جـــــــــــامـــــــــــعـــــــــــة
المسيـــــــــــلـــــــــــة
كـــــــــــلـــــــــــيـــة الحـــــــــقـــــــــوق
قسم الحقوق

العنوان

إثبات الجريمة الإلكترونية

مذكرة تكميلية لنيل شهادة الماستر تخصص
قانون جنائي

إعداد الطالب:
❖ كيحل خير الدين

تحت إشراف الأساتذ:
❖ بلواضح الطيب

السنة الجامعية: 2013/2012

* وفوق كل ذي علم عليم *

صدق الله العظيم

شكر و

أول الشكر شكر الله تعالى و حمده و الثناء عليه حمدا يليق بجلاله أن

وفقنا لصالح الأعمال و لإنجاز هذا العمل المتواضع.

شكر جزيل مرفق بأرقى عبارات
المحبة و الامتنان لأستاذي القدير

الطيب بلواضح الذي كان خير معين لي خلال انجازي لهذا العمل المتواضع.

شكري للأستاذ الكريم زرواق نصير وكل
الأساتذة الذين اجتمعت بهم

خلال مشواري الدراسي و إلى كل من ساهم من قريب أو من بعيد

في انجاز هذه المذكرة.

الإهداء

إلى أعز إنسان على قلبي ... والدي الغالي

إلى لمن كانت جنتي تحت قدميها ...أمي الحبيبة

إلى إخوتي و أخواتي و أستاذي .....

إلى أعز و أجمل و خير رفيق عرفته في حياتي ... وفاء الغالية

أليكم أهدي هذا العمل....

مقدمة

مقدمـــــة:

الجريمة ظاهرة تاريخية ، ترتبط بالوجود الإنساني و تواكب تقدم الإنسان و ارتقاءه في كل أطواره الحضارية. ومع دخول العقد السادس من القرن الماضي ، القرن العشرين، ظهر في عالم الجريمة نوع جديد من الجرائم ،يرتكب عبر الوسائط الالكترونية ،مواكبا لنشوء نظم الحواسيب و تطورها و نشوء شبكاتها العالمية و ثورة التكنولوجيا المعلوماتية، وقد أكدت الدراسات القانونية الحديثة أن الجرائم الالكترونية تنطوي على مخاطر جمة ،سياسية و اقتصادية واجتماعية و تلحق بالمؤسسات و الأفراد خسائر باهظة باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة ،وتطول المعلومات الحيوية ، و برمجيات التشغيل الحديثة و،والبيانات الرقمية ،و سلامة النفوس و رؤوس الأموال و الحياة الخاصة للأفراد و غيرها.

و كما يطور الناس علاقات إنتاجهم ووسائله يطور الناس علاقات جرائمهم ووسائلها باعتمادهم على الوسائل الالكترونية لارتكاب أفعالهم مما يستدعي تطوير المشرع لنصوصه الإجرائية و العقابية لتحسين كفاءة المحققين في دفع الجريمة الالكترونية و مواجهة مرتكبيها.الأمر الذي دفع بالمشرع إيجاد نصوص خاصة و آليات جديدة لمتابعة و اكتشاف و تجريم الأفعال المحظورة و التي تمس بأمن و سير أنظمة المعالجة الآلية للمعطيات ،وكذا إيجاد آليات أكثر فاعلية في إثبات هذا النوع الخاص من الجرائم إذ أن طرق الإثبات التقليدية باتت لا تنفع مع مثل هذه الجرائم أو بالأخص في بيئة رقمية لا ترى بالعين. و بهذا

ظهرت أدلة جديدة لها القدرة الفائقة في اكتشاف و إثبات هذا الإجرام والمتمثلة في الدليل الرقمي.

وقد واجه أصحاب الاختصاص في مجال بحث ومكافحة هذه الجرائم قبل ظهور الدليل الرقمي و البروتوكول tcp/ip عدة مشاكل عملية عند اعتمادهم على الأدلة التقليدية – على غرار الشهادة و القرائن و الاعتراف و المعاينة و التفتيش و غيرها – حيث أنها لا تنفع في البيئة الرقمية التي تعتبر في الجرائم الالكترونية مسرح الجريمة وهو عكس المسرح الموجود في الجرائم التقليدية ، اذ أن المسرح الرقمي عبارة عن بيانات أو نبضات مغنطيسية أو كهربائية غي مرئية و غير ملموسة ، و من بين المشاكل العملية التي تواجه أدلة الإثبات التقليدية في إثبات الجرائم الالكترونية سهولة محو أو تدمير الدليل كليا و في فترة وجيزة مما يجعل عملية القبض أو حتى متابعة و التعرف على الجاني وقت ارتكاب الجرم عملية شبه مستحيلة خاصة ما إذا استعمل فنيات إخفاء الهوية أو القيام بالجريمة من بلد أجنبي ،و في حالات كهذه ماذا سيفيد التفتيش أو المعاينة في مسرح مجهول؟ ،وماذا تفيد الشهادة و الاعتراف مع مجرم لم نرى منه إلا جريمته؟ ، و مع استحالة اكتشاف الجريمة أو إثباتها صار من السهل على الجاني الالتفاف حول القانون العقابي و الفرار من العقاب،و مع وجود المواد المعاقبة على أفعاله صار هذا الأمر خرقا واضحا لمبدأ الشرعية .

انطلاقا مما تقدم يتضح أن الجريمة الالكترونية أصبحت تحديا كبيرا للفقه و التشريع و القضاء فاقتنعوا بضرورة مواكبة هذا التطور الملحوظ في الجرائم المعلوماتية و

مواجهتها تشريعيا بقواعد قانونية و إجرائية غير تلك التقليدية لهذا النوع من الجرائم المستحدثة .

التعريف بالموضوع:

إن موضوع الإثبات في الجرائم الالكترونية من المواضيع المستحدثة نظرا للطابع الخاص الذي تمتاز به هذه الجريمة و الإجراءات الخاصة التي ترتكز عليها للوصول إلى مرتكبي هذه الأفعال .

عرف الإثبات في المواد الجنائية على أنه إقامة الدليل لدى السلطات المختصة في الإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية وذلك بالطرق التي حددها القانون وفق القواعد التي أخضعها لها .

و عرفت الجريمة الالكترونية على أنها فعل أو أفعال غير مشروعة تتم بواسطة أو تستهدف النظم البرمجية أو نظم المعالجة الإلكترونية للحاسب الآلي أو الشبكات الحاسوبية أو شبكة الإنترنت و ما على شاكلتها.

من خلال التعريفين يمكن استخلاص تعريف بموضوع الجرائم الالكترونية على أنه : إقامة الدليل أمام السلطات المختصة في الإجراءات الجنائية على وقوع فعل أو عدة أفعال غير مشروعة تتم بواسطة أو تستهدف النظم البرمجية أو نظم المعالجة الإلكترونية للحاسب الآلي أو الشبكات الحاسوبية أو شبكة الإنترنت.

و ما هو مسلم به أن من خصائص الإثبات الجنائي أنه يتم أمام القضاء ،و أن ينصب الإثبات على وجود الواقعة القانونية محل الإثبات بالإضافة إلى أن الإثبات يتم بطرق محددة قانونا و يعتد بها القاضي ، و تتمثل هذه الطرق فيما نصطلح عليه في موضوعنا الطرق التقليدية للإثبات و هي الأدلة الشخصية المتمثلة في الاعتراف ، الشهادة و الأدلة المادية المتمثلة في المحررات ، القرائن و الأدلة الفنية المتمثلة في الخبرة و المعاينة ، بالإضافة إلى هذه الأدلة و بالنظر للطابع الخاص الذي تمتاز به الجريمة الالكترونية و نظرا لمحدودية عمل الأدلة التقليدية على مسرح الجريمة الرقمي وجب الاعتماد على أدلة أكثر فاعلية و تناسبا مع الأفعال المشكلة للجريمة المعلوماتية أو ما يصطلح عليه بالدليل الرقمي و البروتوكول tcp/ip.

أهمية الموضوع:

تكمن أهمية البحث في أنه يقدم دراسة نظرية وعملية عن الإثبات العلمي الجنائي للجرائم المعلوماتية ،من الجانب القانوني والجانب العلمي الفني الشرعي ، حيث أنه يشتمل على تعريفات للجريمة الالكترونية ،وكذا صورها و طرق ارتكابها و المشكلات العملية التي تواجه أصحاب الاختصاص في مكافحة هذا الإجرام و الأهم من هذا طرق اكتشاف و إثبات هذه الجرائم .

أهداف الموضوع:

1-إلقاء الضوء على عملية الإثبات الجنائي للجرائم المعلوماتية ومدى صلاحية الطرق التقليدية في هذا الصدد.

2 -توضيح الدور الذي تقوم به الطرق التقليدية في عملية الإثبات العلمي الجنائي للجرائم الالكترونية و ما هو القصور الذي تعانيه في البيئة الرقمية .

3- إبداء الطرق البديلة و الأكثر فعالية في كشف و إثبات الجرائم الالكترونية و مدى الأخذ بها من طرف القاضي الجنائي .

أسباب اختيار الموضوع:

الأسباب الشخصية :

حب الإطلاع و الاستكشاف و الفهم و البحث في كل ما هو جديد على أساس أن هذه الجريمة مستحدثة و لا تزال خفية المعالم خاصة في الدول النامية .

التعامل الدائم مع جهاز الكمبيوتر و شبكاته وكذا مع الكثير من مرتكبي الاجرام الالكتروني ، وكدارس للقانون ألاحظ الخرق الكبير في مبدأ الشرعية اذ أنني أرى مجرمين و لا أرى متابعة على أفعالهم غير المشروعة مع وجود النصوص المعاقبة .

الأسباب الموضوعية :

– إساءة استخدام النظم الحاسوبية وشبكات الاتصال التي أدت إلى زيادة معدل الإجرام المعلوماتي.

– عدم كفاية النظم والقواعد القانونية التقليدية لعملية الإثبات الجنائي للجرائم المعلوماتية.

– عدم كفاية النظم والقواعد الفنية التقليدية لعملية الإثبات الجنائي للجرائم المعلوماتية

– الآثار الهائلة التي تخلفها و التي تنشأ عن الاستخدام غير المشروع لجهاز الكمبيوتر و أنظمته .

– تفسير و إظهار عمل الطرق الأكثر فعالية في إثبات الجرائم الالكترونية و عدم التركيز على الأدلة التقليدية لوحدها قصد الكشف عن الجرائم الالكترونية و ذلك لعدم تناسبها و البيئة الرقمية .

المنهج المتبع:

في أثناء إعدادنا لهذه الدراسة قمنا بإتباع المناهج التالية:

المنهج التحليلي : هو المنهج القائم على التفسير و التحليل لجزئيات البحث ، وذلك من خلال تأصيل الفكرة و ردها إلى أصلها .

المنهج المقارن : هو المنهج القائم على مقارنة التشريعات في عدة مواضع من هذه الدراسة.

إشكالية الموضوع:

مع التطور التقني لأساليب ارتكاب الجرائم خاصة تلك التي ترتكب عبر جهاز الكمبيوتر أصبح مطلوبا من سلطات إنفاذ القانون أن تتعامل مع أشكال جديدة من الأدلة في إطار إثبات الجرائم لذلك تكمن مشكلة البحث في:ما قدرة الأدلة التقليدية على إثبات الجريمة الالكترونية ؟ و هل يمكن للدليل الرقمي الحلول محل الأدلة التقليدية للإثبات في عملية إثبات الجريمة الالكترونية ؟

تتبع هذه الإشكالية عدة تساؤلات فرعية:

- ماهي الإشكالات العملية التي يواجهها المحقق في حال الاعتماد على الأدلة التقليدية للكشف عن الجرائم الإلكترونية ؟
- ماهي الأركان التي تقوم عليها جريمة المعالجة الآلية للمعطيات ؟
- هل حسنا فعل المشرع الجزائري حين حصر الصور التي تعتبر عند ارتكابها جرائم الكترونية ؟ أم أنه بهذا التضييق أغفل عدة صور أخرى لها نفس الآثار الإجرامية للصور التي حددها ؟

وفي سبيل الإجابة على هذه الإشكالية و التساؤلات الفرعية تم تقسيم المذكرة إلى فصلين بحيث نتناول في الفصل الأول ماهية الجريمة الالكترونية في أربع مباحث ثم في الفصل الثاني نتناول أدلة إثبات الجريمة الالكترونية و تقديرها في إطار نظرية الإثبات كذلك في أربع مباحث .

الفصل الأول : ماهية الجريمة الإلكترونية:

الفصل الأول : ماهية الجريمة الإلكترونية:

في بداية حديثنا عن تعريف الجريمة الإلكترونية لاحظنا من خلال الأبحاث والدراسات التي أجريت في هذا الصدد أنه لا توجد تسمية موحدة للدلالة على هذا النوع من الإجرام، وذلك خشية لحصرها في مجال ضيق قد يسمح للعديد من الصور بالإفلات من الوضع تحت خانة التجريم، وكذلك نظرا لحداثة هذه الجريمة وسرعة تطورها، ولقد أطلق الفقهاء عديد من التسميات لهذه الجريمة منذ ظهورها في إطار وضع تعريف لها.

المبحث الأول : مفهوم الجريمة الالكترونية :

المطلب الأول :الجريمة الإلكترونية وبعض المصطلحات المشابهة:

تكشف مختلف التعريفات المعروضة عن قدر المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها جرائم الحاسبات، إساءة استخدام الحاسبات، الجرائم المتعلقة والمرتبطة بالحاسبات، جرائم المعالجة الآلية للمعطيات، جرائم التكنولوجيا الحديثة، الجرائم الإلكترونية والجرائم المعلوماتية، وأخيرا الجرائم السيبيرية أو السايبر كرايم.

ولعل أهم التسميات تدور حول الجريمة المعلوماتية و الجريمة الالكترونية و كذا جرائم الكمبيوتر و جرائم الإنترنيت . و الحقيقة أن سر هذا الاختلاف يكمن في النسق الذي يعالج فيه الباحث موضوع بحثه أو أن يكون آخذا بعين الاعتبار الحق المعتدى فيها عليه وهو

المعلومة أو ما تسمى حقوق المؤلف أو حتى حقوق الملكية الصناعية أو التجارية. أما من يستخدم مصطلح جرائم الانترنيت فإنه استخدام ضيق لأنه سيقصر هذه الجرائم على سلوكيات غير مشروعة ترتكب عن طريق الولوج إلى الشبكة الدولية للمعلومات المعبر عنها بالانترنيت و التي تعتبر أكبر شبكة يمكن للعقل البشري تصورها ، حيث يمكن للملايين من البشر التلاقي و الارتباط من خلالها أو ما يسمى بالفضاء الاصطناعي ،كما أن لهذا المصطلح أن يخرج الجرائم التي يتصور ارتكابها دون الولوج الى شبكة المعلومات أو الشبكة العنكبوتية و التي يمكن ارتكابها عن طريق جهاز كمبيوتر أو غيره من وسائل الاتصال الحديثة .

أما من يستخدم مصطلح الجريمة الالكترونية فيقصد به الجرائم المرتكبة عن طريق جهاز الكمبيوتر أو إحدى الأجهزة الالكترونية الحديثة التي تعمل عمله ، و الحقيقة أننا فضلنا استخدام مصطلح الجريمة الالكترونية لأسباب متعددة منها ضرورة كون المصطلح القانوني ذو دلالة واسعة أي أن يكون مراعيا و آخذا بالحسبان مستجدات الاختراعات الالكترونية ووسائل الاتصال[1]، هذا من جانب و من جانب آخر فإن استعمال هذا المصطلح يشمل كل جرائم الحاسوب و الشبكة وكل السلوكيات التي من شأنها الحفاظ على أمن المجتمع من هذا الإجرام و كذا تقييد المجرم بحيث لا يمكن له الإفلات من النصوص الجنائية عندما يحاول تحقيق مآربه باستغلال التقدم العلمي و ما قد ينتج عنه من إمكانيات لم تكن موضع حضور في ذهن الشارع عند وضعه للنصوص الجنائية المجرمة لهذه الأفعال.

[1] محروس نصار غايب : الجريمة المعلوماتية، المعهد التقني، الأنبار، 2011.

المطلب الثاني :تعريف الجريمة الإلكترونية:

تعددت تعريفات الجريمة الإلكترونية اتساعا وتضييقا.

1- التعريفات الفقهية: اتخذت عدة اتجاهات وحسب زاوية نظر كل فقيه عرفها.

أ- تعريفات تستند على وسيلة ارتكاب الجريمة:

* **تعريف الفقيه الألماني تريدمان:** كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي[1].

* **تعريف الفقيه ليزلي بال:** فعل إجرامي يستخدم الحاسب الآلي كأداة رئيسية.

* **تعريف للفقيهان توتي وهارد كاستل:** تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب، أو بعبارة أخرى هي تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا[2].

ب- تعريفات تستند على محل الجريمة:

[1]أحمد خليفة الملط : الجريمة المعلوماتية ، دار الفكر الجامعي ، الاسكندرية ، ط 2 ، سنة 2006. ص 36.

[2]نبيلة هبة هروال: الجوانب الإجرائية لجريمة الإنترنيت، دار الفكر الجامعي ، الاسكندرية ، ط1 ،سنة 2007 ، ص 27-28.

ويرى أصحاب هذه التعريفات أن الجريمة ليست هي التي يكون النظام المعلوماتي أداة ارتكابها بل هي التي تقع على النظام أو داخله أو بعبارة أخرى يكون النظام المعلوماتي هدفا لهذا الإجرام.

* **تعريف جاء به روزن بلات:** هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل النظام أو التي تحول عن طريقه.

* **تعريف آخر:** أي عمل ليس له في القانون أو العرف جزاء ويضر بالأشخاص والأموال ويوجه ضد التقنية المتقدمة لنظم المعلومات.

* **تعريف جاءت به منظمة التعاون الاقتصادي للتنمية OCDE:** كل فعل أو امتناع من شأنه الاعتداء على الأحوال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[1].

ج- تعريفات تستند على السمات الشخصية لمرتكب الجريمة الإلكترونية:

[1]عبد الناصر محمود فرغلي ومحمد عبيد سيف سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية،بحث مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي ،جامعة نايف للعلوم الأمنية ، الرياض 2007.

هي تعريفات حاولت لصق الجريمة الإلكترونية بشخص الجاني وقدراته في مجال المعلوماتية.

* **عرفها كيلي 2001:** شخص ما مكنته معرفته واستخدامه لأجهزة الحاسوب والإنترنت أو معرفته لأحدهما من ارتكاب الجريمة المختارة[1].

* **تعريف دافيد تومسون:** جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي.

* **تعريف سولاري:** أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبيه[2].

د- تعريف يستند على الهدف من الجريمة:

كل فعل متعمد مرتبط بأي وجه من أوجه استعمالات الكمبيوتر يتسبب في إلحاق أو إمكانية إلحاق خسارة بالمجني عليه أو حصول أو إمكانية حصول مرتكبها على مكسب[3].

هـ- تعريفات لا تخضع لأي تصنيف من التصنيفات السابقة:

[1] عادل عزام سقف الحيط: جرائم الذم والقدح عبر الوسائل الإلكترونية،دار الثقافة ،الأردن ،ط1 ، 2011 ص 194.

[2] أحمد خليفة الملط: مرجع سابق ، ص 93.

[3] بورزام أحمد: جرائم المعلوماتية، محاضرة ألقيت من طرف وكيل الحمهورية لدى محكمة باتنة، بالمجلس القضائي بباتنة، يوم 2006/06/20.

ومن التعريفات الحديثة جاءت أكثر شمولية واتساعا لتقترب أكثر من مفهوم أوسع وأشمل بجريمة المعلوماتية ومن هذه التعريفات:

* تلك الأفعال غير المشروعة التي تكون شبكة الإنترنت أو أحد تطبيقاتها إما وسيلة لها أو ضحية مستهدفة من قبل الفاعل أو الفاعلين.

* وتلك الجرائم التي لا تعرف حدود جغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت وبواسطة شخص له دراية فائقة بهما.

* تعريف آخر: هي أي جريمة يمكن ارتكابها بنظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية[1].

* **تعرف الجريمة الإلكترونية:** بأنها طريقة لارتكاب الجريمة وتتم بالتسلل إلى المعلومات السرية المحوسبة إضافة إلى أنظمة الحاسوب الأكثر تعقيدا التي تقوم الأجهزة الحكومية والغير حكومية بتشغيلها، وذلك من قبل مستخدمين مهرة للحاسوب عادة ما يكون بقصد الاحتيال على هذه النظم أو اختلاسها أو اختراقها[2].

[1] نبيلة هبة هروال: مرجع سابق ،ص 27،28.

[2] يوسف شمس الدين شابسرغ: نحو مفهوم معاصر للشرطة الإلكترونية، القيادة الكاملة لشرطة الشارقة، إدارة مركز بحث الشرطة، الإمارات العربية المتحدة، ط1، 2011.

* تعريف الباحث عبد الناصر محمود فرغلي ومحمد عبيد سيف سعيد المسماري للجريمة المعلوماتية للحاسب الآلي أو الشبكات الحاسوبية أو شبكة الإنترنت وما على شاكلتها[1].

2- التعريفات القانونية:

نتناول في هذا الفرع مجموعة من التعريفات التي وردت في القوانين العقابية لبعض الدول والتي تناولت تعريف الجريمة المعلوماتية من خلال صورها ومنها قانون العقوبات الجزائري.

أ- ئكةعذإيـ اجنئئل ئكحئزا غى ئكقئمهم ئلآلذإگى: عرف قانون الولايات المتحدة الأمريكية جرائم الحاسب الآلي من خلال حصره لصور الإجرام في الصور التالية:

. العبث بالحاسب الآلي.

. الإخلال بأمن الحاسب الآلي.

. غش الحاسب الآلي.

ب- التعريف بجرائم الحاسب الآلي الإلكترونية الرقمي في القانون الفرنسي:

عرف القانون الفرنسي رقم 19 لسنة 1988 أنماط الجريمة الإلكترونية وميز بين الاعتداء

[1] عبد الناصر محمود فرغلي ومحمد عبيد سيف سعيد المسماري : مرجع سابق.

على برامج ومعلومات الحاسب الآلي وبين الاعتداء على أدواته وآلاته ولم ينص هذا القانون على تجريم سرقة المعلومات والبرامج واعتبارها مالا معلوماتيا.

ج- التعريف بالجريمة الإلكترونية في القانون الجزائري:

مثله مثل المشرع الفرنسي فقد امتنع المشرع الجزائري عن إعطاء تعريف موحد للجريمة المعلوماتية في قانون العقوبات وذلك تجنبا منه للوقوع في الخلافات الفقهية والانفراد عن غيره من التشريعات المقارنة بتعريف الجريمة المعلوماتية، ولكن ما يمكن استخلاصه من المواد التي أدرجها المشرع الجزائري في قانون العقوبات الباب الثاني الفصل الثالث القسم السابع مكرر1 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى 394 مكرر 7، أن المشرع الجزائري قد حصر الأفعال التي تعتبر مجرمة وبالتالي يمكن استخلاص تعريف المشرع الجزائري للجريمة المعلوماتية من خلال الصور المدرجة كالتالي:

جريمة المساس بأنظمة المعالجة الآلية للمعطيات: هل كل تلك الأفعال غير المشروعة ألا تتمثل في فعل الدخول أو إلقاء في كل أو جزء من المنظومة المعلوماتية وكذلك حذف أو تغيير أو تخريب لنظام اشتغال المنظومة المعلوماتية أو إدخال أو تعديل المعطيات التي تتضمنها أو تصميم أو بحث أو نشر أو الاتجار أو معالجة أو مراسلة في المعطيات المتحصل عليها من الجريمة وكذا حيازة أو نشر أو استعمال لأي غرض لهذه المعطيات مع توافر سوء النية المتمثل في القيام بأي من هذه الأفعال عن طريق الغش.

الغاية من التجريم:

إن الجريمة الإلكترونية تطرح أشكالا فيما يتعلق بالغاية من التجريم والسؤال المطروح في هذا الصدد هل أن الحماية الجنائية تستهدف المحتوى وهو النظام المعلوماتي أم المعتدى وهو المعلومة المعالجة عن طريق النظام.

الراجح أن الغاية من التجريم هي حماية النظام المعلوماتي في حد ذاته ومنتجاته لأن هذا الأخير يتضمن إضافة إلى العتاد والبرامج والمعلومات المخزنة في الذاكرة وبالتالي المحتوى، إضافة إلى أن حماية النظام المعلوماتي لا تطرح إشكالا في حماية المعلومة يثير إشكالات باعتبار أن المعلومة شيء معنوي يثير جدلا فيما يتعلق بقابليتها للتملك من عدمه هذا من جهة ومن جهة أخرى هناك ما يرى بأن في الحماية الجنائية للمعلومة مساس بحرية الإعلام[1].

المطلب الثالث :تاريخ الجرائم الإلكترونية:

[1]أمال قارة: الحماية الجنائية للمعلوماتية في التشريع الجزائري،دار هومة،الجزائر،ط1،ص 27.

ظهرت الجرائم الإلكترونية في حقل جرائم التقنية العالية في نهاية الثمانينات وكان ذلك من خلال العدوان الفيروسي وبالأخص دورة موريس المؤرخة واقعتها في نوفمبر 1988.

التطور التاريخي للجرائم الإلكترونية:

مرت الجرائم الإلكترونية بمراحل تبعا لتطور التقنية واستخداماتها، ونعرض ذلك التطور فيما يلي:

المرحلة الأولى: تميزت هذه المرحلة في شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات ظهرت أولى معالجات ما يسمى الجرائم الإلكترونية، وكان ذلك في الستينات واقتصرت المعالجات على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وترافعت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدة، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكات غير أخلاقية في بيئة أو مهنة الحوسبة، وبقي التعامل معها في النطاق الأخلاقي منه إلى النطاق القانوني، ومع تزايد استعمال الحواسيب الشخصية في منتصف السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

المرحلة الثانية: في الثمانينات طفا على السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد، وأنشطة نشر وزراعة الفيروسات الإلكترونية، التي تقوم بعمليات تدميرية للملفات أو البرامج، وشاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الدوافع لارتكاب هذه الأفعال ظل في أغلب الأحيان محصورا بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي إظهار تفوقهم الفقهي، وانحصر الحديث عن مرتكبي الأفعال هذه بالحديث عن صغار السن من المتفوقين الراغبين بالتحدي والمغامرة وإلى مدى نشأت معه قواعد سلوكية لهيئات ومنظمات الهاكرز طلبوا معها بوقف تشويه حقيقتهم وإصرارهم على أنهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات، لكن الحقيقة أن مغامري الأمس صاروا عتاة إجرام فيما بعد، إلى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطرة، القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو تستهدف التجسس أو الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والفكرية.

المرحلة الثالثة: شهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل للعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أنماط جديدة كأنشطة انكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الإنترنت التسويقية النشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين،

ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت، أو المرسلة عبر البريد الإلكتروني المنطوية على إشارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المستهدفة الترويج لمواد أو أفعال غير قانونية وغير مشروعة[1].

المبحث الثاني : أطراف الجريمة الإلكترونية

المطلب الأول: تعريف الحاسب الآلي:

يعرف الحاسب الآلي بعدة تعريفات نظرا لاختلاف زاوية نظر من عرفه، ولعل أنسب تعريف للحاسب الآلي هو الذي جاء في الموسوعة الشاملة لمصطلحات الحاسب الآلي الإلكتروني

[1]عبد الفتاح مراد: شرح جرائم الكمبيوتر والإنترنت، ص 38،39،40.

حيث عرفت تلك الموسوعة الحاسب الآلي بأنه: جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات أو إخراج معلومات وإجراء عمليات حسابية أو منطقية وهو يقوم بالكتابة على أجهزة الإخراج أو التخزين، ويتم إدخال البيانات بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل لوح المفاتيح أو استرجاعها من خلال وحدة المعالجة المركزية التي تقوم بإجراء العمليات الحسابية، وكذلك العمليات المنطقية وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج مثل الطابعات أو وسائل التخزين المختلفة[1].

المكونات المادية والمعنوية للحاسب الآلي:

أ- المكونات المادية للحاسب الآلي:

مع كون المكونات المادية للحاسب الآلي لا تشكل موضوعا مهما يتعلق بموضوع بحثنا على أساس أنها تخضع لقواعد التجريم التقليدية، إلا أننا سنتطرق إليها بإيجاز وبالقدر الذي يعطي

[1]محمد عبد الله أبوبكر: موسوعة الجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، 2007.

فكرة بسيطة عنها استكمالا للموضوع، وذلك لأن المعلوم هو أن الحاسب الآلي لا يمكن أن يراعي عمله إلا إذا توافر عنصرين أساسيين هما المكونات المادية والمكونات المعنوية والتعرض إلى جانب دون الآخر ربما يشكل إخلالا بالموضوع لذلك نتطرق إلى المكونات المادية بالشكل التالي:

1- وحدة الإدخال: هي وحدات لا يمكن إدخال البيانات أو الأوامر إلا من خلالها وهي لوحة المفاتيح والفأرة[1].

2- وحدات التشغيل المركزية: تتكون من الذاكرة الرئيسية للجهاز والتي تستخدم لحفظ البيانات والمعلومات والبرامج المدخلة في الحاسب الآلي حفظا دائما أو مؤقتا، وكذا وحدة الحساب والمنطق وهي المسؤولة عن معالجة البيانات حسابيا ومنطقيا وأخيرا وحدة التحكم وهي التي تقوم بالتنسيق بين وحدات الحاسب الآلي الأخرى والتحكم في البيانات الداخلة والخارجة من وإلى الذاكرة الرئيسية وتوجيهها إلى القنوات المختلفة.

3- وحدة الإخراج: هي الوحدة التي يمكن من خلالها تمويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة ومرئية وذلك بواسطة شاشة العرض، الطابعة وغيرها[2]

ب- المكونات المعنوية للحاسب الآلي:

[1] محمد حماد مرهج الهيتي: جرائم الحاسوب، دار المناهج، ط1،عمان، الأردن، 2006، ص 34،35.
[2] محمد عبد الله أبو بكر: مرجع سابق، ص 42.

تطرقنا فيما سبق إلى أن الغاية من التجريم في الجرائم الإلكترونية هو حماية النظام المعلوماتي ولأن المكونات المعنوية للحاسب الآلي تدخل مباشرة تحت نطاق النظام المعلوماتي فهي معنية بالحماية ولعل جوهر الحماية في الجرائم الإلكترونية هو حماية المعنويات لا الماديات المسلم به أن المكونات المادية للحاسب وكما أشرنا سابقا تخضع لقواعد التجريم التفكيكية، لذا وفي هذا العنوان سنتطرق لبيان مفهوم برامج الحاسب الآلي وبيان أنواعها:

* مفهوم برامج الحاسب الآلي:

تمثل برامج الحاسب الآلي الجزء المنطقي أو المعنوي للحاسوب وبدونها لا يمكن أن يشتغل فهي بمثابة الروح في جسد الإنسان.

وللبرامج مدلولان ضيق وواسع، يقتصر فيه الضيق على أن برامج الحاسب الآلي هي مجموعة من الأوامر والتعليمات التي تصدر إلى الحاسب الآلي لتنفيذها أي المهمة التي يأمر المستعمل الآلة بأدائها، أما المفهوم الواسع فإلى جانب تلك التعليمات والأوامر (المفهوم الضيق)+ التعليمات والأوامر الموجهة إلى العميل "بيانات استعمال البرامج وكيفية المعالجة

الإلكترونية للمعلومات" أي كافة البيانات[1] الأخرى التي يتم إلحاقها بالبرنامج والتي تساعد على سهولة فهم تطبيقه لأنها وصف تفصيلي يتضمن مراحل التطبيق[2].

* أنواع برامج الحاسب الآلي:

- **برامج التشغيل:** وهي برامج تمكن الحاسوب من أداء الوظيفة المحددة له، وهي لهذا السبب تعتبر جزءا من الحاسب نفسه ويتولى الإشراف عليها برنامج مشرف أو مراقب لتنظيم أداء هذه البرامج لدورها.

- **برامج التطبيق:** وقد تكون برامج خاصة بمعالجة الكلمات أو برامج المعطيات أو برامج صفحات القيد، وتقوم البرامج التطبيقية بتوجيه أقسام الحاسب الآلية ضمن النظام الذي وضع لها وفقا لأوامر البرامج التشغيلية المثبتة بالحاسب الآلي نفسه أو في لوحات مستقلة يتم إدخالها معها في نظام الكمبيوتر[3].

- **الحماية الدولية لبرامج الحاسب الآلي:** تتمتع هذه البرامج بالحماية القانونية الدولية التي وردت في اتفاقية TRIPS حيث نصت الفقرة الأولى في المادة 10: تتمتع برامج الحاسب

---

[1] **البيانات:** هي عبارة عن تعليمات موجهة من المبرمج الذي يتولى إعداد البرامج إلى العميل الذي يتعامل مع الآلة.

[2] محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2001، ص 41.

[3] أمال قارة: الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير، جامعة الجزائر، 2002/2001.

الآلي سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1981[1].

المطلب الثاني :المقصود بشبكات الإنترنت وشبكات الاتصال:

الإنترنت أو الشبكة العالمية للمعلومات أو شبكة الاتصالات الدولية هي في أبسط تعريف لها شبكة مشاركة معلوماتية لوكالات حكومية ومعاهد تعليمية وهيئات خاصة في أكثر من 200 دولة عن طريق أجهزة الحاسب الآلي الموصلة بالإنترنت[2].

وقد تكون شبكات الاتصال داخلية في الدولة الواحدة local area network وقد تكون عالمية wide area network الأولى هي عبارة مجموعة من أجهزة الكمبيوتر تربط مع بعضها البعض عن طريق كمبيوتر رئيسي تأخذ منه المعلومات الرئيسية Server أي ملقم الشبكة، وهذا معمول به في المؤسسات التجارية والتعليمية والشركات باختلافها وأجهزة الدولة المختلفة حيث تطوي هذه الشبكات معلومات رئيسية تزود بها الوحدات الفرعية ويتولى الجهاز المركزي مهمة تطوير البيانات وحفظها، أما الثانية فهي غير مقيدة بحدود من حيث الامتداد، فهي خيوط عنكبوتية يرمز لها بـ www ويقصد منها world wide web، فهي بحت مكتبة تضم كما هائلا من المعلومات والوصول لها يساعد المستخدم من الاستفادة من تلك المعلومات، وهذه الشبكة تضم الملايين من الاتصال ببعضهم، فيكون من الطبيعي أن

[1] محمد محمد شتا: مرجع سابق، ص 33.
[2] محمد عبد الله أبو بكر: مرجع سابق، ص 42.

تسوء سلوكيات البشر لما تقدمه هذه التقنية من إغراءات خصوصا إذا ما أخذ بعين الاعتبار سهولة الاستخدام وضعف الرقابة وعدم وجود قواعد قانونية تفرض أنماط معينة من السلوك في هذا المجال، وبذلك أصبح للإجرام في الوقت الحاضر صفة تقنية عندما اقترن بوسائل التطور هذه، فأصبحنا اليوم نسمع بالمجرم المعلوماتي والمجرم الذكي وغيرهم مما جعل هذا التقدم مرتعا لعصابات المتاجرة بالجنس وغسيل الأموال والمخدرات والإرهاب وغيرها، وهذا ما دعا لتعاون المجتمع الدولي من أجل وضع أسس المواجهة القانونية لتلك الجرائم[1].

المطلب الثالث : المجرم والضحية في الجرائم الإلكترونية:

لكي يحقق الجزاء الجنائي غايته في مجال الردع العام أو الردع الخاص، لابد وأن يوضع في الحسبان شخصية المجرم والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا للمجتمع مرة أخرى، ويمكن القول أن الجاني في جرائم الحاسب الآلي يتمتع بقدر كبير من الذكاء علاوة على أنه إنسان اجتماعي بطبيعته[2].

أ-المجرم الإلكتروني:

- في الإصطلاح القانوني:

[1]هلالي عبد الإله محمد: تفتيش نظم الحاسب الآلي وخانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997، ص 17/ 18.

[2]عبد الفتاح مراد: شرح جرائم الكمبيوتر والإنترنت، ص 44،45.

يطلق فقهاء القانون الجنائي مصطلح المجرم المعلوماتي وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه.

- في الاصطلاح الإلكتروني:

يطلق اسم "هاكرز" على أمهر المبرمجين القادرين على التعامل مع الحاسب الآلي وبرامجه والمشاكل الناجمة عنها بخبرة ودراية، بحيث كان الهاكر يقدم أسرع وأبرع الحلول لمشاكل البرمجة، وهذا في مطلع الستينات، وظهر بعد عدة تطورات واتساع لمجال استخدام التقنية الإلكترونية المتطورة ما اصطلح عليه "الكراكرز" وهو مصطلح مرادف للهاكرز، وذلك لتمتعهم بنفس إمكانات الهاكرز في السيطرة على البرمجيات، لكن هذه الفئة جاءت بعكس ما جاءت به الفئة الأولى بحيث كانت تسطو عنوة على البرامج وتكسر رموزها.

* سمات المجرم الإلكتروني:

غالبا ما يكون مجرموا الإنترنت من الأشخاص العاديين، وليسوا من عتاة المجرمين الذين يملكون القدرات والمواهب الفريدة، ويعد مجرما إلكترونيا محتملا كل شخص أيا كان عمره وعلى قدر من المهارة يدفعه إلى الإجرام التحدي التقني أو إمكانية الكسب، أو انتقاما من

سمعة سيئة أو ترويجا لمعتقداته الإيديولوجية أي أن شخص لديه القدرة التقنية التحليلية الموجهة، من المحتمل أن يصبح مجرما في العالم الافتراضي بل حتى الأفراد غير الناضجين تقنيا قادرون على مثل هذه الأعمال إذا توافر لديهم ما يكفي من الحوافز والفرص[1]، ولعل الكثير أو معظم المجرمين الإلكترونيين يمتازون بالذكاء وحب التحدي التكنولوجي والابتكار.

* أنواع المجرم الإلكتروني:

حدد مكتب التحقيقات الفدرالي الأمريكي ثلاثة أنواع من المجرمين الإلكترونيين وفق لنتائج أعمالهم الإلكترونية، بحيث كان التقسيم إلى متسللين وهم عموما من صغار المجرمين الذين يسعون إلى التنشيط الفكري عبر ارتكاب الجرائم الإلكترونية، والمجرمون وهم أغلب الأحيان من البالغين، ومنهم المحتالون أو من يتسببون بإصابة النظام بضرر والجواسيس وغيرهم، أما النوع الثالث فهم المخربون وهم عادة لا يسعون إلى التنشيط الفكري وغالبا ما تكون دوافع الانتقاد متأصلة لديهم سواء استندت إلى أسباب حقيقية أو وهمية.

وقد وضعت الأعمال الكاملة كيشور Kishore 2005 تصنيفا عاما للمجرمين الإلكترونيين يقسمهم فيه إلى خمس مجاميع هي:

1- المجرمون ذو الياقات البيض: ويضع تحت هذه المجموعة المجرمون الذين يسعون إلى الانتقام والمجرمين المصابين باليأس، ويعد العشاق والأزواج المنبوذين والموظفين الذين تم

[1] عادل عزام سقف الحيط: مرجع سابق، ص 199.

الاستغناء عنهم ورجال الأعمال الذين يشعرون أنهم خدعوا وغيرهم من أبرز المجرمين الذين ينتمون لهذه الفئة وتحركهم الرغبة في الانتقام.

2- قراصنة الحاسوب: المراهقون هم ابرز من ينتمي لهذه المجموعة والقرصنة هي الوصول إلى أجهزة الحاسوب بطريقة غير مشروعة سواء لغرض الترفيه أو السطو على المعلومات.

3- منتهكوا حقوق النشر: يشير هذا المصطلح إلى المجرمين الذين ينتهكون حقوق التأليف والنشر الخاصة بأشخاص آخرين لكي يتفادوا دفع حقوق الطبع والنشر مقابل الانتفاع بهذه المواد مثل الأفلام، البرمجيات، الموسيقى والكتب.

4- المجرمون النفسيون: ينتمون لهذه الفئة المتتبعون والمترصدون الإلكترونيون والمهووسون بجنس الأطفال أو المتعصبون المحرضون على الكراهية وغيرهم.

5- المحتالون: وربما تكون هذه الفئة أكثر مكرا وخداعا ضمن المجرمين الإلكترونيين فهم مثل الحرباء من حيث القدرة على تشكيل شخصيتهم وسلوكهم كما شاءوا ومتى أرادوا لخداع ضحاياهم الغافلين وسلب أموالهم.

بشكل عام يختلف مرتكبو الجرائم الإلكترونية عن مرتكبي الجرائم التقليدية بأن أولئك الناس يحتلون في الغالب مكانة عالية في مجتمعاتهم ويتمتعون بقدر كاف من العلم والمهارة والقدرة الفنية والتخصص في مجال أنظمة الحاسوب[1].

[1] عادل عزام سقف الحيط: مرجع سابق، ص 195، 196، 197.

* دوافع المجرم الإلكتروني:

يمارس المجرم الإلكتروني نشاطه الإلكتروني بدوافع مادية غير سوية أو معنوية وترجع هذه الدوافع إلى عدم توازن شخصيتهم[1]، سواء في العنصر المعنوي وهو عدم الفهم الصحيح للدين أو الديانات الأخرى، أدبا وأخلاقا أو في العنصر الاقتصادي وهو عدم توفر مواد مالية لإشباع الطمع نحو المزيد من الرفاهية ورفع مستوى المعيشة أو العنصر الفكري وهو التعلم والخبرة في مجال تقنية المعلومات من الحاسب الآلي وشبكات المعلومات والاتصال والإلمام بالبرامج والنظم ولغة التشغيل مع انعدام العنصر المعنوي أو في العنصر الاجتماعي وبين إقامة علاقات اجتماعية عبر شبكات الاتصال بما يخدم أهدافه غير السوية لعدم توفر العنصر المعنوي لديه[2]، بالإضافة إلى هذه الدوافع تبقى دوافع خاصة وهي الترفيه أو حب المغامرة والتحدي الإلكتروني والانتقام وكذا الدوافع النفسية الجنسية وغيرها.

ب- الضحية الإلكترونية:

المعتدى عليه في الجرائم الإلكترونية أو المجني عليه هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا أو شركة أو مؤسسة تتعامل بمجال الحاسوب، أثناء ممارسة الأعمال التجارية أو الاقتصادية أو السياسية وإلا ينبغي أن تستغل الحاسوب في إدارة أعمالها وأن يكون لدى المجني عليه حاسوب أو أكثر

---

[1] **توازن الشخصية:** يقصد به الثقة بالنفس وتعني التوازن المعنوي والفكري والجسماني والاقتصادي والاجتماعي.

[2] محمد مصطفى موسى: التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة ،القاهرة،2009،ص 15.

مرتبط بشبكة المعلومات الإلكترونية لأن الجريمة تقع على ما يحتويه الحاسوب من برامج ومعلومات وبيانات[1] والتي بدورها تعتبر مناط التجريم، والمعلومات أو المعلومة هي "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة"[2]، وتمتاز المعلومة بعدة خصائص ومميزات تتلخص في التحديد والابتكار والسرية والاستئثار.

ولا تتم الجريمة إلا من خلال حاسوب آخر يخص الجاني، ويلاحظ أنه من الصعب تحديد ضحايا هذه الجرائم على وجه الدقة لأن هؤلاء الضحايا لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل وفي هذه الحالة يدون أنه من الحكمة عدم الإبلاغ عنها وبالتالي لا يحبذ أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضده انتهاك ما، وهذا السلوك السلبي يعتبر مغريا لمرتكبي الجرائم للاستمرار في نشاطهم.

وتوجه هذه الجرائم بصفة خاصة إلى البنوك وإلى المواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة بالجريمة هي التي تعتمد أكثر من غيرها على أجهزة الحاسوب وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضررا إذ بلغت نسبة هذه الجرائم الموجهة ضدها 19% من نسبة الجرائم المكتشفة، والنسبة الموجهة للإدارة 16% والموجهة للإنتاج

[1] محمد عبد الله أبو بكر: مرجع سابق، ص 71،72.

[2] خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ط1، 2011، ص 37.

الصناعي 10% وتليها شركات التأمين والشركات الخاصة حيث أن التطور التكنولوجي الهائل وازدياد أعداد المستخدمين لأجهزة الحاسوب والانتشار الواسع في استعماله أدى إلى الاستعمال السيئ وظهور الجرائم[1].

المبحث الثالث : خصائص الجريمة الإلكترونية:

إن التطور الذي حصل في مجال المعلوماتية كان له الأثر الكبير في ظهور نوع جديد من الإجرام حيث شهد نموا وازدهارا وانتشارا في المجتمع بسبب حجم ودور التقنية الإلكترونية في القطاعات المختلفة، ولقد تميز هذا النوع من الإجرام المستحدث عن غيره من الجرائم التقليدية بلون وطابع قانوني يختلف به عن الأخيرة ويتفق معها في ميزات نذكرها كالتالي:

المطلب الأول: الخصائص المشتركة على بعض الجرائم:

تشترك الجريمة الإلكترونية من حيث خطورتها البالغة والحجم الهائل من الأضرار التي قد تنشأ عنها وكذا بوصفها جريمة عابرة للحدود مع العديد من جرائم القانون الأخرى كالإرهاب والمخدرات وعليه نأتي لتفصيل هذه الخصائص كالتالي:

[1] خالد عياد الحلبي: مرجع سابق، ص 38.

* **خطورة الجريمة الإلكترونية:** وذلك لمساسها بالإنسان في فكره وحياته الخاصة وتمس المؤسسات في اقتصادها والبلاد في أمنها القومي والسياسي والاقتصادي ولعل أكبر دليل على خطر الجريمة الإلكترونية هي لغة الأرقام حيث قدرت دراسة أمريكية قدمت من نقابة المحامين الأمريكيين عام 1984 أن حوالي ثلاثمائة شركة من أكبر الشركات هناك تعاني خسارة سنوية بسبب الإجرام الإلكتروني بحوالي 15 مليون دولار، وتعتبر البنوك (الجيل الجديد) الهدف الرئيسي للجيل الجديد من مجرمي تقنية المعلومات وذلك لاعتمادها كليا على أنظمة التمويل إلكترونيا[1].

* **تعتبر من الجرائم العابرة للحدود:** في عريف سابق لشبكة الإنترنت وصفت الشبكة بأنها عالمية إذ بإمكان أي شخص بجهاز كمبيوتر متصل بالشبكة وفي إطار استعماله غير المشروع لهذه الوسيلة ارتكاب جرائم في إقليم آخر بالتحول في معطيات الضحية وتدميرها أو سرقتها أو ارتكاب أي صورة من وصر الإجرام الإلكتروني.

المطلب الثاني: الخصائص التي تنفرد بها الجريمة الإلكترونية عن الجرائم الأخرى:

[1] سميرة معاشي: مفهوم الجريمة المعلوماتية في التشريع الجزائري،المجلة القضائية ،جامعة بسكرة.

تتميز الجريمة الإلكترونية عن غيرها من الجرائم بخصائص لا توجد في غيرها من الجرائم، ونلخص هذه المميزات في أن الجريمة الإلكترونية تتطلب لارتكابها وجود جهاز كمبيوتر مع معرفة تقنية باستخدامه وكذلك فهي جريمة صعبة الاكتشاف والإثبات.

* **تتطلب لارتكابها وجود جهاز كمبيوتر مع معرفة تقنية باستخدامه:** إذ يجب لقيام هذه الجريمة استخدام الحاسوب أو أحد الأجهزة الإلكترونية المتطورة التي تعمل عمل الحاسوب والتي من خلالها يمكن اختراق أجهزة الضحية والقيام بالفعل ألجرمي وبصفة عامة فجهاز الحاسوب ضروري للقيام بالجريمة الإلكترونية ولا يكفي توافر الحاسوب إنما يجب توافر عنصر المعرفة التقنية لاستخدامه واختفاء أحد هذين العنصرين ينبغي على المتهم قيامه بالفعل غير المشروع، إذ لا يتصور قيام أحد الأميين[1] باختراق أجهزة وأنظمة معلوماتية فائقة الدقة والصعوبة من حيث الحماية فالذكاء عنصر مفترض في المجرم الإلكتروني.

* **صعوبة اكتشافها وإثباتها:**

وسبب ذلك أنه من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها، حيث أن هذه الجريمة لا تترك أثرا ماديا لها بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، حيث أن معظم الجرائم الإلكترونية تم اكتشافها بعد ارتكابها بمدة زمنية طويلة، ولا يهتم في الغالب الإبلاغ

[1] **الأمي:** في الدول المتقدمة من ليست له معرفة في تشغيل والعمل على جهاز الكمبيوتر.

عنها، إما لعدم اكتشاف الضحية لها وإما خشية من التشهير خاصة في حالة ما إذا كانت الضحية بنكا يتعامل بالتقنية الإلكترونية وذلك حفاظا على مصالحه.

*** من حيث الجناة والمجني عليهم:**

وفي هذا العنصر الذي سبق لنا وتطرقنا إليه فإن الجريمة الإلكترونية تتميز عن غيرها من الجرائم التقليدية في صفة الجاني إذ أنه مجرم غير عادي يمتاز بصفات الذكاء والفطنة وهو مجرم لا يعتمد على العنف في قيامه بأفعاله، أما من حيث المجني عليهم فأبرز ما يميز هذه الجريمة هو صعوبة اكتشاف ومعرفة المجني عليهم وتحديد نطاق ضحايا هذا الإجرام، إذ أن الضحية قد لا يكتشف أنه تعرض لفعل غير مشروع إلا بعد مدة طويلة تندثر معها الأدلة والمعطيات ضد فاعلها وبالتالي يفر من العقاب.

المبحث الرابع: أركان الجريمة الإلكترونية في ظل التشريع الوطني:

إن التطور الذي حصل جراء التطور التكنولوجي كان له الأثر الكبير في ظهور نماذج جديدة من الإجرام، وبعيدا عن الصور التقليدية المرتكبة بالوسائل الإلكترونية كالسرقة والاحتيال وغسيل الأموال، نجد أن التكنولوجيا أوجدت وأفرزت العديد من الصور المستحدثة للأفعال التي تضر بمصالح المجتمع مما استدعى تجريمها ووضع حد لها في قانون العقوبات الوطني الخاص بكل دولة.

مثله مثل مشرعي الدول الأخرى فإن المشرع الجزائري سارع إلى احتواء هذا التطور التكنولوجي بالتشريع الجنائي وأحاط الجريمة الإلكترونية بإطار قانوني أورد فيه الصور المستحدثة لهذا النوع من الإجرام ووضع له الجزاءات المناسبة له في قانون العقوبات في الفصل الثالث من الباب الثاني من الكتاب الثالث بالقسم السابع مكرر تحت عنوان "جزاء المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر7.

والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو الجرائم الإلكترونية وإن كانت تختلف في صورها وأركانها وعقوباتها إلا أن ما يجمعها أنها تحقق حماية جزائية تنظم المعالجة الآلية للبيانات، أي أن القاسم المشترك بينها هو نظام المعالجة الآلية للمعطيات، ولذلك فإن دراسة تلك الجرائم تقتضي منا أولا تعريف نظام المعالجة للمعطيات.

مطلب أول: مفهوم نظام المعالجة الآلية للمعطيات –الركن المفترض–

هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل واحدة منها في: الذاكرة، البرامج، المعطيات، أجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة، وهي المعالجة للمعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية[1].

هذا التعريف مستمد من الفقه الفرنسي، إذ يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية وشرط أساسي يجب تحققه حتى يمكن القول بقيام إحدى صور أو أركان جريمة جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط لا يكون هناك مجال أمام جريمة من الجرائم محل هذا البحث كالاعتداء على عنصر بمفرده لا يشكل جزءا في هذا النظام، أو إذا وقع الاعتداء على برامج معروضة للبيع أو على جهاز لم يدخل الخدمة أو على عنصر مودع بالمخازن أو على قطع الغيار أو الأجهزة التي مازالت في حالة تجربة أو حتى الأنظمة التي خرجت من الخدمة تماما، لكن على العكس من ذلك تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات عمله أو على عنصر يشكل جزءا من أنظمة متعددة متصلة فيما بينها، أو حتى في حالة ما إذا كان الدخول للنظام مشروعا لكن إلى حد معين إذ يعتبر تجاوز تلك الحدود اعتداءا على نظام المعالجة الآلية للمعطيات.

- يستخلص من هذا التعريف أن نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

[1] فشار عطاالله: مواجهة البرمجية المعلوماتية في التشريع الجزائري، بحث مقدم بالملتقى المغربي حول القانون والمعلوماتية بجامعة زيان عاشور بالجلفة.

1- أنه مركب يتكون من عناصر مادية ومعنوية مختلفة ترتبط فيما بينها لتحقيق هدف معين.

2- ضرورة خضوع النظام لحماية فنية.

أما أنه مركب يتكون من عدة عناصر مادية ومعنوية فقد سبق الإشارة إليه من خلال تعريفنا للحاسب الآلي في حين وجب التعرض للعنصر الثاني ألا وهو خضوع النظام لحماية فنية.

*** ضرورة خضوع النظام لحماية فنية:**

وهي تلك الإجراءات والتدابير التي تحول دون تعرض النظام لخطر الاعتداء عليه حماية للمعلومات التي تحتويها، وعدم خضوع النظام لحماية فنية ينفي صفة الجريمة عن أي فعل قد يمس به لأنه من المفترض والمسلم به أن هذا النظام ليس حكرا على أحد.

وبالتالي فتطبيق الحماية على نظام المعالجة الآلية للمعطيات "والمتمثل في التشفير والذي هو أفضل وسيلة للحفاظ على أمن وسلامة وسرية البيانات المخزنة على النظام" يجعل من كل فعل يستهدف الاعتداء على النظام فعلا غير مشروع وبالتالي يرتب عليه عقوبات جزائية.

لكن كل ما قيل إلى حد الآن يبقى كلاما فقهيا ومنطقيا إذ لا يمكن معاقبة شخص على فعل يعد مباحا، فهو لم يعتد على نظام لا يخضع للحماية الفنية، غير أنه وبالرجوع إلى نصوص قانون العقوبات نجد أن المشرع لم ينص صراحة على وجود هذا الشرط لقيام المسؤولية الجنائية على الفعل المرتكب ظنا منا أنه استبعد هذا الشرط لخضوع غالبية أنظمة المعالجة الآلية للمعطيات لحماية فنية.

*** الأركان الأساسية:**

المطلب الثاني : الركن الشرعي:

الركن الشرعي للجريمة هو النص القانوني الذي يبين الفعل المكون للجريمة ويحدد العقاب الذي يفرضه على مرتكبيها، وذلك استنادا إلى أن العمل الضار بالمصالح الاجتماعية لا يعتبر جريمة إلا إذا وجد في قانون العقوبات نصا يتطابق معه ويعطيه صفة عدم المشروعية[1]، وعلى هذا المعنى استدرك المشرع الجزائري الفراغ القانوني الحاصل في إطار الجزائر الإلكتروني من خلال التعديل الأخير لقانون العقوبات الذي تمم الفصل الثالث

[1] عبد الله سليمان: شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، ابن عكنون، الجزائر، ص 68.

من الباب الثاني من الكتاب الثالث من الأمر رقم 56/66 بقسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى غاية المادة 394 مكرر 7.

المطلب الثالث :الركن المادي:

"تتخذ جرائم المساس بأنظمة المعالجة الآلية للمعطيات عدة صور وأشكال حسب طريقة وهدف الاعتداء على النظام".

يتكون الركن المادي لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في أغلب صوره من عناصر ثلاث وهي السلوك أو الفعل المجرم والنتيجة وهي التغير في العالم الخارجي أو العالم الافتراضي والعلاقة السببية التي تربط بين السلوك والنتيجة، ففي صورة نشر المعطيات وإفشائها المنصوص عليها 394 مكرر 1 فقرة 1 يتمثل الركن المادي في سلوك الجاني أو نشاطه في نشر هذه المعطيات وإفشائها، أما النتيجة فهي رفع صفة السرية على

هذه البيانات بعدما كانت حكرا على صاحبها فقط، وعلاقة سببية إذا ثبت أن هناك علاقة بين الفعل الذي أتاه الجاني والنتيجة المحققة.

غير أن الركن المادي في جريمة المعالجة الآلية للمعطيات لا يتوافر على هذه العناصر دائما في جميع الصور، فقد اكتفى المشرع الجزائري بالسلوك وحده للقيام بقيام الركن المادي للجريمة دون اشتراطه أن تتحقق النتيجة، وصورة ذلك جريمة الدخول والبقاء في منظومة معلوماتية، إذ لا يترتب على هذه الصور عادة تحقق نتيجة جرمية أو تغيير في العالم الخارجي، وفي التالي بيان لجميع الصور التي تقوم من خلالها جريمة المعالجة الآلية للمعطيات حسب ما نص عليها المشرع الجزائري في قانون العقوبات في المواد من 394 مكرر إلى 394 مكرر 7.

1-جرائم الاعتداء على المنظومة المعلوماتية:

أ- جريمة الدخول الغير المشروع إلى المنظومة المعلوماتية:

تنص المادة 394 مكرر على: "يعاقب بالحبس من 3 أشهر إلى 1 سنة وبغرامة من 30 ألف إلى 200 ألف دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك".

يتخذ الركن المادي في هذه الصورة محل الدخول أو البقاء في منظومة معلوماتية أو محاولة القيام بهذه الأفعال وارتكابها عن طريق الغش.

* **فعل الدخول:** هو عبارة عن نشاط إيجابي من جانب الجاني يتمثل في الدخول إلى نظام المعالجة الآلية للمعطيات كله أو جزء منه، ويكون الاتصال بطريق الغش متى كان الجاني لا يحق له الدخول لأي سبب من الأسباب، وهو تعبير يتسع لاستعمال كل الوسائل المتاحة للدخول إلى النظام، ولكن الضابط والمعيار في ذلك هو انعدام حقه في الدخول بهذا النظام المعلوماتي كله أو جزء منه[1]، كما أن المشرع الجزائري لم يحدد طريقة معينة للدخول أو حصر الطرق التي يتم الدخول بها إلى المنظومة المعلوماتية والتي تعتبر مجرمة إنما فعل الدخول على إطلاقه وجعل الفيصل بين الدخول المشروع والغير مشروع إلى نظام المعالجة الآلية للمعطيات هو الدخول عن طريق الغش.

ويعتبر فعل الدخول إلى نظام المعالجة الآلية للمعطيات صورة بسيطة وذلك لعدم اتصالها بصورة مشددة وذلك في حال ما نتج عن الدخول غير المشروع إما محو أو تغيير للمعطيات الموجودة في النظام كذلك فهي تعتبر جريمة شكلية بمجرد تحقق السلوك الإجرامي فيها إذ لا يلزم لهذه الجريمة نتيجة ما.

ب- فعل البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

يلاحظ في نص المادة 394 مكرر1 بجرم فعل الدخول وكذلك البقاء في المنظومة المعلوماتية بطريق غير مشروع، ويمكننا إيعاز ذلك إلى سبب بسيط يبرر هذه التطرقة هو

[1] خالد عياد الحلبي: مرجع سابق، ص 96.

أنه وإن كان فعل الدخول عن طريق الخطأ ينتفي معه الجرم فإن البقاء عن قصد يشكل جرما قائما بذاته يتم عن إرادة الجاني في الإضرار بالغير[1].

إذ أن فعل البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، ويمكن التفريط في حالة البقاء داخل منظومة معلوماتية بطريق غير مشروع في حالتين:

* حالة اجتماع البقاء غير المشروع بالدخول غير المشروع: كقيام الجاني بالدخول عن طريق الغش لمنظومة معلوماتية قاصدا بذلك الاستفادة من المعلومات الموجودة بهذه المنظومة ثم يبقى فيها لكي يتصفح ما فيها من بيانات وقد ينسخ بعضا منها.

* حالة استغلال البقاء غير المشروع عن الدخول غير المشروع لمنظومة معالجة آلية للمعطيات: نجد هذه الحالة مثلا إذا كان النظام مسموحا في وقت معين وممنوعا في وقت آخر إذ يدخل الجاني في وقت مسموح ويبقى لحين الوقت غير المسموح به دخول النظام، وكذا في حالة الدخول خطأ أو في حالة تجاوز المسموح إذ أن يكون له الحق في التصفح فيقوم بنسخ البيانات.

*** الشروع في فعل الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات:**

[1] زيبحة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، ص 50،51.

واضح من نص المادة 394 مكرر1 السالف الذكر أن المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المشروعين في النظام المعلوماتي بل تجاوز ذلك إلى تجريم مجرد المحاولة وذلك حسب العبارة الواردة في نص المادة "أو ب ود ذلك" غير أن ما يمكن إثارته هنا وهو من الصعوبة بمكان وهو ما يتعلق بفكرة الإثبات وما من شأنه إعطاء تصور يفيد بأن هناك شروع أو محاولة طالما أن الجريمة في حد ذاتها تطرح إشكالا في الإثبات[1].

جـ- جريمة تخريب نظام المعالجة الآلية للمعطيات: وهي صورة مشددة لجرائم الاعتداء على المنظومة المعلوماتية حيث أن المشرع الجزائري نص على هذه الجريمة بموجب الفقرة الثالثة من نص المادة 394 مكرر حيث نصت على أنه "... وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 06 أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج"، والتخريب يأتي بمعنى الإتلاف وهو تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية والمشرع الجزائري اشترط أن يكون هذا التخريب ناجما عن الأفعال البسيطة السابقة له وهي الدخول أو البقاء غير المشروع عن طريق الغش، إذا يفهم من نص المادة 394 مكرر أن جريمة تخريب نظام اشتغال منظومة معلوماتية لا يتصور إلا بعد قيام فعل الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات والقيام بأفعال الحذف أو التغيير للمعطيات الموجودة بداخله، وبالتالي فإن جريمة التخريب هي فعل ناجم أو نتيجة إجرامية لجريمة الدخول والبقاء غير المشروع في كل أو جزء من المنظومة المعلوماتية وما يترتب على هذه الأفعال من حذف وتغيير لمعطياتها.

---

[1]زيبحة زيدان :مرجع سابق ،ص51.

2-جرائم الاعتداء على المعطيات التابعة للمنظومة المعلوماتية:

لقد بادر المشرع الجزائري ومن خلال نص المادة 394 مكرر 1 إلى إعطاء مفهوم واسع لفكرة الحماية الجنائية لنظام المعالجة الآلية للمعطيات وذلك بتجريم أفعال من شأنها الإخلال بعمل هذا النظام بطرق تدليسية غير تلك الصور البسيطة، وهي الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، معتبرا أن أي مساس بالمعطيات الموجودة بالنظام بطريق الغش فعلا معاقبا عليه قانونا، وقد جاء نص المادة 394 مكرر 1 بثلاث صور يعد ارتكابها من قبيل جرائم المعالجة الآلية للمعطيات "يعاقب بالحبس من 06 أشهر إلى 03 سنوات وبغرامة من 50000 إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

***صور الاعتداء على المعطيات التابعة للمنظومة المعلوماتية:**

أ- إدخال بيانات ومعطيات في منظومة معلوماتية:

جريمة إدخال بيانات أو معطيات في حاسب آلي تتمثل في إضافة أو إدراج معلومات على نظام للمعالجة الآلية للمعطيات سواء أكان خاليا أو توجد به معلومات وذلك عن طريق تعليمات بلغة ما يوجهها الجاني إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة.

مما يلاحظ من نص المادة 394 مكرر 1 أن قانون المشرع الجزائري لم يشترط شكلا معينا للبيانات المدخلة سواء أكانت معلومات وهمية أو مزورة أو عبارة عن برامج أو غيرها

إلا أنه اشترط لقيام هذه الجريمة أن يتم الإدخال لهذه المعطيات عن طريق الغش وتختلف خطورة هذا الفعل من جان لآخر، وكل حسب أهدافه من هذا الفعل، فقد يهدف أحد الجناة إلى إدخال معطيات لم تكن موجودة في سجل جامعة ما ويضع لنفسه ملفا ليصبح طالبا بالجامعة المعتدى على منظومتها المعلوماتية، وقد يتعدى الأمر ذلك إذ يمكن أن يقوم الجاني بإدخال برامج على المنظومة المعتدى عليها ويمهد بذلك لأعمال تتعدى فعل الإدخال كسرقة البيانات أو التغيير في المنظومة المعلوماتية أو حتى تدميرها كليا.

ب- جريمة تعديل معطيات المنظومة المعلوماتية:

جريمة تعديل معطيات منظومة معلوماتية تتمثل في المساس بالمعطيات والمعلومات المخزنة في ذاكرة المنظومة المعلوماتية وتغييرها بما يتوافق وأهداف الجاني، ويتم ذلك سواء بمحو المعلومات القديمة واستبدالها بالمدخلة وهذا ما يعد تعديلا كليا أو التعديل الجزئي الذي يتم وفق ما يخدم هدف الجاني ذلك بالتعديل في أجزاء من المعطيات فقط، كأن يقوم الجاني بالولوج إلى المنظومة المعلوماتية للجامعة والتعديل في أجزاء من ملفه أو نقاطه قصد الصعود بها، أو أن يقوم بتعديل كلي لملفه مثلا كأن يقوم استبدال ملفه الجامعي كليا بملف آخر معدل بما يتوافق مع أهدافه، ومن المعلوم أو البديهي أن هذا الفعل لا يتم إلا بعد قيام صورة الدخول غير المشروع لنظام معالجة آلية للمعطيات.

جـ- جريمة إزالة معطيات المنظومة المعلوماتية:

يقصد بجريمة إزالة المنظومة المعلوماتية محو جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[1].

3-جرائم الاعتداء على المعطيات خارج المنظومة المعلوماتية:

لقد قسم المشرع الجزائري جرائم المعالجة الآلية للمعطيات إلى ثلاث مراحل بحسب خطورتها، ويمكن اعتبار المرحلة الثانية والثالثة أخطر المراحل إذ أنها تنصب على إخراج البيانات ولقد جرمت المادة 394 مكرر2 عدة أفعال تمس بسلامة البيانات المعتدى عليها والتي نوردها في الآتي:

أ- تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في المعطيات المستعملة في نظام المعالجة الآلية للمعطيات:

إن المشرع الجزائري وفي محاولة له محاربة الجريمة الإلكترونية قام بتجريم أفعال الدخول والبقاء وتخريب وحتى تدمير منظومة معلوماتية قاصدا من وراء ذلك حماية المعلومة أو البيانات في حد ذاتها الموجودة في هذا النظام ويظهر ذلك جليا في نص المادة 394 مكرر2 بتشديد العقاب على الأفعال التي تهدف إلى استغلال المعلومات المتحصل عليها

[1]مزياني عبد الغاني: مداخلة بعنوان: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، محكمة المسيلة.

من عملية السطو[1]، ونستخلص من نص المادة هذه الأفعال في استخدام المعلومات في عمليات تصميم أو بحث أو القيام بتجميع لهذه البيانات أو توفيرها أو نشرها بأي وسيلة أو الاتجار فيها، والملاحظ أن المشرع الجزائري يستهدف حماية المعطيات في حد ذاتها كما ذكرنا، لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات، وأن يكون قد تم معالجتها آليا فمحل الجريمة هو المعطيات سواء كانت مخزنة على أشرطة أو أقراص مثلا أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون المشرع الجزائري[2].

ب- حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات:

يتحقق الركن المادي بجريمة المساس بأنظمة المعالجة الآلية للمعطيات من خلال نص المادة 394 مكرر2 في فقرتها الثانية القيام بفعل مادي لإحدى الصور المنصوص عليها في الفقرة وهو حيازة البيانات المتأتية من نظام المعلوماتية بغض النظر عن الوسيلة التي بموجبها آلت إليه هذه الحيازة وأن يكون إفشاء المعلومة لشخص أو الغير الذي ليس له الحق في الإطلاع عليها أما إذا كان الإفشاء لشخص معني له الحق في الإطلاع عليها فإن الجريمة تنفى ويضاف إلى ذلك أن يكون النشر أو الإفشاء بدون إذن المجني عليه أو

[1]وكيل الجمهورية طويجني كمال الدين: محاضرة بعنوان الجريمة المعلوماتية في التشريع الجزائري، ملقاة في الملتقى الثاني للقطب الجزائي المتخصص بسيدي أمحمد، في 03-05-2011.
[2]فشار عطا الله: مواجهة الجريمة في التشريع الجزائري،

رضائه[1]، وكذا استعمال هذه البيانات المتحصل عليها من الجريمة بأي وجه كان وذلك بتوظيف هذه البيانات واستخدامها بما يتوافق وأهداف الجاني على أن تكون هذه الأفعال مرتكبة عن طريق الغش وأن تكون عمدية.

المطلب الرابع : الركن المعنوي:

[1] زيبحة زيدان: مرجع سابق، ص 65.

يختلف الركن المعنوي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات من صورة لأخرى وبشكل عام يمكن القول بتوافر القصد الجنائي العام متى يتحقق العنصر المادي في الجريمة الإلكترونية، إذ أنه يستخلص من موقف المشرع الجزائري أن القصد الجنائي يثبت بمجرد قيام الجاني بإحدى الصور المجرمة في الفصل السابع مكرر من قانون العقوبات الجزائري ويستنتج من ذلك قيام عنصر العلم والإرادة لدى الجاني إذ أن هذه الجريمة عمدية، وفي أغلب الصور المنصوص عليها في هذا الفصل فإن الجاني يقوم بفعله متعمدا ولا يتصور في فعله الخطأ أو حسن النية، كالبقاء غير المشروع أو حيازة أو استعمال أو الاتجار في المعطيات أو إفشائها أو تلك الصور التي تعرض نظام المعالجة الآلية للمعطيات للخطر، وهذا ما أكد عليه المشرع في قوله "كل من يقوم عمدا وعن طريق الغش"، غير أنه يمكن للجاني الدفع بالخطأ أو حسن النية في بعض الحالات كالدخول غير المشروع، إذ أن هناك أنظمة يسمح بدخولها لوقت محدود ولم يكن له علم أنه دخل في وقت غير مسموح له الدخول فيه وكذا يمكن له الدفع بإنفاذ الإرادة وذلك في حال الإكراه.

الفصل الثاني: أدلة إثبات الجريمة الإلكترونية وتقديرها في إطار نظرية الإثبات الجنائي:

الفصل الثاني: أدلة إثبات الجريمة الإلكترونية وتقديرها في إطار نظرية الإثبات الجنائي:

المعلوم أن الجريمة بشكل عام يمكن وصفها بأنها حرب بين الجاني الذي يحاول طمس معالمها ومنع ما يتخلف عنها واتخاذ الاحتياطات اللازمة لحدوث ذلك، وتدمير ما يتخلف عنها في حالة تخلف آثار يمكن من خلالها الاستدلال عليه، فيلبس قفازات تمنع أن تخلف بصمات أصابعه، أولا ينتعل حذاء مميزا يمكن من خلاله الوصول إليه... إلخ، وهو فوق كل ذلك يسعى إلى أن يرتكب فعلته في الخفاء وهذا هو الأصل، والجهة الأخرى من هذه الحرب هي أجهزة العدالة الجنائية التي تحاول وبكل ما تسير لها من وسائل وما هو مسموح لها قانونا الكشف عن الجرائم ومرتكبيها، وتقديم الأدلة التي تؤكد نسبة الجريمة إلى شخص معين، فهي حرب غاية أجهزة العدالة فيها كشف الحقيقة بالوسائل والسبل القانونية، وغاية الجاني طمس معالمها وآثارها وعدم الاهتداء إليه، فإذا كانت هذه هي الصورة في نطاق الجرائم بشكل عام، والجرائم الإلكترونية منها طبعا، فإن الجرائم الأخيرة أشد اشتعالا وإشعارا بين الجاني وأجهزة العدالة، يساعد على ذلك طبيعة الجريمة الإلكترونية، الأمر الذي يقودنا إلى القول بأنه إذا كانت الجرائم الإلكترونية هي أصلا خافية المعالم على أجهزة العدالة لجميع طوائفها واختصاصاتها، فإن الأخيرة منها ستواجه صعوبة ليس في اكتشافها فحسب بل وفي إثباتها من أو لا، كل هذا والعديد من الصعوبات والأسباب الأخرى التي خلفتها

الجريمة الإلكترونية أدت إلى ميلاد علم جديد في البحث الجنائي هو علم البحث الجنائي الرقمي الذي يهتم بالآثار الرقمية الجنائية التي يتركها المتهم إذا ما استخدم الكمبيوتر أو الشبكة العالمية للمعلومات، فهو علم يبحث في مسرح الجريمة الرقمي وهو يهدف إلى كيفية استخلاص دليل رقمي يمكن استخدامه في الإثبات ونسب الفعل لفاعله أمام جهات العدالة.

وللإثبات في الجرائم الإلكترونية طبيعة خاص على ضوئها سنقسم الفصل الثاني إلى أربع مباحث نتناول فيها معنى الإثبات وبعض القواعد التي تحكمه ثم نطرح على صور الدليل الإلكتروني التي يمكن استخلاصها من الأدلة التقليدية للإثبات وبعدها الدليل الإلكتروني المتحصل عليه من الوسائل الحديثة للإثبات وتقديرها.

المبحث الأول: ضوء على الإثبات الجنائي:

إن الإثبات الجنائي لا ينشأ إلا بصدد الدعوى العمومية الجنائية التي يقصد بها المطالبة بالحق للقصاص من المجرم عن طريق محاكمته أمام جهات القضاء، هذا وترتبط الجريمة بوجود المجتمع الذي لا يعيبه أن تقع الجريمة بين ثناياه وإنما وقوعها ونسبتها إلى فاعلها، وتعد نظرية الإثبات الجنائي من بين الموضوعات الهامة في مجال العلوم الجنائية لا سيما بعد تقدم فنون الإجرام وارتكاب الجرائم وتزايد قدرة المجرمين على إخفاء معالمها، الأمر الذي

يجعل القضاء في كثير من الأحيان يردد بانتفاء الدعوى العمومية لعدم معرفة الفاعل مما يترتب عليه إهدار الآثار الموجودة من سياسة التجريم وإفلات الجناة من العقاب[1].

المطلب الأول: مفهوم الإثبات الجنائي:

- تعريف الإثبات :

- في الاصطلاح اللغوي: الإثبات من فعل ثبت ثباتا وثبوتا أي استقر ودام، والإثبات بصفة عامة هو تأكيد وجود أو صحة أمر معين بأي دليل أو برهان[2]، أو أنه تأكيد وجود الحق بالبينة.

- في الاصطلاح القانوني: إقامة الدليل أمام سلطة مختصة على حقيقة واقعة وبالطرق التي حددها القانون ووفقا للقواعد التي تخضع لها[3].

- أهمية الإثبات الجنائي:

تكتسي قواعد الإثبات أهمية بالغة، إذ من شأنها أن تشكل حماية قانونية للحق في حد ذاته في حال النزاع، حيث يتوقف على إثبات وجود أو انتفاء الواقعة التي يقيمها القانون سببا

[1] الدكتور الطيب بلواضح: محاضرات ألقيت على طلبة سنة أولى ماستر قانون جنائي بجامعة المسيلة سنة 2012.
[2] محاضرات ألقيت على طلبة سنة أولى حقوق ماستر قانون أعمال بجامعة المسيلة 2012.
[3] الدكتور الطيب بلواضح: مرجع سابق.

في لإنشاء الحق أو انتفاءه ذلك أن الحق إذا جرد من دليله يصبح عند المنازعة فيه والعدم سواء بالرغم من أن الإثبات ليس عنصر من عناصر الحق[1].

تكمن أهمية الإثبات أيضا من خلال تحقيقه للعدالة الجنائية ذلك بالكشف عن الحقيقة التي تهم المجتمع باعتبار أن الجريمة أولا وأخيرا تمثل الاعتداء على الجماعة[2].

المطلب الثاني: القواعد العامة التي تحكم الإثبات الجنائي:

أهم ما يميز نظرية الإثبات مجموعة من القواعد وهي:

*** حرية الإثبات:**

فالحق كامل لإقامة الدليل بأي طريقة كانت ولا تكون هذه الجريمة كاملة إلا إذا أعطي للقضاء حرية في تقدير الأدلة، إذ يجوز إثبات الجرائم بأي طريق من طرق الإثبات ويتطلب تطبيق قاعدة حرية الإثبات الجنائي اللجوء إلى إعمال أي قاعدة كالاعتراف و الشهادة والخبرة وهذه القاعدة تنصب على أدلة الإثبات كما أنها تنصب على أدلة النفي وهذا للحفاظ على حقوق وحريات الأفراد، على أن يخضع هذا الدليل لجملة من الشروط كوجوده ضمن ملف الدعوة وأن يكون مشروعا وأن يستخرج هذا الدليل بطرق مشروعة.

[1] محاضرات طلبة ماستر قانون أعمال، مرجع سابق.
[2] الطيب بلواضح: مرجع سابق.

*** يقينية الدليل:**

اليقين هو حالة ذهنية عقلية تثبت وجود الحقيقة ويتم الوصول إلى ذلك عن طريق ما يستنتجه العقل بوسائل الإدراك المختلفة.

وتتلخص قاعدة يقينية الدليل في بلوغ القاضي ما عرض عليه من أدلة راضي درجة يقين بحقيقة الواقعة المعروضة عليه، والحقيقة أن عدم قدرة أدلة الإدانة على إحداث القطع واليقين يترتب عليه استمرار حالة البراءة وبالتالي انتفاء حالة الإدانة وتطبيق مبدأ البراءة المفترضة.

*** حرية الاقتناع:**

هي حالة عقلانية وجدانية تستنتج من الوقائع المعروضة من القضية عناصر ذات درجة عالية من التأكيد الذي نصل إليه باستبعاد الشك بطريقة قاطعة، وحرية الاقتناع يخاطب بها من توافرت فيه صفة قاضي، ولقاضي الحكم أن يوسع في أي دليل أو يتخذ أي إجراء يصل به لكشف الحقيقة، ذلك ما يشكل للقاضي صورة عن كل طرف من أطراف الدعوى ويبدأ بالموازنة بين أدلة الإثبات والنفي وتكون في الأخير الغلبة للدليل الذي وصل لديه لدرجة قناعته[1].

[1] الطيب بلواضح: مرجع سابق.

المطلب الثاني: أثر الطبيعة الخاصة للجرائم الإلكترونية على إمكانية إثباتها:

نعرض في هذا المبحث الصعوبات العملية التي تواجهها جهات التحقيق في الكشف عن الجرائم الإلكترونية ومرتكبيها ونسبة الأفعال الجرمية لأصحابها وهي صعوبات تتصل بالطبيعة التقنية للوسيط الإلكتروني.

يصعب إقامة الدليل على الجرائم التي تقع على العمليات الإلكترونية المختلفة وذلك بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة، وبخاصة لأن محل تلك الجرائم هو جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإثبات الجرائم المعنوية قد لا تترك وراءها آثار تدل عليها على أساس أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي تتم من خلالها العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسيب التي تحفظها.

المعلوم أن جهات التحري والتحقيق اعتادت الاعتماد في جمع الأدلة على الوسائل التقليدية للإثبات الجنائي، وهي التي تعتمد على الإثبات المادي للجرائم ولكنه في محيط الإلكترونيات فالأمر يختلف، فالمحقق لا يستطيع تطبيق إجراءات الإثبات التقليدية على المعطيات المعنوية بصورة متطابقة.

بالإضافة إلى هذا وذاك فإن الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به، والذي يتميز بالطبيعة الفنية ولذلك فلهم القدرة على إخفاء معالم الأفعال غير المشروعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الإلكترونية ويستخدمون في سبيل ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسوب أو يعدلون برنامجه أو يحرفون البيانات المخزنة بداخله دون أن يخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل.

ومما يزيد من خطورة الأمر إمكانية إخفاء الأدلة المتحصل عليها من الوسائل الإلكترونية أو تدميرها في زمن قصير، ناهيك عن ارتكاب الجريمة يتم عادة من مسافات بعيدة باستخدام وحدات طرفية، وتتعقد المشكلة إذا ما تعلق الأمر بمعلومات أو بيانات تم تخزينها في دولة أخرى بواسطة شبكة اتصال عن بعد وتظهر بذلك قصور القواعد التقليدية في الإثبات إذ أنها لا تكفي لضبط مثل هذه المعلومات بحثا عن الأدلة وتحقيقها، كما أنه من الصعب إجراء التفتيش بالمفهوم العادي التقليدي للحصول على الأدلة ضمن إقليم دولة أجنبية[1].

كما أن بعض التهديدات التقنية ظهرت، وارتبطت بالتكنولوجيا اللاسلكية، واللاسلكي أحد أنواع التكنولوجيا التي لا تميز بين الأشخاص الذين يستخدمونها كما أن الأجهزة الرقمية المحمولة لا يقتصر عملها على مكان واحد، بل تعمل في أثناء حركتها عبر المساحة التي

[1] عادل عزام سقف الحيط: مرجع سابق، ص 224،225.

تغطيها إشارة اللاسلكي، مما يساعد في اتساع مسرح الجريمة وضياع الأدلة، ويشترك في استخدام اللاسلكي أعداد غفيرة من الناس وهو وسيط ناقل كبير وغير مسيطر عليه، لذلك يتسم استخدامه بالخطر، كما أن سهولة استخدام هذه التكنولوجيا وتدني كلفتها عملت على انتشارها، وأدت إلى استهتار مستخدميها فلا يتخذون أساليب تقييم الجرائم، الأمر الذي تركهم عرضة للمجرمين المعلوماتيين.

المبحث الثاني: صور الدليل الإلكتروني المتحصل عليها من الأدلة التقليدية للإثبات:

فيما سلف ذكرنا أن من مشكلات العملية التي تواجه عملية كشف وإثبات الجريمة الإلكترونية عدم رؤية الدليل الملموس على وقوعها وبالتالي يصعب من الناحية العملية كشف هذه الجرائم ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذا المجال سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها وإخفاء الأدلة المتحصل عليها عقب التنفيذ مباشرة[1]، وتواجه أدلة الإثبات الجنائي بصورتها التقليدية عدة صعوبات في مجال إثبات الجريمة الإلكترونية ذلك باعتمادها بشكل كبير على الماديات في إقامة الدليل، غير أنه يمكن اعتماد هذه الأدلة وإسقاطها بما يتوافق والطابع المعنوي أو الطبيعة الخاصة للجريمة الإلكترونية.

[1] خالد عبد الله القائفي: التحقيق الجنائي الرقمي والمعروف أيضا باسم العلوم الجنائية للأجهزة الرقمية وعملية التحقيق والإثبات بالأدلة والبراهين على ارتكاب الجريمة الإلكترونية، منشور يوم 22-12-2010، على الموقع: www.min-maq.com.

المطلب الأول: الأدلة المحصلة من الوسائل الإلكترونية بطريق التفتيش والضبط:

فرع1: الأدلة المحصلة من الوسائل الإلكترونية بطريق التفتيش:

إن الهدف من التفتيش المتصل بجريمة وقعت هو كشف الغموض الذي يحيط بها ومعرفة مرتكبيها، وجمع الأدلة المتعلقة بها مما يوجب إجراء البحث في أماكن لها حرمة خاصة كالحواسيب الشخصية أو علب البريد.

- تعريف التفتيش:

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وإحاطته بضوابط صارمة نظرا لأهميته في كشف الحقائق والأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم.

وكما هو الشأن في مختلف التشريعات العربية خاصة فإن التعريفات تجمع على أن التفتيش "هو إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص أو ذلك بهدف إثبات ارتكابها أو نسبتها للمتهم وفقا لإجراءات قانونية محددة"[1].

[1] أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، ط7، 1993، ص 544.

* شروط التفتيش في منظومة معلوماتية:

1- الشروط الشكلية:

وفقا لأحكام المادة 44 من قانون الإجراءات الجزائية سيما بعد التعديل الذي حصل بموجب القانون 06-22 في 20 سبتمبر 2006 وهي:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.

- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.

- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

- حضور الشخص المعني بالتفتيش أو مسكنه أو حضور من ينوب عنه.

- حالة رفض الحضور يستدعي ضابط الشرطة القضائية من غير الموظفين الخاضعين لسلطته[1].

2- الشروط الموضوعية للتفتيش:

- وقوع جريمة إلكترونية.

- تورط أشخاص أو شخص معين في ارتكاب الجريمة الإلكترونية أو الإشتراك فيها.

[1] زيجة زيدان: مرجع سابق، ص 134.

– توافر إمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات إلكترونية تفيد في كشف الحقيقة لدى المتهم.

– أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به[1].

*** خاصية التفتيش والضبط في الجرائم الإلكترونية:**

نظرا للطبيعة الخاصة للجرائم الإلكترونية وباعتبارها من الجرائم المستحدثة، فقد خصها المشرع الجزائري بإجراءات خاصة من حيث التفتيش والضبط للحصول على أدلة لإثبات الجريمة الإلكترونية تمثلت في نص المادة 47 من قانون الإجراءات الجزائية، والتي تمنح خاصية للتفتيش في هذه الجرائم بقولها: "عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك[2]، يستخلص من هذا النص أن المشرع أطلق حرية أكبر لقاضي التحقيق في عملية الكشف عن الجرائم الإلكترونية وذلك برفع الوقت المحدد والحدود الجغرافية التي كانت تعيقه أثناء قيامه بالتحقيق.

*** نطاق التفتيش في الجرائم الإلكترونية:**

[1] خالد عياد الحلبي: مرجع سابق، ص 153،154.
[2] قانون الإجراءات الجزائية.

المقصود بالتفتيش عن الأدلة الجرمية هنا هو التفتيش عن معطيات الحاسوب غير المادية والمخزنة في الجهاز، أو المخزنة في الأقراص، كما يقصد بالتفتيش البحث في النظم المعلوماتية عبر الشبكات الإلكترونية بحثا عن شيء يتصل بالجريمة الإلكترونية.

إن معطيات الحاسوب غير المادية تخضع للتفتيش لأنها عبارة عن ذبذبات إلكترونية قابلة للتخزين في الجهاز أو التخزين على الأقراص، وأنها مادامت مخزنة على الجهاز الآلي أو الأقراص فهي أشياء مادية محسوسة تخضع للتفتيش ويمكن ضبطها، وإذا كان الأمر يبدوا مقبولا من الناحية النظرية إلا أن ضبط مكونات الحاسوب المعنوية بعد تفتيشها غير ممكنة إلا إذا حولت إلى كيانات مادية عن طريق مخرجات الطباعة المختلفة للحاسوب بكامله كدليل على الجريمة[1].

1- مدى خضوع مكونات الحاسوب المادية للتفتيش:

تحكم الإجراءات القانونية الخاصة بالتفتيش فحص المكونات المادية للحاسوب بحثا عن أي شيء يتصل بجريمة إلكترونية وقعت ويفيد التفتيش في الكشف عن مرتكبيها، ويخضع تفتيش الأجهزة الإلكترونية إلى إحكام التفتيش الخاصة بالجرائم المستحدثة حسب نص المادة 47 ف 3 و4 من قانون الإجراءات الجزائية، إذ يجوز تفتيش كل محل سكني أو غير سكني

[1] خالد عياد الحلبي: مرجع سابق، ص 157،158.

في أي ساعة من ساعات النهار أو الليل على قصد الوصول إلى كل ما يفيد الكشف عن الجرائم الإلكترونية.

2- مدى خضوع مكونات الحاسوب المعنوية للتفتيش:

لقد كان المشرع الجزائري صريحا من خلال نص المادة 47 ف3 إذ أنه أجاز عملية التفتيش لمن له الحق في ذلك إجازة على إطلاقها ولم يحدد المشرع الجزائري كيفية أو نطاق التفتيش في الجرائم الإلكترونية، واعتبر أن أي عمل يقوم به المحقق قصد الكشف عن مستودع السر واستخراج الدليل الذي يؤدي للوصول إلى فاعل الجريمة عملا من أعمال التحقيق، وبذلك فهو لم يفرق بين عملية تفتيش المكونات المادية أو المعنوية للحاسب الآلي، حيث يرى المشرع أن القيمة الإجرائية للتفتيش تكمن في الوصول إلى البيانات دون التسبب في تلفها، ثم قيام المفتش باستنساخ رقمي دقيق لتلك المستمسكات البيانية لتكون حجة على المتهم في مرحلة المحاكمة، لذلك كان من اللازم الإشارة في قانون الإجراءات الجزائية إلى حرية تفتيش المستمسكات المادية أو المعنوية للأجهزة الإلكترونية ذلك للقضاء على أي إشكال قد يعتري عملية التفتيش.

3- مدى خضوع شبكات الحاسوب للتفتيش:

نواجه في هذه الحالة ثلاثة احتمالات وذلك على اختلاف وتنوع الشبكات الحاسوبية:

* الاحتمال الأول: أن تكون الشبكة داخلية، وهذا لا يشكل أي شكل بالنسبة للسلطات التي تقع على عاتقها عملية البحث والتحري وإثبات وقوع الجرائم الإلكترونية، وبذلك فهي تخضع للقواعد الخاصة بالتفتيش المنصوص عليها بالمادة 07 ق إج ف3.

* الاحتمال الثاني: اتصال حاسوب المتهم بحاسوب أو بنهاية طرفية في نفس الدولة، هذه الحالة تأخذ حكم الحالة السابقة لها، إذ أن المشرع أعطى سلطات واسعة لقاضي التحقيق أو الضبطية القضائية، بحيث يمتد اختصاصهم إلى كافة التراب الوطني في حال التحقيق في جريمة مستحدثة.

* الاحتمال الثالث: اتصال حاسوب المتهم بحاسوب أو بنهاية طرفية في مكان خارج الدولة، أقر القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بجواز القيام بتفتيش المنظومة المعلوماتية عن بعد ويقضي ذلك الدخول إليها دون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب والتفتيش فيه، وذلك حسب نص المادة 05 من القانون 09-04 بقولها: "يجوز للسلطة القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد"[1]، وكذا يمكن الاعتماد على آلية الإنابة القضائية خارج الإقليم الوطني والتماشي وسياسة المساعدة القضائية الدولية والتعاون الدولي في مجال محاربة الجريمة الإلكترونية.

[1]القانون 09-04 الصادر في 09/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال.

فرع 2: الأدلة المحصلة من الوسائل الإلكترونية بطريقة الضبط:

الغرض من التفتيش هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت فالضبط في معظم الأحوال هو غرض التفتيش وإن لم يكن هو السبب الوحيد فقد يتم الضبط لأسباب أخرى غير التفتيش من ذلك المعاينة وما يقدمه المتهم أو الشهود ومأموري الضبط القضائية.

تعريف الضبط:

هو التحفظ على الأشياء وحجزها ووضعها في أختام، إذ يجيز القانون لقاضي التحقيق أن يقوم بضبط و حجز الأشياء ووضعها في أحراز مختومة إذا كانت هذه الأشياء والوثائق تنفع في إظهار الحقيقة أو تلك التي يضر إفشاؤها سير التحقيق[1].

* القواعد القانونية لضبط الأشياء :

باستقرار نصوص المواد 47 و84 ق إ ن يمكن ما جاء به المشرع الجزائري في شأن ضبط الأشياء بمناسبة التحقيق في جريمة إلكترونية على النحو التالي:

[1]عبد الله أوهايبية: شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة للطباعة والنشر والتوزيع، 2004، ص 339.

- يجوز لقاضي التحقيق أو لضابط الشرطة المنوب وحدها الحق في الإطلاع على المستندات المتحصل عليها أثناء التحقيق قبل ضبطها.

- لابد من إحصاء وضبط الأشياء والوثائق المطلوبة ووضعها في أحراز مختومة.

- لا يجوز فتح هذه الأحراز والوثائق المطلوبة إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا كما يتم كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء.

- لا يجوز لمن له الحق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة، كما أنه إذا اشتمل الضبط على نقود أو سبائك أو أوراق تجارية أو أوراق ذات قيمة مالية فإنه يصوغ لقاضي التحقيق أن يصرح لكاتب الضبط بإيداعها بالخزينة.

*** مدى صلاحية الجرائم الإلكترونية لأن تضبط أدلتها:**

ويراعى في هذا الصدد التفرقة بين حالتين:

1- الجرائم الواقعة على المكونات المادية للحاسوب:

ليس هناك صعوبة في هذه الحالة إذ يجوز ضبط أدلة الجرائم بموجب القواعد التقليدية المنصوص عليها في قانون الإجراءات الجزائية والسبب في ذلك أن المشرع تناول الضبط وأورده على الأشياء المادية والمعنوية على حد سواء إذ جاء النص على إطلاقه حسب نص المادة 49 ق إج.

2- الجرائم الواقعة عل المكونات غير المادية للحاسب الآلي:

حسب نص المادة 47 ق إج الجديدة فإن الضبط الذي نص عليه المشرع الجزائري والذي أجاز من خلال نص هذه المادة فإنه يمكن أن يقع كما أشرنا على المكونات المادية للحاسوب كما قد يقع الضبط على المكونات المعنوية له، إذ أن النص جاء على إطلاقه ولم يحدد المكونات المادية دون المعنوية، وإذ أن النص جاء خاصا على جريمة مستحدثة خاصة وأن هذه الجريمة تتميز بطابعها المعنوي أكثر منه مادي مثل الجرائم التقليدية.

ويمكن أن يقع الضبط على المكونات المعنوية للحاسوب والمتمثلة في برامج الحاسب الآلي وكذا بياناته على حد سواء والتي يحولها المحقق الإلكتروني من حالتها المعنوية إلى حالة مادية على الشكل الآتي:

- الأوراق: في الجرائم الإلكترونية يقوم الحاسب الآلي وشبكة الإنترنت بحفظ كم هائل من المعلومات والأوراق والملفات، قد يقوم الجاني بطباعتها وذلك لأغراض المراجعة أو المحقق

عند تحويلها من حالتها المعنوية إلى دليل مرئي، والأوراق من الأدلة التي يجب الاهتمام بها عند معاينة مسرح الجريمة وتفتيشه.

– جهاز الحاسب الآلي وملحقاته: للقول بوجود جريمة إلكترونية فإنه يجب القول بجهاز حاسب آلي له علاقته بالجريمة سواء كان أداة أو محلا للجريمة، كما أنه يضبط مع الحاسب الآلي لكل ملحقاته التي قد تعتبر مخزنا وفيرا للمعلومات التي قد تثبت ارتكاب صاحبها للجريمة، والتي تتمثل في وحدات الإدخال، وحدات المعالجة المركزية، وحدات الإخراج، وخاصة وحدات التخزين والبطاقات والمودم وغيرها.

المطلب الثاني: الأدلة المحصلة من الوسائل الإلكترونية بطريق المعاينة والخبرة:

تعتبر الخبرة والمعاينة من بين أهم الإجراءات الهامة ومن أقدر أدلة الإثبات التقليدية على كشف خبايا الجريمة الإلكترونية والتي يمكن من خلالها الحصول على الأدلة اللازمة والضرورية في الجريمة الإلكترونية سواء لإدانة المتهم من خلالها أو لإثبات براءته.

فرع 1: الأدلة المحصلة من الرسائل الإلكترونية بطريقة المعاينة:

تستلزم المعاينة انتقال المحقق إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة وذلك في أسرع وقت ممكن قبل أن تزول آثار الجريمة، بغرض جمع الآثار المتعلقة بها وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة، لكن المعاينة في مظهرها العام كإجراء تقليدي بالنسبة للجرائم الإلكترونية قد تختلف كثيرا عما تكون عليه في الجرائم التقليدية الأخرى.

* مفهوم المعاينة:

- **تعريف المعاينة:** عرف الفقه الجنائي المعاينة على أنها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة"، كذلك عرفت على أنها: إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة.

* أهمية المعاينة في إثبات الجريمة الإلكترونية:

إن إجراء المعاينة وبمفهومه التقليدي بالإطلاع على مسرح الجريمة يكون فقط ذا أهمية متمثلة في تصوير كيفية وقوع الجريمة وظروفها وملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق هذه المعاينة، لكن هذه المعاينة لا تؤدي نفس الدور في كشف غموض الجريمة الإلكترونية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى

مرتكبها[1] ويرجع سبب ذلك إلى الصعوبات العملية التي تواجه عملية الإثبات والتي تطرقنا إليها بالذكر سابقا.

* مدى صلاحية مسرح الجريمة الإلكتروني لمعاينته:

لتقرير هذا الأمر وجب التفرقة في هذا الصدد بين الحالتين الآتيتين:

1- الجرائم الواقعة على المكونات المادية للحاسوب:

مثل جرائم الاعتداء على أشرطة الحاسب وكبلاته وشاشة العرض الخاصة به وغيرها من المكونات المادية، فإن الأمر لا يثير أي إشكال لتقرير بصلاحية مسرح الجريمة الذي يحوي هذه المكونات لمعاينتها، والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها لشخص معين وكذا وضع الأختام في الأماكن التي تمت فيها المعاينة[2].

2- الجرائم الواقعة على المكونات غير المادية للحاسوب أو بواسطتها:

تأتي في مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم بواسطة الإنترنت ومنها كذلك جرائم التزوير المعلوماتي والتخريب الذي يتم بواسطة الفيروسات.

---

[1] عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2002، ص 101.

[2] الدكتور فتوح الشاذلي، تأليف عفيفي كامل عفيفي،جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون،منشورات الحلبي القانونية،2003،ص353.

وتكمن صعوبة استخلاص الدليل بواسطة المعاينة من هذه الجرائم في الشق المعنوي في صعوبتين أساسيتين تتمثلان في:

* الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم الإلكترونية.

* الصعوبة الثانية تكمن في الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة نسبيا، ما بين وقوع الجريمة والكشف عنها الأمر الذي يبحث على إمكانية العبث بمسرح الجريمة وتغيير آثارها أو زوالها[1].

- الإجراءات المتبعة قبل معاينة مسرح الجريمة:

عند تلقي البلاغ حول إحدى جرائم الحاسب الآلي بإحدى الطرق المعروفة حسب قانون الإجراءات الجزائية، يتعين مراعاة الآتي قبل التحرك إلى مسرح الجريمة الإلكتروني:

* ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

* وجود خارطة توضح الموقع الذي سيتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ.

[1] عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية،دار الفكر الجامعي،الاسكندرية، ط1 ،2006، ص 183.

* تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة.

* تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.

* إعداد الفريق المتخصص الذي سيتولى المعاينة مباشرة بعد تلقي البلاغ وذلك لضمان السرعة الكافية لأخذ الأدلة المناسبة وضبط الأدلة وكل الوسائل التي تؤدي إلى إثبات وكشف ملابسات الجريمة.

* تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حده.

* إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على أكمل وجه.

* أن تتم كل هذه العملية والإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الإجرائية.

* تحضير كل الوسائل اللازمة والأجهزة الإلكترونية التي تساعد المحققين على إنجاز المعاينة على أكمل وجه وعدم تضييع الدليل.

- إجراءات معاينة مسرح الجريمة المعلوماتية:

* تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة وسائر ملحقاته والأجهزة الطرفية المتصلة به، مع التركيز بوجه خاص على تصوير الأجهزة الخلفية لحاسب.

* أخذ معلومات الجهاز ونوعه وكافة البرامج المثبتة خلاله.

* عدم نقل أي معلومات من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجالات لقوى مغنطيسية يمكن أن تسبب في محو أو إتلاف البيانات المسجلة.

* التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة وغير السليمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

* التحفظ على مستندات الإدخال ومخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.

* وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.

* فصل التيار الكهربائي لفصل الجاني عن مسرح الجريمة وذلك لعدم تمكينه من تغيير مسرح الجريمة.

* إبعاد الموظفين عن أجهزة الحاسب الآلي وكذلك عن الأماكن التي تتواجد بها أجهزة الحاسوب.

* عدم الاعتماد إلا على فئة معينة من الباحثين والمحققين الذين تتوافد لديهم الكفاءة العلمية والخبرة الفنية في مجال الكمبيوتر والشبكات ونظم المعلومات واسترجاع المعلومات والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية[1].

فرع 2: الأدلة المحصلة من الوسائل الإلكترونية بطريق الخبرة:

يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة وفاعلها باتخاذ العديد من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ولما كان ذلك يحتاج إلى جهد لا يستطيع القيام به بمفرده ويسيرا له لأداء عمله، فإن الأمر يقتضي الاستعانة والاستفادة من أهل الخبرة.

ماهية الخبرة القضائية:

[1] خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 183،184.

الخبرة القضائية هي إجراء للتحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير، تتعلق بواقعة أو وقائع مادية يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علما أو فنا لا يتوافر في الشخص العادي ليقدم له رأيا أو بيانا فنيا لا يستطيع المحقق الوصول إليه وحده[1].

تعرف الخبرة كذلك على أنها استشارة فنية يستعين بها القاضي في مجال إثبات الجرائم ذلك لمساعدته عل تقدير مسائل فنية والتي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لدى القاضي بحكم تكوينه، فالقاضي يتمتع بسلطة تقديرية واسعة في كل ما يستدعي من خبرة وهي خاضعة للرقابة ويجب أن تكون مرتبطة بشرطين[2].

- شروط الخبرة:

* أن تكون المسألة من المسائل الفنية: وذلك فيما يخرج عن اختصاص القاضي القانوني، مثلا كإجراء خبرة لمعرفة كيفية وسبب الوفاة أو في حال الجرائم الإلكترونية إعداد خبرة لمعرفة كيفية وقوع الجريمة كتدمير منظومة معلوماتية، هنا نجد أن للقاضي خبرة قليلة وقد تكون منعدمة في مثل هذه الجرائم وتحتاج لخبير معلوماتي يفقه في المسائل الإلكترونية كالمهندس في الإعلام الآلي.

* عدم قدرة المحكمة على إدراك المسألة: بمعنى أن القاضي الجنائي لا يمكن فهمه للمسألة أو إدراكها خارج عن دائرة المعارف التي يستطيع القاضي فهم الوقائع.

[1] خالد ممدوح إبراهيم: مرجع سابق، ص 283.
[2] الطيب بلواضح: محاضرات سنة أولى ماستر، مرجع سابق.

- **تعريف الخبير:**

هو شخص مختص فنيا في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى خبرة فنية خاصة.

مجالات الاستعانة بالخبرة القضائية في إثبات الجريمة الإلكترونية:

إن الخبير وبصفته وسيلة في يد القضاء الذي يقوم من خلاله بالتحري حول الجرائم وإثباتها لأصحابها أو نفيها عنهم، يعد حلقة قوية في مجال إثبات الجريمة الإلكترونية ذلك للطابع الحديث والجهل الكبير بمعالمها لدى السلطات القضائية، لذا فإن مجال الاستعانة بالخبراء في مجال إثبات الجريمة الإلكترونية واسع جدا ليشمل جميع الجرائم المنصوص عليها في المواد 394 مكرر حتى 394 مكرر7، إذ يقع على عاتق الخبير إثبات هذه الجرائم أو نفيها عن صاحبها، وهناك مجالات عديدة أخرى يمكن فيها أو يجب فيها على القضاء الاستعانة بالخبراء المعلوماتيين لا يمكن حصرها وخاصة ما تعلق فيها بـ:

* تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.

* التلاعب في البيانات.

* التلاعب في البرامج الأساسية أو التطبيقية.

* الغش أثناء نقل أو بث البيانات[1].

ويمكن إجمال المسائل التي يحتاج فيها المحقق إلى خبير معلوماتي كما يلي:

* وصف وتركيب الحاسبات ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها.

* وصف طبيعة الحاسب أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية للمعلومات.

* وصف الوضع المحتمل لوضع الإثبات أو الشكل أو الهيئة التي تكون فيها.

* أثر الاستدلالات والتحقيقات من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام.

* القيام عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يصيبها التلف.

* كيفية تجسيد الأدلة في صورة مادية ينقلها إذ أمكن إلى أوعية ورقية بحيث يتاح للقاضي فهمها[2].

المطلب الثالث: الأدلة المحصلة من الوسائل الإلكترونية بطريقة الشهادة والاستجواب:

[1]علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظر الإثبات الجنائي، منشور على الموقع www.arablawinfo.com، ص 52.
[2]عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية، ص 179،180.

فرع1: الأدلة المتحصل من الوسائل الإلكترونية عن طريق سماع شهادة الشهود:

إن الشهادة هي معلومات يدلي بها الشاهد أمام قاضي التحقيق، تتعلق بالجريمة موضوع التحقيق، ويقصد بسماع الشهادة السماح للغير وهم ليسوا أطرافا في الدعوة العمومية بالإدلاء بما لديهم من معلومات بشأن الوقائع المعروضة على قاضي التحقيق[1].

- **تعريف الشهادة:** الشهادة في الأصل هي إخبار الشخص بما قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه ومن ثم فإن الشهادة هي دليل مباشر في الدعوى، لكن الأمر قد يختلف فيما هو عليه في الجرائم الإلكترونية فالشهادة في الجرائم الإلكترونية هي إخبار الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي بمعلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات تفيد في إثبات وكشف الجرائم الإلكترونية، ويطلق على هذا الشخص اسم الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي.

- **نماذج عن الشهود المعلوماتيين:**

مشغلوا الحاسب الآلي: هم الأشخاص المسؤولون عن تشغيل الجهاز والمعدات المتصلة به ولابد أن تكون لديهم خبرة كبيرة في استخدام الحاسب الآلي ومكوناته.

مخططوا البرامج: هم الأشخاص المختصون في كتابة أوامر البرامج.

[1] عبد الله أوهايبية: مرجع سابق، ص 344.

المحللون: هم الذين يحللون الخطوات ويقومون بجمع البيانات الخاصة بنظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات.

مهندسوا الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وشبكاته.

مديروا النظام: هم الذين توكل لهم الإدارة في النظم المعلوماتية[1].

- أهمية الشهادة في إثبات الجرائم الإلكترونية:

تختلف الشهادة فيما هي عليه في الجرائم التقليدية: إذ أنها أقل قوة ثبوتية في الجرائم الإلكترونية وذلك لطبيعة هذا النوع من الإجرام إذ أنها جريمة غير مرئية كما أنها لا تخلف أدلة وكذلك فهي تحدث في الخفاء أو قد يقوم بها الجاني من بعد مكاني آخر.

لكن ومن جهة أخرى تعتبر الشهادة مهمة ودليل يمكن الاعتماد عليه على أنه يخضع لتقدير القاضي، ذلك من خلال أن الشاهد فيها شخص مميز ويختلف عن شهود الجرائم التقليدية، فهو يملك كل صفات المجرم المعلوماتي من تعلم وذكاء وقدرة على السيطرة على جهاز الحاسوب ويختلف عنه فقط كونه ليس مجرما إنما يساعد على إثبات ما قام به الجاني.

[1] عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية مرجع سابق، ص 340.

تبقى شهادة الشاهد المعلوماتي كغيرها من أدلة الإثبات الأخرى تخضع بدورها لسلطة القاضي التقديرية.

فرع 2: الأدلة المحصلة من الوسائل الإلكترونية بطريق الإستجواب:

يعتبر الاستجواب من أهم إجراءات التحقيق المستخدمة في كشف الحقيقة، حيث يمكن الاستجواب السلطة المناط بها التحقيق من طرح الأسئلة الدقيقة والولوج في موضوع الدعوى والتعرف على أنها التفاصيل يتعلق بالجريمة.

- المقصود بالاستجواب:

يعرف الاستجواب على أنه إجراء من إجراءات التحقيق تتم فيه مناقشة المتهم فيما هو منسوب إليه من جرم ويطلب إليه الرد على الأدلة القائمة ضده إما بنفيها أو التسليم بها.

ويقصد باستجواب المتهم مجابهته بالأدلة المختلفة قبله ومناقشته فيها مناقشة تفصيلية كي يفندها إن كان منكرا التهمة أو يعترف بها إذا شاء الاعتراف بارتكاب الواقعة فالاستجواب في مرحلته الأولى من التحقيق الابتدائي الغاية منه هو جمع الأدلة، لذا لا يجوز إجراء الاستجواب في مرحلة المحاكمة إلا إذا قبله المتهم هو ومحاميه إن وجد.

والاستجواب لا يكون إلا بتوجيه التهمة ومناقشة المتهم تفصيليا عنها ومواجهته بالأدلة القائمة ضده فلا يتحقق الاستجواب بمجرد سؤال المتهم عما هو منسوب إليه وإحاطته علما بنتائج التحقيق إذا لم يتضمن ذلك مناقشة تفصيلية في الأدلة المسندة إليه.

- ضمانات الاستجواب:

* مباشرة الاستجواب بواسطة سلطة التحقيق: أي أن الاستجواب كأصل عام هو عمل من أعمال سلطة التحقيق، وما خالف هذا الأصل عد مخالفة لقانون الإجراءات الجزائية، وبالتالي اعتبر إجراءا باطلا.

* حرية المتهم في إبداء أقواله: أي أن المتهم حر فيما يقول أو أن يصمت ولا أن يجبر على أي قول أو أن يحلف.

* حق الاستعانة بمحامي أثناء الاستجواب: للمتهم حق الاستعانة بمحامي كما أن له الحق في التنازل عن هذا الحق، فإن لم يستطع عين له محام تلقائيا من قاضي التحقيق.

* اطلاع المحامي على التحقيق: وهي ضمانة مكفولة للدفاع إذ يتعين على سلطة التحقيق اطلاع محامي الدفاع على كامل ملف التحقيق وكل ما توصل إليه القاضي المكلف بالتحقيق دون إنقاص أي ورقة من الملف.

- أهمية الاستجواب في إثبات الجريمة الإلكترونية:

إن للاستجواب أهمية بالغة في استخراج الدليل لإثبات الجريمة الإلكترونية، وذلك من خلال مواجهة المتهم بالتهم الموجهة إليه، وقد لا تكون قيمة للاستجواب في حال امتناع

المتهم عن الإجابة لكن تكمن أهميته البالغة حين يقر بما وجه له من اتهامات أو أن يفهم من خلال استجوابه معرفته بكيفية استخدام الحاسب الآلي وتقنياته.

* ويبقى محضر الاستجواب دليلا من الأدلة التي يستعين فيها القاضي لبناء قناعته حول كيفية ارتكاب الجريمة وحصولها.

المبحث الثالث: الأدلة الإلكترونية التي يمكن الحصول عليها من الأدلة الحديثة للإثبات:

نتيجة التطور العلمي وثورة المعلومات والأعمال الإلكترونية فإن الدليل الجنائي التقليدي أصبح لا يتفق بشكل كامل مع طبيعة الوسط الذي ارتكبت فيه الجريمة حتى يستطيع القاضي أن يبني القناعة الكاملة في الإثبات، ولهذا ظهرت طائفة جديدة من الأدلة تتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهو الدليل الإلكتروني أو الدليل الرقمي الذي يستطيع القاضي بموجبه أن يبقي عليه قناعته ويصدر قراره.

المطلب الأول: ماهية الدليل الرقمي:

– **تعريف الدليل:** لغة: هو ما يستدل به، والدليل هو الدال أيضا، ودله على الطريق أي أرشده، والاسم الدال بتشديد اللام، وفلان يدل فلان أي يثق به، فالدليل في اللغة هو المرشد وما به الإرشاد، وما يستدل به، والدليل الدال، والجمع أدلة ودلالات.

– الدليل اصطلاحا: هو ما يلزم من العلم به علم شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني فيها كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة[1].

يعرف إسوانسون الدليل بأنه: أي شيء مفيد في إثبات أو نفي مسألة في قضية معينة أو كل ما يتصل اتصالا مباشرا بإدانة متهم أو تبرئته استنادا إلى المنطق، ويجب التركيز على كلمة "أي شيء" لأن أي شيء بالمفهوم الواسع يمكن أن يكون دليلا:

Evidence can be defined as anything that tends logically to prove or disprove a fact at issue in a judicial case or controversy, the word "anything" should be emphasized because, in its broadest sense, anything can be evidence.[2]

– 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[3].

---

[1] محمد الأمين بشري:التحقيق في الجرائم المستحدثة،ط1،منشورات جامعة نايف للعلوم الأمنية،الرياض،2004، ص 104،105.

[2] Charless R, swanson, Neil chamelin and Lionard Territo: Criminal investigation (7th , ed) London, ME Growhill, 2000, p 658.

[3] محمد الأمين بشري: مرجع سابق، ص 105.

التمييز بين الأدلة الجنائية والإثبات:

يخلط البعض أحيانا بين الدليل الجنائي والإثبات لما بينهما من علاقة في الإجراءات القضائية، ولكن يمكننا في الواقع الفصل بينهما، فالدليل يتكون من حقائق متنوعة تقدم للمحكمة ولكن نتيجتها هي الإثبات، فالإثبات هو مجموعة جميع الحقائق أي الأدلة المستخدمة لإدانة أو تبرئة المتهم، وبهذا يبدوا واضحا أن مفهوم الإثبات أوسع من أن تنحصر في كلمة دليل، فكلمة إثبات أوسع وأكثر عمومية وتشمل مجموعة من الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق وتحقيق العدالة الجنائية.[1]

- تعريف الدليل الجنائي الرقمي:

تعرف 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] المرجع نفسه، ص 107.

Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its perpetrator.[1]

يعرف الدكتور محمد الأمين بشري الدليل الرقمي على أنه: معلومات يقبلها العقل والمنطق 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 أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.[2]

يعرف الدكتور عمر بن يونس الدليل الرقمي على أنه: الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة، فهو كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني بحيث تمكن الحاسوب من إجراء مهمة ما.[3]

يعرف الدكتور عبد الحميد ممدوح عبد المطلب الدليل الرقمي على أنه: الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات ونبضات مغنطيسية أو كهربائية، يمكن

[1]Eoghan casey: digital evidence and computer crime, london, academic, press, 2000, p 260.

[2]محمد الأمين بشري: مرجع سابق، ص 101.

[3]خالد عياد الحلبي: مرجع سابق، ص 229.

تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.

وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون.[1]

كذلك جاء تعريف للدليل الرقمي في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي للخبير محمد محمود فرغلي والدكتور سعيد المسماري: هو الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات وأشكال وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها.[2]

[1]ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث وتحقيق الجرائم عبر الكمبيوتر، بحث منشور على الموقع www.arablawinfo.com.

[2]محمد محمود فرغلي، سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية ،مرجع سابق.

- موقع الأدلة الرقمية:

بصفة عامة تنقسم الأدلة إلى أربعة أنواع هي:

* **الدليل القانوني:** ويقصد به الأدلة التي حددها المشرع وعين حالات استخدامها وحجية كل منها.

* **الدليل الفني:** يقصد به الدليل الذي ينبعث من رأي الخبير الفني حول تقرير دليل مادي أو قولي وفق معايير ووسائل علمية معتمدة.

* **الدليل المادي:** الدليل الناتج من عناصر مادية ناطقة بنفسها ويؤثر في اقتناع القاضي بصفة مباشرة.

السؤال المطروح في هذه الحالة: ما موقع الأدلة الرقمية من بين هذه الأنواع؟

يرى البعض أن الأدلة الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ووسائل التقنية العالية ومنها الحاسوب محور الأدلة الرقمية، أو الأدلة الجنائية الرقمية في منظور أنصار هذا الاتجاه لا تختلف عن آثار البصمات والأسلحة والبصمة الوراثية DNA.[1]

[1] محمد الأمين بشري: مرجع سابق، ص 110.

ويرى رأي آخر أن الأدلة الرقمية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية والمواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأربعة الأنفة الذكر، وذلك للأسباب التالية:

- الأدلة الرقمية تتكون من دوائر وحقول مغنطيسية ونبضات كهربائية غير ملموسة، ولا يدركها الرجل العادي بالحواس الطبيعية للإنسان.

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

- يمكن التعرف على الأدلة الرقمية المزورة التي جرى تحريفها بمضاهاتها مع الأدلة الأصلية بالقدر الذي لا يدع مجالا للشك.

- من الصعب القضاء وإتلاف الأدلة الجنائية الرقمية التي يمكن استرجاعها من الحاسوب بعد محوها.

- علاوة على وجود الأدلة الرقمية في مسرح الجريمة التقليدي يمكن وجودها أيضا في مسرح أو مكان افتراضي Virtuel scène of crime.

- تتميز الأدلة الجنائية الرقمية عن غيرها من أنواع الأدلة بسرعة حركتها عبر شبكات الاتصال.[1]

[1] محمد الأمين بشري: مرجع سابق، ص 111.

تقسيمات الدليل الرقمي:

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في كون الأول تتم في بيئة غير مادية عبر نظام حاسب آلي أو شبكة المعلومات الدولية الإنترنت حيث يمكن للجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يعبث في بيانات الحاسب أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية كما يمكن محوها في زمن قياسي كذلك قبل أن تصل يد العدالة إليه، مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تطلب الطبيعة الإلكترونية على الدليل المتوافر[1].

كما أن الدليل الرقمي ليس صورة واحدة بل يوجد له العديد من الصور والأشكال وقد قسمها البعض إلى الأقسام الرئيسية التالية:

1- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها.

2- أدلة رقمية خاصة بالشبكة العالمية للمعلومات والإنترنت.

3- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

4- أدلة خاصة بالشبكة العالمية للمعلومات.[2]

[1] نبيل عبد المنعم جاد: جرائم الحاسب الآلي، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال، دبي، 2005، ص 127.
[2] محمد محمود فرغلي، سعيد المسماري: مرجع سابق،

وهذا التقييم يتوافق ويتطابق مع تقسيم الجريمة عبر الحاسب الآلي.

خصائص الدليل الجنائي الرقمي:

1- يعتبر الدليل الرقمي دليلا غير ملموس أي أنه ليس دليلا ماديا، فهو تلك المجالات المغنطيسية أو الكهربائية ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل ملموس لا يعني أن هذا التجمع يعتبر هو الدليل بل إن هذه العملية لا تعدوا أن تكون عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة.[1]

2- يمكن استخراج نسخ من الدليل الإلكتروني مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوافر في الدليل التقليدي مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقدان والتلف والتغيير عن طريق عمل نسخ طبق الأصل عن الدليل.

3- الأدلة الإلكترونية يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها وإظهارها بعد خفائها مما يؤدي إلى صعوبة الخلاص منها، وهذا أهم ما يميز الدليل الإلكتروني عن الدليل التقليدي، فيمكن إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف.

[1] علي محمود حمودة: الأدلة المتحصلة من الرسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل المؤتمر العربي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص 22.

4- الدليل الجنائي الإلكتروني ذو طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.[1]

5- يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت، فالدليل الرقمي يمكن أن يسجل تحركات الفرد كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.[2]

المطلب الثاني: كيفية الحصول على الدليل الرقمي من الأجهزة والنظم والشبكات:

من الممكن أن يكون مرتكب الجريمة أكثر دهاءا مما تتصور سلطات التحري أو سلطات التحقيق فيقوم حال إحساسه بالمداهمة بمسح البيانات أو بإتلافه الأقراص الإلكترونية أو بإطلاق فيروسات أو برامج تدميرية لطمس الدليل المتولد من جريمته لذلك وجب على

[1] عمر محمد بن يونس: مرجع سابق، ص 972.

[2] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر،منشور على موقع الدليل الالكتروني للقانون العربي www.arablawinfo.com.

سلطات التحري والتحقيق في مرحلة التحقيق الابتدائي أو في مراحل متقدمة توخي الحذر واتخاذ الإجراءات اللازمة التي تحول دون ضياع الدليل الرقمي، وعليه وجب اتباع التصرفات التالية لاستخراج الدليل الرقمي:

فرع 1: فحص الحاسوب والكيانات المادية والمعنوية المتصلة به:

بعد التوصل إلى ضبط وحجز جهاز الحاسب الآلي المستخدم في الجريمة يقوم المحقق المختص بتفحص أجهزة الحاسوب واستخراج الدليل منها على النحو التالي:

1- فحص القرص الصلب:

يضم القرص الصلب داخله مجموعة البيانات الرقمية ذات الطابع الثنائي (1 ، 0) ويمكن إجراء الفحص الكلي أو الجزئي على القرص الصلب وذلك لهدف التعرف على محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها إلى الكشف عن القيمة الاستردادية للبيانات في القرص سواء أكانت مكتوبة أم على هيئة صور وأصوات كما يهتم المفتش باستعراض ملفات النسخ الإضافية التي يحتويها نظام التشغيل، والتي تظهر مثلا كل صفحات الإنترنت التي تم تصفحها حتى تاريخ قد يصل إلى 06 أشهر، وكل الملفات التي قام مستخدم الجهاز بتنزيلها، وكذلك الملفات وكل ما تم حذفه من بيانات وبرمجيات، ويتم ذلك من خلال استخدام برامج متخصصة أهمها:[1]

[1] عادل عزام سقف الحيط: مرجع سابق، ص 244،247.

أ- برنامج إذن التفتيش:

هو برنامج قاعدة بيانات يسمح بإدخال المعلومات الهامة لترقيم الأدلة وتسجيل البيانات منها ويمكن لهذا البرنامج أن يصور إيصالات باستلام الأدلة والبحث في قواعد الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ب- قرص بدأ تشغيل الكمبيوتر:

هو قرص يمكن المحقق من تشغيل الكمبيوتر، إذا كان نظام التشغيل فيه محميا بكلمة مرور ويجب أن يكون القرص مزودا ببرامج مضاعفة المساحة فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ج- برنامج معالجة الملفات مثل Xtree pro gold:

هو برنامج يمكن المحقق من العثور على الملفات في أي مكان من الشبكة أو على القرص الصلب ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة

المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية كما يمكن من البحث عن كلمات معينة أو عن أسعار ملفات أو غيرها.[1]

د- برامج النسخ مثل Lap Link:

هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من كمبيوتر المتهم ونقلها لقرص صلب آخر سواء على التوازي أو على التوالي وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

هـ- برنامج كشف الدسك مثل AMA DISK, VIEW DISK:

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة.

و- برنامج اتصالات مثل LAN tastic:

هو برنامج يستطيع ربط جهاز المحقق بجهاز حاسب المتهم لنقل ما به معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر.

هذه هي أهم الطرق العامة لجمع الأدلة الرقمية والتي يجب أن يقوم بها الجزاء في هذا المجال نظرا لعلمية ودقة هذه الأدلة.[1]

2- فحص البرمجيات:

تكون من خلال الفحص الداخلي والخارجي لتلك البرمجيات، ففي الفحص الداخلي يتم التأكد من البقاء الداخلي للبرمجية والبحث عن مصدر الملفات، فصور دعارة الأطفال المخزنة في القرص الصلب في جهاز المعتدى عليه، هل جرى تخزينها من المواقع الإلكترونية؟ أم أن المعتدي قام بتنزيلها رقميا إلى القرص الصلب في جهازه من كاميرا ديجيتال ومن ثم قام بتحميلها على مواقع الإنترنت للدعارة؟، ومن ثم فقد يكون المعتدي متهما يلعب دورا هاما في جريمة الاتجار بالأطفال أو ما شابه، أما الفحص الخارجي فيتم بموجبه فحص بناء البرمجية، مثلا فحص ما إذا كانت البرمجيات منسوخة عن أصل محمي وحينئذ تجري مطابقة النسختين للتأكد من كون إحداهما منسوخة عن الأخرى مما يعني قيام جريمة تقليد البرمجيات.

3- فحص النظام المعلوماتي:

هو ضبط كافة المعلومات التي يحتويها الحاسوب من النظام المعلوماتي الذي يعتبر في جوهره بيانات رقمية مخزنة في أنساق معينة للرقمين (0 ، 1) وحين يتم استدعاؤها يظهرها

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر

النظام الحاسوبي في صورة معلومات محددة، يفهمها المستدعي مستخدم الجهاز، لكن تكمن الصعوبة إذا كانت الجريمة قد ارتكبت منذ فترة طويلة، فيصعب جدا فحص النظام المعلوماتي أيضا، فإذا كان الجهاز يحوي كلفة مدور، فيجب فكها قبل الشروع في الفحص علما أن بعض الأنظمة أعدت لتقوم بتدمير نفسها في حالة محاولة الولوج إليها بطرق ملتوية[1].

4- فحص نظام ذاكرة التخزين:

إن نظام ذاكرة التخزين هو قدرة الحاسوب الآلية على الاحتفاظ في ذاكرته بنسخة كاملة مما اطلع عليه عضو الإنترنت في أثناء إبحاره عبر العالم الافتراضي، حيث يمكن فحص نظام الحاسوب لمعرفة مواقع الإنترنت التي زارها المعتدي فترات طويلة من الزمن تصل إلى 06 أشهر كاملة، حتى وإن قام المعتدي بحذف كافة الملفات التي قام نظام التشغيل بتخزينها، فيمكن استخدام برمجيات كالمذكورة آنفا استعادة كل الملفات المحذوفة التي تبين على وجه الدقة رحلات المتصفح في ربوع المواقع الافتراضية.

5- فحص الطابعة:

الطابعات الحديثة تتميز بميزة تخزين آخر مجموعة من الصفحات تم طباعتها حتى عدد معين وإذا كانت تلك الملفات تعرضت لأمر إلغاء، فبرمجيات الاسترجاع المتخصصة يمكنها

[1] عادل عزام سقف الحيط: مرجع سابق، ص 248.

الاستعانة، بنظام الحاسوب لإعادتها وتحديد عدد النسخ المطبوعة وتاريخ طباعتها وساعة الطباعة.

6- فحص المودم:

يحوي المودم معلومات قد تفيد في كشف الجريمة أو على الأقل قد تساعد المحقق على كشف غموضها أو الوصول إلى كشف ملابساتها، فالمودم يحوي قبل فصله عن الإنترنت عنوان ip أو آخر رقم تم الاتصال به أو أرقام اتصال أخرى.

فرع 1: فحص نظام الاتصال بالإنترنت:

1- فحص مسار الإنترنت:

هي الحركة التراسلية للنشاط الممارس عبر شبكة الإنترنت من خلال الحاسوب، بمجرد أن يتعرف على المسار، ويقوم تلقائيا باختبار البروتوكول التراسلي، ومن خلاله يقوم باستدعاء البيانات، ويستخدم نظام الفحص الإلكتروني في تتبع حركة مسار الإنترنت الذي يطلق عليه علم البصمات المعاصر في القرن الواحد والعشرين، وهو عبارة عن منهج ينشط في تتبع الحركة العكسية لمسار الإنترنت.

2- فحص بروتوكول الإنترنت IP ADRESS:

يعد هذا البروتوكول الطابع المميز لاستخدام الإنترنت، فأي شخص يحصل على بروتوكول الإنترنت يمكنه الإبحار في ربوع المواقع الافتراضية، فيباشر تصفح المواقع والانتفاع بخدماتها، وعملية البحث في قواعد البيانات لدى مسجلي بروتوكول الإنترنت عملية سهلة تمكن سلطات التحقيق من تحديد حائز هذا البروتوكول من ذاك عن طريق البحث في قاعدة بيانات خاصة بالمسجلين[1].

3- فحص الخادم أو الملقم:

الخادم هو حاسوب ضخم مهمته تحديد حركة الاتصال بالمواقع والصفحات وكذلك تحديد مسارات الاتصال المعقدة، على هيئة بيانات رقمية، على شبكة الإنترنت، ومن الخوادم ما لا تكون مهمته تحقيق اتصال مع المواقع والصفحات وإنما القيام بالتواصل مع حلقات النقاش والحديث المباشر، أو تخزين البريد الإلكتروني لا غير، على أن يعمل هذا الخادم على ربط أعضاء الإنترنت بغرف التداول والحديث المتواصل، فيبرز عضو الإنترنت كما لو كان يستضيف من يتحدث معه[2].

المطلب الثالث: استخدام البروتوكول TCP/IP كدليل رقمي للإثبات الجنائي:

يعتبر نظام TCP/IP من أكثر البروتوكولات المستخدمة في شبكات الإنترنت فهي جزء أساسي منه، لذلك وجب إبراز أهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن

---

[1] عادل عزام سقف الحيط: مرجع سابق، ص 249.
[2] عادل عزام سقف الحيط: مرجع سابق، ص 250.

أن يحتويها هذا البروتوكول في تحقيق جرائم الكمبيوتر، حيث أنها تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة.

1- المفاهيم المستخدمة في البحث:

- البروتوكول PROTOCOL:

هو اتفاق يحكم الإجراءات المستخدمة لتبادل المعلومات بين كيانين متعاونين، يشمل الاتفاق على كيفية إرسال الرسائل وعدد مرات الإرسال وكيفية العودة إلى الوضع السوي من أخطاء الإرسال ومن الذي يستقبل المعلومات، وبصورة عامة أن البرتوكول يتضمن شكل الرسالة الإلكترونية وتسلسل القواعد الخاصة بها والقواعد التشفيرية الخاصة بالرسائل المرسلة بتتابع صحيح.

- بروتوكول الاتصالات Communication Protocole:

هو مجموعة من القوانين والمقاييس المصممة لتمكين عدة أجهزة كمبيوتر من الاتصال ببعضها البعض ومن تبادل البيانات بأقل قدر ممكن من الأخطاء ويتألف البروتوكول المقبول عادة لتنظيم اتصالات الكمبيوتر بشكل عام من سبع طبقات من الأجهزة والبرمجيات والتي تعرف بنموذج (OSI ربط الأنظمة المنتج).

- **بروتوكول التحكم بالنقل / بروتوكول الإنترنت TCP/IP:**

هي عائلة بروتوكولات الاتصالات بين عدة أجهزة كمبيوتر طورت أساسا لنقل البيانات الرقمية عبر شبكة الإنترنت بواسطة الاتصال الهاتفي.

والبروتوكول TCP/IP يضم في الواقع بروتوكولين مستقلين في شبكة الإنترنت هما بروتوكولات TCP وبروتوكول IP حيث يعملان معا وبشكل متزامن، ويركزان على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (PACKET) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها[1].

- **الحزم المعلوماتية (PACKET):**

هي جزء أو قسم من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه بحيث تعتبر كل حزمة عبر شبكة الإنترنت بشكل مستقل ويترواح حجم الحزمة من 40 و 32000 بت، وعند كل وصلة تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المرسل إليه النهائية.

[1]ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

- بروتوكول الإنترنت IP:

هو بروتوكول عنونة البيانات والمواقع في شبكة الإنترنت وبمقتضى هذا البروتوكول يتم التعرف على الكمبيوتر بشبكة الإنترنت من خلال عناوين عددية، حيث لكل كمبيوتر موصول بها عنوانه الوحيد الخاص به تماما.

2- كيفية عمل بروتوكولات الإنترنت:

بروتوكول TCP/IP كدليل رقمي:

مقرن تزيكرم TCP/IP كذملآم لآهپفلآ نغزقت كيقيق غنم كم نه تزيكرم TCP ويزيكرم IP؛ ركنب وصزهب نه كهقم قرئه تزيكرم TCP/IP يغثتز نه وصرز بمتزيكرث بمنشثذنتت قلآ صپكت بلاهثزه ربثضبث؛ قرلآ حسآ وشبشلآ نه بلاهثزه رفثلره ورب بمتزيكرم ننب لآملآ[1]:

1- تزيكرم User Data gsam Protocole: UDP.

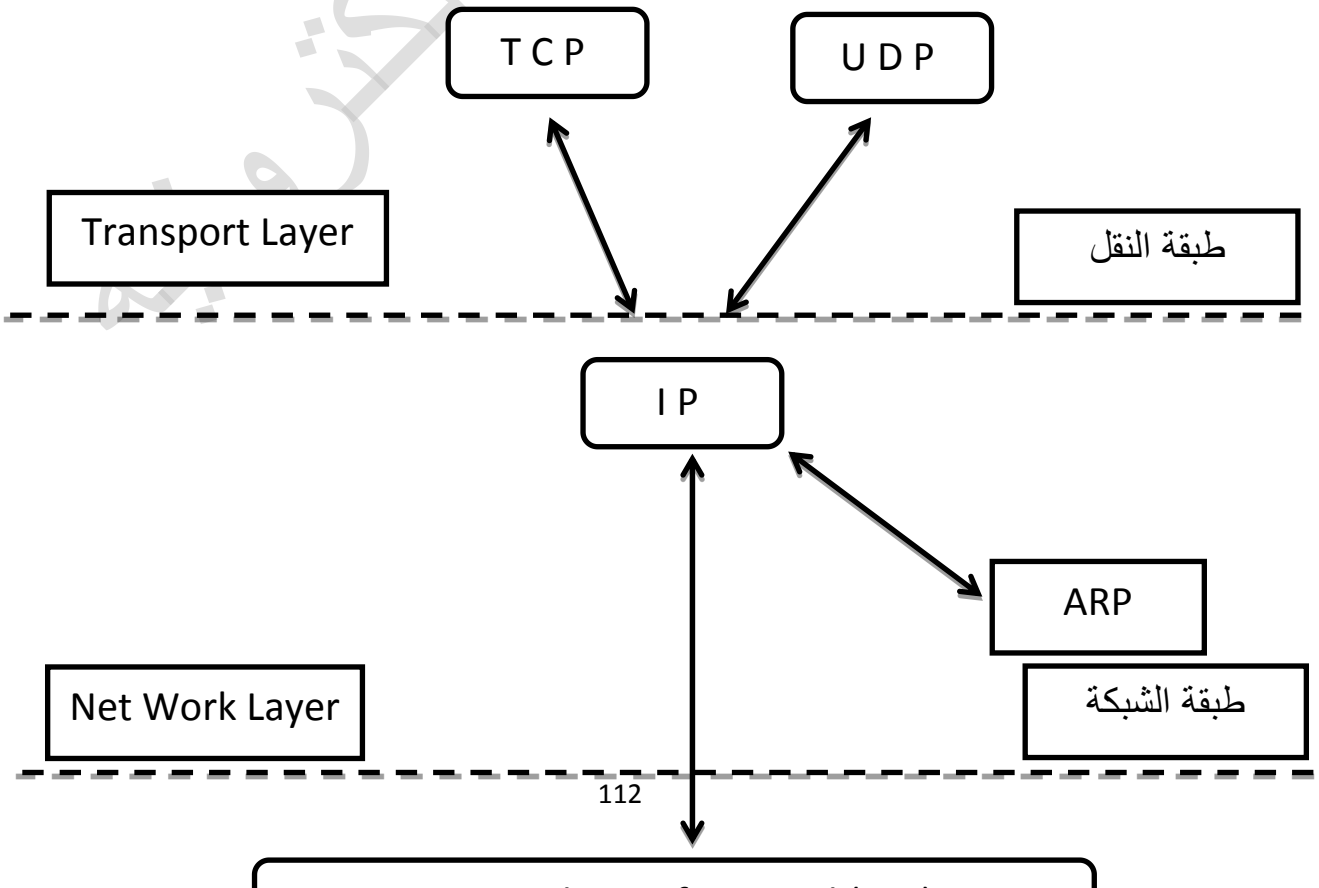
2- تزيكرم Transport Control Protocole: TCP.

3- تزيكرمInternet Protocole: IP.

[1]ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

ىڭغنم ورھ بەمەزىڭىكىۋىڭ بەمچ چەت نغب مەكم بەمنغمىنبڭ بەمذبضت پيمنشڭذن ظپكب

مەعبن ويكمت ڭپيذم بەمنغمىنبڭ بەمنغزىق پيشن: With O S I TCP/IP.



1- يقوم بروتوكول TCP بتسليم مجموعة المعلومات المطلوب إرسالها أو إعادة إرسالها حينما يكون ذلك ضروريا وبمساعدة البروتوكول U D P المصمم لمواجهة بعض التطبيقات التي لا تستخدم TCP، ويلاحظ أن هذه التطبيقات U D P T/CP مصممة أيضا لمواجهة المشكلات الشائعة التي قد تحدث أثناء عملية تبادل المعلومات ويشمل ذلك إخفاق الهارد ووير والمعلومات المتأخرة وازدحام الشبكات والأخطاء المتكررة أو المتتالية.

2- ولمواجهة حالات التدفق المعلوماتي الناشئ من استخدام الشبكة من قبل عدة مستخدمين وخصوصا في حالات المشاركة في الهارد ووير أو في خط هاتفي واحد أو في وسيلة اتصال واحدة، يتم تقسيم المعلومات باستخدام طريقة Pac kets وهي طريقة من شأنها تقسيم المعلومات لمساعدة أكثر من جهاز كمبيوتر لاستخدام نفس وسيلة الاتصال أو نفس الأجهزة وتمكنها في نفس الوقت من فتح أكثر من قناة.

3- بعد تقسيم المعلومات يتم ترقيمها بنظام Port وهو نظام من شأنه التعريف بمجموعات المعلومات المقسمة والمتبادلة بين أجهزة الكمبيوتر، فتأخذ كل مجموعة رقما معينا يمكنها الاستدلال عليه لاحقا والترقيم المعتمد كنموذج لصفحات الويب والإميل ومجموعات الأخبار هو 80، 25، 119 على التوالي، وعلى ذلك حينما يستقبل الملقم Server باكت برقم 25 يعرف أن هذا الباكت هو email، وإذا لم تكن الحزمة المرقمة بهذا الرقم email فإن الملقم لا يتعرف عليها ويعيدها برسالة خطأ أو يقوم بإهمالها.

4- بعد تقسيم المعلومات، يقوم بروتوكول TCP بتحقيق الاتصال بالكمبيوتر المرسل إليه يعتمد في هذا الشأن ثلاث طرق وهي باستخدام S Y N أو A C K أو كليهما كالآتي[1]:

الأولى: يقوم الكمبيوتر المرسل بإرسال باكت S Y N وهي باكت يحتوي على معلومات مؤداها أن المرسل يرغب في فتح قناة اتصال مع المرسل إليه، وعادة يستخدم T C P مثل هذا الباكتات محفوظة في أرقام متتالية وتحت الطلب إلى كمبيوتر المرسل إليه.

الثانية: يقوم كمبيوتر المرسل إليه عند استلام طلب كمبيوتر المرسل بإرجاع باكت خاص يسمى A C K وهذا اختصار لمصطلح Acknowledgement وهذا الباكت يحتوي أيضا على S Y N بت B I T قادر على جعل الاتصال يتزامن في نفس الوقت.

الثالثة: كمبيوتر المرسل يقوم بإرسال باكت يحتوي على معلومات مع A C K بت إلى كمبيوتر المرسل إليه، لتحقيق الاتصال وتلقي المعلومات.

5- وفي خلال فترة زمنية معينة، إذا لم يستلم T C P رسالة بأن الاتصال قد تم بين المرسل والمرسل إليه، فإنه يعيد الإرسال مرة أخرى، حتى في الحالات التي يتم فقد الباكت فيها أو عدم صلاحيتها.

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

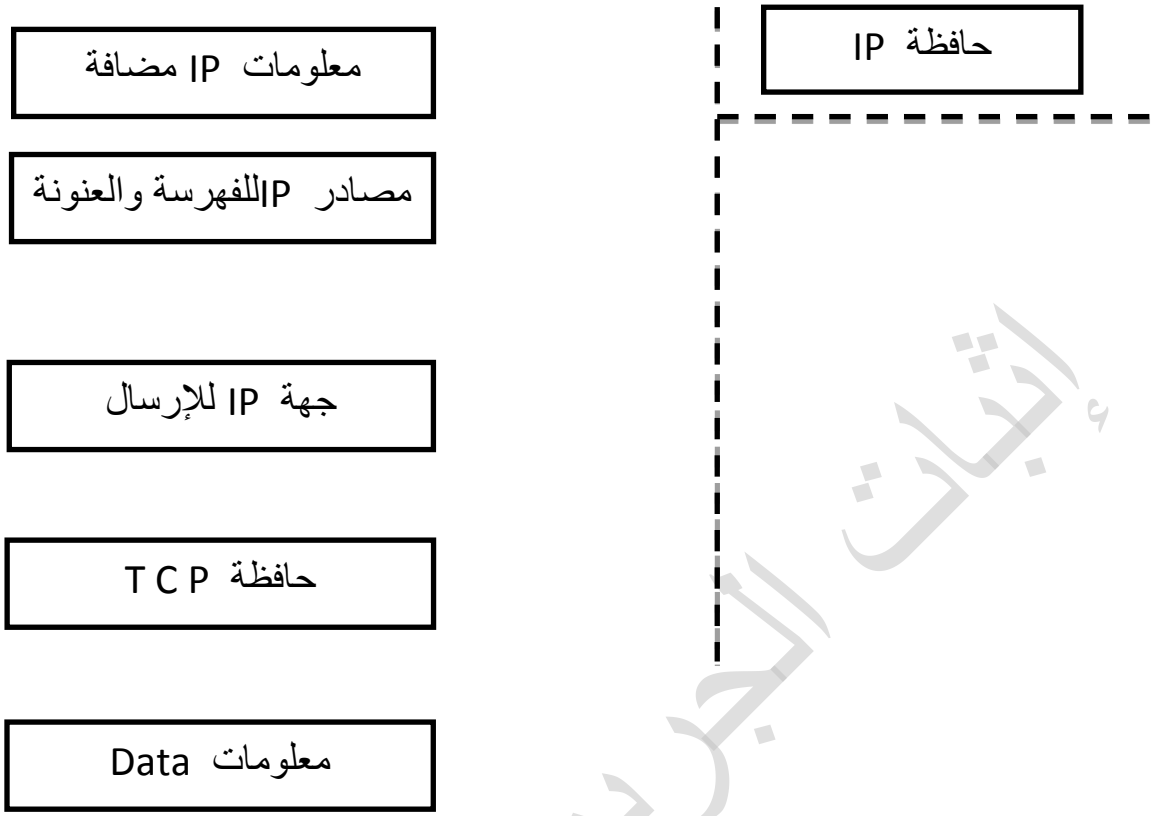
6- إذا ما تحقق الاتصال، يقوم T C P بالتأكد من أن الباكت قد أرسلت فعلا إلى المرسل إليه وفي الزمن المطلوب طبقا للمعدلات الزمنية، وأرسلت أيضا في الشكل المطلوب وطبقا للتعريفات الرقمية المحددة والمتعارف عليها.

7- حينما ينتهي الاتصال بين المرسل والمرسل إليه، يقوم بروتوكول T C P بإرسال باكت يفيد الانتهاء FIN(BIT).

ولكن ما هو عمل برتوكول IP ؟!

1- بروتوكول IP هو المسؤول الأول عن العنونة والمعلومات المرفقة، فبعد قيام T C P بتقسيم المعلومات إلى حزم معلوماتية (الباكت) يقوم برتوكول I P بعنونة كل حزمة مع إضافة معلومات أخرى إليها لتصبح الباكت المحتوي على حزمة مع إضافة معلومات أخرى إليها لتصبح الباكت المحتوي على حزمة TCP/IP بهذا الشكل[1]:

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.



2- ويلاحظ أن كل كمبيوتر بالإنترنت له عنوان خاص به يسمى P Adresses وكل عنوان مكون من جزئين، الأول يشمل أرقام الشبكة Net Work Numbers والثاني يشمل أرقام مقدم الخدمة Host Numbers.

3- ولقد اعتمد نظام لفهرسة العناوين عن طريق تقسيم العناوين إلى مستويات ثلاثة، مستوى يستطيع أن يتعامل في نطاق جغرافي معين (على مستوى المدن الأحياء، الدول...هكذا).

4- وعلى الرغم من أن الكمبيوتر، بتعامل أفضل من الأرقام، إلا أن المستخدمين يفضلون الحروف والأسماء وحينما تكتب اسما معينا، كشرطة الشارقة مثلا، فإن هذا الاسم يتحول أوتوماتيكيا إلى أرقام دالة على الموقع المطلوب.

5- وحينما تصبح المعلومات جاهزة للإرسال إلى كمبيوتر المرسل إليه، فإن الحزم المعلوماتية المرقمة تمر خلال عدة طرق محددة سلفا ويقوم برامج IP في كل طريق بتحديد المسارات التي تسلكها الحزم حتى تصل إلى الوجهة المحددة وعادة يقوم IP في كل مرة بتحديد أفضل المسارات طبقا لزمن الشبكة وازدحامها وجهة الوصول وغيرها[1].

6- ويوجد برنامج يسمى Trace route يمكنه تقديم قائمة بالطرق والمسالك التي يمكن أن تسلكها الحزم المعلوماتية للوصول إلى الكمبيوتر المقصود، وعادة ما يتم إدراج هذا البرنامج ضمن نظم التشغيل الرئيسة Operating System وعادة تسلك المعلومات أو الحزم المعلوماتية نفس المسار دائما، ما لم يتم تغيير هذا الاتجاه بتغير الأجهزة مثلا.

ويعتبر هذا البرنامج برنامج Trace Route ذا أهمية في الكشف الجنائي، حيث أنه يحدد بدقة أي من أجهزة الكمبيوترات التي اشتركت في نقل البيانات عبر الإنترنت، وتحديد مساراتها حتى وصلت إلى المرسل إليه وتحديد الملفات التي تم الولوج إليها لذلك تصبح كل

[1]How the TCP/IP Protocol Works, *Les Cottrell – SLAC*
Lecture 1 presented at the 26th International Nathiagali Summer College on Physics and Contemporary Needs, 25th June – 14th July, Nathiagali, Pakistan

المسارات بها آثار أو أدلة رقمية يمكن الاستدلال بها على نشاط الجاني، كما أنه من جهة أخرى يحدد المسار الذي أخذته المعلومة وتحديد أي اختراق أو عبور أو تجاوز خلال الإعداد للجريمة، كما أنه يستدعي أو يمكنه أن يحيط بكافة المعلومات المتعلقة بدخول أشخاص مواقع معينة وتحديد مسارات ولوجهم وخروجهم من المواقع المحددة.

ولفهم ذلك كله هناك سيناريو يمكن تخيله، لنفترض أنك تريد أن تنشئ شبكة داخلية، بينك وبين أصدقائك وجيرانك لذلك ستعمل على اتخاذ الخطوات التالية:

أ- يتم توصيل كافة أجهزة الكمبيوتر الخاصة بجيرانك المستهدفين ببعضها البعض وتستخدم المودم Modem للربط بينهم جميعا.

بـ- حينما تريد توصيل شبكتك بالشبكة العالمية للمعلومات لابد أن تحصل على عنوان لك لذلك سوف تحاول الحصول على عنوان من إحدى المنظمات المتخصصة التي تمنح عناوين وبعد ذلك تخصص عناوين لمستخدمي شبكتك من خلال عنوانك الرئيس الممنوح لك وتحتفظ ببعض العناوين الأخرى.

جـ- مسار دخول أو ولوج شبكتك إلى الشبكة سواء قام به أصدقاؤك أو جيرانك أو قمت بها أنت، سوف يتم من خلال طريق أو مسار واحد عن طريق العنوان الممنوح لك في بداية إنشاء شبكتك ويترتب على ذلك:

1. تصبح أنت مزودا بخدمة بالنسبة لجارك أو صديقك المتصل بالشبكة الخاصة بك.

2. تستطيع لذلك مراقبة تحركات صديقك أو جارك على الشبكة في كل زمان ومكان كما يمكنك نسخ هذه التحركات والاحتفاظ بها لاستخدامها عند اللزوم.

3. معظم المعلومات التي أرسلها الجار أو الصديق خلال الإنترنت هي معلومات صادرة منه أو من جهازه تحمل قرينة قضائية بحيث لا يمكن إنكار صدوره منها.

د- ولاستكمال السيناريو، نفترض أن موقعك أصبح معروفا ولذلك لم يعد لدلك عناوين IP كافية لتلبية احتياجات الاتصال للمستخدم، لذلك يتم حل هذه المشكلة عن طريق إعطاء عنوان IP بتفرد خاص بكل مستخدم، بحيث يقوم هذا المستخدم في كل مرة بطلب الاتصال بالإنترنت بالتوقيع بهذا العنوان المخصص له ويلاحظ أن هذه العناوين IP المميزة لكل مستخدم وهي الأسلوب الشائع الآن لمزودي الخدمة.

لذلك فإن البحث الجنائي يمكنه بهذه الوسيلة (الرقم المميز الشخصي لعنوان IP لك مستخدم) أن يحدد من هو المستخدم (طبقا لسجلات اعتماد توصيل الخدمة للمستخدم أو عند الاشتراك في الخدمة) وتحديد زمن الاستخدام الفعلي ووقت الاستخدام الحقيقي والمواقع التي قام بالولوج فيها ومدة المكوث داخل كل موقع، والطرق أو المسالك عبر الشبكة منذ

لحظة الدخول وحتى لحظة الخروج من الموقع، وعادة يتم حفظ كل ذلك لدى مزود الخدمة ولفترة زمنية تحدد طبقا لكل مزود[1].

ومن هنا، تبدو من الأهمية للبحث والتحقيق الجنائي، سرعة الإبلاغ عن الجرائم التي يستخدم فيها الكمبيوتر، حيث يمكن إذا تم الإبلاغ في الفترة المسموح فيها بالاحتفاظ بتاريخ التحركات لدى مزود الخدمة، العثور على الدليل المستهدف من تحريات الشرطة.

ويثور في البحث الجنائي الرقمي صعوبة، عند قيام بعض مزودي الخدمة بإعطاء عناوين غير ثابتة للمستخدمين أو ما يعرف باسم Dynamic IP Address، فكيف يمكن الاستدلال على شخص المستخدم؟!.

الواقع أنه يمكن التفرقة بين كل من العناوين المحددة أو المميزة أو الثابتة لكل مستخدم والتي تعرف باسم Static IP Address والعناوين الغير الثابتة أو غير المحددة لشخص أو ما يعرف باسم Dynamic IP Address، حيث تعرف الأولى بأنها العناوين المحددة لكل مستخدم ويتم استخدامها في كل مرة يتم الولوج للإنترنت، بينما الثانية هي عناوين غير محددة، فكل مرة يتم الاتصال فيها بالإنترنت يتم التوقيع بعنوان جديد فيما يعمد مزود الخدمة لمواجهة تدفقات الاستخدام الطارئ للشبكة من قبل أشخاص لا يريد مزود الخدمة تثبيت رقم محدد لعناوينهم ويمكن الاستدلال على هذا العنوان الديناميكي من خلال وجود كلمة PPP

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

أو كلمة Dial أو يحتوي على أرقام مثل e.g. Czo52.Cyberia.com وهذه الارقام عادة جزء من ديناميكية العنوان ويمكن أن يستدل منها على جهة معينة أو منطقة جغرافية محددة، ويمكن القول بأنه إذا كان المستخدم يقوم بالاتصال عن طريق الخط الهاتفي (المودم) فإن عنوان بروتوكول الإنترنت يكون ثابتا لا يتغير وجميع هذه العناوين سواء أكانت ديناميكية أو ثابتة يتم تحديدها وفق سلسلة معينة من الأرقام من قبل مزود الخدمة.

هذه العناوين الديناميكية يمكن أن تشكل صعوبة لتحديد شخص مستخدم عنوان IP الديناميكي في الوقت المحدد، ولكن لحسن الحظ، أن مسارات ومعلومات الولوج يتم الاحتفاظ بها لبعض الوقت وعن طريقها يمكن الاستدلال عن شخص المستخدم أو تضييق دائرة البحث الجنائي[1].

ويلاحظ أن هناك بروتوكولات خاصة بالتوقيع الرقمي باستخدام عناوين IP، حيث تستخدم بعض الشبكات بروتوكولا يسمى (DHCP)Dynamic Host Configuration Protocol.

وهذه البروتوكولات تستخدم سواء للتوقيع بعناوين محددة أو ديناميكية ووظيفة هذه البروتوكولات منع الكمبيوتر من استخدام عناوين IP خاطئة، ويحدث هذا الخطأ فيما يعمد بعض الأشخاص لتشغيل الكمبيوتر الخاص بهم باستخدام عنوان IP مختلف وذلك لإخفاء

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

تحركاتهم، كما يحدث الخطأ أيضا اعتراضيا إذا لم يستطع الكمبيوتر أن يحدد عنوان IP الصحيح له، ولمنع حدوث ذلك كله تستخدم البروتوكولات.

3-المحددات الفنية لاستخدام بروتوكول TCP/IP كدليل رقمي للإثبات الجنائي أو المدني:

1. هناك عدة تحديات حينما تستخدم بروتوكول TCP/IP كدليل رقمي للإثبات الجنائي أو المدني منها:

أ- بروتوكول IP وحدة معلوماتية، تحتوي على معلومات عن الكمبيوتر ولكن ليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محددا أحدث الفعل غير المشروع، ومع ذلك فإن ذلك يمكن أن يستخدم كقرينة قضائية ضد مالك أو صاحب هذا الجهاز إلى أن يثبت العكس ذلك أن نقطة بدء نشوء مسار بروتوكول TCP/IP يمكن أن تساعدنا للوصول إلى المشتبه فيه، حيث أن مجموعة صغيرة من الأفراد هي التي يمكنها أن تستخدم أجهزة محددة، وبأرقام وعناوين محددة[1].

بـ- التحديث الثاني، حينما يعمد المشتبه بهم أو الجناة إلى استخدام عناوين ديناميكية لارتكاب جرائمهم، أو حينما يضعون معلومات غير صحيحة أو قانونية باستخدام الكمبيوتر الشخصي لهم في ملف خدمات عام من أجل تجنب التعرف عليهم، ويحدث ذلك فيما يقول

[1]ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

المشتبه فيه أو المجرم باستخدام مزود خدمة ذي حجم مستخدمين كبير فالمجرم سوف يوقع باستخدام عنوان IP ويمكن للآخرين في ذات الوقت من استخدام نفس العنوان وبعد مرور فترة زمنية يقوم بغلق الاتصال وبعد فترة يعاود الاتصال مما يجعل غالبا نتائج النشاط الإجرامي موزعة على عدة عناوين لل IP ومع ذلك فإن إمكانية التعرف على المجموعة المختارة من الناس التي استخدمت الكمبيوتر محل الاشتباه في ملف خدمات، أمر يمكن من خلاله الاستدلال على المجرم أو الشخص الحقيقي.

جـ- التحدي الأصعب، حينما تكون المعلومات المحملة في عناوين IP غير حقيقية أو زائفة، وهذا ممكن حينما تحدث حزمة معلوماتية Packet باستخدام مصدر زائف لمصدر عنوان IP، بحيث يظهره بأن المعلومات جاءت من كمبيوتر محدد بينما في الحقيقة جاءت من كمبيوتر آخر، ومثال ذلك حينما يقوم برنامج خبيث Malicious Program، بإدخال معلومات كاذبة أو غير حقيقية عن حقيقة عنوان IP في Packet الإرسال وقبل الولوج في شبكة المعلوماتية، ويحدث ذلك حينما يقوم البرنامج الخبيث بإغراق الشبكة بالمعلومات أو إرسال العديد من الرسائل، أو حث الماكينة الرئيسة في مزود الخدمة أو الشبكة على الإسراع أو التعجيل في العمل ولحسن الحظ أيضا، معظم المجرمين لا يعلمون كيف يزيفون عناوين IP، ولا يعرفون أي من عناوين IP يمكن أن تكون دالة على الشخص المجرم في الجريمة المحددة.

2. الصعبات الفنية لاستخدام ملف الولوج Log files في الإثبات:

تحتوي ملفات الولوج على كمية هائلة من المعلومات عن الاستخدام الشخصي للكمبيوتر وهي بذلك مصدر من أهم المصادر للأدلة الرقمية ويرجع السبب في ذلك إلى ما يلي:

أ- تحتوي هذه الملفات على عناوين IP التي تمكن أجهزة البحث من تحديد أي كمبيوتر بالضبط، قام بالفعل الإجرامي في الوقت المحدد المسجل وفي المكان المحدد المسجل، وتفسير ذلك أن جهاز خادم الولوج Server Log يسجل كافة العناوين والتوقيتات والأزمنة للأجهزة المتصلة به ويشمل ذلك كافة الأنشطة المعلوماتية التي تتم على الشبكة مثل التصفح واستعراض المواقع المختلفة وإرسال واستقبال الرسائل الإلكترونية.

بـ- ترتبط ملفات الولوج Log Files غالبا مع برامج الحماية Firewalls وبرامج تحديد المسارات Routers حيث تسجل غالبا[1] تحركات الدخول والخروج مع بروتوكولات TCP/IP ويلاحظ أن صعوبة البحث هنا، ترجع إلى أن ملفات الولوج في نظام UNIX تتطلب من رجال البحث الجنائي إلماما خاصا بطرق استخراج المعلومات حيث أن إعطاء بعض الأوامر دون البعض الآخر من شأنه أن يظهر بعض المعلومات دون البعض الآخر، لذلك يجب على رجال البحث استخدام أوامر Syslog-Log-Var-More، لاستخراج كافة المعلومات المسجلة عن النشاط الذي تم باستخدام جهاز الكمبيوتر.

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IPفي بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

4- جمع وتوثيق وحفظ الدليل المستخرج من بروتوكول TCP/IP:

1- جمع الدليل المستخرج من بروتوكول: TCP/IP

جمع الأدلة الرقمية من بروتوكولات النقل والشبكات والاتصالات يمكن أن يشكل صعوبة نسبية من وجهة نظر أجهزة إنفاذ القانون، وبالرغم من أن ملفات الولوج Log File تبدو مشابهة للملفات العادية، وممكن جمعها مثل أي ملف آخر وهي تحتوي على كمية هائلة من المعلومات التي قد تفيد البحث والتحقيق الجنائي، إلا أن الصعوبة في جمع هذه المعلومات الجنائية، أنها عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الأبرياء مما قد يشكل تهديدا لخصوصية هؤلاء ويعتبر في ذات الوقت ضبطا بدون تفويض أو تصريح أو أمر قانوني أو قضائي، لذلك تعمد بعض منظمات تشغيل الكمبيوتر والشبكة إلى عدم إفشاء أسرار جميع ملفات الولوج إلا الخاصة بالمتورطين فقط في قضايا مدنية أو جنائية وبناء على أمر قضائي طبقا للنظام القانوني السائد في الدولة.

وهناك صعوبة أخرى في جمع الأدلة الرقمية من جداول الحالة التشغيلية في البروتوكولات والاتصالات وتتمثل هذه الصعوبة في أن هذه الجداول تكون متاحة لفترات قصيرة ولا يمكن التغلب على هذه الصعوبة بالتحفظ الجنائي على أجهزة الهارد وير Hard Ware لحين الفحص، لأن هذه الجداول تزال تلقائيا بمجرد غلق أو انقطاع التيار الكهربائي عن تلك الأجهزة، لذلك فمن المستحسن أن يتم استخدام أسلوب Cut And Past القص واللصق إلى

ملف جديد خاص بجمع الأدلة وقبل غلق الأجهزة، ورغم أن أسلوب القطع واللصق أسلوب ناجح لجمع الأدلة، إلا أن المشكلات القانونية المترتبة على قانونية هذا الأسلوب قد تثير بعض الشك في مدى سلامة جمع المعلومات وحجيتها أمام أجهزة العدالة الجنائية لذلك يقترح ما يلي لسلامة الجمع والتوثيق:

1. أخذ نسخة كاملة من بيانات الجداول التشغيلية عند ضبط الجهاز المستخدم وقبل فصل الجهاز عن التيار الكهربائي وذلك بطباعة هذه النسخة.

2. القيام بعمليات النسخ واللصق والتجميع في File محدد بعد التأكد من خلوه التام من أي معلومات أخرى.

3. مراعاة ترقيم البيانات المجزئة طبقا للتسلسل الحادث بحيث يتم الاستدلال عليها بشكل متسلسل ومنطقي وطبقا للأصل.

وهذه الإجراءات رغم أنها إجراءات طويلة وتتطلب وقتا ومثابرة ودقة في العمل، إلا أنها ضرورية ولازمة للتدوين والحفظ لإمكان اعتمادها كدليل أمام أجهزة العدالة الجنائية.

2- تصنيف وتخصيص وتوثيق الدليل المستخرج من بروتوكول TCP/IP:

ذكرنا من قبل أن ملفات الولوج وجداول الحالة التشغيلية يمكن أن تحتوي على معلومات عن مصادر وطبيعة الجريمة محل التحقيق أو البحث، حيث تحتوي ملفات الولوج على

عناوين IP للكمبيوتر المستخدم والكمبيوتر الوسيط أو الرئيس الخادم، وتحتوي على معلومات من كافة الأنشطة التي قام بها المستخدم أو حاول أن يقوم بها عند استخدامه للشبكة المعلوماتية وتحتوي كذلك على معلومات بشأن أنواع الاتصالات التي تمت وكل هذه المعلومات ممكن أن تستخدم في تصنيف وتخصيص وتوثيق الدليل الرقمي تجاه الجريمة محل البحث والتحقيق[1].

وملفات الولوج وجداول الحالة التشغيلية ممكن أن تصنف كوحدة معلوماتية كاملة مثل:

A linux 5.2 Wtmp Loge, a Solaris syslog, a state table from windows NT primary Domain Controller وهي بذلك يمكن أن تقارن مع وحدة معلوماتية كاملة أخرى وذلك لتحديد الجزء المطلوب للدليل الجنائي.

بالإضافة إلى تصنيف ملفات الولوج وجداول الحالة التشغيلية كوحدة معلوماتية كاملة، فإن احتواء هذه الوحدة على المعلومات الصالحة لتعرف عليها وتصنيفها وتوثيقها يعطي لها أهمية خاصة في البحث والتحقيق الجنائي.

[1] ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر، مرجع سابق.

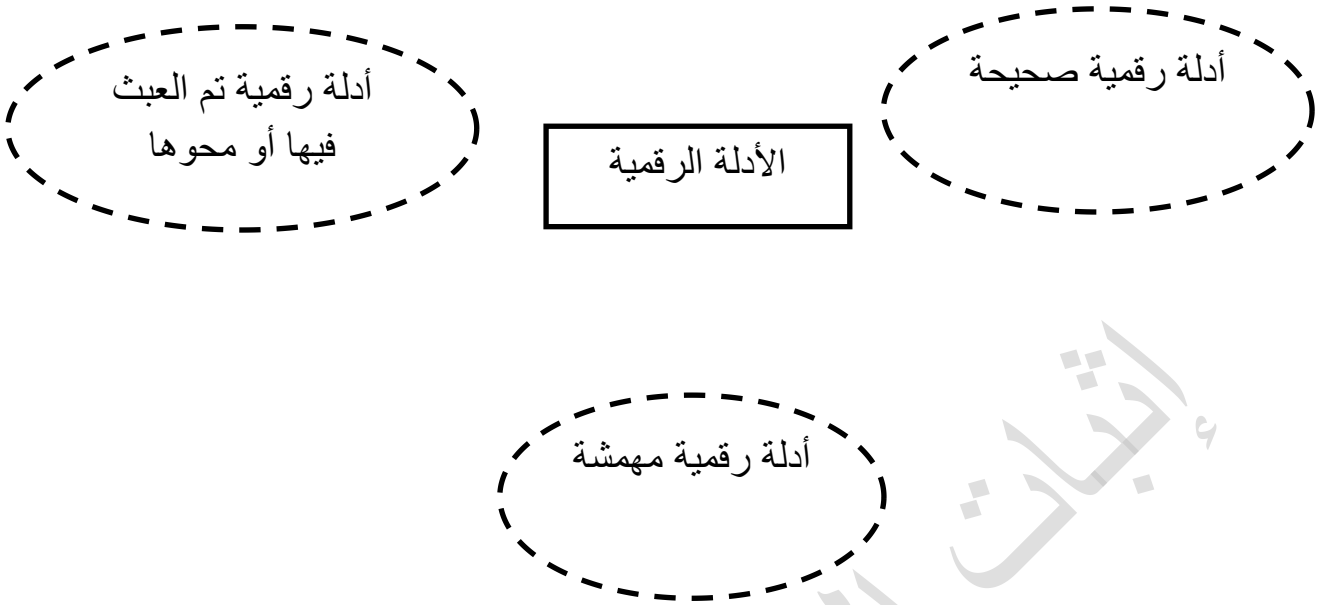
وهناك العديد من أشكال الاتصال باستخدام بروتوكول TCP مثل Web, Email, Telnet وهذه الاشكال ممكن أن تصنف وبعد إتمام عمليات التصنيف يمكن إجراء عمليات المقارنة بين الأفعال المشتبه بها وبين الأفعال الطبيعية الأخرى.

ويلاحظ إذا كان هناك ولوج من مشتبه به أو توافرت باقة معلومات عن عنوان IP لمستخدم ما فإن هذا الولوج وهذه المعلومات قد لا تكون مطابقة لمستويات معروفة ولكن الباحثين الجنائيين يمكنهم مقارنة المعلومات قد لا تكون مطابقة لمستويات معروفة ولكن الباحثين الجنائيين يمكنهم مقارنة المعلومات المتوافرة مع المعلومات الأخرى الرسمية أو المتفق عليها لاكتشاف الفروق التي يمكن أن تدين المشتبه فيه، حيث أن الطابع الشخصي للدلة الرقمية أثناء وجودها في ملفات الولوج أو بروتوكولات الاتصالات، ممكن أن تكون العلاقة بين الجريمة المرتكبة وسلوك المشتبه به المسجل في هذه الملفات ويتم ذلك باختبارات المقارنة.

3- إعادة بناء الدليل المستخرج من بروتوكول TCP/IP:

توجد ثلاثة أنواع من إعادة بناء الأدلة الرقمية وهم الأدلة الرقمية التي تم العبث بها أو محوها والأدلة الرقمية الصحيحة وهناك نوع ثالث يطلق عليه الأدلة الرقمية الهامشية[1].

[1]How the TCP/IP Protocol Works, *Les Cottrell – SLAC*



ويلاحظ أنه من الضروري أن تتم الاستعانة بهذه الانواع الثلاثة فالأدلة الرقمية الصحيحة يتم من خلالها استخلاص المعلومات المتعلقة بالجريمة والمجرم من خلال البحث فيها، كما أن الأدلة الرقمية التي تم محوها أو العبث فيها، تتم إعادة بنائها باستخدام برامج خاصة معروفة لهذا الأمر والأدلة الرقمية المهمشة، وهي أدلة رقمية تلعب دورا حاسما في إعادة ترميم الأدلة الممحاة أو التي تم العبث فيها، كما أنها تكمل أوجه النقص في الأدلة الرقمية المستخلصة من الأدلة الرقمية الصحيحة عن علاقة المجرم بالجريمة المرتكبة.

المطلب الرابع: حجية الدليل الإلكتروني أمام القضاء الجنائي:

Lecture 1 presented at the 26th International Nathiagali Summer College on Physics and Contemporary Needs, 25th June – 14th July, Nathiagali, Pakistan

إن مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ أن الطبيعة الفنية الخاصة للدليل الإلكتروني تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإبلاغ 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؟[1]

فوفقا للنظم القانونية التي تأخذ بالنظام اللاتيني في الإثبات ومنها القانون الأردني والفرنسي والمصري والسوري، فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته الإثباتية، فللقاضي قبول الدليل ورفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل، وهذا المعنى هو ما نصت عليه المادة 147\2 من قانون أصول المحاكمات الجزائية الأردني، فهل يمكن للقاضي الجنائي وفقا لهذا النظام أن يعمل 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

[1] خالد عياد الحلبي ، مرجع سابق ، ص 246

المتعلقة بأصالة الدليل الإلكتروني، فضلا عن ذلك فإن هذا الدليل يتمتع من حيث قوته الإثباتية بقيمة إثباتية قد تصل إلى حد اليقين، فهذا هو شأن الأدلة العلمية عموما، فالدليل الإلكتروني من حيث إثباته على الواقع تتوافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل، ولكن هذا لا يناقض من أن الدليل الإلكتروني هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، حيث حيث يشكك في سلامة الدليل الإلكتروني من ناحيتين[1]:

الأولى: الدليل الإلكتروني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبرا عن واقعة معينة صنع أساسا لأجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون في استطاعة الشخص 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 تمكن من العبث بالدليل الإلكتروني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

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

[1] خالد عياد الحلبي : مرجع سابق ، ص 248/247.

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

2- الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 10% ويحدث هذا غالبا بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ومن خلال ذلك فإننا نرى إلى الشك في الدليل الإلكتروني لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في حجيته، ولكن هل يمكن التثبت من سلامة الدليل الإلكتروني من حيث العيوب وبمعنى آخر ل من الممكن أن يضفى الدليل الإلكتروني اليقين من خلال إخضاعه للتقييم الفني الذي يمكن 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 القواعد أخرى والحكم على حجيته الإثباتية، وذلك يرجع للطبيعة الفنية لهذا الدليل، فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه.

فتوجد عدة وسائل يتم بها تقييم الدليل الإلكتروني وسوف نقوم بتناولها على النحو التالي[1]:

1- تقييم الدليل الإلكتروني من حيث سلامته من العبث:

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

1- يلعب علم الحاسوب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون وشكل الدليل الإلكتروني، 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، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.

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.

[11] خالد عياد الحلبي ، مرجع سابق ، ص 249

3- هناك نوع من الأدلة الإلكترونية تسمى 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 النظم المعلوماتية.

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

فرع 2: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول على الدليل الإلكتروني:

من المعتاد بأن تتبع جملة من الإجراءات الفنية للحصول على الدليل الإلكتروني، وقد بينا بأن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داو بورت) كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ولذا فإننا سنبين باختصار الخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية:

1- إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المبتغاة:

وذلك بإتباع اختبارين رئيسين هما:

أ- 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.

ب- اختبار الإيجابيات الزائفة: ومفادها ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الإلكتروني لاختبار فني يمكن 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 وفي ذات الوقت لم تضف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق جهاز الحاسوب مصداقية في التدليل على الواقع.

2- الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل:

تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الإلكتروني، وفي المقابل أوضحت الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني، فإذا توافرت في الدليل الإلكتروني الشروط العامة لما يمكن أن يمثل أساسا لتأكيد الثقة فيه، فإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل

الإلكتروني بوصفه دليلا علميا فإن دلالته قاطعة بشأن الواقعة المستشهد به عنها، فإذا سلمنا سابقا 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 السابقة بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استنادا لسلطة القاضي التقديرية وفقا للمادة 147\2 أصول جزائية أردني، إذ سلطة القاضي في رد الدليل استنادا 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، ولاشك أن الخبرة تحتل في هذه الحالة دورا مهما في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

ونبين هنا 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 لا يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه

التشكيك في حجيته الإثباتية لكونه وبحكم طبيعته الفنية يمثل إخبارا صادقا عن الواقع، ما لم يثبت عدم صلة الدليل بالجريمة المراد إثباتها[1].

المبحث الرابع: جهاز التحقيق في الجرائم الالكترونية.

المطلب الأول: التعريف بجهاز التحقيق الجنائي في الجرائم الإلكترونية:

يجمع جهاز التحقيق بصفة عامة وجهاز التحقيق الجنائي في الجرائم الإلكترونية بصفة خاصة بين العلانية والسرية في أدائه وفي علاقته التبادلية مع الأجهزة الأخرى سواء محلية أو أجنبية عامة أو خاصة وكذا مع الناس بمختلف تركيباتهم ونظمهم الاجتماعية والثقافية والدينية والاقتصادية والجنائية والسياسية.

يتكون هذا الجهاز من أفراد بمختلف إمكاناتهم ومستوياتهم التنظيمية وإمكانية تقنية من أجل الحد من الجريمة عامة والإلكترونية خاصة وضبطها.

الهدف من هذا المبحث هو التعريف بجهاز التحقيق في الجرائم الإلكترونية عن طريق بيان بعض أساسياته وتطبيقاته، وبذلك يكون لديك فكرة مبسطة عن هذا الجهاز في النظم المقارنة ويكون مشجعا لك لمزيد من المعرفة عما يجب أن يكون عليه السلوك الإداري والقانوني عند التحقيق وضبط الدليل الإلكتروني.

[1] خالد عياد الحلبي ، مرجع سابق ، ص 252.

1-تعريف جهاز التحقيق في الجرائم الإلكترونية:

جهاز التحقيق في الجرائم الإلكترونية هو عبارة عن الوظائف المتخصصة إلكترونيا وقانونيا والتي يصدر بها قرار إداري وتشغل بنوعين من الأفراد : النظاميين (ضباط، ضباط صف) والمدنيين وتحكم علاقتهم الوظيفية التسلسل النظامي للرتب العسكرية وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية الإلكترونية الرقمية ونظمها وبرامجها وشبكاتها.

جهاز التحقيق في الجرائم الإلكترونية "جهاز جديد":

أصبحت الجرائم الإلكترونية في عصر التقنية الإلكترونية أربعة أنواع: جرائم الاعتداء على النفس والمال، وجرائم الاعتداء على المصلحة العامة، والجرائم الإلكترونية الرقمية المعلوماتية) بعد أن كانت ثلاثة أنواع فقط.

2-أسباب إنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية:

يرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية إلى تحقيق الضبط الاجتماعي الإلكتروني حماية للمجتمع من الجرائم الإلكترونية، وذلك للحد

منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة قبل مرتكبيها[1].

ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد وضح أن تقنية المعلومات ستزيد التفاعل بين الإرهابيين ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شبكيا سيكون هنالك مدخل للمعلومات والتقنية والتمويل وللخداع المعقد وتقنيات الأفكار الهدامة، وإذا تم استخدام ذلك سواء عن طريق الدول أو فاعلين غير دوليين سيصبح ذلك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول.

ومما يؤكد ذلك ما يلي:

- تمكن طالب جامعي سويدي من تعليق خدمات هاتف الطوارئ في منطقة كبيرة من ولاية فلوريدا في أوائل عام 1999م.

- عجز مصرف فيرست ناشونال بانك أوف شيكاغو عن فعل أي شيء وهو يشاهد تحويل 65 مليون دولار من حسابات عملائه باستخدام تعليقات إلكترونية مزورة.

- عطل شخص شبكة المراقبة الجوية في مطار "دوستر" الصغير في ولاية "ماشوستش".

[1] محمد مصطفى موسى: التحقيق الجنائي في الجرائم الالكترونية،مرجع سابق.ص 286-287.

وعلى ذلك يمثل استخدام شبكات المعلومات في ارتكاب الجرائم أكبر تهديد للدول من الداخل، فلقد سمح الانتشار السريع لأجهزة الكمبيوتر للمجرمين بتطوير قدراتهم الإجرامية عن طريق الحاسب الآلي وخدمات شبكة الإنترنت في الاتصال وجمع الأموال والتجنيد وجمع المعلومات بالإضافة إلى ارتكاب جرائم الاعتداء على المال والنفس.

بالإضافة إلى هذه الأسباب فإن ملامح الجهاز العصبي الإلكتروني الرقمي على مستوى الناس بدأ يتبلور، وبالتالي بدأت الجريمة الإلكترونية الرقمية في الظهور[1].

المطلب الثاني :عناصر فاعلية وكفاية جهاز التحقيق الجنائي في الجرائم الإلكترونية:

الدولة الآمنة إلكترونيا هي التي لديها جهاز تحقيق جنائي إلكتروني سريع في المعرفة وتطبيقها لجمع المعلومات وتحليلها للوصول إلى الدليل الإلكتروني في الجريمة الإلكترونية للإدانة أو البراءة.

إذا المعرفة المتخصصة وتطبيقها في سرعة وسرية هما المحققان لفاعلية التحقيق الجنائي في الجرائم الإلكترونية وكفايته، وعلى ذلك نتناول:

فرع 1: المعرفة الإلكترونية:

[1] محمد مصطفى موسى: مرجع سابق ، ص 288.

المعرفة الإلكترونية هي سر تقدم جهاز التحقيق الجنائي الإلكتروني في الألفية الثالثة، فالتنمية الإلكترونية لها متطلبات كمية خاصة مثل: المراد البشرية ممثلة في رجل الأمن والإدعاء والقضاء والمشرع والموارد المالية.

وهناك متطلبات نوعية مثل المعرفة العلمية الإلكترونية الرقمية وفي أجهزة الدول النامية تمثل المتطلبات الكمية بشكل عام حوالي 80% أما المتطلبات النوعية فلا تزيد على 20%، والعكس صحيح في أجهزة الدول المتقدمة (الغنية) مثل: ألمانيا والولايات المتحدة الأمريكية وإنجلترا[1].

فمظاهر تخلف المعرفة الأمنية الإلكترونية تتمثل في:

نسبة الأمية الإلكترونية الرقمية العالية، وانخفاض نسبة التعليم الأمني المهني الإلكتروني والمتخصص في مكافحة الجريمة عامة والتحقيق الجنائي خاصة.

*** معايير المعرفة الإلكترونية:**

يمكن أن يصنف تحقيق إلكتروني بأن لديه معرفة إلكترونية بتطبيق المعايير التالية:

- القدرة على الخلق والابتكار.

[1] محمد مصطفى موسى: مرجع سابق، ص 289.

– القدرة على اندماج أجهزة مكافحة الجريمة إلكترونيا بفاعلية التحقيق الجنائي الإلكتروني ومسايرة التطور الإلكتروني.

وعلى الأجهزة العربية لمكافحة الجريمة أن تختار ما يسمى بالإلكترونيات الرقمية الملائمة وهي التي تتلاءم مع ظروفها وعاداتها وتقاليدها وواقعها الأمني (المجرم والجريمة والأمن والقضاء).

وهذا لا يعني الإلكترونية البسيطة وحدها إنما أيضا تتضمن التكنولوجيا المتقدمة حسب الاحتياجات الأمنية التي تشمل على سبيل المثال أمن البيئة والأمن الغذائي والأمن المائي والطاقة وتغطية جميع الاحتياجات الأساسية والضرورية مع مواكبة التقدم الإنساني[1].

وتتكون منظومة العلم الأمني والتكنولوجيا من مكونين:

1– منتجو العلوم الأمنية والقانونية ممثلون في المفكرين (أعضاء هيئات التدريس في كليات الشرطة والحقوق والمعاهد الأمنية) ومنتجو التكنولوجيا.

2– المستخدمون للعلوم الأمنية مثل الدارسين ومستخدمي التكنولوجيا وهم رجال مكافحة الجريمة والناس.

*** المعرفة الإلكترونية ودور المفكرين الأمنيين:**

[1] محمد مصطفى موسى، مرجع سابق ،ص 290.

1- أول هذه الأدوار هو التواصل الوثيق بين البحث العلمي واعتبارات الأمن للحفاظ عليه واستمراره لأن الجرائم في القرن 21 ستفوق بمراحل ما شاهده الناس من جرائم في القرن 21،20، فالجرائم الفضائية ستلعب الإلكترونيات بكل أنماطها الدور الأساسي في الدول التي ستتحول إلى التقنية الرقمية في تعاملاتها.

ويلعب البحث العلمي دوره الأساسي في استحداث تكنولوجيا عسكرية جديدة يمكن أن تتحول فيما بعد إلى الحياة المدنية وتحدث في الحياة الاجتماعية طفرات واسعة تؤثر على نوعية الحياة كما رأينا كيف أن شبكة الإنترنت كانت مجرد شبكة تستخدم للأغراض العسكرية، بميزاتها ما لبثت أن انتقلت إلى عالم البنوك والشركات ثم أصبحت شبكة مدنية بالكامل يستفيد من خدماتها ملايين البشر في كل أنحاء الكرة الأرضية وبلا أي تميز وارتكبت من خلالها جرائم متنوعة[1].

وثاني أدوار المفكرين الأمنيين هي إعداد بحوث أساسية في مجال البحوث التطبيقية الإلكترونية المستندة إلى معرفة علمية مما يتطلب الإنفاق على هذه البحوث، ونقول ذلك لأن هناك ميلا لدى بعض الدول النامية للاستخفاف بالبحوث الأساسية على أساس أنها مكلفة لذلك تقول: هناك أمن غال وآخر رخيص، وتدريب غال وآخر رخيص.

[1] محمد مصطفى موسى، مرجع سابق ،ص291.

إن المعرفة الأمنية الإلكترونية في البلاد المتقدمة إلكترونيا أدت إلى إنشاء أجهزة أمنية لمكافحة الجريمة الإلكترونية على النحو الذي سنعرضه في المبحث الثاني من هذا الفصل.

على المفكرين الأمنيين أن يضعوا البحث العلمي في خدمة مكافحة الجريمة بصفة عامة والإلكترونية بصفة خاصة، ومن هنا تبرز أهمية نشر الثقافة العلمية وعقد الروابط الوثيقة بين المفكرين والمؤسسات التعليمية والتدريبية الأمنية من خلال عقد المؤتمرات.

إن المؤسسات الأمنية للتعليم والتدريب التي تعبئ طاقات الباحثين الأمنيين العلميين فيها بما يعنيه ذلك من إنتاج المعرفة العلمية وتداولها والإسهام بها في المجتمع العلمي الآمن هي المرشحة لتحقيق الأمن الإلكتروني في القرن الحادي والعشرين.

*** المعرفة الإلكترونية سبب جرائم الألفية الثالثة:**

في القرن 21 من سيملك السلطة؟

الإجابة: سيملك السلطة من يملك المعرفة ![1]

سؤال طرحه وأجاب عليه المفكر الأمريكي إلفين توفلر.. والمعرفة التي يقصدها تعني البيانات والمعلومات والصور والأفكار والمواقف والقيم المختلفة للمجتمع والوسائل التي تنقلها.

[1] محمد مصطفى موسى، مرجع سابق ،ص291.

يرى إلفين توفلر أن سؤالا مثل: من هي الأمة التي ستسود العالم في القرن 21 يعد سؤالا غير ذي أهمية لأنه يهمل الطامعين لسلطة الدولة كزعماء تجارة المخدرات الذين يملكون جيشا ووكالات تجسس ودوائر دبلوماسية أقوى بكثير مما تملك العديد من الدول.. أو كالجماعات الدينية المتطرفة التي تهدف أساسا إلى الاستيلاء على سلطة الدولة في كل مكان يمكنها فيه ذلك.

لكن إذا أراد أحد أن يعرف ما هو مستقبل أي أمة ومستقبل الجريمة الإلكترونية الرقمية (المعلوماتية) فعليه أن يسأل عن توزيع أجهزة الكمبيوتر (الحاسب الآلي) الرقمي والهاتف الجيل الثالث وعدد مستخدمي شبكة الإنترنت قبل أن يسأل عن الأرقام الخاصة بالإنتاج القومي.

يوجد في العالم حوالي 364.4 مليون كمبيوتر نصفها منتشر في الولايات المتحدة الأمريكية واليابان وألمانيا ولكن بتوزيع يضع الولايات المتحدة الأمريكية على رأس اللائحة، وقد جاءت هذه الدول بالترتيب: بريطانيا وفرنسا وكندا وإيطاليا والصين وأستراليا وصولا للمكسيك التي جاءت في أسفل اللائحة.

فالدول ذات التكنولوجيا المتقدمة ستواجه مشكلة خطيرة وهي انقسام الناس داخل المجتمع الواحد إلى أغنياء وفقراء معلوماتيا وهو وضع يجب اتخاذ التدابير اللازمة لتفاديه مثل التعديل الدستوري الذي أجرته تايلاند عام 1999م وبموجبه نصت المادة 87 على توفير

سبل الدخول للإنترنت على مستوى البلاد، وأيضا مثل استحداث وزارة للتكنولوجيا المعلوماتية كما حدث في الهند في تشكيل حكومتها في أكتوبر عام 1999.

فجيل التكنولوجيا الرقمية تعود على الاختيار والقدرة على الاختيار ستخلق عالما سيكون فيه سوء توزيع الاتصالات اللاسلكية أكثر خطورة من سوء توزيع المواد الغذائية ويكون فيه قضية توزيع المعلومات ووسائل الإعلام التي تنتج أكثر أهمية من قضية توزيع الثروة أو إعادة توزيعها ... وستندلع الحروب والثورات الاجتماعية والجرائم من أجل الاستيلاء على المواد الخام اللازمة للصناعة وستنتشر فيه القرصنة الفكرية وسيعاد التفكير في كل المفاهيم بصفة عامة والمفاهيم الأمنية بصفة عامة التي تبلورت في العصر الورقي في القرن العشرين[1].

***أسباب الفجوة المعرفية الإلكترونية الأمنية وطرق سدها:**

من أسباب هذه الفجوة عامة والأمنية خاصة ما يلي:

1- إن الفجوة المعرفية تتسع في تسارع متزايد بمقدار الفرق بين سرعة التقدم في العالم المتقدم وبطء حركته في العالم غير المتقدم.

2- إن ثورة الاتصالات جعلت من الكرة الأرضية كرة صغيرة تتفاعل فيها الأحداث بدون فواصل زمنية مؤثرة لحظة حدوثها في كل مكان على الأرض مهما بعد عن موقع الأحداث.

[1] محمد مصطفى موسى، مرجع سابق ،ص292.

3- إن مراكز البحث في كليات الشرطة والمعاهد التأسيسية يقوم عليها اختصاصيون عجزوا في غالب الأحيان عن مواكبة التقدم الإلكتروني الرقمي (المعلوماتي) في مجال تخصصاتهم ومازالت أبحاثهم أبحاث رد الفعل مثلهم في ذلك مثل سياسات أجهزة مكافحة الجريمة في كثير من الدول.

فمواجهته مشكلة سد الفجوة المعرفية الإلكترونية الأمنية ضرورة حياة تفرض على كل مفكر أمني أن يتحرك بسرعة لأن حل المشكلة بسيط وسهل ويتمثل في أن ينقل عن العالم المتقدم أسلوب ونظام عملهم وطرق إدارتهم له ونجاحاتهم في مجال مكافحة الجريمة الإلكترونية وهو ما نسعى إلى تحقيقه وفق مفاهيمنا وعاداتنا وتقاليدنا.

ويتطلب تنفيذ هذه الأفكار إعدادا علميا لرجل التحقيق الجنائي الإلكتروني وتدريبه على إعمال العقل ومواجهة المشاكل بعيدا عن أسلوب التلقين، كما يتطلب النظر في وحدة التعليم العام.

جهاز تحقيق جنائي إلكتروني فعال يحتاج إلى تطبيق إدارة المعرفة.

يتطلب جهاز التحقيق الجنائي في الجرائم الإلكترونية تنظيم وتقسيم المعارف الموجودة فيه وتسهيل انتقالها وتداولها بين شعبها التخصصية في مجال التحقيق، فالجهاز يحتاج إلى توثيق معرفي وهو في حد ذاته محصلة نتاج سنوات التحقيق لمن سبقوها في هذا المجال حتى يستفاد من كل عمليات التحقيق سواء كانت ناجحة أم فاشلة من خلال ما يسمى ببرامج

إدارة المعرفة الأمنية والتي تقسم المعارف الأمنية حسب أحداثها وأنواعها للتقدم للقائمين على التحقيق الميداني والمكتبي رؤية معرفية يرشد بها في التحقيق كل حسب مستوى تخصصه.

إن المعرفة الأمنية بصفة عامة والإلكترونية بصفة خاصة تنبع من رجل المكافحة (شرطة– إدعاء– قضاء– تشريع) العامل باعتباره هو المصدر الحقيقي للتجربة والعمل وبعد ذلك ينتقل إلى القسم ثم الإدارة ثم جهاز التحقيق ككل ويوثق كفكر مجرب لدى جهاز مكافحة الجريمة، تستفيد منه وتعدل عليه متى رأت تطوير أساليب التحقيق ولقد أصبحنا نرى تبادل المعرفة الأمنية سواء على المستوى العلمي أم على مستوى المكافحة مثل تسليم الهاربين[1].

إن إدارة المعرفة الأمنية هي مرحلة تحويلية واكبت التطور العالمي في الإدارة في ظل ما يسمى بالعولمة وتحرير التجارة فقفزت الإدارة فوق المعرفة وأصبحت تتحكم بها وتضبطها وفق أهدافها وإستراتيجياتها، ولقد لعبت أجهزة الأمن الكبرى مثل (F.B.I) الأمريكية دورا من خلال بناء قاعدة المعرفة وإدارتها داخل فروعها وبالتنسيق مع أجهزة الأمن الأخرى في الدول المتعاونة معها لتحقيق رؤية مشتركة في الإدارة والعمل وتطويعها لمكافحة الإرهاب مثلا فالجهاز الإلكتروني لمكافحة الجريمة بكفاية وفاعلية سيحتاج إلى رؤية وفكر معرفي أمني عالمي يمكنه من الوصول إلى البيانات والمعلومات المطلوب دون زيادة أو نقصان في الوقت الملائم دون تأخير.

[1] محمد مصطفى موسى، مرجع سابق ،ص294.

فرع 2: السرعة الإلكترونية:

يقصد بالسرعة الإلكترونية في مجال التحقيق الجنائي سرعة دوران البيانات والمعلومات من خلال شبكة الاتصالات اللاسلكية الإلكترونية الرقمية والمعلوماتية، فإن الغد سيعتمد على السرعة الإلكترونية... سرعة اتخاذ القرارات (أمنيا وإدعائيا وقضائيا)، سرعة خروج الأفكار الإلكترونية الأمنية الجديدة لمواجهة الجريمة الإلكترونية الرقمية.

والسؤال الآن ما هو المصير الذي ينتظر أجهزة مكافحة الجريمة الأقل تقدما إلكترونيا؟ أو بعبارة أخرى المبطئين ليس أمامهم كما يقول توفلر سوى زيادة سرعة إيقاعهم وردود أفعالهم لأن المبطئين من المستقبل سوف يطردون.

ويمكن القول إن العلم ينتقل بسرعة خارقة من العالمية إلى العولمة ونعنى بذلك نتيجة لثورة الاتصالات وخصوصا ذيوع استخدام شبكة الإنترنت فإنه تنشأ شبكات معلومات علمية كونية، يسهم في إمدادها بالنتائج العلمية العلماء في كل مكان وتكون متاحة لأي باحث علمي في العالم، وتكون مسرحا للأساليب الإلكترونية لشياطين الإنس[1].

بالإضافة إلى ذلك ونظرا لأن الاتصال من خلال البريد الإلكتروني والانضمام إلى جماعات النقاش فإن الاتصال السريع والفوري والمستمر بين العلماء يؤدي إلى حالة جديدة من التراكم المعرفي والعلمي غير المسبوق.

[1] محمد مصطفى موسى، مرجع سابق ،ص 299/298.

لذلك ليس من وسيلة إلا بتحويل مجتمعاتنا لتصبح مجتمعات معلوماتية عامة بما فيها أجهزة مكافحة الجريمة.

***معايير مؤشر جهاز التحقيق الجنائي في الجرائم الإلكترونية:**

أولا: البنية التحتية في قطاع أجهزة الكمبيوتر:

- نسبة أجهزة الكمبيوتر الشخصية لكل فرد يكافح الجريمة (رجل أمن – إدعاء – قضاء– تشريع).

- نسبة أجهزة الكمبيوتر الشخصية المكتبية لكل مكتب في الجهاز الإلكتروني لمكافحة الجريمة.

- نسبة أجهزة الكمبيوتر الشخصية المواجهة للمؤسسات التعليمية الأمنية/ الكلية والمعاهد والطلاب.

- الإنفاق على البرامج والأجهزة.

ثانيا: البنية التحتية في قطاع المعلومات:

- نسبة خطوط الهاتف لكل مكتب.

- نسبة أعطال الهاتف لكل خط.

- تكلفة المكالمة المحلية.

– نسبة اقتناء الهاتف المحمول (الجوال) لكل فرد يكافح الجريمة (رجل أمن – إدعاء قضاء تشريع).

– نسبة اقتناء التليفزيون لكل رجل تحقيق.

– نسبة اقتناء القنوات الفضائية لكل رجل تحقيق.

– نسبة اقتناء الفاكس لكل رجل تحقيق.

ثالثا: البنية التحتية في قطاع الإنترنت:

– عدد مستخدمي الإنترنت مكتبيا في جهاز التحقيق الجنائي الإلكتروني.

– عدد مستخدمي الإنترنت تعليميا في مؤسسات مكافحة الجريمة التعليمية (معاهد تدريب الضباط، المعاهد القضائية لتدريب رجال الإدعاء والقضاء والدفاع)[1].

***جهاز تحقيق جنائي إلكتروني بسرعة البرق... يتطلب نظاما عصبيا رقميا:**

يجب أن تكون وظيفة التكنولوجيا الرقمية وشبكاتها مثل وظيفة الجهاز العصبي داخل جسم الكائن الحي، فالجهاز العصبي البيولوجي هو شبكة اتصالات فائقة الحساسية والسرعة بجسم الكائن الحي، يقوم بإثارة استجاباته وسلوكياته اتجاه ما يدور حوله ويجعله يتفاعل بسرعة مطلقة مع الخطر والاحتياجات والفرص أو مع الآخرين ويعطيه المعلومات التي

[1] محمد مصطفى موسى، مرجع سابق ،ص300.

يحتاجها، حينما يقوم بتأمل الموضوعات الأمنية وتحديد الاختيارات ويجعله –دائما– متيقظا متنبها لمعظم الأشياء المهمة، ويقوم باستبعاد المعلومات غير المهمة بالنسبة له.

بهذا المفهوم نفسه يجب أن تلعب الحاسبات وأجهزتها الرقمية وشبكاتها دورها في جهاز المكافحة الجديد وهو يقدم خدماته العصرية المتطورة على كل مستويات، الجهاز (موديل الألفية الثالثة) سواء الفني أو التنظيمي أو مستوى الجهاز ككل، فهي لابد أن تصبح نظاما عصبيا قادرا على توفير اتصالات في غاية السرعة والكفاءة وعلى الاستجابة السريعة للحوادث الطارئة، وتوفير معلومات ذات قيمة حقيقية بسرعة مطلقة وفي الوقت المناسب لمن يحتاجها داخل جهاز مكافحة الجريمة، وتوفير الدعم اللحظي اللازم لاتخاذ قرارات سريعة سليمة ذات تأثير كالتفاعل بين رجال الأمن والمواطنين ومقدمي الخدمات في اجهزة الأمن المختلفة والمتعاملين معها كالمرور ومصلحة وثائق السفر والأحوال المدنية وغيرها.

لذلك يجب توفير النظام العصبي الرقمي كبنية أساسية لجميع مجالات المكافحة لتصبح المكافحة الإلكترونية هي السائدة، وبذلك نكون بصدد سرعة تفكير باستخدام النظام العصبي الرقمي.

***الملامح الرئيسية لجهاز التحقيق الجنائي الإلكتروني ذي النظام العصبي الرقمي:**

إن التغيير الذي سيطرأ على عالم الأعمال خلال السنوات العشر المقبلة سيفوق ما طرأ من تطور خلال السنوات الخمسين الماضية، فإن العقد الأول من القرن الحالي سيركز على

السرعة الفائقة (مثل الفيمتو ثانية) في تبادل المعلومات والنفاذ إليها بمعدلات ستغير جذريا من طبيعة أو نمط حياة الناس وتوقعاتهم من عالم الأعمال ومن ثم فإن عالم الأعمال ككل سيتعرض لتغيرات مستمرة وسريعة بالدرجة نفسها مما سيؤدي لظهور الجهاز الإداري أو الحكومي أو الخدمي مثل جهاز الأمن الذي يستجيب لهذه التغيرات خلال ساعات بدلا من أيام وأسابيع وشهور كما يحدث الآن، وقد يكون هذا التغيير في صورة تعديل لمواصفات منتج، أو بدء خدمة جديدة أو تغيير في إستراتيجيات التعامل مع الناس.

فقد أمكن لأول مرة تخزين كل أنواع المعلومات: الأرقام والبيانات والأصوات والصور ومعالجتها واسترجاعها بشك مشترك وسهل اعتمادا على تكنولوجيات التخزين الرقمي.

وللمرة الأولى أوجدت الأجهزة والمعدات العادية المصحوبة بالبرمجيات كيانات على مستوى يمكنها من إنجاز حلول قوية جدا ومتاحة بأسعار معقولة، وثورة المعالجات الدقيقة أعطت الحاسبات الشخصية الفرصة لإنتاج جيل جديد من الأدوات الشخصية الكمبيوترية كالحاسبات الشخصية المخصصة للسيارات والكروت الذكية وغيرها من الأجهزة الأخرى على الشكل الذي ظهر وانتشر بفعل التخزين الرقمي[1].

***مراحل تحويل جهاز التحقيق الجنائي والإلكتروني إلى جهاز ذي نظام عصبي رقمي:**

[1] محمد مصطفى موسى، مرجع سابق ،ص301.

الدولة الآمنة في ظل التقنية الإلكترونية الرقمية: هي التي تكون لديها أجهزة تحقيق جنائي إلكتروني في سرعة البرق لجمع المعلومات وتحليلها لاتخاذ القرارات وصدور الأحكام في الوقت المناسب ورد الفعل الملائم.

فهي في حاجة إلى جهاز تحقيق ذي نظام عصبي رقمي، ويحتاج الأمر تنفيذ ثلاث مراحل:

المرحلة الأولى: المعرفة بالعمل الإلكتروني الرقمي وضم خمس خطوات:

1- الإصرار على أن يكون تدفق الاتصالات عبر المنشأة من خلال البريد الإلكتروني ووسائل الاتصال الأخرى (حسب مدى سرية الموضوع) حتى يمكن التعامل مع الأخبار والمعلومات الجديدة دائما بسرعة كافية.

2- دراسة البيانات الجديدة –الجرائم- لحظيا لمعرفة الأساليب الجدية لسلوك المجرمين، وزمان ومكان الجرائم بسهولة وفهم الظواهر الإجرامية واتجاهات الجريمة وتفصيل أساليب المكافحة الأمنية حسب كل مجرم وجريمته وإعداد الخرائط الإلكترونية للتنبؤ بالسلوك الإجرامي.

3- استخدام الحاسبات الإلكترونية الرقمية الشخصية في تحليل الأعمال الأمنية وتحويل معارف رجال المكافحة إلى مستويات عليا من العمل المفكر الخلاق حول مكافحة المجرم والجريمة والخدمات الأمنية الأخرى.

4- استخدام الأجهزة والأدوات الإلكترونية الرقمية (التي ظهرت في الأسواق والتي ستظهر في المستقبل) في تشكيل فرق عمل مؤقتة من أي عدد من الإدارات داخل جهاز المكافحة يمكنها المشاركة في المعارف وبناء أفكار منهم في الوقت المناسب واستخدام النظم الرقمية في أرشيف جهاز المكافحة (تسجيل جنائي –مرور- وثائق السفر – الأحوال المدنية- مكافحة المخدرات والآداب...إلخ).

5- تحميل جميع العمليات الورقية إلى عمليات إلكترونية رقمية... والتعامل معها جنبا إلى جنبا، وإزالة أية اختناقات إدارية وتحرير معارف رجال مكافحة الجريمة وتوجيههم من أجل المهام الأكثر أهمية.

المرحلة الثانية: تنفيذ وأداء الأعمال الإلكترونية الرقمية وتضم أربع خطوات:

1- استخدام النظم الرقمية في تلقي البلاغات والشكوى وتدويرها فوريا إلى المختص الذي يمكنه التحقيق الجنائي في سرعة.

2- إيجاد رد فعل رقمي لتحسين الكفاءة للعمليات الأمنية الجارية وتحسين التحقيق الجنائي والخدمات وأن يكون من السهل على كل رجل مكافحة تتبع كل وسائل القياس والتقويم (الإدارة بالأهداف).

3- استخدام الأدوات الرقمية للقضاء على المهام ذات الهدف الواحد او تغييرها إلى مهام ذات قيمة تستخدم المهارات الناشئة عن معارف رجال مكافحة الجريمة.

4- استخدام الاتصالات الرقمية لإعادة تحديد طبيعة الأعمال وطبيعة الحدود بين كل مهمة أمنية وأخرى.

المرحلة الثالثة: خاصة بالأمن والإدعاء والقضاء والدفاع والتشريع: وتضم ثلاثة أمور:

1- المعلومات التي يمكن من خلالها تخفيض الدورة الزمنية باستخدام المعاملات الرقمية مع المواطنين وتغيير عمليات الأعمال الأمنية في التوقيت المناسب (السرعة).

2- استخدام التوزيع الرقمي للخدمات الأمنية مثل بطاقة الأحوال المدنية للمواطنين وبطاقة الإقامة للأجانب للقضاء على الوسطاء (مثل المعقب في النظام السعودي) في معاملات العملاء[1].

3- استخدام الأدوات الإلكترونية الرقمية لمساعدة المتعاملين مع جهاز مكافحة الجريمة على حل مشكلاتهم بأنفسهم وتوجيه الاتصالات الشخصية لحل المشكلات المعقدة التي تمثل قيمة عالية للمتعامل مع أجهزة مكافحة الجريمة عامة وجهاز الأمن خاصة.

4- هل الأجهزة العربية لمكافحة الجريمة مهيأة للمكافحة في زمن الحاسب الآلي وشبكات المعلومات؟!

[1] محمد مصطفى موسى، مرجع سابق ،ص304.

يبدو الأمر صعبا في ظل الظروف الحالية، والأمر لا يتطلب فقط حيازة الأجهزة الإلكترونية الرقمية وبناء النظم ولكنه يحتاج أيضا إلى تغيير جذري في طرق التفكير واتخاذ القرار، والتعامل مع المعلومات على كل المستويات وإعطاء أهمية قصوى لعامل الزمن (التاريخ DATA والوقت) في اتخاذ القرار وصدور الأحكام وقناعة مطلقة بالأهمية البالغة لتوفير مناخ يسمح بدوران كل البيانات والمعلومات بين أطرافه المختلفة دون عائق.

لذلك بدأت وزارة العدل بتطوير مقار محاكمها وأبنيتها وأبنية النيابة العامة والشهر العقاري وتزويدها بالتكنولوجيا الإلكترونية وأجهزة الحاسب الآلي الرقمي المتصلة بشبكات مركز المعلومات بوزارة العدل ومحكمة النقض لنشر شبكة المعلومات التشريعية والقضائية وتطوير وتحديث مكتبات المحاكم وتزويدها بالمراجع القانونية[1].

وفي هذا الصدد قام المركز القضائي بوضع برنامج للحاسب الآلي يتم من خلاله إدخال جميع بيانات كل قضية من واقع بطاقة بياناتها ومرافقاتها المسجلة من اسم القضية ونوعها "جناية، أو جنحة أو مخالفة" ورقمها وتاريخها ووصف التهمة وموضوعات التهم ومواد العقاب التي طبقت واسم المحكمة التي نظرت القضية ومراحل المحاكمة المعلقة من ابتدائي واستئناف ونقض وأسماء القضاة والإدعاء والأحكام التي صدرت ضدهم وأسماء المجني عليهم والمتهمين وتواريخ الحكم والتصديق والتنفيذ والأحراز المضبوطة في القضية.

[1] محمد مصطفى موسى، مرجع سابق ،ص305.

وهدف المركز من ذلك استخدام هذه القاعدة من البيانات لتدريب رجال القضاء والنيابة العامة بحيث يستطيع من خلالها التزود بالمعلومات والخبرة القضائية، وفي الوقت نفسه كأداة للتدريب لتعريفهم بالأساليب المختلفة في التحقيق الجنائي واستفادتهم مما حوته من مرافعات قيمة لكبار رجال النيابة العامة والمحامين تحقيقا للهدف الذي تنشده العدالة بارتفاع المستوى الفني والعلمي لهم.

ويمكن للمتدرب والباحث الاسترجاع مباشرة من الحاسب الآلي بدلالة أي من محددات القضية والذي يحقق السرعة العالية والمرونة في استرجاع المعلومات.

مثال ذلك: يمكن استرجاع البيانات الكاملة لقضية بذاتها بمراحل المحاكمة فيها وتطلب سواء باسمها أو رقمها[1].

والأهم من ذلك يمكن استرجاع مجموعة من البيانات على مستوى جميع القضايا كطلب بيان عن القضايا التي نظرت في محكمة بذاتها كمحكمة النقض مثلا أو بطلب هذا البيان برقم النقض أثناء فترة معينة، أو بيان عن موضوع معين للتهم والقضايا الخاصة به.

وأيضا يمكن استخراج بيان لحيثيات ومرافعات النيابة لقاض معين أو مرافعات الإدعاء والأحكام الصادرة عن قاض معين ويمكن استخراج بيان على مستوى الأحكام الصادرة بجميع هذه القضايا سواء بالإعدام أو الأشغال الشاقة المؤبدة أو المؤقتة أو بالسجن، وأيضا تتبع الأحكام الغيابية التي صدرت على بعض المتهمين وغير ذلك من البيانات.

[1] محمد مصطفى موسى، مرجع سابق ،ص 306.

إذن لكي تتعامل الأجهزة الحالية لمكافحة الجريمة مع العصر الإلكتروني الرقمي لابد من إنشاء بنية تحتية أساسية عصبية رقمية يتم فيها توحيد ومزج جميع الأجهزة والحاسبات والبرمجيات والشبكات وجميع أشكال البنية الأساسية المعلوماتية بأجهزة مكافحة الجريمة، وتغير طريقة تفكير رجال مكافحة الجريمة من خلال تطوير ثقافتهم بحيث توفر هذه البنية نظاما متكاملا تتناغم فيه التفاعلات بين كل جزء وآخر (شرطة – إدعاء– قضاء– دفاع– تشريع).

أضف إلى هذه قضية القوانين والقرارات المنظمة لجمع وتداول المعلومات والتي تحتاج إلى تعديل بما يتفق مع الأوضاع الإلكترونية التي تتطلب السرعة في جميع وتحليل المعلومات بما يخدم الاقتصاد والتجارة الإلكترونية عامة والمكافحة الإلكترونية للجريمة الإلكترونية[1].

فرع 3: السرية الإلكترونية:

يقصد بالسرية الإلكترونية في مجال التحقيق الجنائي في الجرائم الإلكترونية الأخبار والمعلومات المتعلقة بالتدابير والإجراءات التي تتخذ لكشف الجرائم الإلكترونية الرقمية أو تحقيقها أو محاكمة مرتكبيها.

فإفشاء المعلومات المتعلقة بهذه الجرائم، أو نقلها فيه ما يفيد منه الجناة أو بعضهم في الفرار من وجه القضاء أو العمل على تضييع الأدلة أو إفسادها.

[1] محمد مصطفى موسى، مرجع سابق ،ص307.

لذلك كان إضفاء السرية على أخبار تدابير الكشف عن هذه الجرائم أو تحقيقها أو محاكمة مرتكبيها لحصر نطاق هذه الجرائم وعدم إفلات الجناة فيها من القصاص.

ويتناول التعريف السابق ثلاثة أنواع من الأخبار والمعلومات يجب أن تكون سرية وهي:

1- المعلومات المتعلقة بالتدابير والإجراءات التي تتخذ للكشف عن الجرائم الإلكترونية الرقمية التي تمس أمن الدولة والوصول إلى الجناة فيها من فاعلين وشركاء ومن ذلك جمع الاستدلالات بمعرفة الشرطة أو رجال المخابرات، والتحقيق الإداري الذي يسبق تحريك الدعوى وتقديم البلاغ أو شكوى عن ارتكاب إحدى هذه الجرائم، ومن ذلك ما يقوم به رجال الشرطة بصفة عامة والمباحث ورجال المخابرات بصفة خاصة من طرق وأساليب أو حيل تستهدف إيقاع مرتكبي هذه الجرائم في قبضة القانون.

2- الأخبار والمعلومات المتعلقة بالتحقيق في إحدى الجرائم الإلكترونية الرقمية كما هو الشأن في المعلومات المتصلة بتحريك الدعوى والأمر بالقبض على أحد الجناة الإلكترونيين أو التفتيش لشخصه أو مسكنه أو حاسوبه الرقمي، المعلومات المتعلقة باستجواب المتهمين أو أقوال الشهود في أثناء التحقيق، إجراءات المعاينة والمواجهة وقرار الاتهام أو الأمر بألا وجه لإقامة الدعوى لما تتضمنه هذه القرارات عادة من تفصيلات أو معلومات مستمدة من التحقيق.

3- المعلمات المتعلقة بالمحاكمة في إحدى الجرائم الإلكترونية الرقمية بما في ذلك المرافعات والتحقيق النهائي، ويجوز للمحكمة التي تتولى المحاكمة أن تأذن بإذاعة ما تراه من مجرياتها.

***أما الأسرار الإلكترونية الأخرى فهي:**

1- المعلومات التي بحكم طبيعتها الإلكترونية لا يعلمها إلا الأشخاص الذين لهم صفة في ذلك، ويجب مراعاة لمصلحة البلاد أن تبقى سرا على من عدا هؤلاء الأشخاص ما لم يصدر إذن كتابي من الجهات المختصة بنشره أو إذاعته.

2- الأشياء والديسكات والأسطوانات الليزر وغيرها من المكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات والصور وغيرها سواء كانت ورقية أم رقمية من الأشياء التي يجب لمصلحة البلاد ألا يعلم بها إلا من يناط بهم حفظها أو استعمالها والتي يجب أن تبقى سرا على من عداهم خشية أن تؤدي إلى إفشاء المعلومات.

***الأسرار بين السرية والتسريب الموجه... تكتيك معلوماتي:**

وقع في 1967/7/4 الرئيس الأمريكي ليندون جونسون في البيت الأبيض "قانون حرية المعلومات وبهذه المناسبة ألقى كلمة قال فيها "حرية المعلومات من الحيوية بحيث لا يجوز تقييدها إلا لدواعي الأمن القومي، وليس لرغبات مسؤولي الدولة أو المواطنين".

وفور انتهائه من كلمته طلب منه أحد الصحفيين الحصول على نسخة من المسودة الأصلية لتلك الكلمة، وكان هذا أول طلب يقدم في ظل القانون الجديد للحريات.

ورفض الرئيس ليندون جونسون الطلب ببرود.

فتكتيك السرية من أقدم تكتيكات المعلومات بصفة عامة والأمنية خاصة وأكثرها انتشارا وهي مسألة نسبية لدى الدول.

فمعرفة كيف ومتى تستخدم السرية هي إحدى فعاليات جهاز مكافحة الجريمة فالسرية هي التي تتيح إمكانية استخدام تكتيك المعلومات الآخر ألا وهو التسريب الموجه للمعلومات، فبعض الأسرار تظل كذلك وبعضها يتم تسريبه وعندما يتسرب سر بشكل غير مقصود فمعنى ذلك أنه سر لم يحسن كتمانه[1].

المطلب الثالث: قضايا حول إثبات بعض الجرائم الالكترونية

[1] محمد مصطفى موسى، مرجع سابق ،ص308.

القضية الأولى: "المكان نيويورك– الولايات المتحدة الأمريكية":[1]

– المتهم "أوليفر جوفانوفيك"، خريج جامعة كولومبيا في نيويورك.

– التهمة: اختطاف طالبة وإساءة استخدامها جنسيا.

– العلاقة بين المتهم والمجني عليه: صداقة نشأت عبر الإنترنت.

– ملخص القضية: في أبريل 1996م قام المتهم بالتحضير لمقابلة المجني عليها عبر رسائل إلكترونية ثم وجه لها دعوة لمشاهدة أفلام مسجلة على الفيديو، عند وصول الفتاة قام المتهم باحتجازها لمدة 20 (ساعة) واعتدى عليها جنسيا بطريقة وحشية مع الضرب والحرق والتعذيب، والتهديد بتقطيع أوصالها، لقد لعب الإنترنت دورا في ارتكاب الجريمة كأداة للتواصل والتعارف ونقل الدعوة بعد تهيئة الضحية نفسيا، وفي نفس الوقت لعب الإنترنت دورا رئيسيا في حفظ الأدلة الرقمية المضمنة في رسائل البريد الإلكتروني.

في مرحلة المحاكمة لم يتمكن الاتهام من استخدام معظم الأدلة الرقمية المتوفرة في البريد الإلكتروني للمتهم لعدم ضبطها بالطرق المشروعة، كما حرم الدفاع من استخدام الأدلة الرقمية المخزنة في البريد الإلكتروني للمجني عليها لأن قوانين نيويورك تمنع كشف بعض المعلومات الخاصة بالأفراد بما في ذلك التحقق من الشخصية أو كشف تاريخها الجنسي.

[1] محمد الأمين بشري ، مرجع سابق ، ص143.

أخذت المحاكمة اهتمام أجهزة الإعلام وأصبحت منفذا لإثارة مفهوم الجريمة الجنسية التخيلية، مما أثر على نتائج المحاكمة، ورغم نقص الأدلة التي قدمتها المجني عليها حكمت المحكمة على "جوفانوفيك" بالسجن لمدة (15) عاما.

تكشف هذه القضية كيف أن الإنترنت لعب دورا في جريمة عنف تقليدية من حيث الإعداد لها وتنفيذها ومحاكمتها وإثارة الرأي العام حولها، وتشير وقائع القضية إلى الكم الهائل من الأدلة الجنائية الرقمية التي وفرها الإنترنت في أكثر من مسرح إفتراضي Virtual Scene of crime إلا أن القوانين المحلية القديمة السابقة لعصر الإنترنت وقفت دون استخدام تلك الأدلة لكشف الحقائق، كما أن جهل رجال التحقيق بالإجراءات القانونية الخاصة بضبط الأدلة الرقمية كان سببا في الإضرار بالعدالة.

القضية الثانية[1]:

- المكان: "قرين فيلد" كاليفورنيا – الولايات المتحدة الأمريكية.

- المتهم: "رونالد ريفا"

- التهمة: التحرش الجنسي.

- العلاقة بين الجاني والمجني عليها: التقى الجاني بالمجني عليها في حفل ترفيهي نظمته ابنته لأصدقائها وصديقاتها.

[1] محمد الأمين بشري ، مرجع سابق ، ص135.

– ملخص القضية: في عام 1997م، قام المتهم وصديقه "ملتون ريفا" بالتقاط صور فاضحة للمجني عليها ولفتاة أخرى تبلغ من العمر (10) سنوات، قاد التحقيق مع المتهمين إلى حلقة دولية تعرف باسم "أورشد" تعمل في الإتجار بالصور الفاضحة للأطفال واستغلالهم جنسيا عبر الإنترنت، وذلك من خلال غرف النقاش تم توجيه تهم إلى (16) رجلا من فنلندا، كندا، الولايات المتحدة وأستراليا، بفحص المعلومات الرقمية المخزنة في البريد الإلكتروني تم العثور على اعترافات للمتهمين يصفون فيها أنشطتهم تجاه الأطفال وطريقة إغوائهم للأطفال والتقاط الصور العارية لهم، بعد عامين من التحقيق توصل المحققون في النهاية إلى مجموعات من المجرمين تعمل في حلقة دولية تطلق على نفسها نادي "الوندرلاند" وتعمل في (40) دولة، تم تبادل الأدلة الجنائية الرقمية في أجهزة الحاسوب وصناديق البريد الإلكتروني بين الأجهزة المختصة لمحاكمة (200) شخص.

تكشف هذه القضية مدى إمكانية انتشار الجرائم عبر الإنترنت دون أن تكون هناك علاقة مباشرة بين الجناة، كما أن الأدلة الجنائية الرقمية، مهما طالت مدتها تظل ذات قيمة ومصداقية متى تم ضبطها وتأمينها بالطرق المشروعة والأساليب الفنية السليمة.

القضية الثالثة:[1]

– المكان: واشنطن – الولايات المتحدة الأمريكية.

[1] محمد الأمين بشري ، مرجع سابق ، ص 136

- المتهم: وكالات سرية تتبع الحكومة الاتحادية في الولايات المتحدة.

- التهمة: الإغارة على شركة خاصة بطريقة غير مشروعة، وسرقة ممتلكاتها.

- ملخص القضية: في عام 1990م، قامت وكالات سرية تتبع للحكومة الاتحادية بالإغارة على شركة "استيف جاكسون" للألعاب بحثا عن أدلة تتعلق بعصابة من المتطفلين Hackers تطلق على نفسها "لقيون دووم".

كانت شركة "استيف جاكسون" للألعاب تقوم بتصميم ونشر العاب تقوم على طرق خيالية للسطو على نظام الحاسوب، كما كانت تقوم بإصدار نشرة دورية لتقديم خدمات البريد الإلكتروني لعملائها، قامت الوكالة الاتحادية بمصادرة جميع أجهزة الحاسوب وملحقاته ونسخ من كتاب تحت الطبع، ولم توجه تهم جنائية لشركة "جاكسون"، إلا أنها تعرضت لخسائر مالية كبيرة.

بعد فشل العديد من المحاولات الرامية لاسترداد الأشياء المصادرة قررت الشركة مقاضاة الوكالة السرية الحكومية بتهمة الاعتداء على مقر الشركة وسرقة ممتلكاتها.

وضح أثناء المحاكمة أن موظفي الوكالة الحكومية قاموا بمحو رسائل بريدية خاصة لم تكن قد سلمت لأصحابها، وقد أنكرت الوكالة التهمة، لصعوبة التعامل الفني مع الأدلة الجنائية الرقمية سحبت الشركة التهم الجنائية، ومع ذلك حكمت المحكمة بإدانة الوكالة تحت

قانون سرية الاتصالات الإلكترونية وقانون حماية الحريات الشخصية وقررت تعويض الشركة بمبلغ (300) ألف دولار مقابل الأضرار التي لحقت بالشركة.

تكشف القضية جوانب فنية وقانونية عديدة تتصل بالأدلة الجنائية الرقمية أهمها:

1- ضرورة الالتزام بالإجراءات القانونية في حالات التفتيش والضبط.

2- أن تتم عمليات الإغارة والضبط وتوثيق الأدلة الرقمية، مثل استرجاع الأدلة الرقمية بواسطة متخصصين.

3- ضرورة تمكين الدفاع من فحص الأدلة الجنائية الرقمية، مثل استرجاع الأدلة الرقمية التي تم محوها.

4- أهمية إلمام المحققين بالقوانين ومبادئ حقوق الإنسان.

القضية الرابعة[1]:

- المكان: لوس أنجلس – الولايات المتحدة الأمريكية.

- المتهم: -"كافين متنك"

- التهمة: السطو على نظم الحاسوب وسرقة البرامج.

[1] محمد الأمين بشري ، مرجع سابق ، ص 137.

– ملخص القضية يعتبر "مافين متنك" من أشهر مرتكبي السطو على نظم الحاسوب، بدأ "متنك" نشاطه في السبعينات في الثانية عشرة من عمره، إذ كان يمضي وقت فراغه في ممارسة هواية الاعتداء على نظم الهاتف في لوس أنجلس في عام 1981 تم إلقاء القبض عليه لأول مرة بسبب إتلافه بيانات حاسوب وسرقة دليل العمليات من إحدى شركات الهاتف.

منذ ذلك الوقت اعتاد "متنك" ارتكاب العديد من جرائم السطو على نظم الحاسوب وسرقة البرامج والمعلومات وأرقام بطاقات الائتمان، حتى تم إلقاء القبض عليه في عام 1989م بعد أن سرق برامج تقدر قيمتها بملايين الدولارات في شركة المعدات الرقمية (DEC)، وأصبح "متنك" أول من تم إدانته تحت قانون التزوير وسوء استخدام الحاسوب، حكم على متنك بالسجن لمدة عام ثم أفرج عنه لصغر سنه، اختفى "متنك"، وواصل نشاطه الإجرامي الذي أقلق المجتمع الأمريكي حتى تم القبض عليه مرة أخرى في عام 1995 وهو يحاول السطو على شبكة معلومات مكتب التحقيقات الاتحادي (FBI).

تثير هذه القضية مسألة هامة تتصل بنظرية المسؤولية الجنائية وعامل السن، بعد أن أصبح من الممكن أن يصبح الطفل (دون سن المسؤولية الجنائية) أو الشاب دون السادسة عشر، على درجة عالية من الوعي والمهارة باستخدام تقنية الحاسوب والسؤال هنا، هل يعامل صغار السن الذين يرتكبون جرائم الحاسوب وفقا لنظرية القانون الجنائي التقليدية، أم يعتبر الطفل مسؤولا جنائيا وتوقع عليه العقوبات السالبة للحرية الملائمة لجريمته؟

القضية الخامسة[1]:

- المكان: بوسطن – الولايات المتحدة الأمريكية.

- المتهم: ريتشارد رميرو.

- التهمة: السطو على متحف الفنون الجميلة.

- ملخص القضية: في 1999/3/19، قام المتهم بالسطو على متحف الفنون الجميلة وسرقة بعض الأعمال الثمينة، أوضحت كاميرات التصوير أن شخصا ملثما دخل المتحف الساعة الثامنة مساء وخرج منه الساعة الثامنة والنصف عند التحقيق مع المتهم الأساسي، أنكر التهمة مدعيا أنه كان في منزله في نيويورك على بعد مئات الأميال وقت ارتكاب الجريمة، ولتأكيد ذلك أبلغ المحققين أنه قام بإرسال رسالة إلكترونية "E-mail" لأحد أصدقائه حصل المحققون على نسخة الرسالة الإلكترونية من الصديق وكانت كما يلي:

تشير الرسالة الإلكترونية أنها بالفعل أرسلت وقت ارتكاب الجريمة مما يدل على أن المتهم كان بعيدا عن مكان الجريمة وقت ارتكابها مما يعد دليلا لبراءة Alibi، ولكن كان المحققون على دراية برسائل البريد ومحتوياتها التي تحدد آليا الوقت والتاريخ والأجهزة والوسائط التي مرت من خلالها الرسالة وكانت محتويات الرسالة التي قدمها المتهم كالتي:

[1] محمد الأمين بشري ، مرجع سابق ، ص 139.

وبالمقارنة يتضح أن المتهم قام بتزوير الرسالة الإلكترونية مساء 1999/3/20 بعد ارتكاب الجريمة.

ويلاحظ من وقائع هذه القضية ما يلي:

1- تلعب الأدلة الرقمية دورا هاما في الدفع بوجود المتهم في مكان آخر وقت ارتكاب الجريمة.

2- الأدلة الرقمية مقومات تكفل مصداقيتها مما يجعل سوء استغلالها أو تزويرها غير ممكن، طالما كان المحققون على دراية بتقنياتها الدقيقة.

3- اتساع فرص الإبداع وإمكانيات الغش والتحايل المتوفرة في تقنيات الحاسب الآلي يدعو إلى اليقظة والتعامل بذكاء مع الأدلة الجنائية الرقمية.

القضية السادسة[1]:

- المكان: واشنطن – الولايات المتحدة الأمريكية.

- المتهم: العقيد "أليفر نوارث"

- التهمة: الاتجار غير المشروع في الأسلحة.

[1] محمد الأمين بشري ، مرجع سابق ، ص 141.

– ملخص القضية: في الثمانينات اتهم عقيد جهاز المخابرات الأمريكية C.I.A "أليفر نوارث" بالاتجار غير المشروع في الأسلحة في القضية الشهيرة المعروفة بـ "إيران كونترا"، ورغم أن العمل الذي قام به المتهم في إطار مسؤولياته الاستخباراتية إلا أن بعض التجاوزات جعلته عرضة للمساءلة الجنائية.

لم تتوفر للاتهام أدلة مادية أو معنوية يقدمها ضد المتهم خاصة والجريمة قد ارتكبت من خلال عمليات على درجة عالية من السرية الاستخباراتية، وضح للمحققين أن المتهم كان حريصا على إتلاف الوثائق ومحو جميع الرسائل الإلكترونية في جهاز الحاسوب الخاص به، ولكن –وبدون علمه– كانت جميع الرسائل الإلكترونية الحكومية وشبه الحكومية تحفظ يوميا Backed up بنظام خاص يعرف بنظام آي.بي.إم للمكاتب المهنية IBMProfessional Office System وقد جرى استرجاع تلك الرسائل من المحفوظات واستخدامها في إدانة الملف.

تعكس هذه القضايا، ما تتميز به الوثائق الرقمية من إمكانيات الحفظ والاسترجاع، ورغم كثافة المعلومات والبيانات الحكومية وشبه الحكومية الخاصة بدولة في حجم الولايات المتحدة الأمريكية من الممكن رصد حركة جميع المعاملات الإلكترونية مهما كانت قيمتها والرجوع إليها بيسر عند الحاجة.

خاتمة

خاتمـــة :

تعد هذه الدراسة حصيلة جهد قمنا به بهدف التصدي لهذا الموضوع ذو الصبغة العلمية المستحدثة على رجال القانون ،غير أنه لا يجب أن يكون هذا الطابع العلمي عقبة تمنعنا من التوسع في قاعدة النقاش حول الإجرام ألمعلوماتي ؛ و حتى لا يبق موضوع الجريمة المعلوماتية من المناطق المحرمة التي يتجنب معظم الباحثين و دارسي القانون الخوض فيها.

لا ننكر الصعوبة التي واجهتنا لانجاز هذه الدراسة نظرا لنقص المراجع في هذا الميدان و نظرا لضرورة إلمامنا بالجوانب التقنية حتى نتمكن من الإحاطة بالجوانب القانونية ،إلا أن ذلك لا يمنع أننا توصلنا في ختام دراستنا لهذا الموضوع إلى عدة جوانب يمكن بلورتها فيما يلي :

النتائـــج :

1- هناك قناعة عامة بوجود مخاطر أمنية متزايدة للجرائم التخيلية Cyber crime، فهي ليست قاصرة على جرائم الحاسب الآلي والإنترنت، بل تمتد لتصبح عنصرا أو أداة في مختلف أنماط الجرائم التقليدية والمستحدثة، فالجرائم التخيلية بالإضافة إلى الخسائر المالية الكبيرة التي تسببه لمؤسسات القطاع العام والخاص، أصبحت تلحق أضرارا بالغة بالمجتمعات المحافظة، ولعل من مقتضيات مواجهة هذه الظاهرة الإعداد العلمي لأجهزة العدالة الجنائية وتزويدها بالمعرفة الفنية والقانونية ذات العلاقة بهذا النوع من الجرائم.

2- مع تزايد أنماط الجرائم التخيلية تتضاعف حالات لجوء المحققين ورجال الشرطة والقضاء إلى خبراء الحاسوب والإنترنت للاستعانة بهم في كشف غموض المعلومات والأدلة الجنائية الرقمية الآخذة في الانتشار، ولكن مع مرور الزمن سوف تصبح الأدلة الجنائية الرقمية جزءا أو عنصرا من عناصر الجريمة بمختلف أنواعها، عندئذ لن يتمكن خبراء الحاسب الآلي والإنترنت من تقديم العون لأجهزة العدالة الجنائية، الشيء الذي يقتضي الشروع في إعداد رجال الشرطة والنيابة العامة والقضاء بالكيفية التي تمكنهم من التعامل مع الأدلة الجنائية الرقمية، والتي لا غنى عنها.

3- تعتبر الأدلة الجنائية الرقمية من أكثر أنواع الأدلة المادية وفرة وثباتا، وهي مخزنة في الأجهزة الرقمية المختلفة أو منقولة عبر شبكات الاتصال وتشكل ثروة للعدالة الجنائية متى أحسن استغلالها.

4- للأدلة الجنائية الرقمية حجية في الإثبات أمام المحاكم المدنية والجنائية، لما لها من أسس علمية مؤهلة نالت بها الثقة والمصداقية، فالنظرية الرقمية مصدرها علم تقنية المعلومات الذي فرض نفسه على الإنسان بإنجازاته الملموسة.

5- يتطلب التعامل مع الأدلة الجنائية الرقمية معرفة تامة بأصولها ونظرياتها وتقنية المعلومات، كما يتطلب مبادئ جديدة للبيئة وتشريعات تنظم إجراءات جمع وتأمين هذا النوع من الأدلة، بالقدر الذي لا يتعارض مع الحقوق الدستورية وسرية المعاملات الفردية.

6- تتجه المختبرات الجنائية الحديثة نحو استخدام التقنية الرقمية في التعامل مع الأدلة المادية المعروفة كالبصمات، الآثار البيولوجية وغيرها، عليه من باب أولى الاتجاه نحو تطوير استخدامات الأدلة الجنائية الرقمية باعتبارها أداة المستقبل لتحليل الأدلة المادية.

7- ان الأدلة الرقمية المستخلصة من أجهزة الكمبيوتر، ما هي إلا تطبيقات الدليل العلمي الذي يتميز بالموضوعية، والحياد والكفاءة في إقناع أجهزة إنفاذ وتطبيق القانون.

8- إذا كان تقدير أجهزة إنفاذ وتطبيق القانون في التشريعات اللاتينية لا تتناول القيمة العلمية القاطعة للدليل باعتبار علميته وموضوعيته وحياده وكفاءته، فإنها يمكنها أن تناقش الظروف والملابسات التي وجد فيها هذا الدليل، وذلك على خلاف التشريعات الأنجلو سكسونية، حيث يقوم المشرع بالدور الإيجابي في عملية الإثبات بالدعوى فهو الذي ينظم قبول الأدلة وينحصر دور القاضي في مراعاة توافر الأدلة وشرائطها القانونية بحيث إذا لم تتوافر لا يجوز أن يحكم بالإدانة بل يحكم باستبعاد الدليل، وفي هذا الصدد لا يتم قبول مستخرجات الكمبيوتر المستخرج منه وكان القائم عليه تتوافر فيه الثقة والاطمئنان.

9- الوسائل العلمية وإن كانت تفيد في مهمة الكشف عن الحقيقة الغائبة، إلا أنها قد تعصف بحريات وحقوق الأفراد إذا لم يحسن استخدامها ولذلك يجب مراعاة الأحكام القانونية عند استخلاص الأدلة العلمية حتى يمكن قبولها.

10- يتوقف استخدام تقنية الأدلة الجنائية الرقمية على الآتي:

أ- إنشاء مختبرات الذكاء الاصطناعي Artificial Intelligence Laboratory وتعميم الاستفادة منها للتعامل مع الأدلة الجنائية الرقمية.

بـ- جعل ثقافة الأدلة الرقمية جزءا من تدريب وتكوين رجال تنفيذ القوانين وخاصة الشرطة والقضاء.

جـ- تعزيز التشريعات المنظمة للتعامل مع الأدلة الجنائية الرقمية.

د- تحقيق التعاون والتنسيق بين أجهزة العدالة الجنائية وشركات تقنية المعلومات.

هـ- توعية الجمهور بدور الأدلة الجنائية الرقمية في تحقيق العدالة الجنائية.

و- أن يتم استخلاص الدليل ضمن ضمانات قانونية إجرائية تضمن سلامة وصحة ودقة هذا الاستخلاص.

ز- أن يتم التأكد من حجية هذا الدليل بإجراء اختبارات الثقة، والتي تشمل ثلاثة عناصر الأول القائم على استخراج الدليل والثاني الجهاز المستخدم والثالث التطبيقات المقارنة.

كـ- إذا اجتاز الدليل اختبارات الثقة أصبح ذا حجية قضائية.

م- أن يتم استخلاص الدليل طبقا لمبادئ المشروعية الإجرائية والقانونية.

وعلى ذلك إذا استوفى الدليل الرقمي الشروط الموضوعية اعتماده كدليل قضائي، انحصر دور أجهزة إنفاذ وتطبيق القانون في بحث مدى الملائمة الموضوعية لظروف استخراجه واستخلاصه فقط.

المقترحـــات

مقترحات وتوجيهات عامة لأجهزة إنفاذ القانون لضبط الأدلة الرقمية في بروتوكولات النقل والاتصالات والشبكات:

1- في مرحلة التعرف على الأدلة:

أ- يتم تشغيل الكمبيوتر محل الاشتباه ويبدأ بالبحث عن ملفات الولوج في كل من الأجهزة المستخدمة في التشغيل والاستضافة Hostess ويشمل ذلك خدمات الشبكات وخدمات الملفات والمسارات، وبرامج الحماية وكذلك في بروتوكولات تعريف المضيف ديناميكيا DHCP.

ب- يتم فحص جداول الحالة التشغيلية "State Tables" في الأجهزة محل الاشتباه.

2- مرحلة جمع وتوثيق وحفظ الأدلة:

أ- يتم الاحتفاظ بمفكرة معلومات لتساعد على تذكر التفصيلات المتعلقة بإعادة بناء الأدلة الرقمية حتى التفصيلات المهمشة التي قد تبدو في أول وهلة أنها بلا معنى فقد يتضح أن لها أهمية ومعنى لاحقا.

بـ- تتم ملاحظة التاريخ والوقت المدون في الكمبيوتر والتاريخ والوقت الذي بدأ فيه إجراء عملية البحث والتحقيق ومحاولة إيجاد الفروق بينها.

جـ- يتم طبع التوقيع الخاص بـ IP وتاريخ كل صفحة من صفحات الويب للحفظ في دولاب الأدلة الرقمية.

د- يتم إعداد قائمة بجرد كل الأدلة الرقمية التي تم الحصول عليها في الديسك الخاص بالفاحص مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في كمبيوتر آخر للتأكد من سلامة القائمة.

هـ- يتم إعداد نسختين من كل الأدلة لمواجهة عطب إحدى النسخ حتى تكون النسخة الأخرى صالحة للاستخدام.

و- في الأحوال التي لا يكون مصرحا فيها بجمع كافة الملفات في الولوج، حينئذ يتم جمع الرسائل الرقمية لكل الملفات ونسخ صورة منها للحفظ حتى يتم الحصول عل التصريح القانوني اللازم.

ز- يتم تصوير الشاشة والأجهزة المتصلة بها وكافة الأجهزة الأخرى والاحتفاظ بهيكل ذلك في الملف الجنائي الخاص بالواقعة الجنائية.

ح- يتم جمع البرامج التي قد تكون استخدمت في ارتكاب الجريمة ويتم تشغيل هذه البرامج مثل أي برنامج آخر مع الاحتفاظ بهذه البرامج في ملف الواقعة الجنائية.

3- مرحلة التعرف والمقارنة:

أ- يتم جمع الملفات الخاصة بالمشتبه فيه سواء ملفات الولوج أو الجداول التشغيلية مع ملاحظة أوقات الدخول والرسائل الرقمية للملفات.

ب- يتم اختبار كل ملفات الولوج وجداول الحالة التشغيلية بكل عناية ممكنة لتحديد المعلومات المطلوبة من الفحص سواء أكانت تخص المتهم أو شخصا آخر.

ج- تتم المقارنة بين برامج تشغيل النظام وأوامره مع البرامج والنظم المعتمدة،، وإيجاد الفرق بينها مع إجراء مقارنة بين المعلومات الخاصة بملفات الولوج وجداول الحالة التشغيلية مع جداول وملفات مشابهة وإيجاد الفروق الشخصية الدالة على الشخص، حيث إن لكل فرد ظروفه وشخصيته ومعلوماته التي تخصه مثل الحاسب المالي، شكل الصفحات التي يقوم بتصفحها وهكذا.

د- يتم البحث عن أي برامج أخرى قد تكون لها علاقة بالجريمة أو المجرم يتم مقارنتها بالأصل وإيجاد الفروق الشخصية المميزة للمشتبه فيه.

4- مرحلة إعادة بناء الأدلة:

أ- يتم إعداد بناء حزم المعلومات في شكل متكامل.

بـ- يتم استكمال المعلومات المخزنة أو التالفة، وذلك بالبحث في بقايا الآثار المعلوماتية التي يمكن أن تفيد وذلك باستخدام البرامج المخصصة لذلك.

جـ- يتم تخيل بانوراما للجريمة مع جميع كافة الأدلة وتحديد أين يمكن أن تكون وما هي تلك الأدلة التي لها علاقة بالجريمة، وما هو غرض كل دليل وكيف يعمل وكيف استخدم ومتى استخدم وما هو الكمبيوتر الذي استخدم فيه والأجهزة التي أجرى الاتصال بها.

قائمة المراجع :

المراجع العامة :

*أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، ط7.

*عبد الله أوهايبية: شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة للطباعة والنشر والتوزيع، 2004.

*عبد الله سليمان: شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، ابن عكنون، الجزائر.

1993.

المراجع المتخصصة:

*أحمد خليفة الملط : الجريمة المعلوماتية ، دار الفكر الجامعي ، الاسكندرية ، ط 2 ، سنة 2006.

*أمال قارة: الحماية الجنائية للمعلوماتية في التشريع الجزائري،دار هومة،الجزائر،ط1.

*الدكتور الطيب بلواضح: محاضرات ألقيت على طلبة سنة أولى ماستر قانون جنائي بجامعة المسيلة سنة 2012.

*خالد عبد الله القائفي: التحقيق الجنائي الرقمي والمعروف أيضا باسم العلوم الجنائية للأجهزة الرقمية وعملية التحقيق والإثبات بالأدلة والبراهين على ارتكاب الجريمة الإلكترونية، منشور يوم 22-12-2010، على الموقع: www.min-maq.com

*خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، ط1، 2011.

*خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

*فتوح الشاذلي، تأليف عفيفي كامل عفيفي،جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون،منشورات الحلبي القانونية،2003

*عادل عزام سقف الحيط: جرائم الذم والقدح عبر الوسائل الإلكترونية،دار الثقافة ، الأردن، ط1 ، 2011.

*عبد الناصر محمود فرغلي ومحمد عبيد سيف سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية،بحث مقدم في المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي ،جامعة نايف للعلوم الأمنية ، الرياض 2007.

* عبد الفتاح مراد: شرح جرائم الكمبيوتر والإنترنت،مصر.

*عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2002

*عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية،دار الفكر الجامعي،الاسكندرية، ط1 ،2006.

*علي محمود حمودة: الأدلة المتحصلة من الرسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل المؤتمر العربي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي،2003 .

*محروس نصار غايب : الجريمة المعلوماتية، المعهد التقني، الأنبار، 2011.

* محمد عبد الله أبوبكر: موسوعة الجرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، 2007.

*محمد حماد مرهج الهيتي: جرائم الحاسوب، دار المناهج، ط1،عمان، الأردن، 2006.

*محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2001.

*محمد مصطفى موسى: التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة ،القاهرة،2009.

*محمد الأمين بشري:التحقيق في الجرائم المستحدثة،ط1،منشورات جامعة نايف للعلوم الأمنية،الرياض،2004.

*ممدوح عبد الحميد عبد المطلب: استخدام البروتوكول TCP/IP في بحث وتحقيق الجرائم عبر الكمبيوتر، بحث منشور على الموقع www.arablawinfo.com.

*زيبحة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر.

*نبيل عبد المنعم جاد: جرائم الحاسب الآلي، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال، دبي، 2005

*نبيلة هبة هروال: الجوانب الإجرائية لجريمة الإنترنيت، دار الفكر الجامعي ، الاسكندرية ، ط1 ،سنة 2007.

*يوسف شمس الدين شابسرغ: نحو مفهوم معاصر للشرطة الإلكترونية، القيادة الكاملة لشرطة الشرقة، إدارة مركز بحث الشرطة، الإمارات العربية المتحدة، ط1، 2011.

*هلالي عبد الإله محمد: تفتيش نظم الحاسب الآلي وخانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، 1997.

المذكرات و المحضرات :

*أمال قارة: الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير، جامعة الجزائر، 2002/2001.

*بورزام أحمد: جرائم المعلوماتية، محاضرة ألقيت من طرف وكيل الحمهورية لدى محكمة باتنة، بالمجلس القضائي بباتنة، يوم 2006/06/20.

*سميرة معاشي: مفهوم الجريمة المعلوماتية في التشريع الجزائري،المجلة القضائية ،جامعة بسكرة.

*مزياني عبد الغاني: مداخلة بعنوان: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، محكمة المسيلة.

*فشار عطاالله: مواجهة البرمجية المعلوماتية في التشريع الجزائري، بحث مقدم بالملتقى المغربي حول القانون والمعلوماتية بجامعة زيان عاشور بالجلفة.

*طويجني كمال الدين: محاضرة بعنوان الجريمة المعلوماتية في التشريع الجزائري، ملقاة في الملتقى الثاني للقطب الجزائي المتخصص بسيدي أمحمد، في 03-05-2011.

*محاضرات ألقيت على طلبة سنة أولى حقوق ماستر قانون أعمال بجامعة المسيلة 2012.

مراجع أجنبية :

*Charless R, swanson, Neil chamelin and Lionard Territo: Criminal investigation (7^{th} , ed) London, ME Growhill, 2000,

* Eoghan casey: digital evidence and computer crime, london, academic, press, 2000

*How the TCP/IP Protocol Works, *Les Cottrell – SLAC*

Lecture 1 presented at the 26th International Nathiagali Summer College on Physics and Contemporary Needs, 25th June – 14th July, Nathiagali, Pakistan

القوانين :

*قانون الإجراءات الجزائية الجزائري، الأمر 66-155 المؤرخ في 18 صفر عام 1386هـ الموافق ل 08 يونيو سنة 1966 المعدل و المتمم بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006.

*القانون 09-04 الصادر في 09/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.

المحتويات :

مقدمـــة:..... 4

الفصل الأول :ماهية الجريمة الالكترونية..... 16

المبحث الأول : مفهوم الجريمة الالكترونية..... 16

المطلب الأول : الجريمة الالكترونية و بعض المصطلحات المشابهة لها..... 16

المطلب الثاني : تعريف الجريمة الالكترونية..... 19

المطلب الثالث : تاريخ الجريمة الالكترونية..... 26

المبحث الثاني : أطراف الجريمة الالكترونية..... 29

المطلب الأول : تعريف الحاسب الآلي..... 31

المطلب الثاني : المقصود بشبكة الإنترنيت و شبكات الاتصال.....33

المطلب الثالث : المجرم و الضحية في الجرائم الالكترونية. 34

المبحث الثالث : خصائص الجريمة الالكترونية..... 41

المطلب الأول : الخصائص المشتركة مع الجرائم الأخرى..... 41

المطلب الثاني : الخصائص التي تنفرد بها عن الجرائم الأخرى..... 42

المبحث الرابع : أركان الجريمة الالكترونية في ظل التشريع الوطني..... 44

المطلب الأول : مفهوم نظام المعالجة الآلية للمعطيات 45

المطلب الثاني : الركن الشرعي.....48

المطلب الثالث : الركن المادي..... 49

المطلب الرابع : الركن المعنوي..... 59

الفصل الثاني: أدلة إثبات الجريمة الإلكترونية وتقديرها في إطار نظرية الإثبات الجنائي..... 60

المبحث الأول: ضوء على الإثبات الجنائي..... 62

المطلب الأول: مفهوم الإثبات الجنائي..... 63

المطلب الثاني: القواعد العامة التي تحكم الإثبات الجنائي..... 64

المطلب الثاني: أثر الطبيعة الخاصة للجرائم الإلكترونية على إمكانية إثباتها..... 66

المبحث الثاني: صور الدليل الإلكتروني المتحصل عليها من الأدلة التقليدية للإثبات..... 68

المطلب الأول: الأدلة المحصلة من الوسائل الإلكترونية بطريق التفتيش والضبط..... 69

المطلب الثاني: الأدلة المحصلة من الوسائل الإلكترونية بطريق المعاينة والخبرة..... 79

المطلب الثالث: الأدلة المحصلة من الوسائل الإلكترونية بطريقة الشهادة والاستجواب..... 88

المبحث الثالث: الأدلة الإلكترونية التي يمكن الحصول عليها من الأدلة الحديثة للإثبات..... 93

المطلب الأول: ماهية الدليل الرقمي..... 93

المطلب الثاني: كيفية الحصول على الدليل الرقمي من الأجهزة والنظم والشبكات..... 103

المطلب الثالث: استخدام البروتوكول TCP/IP كدليل رقمي للإثبات الجنائي..120

المطلب الرابع: حجية الدليل الإلكتروني أمام القضاء الجنائي.....132

المبحث الرابع: جهاز التحقيق في الجرائم الالكترونية..... 139

المطلب الأول: التعريف بجهاز التحقيق الجنائي في الجرائم الإلكترونية..... 139

المطلب الثاني :عناصر فاعلية وكفاية جهاز التحقيق الجنائي في الجرائم الإلكترونية..... 142

المطلب الثالث: قضايا حول إثبات بعض الجرائم الالكترونية..... 166

خاتمـــة 175

المراجع 184

المحتويات 190