جامعة النيلين
كلية الدراسات العليا

بحث تكميلي لنيل درجة الماجستير في القانون
بعنوان:

حجية الدليل الإلكتروني في الإثبات الجنائي

إعداد الطالب:
أحمد إسماعيل عبد الوهاب

إشراف الدكتور:
طارق دفع الله الإمام

1440هـ - 2018م

بسم الله الرحمن الرحيم

استهلال

قال تعالى:

(صُنْعَ اللَّهِ الَّذِي أَتْقَنَ كُلَّ شَيْءٍ إِنَّهُ خَبِيرٌ بِمَا تَفْعَلُونَ).

صدق الله العظيم

سورة النمل، الآية: 88.

إهداء

إلى ما رضا الله إلا برضائها.... إلى من أنا منها ولها أعيش بينابيع الخير والعطاء إلى رموز الصبر والتضحية والوفاء، إلى من تدعو لي دوماً بالتوفيق والسداد أطال الله عمرها وبارك فيها.

والدتي العطوفة..

إلى من نذر نفسه قرباناً محترقاً من أجلنا، نبع الحنان والعطاء شمس وجودنا في هذه الدنيا، إلى من بذل قصارى جهده في تعليمي.

والدي..

إلى من كان له الفضل في تعليمي.... إلى من جعل العلم يكبر معي في سنين. إلى من علمني حرفاً وأنار لي سبيل المعرفة، إلى كل من وجه لي نصحاً.... إلى كل من أضاء الشعلة التي أنارت لي الطريق.

أساتذتي الأفاضل احتراماً وعرفاناً وثناءً..

إلى العقول المفكرة التي تنير دروب العلم والمعرفة إلى النفوس العظيمة المؤمنة بخير الإنسانية إلى من صار عدل الحياة بالتجربة والعلم والعزيمة إلى الذين فكروا كثيراً أو قليلاً في القانون وأحسوا بالحاجة إلى مزيد من الضياء يلقى عليه في مختلف مراحله وأطواره في الشرق والغرب. إلى كل مناضل في سبيل الحق والحرية إلى كل من رفع راية العدل والمساواة سلاماً واحتراماً واعتزازاً.

زملائي.. ورجال القانون..

إليهم جميعاً أهدى خلاصة جهدي المتواضع.

شكر وتقدير

الحمد لله الذي تتم بنعمته الصالحات، فالحمد والشكر والثناء لله تعالى الذي شملني بفضله وكرمه ورحمته ومنحنى العزم والقدرة على إنجاز هذا العمل، فيا رب لك الحمد كما ينبغي لجلال وجهك وعظيم سلطانك، على ما أنعمت به عليَّ وتفضّلت.

وبعد... قال الرسول صلى الله عليه وسلم (لا يشكر الله من لا يشكر الناس) فأحمد الله بأن هيأ لي أستاذي الجليل الدكتور/ **طارق دفع الله الإمام**، ليكون عوناً لي بعد عون الله سبحانه وتعالى ومشرفاً لي على هذا العمل وإخراجه على النحو الذي أرجو أن يكون مفيداً ومشرقاً.

كما أخص بالشكر أيضاً:

كل من ساهم في مدَّ العون وأخص بالشكر وكل أساتذتي بجامعة النيلين وزملاء الدفعة جميعهم.

المستخلص

تناولت الدراسة حجية الدليل الإلكتروني في الإثبات الجنائي، وتدور مشكلة الدراسة حول المشكلات الناجمة عن استخدام الثورة التقنية في عالم الحاسوب أو الكمبيوتر، حيث تمخض عن استخدام هذه الأجهزة، وما توفر لديها من برامج بعض أنواع الجريمة أو الأفعال التي يمكن وضعها في إطار الأفعال الإجرامية مكتملة العناصر. نبعت أهمية موضوع الدراسة من كون أن الجريمة الإلكترونية هي جريمة العصر وهي الأدوات المتوفرة حالياً في الجريمة. هدفت الدراسة إلى إثبات حجية الدليل الإلكتروني في قانون الإثبات السوداني، كما يهدف إلى مقارنة القانون السوداني مع بعض القوانين العربية والدولية في حجية الإثبات الإلكتروني. اتبعت الدراسة المنهج الوصفي والتحليلي والمنهج الاستقرائي في استعراض موضوعاتها. توصلت الدراسة إلى عدة نتائج من أهمها: إن هناك قصوراً واضحاً في الكثير من التشريعات الجنائية الموضوعية والإجرائية في مواجهة ظاهرة الجرائم التي تقع بالوسائل الإلكترونية أو على هذه الوسائل، مما قد يترتب عليه إفلات الكثير من الجناة من العقاب. ترتب على النتائج عدة توصيات منها: إيجاد تشريع قانوني يتعامل مع جرائم الإنترنت من حيث الوقاية والتحقيق والضبط والعقاب.

Abstract

The study deals with the problems of using the technical revolution in the world of computer or computer, which resulted in the use of these devices and the programs that provide some types of crime or acts that can be placed in the framework of criminal acts completed Elements. The importance of the subject of the study stems from the fact that cybercrime is the crime of the age and is currently available in crime. The study aimed to prove the authenticity of the electronic evidence in the Sudanese Evidence Law. It also aims to compare the Sudanese law with some Arab and international laws in the field of electronic evidence. The study followed descriptive, analytical and inductive methods in reviewing its subjects. The study reached several conclusions, the most important of which are: There is a clear lack in many of the substantive and procedural criminal legislation in the face of the phenomenon of crimes that occur by electronic means or on these means, which may result in the impunity of many of the perpetrators. The results of the results are several recommendations, including: the creation of legal legislation dealing with the crimes of the Internet in terms of prevention, investigation, control and punishment.

فهرس المحتويات

عنوان الموضوع	الصفحة
البسملة	أ
استهلال	ب
إهداء	ج
شكر وتقدير	د
المستخلص	هـ
Abstract	و
فهرس الموضوعات	ز
مقدمة	1
مشكلة البحث	2
أهمية البحث	2
أهداف البحث	2
منهج البحث	3
هيكل البحث	3
الفصل الأول	
مفهوم وأنواع الدليل الإلكترونية	
المبحث الأول: تعريف الجريمة الإلكترونية وأنواعها	5
المطلب الأول: تعريف الجريمة الإلكترونية	5
المطلب الثاني: أنواع الجرائم الإلكترونية	6
المبحث الثاني: مفهوم الأدلة الجنائية الإلكترونية	24
المطلب الأول: مفهوم الأدلة الجنائية لغةً وشرعاً	24
المطلب الثاني: مفهم الدليل اصطلاحاً وقانوناً	25
المطلب الثالث: تعريف الأدلة الجنائية الإلكترونية	27
المبحث الثالث: وسائل جمع الأدلة الإلكترونية ومقارنتها	32

المطلب الأول: جمع الأدلة الإلكترونية	32
المطلب الثاني: رسالة التصنيف والتوقيعات الرقمية	34
الفصل الثاني	
حجية الدليل الإلكتروني	
المبحث الأول: التعريف بالدليل الإلكتروني	37
المطلب الأول: تعريف بالدليل الإلكتروني	37
المطلب الثاني: أنواع الدليل الإلكتروني ومجاله في الإثبات الجنائي	40
المبحث الثاني: القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي	47
المطلب الأول: مشروعية الدليل الإلكتروني	47
المطلب الثاني: حجية الدليل الإلكتروني أمام القضاء الجنائي	49
المبحث الثالث: مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي	56
المطلب الأول: شروط الدليل الإلكتروني المستمد من التفتيش	57
المطلب الثاني: حجية الدليل الإلكتروني الناشئ عن التفتيش	68
الخاتمة	77
النتائج	77
التوصيات	78
قائمة المصادر والمراجع	79

مقدمة

أصبح الدخول إلى شبكة المعلومات الدولية "الإنترنت" مخاطرة غير محسوبة العواقب حيث انتشر الهاكرز على جنباته منتظرين الانقضاض على أول فريسة تقابلهم وهي بالطبع المستخدم الذي لا يملك في جعبته إلا مجرد برامج إلكترونية لا تغنى ولا تسمن من جوع، ليتحول الانترنت من وسيلة إعلامية إلى ساحة قتال اختلفت فيها الأسلحة، إلا أن النتيجة واحدة وهى الخسائر الفادحة للضحية وغنائم الحرب للقراصنة. ومع ازدياد عمليات القرصنة ظهرت جرائم الإنترنت وهي جرائم تختلف عن الجرائم المتعارف عليها، فالجاني لا يحمل مسدساً ولا يسطو على متجر، فهو جالس في بيته ولا يجد عناء في مجرد الضغط على زر يدخل به إلى شبكة الإنترنت ويبدأ في اصطياد ضحاياه، وجرائم الإنترنت تعددت صورها وأشكالها فلم تعد تقتصر فقط على اقتحام الشبكات وتخريبها أو سرقة معلومات منها بل شملت أيضاً جرائم أخلاقية مثل الاختطاف والابتزاز والقتل وغيرها.

وفي ظل التطورات الهائلة لتكنولوجيا المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، فقد أصبح من السهل ارتكاب أبشع الجرائم بحق مرتاديها سواء كانوا أفراداً أم مؤسسات أم مجتمعات محافظة بأكملها. ويقوم مجرمو الإنترنت بانتحال الشخصيات والتغرير بصغار السن بل تعدت جرائمهم إلى التشهير وتشويه سمعة ضحاياهم الذين عادةً ما يكونوا أفراداً أو مؤسسات تجارية ولكن الأغرب من ذلك أنهم يحاولون تشويه سمعة مجتمعات بأكملها خاصة المجتمعات الإسلامية، وهذا ما حد بالعالم لتحرك حيث وقعت 30 دولة على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية بودابست، وشملت المعاهدة عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

مشكلة البحث:

تكمن مشكلة البحث في بعض المشكلات الناتجة عن استخدام الثورة التقنية، في عالم الحاسب الآلي، أو الكمبيوتر، وكذلك في شبكة المعلومات العالمية (الإنترنت)، حيث تمخض عن استخدام هذه الأجهزة، وما توفر لديها من برامج بعض الجريمة، أو الأفعال التي يمكن وضعها في إطار الأفعال الإجرامية مكتملة العناصر، على أقل تقدير من الناحية النظرية، والتي يمكن كذلك تصنيفها في إطار فهمنا لها كجريمة في القانون العام، وذلك لغياب أو عدم وجود قانون خاص يتناول هذه الأفعال بالتجريم. ذلك لأن الحاسب الآلي نفسه، لم يكن في تصور أو في ذهن المشرع السوداني، حينما وضع القانون الجنائي لسنة 1991م. والذي أعقبه صدور قانون خاص بالجريمة المعلوماتية في العام 2007م.

كما أن مشكلة البحث تتمثل في عدم وجود التشريعات الكافية وذلك نسبة لأن الجريمة المعلومات من الأشياء الجديدة على هذا العصر، كما تمثلت في أن التقنية المعلوماتية أدت إلى ظهور مشاكل قانونية عجزت عنها القوانين القائمة لمواجهتها.

أهمية البحث:

1/ تتبع أهمية البحث من كون أن الجريمة الإلكترونية هي جريمة العصر وهي الأدوات المتوفرة حالياً.

2/ يكتسب موضوع البحث أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثة كالفاكس والإنترنت ووسائل صور الاتصال الإلكتروني عبر الأقمار الاصطناعية في الجريمة الإلكترونية.

أهداف البحث:

يهدف هذا البحث إلى إثبات حجية الدليل الإلكتروني في قانون الإثبات السوداني، كما يهدف إلى مقارنة القانون السوداني مع بعض القوانين العربية في حجية الإثبات الإلكترونية.

منهج البحث:

بغيــة تحقيــق أكبــر قــدر مــن الفائــدة، اتبعــت الدراســة المــنهج الوصــفي والتحليلــي والمــنهج الاســتقرائي فــي اســتعراض موضــوعاتها، وذلــك فــي تنــاول حجية الدليل الإلكتروني في الإثبات الجنائية

هيكل البحث:

اشـتمل هـذا البحـث علـى مقدمـة وفصـلين وكـل فصـل اشـتمل علـى عـدة مباحـث، حيـث تناولـت المقدمـة مشـكلة البحـث – أهميـة البحـث – أهـداف البحـث – منهج البحث – هيكل البحث.

وتطرقنــا فــي الفضــل الأول لمفهــوم وأنــواع الــدليل الإلكترونــي وقســم الفصــل إلــى ثلاثــة مباحــث؛ تنــاول الأول الجــرائم الإلكترونيــة، والثــاني مفهــوم الأدلة الجنائية الإلكترونية، والثالث وسائل جمع الأدلة الإلكترونية.

فــي الفصــل الثــاني تحــدثنا علــى حجيــة الــدليل الإلكترونــي وأيضــاً قسم إلــى ثلاثــة مباحــث؛ تطــرق الأول لحجيــة الــدليل الإلكترونــي، والثــاني تطــرق للقيمــة القانونيــة للــدليل الإلكترونــي فــي مجــال الإثبــات الجنــائي، أمــا الثالــث تطــرق لمشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي.

وخــتم البحــث بخاتمــة اشــتملت علــى النتــائج والتوصــيات، وذيــل بقائمــة المصـــــــــــــــــــــــــــــــادر والمراجـــــــــــــــــــــــــــــــــــع.

الفصل الأول

مفهوم وأنواع الدليل الإلكترونية

المبحث الأول: تعريف الجريمة الإلكترونية وأنواعها

المبحث الثاني: مفهوم الأدلة الجنائية الإلكترونية

المبحث الثالث: وسائل جمع الأدلة الإلكترونية ومقارنتها

تمهيد:

أن القانون في مفهوم كثير من الناس ما هو إلا تعبير عن احتياجات المجتمع أو هكذا ينبغي أن يكون. ومن ثم فإن أوامره ونواهيه، ما هي إلا تنظيم لما ينشأ في المجتمع من علاقات، ولذلك فإنه من الطبيعي، أن ينشغل ويهتم القائمون على أمره وفروعه المختلفة بمراجعة النصوص الموجودة كلما جدّ جديد، في أمور المجتمع للاطمئنان على أن هناك ما يواجه القادم الجديد، أو النظر فيما ينبغي عمله إزاءه، وليس ذلك من قبيل الوقوف في وجه القادم الجديد، ولكن من باب التحوط لما ينشأ من إشكاليات، ولهذا فإننا سوف نتناول في هذا الفصل بالعرض والتوضيح مفهوم الدليل الجنائي بصفة عامة والدليل الجنائي المادي على وجه الخصوص، وصولاً إلى تعريف الدليل الرقمي، وتحديد موقعه بين الأدلة الجنائية وبيان حكمه شرعاً وقانوناً، ولحداثة مفهوم الأدلة الجنائية الرقمية وندرة مراجعها وتطبيقاتها في الدول العربية، نعول على بعض الدراسات وتجارب المجتمعات المتقدمة تقنياً والتي أيقنت بسلامة منطق الأدلة الرقمية ومنظورها العلمي، وذلك من خلال التالي:

المبحث الأول

تعريف الجريمة الإلكترونية وأنواعها

في هذا المبحث سوف نتعرف على الجريمة الإلكترونية في مطلب أول، ومن ثم نعرج إلى أنواع الجريمة الإلكترونية مطلب ثاني كالآتي:

المطلب الأول: تعريف الجريمة الإلكترونية:

أن ظاهرة جرائم الكمبيوتر والإنترنت، أو جرائم التقنية العالية كما يطلق عليها البعض، أو الجرائم الإلكترونية في أحيان أخرى، أو جرائم الياقة البيضاء ظاهرة إجرامية مستجدة ومستحدثة، إلا أنها تستهدف المعطيات

بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج). وقيم مادية ومعنوية بكافة أنواعها ولهذا ينبغي الالتفات بجدية لمعالجة هذه الظاهرة[1].

جاء تعريف الجريمة الإلكترونية في الإطار العربي حينما أقامت الجامعة العربية الندوة العربية في إطار تعريف الجريمة المنظمة وجاء تعريف الجريمة المنظمة بأنها "كل سلوك إجرامي ترتكبه مجموعة من الأشخاص يحترفون الإجرام بشكل مستمر لتحقيق أهدافهم ضمن نطاق أكثر من دولة"[2].

المطلب الثاني: أنواع الجريمة الإلكترونية:

الجريمة الإلكترونية صارت تتم بأشكال وأنواع متعددة مستحدثة بالنسبة لمجتمعاتنا العربية المختلفة، وذلك لطابع الحداثة والجدة الذي صاحبها، وعليه يمكننا تناول بعض أنواعها وفق الآتي:

1/ التجسس الإلكتروني:

لقد ارتبطت غالبية دولنا العربية في الآونة الأخيرة بشبكة الإنترنت. وشهدت بدايات هذا القرن في السودان الانتشار الواسع لاستخدام شبكة الإنترنت بعد ازدياد استعمال الحاسب الآلي بصفة عامة، ولقد توسع استخدام الحاسب الآلي لدى الأفراد والوحدات الحكومية على السواء وكذلك في الوحدات الإدارية والعلمية والبحثية وازدادت في ذات الوقت الأخطار التي يمكن أن تتعرض لها شبكات البيانات الحكومية في معظم الدول العربية ومن بينها السودان، ولا يكمن الخطر في مجرد ارتباط هذه الدول أو المؤسسات الحكومية بشبكة الإنترنت أو الشبكات العالمية الأخرى فقط، ولكن في الضعف الأمني لمعظم الشبكات الحكومية في الوطن العربي، واعتماد

---

[1] أحمد حسام طه تمّام، **الجرائم الناشئة عن استخدام الحاسب الآلي**، دار النهضة العربية، القاهرة، 2000م، ص: 22.

[2] **الندوة العربية حول الجريمة الإلكترونية**، الجامعة العربية – القاهرة، الخرطوم 1998/2/1م.

الشبكات العربية بصورة أساسية على الشبكة العالمية. وغياب التواصل العربي في مجال الاتصال الإلكتروني ولا شك أن معظم خبراء الشبكات يعرفون أدق التفاصيل عن الشبكة العالمية وهي بذلك سهلة الاختراق نسبيا إذا لم تتوفر بعض الحلول الأمنية لهذه الشبكات[1].

2/ الحرب الإلكترونية:

أنها الحرب غير المنظورة التي تقع في واقع افتراضي وبهذه العبارة صرح السيد/ حبيب العدلي وزير الداخلية المصري السابق أمام مؤتمر وزراء الداخلية العرب معربا عن تزايد جرائم الإنترنت على نحو هائل وقال انه يتعين بصورة قاطعة التصدي للمخاطر التي أفرزتها ثورة الاتصالات الحديثة, حيث أن بعض المنظمات أنشأت دولا افتراضية على شبكات الإنترنت تجاوزت الحدود والرقابة[2].

ثانياً: القرصنة عبر الإنترنت:

إن الخطر الثاني الناجم عن استخدام شبكة الإنترنت والحاسب الآلي على السواء هو خطر القرصنة عبر الإنترنت ذلك أن نمط القرصنة التقليدية قد تغير إلى قرصنة عبر الإنترنت وهذا ما أعلنته أحدث دراسات اتحاد البرمجيات وهي منظمة تمولها كبرى شركات البرمجيات في العالم مثل مايكروسوفت ولوتس لمراجعة وتحليل سوق البرمجيات[3].

القرصنة في الدول العربية:

---

[1] يونس عرب، **جرائم الكمبيوتر والإنترنت**، ص: 152، وموقع: www.unicfing.hotmail.com على شبكة الإنترنت.

[2] يونس عرب، **جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص: 153.

[3] محسن شفيق، **نقل التكنولوجيا من الناحية القانونية**، جامعة القاهرة، 1984م، ص: 91.

لا يبدو للمتتبع والدارس وجود اهتمام واضح في معظم الدول العربية بالتشريع الذي يكافح القرصنة في البرمجيات والأقراص المدمجة، ويعود ذلك إلى وضع هذه الدول باعتبارها دولاً مستهلكة وليست منتجة للبرمجيات حيث لا يحدث في الدول العربية سوى القليل من إنتاج البرمجيات.

ثالثاً: الجرائم المنظمة عبر الإنترنت:

تعد الجريمة المنظمة وعاءاً إجرامياً يضم صور إجرام القرن الحادي والعشرين ولقد حددت التوصية الأولى من ندوة الجريمة المنظمة عبر الحدود العربية (جامعة الدول العربية – القاهرة، 1998/11/2م) عدداً من الأمثلة البارزة لهذه الصور ومنها صورة الجرائم الإلكترونية، ولكن يلاحظ أن هذه الجرائم لا تحتل مكانة الخطورة الإجرامية الممنوحة لجرائم المخدرات وغسيل الأموال، إلا أنها تلتقي في النتائج الضارة بالمجتمع الوطني والعربي والعالمي، وذلك على مستوى النواحي الاقتصادية والسياسية والاجتماعية، فالجرائم الإلكترونية ذات نشاط إجرامي معقد تنفذها جماعات على درجة كبيرة من التنظيم تستهدف الثراء والسكب غير المشروع بصورة مستمرة[1].

رابعاً: غسيل الأموال عبر الإنترنت:

تمثل ظاهرة ما يعرف بغسيل الأموال وعائدات الجرائم إحدى الظواهر التي أقلقت مضاجع العالم في الآونة الأخيرة، وتتم عملية غسيل الأموال بأساليب وأشكال عديدة تتدرج من البساطة إلى التعقيد وحسب ظروف طبيعة العملية، وقد كان للتكنولوجيا دور خطير في تطوير الأساليب التي تستخدم

---

[1] د. عبد الرحيم صدقي، **الإجرام المنظم في مصر والبلاد العربية**، كلية الحقوق، جامعة القاهرة، 2001م، ص: 75. وانظر أيضاً: موسوعة صدقي في القانون الجنائي، المجلد التاسع، دار النهضة العربية، القاهرة، 1986م، 9. وانظر أيضاً: الورقة التي قدمها في الندوة المصاحبة لاجتماع مجلس وزراء العدل العرب بالخرطوم في الفترة من 4 – 6 مارس 2002م.

لغسيل الأموال ولعل التهريب هو أبسط وأقدم الوسائل التي أستخدمها غاسلو الأموال كما استخدمت أساليب أخرى مثل شركات الواجهة، والقيام ببعض التصرفات العينية المادية.

ولكن المتعامل مع البنوك السيبرانية يقوم بإدخال الشفرة السرية من أرقام أو خلافه أو طباعتها على الكمبيوتر ومن ثم تحويل أموال بالطريقة التي يأمر بها الجهاز وهذه الوسيلة تتيح لغاسلي الأموال، نقل أو تحويل كميات ضخمة من الأموال بسرعة وأمان.

خامساً: تجارة المخدرات عبر الإنترنت:

لقد بدأ لنا وبعد فحص دقيق لأحوال وأعمار مستخدمي شبكة الإنترنت في الوطن العربي أن نسبة كبيرة منهم، هي من طائفة الشباب، وأن معظمهم من المراهقين. ولهذا حرص المواطنون العرب وفي مختلف البلدان العربية علي الاهتمام بشئون أبناءهم، وعلى وجه التحديد المراهقين منهم، من خطر ظاهرة انتشار المخدرات. إلا أن هذا الحرص والاهتمام أصبح أمراً صعباً بعد انتشار استخدام الشبكة العالمية للإنترنت، والتي أصبحت المخدرات تستعملها كسوق مغرية حيث أصبح في الإمكان لأي شخص أن يكتشف كيفية الحصول على المخدرات، من خلال هذه الشبكة، بل وأن يتعلم كيفية استنشاق الهيروين، والكوكايين وأن يتعرف على أسعار الماريجوانا والمخدرات الرقمية، وأن يتعرف على الصيغة الكيميائية للمينا فيتامين المنشط الكيميائي المعروف والأكثر انتشاراً[1].

أما المخدرات الرقمية: هي "عبارة عن ملفات صوتية يتم تحميلها عبر مواقع إنترنت عالمية معروفة, أو من خلال رسالة بينية وهذه الملفات الصوتية

[1] د. عبد الرحيم صدقي، **الإجرام المنظم في مصر والبلاد العربية**، مرجع سابق، ص: 79.

بهـا نغمـات حيـث يسـمعها الإنسـان فـي كـل أذن بتـردد مختلـف, ويعـادل الأثـر الـذي يتركـه الملـف الأثـر ذاتـه مـن تـدخين سـيجارة مـن الحشـيش أو تنـاول جرعـة مـن الكوكـايين, ولهـا تـأثير المخـدرات والجـنس والرعـب..." الأمـر الـذي يـؤدي إلـى الحصـول علـى مـزاج خـاص ترغـب فيـه الفئـات العمريـة الشـبابية تحديـداً ممـن يتقيـد ويحـذر مـن اللجـوء إلـى المخـدرات التقليديـة لأسـباب اجتماعيـة أو دينيـة اعتقـاداً مـنهم أن هـذه الممارسـة لـم يشـكل أو يعتـرض عليهـا أحـد أو يحرمهـا الـدين بوصـفها غيـر مشـاعة بعـد أو لأنهـا لا تكشـف عـن أدلتهـا الماديـة الجرميـة, لكـن المهـم هـو تحقـق النشـوة لهـم أو حالـة السـكر القريبـة مـن حالـة السـكر المعروفة[1].

وتجـدر الإشـارة هنـا إلـى أن تصـنيف الجـرائم الإلكترونيـة تشـوبه الكثيـر مـن المشـاكل فلـذا نجـد عـدة تصـنيفات لهـذه الجـرائم ويمكـن حصـر هـذه التصنيفات في الآتي:

أولاً: تصنيف الجرائم الإلكترونية تبعاً لنوع ومحل الجريمة والمعطيات:

هـذا التصـنيف تـزامن مـع موجـات التشـريع فـي ميـدان تقنيـة المعلومـات، فـي بعـض البلـدان العربيـة والأجنبيـة وهـذا التصـنيف يعكـس وبصـورة واضـحة أيضـاً .التطـور التـاريخي لظـاهرة الجـرائم الإلكترونيـة أو جـرائم الكمبيـوتر والإنترنـت، وهـو التصـنيف السـائد فـي مختلـف مؤلفـات الفقيـه ألـرش سـلبر (Ulrich Sileber) وهـو مـن فقهـاء القـانون الفرنسـي والمؤلفـات المتـأثرة بـه، وعلـى ضـوء هـذا التصـنيف يمكـن تقسـيم الجـرائم الإلكترونيـة إلـى ثلاثـة أنـواع، وهي:

---

[1] أ. د. محمد حسين حبيب، ورقة عمل بعنوان: **المخـدرات الرقميـة بـين الحقـوق الشخصـية والجريمـة السـيبرانية**، مقدمـة لفعاليـات الأيـام العربيـة للأمـن السـيبراني: أفـق التعـاون لحمايـة الفضـاء السـيبراني، العراق، 1-2015/12/2م، ص: 2.

- الجرائم الماسة بقيمة معطيات الحاسب الآلي.
- الجرائم الماسة بالمعطيات الشخصية.
- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسب الآلي ونظمه وجرائم القرصنة للبرمجيات "قرصنة البرمجيات"[1].

ثانياً: تصنيف الجريمة الإلكترونية تبعاً لدور الكمبيوتر في الجريمة:

يقسم بعض الفقهاء الجرائم الإلكترونية إلى جرائم هدف ووسيلة. وتبعاً لذلك تم تصنيف الجريمة الإلكترونية إلى جرائم تستهدف نظام المعلومات كالاستيلاء على المعلومة وإتلافها وجرائم ترتكب بواسطة الحاسب الآلي كجرائم الاحتيال. أما تقسيمها كجرائم هدف ووسيلة ومحتوى فيعتبر الاتجاه العالمي الجديد في ضوء تطور التدابير الشرعية في بعض بلدان أوروبا، والغرب بصفة عامة ولعل أبرز ما يلقي الضوء على هذا التقسيم مشروع الاتفاقية الأوروبية لجرائم الحاسب الآلي "الكمبيوتر" والإنترنت لعام 2000م – 2001م. ولقد أوجد مشروع الاتفاقية الأوروبية تقسيماً جديداً وهو تقسيم نسبى إلى حد ما حيث تضمن أربع طوائف رئيسية، هي:

1/ الجرائم التي تستهدف عناصر المعطيات والنظم وتضم:

(أ) الدخول غير القانوني "غير المصرح به".

(ب) الاعتراض غير القانوني.

(ج) تدمير المعطيات.

(د) إساءة استخدام الأجهزة.

2/ الجرائم المرتبطة بالحاسب الآلي:

---

[1] انظر: **حكومة السودان/ ضد/ مجدي مصطفى البغدادي**، محكمة الملكية الفكرية الخرطوم، غير منشورة.

(أ) التزوير المرتبط بالحاسب الآلي.

(ب) الاحتيال المرتبط بالحاسب الآلي.

3/ الجرائم المرتبطة بالمحتوى: وتضم طائفة واحدة وفقاً لهذه الاتفاقية (مشروع الاتفاقية الأوربية لجرائم الحاسب الآلي) وهي الجرائم المتعلقة بالأفعال الإباحية واللا أخلاقية.

4/ الجرائم المرتبطة بالإخلال وبحقوق الملكية الفكرية وعلى وجه التحديد الجرائم المرتبطة بالتعدي على حق المؤلف والحقوق المجاورة أو فيما يعرف بقرصنة البرمجيات[1].

ثالثاً: تصنيف الجريمة الإلكترونية تبعاً لمساسها بالأشخاص والأموال:

يصف الأستاذ/ يونس عرب هذا التصنيف بأنه الشائع في الدراسات والأبحاث الأمريكية كما أنه المعيار المتبع في تقسيم الجرائم الإلكترونية في مشروعات القوانين النموذجية وأشار في هذا الصدد إلى مشروع نموذجي يسمى "Model State Computer Crime Code":

وفي نطاق هذا القانون النموذجي تقسم الجرائم الإلكترونية إلى:

1/ الجرائم الواقعة على الأشخاص.

2/ الجرائم الواقعة على الأموال عدا السرقة.

3/ جرائم السرقة والاحتيال.

4/ جرائم التزوير والمقامرة والجرائم المنافية للآداب.

5/ الجرائم الماسة بالمصالح الحكومية[1].

---

[1] يونس عرب، **جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص: 134.

وتبعاً لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي فإن تصنيف الجريمة جاء على النحو الآتي:

أولاً: طائفة الجرائم التي تستهدف الأشخاص:

الجرائم غير الجنسية التي تستهدف الأشخاص وتشمل هذه الطائفة جرائم القتل بالحاسب الآلي وجرائم الإهمال المرتبط بالكمبيوتر والتي تسبب الوفاة والتحريض على الانتحار عبر الإنترنت وهنالك جرائم التحرش والمضايقة عبر وسائل الاتصال والإضرار المتعمد وذلك بإحداث الضرر العاطفي أو تسبيب ضرر عاطفي عبر وسائل التقنية وغيرها.

ومنها طائفة الجرائم الجنسية وتشمل هذه الطائفة ضمن التقسيم مجموعة جرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية ومحاولة إغواء القاصرين بارتكاب أنشطة جنسية غير مشروعة والتحرش الجنسي بالقاصرين أو تلقي ونشر المعلومات عبر الإنترنت عن القاصرين، من أجل أنشطة جنسية غير مشروعة[2].

ثانياً: الجرائم المتعلقة بالأموال عدا السرقة:

تشمل هذه الطائفة الاقتحام أو الدخول أو التوصل غير المصرح به مع نظام الحاسب الآلي، أن كان الدخول مجرداً أو لحجة ارتكاب فعل معين في الموقع المقتحم أو بقصد ارتكاب فعل أخر ضد البيانات والبرامج والمخرجات.

ويقع تخريب المعطيات ضمن مفهوم تخريب الحاسب الآلي وإيذائه واغتصاب ملكية البرامج وخلق البرمجيات الخبيثة والضارة والفيروسات، ونقلها

---

[1] ماهر الجنيدي، **رائحة الماريجوانا تنبعث من أوكار إنترنت**، مجلة إنترنت العالم العربي، نوفمبر 1999م، ص: 39 – 40.

[2] ماهر الجنيدي، **رائحة الماريجوانا تنبعث من أوكار إنترنت**، مرجع سابق، ص: 63.

عبر الإنترنت والشبكات، ويدخل فيها أيضاً استخدام أسم النطاق أو النافذة أو العلامة التجارية أو اسم الغير دون ترخيص وهي طائفة واسعة محلها نشاط أو مجال التجارة الإلكترونية وحقوق الملكية الفكرية والصناعية. والمواقع المالية مثل البنوك والصرافات الإلكترونية[1].

ثالثاً: طائفة جرائم الاحتيال والسرقة:

هذه الطائفة من أكبر وأوسع الجرائم انتشاراً حتى الآن, وهي تشمل جرائم الاحتيال عن طريق التلاعب بالمعطيات والنظم واستخدام الكمبيوتر للحصول على البطاقات المالية للغير. وهذه الجرائم تشمل أيضاً عمليات التدمير عبر الحاسب الآلي أو بواسطته، وسرقة معلومات الحاسب الآلي وكذلك سرقة أدوات التعريف والهوية، عبر انتحال الصفات أو المعلومات داخل الكمبيوتر.

رابعاً: طائفة جرائم التزوير:

وتشمل هذه الطائفة تزوير البريد الإلكتروني وتزوير الرقائق والسجلات وتزوير الهوية، أو تزوير بطاقات الائتمان والمستندات العادية المعدة بواسطة الحاسب الآلي، أو الأجهزة المساعدة له مثل أجهزة التصوير الإلكتروني. أو تزوير التوقيع الإلكتروني والبصمة الإلكترونية وتزوير بطاقات الائتمان وبطاقات الدفع الإلكتروني.

خامساً: طائفة جرائم المقامرة والجرائم الضارة بالصحة:

---

[1] د. محمد السيد اليماني، **الجوانب القانونية لدور براءة الاختراع في نقل التكنولوجيا**، مجلة الدراسات القانونية، العدد الثاني، كلية الحقوق، جامعة أسيوط، 1980م، ص: 9.

تشمل هذه الطائفة تملك وإدارة مشروعاً للمقامرة على الإنترنت مثال ذلك: ما يعرف الآن ببطاقات الاشتراك في برنامج البنتاغون، وهو عبارة عن برنامج اشتراك مالي يصبح فيه الفرد رابحاً إذا تمكن من إحضار عدد من المشتركين ويزداد ربحه كلما احضر مشتركين جدد. وهو برنامج تسهل فيه مشاريع إدارة القمار على الإنترنت أو تشجيع مشاريع المقامرة عبر الإنترنت، أو استخدام الحاسب الآلي وشبكة الإنترنت للترويج للكحول ومواد الإدمان الأخرى كالحشيش والأفيون وسائر المخدرات المعروفة عالمياً ومحلياً.

سادساً: الجرائم الإلكترونية الماسة بالحكومة:

تشمل هذه الطائفة من الجرائم قطاع واسع بحيث تضم كافة جرائم تعطيل الأعمال الحكومية، أو تعطيل تنفيذ القانون، أو تهديد السلامة العامة ويشمل ذلك: الإرهاب الإلكتروني والأنشطة الثأرية. وأنشطة التدمير والاختراق الإلكتروني وأقرب مثال لذلك ما قام به أحد الهواة من القصر بتدمير موقع سودانت في شبكة الإنترنت مؤخراً[1].

سابعاً: تصنيف الجرائم الإلكترونية كجرائم حاسب آلي وجرائم إنترنت:

إن استخدام الشبكة العالمية للاتصال والمعروفة اختصاراً باسم (الإنترنت) (www.) وهي تعتبر من وسائل الاتصال العالمية التي راج استخدامها عالمياً. بدأت كظاهرة بظهور الحاسب الآلي في الحياة العامة وتطورت من وسيلة للاتصال إلى استخدامها في ارتكاب الجرائم تبعاً لما حدث من تطور تقني ونتيجة لهذا التطور كان لابد من ظهور مفهومين جديدين لجرائم ترتكب علي الحاسب الآلي وبواسطته وتسمى الأولى جرائم الحاسب الآلي، كما أن ظهور الشبكة العالمية للمعلومات والاتصالات (الإنترنت) أفرز

---

[1] محمد إبراهيم السيف، **الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي: بين التصور الاجتماعي وحقائق الاتجاه الإسلامي**، مكتبة العبيكان، الرياض، 1417هـ، ص: 107.

أنماطـاً إجراميـة مسـتحدثة مرتبطـة فقـط بهـذه الشـبكة وسـميت باسـمها وهـي الثانية.

ونعـود ونقـول أن هـذا التقسـيم والـذي اعتمـد علـى نطـاق اسـتهداف الفعـل الإجرامـي للحاسـب الآلـي وشـبكة الإنترنـت تصـنيفً غيـر دقيـق بـل ومخـالف لمـا وصـل إليـه التقـدم التقنـي وعمليـات التكامـل والـدمج التـي تمـت بـين الحوسـبة ووسـائل الاتصـال، الأمـر الـذي جعـل شـبكات الاتصـال جـزءاً لا يتجـزأ مـن الحاسب الآلي بل هي من ضمن فكرة متكاملة في نطاق نظام الحاسب الآلي.

الجريمة الإلكترونية في القانون السوداني:

صـدر فـي السـودان قـانون جـرائم المعلوماتيـة لسـنة 2007م, والـذي أسـس لتجـريم الأفعـال التـي تسـتهدف نظـم ووسـائط وشـبكات المعلومـات هـذا القـانون يعتبـر نسـبياً مـن أحـدث القـوانين العربيـة, مـن حيـث تـاريخ صـدوره, حيـث سـعى فيـه المشـرع إلـى اسـتيعاب تجـارب الآخـرين حسـبما ورد فـي المـذكرة التفسـيرية لـه فأخـذ بمـا جـاء فـي القـوانين النموذجيـة العربيـة وقـوانين الـدول الغربيـة وخلافـاً لقـوانين الـدول العربيـة التـي سـبقته فقـد جـرم طائفـة واسـعة مـن الأفعـال, وفـي إطـار هـذا التجـريم نـص المشـرع علـي أفعـال معينـة خصـها بالـذكر وحـدد عقوباتهـا وهـي تنحصر في الآتي:

أولاً: دخول المواقع وأنظمة المعلومات المملوكة للغير:

جـرم هـذا القـانون دخـول المواقـع وأنظمـة المعلومـات مـن موظـف عـام أو أي شـخص آخـر وفـي هـذا جـرم كـل مـن يـدخل موقعـاً أو أي نظـام معلومـات دون أن يكون مصرحاً له بدخوله ويقوم بناءا علي هذا الدخول بالآتي:

(أ) بـالإطلاع عليـه أو نسـخه (وعاقـب علـي ذلـك الفعـل بالسـجن مـدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معاً).

(ب) أو يقوم بإلغاء بيانات أو معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه وعاقب القانون من يقوم بذلك الفعل بالسجن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً كم جرم أيضاً في إطار هذه الجريمة فعل دخول المواقع وأنظمة المعلومات من موظف عام فعاقب كل موظف عام يدخل بدون تفويض موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير وعاقبه بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً وهي تعتبر عقوبة مشددة خاصة بالموظف العام وفقاً لصفة الائتمان المفترضة فيه[1].

ثانياً: التنصت أو التقاط أو اعتراض الرسائل:

جرم المشرع فعل التنصت فكل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً ولم يحدد المشرع الغرض من التنصت أو الاعتراض وكان ينبغي أفراد فقرة خاصة بتشديد العقوبة إذا كان الغرض من هذا الفعل التجسس على الأسرار الحكومية أو العسكرية كما الحال بشأن القانون الأمريكي الذي يعاقب بشدة علي التجسس علي أسرار البنتاجون[2].

---

[1] المادة (4) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

[2] انظر: المادة (6) من قانون جرائم المعلوماتية السوداني لسنة 2007م والتي تنص على: (كل من يتصنت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً).

ثالثـاً: جريمـة دخـول المواقـع عمـداً بقصـد الحصـول علـى بيانـات أو معلومـات أمنية:

فـي هـذه الجريمـة عاقـب المشـرع كـل مـن يـدخل عمـداً موقعـاً أو نظامـاً مباشـرة أو عـن طريـق شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب ومـا فـي حكمهـا بغرض الآتي:

أ/ الحصول على بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً،

ب/ إلغـاء بيانـات أو معلومـات تمـس الأمـن القـومي للـبلاد أو الاقتصـاد الـوطني أو حـذفها أو تـدميرها أو تغييرهـا يعاقـب بالسـجن مـدة لا تتجـاوز عشـر سـنوات أو بالغرامـة أو بـالعقوبتين معـاً, وكـأني بـه أراد سـد الخلـل فـي عـدم تشـديد جريمـة التنصـت فـي حـال أن الغـرض منهـا هـو التجسـس وإيقـاف أو تعطيـل أو إتـلاف البـرامج أو البيانـات أو المعلومـات فـي هـذه الجريمـة عاقـب المشـرع السـوداني كـل مـن يـدخل بـأي وسـيلة نظامـاً أو وسـائطاً أو شـبكات المعلومـات ومـا فـي حكمهـا ويقـوم عمـداً بإيقافـها أو تعطيلهـا أو تدميـر البـرامج أو البيانـات أو المعلومـات أو مسـحها أو حـذفها أو إتلافهـا بالسـجن مـدة لا تتجـاوز سـت سـنوات أو بالغرامـة أو بـالعقوبتين معـاً وجريمـة الإتـلاف الإلكترونـي هـي مـن أخطـر أنـواع الجـرائم إذ أن مـا يتلـف إلكترونيـاً لا يمكـن إصـلاحه بسـهولة, خاصـة إذا كانـت المعلومـة الإلكترونيـة بـين برمجيـات معقـدة ومرتبطـة بأنظمـة التشغيل،

ج/ إعاقة أو تشويش أو تعطيل الوصول للخدمة،

د/ فـي هـذه الجريمـة عاقـب المشـرع كـل مـن يعـوق أو يشـوش أو يعطـل عمـداً وبـأي وسـيله الوصـول إلـى الخدمـة أو الـدخول إلـى الأجهـزة أو البـرامج أو

مصـــادر البيانـــات أو المعلومـــات عـــن طريـــق شـــبكة المعلومـــات أو أحـــد أجهـــزة الحاســـوب أو مـــا فـــي حكمهـــا بالســـجن مـــدة لا تتجـــاوز ســـنتين أو بالغرامـــة أو بـــالعقوبتين معـــاً, وهـــي جريمـــة تفـــرد بهـــا القـــانون الســـوداني لجـــرائم المعلوماتيـــة اعتبار أن الجاهزية التقنية في توفير جدر الحماية غير متوفرة[1].

رابعاً: الجرائم الواقعة على الأموال والبيانات والاتصالات:

فـي هـذه الطائفـة مـن الجـرائم عاقـب المشـرع السـوداني علـى ارتكـاب جملـة مـن الأفعـال تطـال الأمـوال أيـاً كـان شـكلها والبيانـات والاتصـالات فعاقـب علـى ارتكـاب جريمـة التهديـد أو الابتـزاز فكـل مـن يسـتعمل شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب أو مـا فـي حكمهـا فـي تهديـد أو ابتـزاز شـخص آخـر لحملـه علـى القيـام بفعـل أو الامتنـاع عنـه ولـو كـان هـذا الفعـل أو الامتنـاع مشـروعاً يعاقـب بالسـجن مـدة لا تتجـاوز سـنتين أو بالغرامـة أو بـالعقوبتين معـاً[2]. وعاقـب أيضـاً علـى الاحتيـال أو انتحـال صـفة غيـر صـحيحة فكـل مـن يتوصـل عـن طريـق شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب ومـا فـي حكمهـا عـن طريـق الاحتيـال أو اسـتخدام اسـم كـاذب أو انتحـال صـفة غيـر صـحيحة بغـرض الاسـتيلاء لنفسـه أو لغيـره علـى مـال أو سـند أو توقيـع للسـند يعاقـب بالسـجن مـدة لا تتجـاوز أربـع سـنوات أو بالغرامـة أو بـالعقوبتين معـاً[3]. وكـذلك عاقـب علـي فعـل الحصـول علـى أرقـام أو بيانـات بطاقـات الائتمـان فكـل مـن يسـتخدم شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب ومـا فـي حكمهـا للوصـول إلـى أرقـام أو بيانـات للبطاقـات الائتمانيـة أو مـا فـي حكمهـا بقصـد اسـتخدامها فـي الحصـول علـى بيانـات الغيـر أو أموالـه أو مـا تتيحـه تلـك البيانـات أو الأرقـام مـن خـدمات يعاقـب بالسـجن مـدة

---

[1] المادة (7) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

[2] المادة (10) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

[3] المادة (11) من نفس القانون.

لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً[1]. أيضاً جرم المشرع السوداني في إطار حملته الواسعة لتجريم بعض الأعمال الإلكترونية فعل الانتفاع دون وجه حق بخدمات الاتصال فكل من ينتفع دون وجه حق بخدمات الاتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً[2].

خامساً: جرائم النظام العام والآداب:

تحت هذه الطائفة جرم المشرع الأفعال المخلة بالنظام العام والآداب في البيئة الإلكترونية فكل من ينتج أو يعد أو يهيئ أو يرسل أو يخزن أو يروج عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها أي محتوى مخل بالحياء أو النظام العام أو الآداب يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً كما جرم أيضاً كل من يوفر أو يسهل عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها للوصول لمحتوى مخل بالحياء أو منافٍ للنظام العام أو الآداب ويعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً[3].

وشدّد في العقاب إذا وجه الفعل المشار إليه في الأفعال السابقة إلى حدث, حيث يعاقب مرتكبها بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً أيضاً في إطار ملاحقة الأفعال المخلة بالآداب والنظام العام جرم المشرع السوداني إنشاء أو نشر المواقع بقصد ترويج أفكار

---

[1] المادة (12) من نفس قانون.

[2] المادة (13) من نفس قانون.

[3] المادة (14) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

وبـرامج مخالفـة للنظـام العـام أو الآداب فعاقـب كـل مـن ينشـئ أو ينشـر أو يسـتخدم موقعـاً علـى الشـبكة المعلوماتيـة أو أحـد أجهـزة الحاسـوب أو مـا فـي حكمهـا لتسـهيل أو تـرويج بـرامج أو أفكـار مخالفـة للنظـام العـام أو الآداب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً[1].

سادساً: انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة:

تحـت هـذه الطائفـة جـرم المشـرع فـي هـذا القـانون كـل مـن ينتهـك أو يسـئ أي مـن المعتقـدات الدينيـة أو حرمـة الحيـاة الخاصـة عـن طريـق شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب أو مـا فـي حكمهـا وعوقـب بالسـجن مـدة لا تتجـاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً[2].

سابعاً: جريمة إشانة السمعة:

جريمـة إشـانة السـمعة عـن طريـق الوسـائط الإلكترونيـة تعتبـر مـن الأفعـال سـريعة الانتشـار فـي ظـل تنـامي الاسـتخدام الواسـع للإنترنـت ولهـذا فـإن تجـريم إشـانة السـمعة عبرهـا قـد أفـرد لـه المشـرع عقوبـة خاصـة, فـي ظـل قـانون الجـرائم الالكترونيـة, فكـل مـن يسـتخدم شـبكة المعلومـات أو أحـد أجهـزة الحاسـوب أو مـا فـي حكمهـا لإشـانة السـمعة يعاقـب بالسـجن مـدة لا تتجـاوز سـنتين أو بالغرامـة أو بـالعقوبتين معـاً, ويلاحـظ أن المشـرع لـم يتنـاول تعريفـاً خاصـاً بجريمـة إشـانة السـمعة الإلكترونيـة وإنمـا تـرك ذلـك وفقـاً لمـا ورد فـي القـانون الجنـائي العـام مـن تعريـف لإشـانة الشـمعة, مـع الوضـع فـي الاعتبـار اخـتلاف الوسـيلة المرتكـب بهـا الجريمة إلكترونياً[3].

ثامناً: جرائم الإرهاب والملكية الفكرية:

---

[1] المادة (15) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

[2] المادة (16) من قانون جرائم المعلوماتية السوداني لسنة 2007م.

[3] المادة (17) من القانون السابق.

هذه الطائفة من الجرائم تحتوي على نوعين من الأفعال الأولى منها هي أفعال إنشاء أو نشر المواقع للجماعات الإرهابية والثانية هي نشر المصنفات الفكرية ففي الأفعال الأولى جرم المشرع في المادة (18) من قانون جرائم المعلومات التي تنص على أن: (كل من ينشئ أو ينشر أو يستخدم موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابية تحت أي مسمي لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً)[1] ومن المعلوم أن هذه الطائفة من الأفعال راج الحديث عنها وتناولها إعلامياً بعد أحداث الحادي عشر من سبتمبر بالولايات المتحدة الأمريكية, ولما كان الإرهاب لا وطن له ولا دين فقد أحسن المشرع صنعاً بالنص على هذه الجريمة.

أما جريمة نشر المصنفات الفكرية في البيئة الإلكترونية فقد جاءت مواكبة للثورة في مجال حماية الملكية الفكرية ولهذا فقد عاقب المشرع السوداني كل من ينشر دون وجه حق عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها أي مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها بالسجن مدة لا تتجاوز سنة أو الغرامة أو بالعقوبتين معاً[2].

فقط نلاحظ إن المشرع جمع بين جرائم الإرهاب الإلكتروني وجرائم الملكية الفكرية بلا أدنى رابط يجمع بينهما والرؤية لدينا أن يتم الفصل بينهما.

تاسعاً: جرائم الاتجار في الجنس البشرى والمخدرات وغسل الأموال:

---

[1] المادة (18) من قانون جرائم المعلوماتية لسنة 2007م السوداني.

[2] المادة (19) من قانون جرائم المعلوماتية لسنة 2007م السوداني.

في سبيل مكافحة كل الأنشطة الإلكترونية التي تروج للجنس والمخدرات وغسل الأموال والاتجار في الجنس البشري عاقب المشرع السوداني كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الاتجار في الجنس البشرى أو تسهيل التعامل فيه بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً وهي من العقوبات المشددة[1].

أما في فعل الاتجار أو الترويج للمخدرات أو المؤثرات العقلية عبر الوسائط الإلكترونية فعاقب المشرع كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية أو ما في حكمها أو يسهل التعامل فيها بالسجن مدة لا تتجاوز عشرين سنة أو بالغرامة أو بالعقوبتين معاً[2]، أما عن الأفعال التي تستهدف غسل الأموال من خلال الوسائط الإلكترونية فعاقب المشرع كل من يقوم بعملية غسل الأموال بالتسهيل أو التحويل أو الترويج أو إعادة تدويرها بواسطة شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ليكسبها الصفة القانونية مع علمه بأنها مستمدة من مصدر غير مشروع ويعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً[3].

من خلال هذا الاستعراض لما أدرجه المشرع السوداني في قانون الجريمة المعلوماتية من أنماط وأشكال الجريمة الإلكترونية يتضح أنه قانون متقدم من حيث تجريم الأفعال. إلا أن ذلك وحده لا يكفي إذ لابد من مواكبة ذلك لطفرة أخرى في مجال قانون الإثبات وقانون الإجراءات الجنائية, حتى يتحرك هذا القانون في مكافحة الجرائم التي تمشي على قدمين ثابتين.

المبحث الثاني
مفهوم الأدلة الجنائية الإلكترونية

---

[1] المادة (20) من قانون جرائم المعلوماتية لسنة 2007م السوداني.

[2] المادة (21) من قانون جرائم المعلوماتية لسنة 2007م السوداني.

[3] المادة (22) من قانون جرائم المعلوماتية لسنة 2007م السوداني.

فـي هـذا المبحـث سـوف نتطـرق لمفهـوم الأدلـة الجنائيـة الإلكترونيـة لغـةً وشـرعاً فـي مطلـب أول، والمفهـوم فـي الاصـطلاح والقـانون فـي مطلـب ثـاني، وتعريف الأدلة الجنائية الإلكترونية في مطلب ثالث، بالتفصيل التالي:

المطلب الأول: مفهوم الأدلة الجنائية لغةً وشرعاً:

تعريـف الـدليل لغـةً: جـاء فـي مختـار الصـحاح أن الـدليل هـو مـا يسـتدل بـه والـدليل الرجـال أيضـاً، وقـد (دلـه) علـى الطريـق يدلـه بالضـم و(دلالـه) بفـتح الـدال وكسـرها و(دلولـه) بالضـم والفـتح أعلـى، ويقـال (أدل) فأمـل والاسـم (الدالـة) بتشديد اللام، وفلان (يدل) بفلان أي يثق[1].

كمـا جـاء أيضـاً فـي تعريـف الـدليل فـي اللغـة هـو المرشـد ومـا بـه الإرشـاد، وما يستدل به. والدليل الدال والجمع أدلة ودلالات[2].

أمـا تعريفـه فـي الشـرع فقـد عرفـه الجرجـاني بأنـه: (هـو مـا يلـزم مـن العلـم بـه العلـم بشـيء آخـر، فـإذا اعلـم القاضـي بحجتـه علـى دعـواه لـزم علـى مـن علـم القاضـي بتلـك الحجـة مـع اقتناعـه بهـا عامـة بصـدق دعـوى المـدعي فيمـا ادعـاه والحكم له به)[3].

---

[1] زيـن الـدين أبـو عبـد الله محمـد بـن أبـي بكـر بـن عبـد القـادر الحنفـي الـرازي، **مختـار الصـحاح**، تحقيـق: يوسـف الشـيخ محمـد، المكتبـة العصـرية – الـدار النموذجيـة، بيـروت – صـيدا، الطبعـة الخامسـة، 1420هـ – 1999م، ج2، ص: 357.

[2] جميل صليباً، **المعجم الفلسفي**، دار كتب اللبناني، بيروت، الطبعة الأولى، 1971م، ص: 35.

[3] علـي بـن محمـد بـن علـي الـزين الشـريف الجرجـاني، **التعريفـات**، حققـه وضـبطه وصـححه: جماعـة مـن العلمـاء بإشـراف الناشـر، دار الكتـب العلميـة، بيـروت، لبنـان، الطبعـة الأولـى، 1403هـ – 1983م، 135/1.

وقال ابن القيم: (هو ما يلزم من العلم به العلم بشيء آخر، فإذا قدم المدعي حجته للقاضي واقتنع الأخير بتلك الحجة لزم عليه الحكم للمدعي فيما ادعاه)[1].

وتستعمل كلمة الدليل في الشرع بمعنى البينة أي الحجة أو البرهان، فالبينة اسم لكل ما يبين الحق، وهنالك رأيان في الفقه الإسلامي في معنى الدليل أو البينة؛ الأول هو رأي جمهور الفقهاء الذي يقوم على ضرورة حصر الأدلة أو البينة والتقيد بها حسبما جاءت قرينة كل جرم بما لا يخرج عن: الإقرار، اليمين، الشهادة، علم القاضي، النكول، القرائن والقسامة. أما الرأي الثاني، فهو رأي ابن تيمية وابن القيم الجوزية اللذين أطلقا حرية تقديم الأدلة التي يرونها، كما أطلقا للقاضي حرية اعتماد ما يراه مفيداً للدعوى ومثبتاً للواقعة[2].

المطلب الثاني: مفهوم الدليل اصطلاحاً وقانوناً:

هو ما يلزم من العلم به علم شيء آخر. وغايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة[3].

ونجد أن التعريف الأمثل هو ما جاء به الدكتور فاضل، إذ عرف الدليل بأنه: (الوسيلة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى الحقيقة من خلال تقديره السليم لها)[4].

---

(1) ابن القيم الجوزية، **إعلام الموقعين عند رب العالمين** – الجزء الأول، المكتبة التجارية، القاهرة، الطبعة الأولى، 1955م، ص: 450.

(2) أحمد أبو القاسم أحمد، **الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص**، أكاديمية نايف العربية للعلوم الأمنية، ج1، 1994م، ص: 183.

(3) أحمد أبو القاسم أحمد، المرجع السابق، ص: 174.

(4) د. فاضل زيدان، **سلطة القاضي الجنائي في تقدير الأدلة**، دار العلم والثقافة للنشر والتوزيع، الطبعة الأولى، 2006م، ص: 142.

واتفق مع هذا التعريف لأن القاضي أثناء نظر الدعوى يقوم بتقييم الأدلة ويقوم بوزنها وتكييفها ويستقى منها قناعته في المرحلة النهائية والحاسمة عند الفصل في الدعوى فيحكم وفقاً للقناعة التي توصل إليها إما بالبراءة أو الإدانة وكل حسب قوة الأدلة المطروحة أمامه.

الدليل في الاصطلاح القانوني هو الحجة والبرهان وما يستدل به على صحة الواقعة. ويعرف بعض فقهاء القانون الدليل بأنه: (الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها). والمقصود بالحقيقة في هذا السياق هو كل ما يتعلق بالوقائع المعروضة على القاضي لإعمال حكم القانون عليها[1].

ويعرف البعض الآخر الدليل بأنه: (الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه)[2]، كما قيل بأن الدليل: (هو كل ما يقود إلى صحة أو عدم صحة الواقعة أو الوقائع موضوع التحقيق)، سواءً كان موضوعاً جنائياً أو مدنياً[3].

تأسيساً على ما تقدم يمكننا القول بأن الدليل الجنائي هو معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية ووسائل فنية أو مادية أو قولية، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.

---

(1) أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، دار النهضة العربية، القاهرة، الطبعة الثانية، 1981م، ص: 418.

(2) مأمون سلامة محمد، **الإجراءات الجنائية في التشريع المصري**، دار الفكر العربي، القاهرة، 1973م، ص: 39.

(3) محمد محي الدين عوض، **قانون الإجراءات الجنائية السوداني معلقاً عليه**، المطبعة العالمية، القاهرة، 1971م، ص: 450.

وقد يخلط البعض – أحياناً – بين الدليل الجنائي والإثبات لما بينهما من علاقة في الإجراءات القضائية. ولكن في الواقع يمكننا الفصل بين الدليل والإثبات.

الدليل يتكون من حقائق متنوعة تقدم للمحكمة ولكن نتيجتها هي الإثبات. فالإثبات هو مجموعة جميع الحقائق – الأدلة – المستخدمة لإدانة أو تبرئة متهم معين.

وبهذا يبدو واضحاً أن مفهوم الإثبات أوسع من أن تنحصر في كلمة دليل. فكلمة الإثبات أكثر عمومية وتشمل مجموعة من الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق وتحقيق العدالة الجنائية، وتبدأ بتلقي البلاغ أو الشكوى وتمر بمرحلة المعانية وجمع الأدلة والتفتيش والضبط والاستجواب والمحاكمة.

المطلب الثالث: تعريف الأدلة الجنائية الإلكترونية:

يمكننا القول بأن الدليل الإلكتروني نوع من أنواع الأدلة الجنائية، لذا ينطبق عليه خصائص الأدلة الجنائية وشروطها واستخداماتها إلا أنها تتميز عنها بخصائص نوعية لا تتوفر في غيرها من الأدلة الجنائية.

يُعرف "كيسي" الأدلة الجنائية الرقمية بأنها تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها. والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة[1].

---

[1] أحمد أبو القاسم أحمد، **الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص**، مرجع سابق، ص: 185.

إذاً، الأدلة الجنائية الإلكترونية هي معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.

وتنقسم الأدلة بصفة عامة إلى أربع أنواع هي:

1/ الدليل القانوني، ويقصد به الأدلة التي حددها المشرع وعين حالات استخدامها ومدى حجية كل منها.

2/ الدليل الفني ويقصد به الدليل الذي ينبعث من رأي الخبير الفني حول تقدير أو تقييم دليل مادي أو قولي وفق معايير ووسائل علمية معتمدة.

3/ الأدلة القولية، وهي الأدلة التي تنبعث من أشخاص أدركوا معلومات مفيدة للإثبات بإحدى حواسهم كالاعتراف وأقوال الشهود.

4/ الأدلة المادية، وهي الدليل الناتج من عناصر مادية ناطقة بنفسها، ويؤثر في اقتناع القاضي بطريق مباشر.

فأين تقع الأدلة الإلكترونية بين هذه الأنواع؟ هل تعبر الأدلة الرقمية أدلة مادية لكونها ناتجاً من عناصر مادية ملموسة وتستخدم العلم ونظرياته؟ أم تعتبر من الأدلة الفنية لانبعاثها من رأي خبير فني ووفق معايير علمية معتمدة؟[1].

يرى البعض أن الأدلة الجنائية الإلكترونية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية

---

[1] اللواء د. محمد الأمين البشري، **الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات**، المجلة العربية للدراسات الأمنية والتدريب، المجلد السابع عشر، العدد الثالث والثلاثين، السنة السابعة عشرة، الرياض، أبريل 2002م، ص: 110.

للإنسان إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ووسائل التقنية العالية ومنها الحاسوب محور الأدلة الإلكترونية. فالأدلة الجنائية الإلكترونية في منظور أنصار هذا الاتجاه لا تختلف عن آثار الأسلحة والبصمات أو البصمة الوراثية D.N.A.

ويرى اللواء محمد الأمين غير ذلك[1]. إن الأدلة الإلكترونية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية والمواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأربعة آنفة الذكر، وذلك للأسباب التالية:

1/ الأدلة الإلكترونية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة، ولا يدركها الرجل العادي بالحواس الطبيعية للإنسان.

2/ الأدلة الإلكترونية ليست – كما يقول البعض – أقل مادية من الأدلة المادية فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان وجودها غير المعين.

3/ يمكن استخراج نسخ من الأدلة الجنائية الإلكترونية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوفر في أنواع الأدلة الأخرى.

4/ يمكن التعرف على الأدلة الإلكترونية المزورة أو التي جرى تحريفها بمضاهاتها مع الأدلة الأصلية بالقدر الذي لا يدع مجالاً للشك.

5/ من الصعب الإتلاف أو القضاء على الأدلة الجنائية الإلكترونية التي يمكن استرجاعها من الحاسوب بعد محوها.

---

[1] اللواء د. محمد الأمين البشري، مرجع سابق، ص: 111.

6/ علاوة على وجود الأدلة الإلكترونية في مسرح الجريمة التقليدي يمكن وجودها أيضاً في مسرح أو مكان افتراضي.

7/ تتميز الأدلة الجنائية الإلكترونية عن غيرها من أنواع الأدلة بسرعة حركتها عبر شبكات الاتصالات[1].

وقد قضت المحاكم بإمكانية اعتماد مثل تلك الأدلة غير الملموسة لأنها تتميز عن غيرها من أنواع الأدلة المادية الأخرى بما يلي:

1/ يمكن استخراج نسخ منها مماثلة ومطابقة للأصل ولها ذات الحجية.

2/ يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ما إذا كانت الأدلة الرقمية قد تعرضت لتعديل أو تحريف.

3/ من الصعب إتلاف الأدلة الجنائية الإلكترونية، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب.

4/ إذا حاول المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن آمنة علماً بأن للنسخ قيمة الأصل.

وتقدم الشبكات المعلوماتية تسهيلات للعديد من الأنشطة اليومية، بما في ذلك المحادثات الهاتفية، التجارة الإلكترونية، سحب وإيداع الأموال آلياً وغيرها من الخدمات التي توفرها الرفاهية للإنسان. ولكن مع تلك التسهيلات الكبيرة تأتي المخاطر والتعقيدات أيضاً. لقد أصبح دور الشبكات المعلوماتية واضحاً في كثير من الجرائم الخطيرة مثل التعامل بالصور الإباحية للأطفال، إغواء الصغار، المطاردة، المضايقات، التزوير، التجسس، السرقة، التخريب، الاعتداء على الحريات الخاصة وإشانة السمعة.

---

[1] اللواء د. محمد الأمين البشري، مرجع سابق، ص: 115.

يقوم المجرمون باستغلال مميزات تقنية المعلومات في الأنشطة الإجرامية بكفاءة وبسرعة تفوق قدرات المحققين، مما يمكنهم من التقدم على أجهزة العدالة الجنائية خطوات. وفي ذلك يقول "كارتر وكاتز": لقد صمدت أجهزة الشرطة خلال السنوات الماضية أمام العديد من التحديات، الجريمة المنظمة، الشغب، تجارة المخدرات وجرائم العنف من أمثلة المشاكل المعقدة التي واجهت الشرطة مشكلة غير عادية، ألا وهي مشكلة جرائم المعلوماتية. وهنالك عوامل عديدة تجعل من الصعب مواجهة هذا النوع من الجرائم[1].

لقد قام المجرمون بالدمج بين وسائل التقنية العالية مع الجرائم التقليدية ليخرجوا لنا بأنماط جديدة ومعقدة من الجرائم. استخدم المجرمون تقنية المعلوماتية عبر الحدود الولائية والدولية في التخطيط والتنفيذ وإخفاء عائدات الجرائم وآثارها. ومما يضاعف التعقيد، أن الأدلة المطلوبة في مثل هذه الجرائم ليست أدلة مادية أو مشاهدة، بل هي نبضات إلكترونية وبرامج مشفرة. ومن المؤسف أن أجهزة الشرطة تخلفت كثيراً في مجال تقنية المعلومات، وعليها أن تستيقظ من أجل العمل الجاد لمواكبة المتغيرات. لقد أصبح من الصعب على ضباط الشرطة إدراك أبعاد جرائم المعلوماتية على المستوى المحلي والعالمي[2].

---

[1] Carter David L. and Katz, A.J., **Computer Crime: An Emerging Challenge for Law Enfacement**, F.B.I. Bulletin, 1996, (Available at Http/www.Fbi.gov/leb.96text.).

[2] علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 1، 26 أبريل – 28 أبريل 2003، دبي، الإمارات العربية المتحدة، 2003م، ص: 118.

المبحث الثالث

وسائل جمع الأدلة الإلكترونية ومقارنتها

لابد من وسائل لجمع الأدلة الإلكترونية حتى تتم مقارنتها، ومن ثم اعتمادها والشروع في الإجراءات لعمل التصنيف والتوقيعات الرسمية وذلك من خلال مطلبين كالتالي:

المطلب الأول: جمع الأدلة الإلكترونية:

إن أول سؤال قانوني ينبغي طرحه عند الحديث حول التحقيق في جرائم المعلوماتية هو؛ من هو الشخص الذي يحق له جمع وتحليل الأدلة الجنائية الإلكترونية؟ وللإجابة على ذلك نقول: الشخص الذي يُكلف بجمع الأدلة الرقمية هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها. إن عمليات الضبط والحجز والتأمين وتحليل الأدلة الرقمية المخزنة في شبكات المعلوماتية هي التحدي الذي يواجه أجهزة العدالة الجنائية في هذه المرحلة التي تعاني فيها تلك الأجهزة من الأمية المعلوماتية.

وفي الوقت الذي تم فيه إعداد الخبراء والمختبرات الجنائية اللازمة للتعامل مع الأدلة المادية، برزت مشكلة الأدلة الرقمية كنتيجة لتقنية المعلومات في مجال الجريمة.. الشيء الذي يتطلب معامل ومختبرات خاصة وإعداد خبراء يجمعون بين المعرفة القانونية ومهارة التحقيق وعلوم تقنية المعلومات. وعلاوة على ذلك، يتطلب مواجهة التحدي الجديد بناء قدر من التعاون والثقة بين أجهزة تنفيذ القوانين والمؤسسات التي تقوم بتقديم خدمات المعلومات والاتصالات[1].

---

[1] ممدوح عبد الحميد عبد المطلب، **جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية: الجريمة عبر الإنترنت**، مكتبة دار الحقوق، الشارقة، 2001م، ص: 91.

الأدلة الجنائية الإلكترونية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين بالقدر الذي يكفل لها المصداقية ويُبعد عنها العيوب.

ونجد لذلك عدد من الأسباب منها:

1/ التوثيق الذي يحفظ الأدلة الإلكترونية في شكلها الأصلي يستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل. الصورة المسجلة بالفيديو – مثلاً – يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية بين طرفين عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.

2/ الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة والتوثيق هو الأسلوب الوحيد الذي يمكن المحققين من القيام بهذا الدور أمام القضاء، ويعتبر فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سبباً في بطلان الدليل.

3/ من المهم توثيق مكان ضبط الدليل الإلكتروني في حالة إعادة تكوين الجريمة، إذ أن تشابه أجهزة الحاسوب وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.

4/ يشكل التوثيق جزءاً من عمليات حفظ الأدلة الإلكترونية حتى انتهاء إجراءات التحقيق والمحاكمة، إذ أن التوثيق يشمل تحديداً دقيقاً للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدد – قدر الإمكان[1].

---

[1] قدري عبد الفتاح الشهاوي، **أساليب البحث العلمي الجنائي والتقنية المتقدمة**، منشأة المعارف، الإسكندرية، 1999م، ص: 223.

عند توثيق الدليل الإلكتروني يجب التأكد من، أين؟ كيف؟ متى؟ وبواسطة من تم ضبط الدليل وتأمينه؟ كما أنه من الضروري توثيق الأدلة الإلكترونية بعدة طرق كالتصوير الفوتوغرافي التصوير بالفيديو، الخرائط الكروكية وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص. وعند الأدلة الإلكترونية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها:

- التاريخ والوقت.
- توقيع الشخص الذي قام بإعداد النسخة.
- اسم أو نوع نظام التشغيل.
- اسم البرنامج أو الأوامر المستعملة لإعداد النسخ.
- المعلومات المضمنة في الملف المحفوظ.

المطلب الثاني: رسالة التصنيف والتوقيعات الرقمية:

رسالة التصنيف الحسابي هي مجموعة من الأحرف والأرقام المركبة بطريقة حسابية خاصة تمثل أي نوع من البيانات الرقمية. ويمكن ترجمة جميع محتويات أي ملف إلى كود محدد من الأحرف والأرقام أشبه بقراءة بصمات الأصابع. إن إعداد التصنيف السليم ينتج دائماً قراءة خاصة ومميز لكل ملف، تختلف تماماً عن قراءة الملفات الأخرى، إلا أنها مطابقة لقراءة النسخ الصحيحة لنفس الملف.

تستخدم رسالة التصنيف الحسابي لمضاهاة الأدلة الإلكترونية الأصلية مع النسخ للتأكد من صحتها وعدم تعرضها لأي تلاعب أو تحريف. وعند إدخال ملف الدليل الإلكتروني على رسالة التصنيف تظهر قراءة الملف بالحروف والأرقام مطابقة لقراءة النسخ الصحيحة لنفس الملف. ولكن في حالة حدوث أي تعديل في النسخة فإن الناتج يكون قراءة مختلفة. ولذا توصف رسالة التصنيف الحسابي بالبصمة الرقمية[1].

---

[1] قدري عبد الفتاح الشهاوي، **أساليب البحث العلمي الجنائي والتقنية المتقدمة**، مرجع سابق، ص: 227.

الفصل الثاني

حجية الدليل الإلكتروني

المبحث الأول: التعريف بالدليل الإلكتروني

المبحث الثاني: القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

المبحث الثالث: مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي

تمهيد:

من القواعد المستقرة في مجال الإثبات الجنائي أن القاضي لا يمكنه أن يقضي بعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة، ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته، ولهذه الأهمية التي يتمتع بها الدليل عموماً حظي باهتمام المشرع في مختلف الأنظمة القانونية من حيث تحديد شروط مشروعيته وتقدير قيمته الإثباتية، مع اختلاف النظم القانونية في الاتجاه الذي تتبناه بين موسع ومضيق. وعلى ذلك فكلما استُحدِث نوع من الأدلة كان من اللازم أن تتوافر فيه الشروط التي يحددها النظام القانوني الذي يقدم في ظله هذا الدليل.

ولذلك فإني سأحاول من خلال هذا الفصل تناول هذه الإشكاليات التي يثيرها الدليل الإلكتروني، مع الاقتصار على موقف المشرع السوداني في ضوء القواعد العامة، وذلك وفق الخطة التالية:

المبحث الأول: التعريف بالدليل الإلكتروني.

المبحث الثاني: القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي.

المبحث الثالث: مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي.

المبحث الأول
التعريف بالدليل الإلكتروني

إن تقييم أي نظام قانوني لا يمكن أن يصل إلى نتائج صحيحة إلا إذا توافر لدى المقوم تصوراً واضحاً لذلك النظام، إذ الحكم على الشيء فرع عن تصوره، ولذا فإننا إذ نتطلع في هذا المبحث إلى دراسة نظام الأدلة الإلكترونية إن جاز التعبير نعتقد أنه من الواجب تناول هذا النوع من الأدلة بالتعريف ليتسنى فهم ماهيته لنتمكن في النهاية من الحكم عليه، ولذلك سنتناول هذا المبحث في مطلبين:

المطلب الأول: تعريف الدليل الإلكتروني.

المطلب الثاني: أنواع الدليل الإلكتروني ومجاله في الإثبات الجنائي.

المطلب الأول: تعريف الدليل الإلكتروني:

يُعرِّف الدليل الإلكتروني بأنه: (هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون)[1].

والذي يلاحظ على هذا التعريف أنه يقصر مفهوم الدليل الإلكتروني على ذلك الذي يتم استخراجه من الحاسب الآلي، ولاشك أن ذلك فيه تضييف لدائرة الأدلة الإلكترونية، فهي كما يمكن أن تستمد من الحاسب الآلي، فمن الممكن أن يُتحصل عليها من أية آلة رقمية أخرى، فالهاتف وآلات التصوير

---

[1] د. خالد ممدوح إبراهيم، **الدليل الإلكتروني في جرائم المعلوماتية**، بحث منشور على الإنترنت: http://www.f-law.net تاريخ الزيارة: 2009/8/15م، ص: 2.

وغيرها من الأجهزة التي تعتمد التقنية الإلكترونية في تشغيلها يمكن أن تكون مصدراً للدليل الإلكتروني، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الإلكتروني ومسألة استخلاصه، حيث عرَّفه بأنه الدليل المأخوذ من الكمبيوتر... الخ، وهذا يعني أن الدليل الإلكتروني لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره، وهذا برأينا ليس صحيحاً؛ إذا من شأن التسليم بذلك القول إن تلك المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الإلكتروني، أي أن مخرجات الآلة الإلكترونية لا تكون لها قيمة إثباتية مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته، وهذا غير دقيق كما سنبين ذلك في محله، وهو ما يوصم هذا التعريف بالقصور لكونه لا يعطى تعريفاً جامعاً للدليل الإلكتروني[1].

ولذا فإننا بالاستفادة مما سبق نرى تعريف الدليل الإلكتروني بأنه: ((مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية)).

وترجع تسمية الدليل الإلكتروني إلى أن البيانات داخل الوسط الافتراضي سواء كانت صوراً أو تسجيلات أو نصوص تأخذ شكل أرقام على هيأة الإلكترونين (1 أو 0) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل[2].

---

[1] د. خالد ممدوح إبراهيم، **الدليل الإلكتروني في جرائم المعلوماتية**، مرجع سابق، ص: 2.

[2] د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، **أنموذج مقترح لقواعد اعتماد الدليل الإلكتروني للإثبات في جرائم الكمبيوتر**، منشور ضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية" نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من 10-12/5/ 2003م، المجلد الخامس، ص: 2237.

خصائص الدليل الإلكتروني:

1/ يعتبر الدليل الإلكتروني دليلاً غير ملموس أي هو ليس دليلاً مادياً، فهو – أي الدليل الإلكتروني – تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عمليه نقل لتلك المجالات من طبيعتها الإلكترونية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة.

2/ يعتبر الدليل الإلكتروني من قبيل الأدلة الفنية أو العلمية[1]، وهو من طائفة ما يعرف بالأدلة المستمدة في الآلة.

3/ إن فهم مضمون الدليل الإلكتروني يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً رقمياً، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدم قيمته التدليلية في إثبات الجريمة ونسبها إلى الجاني.

مميزات الدليل الإلكتروني:

يتميز الدليل الإلكتروني بعدة مميزات أهمها[2]:

1/ يتميز الدليل الإلكتروني بصعوبة محوه أو تحطيمه، إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل.

---

[1] د. علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الإلكترونية في أطار نظرية الإثبات الجنائي**، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمته أكاديمية شرطة دبي، في الفترة من 26-2003/4/28م، دبي، ص: 22.

[2] د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2240.

2/ إن محاولة الجاني محو الدليل الإلكتروني بذاتها تسجل عليه كدليل، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده.

3/ إن الطبيعة الفنية للدليل الإلكتروني تمكِّن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف كما سنرى لاحقاً.

المطلب الثاني: أنواع الدليل الإلكتروني ومجاله في الإثبات الجنائي:

سنتناول في هذا المطلب أنواع الدليل الإلكتروني والأشكال التي يبدو عليها كدليل، ثم نتناول الجرائم التي يصلح الدليل الإلكتروني ليكون دليلاً لإثباتها، وذلك على النحو التالي:

أولاً: أنواع الدليل الإلكتروني وأشكاله:

إن التعريف بالدليل الإلكتروني يحتم علينا تحديد أنواعه وأشكاله حتى يتسنى فهم الهيأة التي يتخذها للحكم على قيمته القانونية فيما بعد، ولذ سنتناول أولاً أنواعه ثم نحدد الأشكال التي يبدو عليها هذا الدليل وذلك على النحو التالي:

1/ أنواع الدليل الإلكتروني:

يمكن تقسيم الدليل الإلكتروني لنوعين رئيسين:

- أدلة أعدت لتكون وسيلة إثبات.
- أدلة لم تعد لتكون وسيلة إثبات.

أ) أدلة أعدت لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية يمكن إجماله فيما يلي:

1/ السجلات التي تم أنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي[1].

2/ السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة وتتمُّ معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب) أدلة لم تعد لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الإلكترونية، وهي ما يمكن تسميه أيضاً بالآثار المعلوماتية الإلكترونية[2]، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافه الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية[3].

والواقع أن هذا النوع من الأدلة لم يُعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجرى عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك[4].

---

(1) د. خالد ممدوح إبراهيم، مرجع سابق، ص: 2.

(2) د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2238.

(3) د نفس المرجع ، نفس الصفحة.

(4) حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول IP والذي يمكِّن من ضبط تحركات مستخدم الشبكة تحدي الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة، راجع في ذلك: د. عبد الفتاح بيومي حجازي، **الدليل الإلكتروني والتزوير في جرائم الكمبيوتر والانترنت، دراسة معمقة في جرائم الحاسب الآلي والإنترنت**، بهجات للطباعة والتجليد، مصر، 2009م، هامش ص: 63 – 64.

وتبدو أهمية التمييز بين هذين النوعين فيما يلي:

1/ النوع الثاني من الأدلة الإلكترونية هو الأكثر أهمية من النوع الأول لكونه لم يُعد أصلاً ليكون أثراً لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

2/ يتميز النوع الأول من الأدلة الإلكترونية بسهولة الحصول عليه لكونه قد أُعد أصلاً لأن يكون دليلاً على الوقائع التي يتضمنها، في حين يكون الحصول علي النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

3/ لأن النوع الأول قد أُعدَّ كوسيلة إثبات لبعض الوقائع فإنه عادة ما يُعمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل من إمكانية فقدانه، وعلى عكس النوع الثاني حيث لم يُعد ليحفظ ما يجعله عرض للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلاً.

2/ أشكال الدليل الإلكتروني: يتخذ الدليل الإلكتروني ثلاثة أشكال رئيسة هي:

- الصور الإلكترونية.
- التسجيلات.
- النصوص المكتوبة.

ونتناول هذه الأشكال على النحو التالي:

أ/ الصور الإلكترونية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفى العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الإلكترونية تمثل تكنولوجيا بديلة

للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصور التقليدية[1].

ب/ التسجيلات الصوتية: وهى التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الإلكترونية، وتشمل المحادثات الصوتية على الانترنت والهاتف.الخ.

ج/ النصوص المكتوبة: وتشمل النصوص التي يتم كتابها بواسطة الآلة الإلكترونية، ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي،.... الخ.

ثانياً: نطاق العمل بالدليل الإلكتروني:

إن الاهتمام الذي يحظى به الدليل الإلكتروني قياساً بغيره من الأدلة الأخرى المستمدة من الآلة مرده انتشار استخدام تقنية المعلومات الإلكترونية، والتي تعاظم دورها مع دخول الانترنت شتى مجالات الحياة، وأصبح بذلك هذا الوسط مرتعاً لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين، فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الإلكتروني، ولذا كان الدليل الإلكتروني هو الدليل الأفضل لإثبات هذا النوع من الجرائم، لأنه من طبيعة الوسط الذي ارتكبت فيه، ومن هنا بدت أهمية هذا النوع من الأدلة، ولكن أيعني ذلك أن الدليل الإلكتروني ينحصر مجاله كدليل إثبات فقط على جرائم المعلوماتية؟

يجب التنويه إلى أنه لا تلازم بين نطاق العمل بالدليل الإلكتروني ومشكلة إثبات الجريمة المعلوماتية، فمن ناحية فإن الدليل الإلكتروني مثلما يصلح لإثبات الجريمة المعلوماتية ويعتبر في ذات الوقت الدليل الأفضل

---

[1] د. ممدوح عبد الحميد عبد المطلب، **أدلة الصور الإلكترونية في الجرائم عبر الكمبيوتر**، مركز شرطة دبي، 2005م، ص: 9 – 10.

لإثباتها، فإنه من ناحية أخرى يصلح لإثبات الجرائم التقليدية إن جاز التعبير، حيث يميز الفقه في هذا الشأن بين نوعين من الجرائم[1]:

أ/ الجرائم المرتكبة بواسطة الآلة: وهذا النوع من الجرائم يستخدم فيه الحاسب الآلي والانترنت كوسيلة مساعده لارتكاب الجريمة، مثل استخدامه في الغش أو الاحتيال أو غسل الأموال أو لتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة، وبكلمة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة رقمية، فبرغم عدم اتصال هذه الجريمة بالنظام المعلوماتي فإن الدليل الإلكتروني يصلح كدليل لإثباتها.

ب/ جرائم الانترنت والآلة الإلكترونية: وهذا النوع من الجرائم يكون محله جهاز الحاسب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعاً إما على الكيان المادي للآلة، وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول، وإما يكون الاعتداء واقعاً على الكيان المعنوي للحاسب أو الآلة أو على قاعدة البيانات أو المعلومات التي قد تكون على شبكة المعلومات العالمية، مثال انتهاك الملكية الفكرية، وجرائم القرصنة وغيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بجرائم المعلوماتية والتي يكون الدليل الإلكتروني هو الدليل الأفضل لإثباتها إن وجد[2].

ومع ذلك فإننا نعتقد أن الجريمة المعلوماتية رغم شدة صلتها بالدليل الإلكتروني إلا أن إثباتها لا يقتصر عليه ، فمن الممكن إثباتها بأدلة الإثبات

---

[1] د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2237.

[2] هناك خلاف في الفقه حول تحديد مفهوم الجريمة المعلوماتية وليس في نيتنا التعرض لهذا الخلاف، راجع بِشأنه؛ راشد بن حمد البلوشي، **الدليل في الجريمة المعلوماتية**، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، القترة 2- 4/يونيو 2008م، منشور على الانترنت http://www.f-law.net.، ص: 5 وما بعدها.

التقليدية كالشهادة و الاعتراف وغيرها[1]، ولذلك يمكننا أن نقول إنه لا تلازم بين مشكلة الدليل الإلكتروني واثبات الجريمة المعلوماتية، فلهذه الأخيرة إشكاليات قانونية أخرى لا شأن لها بالدليل الإلكتروني، فإذا كانت غاية الدليل عموماً هي إثبات الجريمة ونسبها إلى مرتكبها، فإن هذا الدليل لا يكون قاصراً في تقديرناً إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها، إذ مع ذلك تصح تسميته كدليل، وتبدو أهمية هذا النوع من الأدلة بالنسبة للجريمة المعلوماتية لصعوبة إثبات وقوعها عادة.

غير أنه إذا كان من الصعوبات التي تواجه إثبات الجريمة المعلوماتية تحديد مفترق الجريمة، فإن هذه المشكلة لا شأن لنا بها عند تناول إشكاليات الدليل الإلكتروني، فتلك مسألة ربما يتعذر إثباتها في بعض الحالات ومن ثم لا نكون في شأنها بصدد دليل، ونحن هنا في هذه الدراسة ندرس الدليل الإلكتروني حينما يتوافر لإثبات واقعة معينة.

مع ملاحظة أنه قد يكون الدليل الإلكتروني متضمناً إثبات الجريمة ومربكها معاً، فجسم الجريمة المعلوماتية عادة هو الدليل الإلكتروني ذاته، وقد يكون هذا الجسم "الدليل الإلكتروني" متضمناً ما يفيد نسبة الجريمة لشخص ما، كما لو أرسل شخص لآخر رسالة عبر البريد الإلكتروني تتضمن فيروسات تؤدى إلى إتلاف الموقع الإلكتروني الخاص بذلك الشخص، فإن هذه الرسالة بذاتها تعد دليلاً على وقوع الجريمة، وفى الوقت نفسه ستعد دليلاً على نسبة ارتكابها لشخص معين وهو المرسل إذا تضمنت بيانات تدل على شخصية.

---

[1] مع ملاحظة أن بعض الأدلة التقليدية تحتاج لتطوير لتتناسب مع الطبيعة الخاصة لهذه الجرائم، فالخبرة مثلاً تصلح لإثبات الجريمة المعلوماتية إلا أنها تحتاج إلى أن يكون الخبير متمتعاً بمستوى عال من العلم والمهارة الفنية التي تمكنه من شق طريقة بنجاح في مجال إثبات هذه الطائفة من الجرائم، د. علي محمود علي حمودة، مرجع سابق، ص: 23.

ومما تقدم نخلص إلى أن الدليل الإلكتروني يصلح الإثبات الجريمة التي ترتكب باستعمال الآلة الإلكترونية – حاسوب – هاتف،... الخ، أو الجريمة التي ترتكب ضد الكيان المعنوي للآلة أو ضد شبكة المعلومات العالمية.

بالإضافة إلى ذلك فإن هذا الدليل يصلح لإثبات بعض الجرائم وإن لم تكن من ضمن النوعين المذكورين، وذلك إذا استعملت الآلة الإلكترونية للتمهيد لارتكاب الجريمة، أو لإخفاء معالمها، كالمراسلات التي يبعث بها الجاني لشريكه وتتضمن معلومات عن جريمة ينويان ارتكابها أو يطلب منه إخفاء معالم هذه الجريمة، فتلك المراسلة تصلح كدليل إثبات لهذه الجريمة حال وقوعها رغم أنها لم ترتكب ضد الآلة الإلكترونية ولا بواسطتها.

المبحث الثاني

القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

مجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، إذ يلزم أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائي تتوقف على مسألتين رئيستين، الأولى المشروعيةً، والثانية اليقينية في دلالته على الوقائع المراد إثباتها، ولذلك سنحاول في هذا المبحث تحديد القيمة القانونية للدليل الإلكتروني وذلك في مطلبين على النحو التالي:

المطلب الأول: مشروعية الدليل الإلكتروني.

المطلب الثاني: حجية الدليل الإلكتروني.

المطلب الأول: مشروعية الدليل الإلكتروني:

يقصد بمشروعية الوجود أن يكون الدليل معترف به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة التي تُقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، فهناك اتجاهان رئيسان؛ الأول نظام الأدلة القانونية، والثاني نظام الإثبات الحر.

أولاً: نظام الأدلة القانونية:

فوفقاً لهذا النظام فإن المشرع هو الذي يحدد حصراً الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون[1]، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه

[1] د. هلالي عبد الإله أحمد، **حجية المخرجات الكمبيوترية في المواد الجنائية**، دراسة مقارنة، (د.ن)، (د. ط)، 1999م، ص: 49.

صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد، حيث إن القانون قيد القاضي بقائمة من الأدلة التي حددت قيمتها الإثباتية، وهذا النظام ينتمي للنظم ذات الثقافة الأنجلوسكسونية، مثل المملكة المتحدة "بريطانيا" والولايات المتحدة الأمريكية، ولذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الإلكتروني بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته.

وتطبيقاً لهذا الفهم نصَّ قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الإلكتروني وحدد قيمته الإثباتية اتفاقاً وطبيعة النظام القانوني في بريطانيا[1].

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون، ولذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له، فنجد بريطانيا مثلاً قد بدأت تخفف من غلوائه، حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك، والتي مفادها أن القاضي يستطيع أن يكوِّن عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعاً في دلالته[2].

---

[1] د. علي محمود علي حمودة، مرجع سابق، ص: 30.

[2] د. هلالي عبد الإله أحمد، **حجية المخرجات**، مرجع سابق، ص: 91.

ثانياً: نظام الإثبات الحر:

يسود الإثبات الحر في ظل الأنظمة اللاتينية، ووفقاً لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبنى هذه القناعة على أي دليل وإن لم يكن منصوص عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يُطرح عليه ما يراه صالحاً للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع[1].

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل الإلكتروني من حيث الوجود، على اعتبار أن المشرع لا يُعهد عنه سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الإلكتروني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي.

إذن وفقاً لهذا النظام فإن الأصل في الأدلة مشروعية وجودها، فالدليل الإلكتروني سيكون مشروعاً من حيث الوجود استصحاباً للأصل.

المطلب الثاني: حجية الدليل الإلكتروني أمام القضاء الجنائي:

إن مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الإلكتروني تُمكِّن من

---

[1] د. هلالي عبد الإله أحمد، **حجية المخرجات**، مرجع سابق، ص: 29 وما بعدها.

العبث بمضمونه على نحو يحرِّف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة ، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فهل من شأن ذلك استبعاد الدليل الإلكتروني من دائرة أدلة الإثبات الجنائي لتعارضه وقرينة البراءة؟

في ظل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته التدليلية، فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل[1]،، فهل يمكن للقاضي الجنائي وفقاً لهذا النظام أن يُعمل سلطته التقديرية لقبول هذا الدليل أو رفضه بما يمكنه من استبعاد الدليل الإلكتروني لعدم الاقتناع به أو للشك في مصداقيته ؟

إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن أن نتوسع في شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية ، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، فضلاً عن ذلك فإن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عموماً، فالدليل الإلكتروني من حيث تدليله على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك لدليل، ولكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل الإلكتروني هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة

---

[1] يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة.

في الحصول عليه من ناحية أخرى، حيث يشكك في سلامة الدليل الإلكتروني من ناحيتين:

الأولى: الدليل الإلكتروني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبراً عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافاً للحقيقة، وذلك دون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث، على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة الإلكترونية التي قد تقدم للقضاء، فالتقنية الحديثة تمكِّن من العبث بالدليل الإلكتروني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

الثانية: وإن كانت نسبة الخطأ الفني في الحصول على الدليل الإلكتروني نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل الإلكتروني لسببين[1]:

الأول: الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الإلكتروني، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

الثاني: الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 100% ويحدث هذا غالباً بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ومن ذلك فإننا نخلص إلى أن الشك في الدليل الإلكتروني لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في مصداقيته، ولكن

---

[1] راجع في ذلك: د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2253.

هل يمكن التثبت من سلامة الدليل الإلكتروني من حيث العيوب؟ وبكلمة أوضح هل من الممكن أن يُضفى على الدليل الإلكتروني اليقين من خلال إخضاعه للتقييم الفني الذي يمكِّن من تفادي تلك العيوب التي تشوبه وما موقف القاضي الجنائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

مثلما يخضع الدليل الإلكتروني لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية، وذلك يرجع للطبيعية الفنية لهذا الدليل، عليه فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه، وسوف نحاول فيما يلي تناول بعض هذه الوسائل.

وسائل تقييم الدليل الإلكتروني:

سوف نتناول وسائل تقييم الدليل الإلكتروني من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي:

أولاً: تقييم الدليل الإلكتروني من حيث سلامته من العبث:

يمكن التأكد من سلامة الدليل الإلكتروني من العبث بعدة طرق نذكر منها:

1/ يلعب علم الكمبيوتر دوراً مهماً في تقديم المعلومات الفنية التي تساهم في فهم مضمون وهيأة الدليل الإلكتروني[1]، وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الإلكتروني من الوسائل المهمة للكشف عن مصداقية الدليل الإلكتروني، ومن خلالها تتم مقارنة الدليل الإلكتروني المقدم للقضاء بالأصل المدرج بالآلة

[1] د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2253.

الإلكترونية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا[1].

2/ حتى في حالة عدم الحصول على النسخة الأصلية للدليل الإلكتروني أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل الإلكتروني من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.

3/ هناك نوع من الأدلة الإلكترونية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الإلكتروني المقصود من حيث عدم حصول تعديل أو تغيير في النظام (الكمبيوتري)[2].

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل الإلكتروني ومطابقته للواقع.

ثانياً: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه:

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل الإلكتروني، وقد قدمنا أن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داو بورت)[3] كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل

---

[1] د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2241.

[2] المرجع السابق، ص: 2247.

[3] ترجع أصول هذا الاختبار (اختبارات داو برت) للحكم الذي أصدرته المحكمة العليا الأمريكية في **قضية داو بورت/ ضد/ ميريل دو للصناعات الدوائية 1993م**، مذكور في: د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2248.

إثبات، ولذا فإننا سنعرض باختصار للخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية[1]:

أ/ إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة، وذلك بإتباع اختبارين رئيسين هما:

– اختبار السلبيات الزائفة: ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني، وأنه لا يتم إغفال بيانات مهمة عنه.

– اختبار الايجابيات الزائفة: ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الإلكتروني لاختبار فني يمكِّن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.

وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الإلكتروني وفى ذات الوقت لم تضِف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.

ب/ الاعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:

حيث تدل البحوث المنشورة في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الإلكتروني، وفى المقابل ثبتت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[2].

---

[1] راجع: د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، مرجع سابق، ص: 2294 وما بعدها.

[2] ذياب البداينة، **جرائم الحاسب والإنترنت**، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، 1420هـ، ص: 93 – 124.

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني، فإذا توافرت في الدليل الإلكتروني الشروط العامة لما يمكن أن يمثل أساساً لانبعاث الثقة فيه، فإنه قد يبدو من غير المقبول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل الإلكتروني بوصفه دليلاً علمياً فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الإلكتروني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل الإلكتروني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية، إذ سلطة القاضي في رد الدليل استناداً لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة.

ولا شك أن الخبرة تحتل في هذه الحالة دروراً مهما في التثبت من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

وهنا ننوه إلى عدم الخلط بين الشك الذي يشوب الدليل الإلكتروني بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل الإلكتروني من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته التدليلية لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع[1]، ما لم يثبت عدم صلة الدليل الجريمة المراد إثباتها.

المبحث الثالث

[1] نصت قوانين بعض الدول التي تعتنق نظام الأدلة القانونية على الحجية القاطعة للأدلة الإلكترونية، راجع: د. هلالي عبد الإله أحمد، **حجية المخرجات**، مرجع سابق، ص: 95.

مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي

الإثبات الجنائي نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي[1]، وبمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين[2].

وتثير مسألة الإثبات في نظم الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق، وذلك لجملة أمور نذكر منها[3]: كالتخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، ويشكل انعدام الدليل المرئي عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال عن بُعد عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تُعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت[4]، ولما كانت أدلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال، فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد

---

(1) د. آمال عبد الرحيم عثمان، **الإثبات الجنائي ووسائل التحقيق العلمية**، دار النهضة العربية، القاهرة، 1975م، ص: 4.

(2) د. محمود محمود مصطفى، **شرح قانون الإجراءات الجنائية**، ط11، القاهرة، 1976م، ص: 414.

(3) للمزيد من المعلومات انظر: د. سعيد عبد اللطيف حسن، **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات**، ط1، دار النهضة العربية، القاهرة، 1999م، ص: 95 وما بعدها.

(4) د.هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة**، مكتبة الآلات الحديثة، أسيوط، 1994م، ص: 35 وما بعدها، وانظر: د. عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، دار الكتب القانونية، القاهرة، 2002م، ص: 46.

يـؤدي إلـى ضـياع الـدليل بـل تـدميره أحيانًـا[1]، لمـا تقـدم مـن صـعوبات ومشـكلات، يثـور التسـاؤل عمـا إذا كـان الـدليل المسـتمد مـن التفتـيش يحتـاج إلـى شـروط وللإجابـة عـن هـذا التسـاؤل ينقسـم هـذا المبحـث إلـى مطلـب أول: فـي شـروط الـدليل الإلكترونـي المسـتمدة مـن التفتـيش، ومطلـب ثـاني: فـي حجيـة الدليل الإلكتروني الناشئ عن التفتيش.

المطلب الأول: شروط الدليل الإلكتروني المستمد من التفتيش:

إن الأدلـة الإلكترونيـة، إمـا أن تكـون مخرجـات ورقيـة يـتم إنتاجهـا عـن طريـق الطابعـات، أو الراسـم، وإمـا أن تكـون مخرجـات غيـر ورقيـة أو أن تكـون إلكترونيـة: كالأشـرطة والأقـراص الممغنطـة وأسـطوانات الفيـديو وغيرهـا مـن الأشـكال الإلكترونيـة غيـر التقليديـة، أو تتمثـل فـي عـرض مخرجـات المعالجـة بواسـطة الحاسـوب علـى الشاشـة الخاصـة بـه، أو الإنترنـت بواسـطة الشاشـات أو وحـدة العـرض المرئـي[2]، ويكـون الـدليل بـاطلاً إذا استحصـل عليـه عـن طريـق مخالفـة القـانون، ولهـذا الموضـوع أهميـة بالغـة لمـا يترتـب علـى بطـلان الـدليل مـن آثـار، فـإذا كـان الـدليل الباطـل هـو الـدليل الوحيـد فـلا يصـح الاسـتناد عليـه فـي إدانـة المـتهم، فـإذ مـا شـاب التفتـيش الواقـع علـى نظـم الحاسـوب عيـب فإنـه يبطلـه، والتفتـيش الـذي يقـوم بـه المحقـق بغيـر الشـروط التـي نـص عليهـا القـانون يعتبـر بـاطلاً بطلانًـا مطلقًـا ولا يجـوز التمسـك بمـا ورد فـي محضـر التفتـيش كمـا لا يجـوز للمحكمـة أن تعتمـد عليـه فـي حكمهـا[3]. ويقـع عـبء إثبـات الجـرائم المعلوماتيـة علـى عـاتق النيابـة العامـة، كمـا أن المـدعي بـالحق الشخصـي يشـارك

---

[1] انظر: أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة، **جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة**، ط1، دار وائل، عمان، 2001م، ص: 289 – 297.

[2] د. هلالي عبد اللاه أحمد، **حجية المخرجات الكمبيوترية في الإثبات الجنائي**، ط1، دار النهضة العربية، القاهرة، 1997م، ص: 14 – 22.

[3] أ. عبد الأمير العكيلي، **أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية**، ج1، ط1، مطبعة المعارف، بغداد، 1975م، ص: 348.

النيابة العامة هذا العبء، وفي أحيان أخرى ينقل القانون عبء الإثبات من النيابة العامة إلى عاتق المشتكي عليه[1]، والدليل المتحصل من تفتيش نظم الحاسوب والإنترنت لا يكون مشروعاً[2]، ويعتبر باطلاً إذا تم الحصول عليه بغير الشروط التالية:

الشرط الأول: يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام الدستور والقانون[3]: إن أهم هدف للدستور هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير الحديثة نصوصاً تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها، بحيث يتقيد المشرع بها عند وضع قانون أصول المحاكمات الجزائية، فهذه النصوص الواردة في الدستور تفرض على المشرع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها، ونرى ضرورة أن يقوم المشرع السوداني بتشريع نصوص إجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب والإنترنت، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانوني،

---

(1) انظر: د. نائل عبد الرحمن صالح، **محاضرات في قانون أصول المحاكمات الجزائية**، ط1، دار الفكر العربي، عمان، 1997م، ص: 17 وما بعدها.

(2) انظر: محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، الإسكندرية، 2001م، ص: 103.

(3) انظر: د. رمزي رياض عوض، **مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها – دراسة تحليلية تأصيلية مقارنة**، دار النهضة العربية، القاهرة، 1997م، ص: 85 وما بعدها. وانظر: د. أحمد عوض بلال، **قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة**، دار النهضة العربية، القاهرة، 1994م، ص: 16 وما بعدها.

حمايـة للحقـوق والحريـات الفرديـة التـي كفلهـا الدسـتور السـوداني، بالإضـافة إلـى المواثيق الدولية[1].

أمـا جـزاء مخالفـة القـانون فـي الحصـول علـى الأدلـة فيترتـب عليـه جـزاءات جنائيـة أو إداريـة فضـلاً عـن الحكـم بـالتعويض، فـالموظف الـذي يعهـد إليـه القـانون بعمـل فيتصـرف علـى وجـه مخـالف يعـد مقصـراً فـي عملـه ومخالفًـا فـي واجباتـه فيسـتحق المؤاخـذة[2]، والمهـم هنـا هـو الجـزاء الإجرائـي إذ لا شـك إن الـدليل المسـتخلص عـن طريـق ارتكـاب جريمـة يكـون بـاطلاً بطلانًـا متعلقًـا بالنظـام العـام، وفـي جميـع هـذه الحـالات يرتـب العمـل المخـالف للقـانون لمـن وقـع عليـه الحـق فـي التعـويض فضـلاً عـن اسـتحقاق القـائم بـه للعقوبـة الجنائيـة مـع وجـوب بطـلان هـذا العمـل كونـه وليـد جريمـة، وبالتـالي بطـلان الـدليل الـذي اسـتمد منـه هـذا العمـل، لأن مـا يبنـى علـى الباطـل يكـون بـاطلاً، ويلاحـظ إمكانيـة انطبـاق القواعـد التقليديـة علـى هـؤلاء المـذكورين فـي النصـوص السـابقة، فـي حالـة اطلاعهـم بحكـم وظـائفهم علـى أسـرار المـواطنين عبـر أجهـزة الحاسـوب أو شـبكاته مـن خـلال أدائهـم لوظـائفهم، لكـن يبقـى التسـاؤل علـى مـن تـم ذكـرهم أعـلاه كشـهود علـى الجريمـة المعلوماتيـة، فهـل هـم ملزمـون أن يقومـوا بطبـع ملفـات البيانـات المخزنـة فـي ذاكـرة الحاسـوب مفشـين للسـر، أو الإفصـاح عـن كلمـات المـرور السـرية، أو الكشـف عـن الشـفرات المدونـة بهـا الأوامـر الخاصـة بتنفيذ البرامج؟

---

[1] د. جميل عبد الباقي الصغير، **أدلـة الإثبـات الجنـائي والتكنولوجيـا الحديثـة** (أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية) – دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م، ص: 116.

[2] انظـر: د. علـي حسـن الطوالبـه، **التفتـيش الجنـائي علـى نظـم الحاسـوب والإنترنـت – دراسـة مقارنـة**، ط1، عالم الكتب الحديث، اربد، 2004م، ص: 179.

لقد اختلف الفقه المقارن في الإجابة عن هذا التساؤل بين مؤيد ومعارض ويمكن بلورة هذا الخلاف في اتجاهين رئيسين هما[1]:

الاتجاه الأول: يذهب أصحابه إلى أنه ليس من واجب الشاهد، وفقاً للالتزامات التقليدية للشهادة – أن يقوم بما تم ذكره سابقًا – ففي لوكسبورغ، الشاهد ليس مجبراً على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة، وبالتالي من الصعب إجباره على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه في ذاكرة الحاسوب، وإن كان يستطيع الوصول إليها نظراً لمعرفته بكلمات المرور السرية[2]، أما إذا تعاون الشاهد على هذا النحو فإن دوره يكون أقرب إلى الخبرة منه إلى الشهادة، وفي ألمانيا، تذهب غالبية الفقه إلى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وفي تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة.

الاتجاه الثاني: ويرى أنصاره أن من الالتزامات التي يجب أن يقوم بها الشاهد، هي طبع ملفات البيانات، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ففي فرنسا يرى جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفًا بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج، ما عدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بأداء الشهادة، وفي هولندا يتيح قانون الحاسوب لسلطات

---

(1) للمزيد من المعلومات انظر: د. هلالي عبد الإله أحمد، **التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة**، النسر الذهبي، القاهرة، 2000م، ص: 52 – 56.

(2) انظر: الرائد كمال الكركي، **جرائم الحاسوب ودور مديرية الأمن في مكافحتها**، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م، ص: 10 وما بعدها.

التحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، أو حل رموز البيانات المشفرة[1].

وفي إطار مشروعية الأدلة الإلكترونية، نجد أن قانون الإجراءات الجنائية السوداني رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب في جرائم الحاسوب والإنترنت، كأن يستخدم أعضاء الضابطة العدلية طرقاً معلوماتية في أعمال التنصت على المحادثات الهاتفية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية، ومن بينها الأدلة المتحصلة من الحاسوب والإنترنت، بطريقة شرعية ونزيهة، ونفس الشيء نجده في سويسرا وبلجيكا[2]. وفي بريطانيا، قامت الشرطة بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناءً على موافقتها، وقد أجرت الشاكية عدة مكالمات هاتفية مع الشخص الذي كانت الشرطة تشك في ارتكابه الجريمة، وقد تم تسجيل هذه المكالمات التي تضمنت موضوعات تدين المتهم، لكن القاضي استبعد هذه التسجيلات على أساس أنها تمت من خلال شرك خداعي[3]، أما في هولندا، فإذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية، فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات، وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة

---

(1) د. هشام محمد فريد رستم، **جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة**، مجلة الدراسات القانونية، جامعة أسيوط، العدد 17، 1995م، ص: 117.

(2) انظر: د. هلالي عبد الاه أحمد، **حجية المخرجات الكمبيوترية**، مرجع سابق، ص: 121 – 122.

(3) د. هلالي عبد الاه أحمد، مرجع سابق، ص: 132.

غير القانونية[1]، أما في اليابان فقد أصدرت محكمة مقاطعة (KOFV) حكماً أقرت فيه مشروعية التنصت للبحث عن الدليل، حيث ضرورة التحريات، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار، لكن الفقه الياباني، يرى أن الأدلة الجنائية التي يتم الحصول عليها بطرق مشروعة يجب أن تكون مستبعدة سواء كانت تقليدية أم أدلة حاسوب أم أدلة إنترنت[2]. ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية، كالتحريض على الغش أو التزوير أو التجسس، والاستخدام غير المصرح به للحاسوب، والتنصت، والمراقبة الإلكترونية عن بُعد[3].

وتُعد من الطرق غير المشروعة أيضاً استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية[4]، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة، ومدة حفظها محددة زمنياً، وعدم إفشائها أو استعمالها في غير الأغراض

---

(1) انظر: د. أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دراسة مقارنة**، ط2، دار النهضة العربية، القاهرة، 1989م، ص: 93 – 94.

(2) د. هلالي عبد الاه أحمد، **حجية المخرجات**، مرجع سابق، ص: 137.

(3) انظر: د. جميل عبد الباقي الصغير، **أدلة الإثبات الجنائي**، مرجع سابق، ص: 111.

(4) المرجع السابق، ص: 112.

المخصصة لها، وحق الشخص المعني في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[1]، ولقد تضمن قانون الشرطة والإثبات الجنائي الإنكليزي لعام 1984م، تحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تقبل أمام القضاء، وتضمن كذلك توجيهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب ، فأوصت المادة (11) منه[2]، بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسوب المقبولة في الإثبات طبقًا للمادة (69) من القانون نفسه، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في وقت معاصر لهذا الأمر أم لا ، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيانات من الحاسوب لديه دافع لإخفاء الوقائع أو تشويهها، وقد نصت المادة (69) على ثلاثة شروط أساسية هي[3]:

1/ يجب ألا يوجد أساس معقول للاعتقاد أن البيان الخاطئ أو غير دقيق، بسبب الاستعمال الخاطئ (الاستعمال غير الملائم للظروف أو للغرض الذي يستخدم من أجله الحاسوب).

2/ يجب أن تكون جميع المكونات المادية للحاسوب كانت تعمل بدقة وعلى نحو متوافق كما ينبغي.

3/ إن أيًا من الشروط المحددة (التي تدخل في متطلبات القبول) المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة، ولقد قضت محكمة الاستئناف الجنائي في إنكلترا بذلك، حيث بينت في حكمها كيفية التعامل مع

---

(1) محمد محمد شتا، مرجع سابق، ص: 104 – 105.

(2) Police and Criminal Evidence Act 1984, Op - Cit, P. 28.

(3) Op - Cit, P. 25..

الأدلــة المســتخرجة مــن الحاســوب، ويــتلخص الحكــم بمــا يلــي: (أنــه يبــدو لهــذه المحكمــة – أنــه مــن الخــاطئ رفــض أو إنكــار أيــة مزايــا أو صــلاحيات مقــررة وفقًــا لقــانون الإثبــات، يمكــن بمقتضــاها التوصــل عــن طريــق التقنيــات الجديــدة والوســائل الحديثــة التأكــد مــن صــحة وصــدق التســجيل، حيــث يمكــن التثبــت مــن ذلــك، وكــذلك يمكــن التعــرف بوضــوح علــى الأصــوات المســجلة، والمســتخلص أيضــاً هــو أن الــدليل وثيــق الصــلة بالموضــوع، مــن جهــة أخــرى، يمكــن قبولــه، ومــن ثــم تؤيــد المحكمــة قبــول هــذه الأشــرطة ويجــب أن ينظــر دائمًــا بعــين الاعتبــار إلــى مثــل هــذا الدليل، وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية)[1].

الشــرط الثــاني: يجــب أن تكــون الأدلــة الإلكترونيــة غيــر قابلــة للشــك أي يقينيــة: يُشــترط فــي الأدلــة المســتخرجة مــن الحاســوب والإنترنــت أن تكــون غيــر قابلــة للشــك حتــى يمكــن الحكــم بالإدانــة، ذلــك أنــه لا مجــال لــدحض قرينــة البــراءة وافتــراض عكســها إلا عنــدما يصــل اقتنــاع القاضــي إلــى حــد الجــزم واليقــين، ويمكــن التوصــل إلــى ذلــك مــن خــلال مــا يعــرض مــن الأدلــة الإلكترونيــة، والمصــغرات الفيلميــة، وغيرهــا مــن الأشــكال الإلكترونيــة التــي تتــوافر عــن طريــق الوصــول المباشــر، أم كانــت مجــرد عــرض لهــذه المخرجــات المعالجــة بواســطة الحاســوب علــى الشاشــة الخاصــة بــه أو علــى الطرفيــات، وهكــذا يســتطيع القاضــي مــن خــلال مــا يعــرض عليــه مــن مخرجــات إلكترونيــة، ومــا ينطبــع فــي ذهنــه مــن تصــورات واحتمــالات بالنســبة لهــا، ان يحــدد قوتهــا الاســتدلالية علــى صــدق نســبة الجريمة المعلوماتية إلى شخص معين من عدمه.

ويشــترط قــانون البــوليس والإثبــات فــي بريطانيــا لســنة 1984م، حتــى تتحقــق يقينيــة الأدلــة الإلكترونيــة أن تكــون البيانــات دقيقــة وناتجــة عــن الحاســوب

---

[1] انظر: د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 199 – 200.

بصورة سليمة[1]، أما في كندا، فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة، لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية.

ونصت بعض قوانين الولايات في أمريكا، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تُعد من أفضل الأدلة المتاحة لإثبات هذه البيانات، وبالتالي يتحقق مبدأ اليقين لهذه الأدلة، وتنص القواعد الفيدرالية على أن: (الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل، كشرط مسبق لقبوله، هو أن يفي بأمارة أو بينة كافية لأن تدعم اكتشاف (أو الوصول) إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعي بها)[2].

الشرط الثالث: إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسوب والإنترنت: ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[3]، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة ليس من خلال ملف

---

(1) Naughan Bevan and Ken Lidstone, **Aguide to the Police and Criminal Evidence Act 1984**, Bulterworthe, London, 1985, P. 497.

(2) د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 159.

(3) قرار محكمة النقض المصرية في 1986/11/20م، رقم 179، المبادئ القانونية، ص: 943.

الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الحواسيب، وأيضًا بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة[1]، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم، أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة وكشفاً للحق[2].

ومن القواعد العامة المستقرة في الفقه الدولي الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية، إلا في حالات استثنائية حصرها القانون بشروط مشددة، ويُعزى عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع، ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجنائية الإلكترونية، على سبيل المثال، لقد تضمنت القواعد الفيدرالية الأمريكية نصاً يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية استثناءً للبينة السماعية، وبناءً على تلك القواعد تعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها

---

[1] والشاهد المعلوماتي: هو الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسوب والذي تكون لديه معلومات جوهرية لازمة لولوج لنظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، انظر: د. هلالي عبد الاه أحمد، **التزام الشاهد**، مرجع سابق، ص: 23 وما بعدها.

[2] د. محمد فهمي طلبه وآخرون، **دائرة المعارف الحاسب الإلكتروني**، مجموعة كتب دلتا، مطابع المكتب المصري الحديث، القاهرة، 1991م، ص: 31 وما بعدها.

معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آليًا بأسلوب علمي[1].

وللإجابة عن التساؤل الذي طُرح في مقدمة هذا المطلب حول إمكانية ضبط الأدلة ومشروعيتها إذا كانت النهاية الطرفية للنظام المعلوماتي في منزل آخر غير منزل المتهم، فهذه المشروعية غير مطلقة بل هي مقيدة بقيود ثلاثة هي[2]:

1/ ألا تكون النهاية الطرفية المتصل بها الحاسوب موجودة ضمن إقليم دولة أخرى حتى لا يؤدي الاتصال بها إلى انتهاك لسيادة الدولة الإقليمية.

2/ أن تحتوي النهاية الطرفية المتصل بها الحاسوب على بيانات ضرورية بصورة كافية لظهور الحقيقة.

3/ أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.

ويبقى السؤال، ماذا لو كانت النهاية الطرفية في إقليم دولة أخرى، فكيف يمكن ضبط الدليل الإلكتروني في هذه الحالة؟ يلاحظ إن المادة (25/أ) من قانون الحاسوب الهولندي استثنت هذه الحالة، فيمكن الحصول على الأدلة حتى لو كانت في إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمني والقضائي والخاصة بالتفتيش وضبط الأدلة، وأخيرًا فإن

---

[1] انظر: د. محمد الأمين البشري، **الأدلة الجنائية الرقمية – مفهومها ودورها في الإثبات**، المجلة العربية للدراسات الأمنية والتدريب، المجلد السابع عشر، العدد الثالث والثلاثون، الرياض، أبريل 2002م، ص: 128 – 129.

[2] د. عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة**، (د. ت)، ص: 347.

متحصلات الجريمة المعلوماتية[1]، التي يتم ضبطها يجب أن تعرض على القاضي المختص بكافة مفرداتها وعناصرها، وذلك لأن حيادية القاضي توجب عليه أن لا يقيم قضاءه إلا على ما طرح أمامه وكان موضوع الفحص والتحقيق والمناقشة.ويترتب على مناقشة أدلة الحاسوب والإنترنت:

النتيجة الأولى: عدم جواز أن يقضي القاضي في الجرائم المعلوماتية بناءً على معلوماته الشخصية.

والنتيجة الثانية: ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والإنترنت بشكل يتماشى مع التقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسوب والإنترنت.

المطلب الثاني: حجية الدليل الإلكتروني الناشئ عن التفتيش:

إنَّ حجية المخرجات المتحصلة من الحاسوب، هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر، بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية، من قوة استدلالية في كشف الحقيقة[2].

لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي **القوانين ذات الصياغة اللاتينية**، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني، فإن حجية الأدلة الإلكترونية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات جرائم الحاسوب والإنترنت، ولا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، وفي فرنسا مشكلة حجية المخرجات المتحصلة من الحاسوب على

---

[1] انظر: د. هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة**، ط1، دار النهضة العربية، القاهرة، 1997م، ص: 139 وما بعدها.

[2] د. هلالي عبد الاه أحمد، **حجية المخرجات الكمبيوترية**، مرجع سابق، ص: 22.

مستوى القانون الجنائي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة[1]، ويدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل أجهزة التصوير وأشرطة التسجيل وأجهزة التنصت، وقد قضت محكمة النقض الفرنسية: (إن أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي)[2]، وكذلك الحال بالنسبة لكل من ألمانيا وتركيا ولوكسمبورج واليونان والبرازيل[3]، وكل هذه الدول تخضع الأدلة الإلكترونية لحرية القاضي في الاقتناع الذاتي، بحيث تكون بمقدوره أن يطرح مثل هذه الأدلة – رغم قطعيتها من الناحية العلمية – ذلك عندما يجد أن الدليل الإلكتروني لا يتسق منطقيًا مع ظروف الواقعة وملابساتها.

أما في النظم الإنجلو سكسونية التي يحدد المشرع فيها أدلة الإثبات ويقدر قيمتها الإقناعية، في طليعة هذه الدول التي تتبنى هذا النظام، بريطانيا، التي أصدرت قانون إساءة استخدام الحاسوب في عام 1990م، الذي لم يتناول الأدلة الناتجة عن الحاسوب، وربما كان السبب هو وجود قانون البوليس والإثبات الجنائي لسنة 1984م، الذي حوى تنظيماً محدداً لمسألة قبول مخرجات الحاسوب والإنترنت، كأدلة إثبات في المواد الجنائية[4]، وفي الولايات المتحدة الأمريكية تناولت بعض القوانين حجية الأدلة الإلكترونية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسوب لسنة 1984م،

---

[1] د. هلالي عبد الاه أحمد، **<u>حجية المخرجات الكمبيوترية</u>**، مرجع سابق، ص: 42 – 43.

[2] المرجع السابق، ص: 43.

[3] السابق، ص: 44 – 46.

[4] لقد صدر تشريع الإثبات بالحاسوب في إنجلترا عام 1983م، وقد ركز بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه والتي تزود بشهادة شفوية تكون مقبولة والتي يتم تقديرها من قبل المحكمة المختصة – انظر: د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 194.

الصادر في ولاية (أيوا)، من أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة 716/أ/16)، كما يتضح من قانون الإثبات الصادر في عام 1983م في ولاية كاليفورنيا، من أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات، وفي كندا، يمكن قبول السجلات الناجمة عن الحاسوب، إذا توافرت شروط معينة يجب توافرها قبل عمل صورة من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان (MC Mullen)، بأنه يشترط لكي تكون سجلات الحاسوب مقبولة بوصفها نسخًا حقيقية من السجلات الإلكترونية، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفًا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كافٍ[1]. أياً كانت الطريقة أو الوسيلة المستخدمة في النسخ، كالطباعة، والتصوير، والتسجيل الميكانيكي، والتسجيل الإلكتروني، بما يسمح بقبول مخرجات الحاسوب في الإثبات، والغالب الأعم في القضاء الأمريكي أنه يُعول على قبول دليل السجلات المحتفظ بها على الحاسوب[2].

أما في **القوانين ذات الاتجاه المختلط**، وهي التي تجمع ما بين النظامين اللاتيني والانجلوسكسوني، فيعتمد النظام المختلط على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطًا في بعض الأحوال، أو يعطي القاضي الحرية في تقدير الأدلة

---

[1] د. هلالي عبد الإله أحمد، **حجية المخرجات الكمبيوترية**، مرجع سابق، ص: 55 – 57.

[2] د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 165.

القانونيــة، أمــا بالنســبة لأدلــة الحاســوب والإنترنــت، فيقــرر الفقــه اليابــاني، أن السـجلات الإلكترومغناطيسـية تكـون غيـر مرئيـة فـي حـد ذاتهـا، ولـذلك لا يمكـن أن تسـتخدم كـدليل فـي المحكمـة، إلا إذا تـم تحويلهـا إلـى صـورة مرئيـة ومقـروءة عـن طريـق مخرجـات الطباعـة لمثـل هـذه السـجلات، وفـي مثـل هـذه الحالـة يـتم قبـول هـذه الأدلـة الناتجـة عـن الحاسـوب والإنترنـت، سـواء كانـت هـي الأصـل أم كانت نسخة من هذا الأصل[1].

وتــنص المــادة (113) مــن قــانون الإجــراءات الجنائيــة الشــيلي، علــى إمكانيــة اســتخدام الأفــلام الســينمائية، والحــاكي (الفونــوغراف)، والــنظم الأخــرى الخاصــة بإنتــاج الصــورة، والصــوت، والاختــزال، وبصــفة عامــة أيــة وســائل أخــرى، قـد تكـون ملائمـة، ووثيقـة الصـلة، وتفضـي إلـى اسـتخلاص المصـداقية، يمكـن أن تكــون مقبولــة كــدليل إثبــات[2]، ويــرى الفقــه الشــيلي، أن الــدليل النــاتج عــن الحاســوب والإنترنــت، يمكــن أن يكــون مقبــولاً فــي المحكمــة، كــدليل كتــابي أو مسـتندي، مثلـه مثـل الـنظم الحديثـة الأخـرى لجمـع وتسـجيل المعلومـات، وحجـة الفقــه الشــيلي تســتهدف توســيع مظلــة الوســائل العلميــة الحديثــة فــي الإثبــات، لتغطي العناصر الإثباتية الناتجة عن جرائم المعلوماتية[3].

تعـد مراقبـة المكالمـات السـلكية واللاسـلكية – تحـت رقابـة القضـاء– مـن الوسـائل الملائمـة لضـبط مـا يفيـد فـي كشـف الحقيقـة أحيانًـا، وقـد أحـاط المشـرع إجـراء المراقبـة الهاتفيـة واللاسـلكية بضـمانات معينـة فـلا يجـوز إجراؤهـا إلا بـأمر مسبب من القضاء وبصورة مشروعة.

لكن ما القوة الإثباتية للتسجيلات الصوتية المُسجلة إلكترونيًا؟

---

(1) نقلاً عن؛ د. هلالي عبد الإله أحمد، **حجية المخرجات الكمبيوترية**، مرجع سابق، ص: 62.

(2) المرجع السابق، ص: 64 – 66.

(3) د. عفيفي كامل عفيفي، مرجع سابق، ص: 373 – 374.

إن الصوت عند تسجيله إلكترونياً، لا يحتمل الخطأ، ويصعب التلاعب به، ويمكن للخبراء أن يكتشفوا أي تلاعب أو خداع بوسائل تقنية عالية الكفاءة، ومن ثم يمكن القول بأن التسجيل الصوتي الممغنط يمكن أن تكون له حجة دامغة في الإثبات[1].

ويمكن باستخدام تكنولوجيا للحواسيب الحديثة والإنترنت وطرق الاتصال المعلوماتي السريع، أن يستخدم تسجيل الفيديو لإثبات تُهم استعمال القسوة أو إساءة استعمال السلطة من قبلِ أعضاء الضابطة العدلية ضد المواطنين، كما يمكن استخدامها لتسجيل عمليات القبض والتفتيش وضبط الأدلة والآثار الأخرى الناجمة عن الجريمة تسجيلاً دقيقًا، كما يمكن استخدامها كتقنية عالية الكفاءة لعمل المعاينات اللازمة لمسرح الجريمة[2]، ويشترط الفقه لمشروعية الدليل المستمد من المراقبة والتسجيل توافر الشروط التالية[3]:

1/ إذا لم يكن التسجيل منطوياً على اعتداء على حق يحميه القانون، فيكون الدليل في هذه الحالة مشروعاً، ويمكن للمحكمة أن تستند إليه في قضائها بالإدانة أو بالبراءة.

2/ تحديد دقيق لشخصية الشخص المراد تسجيل أحاديثه أو بريده الإلكتروني كل ما كان ذلك ممكنًا في حالة الإنابة للتفتيش.

---

(1) د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 211.

(2) بيل جيتس وآخرون، **المعلوماتية بعد الإنترنت (طريق المستقبل)**، ترجمة: أ. عبد السلام رضوان، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون الآداب، العدد 231، الكويت، مارس 1988م، ص: 425.

(3) د. ممدوح خليل البحر، **أصول المحاكمات الجزائية الأردني**، الطبعة الأولى، دار الثقافة، عمان، 1998م، ص: 558 – 750.

3/ تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرح لها بذلك، والمدة الجائز خلالها التقاط الحديث خلالها.

ويمكن استخدام "حاسوب الجيب" على أنه "أداة تبرئة" إذ يمكن أن تكون التوقيعات المشفرة من خلاله دليل براءة غير قابل للدحض في مواجهة أية اتهامات باطلة، فلو أن شخصًا ما أتُهم بأمر معين أو جريمة معينة فبإمكانه أن يُدافع عن نفسه من خلال ما هو مُسجل من أقوال وأفعال في أي وقت[1]. أما البريد الإلكتروني، فعند إرسال رسالة من خلاله فإنه يكون لدى الشخص المستقبل توقيعاً رقمياً (إلكترونياً)، ويكون المستقبل وحده القادر على استعماله، وسيتم تشفير الرسالة، بحيث لن يتمكن من حل شفرتها إلا الشخص المقصود إرسالها إليه، ويمكن لهذه الرسالة أن تكون معلومات من أي نوع، مشتملة على الصوت والفيديو، أو تحويلات بنكية، وسيكون بإمكان متلقي الرسالة أن يتأكد من أن الرسالة مرسلة بالفعل من الشخص الذي أرسلها، وتحديد وقت إرسالها بالضبط، وأنها لم تتعرض لأي تلاعب، وأن الآخرين لا يستطيعون فك شفرتها، وبالتالي يمكن استخدام هذه المعلومات كحجة في الإثبات الجنائي[2].

ويستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما، أن يلفق أو يزور المفترض كتابة أو إرسال الوثيقة فيه فسيكون هذا التلفيق أو التزوير قابلاً للكشف، وسوف يرد ذلك الاعتبار للقيمة الإثباتية للصور الفوتوغرافية والفيديوية، ولقد أضاف علم التصوير للإثبات الجنائي قيمة علمية بما له من

---

[1] وهو حاسوب بحجم صغير جدًا يمكن وضعه داخل الجيب، ويمكن ربطه بمونيوتر أكبر وبالشبكة العامة بمكتب العمل الخاص، ويمكن للمستخدم أن يحفظ فيه كل ما يريد من أرقام ومواعيد، بالإضافة لاستخدامه ككاميرا تصوير وخلوي، انظر: بيل جيتس، مرجع سابق، ص: 423 – 424.

[2] د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 232 – 233.

أثر في نقل صورة صادقة للأماكن والأدلة إلى كل من يعنيه الأمر، اعتمادًا على آلة التصوير والأفلام التي لا تعرف الكذب، بيد أنه لا يمكن إنكار الآثار السلبية والخطيرة التي تنشأ عن استخدام هذه الوسائل، لما قد يحدثه في الحياة الخاصة إذا لم توضع له الضوابط الكافية[1]، وتختلف حجية التوقيع الإلكتروني في الإثبات المدني عنه في الإثبات الجنائي، حيث يخضع في الإثبات المدني لقواعد شكلية، أما في الإثبات الجنائي فيخضع تقديره لمطلق سلطة قاضي الموضوع، واقتناعه بصحته وقوته الإثباتية[2]، كما أن وجود نظام تسجيل الدخول في شبكة الإنترنت يسمح بتحديد الأشخاص الذين دخلوا أو حاولوا الدخول بعد ارتكاب الفعل الجرمي، وتعد حالات ضبط مرتكب الفعل متلبسًا نادرة أو أنها وليدة الصدفة، وحتى لو تم ضبطه متلبسًا، فقد يرجع ذلك إلى خطأ في نظام الحاسوب أو الشبكة أو الأجهزة الأخرى[3]، أو عن طريق مراقبة الشرطة بعد ملاحظة وجود بعض الاعتداءات، والفقه الفرنسي يعتبر انتهاك نظام الأمن لبعض المواقع المحمية، دليل حتمي وقرينة قاطعة على وجود القصد الجرمي وسوء نية مرتكب الفعل[4]، ويمكن

---

(1) وللمزيد من المعلومات انظر: د. عبد الحافظ عبد الهادي عابد، **الإثبات الجنائي بالقرائن – دراسة مقارنة**، دار النهضة العربية، القاهرة، 1998م، ص: 563 وما بعدها.

(2) لقد أصبح التوقيع الإلكتروني بديلاً عن التوقيع التقليدي ويؤدي ذات الوظيفة فيما يتعلق بالوثائق والرسائل الإلكترونية، وهو مهم من حيث أنه يحدد شخصية الموقع، ويعبر عن إرادته في التزامه بمضمون الوثيقة وإقراره لها، وهو دليل على حضور أطراف التصرف وقت التوقيع، أو حضور من يمثلهم قانونًا أو اتفاقًا. انظر في: د. سعيد عبد اللطيف حسن، مرجع سابق، ص: 244 وما بعدها، وانظر: د. هدى حامد قشقوش، **الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت**، دار النهضة العربية، القاهرة، 2000م، ص: 71 وما بعدها. وانظر: د. محمد المرسي زهرة، **حجية التوقيع الإلكتروني في الإثبات، الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف**، مرجع سابق، ص: 145 وما بعدها.

(3) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص: 46.

(4) انظر: د. أحمد حسام طه تمام، **الجرائم الناشئة عن استخدام الحاسوب (الحماية للحاسوب) – دراسة مقارنة**، دار النهضة، القاهرة، 2000م، ص: 274 – 275.

للماسحات الضوئية، وطابعات الليزر أن تكون أداة ارتكاب الجريمة، ففي عام 1994م، قام أحد الأشخاص في مدينة دلاس الأمريكية بتزوير أجازات قيادة سيارات التاكسي باستخدام الماسحات الضوئية، وطابعات الليزر، كما جرت محاولات لإصدار بطاقات التأمين، وأوامر صرف مالية، وبعض أنواع الصكوك من خلال استخدام برمجيات الرسوم المتطورة، وأنظمة الطباعة المتخصصة[1].

ومما تقدم يمكن تأييد الرأي الفقهي الذي يرى أن المحاكم الجنائية قد لا تواجه مشاكل في تعاملها مع الأدلة الجنائية الإلكترونية (الرقمية)، وذلك للأسباب التالية[2]:

1/ الثقة التي اكتسبها الحاسوب والإنترنت والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات[3].

2/ ارتباط الأدلة الجنائية الإلكترونية وآثارها بالجريمة موضوع المحاكمة.

3/ وضوح الأدلة الإلكترونية، ودقتها في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والسلوك الإجرامي.

4/ إمكانية تعقب آثار الأدلة الإلكترونية والوصول إلى مصادرها بدقة.

---

(1) Flusche, Karl J., **Computer Crime and analysis of Computer evidence**, Itain't Just hackers and phreakers anymore, Information System Security, Spring 1998, Vol. 7, Issue 1, P. 24.

(2) انظر: د. محمد الأمين البشري، مرجع سابق، ص: 127 – 128.

(3) ويحقق الحاسوب قدرًا من التأمين، والسرعة في تبادل المعلومات بين أجهزة وأقسام الشرطة وصولاً إلى المجرم أو يمكن التدخل قبل وقوع الجريمة، ويمكن الاستفادة من الحاسوب في تحليل نتائج البحث الجنائي الفني والعلمي، ومضاهاة البصمة ونقلها لوحدات الشرطة، ويكفل الحاسوب سرية المعلومات الشخصية التي تصل إلى وحدات التسجيل الجنائي. انظر: اللواء د. محمد الأمين، **العدالة الجنائية ومنع الجريمة – دراسة مقارنة**، ط1، أكاديمية نايفوو العربية للعلوم الأمنية، الرياض، 1997م، ص: 303 وما بعدها.

5/ قيام الأدلة الإلكترونية على نظريات حسابية مؤكدة لا يتطرق إليها الشك مما يقوي من تقنية الأدلة الإلكترونية.

6/ الأدلة الجنائية الإلكترونية يدعمها – عادة – رأي خبير – وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء.

الخاتمة

خاتمة البحث ليست تلخيصاً لما ورد فيه، فهذا مبين بين دفتيه، ولكنها إبراز لأهم النتائج التي توصل إليها وبيان لأهم المقترحات التي يرنو إليها. فإذا كان موضوع هذا البحث قد تناول حجية الدليل الإلكتروني في الإثبات الجنائي، فإنه يكون بذلك قد تناول مشكلة من المشكلات التي أفرزتها ثورة الاتصالات، وهذه النوعية الجديدة من الجرائم التي ساهمت هذه الثورة في ارتكابها والتي تتميز بطبيعة فنية وعلمية معقدة، ويتصف مرتكبيها بطبيعة ذكية ماكرة. فبدأنا نسمع عن العمليات المصرفية الإلكترونية، وعن النقود الإلكترونية، وعن المستندات الإلكترونية، وعن الحكومة الإلكترونية، وعن التوقيعات الإلكترونية. ولا شك في أن ظهور هذه العمليات الإلكترونية الجديدة ووجوب حمايتها جنائياً من صور الاعتداء المتطورة التي قد تقع عليها بالوسائل الإلكترونية المتطورة، قد أظهر أن هناك قصوراً كبيراً في النصوص الجنائية الموضوعية والإجرائية، بحيث أن هذه النصوص قد أصبحت شائخة وعاجزة عن كفالة الحماية الفاعلة للمصالح والقيم التي أفرزتها ثورة الاتصالات.

أهم النتائج:

1/ إن هناك قصوراً واضحاً في الكثير من التشريعات الجنائية الموضوعية والإجرائية في مواجهة ظاهرة الجرائم التي تقع بالوسائل الإلكترونية أو على هذه الوسائل، مما قد يترتب عليه إفلات الكثير من الجناة من العقاب.

2/ ازدياد الإثبات بالخبرة والقرائن بالنسبة لهذا النوع الجديد من الجرائم، وهو ما يستوجب الاهتمام بالخبراء وتأهيلهم التأهيل العلمي الصحيح الذي يمكنهم من القيام بأعمالهم.

3/ أن هنـاك صـعوبة تكتنـف الـدليل الجنـائي بالنسـبة للجـرائم الإلكترونيـة سـواء مـن حيـث طـرق الحصـول عليـه أو مـن حيـث طبيعتـه وعمليـة تقديره.

4/ أن الإثبـات الجنـائي مهمـا تطـور بالنسـبة للجـرائم الإلكترونيـة وعـلا شـأن الأدلـة العلميـة والفنيـة، فـي هـذا الإثبـات، فإنـه يجـب أن نبقـى علـى سلطة القاضي التقديرية في تقديره لهذه الأدلة العلمية والفنية.

أهم التوصيات:

1/ توصـى الدراسـة بإيجـاد تشـريع قـانوني يتعامـل مـع جـرائم الإنترنـت وقايةً، وتحقيقاً، وضبطاً، وعقاباً.

2/ توصـي الدراسـة بوضـع ضـوابط واضـحة وصـريحة وصـالحة للتعامـل مـع هـذه الجـرائم والممارسـات غيـر الأخلاقيـة، وبمـا يحـدّ مـن خطـورة هـذه الأفعـال وردع مرتكبيهـا، مـع تفعيـل مـا هـو موجـود مـن قـوانين لترتقـي إلـى الحدّ من الجريمة الإلكترونية.

3/ توصـي بتكثيـف الاهتمـام التربـوي بـالنشء، مـن قبـل مؤسسـات المجتمـع المختلفـة، وبخاصـة المؤسسـات التعليميـة مـع تطـوير هـذا الاهتمام بما يتوافق وتعاليم ديننا الحنيف والتطوّر التقني الحديث.

4/ أهميـة تـدريب الخبـراء والمحققـين والقضـاة لأجـل فهـم هـذه الجـرائم علـى قدر المستطاع.

قائمة المصادر والمراجع:

أولاً: القرآن الكريم.

(صُنْعَ اللَّهِ الَّذِي أَتْقَنَ كُلَّ شَيْءٍ إِنَّهُ خَبِيرٌ بِمَا تَفْعَلُونَ). سورة النمل، الآية: 88.

ثانياً: كتب اللغة:

1/ جميل صليباً، **المعجم الفلسفي**، دار كتب اللبناني، بيروت، الطبعة الأولى، 1971م.

2/ زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي الرازي، **مختار الصحاح**، ج2، تحقيق: يوسف الشيخ محمد، المكتبة العصرية، الدار النموذجية، بيروت، ط5، 1420هـ - 1999م.

3/ علي بن محمد بن علي الزين الشريف الجرجاني، **التعريفات**، حققه وضبطه وصححه: جماعة من العلماء بإشراف الناشر، دار الكتب العلمية، بيروت، لبنان، ط1، 1403هـ - 1983م.

ثانياً: كتب الفقه:

4/ ابن القيم الجوزية، **إعلام الموقعين عند رب العالمين**، الجزء الأول، المكتبة التجارية، القاهرة، الطبعة الأولى، 1955م.

ثالثاً: كتب القانون:

5/ أحمد أبو القاسم أحمد، **الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص**، أكاديمية نايف العربية للعلوم الأمنية، ج1، 1994م.

6/ أحمد حسام طه تمام، **الجرائم الناشئة عن استخدام الحاسوب (الحماية للحاسوب)** - دراسة مقارنة، دار النهضة، القاهرة، 2000م.

7/ أحمد عوض بلال، **قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة**، دار النهضة العربية، القاهرة، 1994م.

8/ أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، دار النهضة العربية، القاهرة، الطبعة الثانية، 1981م.

9/ أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة، **جرائم الحاسب الآلي والإنترنت** – دراسة تحليلية مقارنة، ط1، دار وائل، عمان، 2001م.

10/ أسامة عبد الله قايد، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات** – دراسة مقارنة، ط2، دار النهضة العربية، القاهرة، 1989م.

11/ آمال عبد الرحيم عثمان، **الإثبات الجنائي ووسائل التحقيق العلمية**، دار النهضة العربية، القاهرة، 1975م.

12/ جميل عبد الباقي الصغير، **أدلة الإثبات الجنائي والتكنولوجيا الحديثة (أجهزة الرادار، الحاسبات الآلية، البصمة الوراثية) –** دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م.

13/ ذياب البداينة، **جرائم الحاسب والإنترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها**، أكاديمية نايف العربية للعلوم الأمنية، تونس، 1420هـ.

14/ الرائد كمال الكركي، **جرائم الحاسوب ودور مديرية الأمن في مكافحتها**، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

15/ رمـزي ريـاض عـوض، **مشـــروعية الـــدليل الجنـــائي فـــي مرحلـــة المحاكمـــة ومـــا قبلهـــا** – دراســة تحليليــة تأصـيلية مقارنــة، دار النهضــة العربية، القاهرة، 1997م.

16/ ســعيد عبــد اللطيــف حســن، **لإثبـــات جـــرائم الكمبيـــوتر والجـــرائم المرتكبـــة عبـــر الإنترنـــت، الجـــرائم الواقعـــة فـــي مجـــال تكنولوجيـــا المعلومات**، ط1، دار النهضة العربية، القاهرة، 1999م.

17/ عبـد الأميـر العكيلـي، **أصـول الإجـراءات الجنائيـة فـي قـانون أصـول المحاكمـــات الجزائيـــة**، الجـزء الأول، الطبعــة الأولــى، مطبعــة المعــارف، بغداد، 1975م.

18/ عبـد الحـافظ عبـد الهـادي عابـد، **الإثبـات الجنـائي بـالقرائن** – دراسـة مقارنة، دار النهضة العربية، القاهرة، 1998م.

19/ عبـد الـرحيم صـدقي، **الإجـرام المـنظم فـي مصـر والـبلاد العربيـة**، كليـة الحقوق، جامعة القاهرة، 2001م.

20/ عبـد الـرحيم صـدقي، **موسـوعة صـدقي فـي القـانون الجنـائي**، المجلـد التاسع، دار النهضة العربية، القاهرة، 1986م.

21/ عبـد الفتـاح بيـومي حجـازي، **الـدليل الإلكترونـي والتزويـر فـي جـرائم الكمبيـــوتر والانترنـــت، دراســـة معمقـــة فـــي جـــرائم الحاســـب الآلـــي والانترنت**، بهجات للطباعة والتجليد، مصر، 2009م.

22/ عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون** – دراسة مقارنة، (د. ت).

23/ علي حسن الطوالبه، **التفتيش الجنائي على نظم الحاسوب والإنترنت** – دراسة مقارنة، ط1، عالم الكتب الحديث، اربد، 2004م.

24/ فاضل زيدان محمد، **سلطة القاضي الجنائي في تقدير الأدلة**، دار العلم للثقافة والنشر والتوزيع، الطبعة الأولى، 2006م.

25/ مأمون سلامة، **الإجراءات الجنائية في التشريع المصري**، دار الفكر العربي، القاهرة، 1973م.

26/ ماهر الجنيدي، **رائحة الماريجوانا تنبعث من أوكار إنترنت**، مجلة إنترنت العالم العربي، 1999م.

27/ محسن شفيق، **نقل التكنولوجيا من الناحية القانونية**، طبعة جامعة القاهرة، 1984م.

28/ محمد إبراهيم السيف، **الظاهرة الإجرامية في ثقافة وبناء المجتمع السعودي: بين التصور الاجتماعي وحقائق الاتجاه الإسلامي**، مكتبة العبيكان، الرياض، 1417هـ.

29/ محمد الأمين البشري، **الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات**، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السنة 17، الرياض، 2002م.

30/ محمد الأمين، **العدالة الجنائية ومنع الجريمة** – دراسة مقارنة، ط1، أكاديمية نايفوو العربية للعلوم الأمنية، الرياض، 1997م.

31/ محمد السيد اليماني، **الجوانب القانونية لدور براءة الاختراع في نقل التكنولوجيا**، مجلة الدراسات القانونية، العدد الثاني، كلية الحقوق، جامعة أسيوط، 1980م.

32/ محمد حسين حبيب، ورقة عمل بعنوان: **المخدرات الرقمية بين الحقوق الشخصية والجريمة السيبرانية، مقدمة لفعاليات الأيام العربية للأمن السيبراني: أفق التعاون لحماية الفضاء السيبراني**، العراق، 1-2015/12/2م.

33/ محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، الإسكندرية، 2001م.

34/ محمد محي الدين عوض، **قانون الإجراءات الجنائية السوداني معلقاً عليه**، المطبعة العالمية، القاهرة، 1971م.

35/ محمود محمود مصطفى، **شرح قانون الإجراءات الجنائية**، ط11، القاهرة، 1976م.

36/ ممدوح خليل البحر، **أصول المحاكمات الجزائية الأردني**، ط1، دار الثقافة، عمان، 1998م.

37/ ممدوح عبد الحميد عبد المطلب، **أدلة الصور الإلكترونية في الجرائم عبر الكمبيوتر**، مركز شرطة دبي، 2005م.

38/ ممدوح عبد الحميد عبد المطلب، **جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية: الجريمة عبر الإنترنت**، مكتبة دار الحقوق، الشارقة، 2001م.

39/ نائل عبد الرحمن صالح، **محاضرات في قانون أصول المحاكمات الجزائية**، ط1، دار الفكر العربي، عمان، 1997م.

40/ هدى حامد قشقوش، **الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت**، دار النهضة العربية، القاهرة، 2000م.

41/ هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية** – دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

42/ هشام محمد فريد رستم، **جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة**، مجلة الدراسات القانونية، جامعة أسيوط، العدد 17، 1995م.

43/ هلالي عبد الإله أحمد، **التزام الشاهد بالإعلام في الجرائم المعلوماتية** – دراسة مقارنة، النسر الذهبي، القاهرة، 2000م.

44/ هلالي عبد الإله أحمد، **حجية المخرجات الكمبيوترية في المواد الجنائية**، دراسة مقارنة، (د. ن)، 1999م.

45/ هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي** – دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 1997م.

46/ هلالي عبد اللاه أحمد، **حجية المخرجات الكمبيوترية في الإثبات الجنائي**، ط1، دار النهضة العربية، القاهرة، 1997م.

47/ يونس عرب، **جرائم الكمبيوتر والإنترنت**، ص: 152، وموقع: www.unicfing.hotmail.com على شبكة الإنترنت.

رابعاً: الكتب العلمية:

48/ بيل جيتس وآخرون، **المعلوماتية بعد الإنترنت "طريق المستقبل"**، ترجمة: أ. عبد السلام رضوان، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون الآداب، العدد 231، الكويت، 1988م.

49/ قدري عبد الفتاح الشهاوي، **أساليب البحث العلمي الجنائي والتقنية المتقدمة**، منشأة المعارف، الإسكندرية، 1999م.

50/ محمد فهمي طلبه وآخرون، **دائرة المعارف الحاسب الإلكتروني**، مجموعة كتب دلتا، مطابع المكتب المصري الحديث، القاهرة، 1991م.

خامساً: المراجع الإنجليزية:

51/ Carter David L. and Katz, A.J., **Computer Crime: An Emerging Challenge for Law Enfacement**, F.B.I. Bulletin, 1996, (Available at Http/www.Fbi.gov/leb.96text.).

52/ Eoghan Casey, **Digital Evidence and Computer Crime**, London: Academic Press, 2000.

53/ Flusche, Karl J., **Computer Crime and analysis of Computer evidence**, Itain't Just hackers and phreakers anymore, Information System Security, Spring 1998.

54/ Naughan Bevan and Ken Lidstone, **Aguide to the Police and Criminal Evidence Act 1984**, Bulterworthe, London, 1985.

سادساً: البحوث والأوراق العلمية:

55/ الجامعة العربية، القاهرة، **الندوة العربية حول الجريمة الإلكترونية**، الخرطوم، الأول من فبراير 1998م.

56/ خالد ممدوح إبراهيم، **الدليل الإلكتروني في جرائم المعلوماتية**، بحث منشور على الإنترنت: http://www.f-law.net تاريخ الزيارة: 2009/8/15م.

57/ راشد بن حمد البلوشي، **الدليل في الجريمة المعلوماتية**، بحث مقدم للمؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، القترة 2- 4/يونيو 2008م، منشور على الانترنت .http://www.f-law.net

58/ عبد الرحيم صدقي، **ورقة مقدمة في الندوة المصاحبة لاجتماع مجلس وزراء العدل العرب** بالخرطوم في الفترة من 4 – 6 مارس 2002م.

59/ علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الإلكترونية في أطار نظرية الإثبات الجنائي**، مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمته أكاديمية شرطة دبي، في الفترة من 26-2003/4/28م.

60/ علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 1، 26 – 28 نيسان 2003، دبي، الإمارات العربية المتحدة، 2003م.

61/ ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، **أنموذج مقترح لقواعد اعتماد الدليل الإلكتروني للإثبات في جرائم الكمبيوتر**، منشور ضمن أعمال مؤتمر "الأعمال المصرفية والإلكترونية" نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من 10–2003/5/12م.

سابعاً: السوابق:

62/ **حكومة السودان/ ضد/ مجدي مصطفى البغدادي**، محكمة الملكية الفكرية الخرطوم، غير منشورة.