذا التطور موقف جامد، بل يجب الإسراع في إجازة القوانين الموضوعية اللازمة لحماية المعلومات والمعدات اللازمة للتشغيل والتوصيل وكيفية حماية المواقع وأسماء النطاق؛ لإثبات هذه المعاملات وأي أفعال تتم الكترونياً، خاصة وأن التقنيات الحديثة، والتي تتيح المعلومات في كافة المجالات يجب أن تستفيد من هذه المعلومات بواسطة الخبير المختص، فليس هناك ما يمنع أن نستفيد من هذه التطورات العلمية في خدمة تحقيق العدالة.

وقد يرى البعض أن السودان لم يعانِ من هذه الظواهر بدليل عدم وجود أفعال متعلقة بالحاسب الآلي كثيرة، ولكنني . كباحثه في هذا المجال . أردُ لكثير من الدارسين في مجال الملكية الفكرية، والذين يأتون إلى لمعرفة التجربة القضائية في جرائم الحاسب الآلي . بأن عدم وجود سوابق قضائية لا يعني عدم وجود المشاكل المتعلقة بالحاسب الآلي، أو وجود جرائم الكترونية، فهي ترتكب يومياً، وقد تكون بقصد، أو بدون قصد، ولكن للجهل بالتعامل مع الحاسب في قطاعات كبيرة، ومهمة كالنيابة، والشرطة، والقضاء- فإن كثيراً منها لم يتم ضبطه، **مثال** (نسخ برامج الكمبيوتر، الدخول في مواقع أخرى بدون إذن صاحبها وغيرها من الأفعال غير المشروعة)؛ لذلك لابد من رفع الوعى لدى جميع المؤسسات بضرورة رفع قدرات العاملين فى هذا المجال.

ولذلك لا بد من وجود مؤسسات مختصة في التحقيق في جرائم الحاسب الآلي، وجمع الدليل الالكترونى، ووجود شرطة مختصة، ومحاكم مختصة؛ لأن المتهم غالباً ما يستند إلى خبرته ومهاراته المتخصصة في مجال خدمات الحاسوب؛ لذلك فإن توجيهه إلى الهدف يكون دقيقاً، وهذا يتم غالباً في الجرائم الكبيرة، وقد جاء فى قانون الجرائم الالكترونية 2007م فى(المادة28) بأن ينشىء رئيس القضاء محكمة، وفقاً لقانون الهيئة القضائية 1986م محكمة خاصة للجرائم المنصوص عليها فى القانون، كما جاء فى المادة (29) بأن تنشأ بموجب أحكام قانون تنظيم وزارة العدل1983م نيابة متخصصة لجرائم المعلوماتية. أما المادة(30) فقد نصت

على أن تنشأ بموجب أحكام قانون الشرطة1999م شرطة متخصصة لجرائم المعلوماتية ، لذلك هناك ضرورة أولاً من إنشاء هذه الآليات لتنفيذ القانون وفق أحكامه ، ثم القيام بتدريب جميع كوادر هذه الآليات.

وكذلك نحن بحاجةٍ إلى أجهزة مساعدة في مكافحة هذه الأفعال لتأمين المعاملات الالكترونية، ووضع أسس لمنح التراخيص للمواقع، مع تحديد هوية العميل. مع الاهتمام بنظام التشفير ، والذي يغير من شكل الرسالة إلى لغة غير مفهومة لا ترجع إلى طبيعتها إلا بمعرفة مفتاح الشفرة .

ويجب احترام سرية المعلومات، وعدم إفشائها، أو السماح للغير بالاطلاع عليها، وإذاعة محتوياتها. وقد نص القانون على سرية المعلومات بحيث تكون بيانات التوقيع الالكتروني، والوسائط الالكترونية، والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها . بحكم عمله . إفشاؤها للغير، أو استخدامها في غير الفرض الذي قدمت من أجله.

ويجب على مقدم الخدمة الحائز على نظام معالجة البيانات اتخاذ التدابير، والإجراءات التي تكفل حماية وتأمين المعلومات بكافة الوسائل والتقانات المتاحة.

وهناك جانب آخر، وهو فيما يتعلق بالتجارة الالكترونية، هناك إلزام على الجهات المنظمة والمرخصة فيما يتعلق بنظم التوقيع الالكتروني، وبيانات التوقيع الالكتروني، والوسائط الالكترونية، والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني أن تلتزم بالسرية، ولا يجوز لها أي لمن قدمت إليه هذه المعلومات، أو اتصل علمه بها . بحكم عمله . عدم إفشائها للغير، أو استخدامها في غير الغرض الذي قدمت من أجله. وتفقد أدلة الإثبات قوتها إذا تعرضت لأي من الأخطاء التي يمكن أن تحدث في قيمة العناصر الأولية عند إدخالها في الحاسب، أو تحديثها، أو عند تخزينها، أو عند إجراء بعض التعديلات عليها.

ولذلك لا بد من وجود مؤسسات مختصة في التحقيق في جرائم الحاسب الآلي، لجمع المعلومات والأدلة الرقمية، ووجود شرطة مختصة، ومحاكم مختصة؛ لأن المتهم غالباً ما يستند إلى خبرته ومهاراته المتخصصة في مجال خدمات الحاسوب؛ لذلك فإن توجيهه إلى الهدف

يكون دقيقاً، وهذا يتم غالباً في الجرائم الكبيرة، وقد جاء فى قانون الجرائم الالكترونية 2007م (المادة28) بأن ينشىء رئيس القضاء محكمة وفقاً لقانون الهيئة القضائية 1986م، محكمة خاصة للجرائم المنصوص عليها فى القانون. كما جاء فى المادة (29) بأن تنشأ بموجب أحكام قانون تنظيم وزارة العدل1983م نيابة متخصصة لجرائم المعلوماتية. أما المادة(30) فقد نصت على أن تنشأ بموجب أحكام قانون الشرطة1999م شرطة متخصصة لجرائم المعلوماتية ؛ لذلك هناك ضرورة أولاً من إنشاء هذه الآليات لتنفيذ القانون وفق أحكامه ، ثم القيام بتدريب جميع كوادر هذه الآليات.

وكذلك نحن بحاجةٍ إلى أجهزة مساعدة في مكافحة هذه الأفعال لتأمين المعاملات الالكترونية، ووضع أسس لمنح التراخيص بالمواقع ، مع تحديد هوية العميل. مع الاهتمام بنظام التشفير، والذي يغير من شكل الرسالة إلى لغة غير مفهومة لا ترجع إلى طبيعتها إلا بمعرفة مفتاح الشفرة؛ مع ضرورة وضع ضوابط لضمان احترام سرية المعلومات، وعدم إفشائها، أو السماح للغير بالاطلاع عليها ، وإذاعة محتوياتها.

وقد نص القانون على سرية المعلومات بحيث تكون بيانات التوقيع الالكتروني، والوسائط الالكترونية، والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية.

ولا يجوز لمن قدمت إليه، أو اتصل بها بحكم عمله إفشاؤها للغير، أو إستخدامها في غير الفرض الذي قدمت من أجله.

ويجب على مقدم الخدمة الحائز على نظام معالجة البيانات اتخاذ التدابير والإجراءات التي تكفل حماية، وتأمين المعلومات بكافة الوسائل والتقانات المتاحة، وألا يتم اتاحتها إلا وفقاً للقوانين.

وهناك جانب آخر، وهو فيما يتعلق بالتجارة الالكترونية هناك إلزام على الجهات المنظمة والمرخصة فيما يتعلق بنظم التوقيع الالكتروني، وبيانات التوقيع الالكتروني والوسائط الالكترونية، والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني أن تلتزم بالسرية، ولا يجوز لها أي لمن قدمت إليه هذه المعلومات

أو اتصل علمه بها . بحكم عمله . عدم إفشائها للغير، أو استخدامها في غير الغرض الذي قدمت من أجله .

المبحث الرابع :- سلطة القاضي التقديرية في تقدير الدليل الالكتروني:

إن قاضي الموضوع هو صاحب الحق المطلق في تقدير الأدلة لاستخلاص الحقيقة من أجل صحة الاستنتاج الواقعي. ولكن يختلف دور قاضي الموضوع في الدعوى المدنية عن الدعوى الجنائية. ففي الدعوى المدنية ينحصر دوره في القيام بمهمة الحكم بين ما يقدمه الخصوم فقط من بينات، فموقف القاضي المدني يعد سلبياً، ويقتصر فقط فيما يقدمه الأطراف من بينات وفق الطريقة التي نص عليها القانون، ليقوم بعد ذلك بتقييم الأدلة، ثم وزنها، ويضع بعد ذلك قراره بقبولها، أو رفضها أي ثابتة أو غير ثابتة، ولا يقوم القاضي المدني بجمع الأدلة، أو يبحث عن الحقيقة، على خلاف الدعاوى الجنائية التي تنفرد بمبدأ اليقين القضائي، فإن العبء في الإثبات المدني على من يدعى خلاف الأصل، وعليه إثبات الوقائع التي يدعي بها ليستخلص منها أثراً قانونياً، بعد ذلك يقوم القاضي بإصدار حكمه بعد القيام بعملية وزن البينات والحكم وفقاً لمبدأ أرجحية البينات.

ويرجع الدور السلبي للقاضي المدني إلى الدور الإيجابي للخصوم؛ إذ هم يعدون دليل الإثبات مقدماً ، وقبل حدوث النزاع المدني والوقوف أمام القضاء **(23)**.

أما القاضي الجنائي فإنه له دور إيجابي ؛ فهو الذي يسعى وراء تقصي الحقيقة ، وهو الذي يوجه أدلة الإثبات والنفي ؛ فالقاضي في المحاكم الجنائية يكون حراً في تكوين اقتناعه، وحراً في اختيار الأدلة التي يطمئن إليها، ولكن بشرط عدم خروج استنتاجه عن مقتضيات العقل والمنطق، وأن يستند القاضي في حكمه على دليل يجب أن يكون أقوى مصدر ممكن للإثبات لتقرير الإدانة ؛ ولذلك فإن التزام القاضي ببناء حكمه على التثبت واليقين لا الظن والتخمين استوجب مراقبة استخلاص النتائج من المقدمات في حكم محكمة الموضوع ، ومن هنا جاء ضرورة أن يكون حكم القاضي مسبباً، وللقاضي الحق في أن يستعين بالدليل الفني؛ لأن دعاوى الحاسب الآلي تتطلب ـ ولطبيعتها الفنية . رأى فني، أي الاستعانة بأهل الخبرة؛ لتقويم دليل يتعلق بمسائل لا تستطيع المحاكم بحكم تكوين

أعضائها أن تتعرف عليه، والوصول إلى نتائج حاسمة بشأنه، لأن القاضي لا يمكن أن يحل محل الخبير للفصل في مسألة معينة فنية وعلمية، ولا يستطيع فيها أن يصل إلى جانب الحق؛ فالخبرة هي وسيلة من وسائل الإثبات تهدف إلى كشف بعض الدلائل، أو الأدلة لتحديد مدلولها بالاستعانة بالمعلومات العلمية **(24)**.

وقد تضمن قانون الإثبات لسنة 1993م نصاً تناول موضوع الخبرة (المادة 30)؛ إذ جاء فيه: بأنه إذا اقتضى الفصل في الدعوى استيعاب مسائل فنية، كالطب، أو الهندسة، أو المحاسبة، والخطوط، والأثر، وغيرها من المسائل الفنية- فيجوز للمحاكم الاستعانة برأي الخبراء فيها، وتندب لذلك خبيراً، أو أكثر ما لم يتفق الخصوم على اختيارهم. فالدليل الفني هو النتيجة التي تسفر عنها التجارب العلمية والاختبارات المعملية لتعزيز دليل سبق تقديمه، أو نفى الواقعة ذات الأهمية في الدعوى، وهو شكل استثنائي للأدلة التي تقدم في الدعوى.

وإذا كان الدليل الفني يعد بعيداً عن نظر القاضي، ويستخدمه بعد ذلك لحسم مسألة معينة لازمة للفصل في الدعوى، ولكن يخضع لتقدير القاضي على ضوء الأدلة الأخرى المقدمة في الدعوى أي لابد من اقتناع القاضي بالدليل المقدم. وقد نص قانون الإثبات فيما يتعلق بخضوع رأى الخبير لتقدير المحكمة بأنه يجوز للمحكمة تأسيس حكمها على شهادة الخبير، ولها إذا قضت بخلاف رأيه أن تضمن حكمها الأسباب التي أوجبت عدم الأخذ برأي الخبير كله أو بعضه (المادة 32 من القانون أعلاه) .

ولطبيعة هذه المعاملات والجرائم الالكترونية . فإن الأمر يتطلب للإثبات الاستعانه بأهل الخبرة لجمع هذه الأدلة وتأمينها واستخراجها ، بل والتأكد من صحة المعلومات، وعدم تغيرها بقصد، أو بغير قصد أثناء تكوينها، أو معالجتها أو نقلها أو حفظها. الأمر الذي يتطلب الأمانة في نقل هذه الأدلة ، فعلى سبيل المثال تحتاج المحاكم للخبرة عند حدوث نزاع حول التوقيع الرقمى للاستيثاق منه؛ فيتم التحقق بواسطة الخبراء؛ وذلك بالرجوع لمحتويات الرسالة الأصلية بعد استخلاصها، وفك تشفيرها باستخدام المفتاح الخاص للمرسل له، واستخدام المفتاح العام للراسل لفك تشفير التوقيع الرقمى للحصول

على بصمة المستند. ويتم التحقق من البصمة الرقمية للرسالة بإعادة توليد للبصمة من الرسالة، ويتم بعد ذلك مضاهاة البصمة المولدة مع الأصلية فى الرسالة، وفى حالة التطابق يتم تأكيد صحة الرسالة وصدورها من موقعها، والا يتم رفض الرسالة؛ لأنه تم التلاعب بها، وغير صادره من الشخص المدعى توقيعه رقمياً (25).

وقد جاء في قانون المعاملات الالكترونية في المادة 1/29 تطبيق أحكام المعاملات المدنية ، والإثبات والإجراءات المدنية فيما لم يرد بشأن نص في هذا القانون .

وعليه يمكن الرجوع للقانون العام ، قانون الإثبات عند خلو قانون المعاملات من نصوص خاصة بإثبات المعاملة الالكترونية ، وكذلك الجرائم الالكترونية لعدم وجود قانون إثبات الكتروني.

ثالثاً – التوقيع الالكتروني:

1- حجية التوقيع الالكتروني

التوقيع هو وسيلة يعبر بها شخص عن إرادته في الالتزام بتصرف قانوني معين ، ويتطلب التوقيع لإثبات صحة التصرفات.

وينقسم التوقيع إلى توقيع تقليدي ، قد يكون إما بالإمضاء، أو ببصمة الأصبع، أو ببصمة الختم، والتوقيع الآخر هو التوقيع الالكتروني (26).

التوقيع الرقمي حسب تعريف قانون المعاملات الالكترونية لسنة 2007م يقصد به: التوقيع الذي يتم إنشاؤه وإرساله واستقباله وتخزينه بوسيلة الكترونية، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات يكون لها طابع متفرد، ويسمح بتحديد هوية وتمييز شخصية الموقع عن غيره. وأرى إن هذا التوقيع شبيه بالعلامة التجارية والتى توضع لتمييز بضائع شخص عن الآخرين، ويمكن أن تأخذ شكل أى حروف أو رمز أو رسم أو صورة بشكل يكون مميز للعلامة. ويتضح من التعريف أعلاه أن التوقيع يشمل جميع طرائق التوقيع الإلكترونى الموجودة حالياً ، والتى قد توجد مستقبلاً؛ وعليه فإن المشرع يهدف إلى استيعاب جميع أشكال التوقيع الالكترونى.

والتوقيع الالكتروني هو تعبير شخص عن إرادته في الالتزام بتصرف قانوني معين عن طريق تكوينه لرموز سرية يعلمها هو وحده تسمح بتحديد هويته حتى ينتج التوقيع الـلكتروني آثاره القانونية، ولا بد أن يعبر عن هوية صاحبه، بمعنى أن تكون وسيلة التوقيع الالكتروني تحت سيطرة الموقع وحده دون غيره، والغرض من هذا التوقيع هو إسناد مرجعية تحرير السند إلى شخص ما وتحديد هويته.

وعليه فمن الوجهة القانونية فوظائف التوقيع الرقمى هى:

أ- التوقيع الرقمى يثبت الشخص الذى وقع الوثيقة.

ب- يحدد التوقيع الرقمى الشىء(الوثيقة) التى تم توقيعها بشكل لا يحتمل التغيير.(27)

ويمتيز التوقيع الرقمى عن التوقيع العادى بأن التوقيع العادى هو عبارة عن رسم يقوم به الشخص، ومن هنا يسهل تزويره، أما التوقيع الرقمى فهو من حيث الأصل، وفى حدود أمن استخدام برنامجه من قبل صاحب البرنامج، علم وليس فناً، وبالتالى يصعب تزويره، كذلك فى التوقيع العادى يمكن فصل التوقيع عن الأوراق والمحررات واقتطاع التوقيع، ولكن فى التوقيع الرقمى هذا غير متاح؛ لأنه لا يثبت الشخص موقع الوثيقة فقط، وأنما يثبت بشكل محدد الوثيقة محل ذلك التوقيع، فإنه جزء منها ورموز متقطعة ومشفرة، ولدى فك التشفير يتعين أن ينطبق التوقيع ذاته على الوثيقة.(28)

وقد حدد القانون أداة التوقيع بأنها " يقصد بها أى جهاز، أو أى بيانات الكترونية معدة بشكل مميز للعمل بطريقة مستقلة، أو بالاشتراك مع أجهزة بيانات أخرى؛ وذلك لوضع رقمى محدد لشخص معين، وتشمل هذه العملية أى أنظمة، أو أجهزة تنتج أو تلتقط بيانات مميزة كالرموز، أو المناهج الحسابية، أو الحروف، أو الأرقام ، أو المفاتيح الخصوصية، أو أرقام تعريف الشخصية ، أو أى خواص شخصية أخرى. (29)

ويتضح من ذلك بأن المشرع لم يقيِّد الشكل الذى يتم به التوقيع، المهم أن يكون للتوقيع شكل محدد لكل شخص.

ويتم إنشاء التوقيع ، وكذلك التثبت من صحته من خلال التشفير، وهو فرع من الرياضيات التطبيقية المختصة بتحويل الرسائل إلى أشكال تبدو وكأنها لا يمكن فهمها وإعادتها مرة

أخرى كما كانت . وقد عرَّفَ القانون التشفير: " يقصد به بأنه: استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها، أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إليها من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها.(30)

ويحتاج التوقيع الالكتروني إلى شهادة خاصة تصدر من جهة مختصة للتصديق على هذا التوقيع ، وتسمى مستند الاعتماد، وهي علامة رمزية تعطى لإثبات خضوع فرد لهيئة أو جهاز محدد لعملية توثيق (31).

وقد عرف قانون المعاملات الالكترونية هذه الشهادة بأنها : يقصد بها الشهادات التي تصدر من الشخص المرخص له بالتوثيق لإثبات نسبة التوقيع الرقمي إلى شخص معين استناداً إلى إجراءات التوثيق المعتمدة.

وقد أقر قانون المعاملات الالكترونية صحة التوقيع الرقمي في المادة الثامنة من القانون؛ إذ جاء بالأتي:

أ- لا ينكر الأثر القانوني للتوقيع الرقمي من حيث صحة وإمكان العمل بموجبه لمجرد وروده كلياً أو جزئياً في شكل الكتروني.

ب- إذا أوجب القانون التوقيع على مستند أو رتب أثراً قانونياً على خلوه من التوقيع . فإنه إذا استعمل سجلاً قانونياً الكترونياً في هذا الشأن فإن التوقيع الرقمي يفى بمتطلبات القانون.

ج- إذا عرض في إجراءات قانونية توقيع رقمي مقرون بشهادة رقمية معتمدة لأي شخص، يكون ذلك التوقيع معادلاً لتوقيعه اليدوي.

د- وعليه متى ما كان التوقيع الرقمى قادراً على إثبات الشخص الذى وقعه فإنه يماثل التوقيع العادى.

ويتم إنشاء التوقيع الالكتروني في مجال المعاملات الالكترونية عن طريق مرحلتين متتابعتين من البيانات، **المرحلة الأولى** تقوم عن طريق استخدام بيانات معينه يرسلها المرسل إلى المرسل إليه لفتح الرسالة المتضمن التصرف القانوني (**مفتاح عام**)

يستطيع كل ذي شأن الاطلاع عليه ، ولكن لا ينتج أي أثر إلا مع المفتاح الخاص، وهي ما تعرف **بالمرحلة الثانية** وتتم بتركيب مجموعة من البيانات، أو الأرقام تكون تحت سيطرة الموقع وحده دون غيره، ولا يطلع عليها أحد؛ لذلك سمي هذا المفتاح (**المفتاح الخاص**)، ومن صوره أن تحمل بياناته على دعامات من أنواع مختلفة منها ما يتعلق ببرنامج على الكمبيوتر، ومنها الكروت المقواة، ومنها القلم الالكتروني، ومنها الخصائص الوراثية للشخص كالبصمة لتعرف على الوجه البشري **(32)**.

ويرتبط التوقيع الالكترونى بالتشفير ارتباطاً عضوياً، والتشفير هو عملية تغيير فى البيانات،بحيث لا يتمكن من قراءتها سوى الشخص المستقبل وحده، باستخدام مفتاح فك التشفير، وفى تقنية المفتاح العام يتوفر المفتاح ذاته لدى المرسل والمستقبل، ويستخدم فى عمليتى التشفير، وفك التشفير.

وعندما يتم التصرف القانوني يحق لكل من المتعاملين التحقق والتأكد من صحة التصرف من مقدم خدمة التصديق على التوقيع الالكتروني.

ويتميز التوقيع الالكتروني بصعوبة التزوير؛ لأن التوقيع الالكتروني . كما ذكرنا . يتكون من مفتاحين عام وخاص، العام يتم الإعلان عنه في شهادة التصديق على التوقيع الالكتروني الصادرة من جهة مختصة، وهو مفتاح يخص الموقع وحده دون غيره لكنه ينشر لكل ذي شأن.

أما الخاص فهو مجموعة بيانات يستأثر الموقع وحده بحيازتها ، وتُعد بمثابة قلم التوقيع الذي يقوم الموقع من خلاله بتكوين بيانات توقيعه ؛ لذلك فإن كان هناك تزوير لابد أن يستخدم المزور نفس قلم الموقع (المفتاح الخاص) ، وأن يكون عالماً ببيانات التوقيع الالكتروني وبيانات المفتاح العام، وهو أمر لا يكون متاح إلا للموقع.

ولكي يكون للتوقيع الالكتروني حجة في الإثبات لابد أن يكون تحت السيطرة المباشرة للموقع وحده دون غيره، وإذا اختلت هذه السيطرة، فلا ينتج التوقيع أثره القانوني، ولا يكون حجة في الإثبات **(33)**.

وفي هذا الشأن حكمت محكمة فرنسية في 2000/10/20م بضرورة أن تكون سيطرة الموقع على التوقيع الالكتروني دون غيره.

وتتلخص وقائع الدعوى أن محامي أحد الأشخاص (الموقع) احتج بالتوقيع الالكتروني لموكله أمام المحكمة، وقدم في صحيفة دعوى بيانات هذا التوقيع السرية التي من المفترض أن يعلمها الموقع وحده دون غيره. رفضت المحكمة الحكم بصحة هذا التوقيع الالكتروني(**34**).

2- الحفاظ على صحة وحجية التوقيع الالكتروني:

هناك ضرورة مهمة بأن يكون التوقيع الالكتروني بالصورة نفسها، التي صدر فيها من مصدرها حتى وصولها إلى المرسل إليه.

ولا يستطيع أي شخص سواء أكان المرسل إليه، أم الغير أن يمس التوقيع الالكتروني للمرسل بالتغيير، أو التعديل، ولكن المرسل إليه هو الشخص الذي وجه إليه الإيجاب أن يقبل الوثيقة الالكترونية جملةً وتفصيلاً، أو يرفضها، وله الحق في أن يقترح بتعديل بعض البنود ؛ فيصبح هو الموجب في هذه الحالة والمرسل الأول من وجه إليه الإيجاب.

وتحفظ الوثيقة الالكترونية بما يسمى بعملية الضغط الالكتروني بحيث تتحول الوثيقة من بيانات إلى حروف وأرقام، وفي حالة إعادة فك الضغط الالكتروني تظهر البيانات الأصلية للوثيقة، ويحفظ التوقيع الالكتروني الموجود على الوثيقة الالكترونية التي تتضمن تصرف قانوني بالطريقة نفسها أعلاه.

وقد وضع قانون المعاملات الالكترونية المبادىء العامة للتوقيع الالكترونى ، وترك أمر تنظيم تقنية التوقيع الالكترونى للوائح اللازمة لتنفيذ أحكام القانون (المادة30/2/ج)، والتى يصدرها السيد الوزير، والذى يحدده بموجب القانون السيد رئيس الجمهورية ، وبذلك يكون هناك فرصة لتعديل اللوائح كلما تتطلب الأمر ذلك خاصة وإن هذا المجال فى تتطور مستمر. ويجب ومن خلال اللوائح أن يتم وضع،

وتحديد مفاهيم، ومبادىء، ومعايير يمكن بها ضمان سجلات دقيقة وموثوقة والحفاظ عليها، ولا يتم الوصول إليها إلا وفقاً للقوانين.

وعلى كل فإن قانون المعاملات الالكترونية لسنة 2007م قد أضفى حجية الإثبات القانونية للكتابة الالكترونية والتوقيع الالكتروني، ليكون لهما الحجية القانونية نفسها للتوقيع العادي، والكتابة العادية، إذا تمت وفق الشروط التي وضعها القانون.

الخاتمة :

لم تعد شبكة الانترنت مجرد وسيلة لتبادل المعلومات والحصول عليها، بل أصبحت وسيلة يتم من خلالها العديد من التصرفات القانونية، ولما كانت هذه الشبكة مفتوحة، ويسمح لأي شخص من الجمهور بالدخول إليها دون أي قيد، أو شرط سوى أن يكون متصلاً بجهاز الحاسوب . لذلك فإن هذه الشبكة أثارت وتثير العديد من المشكلات القانونية خاصة في الإثبات، وقد نتج عن هذا التطور إشكالية إثبات السند الالكتروني، كمسائل توفر هذا السند، وما يحتويه من بيانات والشكل الذي يفرضه القانون، وتحديد القانون الواجب التطبيق على العقود الدولية، وتحديد مفهوم أصل السند وصورته، وأن النسخه هي تكرار للأصل في كل جزيئياته؛ إذ تُعد النسخة جزء من الأصل.

وتثور تساؤلات أيضاً حول اعتبار الرسالة الالكترونية بعد استخراجها أمام القضاء . على سبيل المثال . في قوة السند الكتابي، علماً بأن المستند المكتوب هو ما تعارف عليه بأنه المستند المحرر بخط اليد أو المطبوع، وهذه الإشكالات لا تجد حلولاً إلا بعد التطبيق، وإصدار سوابق قضائية لتغيير نصوص القوانين السارية.

وقد تثور . أيضاً . مشكلة التوقيعات الرقمية عبر الحدود، لاختلاف الأنظمة القانونية؛ لأن التعاملات قد تتم بين شخص أو مؤسسة محلية مع شخص أو مؤسسة أجنبية يختلف نظامها القانوني عن النظام القانوني المحلي، بمعني أخر عدم توافق المعايير القانونية والتقنية، ويمكن أن نخفف من هذه الاختلافات بالانضمام للاتفاقيات الدولية ذات الشأن، ومنها اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الالكترونية ، وكثير من الاتفاقيات في مجال التجارة الالكترونية لتوحيد المعايير المنطبقة على مثل هذه التزامات، وكثير من الاتفاقيات في مجال التجارة الالكترونية لتوحيد المعايير المنطبقة على مثل هذه النزاعات.

كما قد تثور إشكالات التباعد الجغرافي بين الفاعل والمجنى عليه، أي تباعد بين الفعل والنتيجة ؛ فتثار مسألة الاختصاص والقانون الواجب التطبيق، وفي هذا المقام أيضاً الأمر

متروك لتضافر الجهود الدولية لمكافحة هذه الجرائم ، وإمكانية جمع المعلومة، والتحريات عنها لتدعيم الإجراءات القانونية والقضائية، وذلك باتباع معايير محددة، واستخلاص الأدلة الدقيقة، وعدم السماح بأي انحراف، أو تعديل ليؤدي التتبع إلى القبض على الجناة وتقديمهم للمحاكمة.

وعليه فإننا نرى ضرورة اتباع منهجية، ومعايير محددة تكفل التصدي لهذا النوع من الجرائم لتقديم أدلة ذات فائدة في التعرف على مرتكبى الجرائم وإدانتهم أمام المحاكم.

وعلى كل يجب . وقبل ذلك . أن يتم تدريب، وتأهيل لجميع الأجهزة العدلية؛ لأن القوانين تحتاج إلى بنيات تحتية مؤهلة، وممتدة للقيام بتفعيل هذه القوانين مع ضرورة تنفيذ أحكام القانون، والبدء بانشاء آليات القانون المحكمة والنيابة والشرطة المتخصصة. مع توفير الوسائل الملائمة لتمكين المحاكم من تقييم مصداقية البيانات الواردة في تلك السجلات، وعلى أن يبذل مقدم الخدمة التوثيقية العناية المعقولة والواجبة عند قيامه بالتصديق على التوقيع الالكتروني وتوثيقه لمساعدة الجهات العدلية من تحقيق العدالة.

وعلى كل يجب . وقبل ذلك . أن يتم تدريب وتأهيل لجميع الأجهزة العدلية؛ لأن القوانين تحتاج إلى بنيات تحتية مؤهلة وممتدة للقيام بتفعيل هذه القوانين، خاصة التدريب حول كيفية استقصاء الأدلة الالكترونية الجنائية، وإدارة مسرح الجريمة والتعامل مع الأدلة ، مع ضرورة تنفيذ أحكام القانون والبدء بانشاء آليات القانون المحكمة والنيابة والشرطة المتخصصة. مع توفير الوسائل الملائمة لتمكين المحاكم من تقييم مصداقية البيانات الواردة في تلك السجلات بالاهتمام بالخبراء المختصين، وإنشاء مختبرات مؤهلة ومتطورة تتيح لهم إمكانية الاستفادة من المعلومات، وعلى أن يبذل مقدم الخدمة التوثيقية العناية المعقولة والواجبة عند قيامه بالتصديق على التوقيع الالكتروني وتوثيقه لمساعدة الجهات العدلية من تحقيق العدالة.

التوصيات:

1- **الاهتمام بتعديل قانون الإثبات 1993م لتضمين النصوص الخاصة بالدليل الالكتروني.**
2- **التدريب والتأهيل للأجهزة العدلية حتى تستطيع أن تقوم بتنفيذ وتطبيق هذه القوانين الحديثة، وقبل ذلك ضرورة إنشاء المؤسسات المتخصصة وفقاً لمتطلبات القانون.**
3- خلق التعاون وتبادل خبرات بين الدولة وبقية الدول التي أدخلت الأنظمة الحديثة، وقامت بتطبيق نظام الحكومة الالكترونية والتعاون مع مراكز المعلومات.
4- تطوير نصوص قانون الإجراءات الجنائية التي تبين كيفية جمع الاستدلالات عن تلك الجرائم ، وضبطها، والحفاظ على الدليل.
5- وضع اللوائح المنظمة للمعلومات، والاتصالات لحماية المتعاملين في مسائل التجارة الالكترونية تأكيداً على حماية الحقوق الخصوصية.

6- استحداث التشريعات الخاصة بحماية المستهلك في مجال التجارة الالكترونية.

7- التوعية بأهمية المعاملات الالكترونية ، ومن ثم ضرورة دراسة الوضع القانونى المطلوب لحماية المتعاملين عبر الشبكة الالكترونية.

الهوامش :

1- ابن منظور/ لسان العرب/ ج2/ دار صادر/ باب ثبت.

2- د. عبد الرازق السنهوري، الوسيط نظرية الالتزام بوجه عام، دار إحياء التراث العربي، لبنان، ص 52.

3- المادة (13) قانون الإثبات لسنة 1993م.

4- قانون الإجراءات الجنائية السوداني، معلقاً عليه، القاهرة، المطبعة العالمية، 1971م، ص 657.

5- أكاديمية نايف العربية للعلوم الأمنية، الظواهر الإجرامية المستحدثة وسبل مواجهتها، 1999م، ص92.

6- أكاديمية نايف العربية للعلوم الأمنية، الجرائم الاقتصادية وأساليب مواجهتها، الرياض، 1996م ، ص26.

7- د/ نادر عبد العزيز، الإثبات الالكتروني بين الواقع والقانون، 2007م، موقع المنتدى الوصوي للاستئناف والدراسات القانونية.

8- محمد حمد شتا ، فكرة الحماية الجنائية لبرنامج الحاسب الآلي- دار الجامعة الجديدة للنشر، الإسكندرية 2007م، ص68.

9- بروفسير. أورين كبر، د.عرين يونس، نطاق الجريمة الالكترونية، دار النهضة العربية، القاهرة، 2004م، ص122 .

10- د. نائلة عادل فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ص564.

11- د. شحاته غريب محمد شلقامي، برنامج الحاسب الآلي والقانون، دار النهضة العربية، القاهرة، 2003م، ص126م.

12- د. نائلة عادل فريد قوره، جرائم الحاسب الآلي الاقتصادية – منشورات الحلبي الحقوقية، ص557- 580.

13- المادة (3) قانون المعاملات الالكترونية 2007م.

14- د. خالد مصطفى فهمي، الحماية القانونية لبرنامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2005م .

15- المادة (10) قانون المعاملات الالكترونية 2007م.
16- د. أحمد عبد المجيد الحاج، جرائم النشر الصحفي الالكتروني وأحكام المسئولية الجنائية (دارسة مقارنة)، وزارة الثقافة والإعلام الإمارات العربية، 2007م، ص44.
17- ورقة علم أعدها حسن أحمد الحاج بابا، بعنوان دليل الإثبات الالكتروني في المنتدى القضائي الفصلي الأول 2008م.
18- موقع الفريق العربي للأمن والحماية المعلوماتية، بحث بعنوان الجريمة الإلكترونية .
19- عبد الرحمن محمد عبد الرحمن شرفى، تعارض البينات القضائية، المكتبة الشرعية، 1999م، ص253.
20- د. محمد البشرى، من نظام العدالة الجنائية إلى نظام العدالة المجتمعية، الطبعة الأولى، 2007م – ص84.
21- ورقة عمل أعدها عميد شرطة برالدين الامين، المعاينة الفنية لمسرح الجريمة، للمنتدى القضائى الفصلى، 2009 م.
22- المادة (8) قانون المعاملات الالكترونية 2007م
23- د. رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، دار النهضة العربية، 2004م، ص28.
24- د. رمزي رياض عوض، المرجع أعلاه، ص 62.
25- ورقة عمل م.عبد المجيد نمر، بعنوان التوقيع الرقمى، أعدها للامانة العانة لمجلس الوزراءلمناقشة مشروع قانون المعاملات الالكترونية، ص7.
26- د. أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية ، 2004م ، ص21.
27- أمير فرج يوسف، التوقيع الالكترونى، دار المطبوعات الجامعية، 2008 م، ص69.
28- المرجع السابق، ص69.
29- المادة(2) قانون المعاملات الالكترونية 2007 م.
30- المادة(2) قانون المعاملات الالكترونية 2007م.
31- http://www cdt. Org/ privacy. authentication.
32- د .أيمن سعد سليم، المرجع أعلاه، ص25.

33- منير محمد الجنبيهي – ممدوح محمد الجنبيهي ، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، 2005 ، ص11 .

34- د أيمن سعد سليم، مرجع سابق، ص29.

المصادر والمراجـــع:

القرآن الكريم.

1- د. أحمد عبد المجيد الحاج، جرائم النشر الصحفي الالكتروني وأحكام المسئولية الجنائية، دراسة مقارنة، طبع بإشراف وزارة الإعلام والثقافة، الإمارات العربية، 2007م.

2- أكاديمية نايف العربية للعلوم الأمنية، الجرائم الاقتصادية وأساليب مواجهتها، الرياض، 1996م.

3- أكاديمية نايف العربية للعلوم الأمنية، الظواهر الإجرامية المستحدثة وسبل مواجهتها، الرياض، 1999م.

4- أمير فرج يوسف، التوقيع الالكترونى، دار المطبوعات الجامعية، 2008م.

5- بروفسير. أورين كبر، د. عرين يونس ، نطاق الجريمة الالكترونية، دار النهضة العربية، 2004م.

6- د. أيمن سعد سليم، التوقيع الالكتروني، دار النهضة العربية، 2004م .

7- د. خالد مصطفى فهمي، الحماية القانونية لبرنامج الحاسوب الآلي، دراسة مقارنة ، دار الجامعة الجديدة للنشر، الأسكندرية، 2005م.

8- د. رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة دراسة مقرنة ، دار النهضة العربية 2004م

9- د. شحاتة غريب محمد شلقامي، برنامج الحاسب الآلي والقانون، دار النهضة العربية، القاهرة، 2003م.

10- عبد الرازق السنهوري، الوسيط، نظرية الالتزام بوجه عام، دار إحياء التراث العربي ، لبنان .

11- عبد الرحمن محمد عبد الرحمن شرفى، تعارض البينات، طبع بإشراف المكتب الاسلامى، 1999 م.

12- د. محمد البشرى، من نظام العدالة الجنائية إلى نظام العدالة المجتمعية الطبعة الأولى ، 2007م .

13- محمد حمد شتا، فكرة الحماية الجنائية لبرنامج الحاسب الآلي، دار الجامعة الجديد للنشر، الإسكندرية، 2001م.

14- د. محمد محي الدين عوض، قانون الإجراءات الجنائية السوداني معلقاً عليه، المطبعة العالمية, القاهرة.

15- إبن منظور الإفريقي المصري، لسان العرب, الجزء الثاني، دار صادر.

16- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، 205م .

17- د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشور الحلبي الحقوقية.

المواقع:

1- موقع الفريق العربي للأمن والحماية المعلوماتية ، بحث بعنوان الجريمة الالكترونية .

2- موقع المنتدى السوري للاستشارات والدراسات القانونية، د. نادر عبد العزيز، الإثبات الالكتروني بين الواقع والقانون.

3- http://www cdt. Org/ privacy. authentication/ interim – shtml

أوراق:

1- حسن أحمد الحاج بابا ، ورقة عمل بعنوان : دليل الإثبات الالكتروني في المنتدى القضائي الفصلي الأول 2008م .

2- م.عبد المجيد نمر ورقة عمل بعنوان : التوقيع الرقمى ، للامانة العامة لمجلس الوزراء عند مناقشة مشروع قانون المعاملات الالكترونية.

3- عميد شرطة بدرالدين الأمين ، ورقة عمل بعنوان : المعاينة الفنية لمسرح الجريمة ، للمنتدى القضائى الفصلى ، 2009م.

القوانين :

1- قانون الإثبات لسنة 1993م .

2- القانون الجنائي لسنة 1991م .

3- قانون جرائم المعلوماتية 2007م .

4- دستور السودان الانتقالي لسنة 2005م .

5- قانون المعاملات الالكترونية لسنة 2007م .

السوابق القضائية :

* م ع / ف ج / 130 / 2007م (غير منشورة).