جرائم تقنية المعلومات وإثباتها

إعداد

د. طالب محمد جواد عباس
مدرس الحاسبات
كلية الحقوق / جامعة النهرين

عبدالجبار ضاحي عواد
مدرس القانون الجنائي
كلية الحقوق / جامعة النهرين

الملخص

عمت تقنيات ونظم المعلومات جميع المجتمعات في الدول المتقدمة والنامية، وباتت تؤثر على حركتها. تنظم المعلوماتية اليوم وسائل النقل والاتصال، حركة الاقتصاد والتجارة، مدخلات الصناعة والزراعة، أدوات التعليم والصحة وآلات الحرب والسلام. ونتيجة لهذا التطور العلمي الذي شهده العصر الحديث، تطورت الجريمة وظهرت نوعية من المجرمين الذين انتقلوا بالجريمة من شكلها التقليدي وأبعادها المحدودة إلى آفاق جديدة تعتمد على التقنية الحديثة.

موضوع هذا البحث هو جرائم تقنية المعلومات وكيفية إثباتها، أي الجرائم التي تقع بطريق الحاسوب والإنترنت. ويعتبر هذا الموضوع من الموضوعات المهمة التي تثير جوانب جديدة ترجع إلى اتصالها بتطور وسائل التعاملات بسبب انتشار استخدام الحاسوب وخاصة استعمال شبكة الإنترنت. وانطلاقاً من الأهمية البالغة لهذا الموضوع على نحو ما أوضحنا فيما تقدم، تبين أن هناك حاجة للبحث المعمق في المسائل العملية المتصلة بتحقيق وإثبات جرائم تقنية المعلومات، لذا فأن هذا البحث ينصب على سبر غور المسائل الفنية والقانونية ذات الصلة بالتحقيق والإثبات.

إن تناول موضوع البحث الرئيس يتطلب ابتداء التمهيد له باستعراض موجز بالتعريف بتقنية المعلومات، وهذا ما سيكون محلاً للمبحث التمهيدي باعتباره مدخلاً موضوعياً يحتاجه القارئ الكريم غير المحيط بالأبعاد الفنية. وليتحقق بحث جرائم تقنية المعلومات لابد من تحديد أركان جريمة تقنية المعلومات وأنواعها، وهو ما سيكون محلاً للمبحث الأول. وفي المبحث الثاني، فأننا نتناول موضوع الإثبات والتحقيق الابتدائي والنهائي.

المقدمة

شهد القرن الماضي ثورة من نوع غير مألوف اصطِلح على تسميتها بثورة المعلومات[1]، فثورة المعلومات التي نعيشها اليوم دخلت تقنية المعلومات جميع مجالات الحياة. وقد ساعد دخول شبكة الإنترنت وزيادة أعداد المستخدمين لهذه التقنية على انتشار تقنية المعلومات بشكل كبير خلال السنوات القليلة الماضية. وما كان لهذه التقنية أن تنتشر بهذه السرعة لولا الإمكانات الهائلة لهذه التقنية و المعلومات الواسعة التي تقدمها شبكة الإنترنت. وتدل الإحصاءات على هذا الازدياد المتسارع في استخدام تقنية المعلومات.

مع شيوع استخدام وسائل تقنية المعلومات وتزايد الاعتماد على نظم المعلومات وشبكات الحاسوب وفي مقدمتها الإنترنت كما أسلفنا، تطور معها الفكر الإجرامي، فظهر نوع جديد من الجرائم هو ما يعرف بالجرائم المعلوماتية أو الجرائم الرقمية أو جرائم تقنية المعلومات، مما ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئاً شديدا ومهاما جساماً تفوق القدرات المتاحة لهم، وفق أسس وقواعد إجراءات التحري والتحقيق والإثبات الجنائي التقليدية؛ نظراً لعدم كفاية، وعدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم -سواء من الناحيتين القانونية أو التقنية، كما تستدعي مراجعة شاملة للأحكام والنصوص القانونية، هذه المراجعة تظهر دون عناء إن القوانين التقليدية قاصرة عن تغطية هذه الجرائم لأن تطبيق هذه القوانين يفترض وقوع الجرم على أموال مادية بينما جرائم المعلومات تقع على أموال معنوية لا تغطيه هذه القوانين[2]، فضلا عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمي الفني لهذه الجرائم.

انطلاقاً من الأهمية البالغة لهذا الموضوع على نحو ما أوضحنا فيما تقدم، تبين أن هناك حاجة للبحث المعمق في المسائل العملية المتصلة بتحقيق وإثبات جرائم تقنية المعلومات، لذا فأن هذا البحث ينصب على سبر غور المسائل الفنية والقانونية ذات الصلة بالتحقيق الإثبات.

ومن ثم نرى أن نبحث هذا الموضوع في ثلاثة مباحث، مبحثُ تمهيدي يهدف إلى توفير مدخل موضوعي لموضوع الدراسة، إذ هناك حاجة لمعرفة غير المتخصص تقنياً حول ماهية تقنية المعلومات و تطبيقاتها. وتحديد أركان جريمة تقنية المعلومات وأنواعها، وهو ما سيكون محلاً للمبحث الأول. وفي المبحث الثاني، فأننا نتناول موضوع الإثبات والتحقيق الابتدائي والنهائي.

خطة البحث

المبحث التمهيدي: التعريف بتقنية المعلومات

المبحث الأول: أركان جريمة تقنية المعلومات وأنواعها

المبحث الثاني: أثبات جريمة تقنية المعلومات

الخاتمة

المراجع

المبحث التمهيدي

التعريف بتقنية المعلومات

سنتناول في هذا المبحث تعريف بتقنية المعلومات وأهميتها وتصنيفها والوظائف التي تؤديها، مع عرض لمفهوم جرائم تقنية المعلومات أو جرائم المعلوماتية وتطورها التاريخي، كل في مطلب مستقل:

المطلب الأول: تعريف تقنية المعلومات وبيان أهميتها

المطلب الثاني: التطور التاريخي لجريمة تقنية المعلومات والتعريف بها

المطلب الأول

تعريف تقنية المعلومات وبيان أهميتها ووظائفها

المعلومات مورد لا يقل ولا ينضب، تتزايد دوما ولا تتناقص بالاستخدام أو تستهلك، وترتبط بالزمان والمكان وتتفاعل مع التطور، وعلى متلقيها ومدى علاقتها بحاجته تتوقف، إلى حد كبير قيمتها. وهي في الحقبة المعاصرة مفتاح للموارد الأخرى، و خدمة تباع وتشترى، ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها. المعلومات مصطلح واسع يستخدم لعدة معانٍ حسب سياق الحديث، وهو بشكل عام يرتبط بمصطلحات مثل: المعنى والمعرفة والتعليمات والتواصل.

بدأت المعلومات تتزايد بمتوالية هندسية واسعة وبقفزات بدت الطرق التقليدية عاجزة على جمعها وتنظيمها، لذا ظهرت مساعٍ للتغلب على هذه المشكلة بمسارين رئيسين: تمثل (أولهما) على تحسين وتطوير عملية الفهم لطبيعة المعلومات ومكوناتها وتجميعها وتحليلها بهدف لاستفادة منها بفاعلية. وتبدو (ثانيهما) في ظهور تقنية متقدمة للتحكم في المعلومات وتجميعها ومعالجتها و اختزانها واسترجاعها كالحاسبات والوسائط المتنوعة ووسائط الاتصال، والتي تشكل باندماجها معا، ما يعرف **بتقنية المعلومات** ((Information Technology(IT)) أو **المعلوماتية** (Informatics))[٤].

فالمعلوماتية مشتقة من المعلومة أو المعلومات وفنيا هناك علاقة بين البيانات والمعلومات، فالبيانات هي مجموعة من الحقائق أو المشاهدات، القياسات التي تكون عادة في شكل حروف أو أرقام أو أشكال خاصة تُوصف أو تمثل فكرة أو موضوعاً أو هدفا أو شرطا أو أية عوامل أخرى، و تمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات. فالبيانات تعد مصطلحا عاما لكل الحقائق والأرقام والرموز والحروف، فهي معطيات أولية يمكن معالجتها و إنتاجها عن طريق نظم المعلومات. ويتضح لنا من ذلك أن البيانات هي المادة الخام للمعلومات والتي لم يتم معالجتها بعد، أما بعد معالجتها فأنها تتحول من بيانات إلى معلومات[٥].

وبناءً على ما تقدم أصبح الآن بالإمكان تعريف تقنية المعلومات بأنها:((مجموعة من الأدوات التي تساعد المستفيد للعمل مع المعلومات ولإنجاز الواجب المتعلق بمعالجتها)) و تقنية المعلومات في معناها الواسع تعني التعامل الفوري مع المعلومة، وهي علم التعامل المنطقي مع المعلومات باعتبارها ناقلة المعارف الإنسانية، والعلاقة وثيقة بين القانون و تقنية المعلومات، فالقانون يحدد القواعد التي تحكم أنماط السلوك المختلفة والكثير من أنماط السلوك تتعامل الآن مع تقنية المعلومات كظاهرة تفرض نفسها على الواقع الاقتصادي والسياسي والاجتماعي والحربي[٦].

اهمية تقنية المعلومات

كما نتج عن التحكم البشري في القدرة الميكانيكية وإحلالها بدرجة كبيرة مكان القوة العضلية للإنسان والحيوان ما يسمى (بالثورة الصناعية)، كذلك يقف التحكم في المعلومات من خلال التطوير المتواصل لتقنية المعلومات كمساعد للقدرات التنظيمية للعقل البشري وراء ثورة كلية شاملة تجتاح العالم، وهي الثورة المعلوماتية الموسومة أيضاً (بالثورة الصناعية الثالثة)، التي تعزز الإمكانات الفكرية والقدرة المنطقية للإنسان وتنقل الحضارة الإنسانية من عصر الصناعة إلى عصر، أو مجتمع، المعلومات[٧]. ونستطيع أن نستخلص اهمية المعلوماتية (تقنية المعلومات) باستعراض النقاط الآتية[٨]:

١. **هي في كل مكان تستخدم لإنجاز الأعمال كافة.**
٢. **تساعد المنتج ليكون أكثر إنتاجية.**
٣. **دائمة التغيير ومواضيعها مثيره للغاية.**
٤. **تغني مهنة المستفيد بالخبرات.**

أسلفنا أن المعلوماتية (تقنية المعلومات) يمكن أن يطلق عليها بالثورة الصناعية الثالثة ومع هذه الثورة، وما نجم عنها من تحولات اقتصادية واجتماعية تشهد ببزوغ فجر مجتمع المعلومات، وتزايد استخدام الحواسيب كأداة لتخزين ومعالجة واسترجاع المعلومات وكمعاون مهم في عمليات التصميم والتصنيع والتحكم والإدارة، وتطورت تطبيقاته من أداء بعض العمليات الحسابية إلى أداء الخدمات في مجالات عديدة كما أشرنا إليها آنفاً. ولكن الذي يحقق كل هذه النشاطات والفعاليات ست **وظائف** أساسية تقوم بها المعلوماتية وهي على النحو الآتي[٩]:- (١) عملية جمع(Data Capture) (٢) عملية تحويل (Processing) (٣) عملية التوليد (Generation) (٤) يُمكّنُ الخزنُ (Storage) (٥) هي عملية استرجاع (Retrieval) (٦) هي عملية نقل (Transmission).

المطلب الثاني

التطور التاريخي لجريمة تقنية المعلومات والتعريف بها

وكطبيعة النفس البشرية حيث يستغل بعض الأشرار المخترعات العلمية وما تقدمه من وسائل متقدمة في إرتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المستحدثات، أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلاً لهذه الجرائم أو وسيلة لارتكابها. وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين على وجه الخصوص، بصورة أدت إلى بروز ظاهرة إجرامية جديدة تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني[١٠].

بدأت الدراسات البحثية الأكاديمية تشير إلى أن ظاهرة جرائم تقنية المعلومات قد بدأت في نهاية الخمسينات من القرن العشرين، ولكن ضمن إطار مفهوم "إساءة استخدام الحاسوب" المؤسس على البعد الأخلاقي، وحتى عقد الستينات اتسعت دائرة تناول أنشطة إساءة استخدام الحاسوب عبر وسائل الإعلام[١١]. ومنذ الحالة الأولى الموثقة عام ١٩٥٨م لجريمة ارتكبت في الولايات المتحدة الأمريكية بواسطة الحاسب، وإلى حد الان، كبر حجم هذه الجرائم وتنوعت أساليبها وتعددت اتجاهاتها وزادت خسائرها و أخطارها حتى صارت من مصادر التهديد

البالغة للأمن القومي للدول، خصوصا تلك التي ترتكز مصالحها الحيوية على تقنية المعلومات وتعتمد عليها في تسيير شؤونها[١٢]. وعلى هذا يمكننا تعريف جريمة تقنية المعلومات بأنها أي سلوك سيئ متعمد يستهدف الإضرار بتقنية المعلومات أو يستخدم تقنية المعلومات لإلحاق الضرر، أو ينتج عنه حصول أو محاولة حصول المجرم على فائدة لا يستحقها[١٣]. لقد طرحت تعريفات عديدة ومتفاوتة فيما بينها ضيقا واتساعا، ويمكن بوجه عام تصنيفها إلى الفئات الأربع التالية[١٢]:

١. التعريفات المتمركزة حول وسيلة ارتكاب الجريمة.
٢. التعريفات المتمركزة حول موضوع الجريمة.
٣. التعريفات المرتبطة بتوافر المعرفة بتقنية المعلومات.
٤. تعريفات مختلطة ومتنوعة.

المبحث الأول

أركان جريمة تقنية المعلومات وأنواعها

وجدت الجريمة بوجود الإنسان فقاومها وابتكر السبل لمواجهتها أو القضاء عليها وتنوعت العقوبات التي يحكم بها على مرتكب السلوك الإجرامي فلكل سلوك إجرامي عقوبة تتناسب مع الخطورة الكامنة في نفس فاعل الجريمة وتلك معادلة طبيعية عادلة لازمة لنجاة البشرية واستقرارها في حياة آمنة مطمئنة[١٤] فكل جريمة لها أركانها الخاصة بها حددها المشرع لمعاقبة كل من ينتهج السلوك الإجرامي إذا انتفى احدها لا تقوم الجريمة ولا يبقى لها وجود ولا تترتب على الفعل المسؤولية الجنائية وهذه الأركان قد تختلف من جريمة إلى أخرى بحسب نوعها وطبيعتها وان كانت كلها مستمده من النظرية العامة للتجريم وهذه الأركان: هي الركن المادي، الركن المعنوي، وركن الشرعي(مبدأ لا جريمة ولا عقوبة إلاَّبنص).

المطلب الأول

أركان جريمة تقنية المعلومات

فإذا كانت الجرائم العادية تتكون من أركان تتصل فيما بينها حيث أن هدم أي ركن يؤدي إلى زوال النموذج الإجرامي للفعل، فأن جرائم تقنية المعلومات تتطابق مع الجرائم العادية وبذلك فهي تتكون من الأركان الآتية:

أولا: الركن المادي

يتكون الركن المادي عادة من سلوك ونتيجة وعلاقة سببية بين السلوك والنتيجة[١٥]. وهو ذلك السلوك الظاهر المحسوس للإنسان الذي ينشأ عند إحداث اثر في العالم الخارجي ويترتب على ذلك اعتداء على مصلحة للغير يحميها القانون بإنزال العقاب بمن يلحق الضرر بها وعلى هذا الأساس فأن الرغبات والنيات والأماني والتي تعتبر من المعاني الداخلية المستقرة في النفس والتي لا تفصح خارجياً عن الإخلال بالمبادئ الإنسانية أو الاجتماعية أو الإخلال بالحقوق العامة لا تعتبر من الجرائم المعاقب عليها[١٦] .

أما في جرائم تقنية المعلومات فهي كثيرة ومتنوعة يجعل من الصعب جداً على هذا البحث تغطيتها، لذلك سنقتصر في هذا المجال على التطرق إلى بعض أنواع هذه الجرائم الأكثر شيوعاً وتحديداً بما يتعلق بالركن المادي للجريمة[١٧].

النوع الأول: جريمة الدخول غير المشروع

يتمثل الركن المادي في جريمة الدخول بدون وجه حق في القيام بصورة واحدة من النشاط، وهي الدخول غير المشروع، وهي صورة أخرى تعرفها التشريعات المقارنة وهي صورة البقاء غير المصرح به، وهي جريمة من يكون من حقه أن يدخل إلى نظام معين لمدة معينة ولكنه يستمر بعد المدة المصرح له بها، وهو ما يحدث من بعض الموظفين الذين يعملون في جهات معينة ومن حقهم أن يستخدموا أجهزة الحاسوب تلك الجهات في فترات معينة ولكنهم يسيئون استخدامها في غير تلك الأوقات.

فإذا كانت هذه الجريمة قد عالجتها ونصت عليها القوانين العربية، كما هو الحال في تونس حيث يوجد قانون خاص بالتجارة الالكترونية وهو القانون رقم(٨٣) لسنة ٢٠٠٠ بشأن المبادلات التجارة الالكترونية. غير أن قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ لم يورد نصوص بشأن جرائم تقنية المعلومات الا أن المحقق أو القاضي يستطيع الرجوع إلى قواعده العامة لتوقيع العقاب بحق من يرتكب الجريمة فمثلاً المادة (٣٠٤) ق.ع.ع ((يعاقب كل من يذيع بطريقة من الطرق العلانية وقائع ملفقة أو مزاعم كاذبة وهو يعلم بتلفيقها أو بكذبها وكان من شأن ذلك إحداث هبوط في أوراق النقد الوطني أو إضعاف ...)).

النوع الثاني: جريمة العبث بالنظام أو بالبيانات

يتكون الركن المادي من نشاط ونتيجة وعلاقة سببية، فهي إذن جريمة مادية أي جريمة ضرر وليست مجرد جريمة خطر كجريمة الدخول. والعبرة ليس بطريقة معينة اتبعها الجاني، بل بقيامه بسلوك إيجابي يتمثل في استخدام أية وسيلة يحقق بها غاية معينة وقد حددها نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية الصادر في١٤٢٨/٣/٧هجرية الموافق٢٠٠٧/٣/٢٦م ضمن عدد معين من الأضرار منها أن يتوصل الجاني إلى إيقاف الشبكة المعلوماتية عن العمل. وعلى الرغم من عدم وجود قانون عراقي للمعلوماتية فأنه يمكن الاستعانة بالقوانين العقابية لتوقيع العقوبة بحق مرتكب مثل هذه الجريمة، حيث بينت المادة (٣٠٠) الفقرة (١) ق.ع.ع ((يعاقب بالسجن مدة لأتزيد على سبع سنوات كل من اتلف أو أفسد أو عيب أو ...)).

النوع الثالث: جريمة التصنت على النظام

جريمة التصنت على النظام جريمة نشاط وليست جريمة نتيجة، وتتضمن الاطلاع أو مشاهدة البيانات أو الحصول عليها بأية طريقة أخرى ودون مسوغ قانوني، وتمتد هذه الجريمة لتشمل انتهاك سرية المراسلات الإلكترونية.

أن قانون العقوبات العراقي لم يورد نصاً يعالج هذه المشكلة ولكن أذا كان من شأن التصنت على الشبكة أن يخلق ضرراً بالغير سواء أكان هذا الضرر واقعاً على الأشخاص أو الأموال فيمكن اللجوء إلى نصوص قانون العقوبات العراقي فإذا كان القصد من يندرج تحت نص من هذه النصوص فيمكن محاسبة الفاعل وتوقيع

العقوبة الملائمة بحقه، فمثلاً أذا كان من ارتكب عمل التصنت يريد الحصول على معلومات سرية لغرض إفشائها فهنا يمكن معاقبته وفق نص المادة(٤٣٧) ق.ع.ع.

النوع الرابع: جريمة الاستيلاء على أموال الغير

يتمثل الركن المادي في هذه الجريمة في الاستيلاء الفعلي على أموال الغير، إذن فهذه الجريمة من نوع الجرائم ذات النتيجة المادية وهي وقوع الضرر. ولا يشترط أن يستولي الجاني لنفسه على المال ولكن تقع الجريمة تامة حتى ولو سهل استيلاء الغير على تلك الأموال، ويحدث ذلك بتزويد الغير ببرامج تسهل ذلك إذا استعملوها وتمكنوا بالفعل من هذا الاستيلاء. الجرائم الواقعة على الأموال تناولها المشرع العراقي في الباب الثالث – الفصل الأول من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.

***ثانياَ* : الركن المعنوي**

أذا كان الركن المادي للجريمة هو الوجه الخارجي المحسوس للسلوك المكون لها كما وصفه نص التجريم فأن ركنها المعنوي هو الوجه الباطني أو النفساني لهذا السلوك الذي لا يتعدى انتساب السلوك الإجرامي إلى نفسية صاحبه فهو الرابطة النفسية بين الفعل والفاعل وقد يتخلف هذا الانتساب النفسي حين يصبح جسم الإنسان أداة في يد قوة خارجية عنه وتفلت سيطرة صاحبه عليه. على أن كيفية انتساب السلوك إلى نفسية صاحبه ليست واحدة، فحين ينتج السلوك حدثاَ إجراميا ما يحتمل أن تكون نفسية صاحب متخذه من هذا الحدث موقفاَ من ثلاثة مواقف. إما الإرادة الدافعة إلى تحقيق الحدث وأما الإرادة المؤيدة لوقوعه وأما محض الإرادة الخاملة، فالموقف الأول يسمى القصد المباشر والثاني القصد غير المباشر والثالث الإهمال وعدم المبالاة[١٨]. ولكل حالة من هذه الحالات أحكامها في تحديد الركن المعنوي للجريمة ففي الوقت الذي يتطلب فيه الركن المعنوي إرادة كاملة متجهة نحو تحقيق السلوك الإجرامي وعلم كامل بكافة عناصره فهنا يتحقق العمد في ارتكاب الجريمة أما إذا كان السلوك ناتجاً عن إهمال وعدم انتباه وعدم مراعاة القوانين والأنظمة فأن الفاعل يكون قد ارتكب خطأ قد يحاسب عليه القانون.

وهذا التحليل للركن المعنوي في الجرائم التقليدية ينطبق على جرائم تقنية المعلومات فالفاعل عندما يرتكب جريمة من هذه الجرائم يجب أن تتوافر العلاقة النفسية بين الفعل والفاعل في صورة علم بكل عناصر السلوك المادي وإرادة متجهة نحو هذه العناصر، ولهذا نجد أن قانون مكافحة جرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦ الاماراتي أوضح ذلك في المادة (٢) فقرة (١)، حيث بينت أن جريمة تقنية المعلومات هي ((كل فعل عمدي)) وهذا يعني وجوب توافر القصد الجنائي لكل عمل تقوم به المسؤولية الجنائية، فمن يدخل إلى موقع أو نظام أو يلغي أو يحذف بيانات أو معلومات أو يفشي أسرارها يجب أن يكون عالماً ومريداً لسلوكه ذلك والنتائج التي تترتب على هذا السلوك مما يجعله خاضعاَ للمسؤولية الجنائية أما إذا كان فعله نتيجة خطأ فلا تقوم عليه المسؤولية ما لم ينص القانون على خلاف ذلك.

بذلك فأن جريمة الدخول غير المشروع، وجريمة العبث بالنظام أو بالبيانات، وجريمة التصنت على النظام، وجريمة الاستيلاء على أموال الغير تعتبر جرائم عمدية يتطلب القانون علم الجاني بعناصرها ولارادتهِ المتجهةِ إلى هذه العناصر.

***ثالثاً*: ركن المشروعية(مبدأ الشرعية)**

يقصد بهذا المبدأ أن التجريم والعقاب هو احد مظاهر سيادة الدولة وسلطتها وأن القانون هو المصدر الوحيد لتحديد الأفعال التي تعتبر جرائم والعقوبات المقررة لها تطبيقاً لمبدأ (لا جريمة و لا عقوبة إلا بنص) وأصبح هذا المبدأ من أهم الضمانات للحرية الشخصية، وقد نصت عليه المادة الحادية عشر من الإعلان العالمي لحقوق الإنسان الصادر عن هيئة الأمم المتحدة في ١٠ ديسمبر سنة١٩٤٨ [٢٠] وجسدته اغلب الدساتير ضمن نصوصها. فإذا اغفل المشرع وضع نص يجرم واقعة ضاره بالمجتمع أو تهديد مصالحه القانونية فلا يمكن وصف هذه الواقعة بعدم المشروعية طالما لا يوجد نص سابق بتجريمها وبتحديد العقاب المترتب على ارتكابها، وبذلك فأن عدم المشروعية لا يتوافر بمجرد الاعتداء على مصلحة اجتماعية أيا كانت أهميتها ما لم يكن المشرع قد نص صراحة على تجريم هذا الاعتداء [٢١]، وذلك تطبيقا لمبدأ لا جريمة ولا عقوبة إلا بنص الذي تضمنه اغلب دساتير العالم وبذلك فأنه لا يجوز القياس أو التوسع في التفسير لشمول ذلك السلوك بالتجريم والعقاب.

فإذا كانت جرائم تقنية المعلومات من الجرائم التي رافقت النهضة التقنية والتطور العلمي الذي طرأ على عالم تقنية المعلومات والانترنت ولم تكن قديمة العهد فنجد أن اغلب قوانين العقوبات وخاصة قوانين الدول النامية تخلو من نصوص عقابية لمن يرتكب سلوكاً يجعله فاعلاً أو شريكاً في جريمة من جرائم الانترنت أو الحاسوب، بذلك فأن ضرورة توقيع العقاب بمن يرتكب مثل هذه الجرائم يستوجب الرجوع إلى قوانين العقوبات التقليدية وتكييف سلوك الجاني وفق مفهوم الجريمة العادية. ولغرض قطع الطريق أمام الجناة من الإفلات من العقاب فلابد من وجود نصوص عقابية صادرة من السلطة التشريعية تحدد الأفعال الجريمة في تقنية المعلومات والعقوبات المناسبة لهذه الأفعال بذلك نصون حقوق الأفراد وحرياتهم وينال الجاني العقاب الذي يستحقه.

فإذا كانت اغلب دول العالم قد وضعت القواعد القانونية العقابية لمحاسبة مرتكبي جرائم المعلوماتية فأن العراق لحد الآن لم يضع مثل هذا القانون الذي أصبحت الحاجة ملحة لوضعه بسبب التطور العلمي والتقني والمعلوماتي الهائل والسريع ولغرض مواجهة الجرائم التي تتطور بنفس الوتيرة اعلاه٠ فلو أمعنا النظر لوجدنا أن الدول الأوربية وأمريكا قد شرعت قوانين لمكافحة جرائم المعلوماتية وقطعت شوطاً بعيداً. وكذلك بعض الدول العربية فنجد السعودية قد شرعت نظام مكافحة جرائم المعلوماتية الصادر في٢٦/ ٣/٢٠٠٧ حيث عرف هذا النظام الحاسب الآلي وعنى بالتعاملات الالكترونية وبين كيفية مكافحة جرائم تقنية المعلومات. كذلك صدرت تشريعات عربية أخرى فنرى التشريع التونسي سن قانون خاص بالتجارة الالكترونية وهو القانون رقم(٨٣) لسنة ٢٠٠٠. كما صدرت الإمارات العربية القانون الاتحادي رقم(٢) لسنة ٢٠٠٦. وقانون الجزاء العماني رقم(٢٤١٧) لسنة٢٠٠١ جرائم الكمبيوتر والانترنت وفي مصر صدر قانون رقم(١٥) في شأن تنظيم

التوقيع الالكتروني. وحيث نرى أن الدول تتسابق في إصدار التشريعات الخاصة بالمعلوماتية والانترنت، فنجد أن التشريعات العراقية تخلو من هذه القوانين، رغم أهميتها وتزايد الحاجة إلى وجودها لمواكبة التطور العلمي والتكنولوجي فيستلزم الأمر أن يقوم المشرع العراقي بإصدار قانون المعلوماتية لمواجهة المد الإجرامي وتوقيع العقوبة الملائمة وعدم إعطاء المجرمين فرصة التحايل على نصوص القانون للتخلص من العقاب.

المطلب الثاني

جرائم تقنية المعلومات تصنيفها وخصائصها

لاشك أن الجرائم التي ترتكب أما أن تكون متضمنة اعتداء على حياة الأفراد وحرياتهم أو على أموالهم وقد وفر المشرع الحماية القانونية لهذه الحقوق والمصالح. وحيث أن الجرائم العادية ترتكب وفق المبادئ والأسس التي اشرنا إليها سابقاً فأن ما ينطبق عليها من أحكام ينطبق على جرائم تقنية المعلومات التي تتضمن أيضاً اعتداء أما على حياة الأفراد وحرياتهم أو على أموالهم[٢٣].

- **أبرز التصنيفات**

ليس ثمة اتفاق على مستوى الدول حول أنماط إساءة استخدام الحاسوب الواجب تجريمها. وكخطوة تمهد السبيل لتحقيق هذا الاتفاق، اتبع المجلس الأوربي مسلكا، حظي بتأييد بعض المؤتمرات وأكثر الباحثين، قوامه وضع قائمة بالحد الأدنى من الأفعال الواجب تجريمه في التشريعات الوطنية لمختلف الدول، وقائمة أخرى اختيارية وتضم عدداً من الأفعال التي يمكن تجريمها في هذه التشريعات. وتضم **الأولى** الغش والتزوير في مجال الآلية للبيانات،والأضرار التي تصيب البيانات أو البرامج، إتلاف أجهزة ووسائل الاتصال المعلوماتي وولوج الأنظمة المعلوماتية وشبكات الحاسبات بطريق غير مشروع، والتدخل غير المشروع في الاتصالات التي تتم بين الحاسبات أو عبر شبكات الاتصال بينها، والنسخ غير المشروع للبرامج المعلوماتية المشمولة بالحماية. أما القائمة **الثانية** فتضم : إتلاف البيانات وبرامج الحاسوب، والتجسس المعلوماتي، والاستعمال غير المصرح به للحاسوب، والاستخدام غير المأذون به للبرامج المعلوماتية المشمولة بالحماية[٢٤].

- **أبرز الخصائص**

جرائم المعلوماتية هي إفراز ونتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع، مما يعطيها لونا أو طابعاً قانونياً خاصاً ويميزها بمجموعة مشتركة من الخصائص، بعضها قد يتطابق مع خصائص أخرى من الجرائم. أبرز خصائصها يمكن تجميعه حول المحاور التالية[٢٥] [٢٦]: (١) الهدف والدافع وراء الارتكاب (٢) موضعها من مراحل تشغيل نظام المعالجة الآلية للبيانات (٣) التعاون والتواطؤ على الإضرار (٤) أعراض النخبة (٥) الأضرار (٦) صعوبة الاكتشاف والإثبات.

المبحث الثاني

إثبات جريمة تقنية المعلومات

عندما ترتكب الجريمة التقليدية فلابد من تحريك الدعوى الجنائية بحق المتهم ولابد من خضوع الدعوى للضوابط القانونية التي ترسمها قوانين أصول المحاكمات الجنائية وقانون الإجراءات الجنائية فهذه الإجراءات

ليست مجرد وسائل فنية بحته، بل هي أعمال تمس الحرية الشخصية عند مباشرتها في مواجهة المتهم [٢٧]فالإجراءات التحقيقية تعكس الصورة الحقيقية للحريات العامة. فالمحقق يبحث عن الحقيقة بأية وسيلة ويفترض الدفاع الاجتماعي أن الإجراءات الجنائية تدخل في وظيفة الدولة وليست فض نزاع شخصي، فالتأكد من الحقيقة بمعناها المادي والشخصي يفترض وجود مناخ إجرائي يختلف عن مناخ النظام ألاتهامي الذي لا يتيح للقاضي أن ينفذ إلى الحقيقة إلا من خلال حجج الخصوم. وبذلك فأن الدعوى الجنائية سواء أكانت حول جريمة تقليدية أو معلوماتية فلابد أن تمر بمراحل التحقيق التي تصون حرية الفرد وحقوقه سواء أكان في دور التحقيق الابتدائي أم التحقيق النهائي. لذا سيتضمن هذا المبحث من ثلاثة مطالب، الأول سيخصص لتعريف الإثبات أما الثاني فسيكون آلية التحقيق الابتدائي والأخير للتحقيق النهائي.

المطلب الأول

المقصود بإثبات جرائم تقنية المعلومات

يختلف معنى الإثبات في اللغة باختلاف موضع الهمزة، فالإثبات بهمزة القطع مصدر من الفعل أثبت حجته بمعنى أقامها وأوضحها. وتسمى الحجة التثبت بمعنى البرهان أو البينة أما الإثبات بهمزة الوصول فهو اسم مشتق من الفعل ثبت بمعنى دام واستقر مكانه، ويقال ثبت الشيء ثباتا وثبوتا. أما المعنى القانوني للإثبات فهو تأكيد حق متنازع فيه له أثر قانوني بالدليل الذي أباحه القانون لإثبات ذلك الحق[٢٨].

لما كان أساس توقيع العقوبة على المتهم إثبات إدانته بإقامة الأدلة التي تثبت وقوع الجريمة، ونسبتها إلى المتهم بوجه قاطع، ووجود الأدلة الجازمة لدى القاضي بالحكم عليه من واقع الأدلة المعروضة عليه، لذلك فإن الإثبات موضوع في غاية الأهمية، وبخاصة عند ظهور جرائم تقنية المعلومات وصعوبة اكتشافها وإثباتها، وذلك لما يتسم به هذا الإجرام من المكر والحيلة والغش والاحتيال باستخدام تقنيات معلوماتية عالية الكفاءة. وترجع صعوبة إثبات جرائم تقنية المعلومات إلى خصائص هذه التقنية ذاتها وبخاصة السرعة الفائقة التي ترتكب بها، وهو ما يسهل ارتكابها ويسهل طمس معالمها ومحو آثارها قبل اكتشافها إذ يستطيع الجاني أن يرتكب جريمة دون أن يترك وراءه أي أثر خارجي ملموس، وعدم ملائمة الأدلة التقليدية في إثباتها، ومن هنا تبدأ صعوبة البحث عن الدليل، وجمع الأدلة ومدى قبولها إن وجدت، ومدى مصداقيتها في إثبات وقائع الجريمة[٢٩].

طرق مقترحه لإثبات جرائم تقنية المعلومات

وهكذا تحددت إلاشكالية من السطور السابقة في وجود صعوبة إثبات الجرائم التي تحصل في العالم الرقمي، وذلك للطبيعة الفنية المعقدة لهذه الجرائم. ونستطيع أن نقول رأينا بأنه يجب أن يتزايد الإثبات بالخبرة والقرائن بالنسبة لهذا النوع الجديد من الجرائم، وهو ما يستوجب الاهتمام بالخبراء وتأهيلهم التأهيل العلمي الصحيح الذي يمكنهم من القيام بأعمال الخبرة.

وإن هذا الاهتمام بوسائل الإثبات، يُمكن القضاء العراقَّي من اللجوء إلى القرائن القضائية بجرأة اكبر في المسائل العلمية ويُمكنَّهم من استنباط الأمور العلمية ذات البعد الجنائي أو القانوني بوجه عام، من الأمور

الثابتة، وهذه هي فحوى القرائن (المادة ١٠٢/اولاً من قانون الإثبات رقم ١٠٧ لسنة ١٩٧٩ المعدل)، لكي يتمكن القضاة من الوصول إلى الحقيقة، من خلال القرائن القضائية بالذات، التي يعتبرها القضاء في بعض الأحيان من المسائل العلمية فيتوقف عند خبرة الخبراء ولا يلجأون إليها عملياً.

وعلى أي حال فيمكننا اقتراح عدة طرق لجمع الأدلة عن الجرائم المعلوماتية، وهي في الوقت نفسه تعد من طرق الإثبات للوصول إلى حقيقتها، والطرق المذكورةً كلها يمكننا إدراجها في نطاق القرائن القضائية التي تعُّد إحدى وسائل الإثبات المدنية ومن باب أولى تعُّد من أهم طرق الإثبات الجنائية، التي سبق الإشارة إليها وهي : **(١) المعاينة**[٣٠] **(٢) التفتيش (٣) الشهادة (٤) الخبرة في جرائم المعلوماتية**[٣١].

المطلب الثاني

التحقيق الابتدائي في جرائم تقنية المعلومات

إن القائمين على تطبيق القانون يتطلب منهم أن يملكوا معرفة محدثة ومعدات فعالة للكشف والتحري عن النشاطات اليومية للجريمة للحصول على أدلة رقمية تدين المجرمين. لأنهم يواجهون تحديات كبيرة لمهمات تحديد الأشخاص وتشخيصهم و مقاضاتهم وكذلك المؤسسات التي تعمل على استخدام التقنيات لدعم عملياتهم غير الشرعية و إسنادها.

أن عملية التحري الرقمي تختلف عن التحري في الجرائم المعتادة، بأنها تتعامل مع وسائط وأجهزة رقمية وأدلة غير ملموسة، وعلى أجهزة التحري أو مسؤولي امن المعلومات مثلا تحديد من قام باختراق النظام، وكيف تم الاختراق، وما الأضرار الناتجة عن هذا الاختراق وفقا" لمعايير واطر عملية تمنع فقدان الأدلة ومسحها. هذه الأسئلة من المهم الإجابة عنها لأنها سوف تستخدم لتدعيم الإجراءات الإدارية والمدنية والقانونية ضد مرتكبها، فالحصول على أدلة رقمية ذات فائدة سوف يوفر الوقت والموارد البشرية والمالية.

- **إجراءات التحقيق الابتدائي في مسرح الجريمة:**

من أولى الخطوات التي يجب أن تؤخذ عند مسرح الجريمة [٣٢] تأمين الحماية لجميع الأفراد المتواجدين، وصيانة الأدلة بما يمنع إتلافها أو تغيرها على أن تكون الإجراءات وفقاَ لقواعد القانون وحقوق الإنسان ثم تقيم الأدلة ليحال منها إلى القضاء ويتم توثيق كل الإجراءات في محضر يسمى محضر جمع الأدلة. وجمع الأدلة في مسح الحادثة الالكترونية يتطلب الدقة والحذر لكونه يملك قيمة في إثبات الجريمة، وهناك أنواع معينة من أدلة الحاسوب يتطلب جمعها ورزمها ونقلها بطريقة خاصة لكي لا تكون عرضه للتلف أو التبديل. ويعتبر التحقيق الابتدائي المرحلة الأولى في الخصومة الجنائية من اجل إثبات حق الدولة في العقاب. فهو يهدف إلى تحديد مدى جدوى تقديم المتهم إلى المحاكمة الجنائية لإقرار هذا الحق في مواجهته، ولقد أدت خطورة الجزاء الجنائي إلى أن يعهد إلى نوع معين من القضاء، هو قضاء التحقيق.

بالبحث عن الأدلة الجنائية لإثبات سلطة الدولة في العقاب أو نفيه، وهو أمر يتوقف على مدى إثبات وقوع الجريمة ونسبتها إلى المتهم، وفي هذه المرحلة يقوم قضاة التحقيق بدور ايجابي في جميع أدلة الإثبات أو

النفي للوصول إلى الحقيقة. وتبدو أهمية مرحلة التحقيق الابتدائي إلى تحضير الدعوى وتحديد مدى قابليتها للنظر أمام قضاء الحكم، ونظراً إلى أنها تتم على أثر وقوع الجريمة فأنها تتاح لها جميع الأدلة قبل ضياعها لأن كل تأخير في تحقيق هذه المهمة، قد يؤدي إلى تشويه صورة الحقيقة، كما أن الحاجة تبدو مهمة في تأكيد التوازن بين حق الدولة في العقاب الذي يدعو إلى اتخاذ بعض الإجراءات الماسة بحرية المتهم ويعتبر من ضمن أعمال التحقيق الابتدائي أعمال التحقيق الخاصة بجمع الأدلة، حيث يتم الانتقال إلى موقع الحادث للمعاينة، وندب الخبراء والتفتيش وضبط[٣٦] الأشياء المتعلقة بالجريمة وسماع الشهود والحبس الاحتياطي، فأن توفرت الأدلة الكافية لدى السلطة التحقيقية تأمر بإحالتها إلى المحكمة المختصة.

المطلب الثالث

التحقيق النهائي في جرائم تقنية المعلومات

لكون جرائم تقنية المعلومات تتضمن أفعال إجرامية تعرض حياة الأفراد وسلامة أجسامهم للخطر، وكذلك أموالهم فلابد من تحديد هذه الأفعال الجرمية وبيان العقوبة الملائمة لكل فعل من هذه الأفعال تطبيقاً لمبدأ (لا جريمة ولا عقوبة إلا بنص). وبذلك فأن إجراءات التحقيق النهائي التي تطبق عند ارتكاب الجرائم العادية يجب مراعاتها عند ارتكاب جريمة من جرائم المعلوماتية. فالمحكمة لا يجوز لها أن تكتفي بالتحقيقات الأولية للحكم في الدعوى. وإنما عليها أن تحقق بنفسها في التهمة المعروضة أمامها ما لم يوجد نص خلاف ذلك وتتقيد المحكمة في التحقيق الذي تجريه بقواعد معينة تختلف أحياناً بأختلاف المحكمة التي تنظر الدعوى، وتلتزم بالقواعد المقررة في الإثبات. حيث أن كافة التشريعات تتفق في أن تكون جلسات المحكمة علنية، وليس المقصود بعلانية الجلسة أن تجري المحاكمة بحضور الخصوم و أنما علنية الجلسة يقصد بها أن تفتح أبواب قاعة الجلسة للجمهور فيحضر المحاكمة من يشاء حيث يستدعى المتهم والشهود ويحق للمحكمة أن تأمر بالقبض على المتهم وإحضاره أمامها ويجوز للمحكمة أن تحكم بغياب المتهم سواء أكان بالإدانة أم بالبراءة.

حيث يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته ويأخذ الحقيقة التي ينشدها من أي مواطن يراه فقد تأبى نفسه الأخذ بإقرار المتهم لما يداخله من شك في صحته. وقد يأخذ ببعض الشهادة وينبذ البعض الآخر وأن يستند على دليل بالنسبة لمتهم دون آخر ويستطيع الاستعانة بالخبراء كوسيلة من وسائل الاستدلال للكشف عن المجرمين وأن يعزز الأدلة المتوافرة لديه. ويلاحظ الآثار المعلوماتية المستخلصة من الإجهزة الحاسوبية التي من الممكن أن تكون ثرية جداً بما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الالكتروني والصوت الرقمي وغرف الدردشة والمحادثة والملفات المخزنة في الحاسوب الشخصي والدخول للخدمة والاتصال بالانترنت أو الشبكة عن طريق مزود الخدمات.

لذلك فأن الآثار الرقمية تشمل رؤية لمسرح الجريمة الحقيقي، ومسرح الجريمة الرقمي نفسه فإذا كانت هناك جريمة حدثت فعلياً في العالم الحقيقي واستخدم حاسوب بطريقة ما في احد أفعالها فعلى يجب المحققين أن يبحثوا في كلا المسرحين، المسرح الحقيقي المادي والمسرح المعلوماتي الرقمي[٣٨]. وحيث أن قاضي الموضوع له سلطة الفصل في التحقيقات الأولية وبين الأدلة المنتجة التي يمكن الاعتماد عليها في تكوين قناعته

لإصدار الحكم لذا يدخل ضمن صلاحيته في التحقيق النهائي أن يتحرى عن الأدلة الجرمية الرقمية، وبذلك فلابد أن يكون القاضي ملماً في العمليات الالكترونية التي تمكنه من اكتشاف هذه الأدلة للتأكد من الأدلة التي تحال إليه من الجهات التحقيقية الأولية، لمطابقتها والتأكد من صحتها. حيث أن مبدأ حرية القاضي في الاقتناع يتيح له أن يستمد عقيدته من أي دليل يرتاح إليه وجدانه[٣٩]. بالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الإلكترونية وما قد يصاحب الحصول عليها من خطوات معقدة فأن قبولها في الإثبات قد يثير العديد من المشكلات فكما نعلم أن مستودع هذه الأدلة هي الوسائل الإلكترونية ، لذلك فيمكن التلاعب فيها وتغيير الحقيقة التي يجب أن تعبر عنها. وبذلك فأن القاضي يجب أن يكون ملماً بكل ما يتعلق بالجرائم المعلوماتية وأن يستعين قبل إصدار الحكم بأصحاب الخبرة والاختصاص للنطق بالحكم العادل.

الخاتمة والتوصيات

الخاتمة

ولقد شغلت الآثار الخطيرة التي ترتبت على ظهور تقنية المعلومات كل من الفقه والقضاء، فاجتهدا في محاولة إخضاع الجرائم المستجدة التي أفرزتها التقنيات الحديثة للنصوص العقابية التقليدية في ظل تطبيق أحكام النصوص الإجرائية. وعندما تبين خطر ذلك على مبدأ الشرعية الجنائية في شقيه الموضوعي والإجرائي، فقد بدأت التشريعات في الكثير من الدول بسن تشريعات جديدة، وهذا ما تم عرضه خلال البحث، أو إجراء تعديلات في النصوص المطبقة لمواجهة هذه الجرائم المستجدة كجريمة الدخول غير المشروع، وجريمة العبث بالنظام أو بالبيانات، وجريمة التصنت على النظام، وجريمة الاستيلاء على أموال الغير. كما نود أن نذكر أن هذا البحث كان بحثاً في جرائم تقنية المعلومات بكافة اركانها (المادية، المعنوية، والمشروعية).

ولقد ترتب على ذلك ظهور مشكلة في الإثبات الجنائي لهذه الجرائم، حيث أن أدلة الإثبات التقليدية قد لا تقوى على إثبات هذا النوع الجديد من الجرائم الذي أتت بها تقنية المعلومات، الأمر الذي يبرز أهمية إعادة النظر فيها في ضوء الأدلة الجديدة. مما يتطلب لاكتشاف هذه الطائفة من الجرائم الفنية والتوصل إلى أدلة الإثبات التي يمكن تقديمها إلى القضاء ضد مرتكبيها، بعد تأثيمها جنائياً في التشريع الوطني، توافر معارف ومهارات خاصة لا يتسنى دون تأهيل علمي وتدريب تخصصي، إضافة إلى استخدام وسائل وأساليب مبتكرة في عمليات البحث والتحقيق الجنائي الفني تتوافق مع طبيعة وتعقيد تقنيات المعلومات.

التوصيات

- وما نوصى به في ختام هذا البحث هو أن على المشرع الوطني أن يسرع الخطى–ولكن دون تسرع– في معالجة الثغرات التي كشف البحث عنها كما تقدم، والتي لاتغطيها النصوص الحالية، وذلك حتى تكون مواجهة هذه الطائفة من الجرائم– أسوة بمواجهة غيرها– في ظل الشرعية الجنائية: شرعية الجرائم والعقوبات.

- نوصي في تطوير مناهج الدراسة الاكاديمية في كليات القانون بما يكفل إحاطة طلابها بأساسيات تقنية المعلومات وطرق وكيفية استخدام أجهزتها وصور الإجرام التي يمكن أن تتم من خلالها وكيفية التفطن إليها واكتشافها.

وفي النهاية فهذه محاولة متواضعة، نرجو أن تكون قد وفقنا فيها –بعون من الله وفضله– للإجابة عن تساؤلات نلمحها في العيون، وفي الأذهان، وعلى ألسنة، كل من يهتم بأمور القانون الجنائي، حيث يصوب البصر إلى بداية القرن الجديد، قرن تقنية المعلومات.

Crimes of Information Technology and Their Proof

Abid Aljabar Th. Awad
Criminal Lecturer
College of Law
Al-Nahrain University

Dr. Talib Mohammed Jawad Abbas
Computer Lecturer
College of Law
Al-Nahrain University

Abstract

Technologies and information systems are spread in all societies in advanced and less developed countries. These technologies affect their movement as they organize means of transport, communication, commerce, economy, industry and means of war and peace etc. Because of this scientific progress, the crime developed also, and new type of criminal appeared with new means far from the known classical form of crimes.

The subject of this research is the crimes of information technology and how to prove it. This subject considered as a very important subject because it revealed new aspects and forms of crimes that connected with the development of means of usage to computers and Internet. Therefore, real need and deep research in the practical problems connected with this investigation of proof to information technology crimes, considered very important.

This paper will deal, at the beginning briefly with a definition of information technology. The second topic is including the identification of elements and types of information technology crimes. The last topic deals with proofs and primary and finally investigation.

هوامش البحث

---

(١) القاضي/وليد عاكوم، "التحقيق في جرائم الحاسوب"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص٥١٩.

(٢) القاضي/وليد عاكوم،"مفهوم وظاهرة الإجرام المعلوماتي"، بحوث مؤتمر القانون والكمبيوتر و الإنترنت، جامعة الإمارات العربية المتحدة –كلية الشريعة والقانون، المجلد الأول، من ١–٣ مايو ٢٠٠٠م، الطبعة الثالثة ٢٠٠٤م، ص١٢.

(٤) أ.د.هشام محمد فريد رستم،"الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب، التخصصي"، بحوث مؤتمر القانون والكمبيوتر و الإنترنت، جامعة الإمارات العربية المتحدة –كلية الشريعة والقانون، المجلد الثاني، من ١–٣ مايو ٢٠٠٠م الطبعة الثالثة ٢٠٠٤م.

(٥) خبير. عبدالناصر محمد محمود فرغلي و د.محمد عبيد سيف سعيد،مصدر سابق، ص٥.

(٦) أ.د.هدى حامد قشقوش،"الإتلاف غير ألعمدي لبرامج وبيانات الحاسب الالكتروني"، بحوث مؤتمر القانون والكمبيوتر و الإنترنت، جامعة الإمارات العربية المتحدة –كلية الشريعة والقانون، المجلد الثاني، من ١–٣ مايو ٢٠٠٠م، الطبعة الثالثة ٢٠٠٤م، ص٨٨٧.

(٧) أ.د.هشام محمد فريد رستم، المرجع السابق، ص٤٠٢.

(٨) Stephen Haag, Peter Keen, "Information Technology Tomorrow's Advantage Today", McGraw-Hill Companies Inc, 1996, p(5,6,7).

(٩) James A. Senn, "Information Technology in Business", Prentice Hall, 1995.

(١٠) د.محمد أبو العلا عقيدة، "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص١٩.

[١١] د.نائل عبدالحمن صالح، "واقع جرائم الحاسب في التشريع الأردني"، بحوث مؤتمر القانون والكمبيوتر و الإنترنت، جامعة الإمارات العربية المتحدة –كلية الشريعة والقانون، المجلد الثاني، من ١–٣ مايو ٢٠٠٠م، الطبعة الثالثة ٢٠٠٤م، ص١٩٠.

[١٢] أ.د.هشام محمد فريد رستم، المرجع السابق، ص٤٠٥.

[١٣] د.رشيد بن مسفر الزهراني، د.محمد بن عبدالله القاسم، "نموذج وطني مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور الأمني و الإداري، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص٦٨٥.

[١٤] د. رؤوف عبيد، "القسم العام من التشريع العقابي"، الطبعة الرابعة، ص٣.

[١٥] د.علي عبدالقادر القهوجي، "الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص٩٨.

[١٦] د. عبد الستار البزركان، "قانون العقوبات القسم العام"، مجلة التشريع والقضاء، ص٥٤.

[١٧] د. شيماء عبدالغني محمد عطاالله، " مكافحة جرائم المعلوماتية في المملكة العربية السعودية"، منتدى د.شيماء عطاالله–منتدى القانون الجنائي،٢٠٠٨، ص ص(٧–١٠)
www. shaimaaatalla.com

[١٨] قانون مكافحة جرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦ الاماراتي.

[٢٠] د. محمود محمود مصطفى ،"شرح قانون العقوبات القسم الخاص"، الطبعة الثانية، ١٩٨٨، ص٦٣.

[٢١] د. احمد فتحي سرور،"الوسيط في قانون العقوبات"، الطبعة الأولى، ص٢٦٣.

[٢٣] منير محمد الجهنيي المحامي، ممدوح محمد الجهنيي المحامي، "جرائم الانترنت والحاسب الآلي ووسائل مكافحتها". ص٢٨.

[٢٤] أ.د.هشام محمد فريد رستم، المرجع السابق، ص٤١٢.

[٢٥] المحامي الشهيدي، " جرائم الكمبيوتر و الانترنت"، **www.alquma.net**

[٢٦] أ.د.هشام محمد فريد رستم، المرجع السابق، ص(٤٤٥–٤٤٨).

[٢٧] د. محمد ياسر أبو الفتوح، "خصائص وتصنيفات الجريمة المعلوماتية"، منتدى د.شيماء عطاالله–منتدى القانون الجنائي،٢٠٠٨، **shaimaaatalla.com**.www

[٢٨] د. احمد فتحي سرور، مصدر سابق، ص٢١.

[٢٩] د. محمد السعيد رشدي، "حجية وسائل الاتصال الحديثة في الإثبات"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور المعاملات المدنية، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص ص(٣٦١–٣٦٢).

[٣٠] خبير. عبدالناصر محمد محمود فرغلي و د.محمد عبيد سيف سعيد،مصدر سابق، ص١٧.

[٣١] لواء نبيل عبدالمنعم جاد، "أسس التحقيق والبحث الجنائي العلمي"، اكاديمية الشرطة، مطبعة كلية الشرطة–القاهرة، ٢٠٠٥/٢٠٠٦، ص١١٢.

[٣٢] حسن رجب حسن الزهراني، "إثبات جرائم تقنية المعلومات"، بحث تكميلي مقدم لنيل درجة الماجستير، المملكة العربية السعودية، وزارة التعليم العالي، جامعة الإمام محمد بن سعود الإسلامية، المعهد العالي للقضاء، ٢٠٠٥، ص٢ www.imamu.edu.sa

[٣٦] د. احمد فتحي سرور، مصدر سابق، ص٨٨.

[٣٨] د. محمود محمود مصطفى ،مصدر سابق، ص٣٩٠.

[٣٩] د. ممدوح عبد الحميد عبدالمطلب، "استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم عبر الكمبيوتر"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي–الإمارات العربية المتحدة، ٢٦–٢٨ أبريل ٢٠٠٣، ص٦٤٦.