جامعة قاصدي مرباح – ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون جنائي

عنوان المذكرة

دليل إثبات الجرائم المعلوماتية

إعدادالطالبين:

- بوزيد أحلام
- بن الزين أسماء

إشراف الأستاذ:

- طيبي طيب

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
بلقاسم سويقات	أستاذ محاضر "أ"	رئيسًا
طيبي طيب	أستاذ محاضر قسم "ب"	مشرفًا
بامون لقمان	أستاذ مساعد قسم"أ"	مناقشًا

السنة الجامعية:2022 - 2023

جامعة قاصدي مرباح – ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون جنائي

عنوان المذكرة

دليل إثبات الجرائم المعلوماتية

إعداد الطالبين: إشراف:

بوزيد أحلامطيبي طيب

بن الزين أسماء

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
بلقاسم سويقات	أستاذ محاضر قسم "أ"	رئيسًا
طيبي طيب	أستاذ محاضر قسم "ب"	مشرفًا
بامون لقمان	أستاذ مساعد قسم"أ"	مناقشًا

السنة الجامعية: 2022 - 2023

الشكر والعرفان

فالشكر لله اولا واخيرا

والى كل من

كان

سببا في وصولنا الى هنا ونخص بالذكر أستاذنا الكريم المشرف

الإهداء

الى والدي جزاهما الله عني خيرالجزاء والى ابنتي فلذة

كبدي تسنيماسال الله ان يجعلها قرة عيني

لي والى اخوتي الاعزاؤ واخواتي

والى كل من اعانني في هذهالمذكرة ولو بكلمة.

وجميع أفراد عائلتي وإلى جميع الأساتذة الأجلاء الذين أضاءوا طريقي بالعلم وإلى كل

أصدقاء الدراسة والعمل ومن كانوا برفقتي أثناء

إنجاز هذا البحث إلى كل هؤلاء وغيرهم ممن تجاوزهم قلمي ولن يتجاوزهم قلبي أهدي ثمرة جهدي المتواضع

احلام

الإهداء

أهدي هذا العمل إلى أعز ما يملك الإنسان في هذه الدنيا

إلى ثمرة نجاحي

إلى من أوصى بهما الله سبحانه وتعالى " : وبالوالدين إحسانا"

إلى الشمعة التي تحترق من أجل أن تضئ أيامي إلى من ذاقت

مرارة الحياة وحلوها، إلى قرة عيني وسبب نجاحي وتوفيقي في دراستي إلى "أمي"

أطال الله في عمرها إلى الذي أحسن تربيتي وتعليمي

وكان مصدر عوني ونور قلبي وجلاء حزني ورمز عطائي ووجهني نحو الصلاح والفلاح

إلى "أبي " أطال الله في عمره إلى اخوتي وأخواتي

وجميع أفراد عائلتي وإلى جميع الأساتذة الأجلاء الذين أضاءوا طريقي بالعلم وإلى كل

أصدقاء الدراسة والعمل ومن كانوا برفقتي أثناء

إنجاز هذا البحث إلى كل هؤلاء وغيرهم ممن تجاوزهم قلمي ولن يتجاوزهم قلبي أهدي

ثمرة جهدي المتواضع

أسماء

قائمة المختصرات

ج. ر. ج. ج: الجريدة الرسمية للجمهورية الجزائرية

ص: صفحة.

ق. أ. ج:قانون الأسرة الجزائري.

ق. إ. م. إ:قانون الاجراءات المدنية والادارية.

ق. ع. ج: قانون العقوبات الجزائري.

.....

.....

.....

مقدمة

تعيش المجتمعات الحديثة في عصر رقمي يتسم بتطور التكنولوجيا والتواصل الإلكتروني، وذلك نتيجة الثورة المعلوماتية التي ضربت جميع ميادين الحياة سواء على مستوى الفردي أو على الصعيد الدولي، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها على نظام المعلوماتية نظرا لما يتميز به من سرعة ودقة نتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية خاصة شبكة الانترنت والتي شكلت قفزة حضارية ونوعية في حياة الأفراد .كما أصبحت هذه الأنظمة مستودعا لأسرار الاشخاص المتعلقة بحياتهم الشخصية او بطبيعة اعمالهم الماليةالاقتصادية وغيرها ، نفس الشيء بالنسبة للمجتمعات الدولية في شتى الميادين الاقتصادي او الحربي والصناعي ... الخ .

إلا ان هذا الجانب المشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية والمتمثلة في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة تضر مصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع ككل حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم سميت بالجرائم المعلوماتية[1].

تشكل الجرائم المعلوماتية تهديدًا خطيرًا للأفراد والمؤسسات، لتعرضهم لسرقة المعلومات الحساسة والبيانات الشخصيةومختلف التجاوزات الرقمية، وتعرض الشركات والحكومات لاختراق أنظمتها الأمنية. لهذا تمثل الجريمة الالكترونية تحديًا كبيرًا أمام الجهات القضائية والمحققين، حيث يواجهون صعوبة في جمع الأدلة اللازمة لإثبات الجريمة وتحقيق العدالة. لذا، فإن توفير طرق فعالة لإثبات هذا النوع من الجرائم يساعد على حماية المجتمعات والتصدي للجرائم الالكترونية. ومن هنا تأتي أهمية وجود دليل يقدم إرشادات وإجراءات لإثبات الجريمة المعلوماتية.

[1]– عائشة مصطفى بن قارة حجية الدليل الالكتروني مجال الاثبات الجنائي دار الجامعة اسكندلرية مصر 2010 ص 14[1]

أهمية الموضوع :

– تكمن دراسة هذا الموضوع "دليل اثبات الجريمة المعلوماتية انها تمكننا من ــ مكافحة هذا النوع من الجرائم من خلال فهم كيفية اثبات الجرائم الرقمية وهذا بالتعرف على الأدلة اللازمة لتقديم المتسببين في الجرائم الى العدالة وتطبيق العقوبات المناسبة . وهذامن خلال ايضاح اجراءات البحث والتحري في هذه الجريمة باعتبارها ظاهرة اجرامية حديثة ذات طبيعة خاصة لا تكفيالإجراءات التقليدية في الكشف عنها وعن مرتكبيها.

كما تبرز اهمية هذا البحث في التعرف على كيفية حماية المعلومات الشخصية عن طريق معرفة اساليب ارتكاب هذا النوع من الجرائملأنها اساليب عصرية ومتطورة يصعب اكتشافها دون دراسة هذا السلوك الاجرامي، وتحليل هذه الظاهرة الاجرامية المستحدثة والتي هي وليدة التطور التكنولوجي المستمر.

كذلك تظهر اهمية هذا البحث حول تحليل الادلة المتعلقة بالمجال الرقمي المتمثلة في الأدلة الالكترونية وحول مدى تأثير طبيعة هذا الدليل في اقتناع القاضي الجنائي

ان من اهم الاسباب والدوافع التي جعلتنا هذا الموضوع تتمثل في اسباب ذاتية واخرى موضوعيفبالنسبةللأسباب الموضوعية باعتبارها ظاهرة اجرامية غامضة ومستحدثة ،مما يثير الاهتمام لاكتشافها والتعرف عليها اكثر ،زد على ذلك ان هذه الجرائم اضحت واقعا نعيشه راح نتيجة ارتكابها الاف الضحايا، مما يستوجب الدراسة ومحاولة ايجاد حلوللمكافحتها و الحد من انتشارها.

اما فبالنسبةللأسباب الذاتية هو ميولنا الشخصي وفضول حول معرفة طبيعة هاته الجرائم وكيفية اثباتها ،إضافة الى ان مجال تخصصنا الدراسي يتمحور حول علم الاجرام والمجرمين

ومن بين الاهداف المرجوة من هاته الدراسة هو ازاحة الغموض الذي يشوب مظاهر الجريمة المعلوماتية واختراق دواليبها من خلال تبيان الادلة والاجراءات المتبعة للكشف عنها، زيادة

عن ذلك معرفة مدى فاعلية الادلة المستحدثة في اثبات هذه الجرائم وتأثيرها على اقتناع القاضي الجزائي،

وعليه تأتي صياغة اشكالية هذا الموضوع كالتالي: أينتكمن خصوصية دليل اثبات الجريمة المعلوماتية؟

والتي بدورها تتفرع عنها التساؤلات التالية :

- ما المقصود بالجريمة المعلوماتية؟
- وما هي طبيعة الدليل الرقمي؟
- وهل دلالة الرقمية فاعلية في اثبات هذا النوع من الجرائم وما مدى تأثير الادلة الرقمية في الاقتناع الشخصي للقاضي؟

وللإجابة عن هذه التساؤلات ارتأينا الى اعتماد المنهج الوصفي بتطرقنا لخصائص ومميزات التي تتسم بها الجريمة المعلوماتية وكذا لاسيما الدليل الرقمي والتحليلي في مناقشة ما يحتاجه لجمع الحقائق والبيانات، والتعرض الى مدى تأثيره على الاقتناع القاضي الجنائي .

ومن أجل الاحاطة بكل جوانب الموضوع والإجابة على اشكالية البحث قمنا باتباع الخطة التالية وهي تقسيم المذكرة الى فصلين الفصل الاول نتناول فيه اساسيات حول اثبات الجريمة المعلوماتية حيث قسمنا الفصل الأول بدوره الى مبحثين المبحث الاول بعنوان مفهوم الجريمة المعلوماتية واساسها القانوني والمبحث الثاني بعنوان اداة اثبات الجرائم الالكترونية.

اما الفصل الثاني ادرجناه تحت عنوان الاحكام الإجرائية لإثبات الجرائم الإلكترونية قسمناه هو الاخر الى مبحثين المبحثالأولتطرقنا الى اجراءات ووسائل استخلاص الادلة الجنائيةالرقميةوالمبحث الثاني تناولنا فيه السلطة التقديرية للقاضي الجزائي في تقيم الدليل الرقمي.

الفصل الأول

أحكام الموضوعية في اثبات الجريمة المعلوماتية

تمهيد:

تعد الجريمة المعلوماتية واحدة من اهم التحديات التي يواجهها العالم الرقمي الحديث، فهي تمثل تهديدا خطيرا للأمن السيبيراني، والخصوصية الشخصية حيث تتمثل الجريمة المعلوماتية في استخدام التقنية الحاسوبية والانترنت للقيام بأنشطة غير قانونية والاعتداءات الرقمية الاخرى وهذه الانشطة يمكن ان تتضمن الاحتيال والتلاعب بالبيانات والتجسس والاختراق والقرصنة الالكترونية والاعتداءات الالكترونية الأخرى.

ان الجريمة المعلوماتية قد تتخذ اشكال نفس مختلفة الا انها تتشارك في العنصر مثل استخدام الحاسوب والانترنت كأدوات للجريمة والتي تشكل اضرارا في النظام الحاسوبي او البيانات او الشبكات ورغم ان الدليل الرقمي يعد من اهم ادوات العمل القضائي الا انه يتضمن بعض التحديات والمشكلات الخاصة فيما يتعلق بالجرائم المعلوماتية حيث يمكن للمجرمين المعلوماتيين التلاعب بالأدلة الرقمية ،بشكل صحيح ولكن قبل الحديث عن التحديات التي يواجهها الدليل في الجرائم المعلوماتية يجب علينا التعرف اولا عن المفاهيم الاساسية للجريمة المعلوماتية مع تبيان اركانها وذلك بالنسبة للمبحث الاول، ثم نتطرق للدليل الرقمي في المبحث الثاني بشكل مفصل.

المبحث الأول: مفهوم الجريمة المعلوماتية واساسها القانوني.

من خلال هذا المبحث سنحاول التعريف على الجريمة المعلوماتية وما يميزها عن غيرها من الجرائم، باعتبارها جريمة مختصة بالعالم الافتراضي لا الواقعي، وكذا تبيان أنواعها ثم الأركان التي تتركز عليها وذلك من خلال المطلبين التاليين:

- المطلب الأول: ماهية الجريمة الالكترونية.
- تعريفه.
- خصائصه.

المطلب الأول: ماهية الجريمة الالكترونية وخصائصها.

ظهرت الجريمة الالكترونية لأول مرة في الدول المتقدمة ذات التكنولوجيا العالية ثم انتقلت الى الدول الأخرى، وأخذت ظاهرة الجريمة المعلوماتية حيزا كبيرا من الدراسات من اجل تحديد مفهومها مما أنجز عنه وضع عدة مصطلحات لدلالة عليها من بينها جرائم الحساب، جرائم التقنية العالية، جرائم معلوماتية، جرائم الغش ألمعلوماتي، وصولا إلى جرائم الانترنت .

ويعد عدم الاستقرار على مصطلح واحد للتعبير على الجريمة المعلوماتية من الصعوبات الواردة عليها، وسنحاول من خلال هذا المطلب التعرف على ما يقصد بالجريمة المعلوماتية وكذا الخصائص التي تميزها وذلك ضمن فرعين منفصلين:

الفرع الأول: تعريف الجريمة الالكترونية.

لقد تعددت أراء الفقهاء حول إيجاد تعريف للجرم ضمن المعايير التالية الذكر.

أولا: التعريف الفقهي للجريمة المعلوماتية:

1/ تعريفات تقوم على أساس وسيلة ارتكاب الجريمة: من هذا التصور تتحقق الجريمة الالكترونية باستخدام الكمبيوتر كأداة رئيسية لارتكابها فالأستاذ جون فورستر يعرفها بأنها فعل إجرامي يستخدم الكمبيوتر كأداة لارتكابه، وهذا ما ذهب إليه أيضا الفقيه تايدمان (TIEDEMAN)حيث أشار إلى أنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب، ويصف هذه الجريمة مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا[1].

أما منظمة التعاون الإقتصادي والتنمية OECD فقد عرفتها بأنها كل فعل او امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية.[2]

2/ تعريفات تقوم على أساس موضوع الجريمة: يرى اخرون أن تعريف الجريمة المعلوماتية انهاترجع الى موضوعها وغير متعلقة بالوسيلة المستعملة أو الفاعل حيث يرى هؤلاء ان الجريمة هي التي يكون موضوعها المال ألمعلوماتي المعنوي، دون النظر فيما إذا كان الحاسوب هو الأداة المستعملة في ارتكابها من عدمه كالقرصنة، والاستعمال الغير المشروع للأنظمة المعلوماتية أو هي الجرائم التي ترتكب علة الأنظمة الإلكترونية والشبكات المعلوماتية[3]، فالجريمة هي:(كل فعل غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب الآلي والتي تحول عن طريقه) أو هي (غش معلوماتي ينصرف لكل

[1] رحموني محمد ـ خصائص الجريمة الالكترونية ومجالات استخدامها ـ مجلة الحقيقة ـ جامعة أحمد دراية ـ أدرار ـ العدد 41 ص436
[2] عفيف-ي كامل ـ جرائم الكمبيوتر وحقوق المؤلف والمصنفات ـ منشورات الحلبي الحقوقية بيروت لبنان 2003 ص 3
[3] غنية باطلي ـ الجريمة الالكترونية ـ منشورات الدار الجزائرية 2016 ص17

سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها)، فهي إذا تقع اعتداء على حق الملكية أو الحق في سلامة الشرف والاعتبار أو الحق في حماية حقوق الملكية الفكرية أو الحق في الحفاظ على سلامة الحياة الخاصة، بل يمكن الذهاب إلى ابعد من ذلك للقول بإمكانية تصور وقوع اعتداء على حرمة السلامة الجسدية عن طريق أجهزة الحاسب الآلي إذا كان هناك إمكانية تصور ارتكاب جريمة ما كإيقاع الخلل في أجهزة الحاسب التابعي لوسائل النقل كالطيران أو السكك الحديدية أو النقل البحري إذا كان الهدف من إيقاع الخلل الالكتروني هو إلحاق الضرر بالسلامة الجسدية للركاب وإزهاق أرواح[1].

3/ تعريفات تقوم على أساس الإلمام بالمعرفة التقنية للجريمة: يعتمد أصحاب هذا الاتجاه في

تعريفهم للجريمة المعلوماتية على معار إلمام مرتكب الجريمة المعلوماتية بتقنية المعلومات معيار شخصي ومن بين أصحاب هذا الاتجاه الفقيه (DAVID THPMSON) الذي عرف الجريمة المعلوماتية بأنها جريمة يكون متطلبا لافتراضها ان تتوفر لدى فاعلها معرفة بتقنية الحاسب[2] ، كما عرفها جانب من الفقهاء أيضا أنها ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، كما عرفت أيضا بأنها : جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكنه من ارتكابها[3] وهو الاتجاه الذي اعتمدته وزارة العدل الأمريكية في تعريفها للجريمة الالكترونية بعد ماورد في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979. وقد تم توجيه عدة انتقادات لأصحاب هذا الاتجاه من أهمها انه يضيق من مجال الجريمة المعلوماتية[4].

[1] هشام فريد رستم ـ جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة ـ بحث مقدم لدى اللجنة العلمية مصر لمنع الجريمة الالكترونية لمعاقبة المجرمين ـ مجلة الدراسات القانونية ـ جامعة اسيوط العدد 17 1995 ص 31

[2] فايز الظفيري الاحكام العامة للجريمة الالكترونية مجلة العلوم القانونية والاقتصادية العدد 2 كلية الحقوق جامعة عين شمس 2002 ص486

[3] غنية باطلي المرجع نفسه 17

[4] جواحي حد الستار جرائم الحاسوب مذكرة لنيل شهادة ماستر تخصص شرعة وقانون كلية العلوم الجتماعية والعلوم الانسانية جامعة حمى لخضر الوادي 2015/2014 ص6

من خلال هذا التعريف ينصح انه تم حصر مجال او معنى الجريمة الالكترونية ضمن حيز الأشخاص الذين يملكون خبرة ومعرفة تقنية نادرة من نوعها ويستند أيضا هذا الاتجاه إلى أن الجرائم التي تفتقر إلى هذا القدر من المعرفة تعد جرائم عادية تخضع للنصوص التقليدية ، للقوانين الجنائية، ومن ثم فلا حاجة إلى نصوص جديدة لتجريمه، وهو الأمر اقرب مايكون للخيال لان الواقع لا يخلو من هاته الأنواع من الجرائم صادرة في أشخاص عاديين دون الحاجة إلى ما يسمى بالتطور الفكري والمعرفي الخارق، خاصة في ظل وجود برامج ومعطيات مساعدة على ذلك.

4/ تعريفات على اساس محل الجريمة ووسيلة ارتكابها: أو ما يعرف عند البعض بالاتجاه المختلط والذي عمد إلى التوسيع من مفهوم الجريمة الالكترونية لتشمل جميع الجرائم التي لها علاقة بالمعلوماتية والتي تستخدم نفس التقنية سواء كان الحاسوب أو تقنية المعلومات وسيلة في لارتكابها او هدف لها ويعتمد هذا المعيار في تعريفه لهذا النوع من الجرائم على الجمع بين أداة جريمة وموضوعه[1]ا، أو بعبارة أخرى اعتبار جهاز الكمبيوتر الضحية والوسيلة ولتفصيل ذلك نورد التعريفات التالية:

وفق هذا المنظور يعرف الفقيه SMEBING LOFF الجريمة الالكترونية على أنها"" اي ضرب من النشاط الموجه ضد او المنطوي على استخدام نظام الحاسوب "، وفي ذات الاتجاه ذهب كل من الفقيهين "RobertyLindqist" –"jack Bologma" فيعرفانها بأنها " الجريمة التي يستخدم فيها الحاسوب كوسيلة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها"، أما الفقيه (MASSE) فيضيف الهدف من اقتران الجريمة الالكترونية وهو الحصول على الربح فيعرفها بأنها "تلك الاعتداءات التي يمكن أن ترتكب

[1]عميمر عبد القادر ـ التحديات القانونية ـ لإثبات الجريمة المعلوماتية النشر الجامعي تلمسان الجزائر 2021 16ص ص17

بواسطة المعلوماتية بغرض تحقيق الربح"[1] . كما يرى البعض الأخر تعريف الجريمة الالكترونية على أنها كل عمل أو امتناع يأتيه الإنسان أضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها[2].

إن إعطاء تعريف موسع للجريمة المعلوماتية يدخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسب الآلي اي كانت هذه العلاقة وأيا كان دور الحاسب فيها سواء كان وسيلة مناسبة لارتكاب التصرفات الغير المشروعة أو كان موضوعا لها وبالتالي يمتد هذا التعريف الموسع ليشمل كل من:

الحالات التي يكون فيها المال المعلوماتي مناسبة لارتكاب الجريمة.

الحالات التي يكون فيها المال المعلوماتي أداة لارتكاب الجريمة.

الحالات التي يكون فيها المال ألمعلوماتي موضوع الجريمة[3] .

ووفقا لتعريف منظمة التعاون الاقتصادي والتنمية والخاص باستبيان الغش ألمعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات، إذا ليتم هذا التعريف بالوضوح فضلا عن تحديده لماهية السلوك الإجرامي للجريمة التي قد تقع به إذا شمل كل من الفعل الايجابي والسلوك السلبي المتمثل في الامتناع، فهو تعريف أكثر شمولا مما سبقه من التعريفات وإن كان الغرض عن الربح وارد في ارتكابها،

[1] رحموني المرجع السابق ص 473

[2] محمد أمين أحمد شوابكة جرائم الحاسوب والانترنت ـ ط 1مكتبة دار الثقافة للنشر والتوزيع عمان الاردن 2004ص9

[3] غنية باطلي المرجع السابق ص20/19

الا انه ليس العنصر الأهم. فقد يكون الهدف إثبات الذات والريادة من قبل الفاعل أو بغرض الإضرار بالغير...وغيرها من الأسباب[1].

ثانيا: التعريف التشريعي للجريمة الالكترونية:

من المعلوم ان المشرع الجزائري اغفل تنظيم مجال الجريمة الالكترونية قانونا، إلا انه ما فتىء ان تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون رقم04/15 المتضمن تعديل قانون العقوبات والذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات ثم تلاه القانون 09/04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومما يجب الإشارة إليه إن مصطلح نظام المعالجة الآلية للمعطيات تعتبر ذات طابع فني تقني يصعب على القانوني إدراك مغزاه بباسطة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[2] .

ولذلك فالمشروع جريمة على غرار الكثير من التشريعات لم يعرف نظام المعالجة الآلية للمعطيات واوكل بذلك هذه المهمة لكل من الفقه والقضاء.

ولمزيد من التفصيل نتناول كل من القانون 04/15 و09/04 على التوالي:

تعريف الجريمة الالكترونية في التشريع الجزائري وفقا للقانون 04/15: بالرجوع الى قواعد القانون 04/15 من المادة 394مكرر الى المادة 394مكرر2 نجد انه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات حيث حددها في المادة 394 مكرر بالآتي[3]:

[1]أحمد خليفة الملط ـ الجرائم المعلوماتية ط 2 دار الفكر الجامعي ـ الاسكندرية 2006 ص87

[2]رحموني محمد المرجع السابق ص438

[3]علي عبد القادر القهوجي ـ الحماية الجنائية لبرامج الحاسب الالي منشأة المعارف ـ اسكندرية مصر 1999ص 120

-الدخول والبقاء بالغش في كل جزء من منظومة للمعالجة الآلية للمعطيات او محاولة ذلك.

-حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت إلى:

-إدخال بطريقة غش معطيات من نظام المعالجة الآلية أو إزالة أو تعديل بطريق غش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 التالي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات مخزنة او معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم[1].

-حيازة أو إفتاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم .

القانون 09/04 حددت المادة 02 منه يقصد في مفهوم هذا القانون بما يأتي:

-الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

-جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية:

[11]القانون رقم 04/15 المؤرخ 10/نومبر 2004 المتضمن قانون العقوبات المعدل والمتمم لامر 55/156 المؤرخ 8يونيو 1966 الجريدة الرسمية العدد 71 سنة 2004

منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ البرنامج معيين.

معطيات معلوماتية: اي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية تؤدي وظيفتها[1].

الفرع الثاني: خصائص الجريمة المعلوماتية ومرتكبيها:

تختلف الجرائم الإلكترونية عن غيرها من مظاهر الاجرام بل وتجد الجهات المعنية صعوبة خاصة من ناحية إثباتها أو ترصد حركتها وأثارها، فالغالب أن اكتشافها يكون على سبيل الصدفة لا القصد. ومن خلال هذا الفرع نحاول إبراز أهم خصائص ومميزات هذا النوع من الجرائم الذي يعتمد على الجانب التقني أكثر منه ماديا.

أولا: السمات الخاصة بالجريمة المعلوماتية:

1. الجريمة المعلوماتية متعدية للحدود أو عابرة للدول: المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر الشبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينهما آلاف الأميال قد أذت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالحركة المعلوماتية الواحدة في آن واحد[2] ، من ثم فإن هاته الخاصية تشير عدة تحديات في مجال الإختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

[1]القانون رقم 04م09 المؤرخ في 14 شعبان 1430 موافق 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 74 2009

[2]نهلا عبد القادر المومني ـ الجرائم المعلوماتية ط1 دار الثقافة للنشر والتوزيع الاردن 2008 ص 51/50

فالجرائم المعلوماتية قد ترتكب عن طريق الحاسب الآلي في دولة ما في حين يتحقق الفعل الإجرامي في دولة أخرى والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقيقي النتيجة من أكثر المسائل التي تشير إشكالات في مجال الجرائم المعلوماتية وبشكل خاص الاجراءات الجزائي والاختصاص القضائي والقانون الواجب التطبيق، وهذا بدوره عامل رئيسي في تظافر الجهود الدولية لمكافحة هذه الجرائم ويجعلها من المواضيع الرئيسة على أجندة اهتمام المجتمع الدولي[1] ، نظرا لخطورتها وطبيعتها الخاصة فتعالت الاصوات الداعية إلى التعاون المكثف لدول العالم من أجل التصدي لهذه الجرائم تتمثل في الاتفاقيات والمعاهدات الدولية الهادفة للإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.

2. صعوبة اكتشاف الجريمة المعلوماتية: لقد أشرنا سابقا أنه من بين الخصائص التي تتميز بها الجريمة المعلوماتية خاصية صعوبة اكتشافها وغالبا ما يتم ذلك على سبيل الصدفة وهذا ما يخولها لان تعتبر من الجرائم الأكثر فتكا بشرائح المجتمع إذا ما قارناها بالجرائم التقليدية، وذلك لعدم تركها لأي أثر خارجي بصورة مرئية كما أن الجاني يمكنه ارتكاب هذه الجريمة في الدول وقارات أخرى كما سبق الذكر[2].

فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه او لا يدري مت وقوعها والإمعان في حجب السلوك المكون لها وإخفاءه عن طريق التلاعب الغير المرئي في النبضات او الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمرا ليس بالغير بحكم توافر المعرفة والخبرة لدى مرتكبيها[3].

[1]بان مكي نجاة السياسة الجنائية لمكافحة الجرائم المعلوماتية ـ منشورات دار الخلدونية الجزائر 2017 ص22/21

[2]نهلة عبد القادر المرجع السابق ص 54

[3]رستم هشام محمد فريد ,الجوانب الاجرائية للجرائم المعلوماتية ,مكتبة الآلات الحديثة ,ط 1 اسيوط ,مصر 1996 ,ص16

ولعل من أهم المعوقات التي تزيد من صعوبة اكتشاف الجريمة هو عزوف المجني عليه من التصريح بهذا السلوك الاجرامي كما هو الحال بالنسبة للشركات والمؤسسات في مجتمع المال والاعمال عن الابلاغ عما يرتكب داخلها من جرائم، حيث تخشى مجالس ادارتها من إن تؤدي الدعاية السلبية التي قد تنجم عن كشف هاته الجرائم إلى تضاؤل الثقة فيها من جانب المتعاملين معها ولعل من الاسباب التي تدعو المجني عليه لعدم التبليغ عن مثل هاته الجرائم هو خشية الكشف عن مواطن الضعف في ببرنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه[1] .

وكما أسلفنا الذكر أنه غالبا ما يستهدف المجرم الالكتروني أشخاص اعتبارية حيث بلغت نسبة الجريمة فيها 19% من مجموع الجرائم المرتكبة كما تستهدف أيضا المؤسسات العسكرية، كالتجسس العسكري عن طريق الشبكات من خلال الاقمار الصناعية كما يمكن ان يقع الاعتداء على أشخاص طبيعية. كما هو الحال بالنسبة لجرائم القذف والتشهير، كذلك جرائم النصب عبر الشبكات حيث وقع الشعب الامريكي ضحية هذا الاجرام من قبل بعض الاشخاص مستغلين في ذلك أحداث (11 سبتمبر 2001) نتيجة قيام العديد من الجهات بإنشاء مواقع الكترونية لجمع التبرعات لضحايا الحادث[2].

3/ الجريمة المعلوماتية جريمة ناعمة: تم اعطاؤها هذا الوصف لأنها لا تترك أثار مادية كالتي تتركها الجرائم التقليدية فلا وجود للكسر ولا بقع الدم وكل ما تخلفه هي أثار رقمية ليس لها وجود مادي ملموس[3] ، فتلك البيانات والمعلومات تكون عبارة عن ذبذبات الكترونية غير مرئية تنساب عبر نظام المعلوماتي الامر الذي يجعل طمس الدليل ومحوه كليا من قبل مجرم

[1]انظر هشام رستم ,الجوانب الاجرائية ,المرجع السابق ص23

[2]عائشة بن قارة ,المرجع السابق ,ص 40

[3]عميمر عبد القادر ,المرجع السابق ,ص 28

المعلوماتية امرا في غاية السهولة، بل ويتم إزالة كل ما من شأنه إدانته في ثواني فيمكن للجاني أن يرتكب جريمته وهو ممدد على فراشه او يرتشف فنجان قهوة خلف مكتبه وفي قاعة مكيفة دون ان يشعر به احد ولوكان في مكان مكتظ بالأشخاص.

وتجدر الاشارة الى ان الاسباب الحقيقة والاساسية التي تساهم في إخفاء كل دليل يجرم القائمين على الجرائم المعلوماتية هو النقص الفادح سواء على الصعيد التقني والفني وقلة الخبرة لذوي الاختصاص وكذا جانب العتاد اي اجهزة المتطورة فمن ممكن ان يتم طمس الدليل دون قصد وادارية من الجهات المكلفة بالتحقيق.

4/ الجريمة المعلوماتية في الغالب متعددة الجناة: تتميز الجريمة المعلوماتية أنها عادة ما تتم بتعاون أكثر من شخص على ارتكابها اضرار بالجهة المجني علبها وغالبا ما يشترط في إخراج الجريمة الى حيز شخص مخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشرع الإجرامي وشخص أخر من المحيط او من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب اليه[1].

وإذا كان تكوين جماعة أشرار لأجل ارتكاب الجنايات والجنح يتم في الجرائم التقليدية من خلال الالتقاء في مكان معين فان الانترنت سهل هذه العملية بحيث أصبح الاتفاق والتخطيط وتبادل المعلومات يتم عن طريق المنتديات وغرف الدردشة وغيرها من التطبيقات مع إمكانية استخدام برامج بسيطة تحول دون اكتشاف هوية الاشخاص المتصلين بهذه المواقع، مما يصعب مهمة مصالح البحث والتحري في اكتشاف هاته الجماعات[2]

5/ خصوصية مجرمي المعلوماتية: المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية

[1] عفيفي كامل عفيفي ,جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ,ط1 بدون نشر

[2] عميمر عبد القادر ,المرجع السابق ,ص 31, 32

(المجرم التقليدي) فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة علمه.

فإن الامر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الامر، ومن يرتكبها عادة يكون ذوي الاختصاص في مجال تقنية المعلومات، أو على الاقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت فعلى سبيل المثال فإن الجرائم المعلوماتية ذات طابع الاقتصادي مثل تحويل الالكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الاجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي. [1]

ثانيا: السمات الخاصة بالمجرم المعلوماتي:

نجد ان الجريمة المعلوماتية ونظرا لارتباطها بتقنيات الحاسوب والانترنت كما سبق وان ذكرنا هو العامل الاكبر في تمييزها عن الجرائم التقليدية مثلها مثل ما يطلق عليه بالمجرم المعلوماتي، عن غيره من المجرمين واتصافه بسمات معينة جعلت منه محلا لعديد من الأبحاث والدراسات وللمجرم المعلوماتي خصائص وسمات نذكر منها التالي:

1. سيماته الشخصية: للمجرم المعلوماتي سمات شخصية يتمتع بها تميزه عن غيره من مجرمي الجرائم التقليدية حيث يتمتع بكونه من ذوي المناصب رفيعة المستوى وله احترام وتقدير وقدرته على الانسجام الإجتماعي، كما انه يتمتع بمعرفة كبيرة عن الظروف التي تحيط بنوع الجريمة وكيفية تنفيذها وإمكانية نجاحها لاتصافه بالذكاء وتحكمه في تقنيات الحاسوب والانترنت.

[1] نهلا عبد القادر ,المرجع السابق ,ص 59

2المجرم المعلوماتي يبرر ارتكاب جريمته: يعني لدى هذا الاخير شعور أن ما يقوم به لا يدخل في عداد الجرائم، او بمعنى أخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله حيث يفرق مرتكبو هذه الجرائم بين الأضرار بالأشخاص، الامر الذي يعتبرونه غاية في اللاأخلاقية وبين المؤسسات التي تستطيع تحمل نتائج تلاعبهم[1].

3. المجرم المعلوماتي مجرم يتمتع بالاحترافية والذكاء في تنفيذ جرائمه: يكفي ان يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه البيانات او يعطل استخدام البرامج، وليس عليه سوى اللجوء الى زرع الفيروسات في هذه البرامج او استخدام القنابل المنطقية او الزمنية لكي يشل حركة النظام المعلوماتي ويجعله غير قادر بوظائفه الطبيعية[2].

4- خوف المجرم المعلوماتي من كشف جريمته: ان اغلب المجرمين المعلوماتيين عندما يتم اكتشافهم والقبض عليهم لا يستسلمون بل يحاولون مرة اخرى من اجل تدارك الثغرات التي ادت الى التعرف عليهم في المرة السابقة، وهو ما يجعلهم يعودون للإجرام مما ادى الى إطلاق وصف المجرم العائد او المجرم الانتكاسي على المجرم المعلوماتي.[3]

الفرع الثالث: انواع الجريمة المعلوماتية.

من المتعارف عليه ان لكل جريمة انواع وهذا النوع من الجرائم تتميز بأنواعها المتعددة والتي يصعب حصرها ضمن قائمة مضبوطة ، نظرا للتطور الشديد والسريع التي تشهده الجرائم

[1]نهلا عبد القادر ,المرجع السابق ,ص78

[2]بن مكي نجاة ,المرجع السابق ص41

[3],عبد الفتاح بومي حجازي مكافحة جرائمالكمبوتروالانترت في القانون العربي النموذجي دار الكتب القديمة مصر 2007 ص 107

المعلوماتية وبالتالي سوف نحاول من خلال هذا المطلب تناول بعض منها ، بما فيها من اركان ترتكز عليها الجريمة الرقمية.

ولقد اختلف جمهور الفقهاء حول اعطاء تقسيم محدد وثابت لأنواع الجريمة الالكترونية فلكل منهم رايه ولعل من اهم التقسيمات التقسيم الذي سنوضحه لاحقا والذي يقسم الجريمة المعلوماتية الى قسمين ،قسم يقوم على الجرائم التي تقع على الاشخاص ،وكذا الجرائم التي تقوم على الاموال،،.

1.الجرائم التي تقع على الأشخاص: هي الجرائم التي تنال بالاعتداء وتهدد بالخطر الحقوق ذات الطابع الشخص البحث اي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية تخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف[1].

جريمة انتحال الشخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخد هذا النوع شكلا جديد الا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي ومشابهها من أجل الحصول على بطاقات انتمائية وغيره ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت[2].

[1]عمار حشمان ,مذكرة :الجريمة المعلوماتية في التشريع الجزائري ,مذكرة لنيل الماستر كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ,جامعة قاصدي مرباح –ورقلة – 2018-2019 ص05

[2]منير محمد الجنبيهي–جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها ,دار الفكر الجامعي ,الاسكندرية ,2005,ص42,43

جريمة المضايقة والتهديد: ويقصد بالتهديد الوعيد بالشر، وهو زرع الخوف في النفس بالضغط على إرادة الانسان وتخويفه بما سيلحقه من اضرار أو يلحق أشياء له صلة بها، ويعد تهديد الغير من خلال البريد الالكتروني واحد من أهم الاستخدامات غير المشروعة للأنترنت حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها. وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، وجرائم الملاحقة تتمثل في رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني ولا تتطلب الجريمة المرتكبة عبر الانترنت أي اتصال مادي بين المجرم والضحية مما يدل ان لها تأثيرات سلبية نفسية، فهي لا تؤدي إلى أي تصرفات عنف مادية[1].

جرائم التغرير والاستدراج: هي من أشهر جرائم الانترنت ومن أكثرها انتشارا، خاصة بين أواسط صغار السن ومن مستخدمي الشبكة وهي تقوم على عنصر الإلمام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة او زواج على الانترنت وهذه الجريمة المعلوماتية قد تتطور الى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية او اجتماعية إذا يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها اي مستخدم حسن النية[2].

[1] محمد امين الشوابكة ,المرجع السابق الصفحة ,45

[2] عبد الكريم شيباني ,الحماية الاجرائية والموضوعية للجريمة المعلوماتية ,مذكرة لنيل شهادة ماستر ,كلية الحقوق والعلوم السياسية ,جامعة الطاهر مولاي ,سعيدة ,2015,2016 ,ص19

جرائم التشهير وتشويه السمعة: مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز الفكرية او سياسية او دينية. وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد وهو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز وكذلك لتسميم أفكار الناس ومحاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم. وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي على المعلومات المطلوبة إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية ومن أمثلها إرسال الصور الغير اللائقة أو معلومات غير صحيحة[1].

الجرائم المخلة بالأخلاق والآداب العامة: إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون آخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معيين قد تشكل جريمة يعاقب عليها القانون في حيث أنها لا تكون كذلك في أي بلد أخر وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الالكترونية أو محاولة إغرائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة وتصوير القاصرين ضمن أنشطة الجنس، والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرهم رواجا خاصة في الدول العربية واروبا والدول الأسيوية. وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الأشكال سواء كانت صور أو فيديوهات او حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز.

1-الجرائم التي تقع على الأموال: وهذا النوع من الجرائم يقع أو يمس بالحقوق المادية ذات القيمة المالية، فإذا كان موضوع الاعتداء على الأموال في نطاقه ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فإنه هنا لا يشير أي صعوبة في

[1]منير الجنبيهي المرجع السابق ص34

تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي.

2-جرائم الفيروس ألمعلوماتي: هناك من عرفه على انه مرض يصيب الحاسب الآلي، فهو ليس فيروس بالمعنى البيولوجي ولكنه برنامج يتم تسجليه أو زراعته على الأقراص أو الاسطوانات الخاصة بالحاسب ويظل هذا الفيروس لفترة محددة، ينشط فجأة في توقيت معيين ليدمر البرامج والبيانات المسجلة في داخل الحاسب ويشمل أثره التخزيني الإتلاف أو الحذف أو التعديل.[1] كما يعرف الفيروس ألمعلوماتي على انه عبارة عن برنامج للحاسب الآلي يهدف إلى إحداث أكبر ضرر بنظام الحاسب، وله القدرة على ربط نفسه بالبرامج الأخرى وكذلك إعادة إنشاء نفسه حتى يبدو انه يتوالد ويتكاثر ذاتيا يقوم الفيروس بالانتشار بين برامج الحاسب المختلفة وبين مواقع مختلفة في الذاكرة[2].

وباعتبار أن هذا الفيروس ألمعلوماتي وثيق الصلة بالجريمة المعلوماتية إذ قد يؤدي الى تلف المعلومات أو تغيير مضمونها.

وتتلخص وسائل عدوى الفيروس في ثلاث طرق حددها اتحاد فيروس الكمبيوتر computer virus in dustry vacationبولاية كاليفورنيا الأمريكية فقد يكون من خلال فعل الأجهزة او من خلال شبكات الاتصال، وقد حدد هذا الاتحاد 4 مراحل للعدوى هي:

- عدوى الذاكرة الإضافية الثابتة.
- عدوى الملفات المشتركة.

[1] هدى حامد قشقوش جرائم الحاسب الالكتروني في الشريع المقارن دار النهضة العربية القاهرة 1992 ص 99
[2] عبد الفتاح بيومي حجاي ـ الجريمة في عصر العولمة ـ ط 1 دار الفكر الجامعي مصر2008 ص 145

- عدوى الذاكرة الداخلية.
- عدوى الذاكرة الإضافية المتغيرة[1] .

3-جرائم النصب والاحتيال: إن أساس جريمة الاحتيال (النصب) يتمثل في الاستيلاء على المال المنقول المملوك للغير بنية التملك يتم برضا المجني عليه في جريمة النصب نتيجة لما وقع عليه من تأثير احتيالي من الجاني

يتحقق الاحتيال المعلوماتي كلما كانت هناك نية تحقيق ربح مادي غير مشروع للجاني ينتج عنه خسارة مادية تلحق بالمجني عليه وكان استخدام الحاسوب وسيلة لارتكاب الاحتيال او تسهليه أو التعجيل بتنفيذه.

ويذهب البعض الأخر الى تعريفه على انه التلاعب العمدي بمعلومات وبيانا تتمثل قيما مادية يختزنها النظام ألمعلوماتي او الإدخال غير المصرح به لمعلومات وبيانات صحيحة او التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة او أي وسيلة أخرى من شأنها التأثير على الحاسوب حتى يقوم بعملياته بناءا على هذه البيانات أو الأوامر والتعليمات من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير[2] ، ومن مظاهر هذا النوع من الجرائم: خرق التعاملات عبر الطرق جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي تزال يقع فيها عدد كبير من مستخدمي الانترنت.

أما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

المطلب الثاني: أركان الجريمة الالكترونية.

[1] احمد خليفة الملط المرجع السابق ص323
[2] بتصرف نهلا عبد القادر ص 189/188

رغم أن من الصفات البارزة في الجريمة المعلوماتية والمتمثل في خاصية صعوبة اكتشافها إلا أنه كان إلزاما على المختصين إثباتها بكامل أركانها والمتمثل في:

الفرع الاول: الركن الشرعي.

ويقصد به وجود نص قانوني يجرم الفعل ويوضح العقاب المترتب عليه في حالة وقوع هذا الفعل كما انه يقصد به الصفة غير المشروعة التي تكون نتيجة انطباق نص التجريم المنصوص عليه في القانون على السلوك أو الفعل الذي اقترفه الفاعل ويمكن لهذه الصفة ان تزول عن الفعل إذا توفر سبب من أسباب الاباحة الذي ينبغي عنه هذه الصفة[1].

فهناك العديد من الجرائم الالكترونية التي لا ينطبق عليها أي وصف قانوني فكان إلزاما على أي مشرع إن يأخذ هذا التقدم التكنولوجي بعين الاعتبار، وان يقوم بتطوير الوسائل اللازمة، أهمها قواعد التجريم لردع هذا الاجرام الالكتروني والذي اخذ بالتزايد والانتشار بشكل مذهل دون معوقات قانونية سواء من المشرع أو المجتمع ككل عن طريق توعية الافراد بالأضرار التي تخلفها هذه السلوكات، وفي العديد من الدول تبقى الجهود الفردية من قبل أصحاب المؤسسات بوضع بعض أنواع الحماية والثغرات الالكترونية[2].

تعتبر الجريمة المعلوماتية كغيرها من الجرائم عملا غير مشروع يجرمه القانون ويعاقب عليه ،وذلك بالنظر لما يقرره القانون الجنائي والقوانين المكملة له من اوامر ونواهي تجرم وتعاقب كل سلوك ترى فيه السلطة المختصة بالتشريع انه يرقى لدرجة التجريم لما يشكله من مساس بمصالح الجماعة وتعريضها بوجه عام للخطر.

[1] عميمر عبد القادر المرجع السابق ,ص 87

[2] باطلي ,المرجع السابق ,ص,44

وبالعودة للنص التشريعي الذي يعزز مبدا الشرعية المتمثل في قانون العقوبات "لا جريمة ولا عقوبة او تدبير امن بغير نص[1] "

وقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بالجرائم الجنايات والجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويشمل على 08 مواد تهتم بذكر كل أنواع الاعتداءات على الانظمة المعلوماتية، وإن كان من المستحسن أن يعتمد مشرع الجريمة شمل هذا النمط من الجرائم المستحدثة بنص قانوني خاص بها وإلى غاية تكريس ذلك يبقى المنهج المعتمد من طرفه سليما نوعا ما ويتفق مع وجود ظاهرة إجرامية مستجدة تستلزم ضرورة التدخل لتجريمها وإفراد عقوبات مناسبة لها، تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير محرمة قانونا فقد عمد المشرع إلى وضع نصوص خاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ليساير بذلك كل الاتجاهات التشريعية المعاصرة في هذا الشأن.[2]

وفي إطار الجريمة المعلوماتية فقد أجمع أغلب فقهاء القانون الجنائي على ضرورة سن نصوص قانونية، يجرم من خلالها المشرع الأفعال والانتهاكات التي تقع على الانظمة المعلوماتية، او من خلالها وفي نفس السياق أصدر المجلس الأوروبي سنة 1989 توصية بهدف تشجيع الدول الاعضاء على تبني نصوص عقابية خاصة بالجريمة المعلوماتية[3].

[1] راجع القانون 155/66 المؤرخ في 1966/06/8 المتضمن قانون العقوبات الجزائري المعدل والمتمم الى غاية 02/16 المؤرخ في 2016/06/19

1

بلعيد منصورية النظام الاجرائي للجريمة المعلوماتية في التشريع الجزائري ,مذكرة لنيل شهادة الماستر ,كلية الحقوق والعلوم السياسية ,جامعة عبد الحميد بن باديس مستغانم ,2020 ,ص21

واختلفت الدول في الطريقة التي نظمت بها هذا الامر فمنها من أدرج هذه النصوص ضمن قانون العقوبات كما هو الحال بالنسبة للمشرع الجزائري ومنها من وضع قانونا خاصا بالجرائم المعلوماتية[1].

الفرع الثاني: الركن المادي.

يجب ان يكون الفعل او السلوك المحرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته ونحن لا نتكلم عن الركن المادي في الجرائم المعلوماتية التي يكون وسيلة ارتكابها إلكترونيا حيث لا يمكن حصرها تحت تكييف واحد، فقد تشكل واقعة قذف او سب او تهديد او تحريض على أفعال غير مشروعة بشكل مطابق للجريمة التقليدية المقررة في قانون العقوبات ويمكن ان ينطبق التفسير الوارد في النصوص التقليدية على هذه الصور[2].

إن السلوك الاجرامي بوصفه الركن المادي والذي تقوم عليه الجريمة التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن صعوبة الجريمة الالكترونية والركن المادي فيها خاصة ان الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك بها ماديا مثل التيار الكهربائي الذي يسرى في توصيله دون أن نراه.[3]وبالتالي نلاحظ ان المشرع الجزائري لم يشترط ضرورة أن تترتب نتيجة معينة بل اكتفى بتوفر السلوك المادي لقيام الجريمة المعلوماتية، بغض النظر عن الضرر الذي تسبب فيه هذا السلوك للضحية .

[1]عميمر عبد القادر ,المرجع السابق ,,ص 87,88
[2]باطلي غنية ,المرجع السابق ,ص 45
[3]عبد الله دغش العجمي المشكلات العملية والقانونية للجرائم الالكترونية ـ مذكرة لنيل درجة الماجيستر قانون عام جامعة الشرق الأوسط الكويت ص27

والدليل على ذلك ان القانون يعاقب على مجرد الدخول للمنظومة المعلوماتية والذي يتحقق بمجرد الوصول الى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبها لان هذا النظام لا يسمح للدخول فيه الا لأشخاص معينين او يسمح بالدخول لكن مقابل نفقات.

دون اشتراط حصول ضرر عن هذا الدخول بل جعل تحقق النتيجة في الدخول والبقاء عن طريق الغش في المنظومة المعلوماتية كظرف مشدد وليس شرطا للعقوبة.

وللتنويه فقط فان المقصود بالبقاء هو التواجد داخل نظام المعالجة البلية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام ويتحقق هذا البقاء غير المشروع عند دخول شخص النظام بتصريح ولكن تجاوز المدة المسموح له فيها بالبقاء ،او يكون ذلك التحول خطا او سهوا في نظام آخر ولم ينسحب فورا ولا يقطع وجوده او يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط ،هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات[1] زيادة على ذلك فان القانون يعاقب على مجرد الشروع في هذه الافعال بنفس العقوبة المقررة للجريمة التامة ويعدو ان يكون الضرر مجرد ظرف مشدد للعقوبة او محلا لدعوى مدنية للمطالبة بالتعويض.[2]

ونجد ان الجريمة المعلوماتية تقوم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت.

مما يجعل الامور تزداد تعقيدا لدى السلطات الامن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون المعلومات والبرامج عبارة عن نبضات إلكترونية غير مرئية تنسب الى النظام المعلوماتي مما يجعل ضم الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة.[3]

[1] انظر المادة 394 مكرر ق ع ج
[2] عميمر عبد القادر ص89
[3] نهلا عبد القادر ص56

كما أن الوصول إلى المتعدي في الوقت الحقيقي Real time أمر جد صعب ومعقد حيث يجب على المحققين التوصل إلى المجرم في الوقت الذي يبدأ بالاتصال وارتكابه للجريمة لأنه من خلال تقنية الحصول على عناوين الحواسيب المتصلة مباشرة بها وليس عنوان مصدر الاتصال، وحتى وان تم معرفة المصدر الاصلي فقد يكون العنوان خاطئ وحتى وإن تم اكتشافها فمن الصعب جدا ملاحقة ومتابعة مرتكبها(فاعلها). كون الجاني يمكنه تدمير الدليل بسرعة مذهلة ولا يترك مجالا لضبطها، ومما يزيد في صعوبة إثباتها هو عدم مساعدة المجني عليهم السلطات فيما لو تم اكتشافها وأكثر من ذلك فإن أغلب القواعد الجنائية غير كافية لوجود صعوبات أخرى تتمثل في البحث عن الدليل وجمعه ومشكلة قبوله إن وجد ومدى مصداقيته وحجيته في إثبات وقائع الجريمة[1].

وتجدر الاشارة إلى ان النشاط أو اسلك المادي في الجريمة المعلوماتية يتطلب توفر بعض الشروط أو الظروف التي تتلاءم مع خصوصية هذا النوع من الجرائم التي ترتكب في بيئة رقمية ومن طرف شخص يفترض فيه قدر من المعرفة بجهاز الحاسوب وطريقة استخدامه، فالسلوك غير المشروع الذي يقوم به المجرم المعلوماتي والذي يعد أساسيا لقيام الجريمة المعلوماتية يدور في نطاق هذه البيئة ويستمد منها خصوصياتها لكونها جريمة يقوم على فعل يستخدم تقنية المعلومات عن طريق المنظومة المعلوماتية كوسيلة لارتكابها أو للاعتداء على هذه المنظومة، وبالتالي يختلف النشاط أو السلوك غير المشروع في الجريمة المعلوماتية باختلاف نوع الجريمة المرتكبة بحيث تتنوع جريمة معلوماتية من جرائم ترتكب بواسطة المنظومة المعلوماتية وأخرى ترتكب ضد هذه المنظومة.[2]

الفرع الثالث: الركن المعنوي.

[1] غنية باطلي المرجع السابق ص46
[2] عميمر عبد القادر ص89

لقد أثر استخدام الوسائل التقنية الحديثة في ارتكاب الجريمة على الفكرة او التصور القديم المتعارف عليه بشأن سذاجة والانحطاط الثقافي للمجرم والظروف الاجتماعية القاسية لهذا الشخص المبرز لخطواته الاجرامية على نحو ملفت للانتباه يستدعي الخوف وأخذ الحيطة والحذر منه، فالوضع اليوم مختلف حيث أصبح المجرم الالكتروني يتمتع بقدر من الفطنة والذكاء ونصيب اوفر من التعليم والاختصاص، فبالنسبة للجرائم الالكترونية لابد من توفر قدر كبير من المعرفة في مجال تقنية المعلومات والحاسوب. حيث أصبحت أصابع الاتهام موجهة للمتعلمين وذوي الاختصاص.

ويعد الركن المعنوي ضروريا بالقيام الجريمة من الناحية القانونية فلا يكفي مجرد وانما يشترط القانون أن تكون هناك رابطة نفسية تربط الجاني بالفعل المادي الذي قام بارتكابه وهو ما يعرف بالركن المعنوي للجريمة فلا جريمة بدون ركن معنوي.

ويتكون القصد الجنائي من عنصريين هما العلم والادارة والذي يعد شرط ضروريا لقيام المسؤولية الجزائية وإذ انتفى أحد الشرطين المذكورين أو كليهما ينتفي معهما القصد الجنائي الذي لا تقوم المسؤولية الجزائية بدونه، ويتخذ القصد الجنائي صورا متعددة فقد يكون القصد عاما أو خاصا، ومباشر وغير مباشر فالقصد العام متوفر في جميع الجرائم العمدية وهو انصراف إرادة الجاني لتحقيق الفعل المجرم مع العلم بعناصر هذا الفعل المنهي عنه قانونا، كالاعتداء على الحق في الحياة في جريمة القتل العمد مثلا.

أما القصد الجنائي الخاص فهو الغاية التي يسعى المجرم المعلوماتي لتحقيقها من خلال ارتكاب الجريمة، وهذا النوع من القصد يتطلب توفره في بعض الجرائم فلا يكفي مجرد تحقيق الغرض من الجريمة، بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم من هنا نسأل عن

القصد الذي يجب توفره في الجريمة المعلوماتية. إن المجرم الالكتروني يتوجه من أجل ارتكاب فعل غير مشروع أي غير مسموح به مع علم هذا المجرم بأركان الجريمة.[1]

وبالتالي فإنه يستوجب أن يعلم مرتكب جريمة الدخول أو البقاء الغير مشروعين داخل نظم المعالجة الآلية للمعطيات أن دخوله إلى هذا النظام غير مشروع أو غير مصرح به فلا يتوافر القصد الجنائي إذا وقع الجاني خطأ كأن يجهل وجود حظر للدخول أو البقاء[2].

إلا انه في الغالب ما يبرر المخترقون الأنظمة والبرامج معلوماتية أفعالهم بأنهم مجرد فضوليين وأنهم قد تسللوا صدفة فلا انتفاء للعلم كركن للقصد الجنائي، كما يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الاطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في الكثير من الأحيان إلى حد العبقرية[3].

إلا أن ما يشير البس حول ما إذا كان القصد الجنائي المطلوب توفره هو القصد العام أ، القصد الخاص هو استعمال المشرع الجزائري لمصطلح عن طريق الغش فأعتبر البعض أن هذه العبارة تعبر على نية المشرع في اشتراط توفر قصد خاص في هذه الجريمة وهو نية تسبب ضرر للغير في ماله أو في حقوقه المختلفة ألا أن هذا الرأي منتقد، لأن عدم إضافة مصطلح الغش إلى نص التجريم يؤدي إلى فهم النص فهما خاطئا بما معناه تجريم فعل إدخال المعلومات وتعديلها ومحوها. وهي من المهام الأساسية لمبرمجي الأنظمة المعلوماتية ومستخدميها وبالتالي فعنصر الغش ضروري لقيام هذه الجريمة. وهذا يعني اشتراط المشرع قصد خاصا لقيام الجريمة لأنه ليست هناك وقائع أخرى يجب أن يتجه إليها قصد الجاني على

[1] بلعيد منصورة ,المرجع السابق ,ص 26
[2] لعاقل فريال ,الجريمة المعلوماتية في ظل التشريع الجزائري ,مذكرة لنيل شهادة الماستر ,في القانون العام ,تخصص القانون الجنائي و العلوم الجنائية ,جامعة آكلي محند اولحاج ,البويرة ,2015,ص 40
[3] بلعيد منصورة ,المرجع السابق ,ص ,40

خلاف بعض التشريعات الأخرى كالقانون البرتغالي والتركي، والفنلندي التي اشترطت لقيام الجريمة المعلوماتية توفر قصد الأضرار بالغير وقصد تحقيق كسب غير مشروع للجاني وللغير فيما يشترط المشرعين الجزائري والفرنسي توفر القصد الخاص لقيام هذه الجريمة[1].

المبحث الثاني: الإطار المفاهيمي لدليل اثبات الجرائم المعلوماتية.

يعد إثبات الجريمة المعلوماتية أحد المهام الحيوية لتحقيق، ولكنه يواجه تحديات كبيرة تتعلق بخصوصية الدليل في الجريمة الرقمية نظرا لطبيعة هذه الجرائم وما تتميز به ن تعقيدات التي بدورها تخلق عائق امام اثباتها والكشف عنها فهي تحتاج الى ادلة ذات طبيعة خاصة ومختلفة عن الادلة الجرائم التقليدية حيث تستخدم تقنيات ناجمة عن الحاسوب والمتمثلة في الدليل الإلكتروني أو ما يسمى بالرقمي وهذا ما ستناوله في هذا المبحث من خلال التطرق الى مفهومه في المطلب الاول والى انواعه وتقسيماته في المطلب الثاني

المطلب الاول: مفهوم دليل الاثبات في الجرائم المعلوماتية.

بما اننا في مجال الجرائم الالكترونية فان وسائل وطرق اثباتها يكون بواسطة الدليل الالكتروني وقبل التطرق الى تعريف الدليل الإلكتروني وخصائصه علينا اولا معرفة تعريف الدليل الجنائي وتميزه عن الاثبات الجنائي ثم التطرق الى تعريف الدليل الرقمي وكل ما يشمله هذا الدليل من خصائص ومميزات عن باقي الادلة الجنائية من خلال فرعين الفرع الاول تعريف الشامل لدليل الاثبات ثم تعريف الدليل الرقمي ثم دراسة خصائصه في الفرع الثاني.

الفرع الاول: مفهوم العام لدليل الاثبات الجنائي.

أولا: تعريف الدليل الجنائي وتميزه عن الاثبات الجنائي.

1. تعريف الدليل الجنائي:

[1] عميمر عبد القادر ,المرجع السابق ,ص 91,92

أ ـ تعريف الدليل لغة: هوما يستدل به والدليل الدال ايضا ، وبفتح الدال وكسرها ودلوله بالضم والفتح على يقال أدل فأمل والاسم الدالة لتشديد اللام . وفلان يدل فلان اي يثق به[1].

ب_ تعريف الدليل شرعا: وهو ما يلزم العلم به شيء اخر ' وغايته ان يتوصل العقل الى التصديق اليقيني بما كان يشك في صحته اي التوصل به الى معرفة الحقيقة.

والدليل في الاصطلاح الشرعي يقصد بها الحجة والبرهان اي ما يثبت فهي كل ما بين الحق[2]، وهذا باتفاق الفقهاء وجاء ذكر الدليل في القران الكريم لقوله تعالى "" الم تر الى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس دليلا[3] ""

ج . تعريف الدليل في الاصطلاح القانوني: تعددت التعريفات والمحاولات الفقهية بخصوص الدليل الإلكتروني.

ـ فعرف " بانه الوسيلة المبحوث عنها في التحقيقات بغرض اثبات صحة واقعة تهم الجريمة او ظرف من ظروفها المادية والشخصية "

وعرف ايضا بانه " هو النشاط الاجرائي الحال والمباشر من اجل الحصول على يقين القضائي وفقا لمبدأ الحقيقة المادية وذلك ببحث او تأكيد التهام او نفيه.

وعرفه قضاة المحكمة العليا بما يلي "الدليل هو البينة او الحجة التي يستمد منها القاضي البرهان على اقتناع بالحكم الذي يصدره قد يكون الدليل مباشرا كالاعتراف وشهادة شهود وتقرير الخبرة او غير مباشرة كالقرائن[4] "

---

[1]ابن منظور لسان العرب ـ الطبعة الثالثة ـ دار الصادر المجلد الحادي عشر , لبنان 1994 ص 249ص 248

[22]شهرا زاد حجيبه الدليل الإلكتروني في مجتال الاثبات الجنائي ـ مإكرة لنيل شهادة ماستر قانون جنائي اجنائي للأعمال جامعة العربي بن مهيدي ـ ام البواقي 2017/2016 ص11

[3]سورة الفرقان الآية رقم 45

[4]نصر دين مروك ـ محاضرات في الاثباتالجنائي ـ الجزء الثاني ت دار هومة للطباعة والنشر والتوزيع ـ بوزريعة الجزائر 2004 ص 8

من خلال التعريف السابقة يمكن تعريف الدليل الجنائي بانه هو معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية لإثبات صحة افتراض ارتكاب شخص للجريمة او دحضه وذلك لرفع او خفض اليقين والاقتناع لدى القاضي في واقعة محل الخلاف. وعلى ذلك فالدليل في المواد الجنائية اهمية عظيمة لأنه هو ال ينصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحول الشك الى اليقين.

فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بان يكون او لا يكون وهذا لا يتحقق بالدليل بحسبان انه معبر عن هذه الحقيقة.

2- تميز الاثبات الجنائي عن الدليل الجنائي.

كثير ما يتم الخلط بين مفهوم الاثبات والدليل ويعبر عن واحدة بالخرى ويبدو كأنهما كلمتان مترادفتان ولكي نستطيع الفريق بينهما علينا معرفة مدلول الاثبات.

تعريف الاثبات الجنائي: الإثبات هو إقامة الدليل إمام القضاء بالطرق واقعية قانونية ترتبت اثارها. ويعتبر الاثبات الوسيلة العملية التي يعتمد عليها الاطراف في صيانة حقوقهم المترتبة عن الوقائع والاداة الضرورية التي يعول عليها القاضي في التحقيق من هذه الوقائع[1].

اما الدليل فهو الواقعة التي يستمد منها القاضي البرهان على اثبات اقتناعه بالحكم الذي ينتهي اليه اي المحصلة النهائية لكل مراحل الاثبات المختلفة او بعبارة اخرى ثمرة الاثبات[2].

3-الانظمة القانونية في الاثبات الجنائي.

ونظرا لأهمية الاثبات في القانون ادى الى اختلاف الانظمة القانونية في تنظيمه فظهرت ثلاث انظمة في الاثبات اعتمدتها االقوانين الوضعية في نظامها القانوني للأثبات:

[1]شيخ سناء ادلة الاثبات المكتوبة التقليدية والإلكترونية في القانون الجزائري النشر الجامعي الجديد ـ دار نشر لطباعة ـ توزيع تلمسان الجزائر ص11

[2]نصر الدين مروك ـ نفس المرجع ص 9

1-نظام الاثبات المطلق

هذا النظام لم يحدد القانون طرقا معينة للإثبات حيث انه منح للخصوم الحرية في اختيار الادلة التي يرونها تؤدي الى تكوين قناعة القاضي وللقاضي له حرية في تقييم وتقدير الادلة المعروضة عليه كما يسوغ له القضاء بعلمه الشخصي بما يناسب حكمه[1].

2-نظام الاثبات المقيد.

عكس النظام السابق فهو يقوم على الحدود التي رسمها القانون، فان للمشرع دور رئيسي في الاثبات وذلك من خلا ل تحديد المسبق للأدلة المقدمة اثناء الدعوى والتي يلجا اليها القاضي الجنائي اثناء اصدار حكمه.

3-النظام المختلط.

هو مزيج بين النظامين حيث قام بالأخذ بمبدأ حياد القاضي ، والادلة وتعين قوة البعض منها في الاثبات وذلك لتحقيق الاستقرار في المعاملات ، وقد اعطى للقاضي سلطة تقديرية واسعة في الادلة التي لم يحدد قيمتها القانون كالشهادة.

ولقد اخذت بهذا النظام اغلب التشريعات كالقانون الفرنسي والبلجيكي كما اخذ به المشرع الجزائري في نظامه القانوني ويتجلى هذا في المادة212 من قانون الاجراءات الجزائية والتي تنص على انه ".. يجوز اثبات الجرائم لأي طريق من طرق الاثبات ماعدا الاحوال التي لم ينص فيها القانون على خلاف ذلك[2]. ""

الفرع الثاني: تعريف الدليل الرقمي.

1/ تعريف الدليل الرقمي في الفقه.

[1]شيخ سناء المرجع السابقص 12

[2]بتصرف ـالهام بولطامين الاثبات الجنائي في المجال الالكتروني مذكرة مكملة لنيل شهادة الماستر جامعة العربي بن مهيدي - ام البواقي 2018/2017

تم تعريفه على انه " الدليل المأخوذ من اجهزة الكمبيوتر والذي يكون في شكل مجالات او نبضات مغناطيسية او كهربائية يمكن تجميعها او تحليلها باستخدام برامج تطبيقات وتكنولوجيا وهو مكون رقمي لتقديم المعلومات في الاشكال المتنوعة مثل: النصص مكتوبة او صور او أصوات او إشكال ورسوم وذلك من اجل اعتماده امام اجهزة انفاذ وتطبيق القانون[1] "

والذي يلاحظ على هذا التعريف انه يقصر مفهوم الدليل الرقمي على ذلك الدليل الذي يتم استخراجه من الاسب الالي ولا شك ان ذلك فيه تضييق لدائرة الادلة الرقمية فهي كما يمكن ان تستمد من الحاسب الالي فمن الممكن ان يتحصل عليها من اية الة رقمية اخرى فالهاتف وآلات التصوير وغيرها من الاجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن ان تكون مصدرا لدليل الرقمي[2] وهناك من عرفه على انه "كل بيانات يمكن اعدادها او تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما "

اما الاستاذ كيسي "فيعرف الادلة الجنائية الرقمية بانها "تشمل جميع البيانات الرقمية التي يمكن ان تثبت تن هناك جريمة قد ارتكبت او توجد علاقة بين الجريمة والجاني او بين الجريمة والمتضرر منها""

اما التعريف المقترح للدليل الالكتروني من قبل المنظمة الدولية لأدلة الحاسوب IOCE)
(بأنه المعلومات المخزنة او المتنقلة في شكل ثنائي ،ويمكن ان يعتمد عليها في المحكمة ، وهو نفس المعنى تقريبا المتبنى من قبل الفريق العلمي العامل على مستولى الادلة الرقمية باعتبار هذا الاخير أنشئ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية لأدلة الحاسوب

[1] عميمر عبد القادر ص 103

امير فرج الله ـ الاثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها ـ الطبعة الاولى الناشر مكتبة الوفاءالاسكندرية مصر 2016 ص 287

[2]

وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استرداد المحافظة ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة[1] .

بعد استعراضنا للتعريفات التي قيلت بشأن الدليل الإلكتروني نلاحظ في البداية انها متقاربة من بعضها البعض وأنها حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته وارتباطه بالتقنية الرقمية. الا ان هناك بعض الملاحظات ينبغي الاشارة اليها:

1. هناك خلط في تعريف الدليل الإلكتروني بمفهوم برامج الحاسب الالي عند بعض الفقهاء، حيث تم اعتبار هذا الدليل كبيانات يتم ادخالها الى جهاز الحاسوب وذلك لإنجاز مهمة ما وهذا التعريف ينطبق تماما مع مفهوم برامج الحاسوب الالي"

الان هناك فرق بين الدليل الالكتروني وبرامج الحاسوب يكمن في الوظيفة التي يؤديها كل واحد منهما فهذا الاخير له دور في تشغيل الحاسوب وتوجيه الى حل المشاكل ووضع الخطط المناسبة وبدونها لا يعدو ان يكون مجرد الة صماء.

اما الدليل الجنائي الرقمي له اهمية كبرى ودور اساسي في معرفة كيفية حدوث الجريمة الإلكترونية، بهدف اثباتها ونسبتها الى مرتكبيها ، لا سيما في البيئة الافتراضية غير المحسوسة حيث يمكن تفتيش القرص الصلب لمعرفة كل مراحل التي مر بها المجرم وهو في سبيل تحقيقه للهدف الاجرامي[2].

الفرع الثالث: خصائص الدليل الرقمي.

نظر لطبيعة الخاصة للجرائم المعلوماتية فان دليل اثباتها يتميز الدليل الجنائي الرقمي عن الدليل الجنائي التقليدي لان هذا النوع من الادلة يعيش في بيئة متطورة بطبيعتها تشتمل

[1] عائشة مصطفى بن قارة المرجع السابق ص 55/54

[2] بتصرف ـعائشة مصطفى بن قارة نفس المرجع ص 56ص 57

انواع متعددة من البيانات الرقمية تصلح مجتمعة او منفردة لكي تكون دليلا للإدانة او البراة ، فيعد ذلك بذلك الدليل الرقمي الوسيلة الرئيسية في عملية اثبات الجرائم المعلوماتية [1]، ويتميز الدليل الإلكتروني بعدة خصائص نذكرها كما يلي:

أولا . الدليل الالكتروني دليل علمي:

يتكون هذا الدليل من بيانات ومعلومات ذات هيئة الكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب ادراكها الاستعانة بأجهزة ومعدات ' وادوات الحاسبات الالية واستخدام نظم برامجية حاسوبية فهو يحتاج الى مجال تقني يتعامل معه 'وهذا يعني انه كدليل يحتاج الى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات ولأجل ذلك فان ما ينطبق على الدليل العلمي ينطبق على الدليل الالكتروني فكما للدليل العلمي له منطقه الذي لا يجب ان يخرج عليه ، اذ يستبعد تعارضه مع القواعد العلمية السليمة فان الدليل الالكتروني له ذات الطبيعة ، فلا يجب ان يخرج هذا النوع من الادلة عما توصل اليه العلم الرقمي والا فقد معناه[2].

ثانيا: الادلة الرقمية متطورة بطبيعتها.

:الذلة الرقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان الى اخر عبر الشبكات الاتصال غير معترفة بحدود الزمان والمكان وتعتمد الادلة الجنائية على التطور التلقائي لبيئتها التقنية المتطورة بطبيعتها ومن خلال الدليل الرقمي يمكن رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه ان يسجل تحركات الفرد كما انه يسجل عاداته وسلوكياته وبعض الامور الشخصية عنه لذا فان البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل التقليدي.

ثالثا : الدليل الرقمي دليل غير ملموس:

[1] عميمر عبد القادر المرجع السابق ص105

[2] عائشة مصطفى بن قارة نفس المرجع ص61 ص62

يرى البعض ان الدليل الرقمي دليل غير ملموس ، وبالتالي فانه دليل ليس له حيز مادي بخلاف الدليل التقليدي ، الان ترجمته واخراجه في شكل مادي ملموس لا يعني هذا تجميع المادي هو الدليل بل ان هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية الى هيئة التي يمكن الاستدلال بها على معلومات معينة الا ان هناك من يذهب الى ابعد من ذلك ويرى ان قابلية الدليل الرقمي تزيد من مثوقيته اذا رعيت في ذلك الاصول العلمية في هذه العملية والشروط المطلوبة في الشخص القائم بها[1].

رابعا: صعوبة طمس او حذف الادلة الرقمية:

الأدلة الرقمية يمكن استرجاعها بعد محوها واصلاحها بعد اتلافها واظهارها بعد اخفائها مما يؤدي الى صعوبة التخلص بعد اتلافها واظهارها بعد اخفائها مما يؤدي الى صعوبة التخلص منها وهي خصيصة من اهم خصائص الدليل الرقمي بالمقارنة مع الدليل التقليدي فهناك العديد من البرامج الحاسوبية التي وظيفتها استرجاع البيانات التي تم حذفها او الغائها سواء تم ذلك بالأمر delete))او حتى لو تم عمل اعادة التهيئة او تشكيل للقرص الصلب باستخدام الامر formatوالبرامج التي تم اتلافها او اخفائها سواء كانت صورا او رسومات او كتابات او غيرها مما يعني صعوبة اخفاء الجاني لجريمته او التخفي منها عن اعين الامن والعدالة طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة ، بل ان محاولة الجاني محو الدليل الرقمي بذاتها تسجل عليه كدليل حيث ان قيامه بذلك يتم تسجيله في ذاكرة الالة وهو ما يمكن استعماله كدليل ضده[2] .

خامسا: الدليل الإلكتروني قابل للنسخ.

[1] عميمرمحمد المرجع السابق ص 106

[2] امير فرج الاثبات الجنائي للجريمة الإلكترونية والاختصاص القضائيبهاص 289

حيث يمكن استخراج نسخ من الادلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في الانواع الأخرى من الادلة، مما تشكل ضمان شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق النسخ طبق الاصل من الدليل.

سادسا: السعة التخزينية العالية: حيث يتميز الدليل الإلكتروني بسعة تخنية عالية فآلة الفيديو الرقمية يمكنها تخزين مئات الصور ، ودسك صغير يمكنه من تخزين مكتبة صغيرة[1].

ـ نظر لهذه الخصائص التي يتميز بها الدليل الإلكتروني عن باقي الادلة تقودنا الى التساؤل حول موقع الدليل الرقمي بين الادلة الجنائي وللإجابة على هذا الاشكال علينا اولا معرفة تقسيمات الدليل الجنائي وتصنيف الدليل الرقمي من بين الادلة.

المطلب الثاني: تقسيمات الدليل الرقمي:

قبل التطرق الى تقسيمات الدليل الرقمي علينا اولا معرفة انواع الادلة الجنائية باعتبار الدليل الإلكتروني دليل جنائي رقمي ومعرفة موقع الدليل الرقمي من بين الادلة الجنائية فنظر لطبيعته المختلفة عن باقي الادلة جعلته محل خلاف بين الفقهاء حول طبيعة الدليل الرقمي

وباعتباره أداة قوية في إثبات الجرائم المعلوماتية حيث يتضمن توفير الأدلة الرقمية اللازمة لدعم القضايا المتعلقة بالجرائم المعلوماتية فلابد اولا دراسة نوع الادلة الجنائية وتصنيف الدليل الرقمي فيها وهذا ما سنراه في الفرع الاول ثم انواع الدليل الرقمي في الفرع الثاني.

الفرع الاول: انواع الادلة الجنائية:

يمكن رد التقسيمات التي وصفها فقهاء القانون الجنائي للدليل الى الانواع التالية:

أولا: من حيث مصدره.

[1] عائشة مصطفى بن قارة المرجع السابق ص 64

ينقسم الدليل من حيث مصدره الى: مادية، وقولية وقانونية وفنية

1-الدليل المادي: وهو الدليل الذي ينبعث من عناصر مادية ناطقة بنفسها ،وتؤثر في اقتناع الشخصي بطريق كمباشر فقد يترك الجاني في مكان الجريمة بعض الادوات التي تم استخدامها في ارتكابها ' ويترك بصمات اصابعه او اقدامه او غير ذلك من الظواهر التي تفيد القاضي في الاثبات وجدير بالذكر ان الحصول على هذه الادلة المادية قد يكون عن طريق المعاينة او التفتيش او الضبط او الخبرة.

2- الدليل القولي او اشفهي:

هو ذلك الدليل الذي ينبعث من العناصر الشخصية تتمثل فيما يصدر من الغير من اقوال تؤثر في اقتناع القاضي بطريقة مباشرة من خلال تأكده من صدق هذه الاقوال والادلة الشفوية هي اعترف المتهم وأقوال الشهود.

3- الدليل القانوني: هو ذلك الدليل الذي حدده المشرع ، ويبين قوته بحيث لا يمكن للقاضي ان يعطي لهذا الدليل قوة اكثر مما اعطاها له القانون ، وهذا هو الاصل في المواد المدنية اما في المسائل الجنائية فان الادلة غير محصورة فالقاضي حر في تكوين عقيدته من اي دليل في الدعوى مع مراعاة الاستثناءات التي ترد على حرية الاقتناع في مجال الاثبات الجنائي كما هو الحال في جريمة الزنا .[1]

4- الادلة الفنية: وهي الادلة التي تستخلص من الخبرة اي من راي الخبير وهذه الادلة اذا كانت كافية في الاثبات تسمى ادلة الاثبات وإذ اكانت ناقصة تسمى ادلة نفي[2].

ثانيا . من حيث صلتها بالجريمة:

[1]نصر دين مرروك المرجع السابق ص 13
[2]نصر دين مروك ـ نفس المرجع ص 19

1/ الأدلة مباشرة: ان لهذه الأدلة أهمية كبيرة أذانها تؤيد وجود علاقة مباشرة بين المتهم والجريمة المرتكبة، وهذه الادلة اما ان تكون ادلة مادية او معنوية، فوجود الأموال المسروق حيازة المتهم يعد من الأدلة المادية المباشرة، أما شهادات الشهود الذين أدركوا وقوع الجريمة بإحدى حواسهم الخمسة فتعد من الأدلة المعنوية المباشرة.

2/ الأدلة غير المباشرة: وهي عبارة عن عدة حقائق تتعلق جميعها بحادثة معينة بالذات ، ومن مجموع هذه الحقائق تتكون سلسلة ظروف يمكن اعتبارها أدلة ثبوتية في تلك الحادثة ، وهذه الأدلة بدورها قد تكون مادية أو معنوية ، ومن الأمثلة على الأدلة المادية غير المباشرة العثور على الأداة التي نفذت بها الجريمة في محل ارتكاب الجريمة وبحيازة المتهم وملابسه ملوثة بالدم من نفس فصيلة دم المجني عليه ، ذلك لأن هذه الأدلة لا تؤيد بصورة قطعية علاقة المتهم بالجريمة موضوع التحقيق لاحتمال كون الدم قد نزف من شخص آخر غير المجني عليه وأن السلاح الذي وجد في حوزة المتهم لا يمكن أن يكون بصورة قاطعة نفس السلاح الذي استعمل في تنفيذ الجريمة لوجود كثير من الأسلحة المتشابهة.

أما الأدلة المعنوية غير المباشرة فيمكن تجسيدها في الأمثلة الآتية:

–شهادة الشهود الذين سمعوا المتهم وهو يهدد المجني عليه بقتله.

–شهادات الشهود الذين يفيدون بوجود عداء بين المتهم والمجني عليه.

–شهادات الشهود الذين يفيدون بأنهم رأوا المتهم والمجني عليه يتشاجران على مقربة من محل العثور على الجثة.[1]

ثالثا. الادلة من حيث الجهة التي يقدم اليها:

[1]د. مازن خلف ـ محاضرة بعنوان /تقسيمات الادلة الجنائية جامعة المستنصرية 2015_2017 ص 1

1. الادلة القضائية: فالدليل القضائي هو الدليل الذي مصدره اوراق الدعوى امام المحكمة سواء كانت في محاضر الاستدلال ام التحقيق.

2. الدليل الغير قضائي: هو الذي لا يكون له اصل في الدعوى المعروضة على القاضي، كان تكون معلومات شخصية يحصل عليها القاضي بنفسه خارج مجلس القضاء[1] .

رابعا . من حيث وظيفته:

1-أدلة اتهام: وهي تلك الأدلة التي متى توفرت لدى المحقق فأنها تكون مهيأة لإحالة المتهم إلى القضاء الجنائي مع رجحان الحكم بإدانته.

2-أدلة الحكم: وهي تلك الأدلة التي يتوافر فيها اليقين التام والقطع الكامل بالإدانة وليس مجرد ترجيح هذه الأدلة.

4-**أدلة نفي**: وهي تلك الأدلة التي تسمح بتبرئة ساحة المتهم من خلال نفي وقوع الجريمة او نفي نسبتها إلى المتهم وهذا النوع من الأدلة لا يشترط فيه أن يرقى إلى درجة القطع واليقين ببراءة المتهم بما اسند إليه من جرم، بل يكفي أن تنال تلك الأدلة ثقة القاضي او تزرع الشك في نفسه فيما توفر لديه من أدلة الإدانة .

5. الدليل من حيث قوة ثبوته:

أ. أدلة كاملة: وهي الأدلة التي تلزم القاضي بالحكم بالعقوبة في القانون إذا توفرت وذلك باعتبار أنها كافية لإقناع القاضي والتأثير في حكمه أيا كان اقتناعه الوجداني الخاص وهذه الأدلة تشمل:

1.شهادة الشهود: وينبغي توافر شاهدي رؤية يشهدان على الواقعة على أن يكونا قد رأيا الواقعة بنفسيهما فلا تقبل الشهادة السماعية، كما ينبغي أن يكونا جازمين في شهادتهما.

[1] عائشة مصطفى بن قارة المرجع السابق ص 65ص66

2.الدليل الكتابي: ولكي يكون الدليل الكتابي كاملا ينبغي أن يتوافر فيه شرطان الأول–أن يكون رسميا او يعترف به المتهم والثاني–أن يكون متعلقا بالجريمة المرتكبة.

3.القرينة: وهي تعد دليلا كاملا متى كانت واضحة وتفيد بالضرورة إثبات ارتكاب المتهم الجريمة.

4.الإعتراف: إذا أعترف المتهم في دور التحقيق وتعزز بأدلة او قرائن أخرى فانه يصبح كافياً للإدانة او التجريم فإذا تعزز اعتراف المتهم بجريمة سرقة مثلا بضبط المواد المسروقة بحوزته او قيامه بالدلالة على مكان إخفائها، فان هذا الإعتراف يصبح كافيا للإدانة وان تراجع المتهم عنه أمام محكمة الموضوع، كما إن الإعتراف بجريمة قتل وتعزز هذا الإعتراف بقيام المتهم بالدلالة على مكان دفن الجثة او مكان إخفائه ملابس او أشياء تعود للمجني علية فأن هذا الإعتراف يكفي للإدانة وان رجع المتهم عن هذا الإعتراف أمام محكمة الموضوع ولكن بشروط وهي:

1.أن يكون الإعتراف مفصلا.

2.أن يكون الإعتراف قد حصل أمام قاضي التحقيق وبحضور عضو الادعاء العام والمحامي المنتدب.

3. أن يكون الإعتراف قد تعزز بكشف الدلالة.

ب– أدلة غير الكاملة: وهي الأدلة الضعيفة او الناقصة التي تجعل المتهم في وضع الاشتباه، أي بمعنى وجود دوافع للشك تسمح بفتح باب التحقيق بيد انه من الممكن أن تكون أدلة مكملة لغيرها تخول القاضي الاستناد إليها في الحكم[1].

[1]د ماز خلف المرجع السابق ص 3 ص 6

– وما يهمنا في هذا المقام هو تقسيم الدليل من حيث نسبته الى مصدره فهو الاساس الذي نقيم عليه المقارنة بين الدليل الالكتروني والادلة الجنائية حيث ينقسم هذا الاخير الى اربعة انواع وهي[1]:

– الدليل القانوني

– الدليل المادي

– والدليل القولي

– والدليل الفني

– لقد حظي هذا النوع من الادلة التي سبق وان شرحنا مفاهيمها بالدراسة من قبل العديد من الفقهاء، خاصة وأنها مرتبطة بشكل مباشر بالوسائل العلمية الحديثة في مجال كشف الجريمة.

– فأين يقع محل الادلة الإلكترونية من بين هذه الانواع؟

– اختلف الفقهاء حول موقع الدليل الرقمي ضمن تقسيمات التقليدية للدليل الجزائي فمنهم من يعتبر الدليل الرقمي صورة متقدمة من الادلة المادية الملموسة التي يمكن ادراكها بإحدى الحواس الطبيعية للإنسان عن طريق الاستعانة بمبتكرات التكنولوجيا الحديثة ومنتجاتها.

الان هناك من يخالف هذا الراي ويعتبر الدليل الرقمي نوع متميز من وسائل الإثباتي وله من الخصائص والمواصفات القانونية ما يؤهله ليكون اضافة جديدة لأنواع الادلة الجنائية[2].

ونحن بدورنا نؤيد هذا الاتجاه، لان الادلة الإلكترونية تتمتع بخصائص جعلتها متميزة عن غيرها من الادلة سواء من حيث البيئة التي تنبعث منها او وهي العلم الافتراضي الغير ملموس او من حيث الشخص القائم على جمعه حيث يشترط فيه على الاقل ان يكون ملما بتقنية المعلومات.

[1] عائشة مصطفى بن قارة المرجع السابق ص66
[22] عميمر محمد المرجع السابق ص108

وهذه الطبيعة الخاصة دفعت الولايات المتحدة الامريكية لإنشاء المنظمة الدولية لأدلة الحاسوب (International O rganization of Computer Evidence).ورافقته بفريق العامل على مستولى الادلة الرقمية) Standard Working)ذلك دليل على تمييزه عن باقي الادلة الجنائية[1] .

الفرع الثاني: انواع الدليل الرقمي

اولا . انواع الدليل الرقمي

يشمل مصطلح الدليل الرقمي كل البيانات والمعلومات الرقمية التي يمكن تداولها رقميا بمختلف اشكالها وانوعها، سواء كانت هذه الادلة متعلقة بالحاسب الالي او غيرها من الاجهزة الاخرى التي تحتوي على النظام المعلوماتي او على شبكة الانترنت او شبكات الاتصال السلطية واللاسلكية، وهو مادي الى تقسيم الدليل الرقمي الى العديد من الانواع:

1.تقسيمه على اساس المصدر:

1.1- الادلة الرقمية الخاصة بأجهزة الكمبيوتر:

يكون مصدر هاته الادلة جهاز الحاسوب او الانظمة المعلوماتية بصفة عامة، وشبكتها الداخلية والتي لا علاقة لها بشبكة الانترنت وتكون الادلة هذه الادلة في شكل اقراص مرنة واقراص صلبة، كما يمكن ان تكون عبارة عن ملفات تترجم بطريق الطباعة او على الشاشة الحاسو ب[2] .

[1] عائشة مصطفى بن قارة . المرجع السابق ص 69 ص70

[2] ممدوح عبد المطلب البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر دار الكتب القانونية , مصر المحل الكبرى ص 88

2 -1- الادلة الرقمية الخاصة بالأنترنت:

وهي الادلة المستخلصة من شبكة الانترنت باتباع الروابط ومحركات البحث المختلفة وتكون على شكل ملفات موجودة في قواعد وبنوك المعلومات الخاصة بالأشخاص وبالمؤسسات ، وتشمل الأنترنت ضمن خدماتها الشبكة العالمية للمعلومات او ما يسمى بالويب وتقنيات التخاطب ، والبريد الالكتروني وبروتوكولات نقل الملفات.

1-3. الادلة الرقمية الخاصة بالبروتوكولات تبادل المعلومات بين أجهزة الشبكة العلمية للمعلومات: تستخدم هذه البروتوكولات لضمان تشغيل نظم الاتصالات على الشبكة المعلوماتية، وهو ما يجعلها مصدرا للأدلة الرقمية نظرا لاحتوائها كافة النشاطات ومستخدمي الشبكة وتحديدها من حيث الزمان والمكان، وتحديد الأجهزة التي تم من خلالها النشاط والاجهزة التي وقع عليها النشاط المجرم قانونا[1].

1-4 . **الادلة الرقمية الخاصة بالشبكة العالمية للمعلومات:**

وهي سلوك انساني يكون فعلا غير مشروع قانونا يقع على أي وثيقة أو نص موجود بالشبكة مثل قرصنة المعلومات وسرقة ارقام بطاقات الائتمان ' وانتهاك الملكية الفكرية للبرامج وغيرها فهذا النوع من الجرائم يتطلب اتصالا بالأنترنت[2].

[1] عميمر محمد المرجع السابق ص 110
[2] شهرزاد حداد المرجع السابق ص 18

– وهناك تقسيم اخر على اساس المصدر وهو الذي قامت به وزارة العدل الأمريكية سنة 2002 الى ثلاث اقسام:

1. السجلات المحفوظة في الحاسوب: وتشمل الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني ورسائل غرف الدردشة، وملف معالجة الكلمات.

2. السجلات التي تم انشاؤها بواسطة الحاسوب: وتعد مخرجات أصلية للحاسوب حيث لم يشارك الأشخاص في اعدادها مثل سجلات الهاتف، وفواتير أجهزة السحب الآلي للنقود.

3. السجلات المختلطة: التي جزء منها تم حفظه بالإدخال ثم تم إنشاؤه عن طريق الحاسب الآلي، منها أوراق العمل المالية التي تم حفظها بالإدخال ثم معالجتها عن طريق برنامج Excel لإجراء العمليات الحسابية عليها[1] .

1. 5: على اساس وسيلة إثبات: كذلك قسم الدليل الجنائي الرقمي الى قسمين:

. أدلة اعدت لتكون وسيلة اثبات: وهي السجلات التي تم انشاؤها بواسطة الحاسوب تلقائيا وتعتبره هذه السجلات من مخرجات الحاسوب التي لم يساهم الافراد في انشائها مثل سجلات الهاتف والفواتير البنكية.

- السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشاؤه بواسطة الحاسوب مثل رسائل غرف المحادثة المتبادلة على الانترنت ورسائل البريد الإلكتروني.

ب ـ أدلة لم تعد لتكون وسيلة اثبات:

النوع من الدليل الالكتروني نشا من دون ارادة الفرد وله اثر يتركه الجاني دون ان يكون راغبا في وجوده ويسمى بالبصمة الالكترونية وتتجسد في الاثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسلة منه او التي يستقبلها وكافة الاتصالات التي تمت ممن خلال

[1]بن فردية محمد محاضر ـ لدليل الجنائي الرقمي وحجيته امام القضاء الجزائي ., كلية الحق والعلوم السياسية جامعة بجاية . الجزائر ص278

الحاسوب وشبكة الانترنت حيث ان هذا النوع من الادلة لم يعد اساسا للحفظ من قبل من صدر عنه غير ان الوسائل الفنية الخاصة تمكن من ضبط هذه الادلة ولو بعد فترة زمنية من نشؤها ل فالاتصالات التي تجرى عبر الانترنت والمرسلات الصادرة عن الشخص او التي يتلقاها كلها يمكن ضبطها بواسطة تقنية خاصة بذلك[1] .

[1]مير فرج يوسف , المرجع السابق ,ص291/290.

الفرع الثالث: صور الدليل الرقمي:

يمكن تصنيف الدليل الرقمي الى ثلاثة صور واشكال رئيسة:

1- النصوص الكتابية: وتشمل النصوص التي تم كتابتها بواسطة الالة الرقمية ومنها رسائل البريد الالكتروني والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسوب ... الخ

2 . التسجيلات: وتشمل وهي التسجيلات التي تم ضبطها وتخزينها بواسطة الالة الرقمية وتشمل المحادثات الصوتية على الأنترنت او الهاتف او غيره.

3. الصور الرقمية: وهي عبارة عن تجسيد للحقائق المرئية ،وهي التي تمثل تكنولوجيا بديلة للصورة الفوتوغرافية وقد تبدو اكثر تطور ولكنها ليست أفضل من صور التقليدية.

اما فيما يتعلق بالتشريع الجزائري فقد اوردت المادة السادسة من القانون09/ 04 اجراء يسمح لسلطات البحث والتحري بنسخ المعطيات محل البحث وكذا معطيات اللازمة لفهمها على دعامة تخزين الالكترونية قابلة للحجز وهو ما جعل البعض ان المشرع الجزائري قد حافظ على البيئة التي يتواجد فيها الدليل الرقمي[1].

[1]عميمر محمد المرجع السابق ص15ص16

خلاصة.

لقد تطرقنا في هذا الفصل الى الإطار العام للجريمة المعلوماتية حيث تناولنا مفهوم الجريمة المعلوماتية والتي حظيت بعدة تعريفات والتي تميزت بالاختلاف لتطور المستمر لهذه الجريمة فهي تختلف عن الجريمة التقليدية وهذا ما جعلها تتميز بخصائص عدة من حيث بيئتها او وسائل ارتكابها وغيرها من الخصائص وحاولنا الالمام بأنواعها فهي متعددة ومتنوعة لا يمكن حصرها في نوع معين وبعدها تناولنا اركانها الشرعي والمادي والمعنوي مع ذكر موقف المشرع الجزائري منها ومحاولته مواكبة تطور هذه الجريمة. ونظر لطبيعة الخاصة لهذا النوع من الجرائم جعلت من مسالة اثباتها امر صعب وهذا ما تناولناه في المبحث الثاني وهو ادلة اثبات الجريمة المعلوماتية والتي تتمحور حول الدليل الرقمي بحكم البيئة التي ترتكب فيها الجريمة الالكترونية فهي بيئة افتراضية رقمية، قمنا بطرح التعاريف التي تناولته والتطرق الى خصائصه وتميزه عن باقي الادلة الجنائية بحكم طبيعته بعدها ذكرنا مسالة تصنيفه من بين الادلة وتقسيمات هذا الدليل. وهذا ما يقودنا الى التعرف على طرق استخلاصه وحجيته في الاثبات في الفصل الثاني.

الفصل الثاني

الاحكام الاجرائية لادلة اثبات الجرائم المعلوماتية

تمهيد:

يعتبر استخلاص الدليل الرقمي أحد الخطوات الحاسمة في عملية جمع الأدلة الرقمية واستخدامها كدليل في الاثبات. يتضمن هذا العمل العديد من الإجراءات التي تهدف إلى استخراج المعلومات الرقمية القابلة للاستخدام وتحليلها بطريقة تضمن صحتها وموثوقيتها مما يجعل منها دليلا للإثبات في الجرائم الالكترونية من خلال تقدير هذا الدليل من طرف القاضي الجزائي ،فالأمر يختلف عن الجرائم التقليدية بحكم التعامل مع عالم افتراضي .لذلك ارتأينا ان نوضح كبقية استخلاص الدليل من خلال اجراءات جمع الادلة الجنائية الرقمية والوسائل والادوات المتبعة في ذلك في المبحث الاول من هذا الفصل والتطرق الى حجية هذه الادلة في الاثبات من خلال سلطة القاضي الجزائي في تقييم وتقدير الدليل الالكتروني في المبحث الثاني .

المبحث الأول: اجراءات استخلاص الدليل الرقمي.

لقد وضع المشرع الجزائري كغيره من المشرعين قواعد وضوابط وقام سن مواد قانونية تكفل السعي لمكافحة السلوكاتالتجريمية المعلوماتية والتي خصها بإجراءات ووسائل تستهدف متابعة مجرمي المعلوماتية سنتناولها في هذا المبحث والذي تم تقسيمه لمطلبين:

المطلب الأول: اجراءات جمع الدليل الالكتروني.

كما سبق وان ذكرنا ان الجرائم المعلوماتية او الرقمية تختلف اختلافا كليا اذ ما قارنها بالجرائم التقليدية وبالتالي فان هذا التباين قائم اساسا الى عدم وجود اثار مادية ملموسة ومن خلال هذا المطلب سنتناول كل من الاجراءات بما فيها من التقليدية والحديثة وكذا وسائل اثبات الجريمة المعلوماتية

الفرع الاول: اجراءات التقليدية استخلاص الدليل الرقمي.

غالبا ما يكون مسرح ارتكاب الجريمة المعلوماتية مركبا من بيئتين احداهما تقليدية وثانية افتراضية تحتوي كلاهما على مجموعة من العناصر والمعطيات التي تساعد في الكشف عن الجريمة وظروف ارتكابها لذلك يتم اللجوء الى الاعتماد على اساليب منظمة اجرائيا لاستخلاص الدليل الذي يبنى عليه اسناد المسؤولية الجزائية واثبات الجريمة[1] وهي كما هو منصوص عليها قانونا المعاينة، التفتيش، الضبط، شهادة الشهود، الخبرة.

1المعاينة:

المقصود بالمعاينة في الجريمة المعلوماتية هو الوقوف على الاثار التي يخلفها مستخدم النظام المعلوماتي حيث يعتبر الانتقال الى عين المكان اولى الخطوات التي يقوم بها رجال الضبطية القضائية في تعاملهم مع مسرح الجريمة لمعاينة واثبات الاثار والمخلفات المادية

[1]علي عبد الله اجراءات استخلاص الدليل الرقمي مجلة دفاتر البحوث العلمية المجلد 9 العدد 1 الناشر ص 229

والمحافظة عليها واثبات حالة الاماكن والاشخاص عن طريق الكتابة والتخطيط والصور ويمنع احداث اي تغيير في معالم مسرح الجريمة كما يراعى وقت وتاريخ التقاط صور الفيديو والسرعة في اتخاذ الاجراءات الكفيلة بإثبات هوية بعض الحضور وسماعهم وفي بعض الحالات منعهم من مغادرة الامكنة واخطار نيابة الجمهورية بطلك فورا كما يجب التأكيد على ضرورة التقيد بالنصوص القانونية التي تنظم اجراءات المعاينة من اجل اضفاء طابع الشرعية على الاجراءات وعدم المساس بالحقوق والحريات الفردية او التعرض لها الا في حدود ما يسمح به القانون احتراما لمبدا قرينة البراءة ،وفي الاخير يجب تدوين المعاينة بكافة تفاصيلها في محضر لتمكين القاضي من الاطلاع عليها، وقد نصت المادة (42) ق اج ج على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو مخول لجهاز الضبطية القضائية _كما سبق الذكر_ سواء في المرحلة العادية او حالات التلبس ،ويترتب على تغيير او تعديل يطرا على المكان وقوع الجريمة الجزاءات المنصوص عليها في المادة (43) ق ا ج ج[1]وحتى يكون التفتيش في بيئة الكتارونية لابد ان يتم ضمن مستويين تتمثل في تفتيش المكونات المادية للحاسب الالي والتي تمثل مسرح الجريمة التقليدي وايضا تفتيش المكونات المعنوية للحاسوب والتي تمثل مسرح الجريمة الافتراضي[2]

مسرح الجريمة المعلوماتية للمعاينة:

1 –مسرح الجريمة التقليدي (الجرائم الواقعة على المكونات المادية):

وهو المسرح الذي يقع خارج بيئة الحاسوب يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب للمسرح الجريمة التقليدية ومن امثلة هذه الجرائم الواقعة على اشرطة

[1] راجع المادتين 43/24 ق ا ج ج

[2] لعلمي جليلة ,مزري صالح ,الدليل الرقمي والاثبات الجنائي ,مذكرة لنيل شهادة الماستر ,تخصص قانون جنائي وعلوم جنائية ,جامعة قاصدي مرباح ورقلة ,2022,ص 08

الحاسب والكابلات الخاصة به ومفاتيح التشغيل والاقراص وغيرها من مكونات الحاسب ذات الطابع المادي المحسوس[1] .

2. مسرح الجريمة الافتراضي: ويقع عادة داخل البيئة الالكترونية ويتكرر من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الاقراص الصلبة الموجودة بداخله وفي مقدمتها الجرائم الواقعة على برامج الحاسب الالي وبياناته والتي تتم بواسطتها وكذلك الجرائم التي تتم بطريقة الانترنت ومنها جرائم التزوير المعلوماتي والتخريب[2] .

2. القواعد الاجرائية لمعاينة مسرح الجريمة المعلوماتية:

هي اجراءات يتعين اتباعها عند اجراء المعاينة ولقد نص المشرع الجزائري ضمن ق. أ .ج والمتمثلة في:

اخطار وكيل الجمهورية: لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الالية للمعطيات الا بعد اخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضباط الشرطة القضائية وهذا ما نصت علي المادة 42 من ق.ا.ج.

واعمالا بنصوص المواد 18، 32. 42 63 من ق.ا.ج بالإضافة الى نص المادتين 42. 49 ق. ع الجزائري من وواجبات ضباط الشرطة القضائية إذا ما عملوا بأية جريمة بان يقوموا بإخطار وكيل الجمهورية سواء كان مدنيا او عياريا باعتباره المسؤول المباشر الشرطة القضائية على ان يكون الاخطار مسبوقا بتأكيد ضباط الشرطة من وقوع الجريمة فعلا.

ـ اوقات المعاينات: نص عليها المشرع ج في المادة 47 ق.ا.ج على الاوقات التي يجوز فيها القيام بإجراء المعاينة.

[1]عبد الفتاح البيومي مبادىء الاجراءات الجنائية في جرائم الكمبيوتر والانترنت ط1 دار الفكر الجامعي الاسكندرية مصر 2006 ص160
[2]عائشة بن قارة ,المرجع السابق ,ص ,87

الفترة او المدة التي يكون بين السعة 5صباحا و8مساءا الا في حالة ما طلب صاحب المنزل ذلك او تم توجيه نداءات من داخل السكن او في حالات استثنائية اقرها القانون.

غير أنه اجاز هذه الاجراءات في اي وقت من النهار او الليل في الجرائم المنصوص عليها في المواد من 342 الى غاية 348وذلك داخل كل فندق أو منزل مفروش او محل لبيع المخدرات ومن على شاكلته وعندما يتعلق بجرائم الماسة بأنظمة المعالجة الالبية للمعطيات وكذا جرائم تبيض الاموال وغيرها من الجرائم وفق هذه المادة في كل ساعة من ساعات النهار او الليل وذلك بناءا على اذن مسبق من وكيل الجمهورية المختص.

رضا صاحب المسكن: وفقا للمادة 64 ق .ا.ج فانه لا يجوز تفتيش المساكن ومعاينتها وضبط الاشياء المشتبه فيها الا برضا صريح من الشخص الذي تتخذ لديه هذه الاجراءات وكذلك الامر بخصوص الجرائم الواقعة على على النظم المعلوماتية هذا ما نص عليه المشرع ج في نص المادة 64 ق .ا.ج

ومن بين الاجراءات التي يتعين اتباعها عند اجراء المعاينة ما يلي:

1عدم التسرع في نقل اي نقل اي مادة معلوماتية في مكان وقوع الجريمة وذلك قبل اجراء الاختبارات اللازمة للتيقن من عدم وجود اي مجالات مغناطسية في المحيط الخارجي حتى لا يحدث اي اتلاف للبيانات المخزنة.

2القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية ذات الصلة بالجريمة ورفع ما قد يوجد عليها من بصمات واثار مادية .

3ربط الاقراص الكمبيوترية التي تحمل مع جهاز يمنع الكتابة او التسجيل عليها مما يتيح للمحققين قراءة بياناتها دون تغيريها.

4. التحفظ على محتويات سلة المهملات والقيام بفحص الاوراق والشرائط والاقراص الممغنطة المحطمة المتواجدة فيها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة[1]

ثانيا . التفتيش:

هو اجراء من اجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر لذلك يعتبر من اهم اجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسفر عن ادلة مادية تؤيد نسبة الجريمة للمتهم ولمزيد من التوضيح نذكر العناصر التالية:

. شروط التفتيش: تنقسم شروط التفتيش الى قسمين شروط شكلية وموضوعية :

الشروط الشكلية للتفتيش :

حددت المادة 44 من ق.ا.ج سيما بعد التعديل الذي حصل بموجب قانون 22.06 في 20 سبتمبر 2006 وهي:

1. وجود اذن مكتوب صادر عن وكيل الجمهورية او قاضي التحقيق

2. استظهار بالإذن قبل الدخول المنزل المراد تفتيشه

3. ان يتضمن الاذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الاماكن المقصودة بالتفتيش

4. حضور الشخص المعني بالتفتيش مكانه او من ينوب عنه

5. في حالة رفض حضور يستدعي ضبط الشرطة القضائية شاهدين من غير موظفين خاضعين لسلطته[2].

6. محضر التفتيش في الجرائم المعلوماتية في الجرائم المعلوماتية: يتم تحرير محضر لكي يثبت فيه ما تم من اجراءات وما اسفر عنه التفتيش من ادلة ولم يتطلب القانون شكل خاص

[1] عائشة بن قارة ص87

[2] زيبحة زيدان الجريمة المعلوماتية في التشريع الجزائري دار الهدى عين مليلة الجزائر 2011,المرجع السابق ,ص 133, 134

للمحضر التفتيش وبالتالي لا يشترط لصحته ما تستجوبه القواعد العامة في المحاضر عموما.

اما في قانون العقوبات الفرنسي فنجده مهدد من الساعة السادسة صباحا إلى تاسعة مساءا طبقا لنص المادة 59 ق.ا.ج ج الا ان هناك حالات استثنائية يصح فيها لجراء التفتيش ليلا او نهارا تتمثل في حالة رضا صاحب المنزل وحالة الضرورة كحالة الاستغاثة من داخل المنزل وحالتي الحريق والغرق وما شبه ذلك.

7. الميقات الزمني لإجراء التفتيش في الجرائم المعلوماتية أشارت إليه المادة74 السالفة الذكر[1].

الشروط الموضوعية: يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة له ويمكن حصرها في ثلاث شروط وهي السبب، المحل، السلطة المختصة بالقيام به وسنفضل في كل شرط على حدي:

محل التفتيش: محل التفتيش في جرائم الحاسوب والشبكة التي تتمثل في مكوناتها الخادم، والمزود الالي والمضيف والملحقات التقنية.

* سبب التفتيش: الهدف من هذا السبب هو الحصول على دليل في تحقيق قائم من اجل الوصول الى حقيقة الحدث ويتمثل في وقوع الجريمة ما جناية او جنحة واتهام شخص او اشخاص معينين في كشف الحقيقة لدى المتهم او في مسكنه او بشخص غيره او مسكنه[2].

.3ـ السلطة المختصة بالتفتيش: ذكرنا سابقا ان التفتيش اجراء من اجراءات التحقيق الابتدائي التي تمس بالجريمة الشخصية وأنهاك حرمة الحياة الخاصة للأفراد لذلك تناتاتل المشرع

[1] عائشة بن قارة ,المرجع السابق ,ص 103,104,111

[2] بن زرت اسيا إثبات الجريمة المعلوماتية في التشريع الجزائري مذكرة لنيل شهادة ماستر تخص قانون جنائي وعلوم جنائية جامعة عبد بن باديس مستغانم, 2019 ,ص , 124

على اسنادها لجهة التي يتيتعةى لها بالتحقيق الابتدائي لتكون صاحب الاختصاص الاصيل بإجراء التفتيش فقد ذهبت بعض التشريعات الى منح هذه السلطة للنيابة العامة.

بخلاف الحال عند كل من الجزائر وفرنسا حيث اخذت بنظام الفصل ما بين سلطتي الاتهام والتحقيق حيث عهدت هذا الاخير لقاضي التحقيق اما الاولى للنيابة العامة.

وإذا كان الاصل ان يقوم قاضي التحقيق او النيابة العامة بإجراء تفتيش بنفسه وهو نادر الحدوث عملا الا انه يمكن لمأمور الضبط القيام بذلك باستثناء حالتين التلبس والانتداب[1].

ـ بطلان اذن التفتيش:

ان مراقبة المحادثات الهاتفية السلكية واللاسلكية وتسجيلها هو اجراء من اجراءات التفتيش الحانه نظرا لخطورة هذا الاجراء باعتباره يتعرض لمستودع السر الفرد ويزيل الخطر على بقاء سريته مقصورة على نفسه ومن اراد ائتمانه عليه فيباح لغيره الاطلاع على مكنون سره فقد حرص الدستور وقانون الاجراءات على تأكيد ذلك واشتراط لمراقبة المحادثات الهاتفية صدور امر قضائي مسبب[2].

ثالثاـــ الضبط :

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها ،ويختلف الضبط في الجريمة في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل وذلك بسبب ان الاول يرد على اشياء ذات طبيعة معنوية وهي البيانات ، والمراسلات ، اتصالات الالكترونية اما الثاني يرد على اشياء مادية منقولة كانت ام عقارات وقد اشارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا واختلاف تشريعيا حول مدى امكانية ضبطها خاصة اذا كانت مجردة من دعامة المادية مثبتة عليها ، يرجع سبب في ذلك ان الضبط. حسب الاصل . لا يرد على الاشياء المادية.

[1] عائسشة مصطفى بن قارة ص 105/104
[2] بن زرت اسيا ص124

وإذا كان الامر قد انتهى بنا الى ضرورة ان يشمل التفتيش المكونات المعنوية للحاسوب فانه من الضروري ان يترتب على ذلك اباحة ضبطها وان كان هذا الامر قد يواجه صعوبات كثيرة من الناحية التشريعية لعدم وجود نصوص خاصة بذلك، خاصة التشريعات العربية ومنها التشريعات الجزائري والمصري[1] .

ولقد نص المشرع الجزائري بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال على انه " عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية المخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل منظومة يتم نسخ المعطيات محل البحث وكذا معطيات اللازم لفهمها على دعامة تخزين الالكترونية تكون قابلة للحجز والوضع في احراز وفق القواعد المقررة في ق.ا.ج" وبالتالي فقد كان اتجاهه هو امكانية حجز المنظومة المعلوماتية برمتها بشروط كما حرص المشرع على جعل المعلومات محل البحث في مأمن باستخدام تقنيات لازمة لمنع الوصول اليها وذلك في حالة استحالة حجزها لأسباب تقنية كما لو كانت معطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها وهو ما نصت عليه م 7 من القانون 09/04 وذلك لمنع تهريبها وتدميرها[2]

ومن خلال ما سبق نستخلص ان هنا نوعين من اجراءات الضبط تسمى الاولى بإجراءات مبدئية تحفيظيه الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهمتها ببقائها في مكانها في النظام المعلوماتي للكمبيوتر او في دعامة التخزين او منع الوصول اليها او الغائها أو التصرف فيها وذلك لكشف مرتكب الجريمة وسهولة اثباتها.

[1] عائشة مصطفى ,نفس المرجع, ص,114
[2] جليلة بلعلمي ,مزري صالح , المرجع السابق , ص17

اما الثانية عبارة عن اجراءات لاحقة بالضبط ويقصد بها جميع البيانات سواء وجذ دعامة تخزين المعلومات او اجذ نسخة من البيانات المخزنة بها او النظام المعلوماتي للكمبيوتر في ورقة او اقراص[1].

الشهادة في الجريمة المعلوماتية:

تعرف الشهادة عامة بأنها " الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق او القضاء بشان الجريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها الى المتهم او براءة منها [2] " والشهادة وسيلة من وسائل الاثبات التي تكتسي اهمية بالغة في الدعوى الجزائية باعتبارها اجراء من اجراءات التحقيق عبر مختلف مراحله من خلالها يتم الحصول على معلومات التي فيها تواجد مسرح الجريمة او كل من توفرت لديه معلومات تفيد في كشف ملابسات الجريمة لإدلاء بها أمام السلطة المختصة اذا كانت الشهادة في الجريمة المعلوماتية لا تختلف من حيث ماهيتها في الشهادة في الجريمة التقليدية ،فان الشاهد في جرائم الحاسوب يختلف من حيث مفهومه عن الشاهد في الجرائم التقليدية . سنتطرق الى مفهومه من خلال:

تعريف الشاهد الالكتروني: الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي ،والذي تكون لديه معلومات جوهرية لازمة للدخول الى نظام المعالجة الآلية للمعطيات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله[3].

طوائف الشاهد الالكتروني: يشمل الشهد الالكتروني عدة طوائف:

[1] **جليلة بلعلمي ,مزري صالح ,المرجع السابق ,ص18**

[2] عائشة بن قارة مصطفى ,ص,125

[3] حليم رامي ,اجراءات استخلاص الدليل الرقمي في الجرائم المعلوماتية ,جامعة البليدة ,الجزائر,دفاتر البحوث العلمية ,المجلد,09,العدد 01 ,2023وص232

1.الفائم على تشغيل الحاسب الالي: وهو المسؤول عن تشغيل الحاسوب الالي والمعدات المتصلة به، ويجب ان تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في ادخال البيانات، كما يجب ان تكون لديه معلومات عن قواعد كتابة البرامج.

2. المبرمجون: هم الاشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم الى فئتين:

تتمثل الفئة الاولى في مخططي البرامج التطبيقات والفئة الثانية تتمثل في مخططي برامج النظم

3. المحللون: المحلل هو الشخص الذي يحلل خطوات ويقوم بتجميع بيانات نظام معين ومعين ودراستها وتحليلها و، وذلك بتقسيم النظام الى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات زكما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدقق البيانات اضافة على ذلك القيام باستنتاج الاماكن التي يمكن ميكنتها بواسطة الحاسب.

مهندسو الصيانة والاتصالات: وهم المسؤولون عن اعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به ،مديرو النظم ،هم الذين يوكل اليهم اعمال الادارة في النظم المعلوماتية بالإضافة الى هاته الفئات هناك اشخاص آجرين يعدون بمثابة شهود في الجريمة الالكترونية ولهم دور كبير في توصيل المستهلك الى شبكة الانترنت ،من بينهم مقدمو الخدمات الوسطية في مجال المعلوماتية والانترنت ايضا متعهدو الوصول ،ومتعهدو الايواء والمسؤولين عن نقل المعلومات ،ومسؤولو متعهدو الخدمات[1] .

[1]عائشة مصطفى بن قارة - ص 127 ص/ص128

5ـالخبرة: هي اجراء يستهدف استخدام قدراي الشخص الفنية والعلمية التي لا تتوافر لدى رجال القضاء، من اجل الكشف عن دليل او قرينة يفيد في معرفة الحقيقة بشان وقوع الجريمة ونسبتها الى المتهم او تحديد ملامح الشخصية الإجرامية.

لهذا فان للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة حيث انه لا يستطيع التعامل مع هذه الجريمة الا شخص ذو دراية وخبرة في مجال الشبكات[1]

ونظرا لان الجريمة المعلوماتية لها خصوصيتها فان الخبير المعلوماتي، لابد ان تتوافر لديهم المقدرة الفنية والإمكانيات العلمية والتقنية في المسالة موضوع الخبرة ،ولا يكفي في ذلك حصول الخبير على شهادة علمية ،بل يجب مراعاة الخبرة العلمية لأنها هي التي تحقق الكفاءة الفنية من اجل كشف الغموض عن الجريمة او تجميع أدلتها والتحفظ عليها، ومساعدة المحققين في ايجاد جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[2]

وللخبير مهام تتمثل:

-تركيب الحاسب الآلي وطرازه ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها.

-بيئة الحاسوب او الشبكة حيث طبيعتها ،تركيزها او توزيعها نمط ووسائل الاتصال.

-المكان المحتمل لأدلة والإثبات وشكلها وهيئتها.

-الآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية.

-كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة او الأجهزة او تدميرها.

-امكانية نقل الادلة الى اوعية دون اخرى والاوعية المادية كالأوراق على ان تكون مطابقة لما هو مسجل على الحاسب الآلي او النظام او الشبكة.

[1]ابتسام بغو ,اجراءات المتابعة الجزائية في الجريمة المعلوماتية ,مذكرة لنيل شهادة الماستر جامعة العربي بن مهيدي ام البواقي 20016ص 21
[2]عبد الفتاح بيومي مبادى الاجراءات في جرائم الكمبيوتر والانترنت 137

شروط صحة الخبرة في الجرائم الحاسوبية: نظرا للأهمية البالغة للخبرة والدور الذي تلعبه في عملية الاثبات في المجال الجنائي فقد حرصت معظم التشريعات، على تنظيم الخبرة ووضع شروط وضوابط لها ومن بين الشروط التالي ذكره:

*اختياره من قائمة الخبراء المحددة اسماؤهم ضمن الجدول المعد مسبقا، وقد نصت المادة 144 ق ا ج ج على ذلك بقولها "يختار الخبراء من الجدول الذي تعده المجال القضائية بعد استطلاع رأي النيابة العامة.

*حلف اليمين القانونية: أذا يجب لصحة الخبير أداء اليمين القانونية وذلك أداء اليمين القانوني وذلك كمله على الصدق والأمانة في عملية وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولا يغني هذا الإجراء أي ضمانة أخرى من الضمانات وقد أوجب المشرع الجزائري بنص "يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس."

وأما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه وفحوصاته يعد تقريرا يضمن خلاصة ما تصل أليه من نتائج بعد تقريرا يضمنه خلاصة ما توصل أليه من نتائج، بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث وان كان المشرع لم يوجب إتباع شكل معين في تقرير الخبرة فقد يكون شفويا وقد يون كتابيا وفقا لما تحدده طبيعة المأمورية[1]

الفرع الثاني: الوسائل المستحدثة لاستخلاص الدليل المعلوماتي:

نتناول في هذا الفرع كما سبق وان أشرنا الى الوسائل المستحدثة لاستخلاص الدليل المعلوماتي والمتمثلة في: التسرب، اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات التقاط الصور وكعنصر أخر إجراء مراقبة الاتصالات الالكترونية.

[1]جواحي عبد الستار المرجع السابق ص 73/ص74

أولا: التسرب

أ/ مفهوم عملية التسريب: عرفه المشرع الجزائري في المادة (65 مكرر12) وان في الأصل ان التعريفات من عمل الفقه، ويرجع سبب ذلك إلى حداثه وخطورة هذا الاجراء.

ويقصد بالتسريب: قيام ضابط او عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق عملية مراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك او جاني. ويلجأ الى هذا الإجراء عادة عندما تقتضي عملية التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر) من هذا القانون وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال والإرهاب، وأيضا الجرائم المتعلقة بالتشريع الخاص بالصرف[1].

والملاحظ ان إجراء المسمى بالتسريب يبدو غريبا وغير مستساغا منذ البداية نظرا لما يكتسبه من خطورة على الحريات وحقوق الإنسان غير أن وضع ضوابط له قد تجعله يقع ضمن الأطراف القانونية المرسومة له فهو من جهة يتم في إطار الاذن المسبق وفقا لمقتضيات المادة (65 فقرة11) ق إج ج والتي أجازت لوكيل الجمهورية إصدار إذن بمباشرة عملية التسرب وذلك لضباط الشرطة القضائية أو أحد أعوانها وتحت مسؤولية ضباط الشرطة القضائية وقد نص المشرع الجرائم المنصوص عليها في المادة (65 مكرر5) والتي من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتسرب[2].

وتمكن الأفعال التي أباحها المشرع للضابط أو العون المتسرب في التالي: نص المشرع صراحة في المادة (65 مكرر14) على أنه يمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض القيام بما يلي:

[1]2عائشة مصطفى بن قارة ص120
[2]زيبحة زيدان المرجع السابق ص169

- اقتناء أو حيازة أ نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها في ارتكاب الجرائم أو مستعملة في ارتكابها.

- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[1].

من خلال هذا النص يتضح لنا أن طبيعة هذه الأفعال تستوجب من القائمين بها مشاركة إيجابية كحيازة متحصلات الجريمة أو وسائل ارتكابها، وهذا النوع من الأفعال له تأثير على المسؤولية الجزائية إلا أن القانون أعفاهم من هذه المسؤولية وذلك بنص صراحة في المادة (65 مكرر14) ".... دون أن يكونوا مسؤولين جزائيا..." ويمتد هذا الإعفاء لظروف أمنية للمتسرب حتى بعدا انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديدها او في حالة تقرير وقف العملية بشرط ألا يتجاوز ذلك مدة 4أشهر سواء من تاريخ انقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخص بإجرائها[2].

شروط صحة إجراء التسرب (المادة 65 مكرر15) ق إ ج ج:

- أن يسلم فقط لضرورة التحري أو التحقيق القضائي.
- أن يكن مكتوبا،
- أن يكون مسببا.

وكل ذلك تحت طائلة البطلان فإغفال أي شرط من هذه الشروط يؤدي إلى بطلان الأذن

- أن يذكر في الأذن طبيعة الجريمة التي ينصب عليها الإذن.
- يذكر فيه ضابط الشرطة القضائية المعني او الذي تتم العملية تحت مسؤوليته.

[1] عائشة بن قارةالمرجعالسابق ص122
[2] عائشة بن قارةالمرجع نفسه ص 123

- يحدد فيه المدة المقررة للعملية والمحددة بأربعة (04) أشهر قابلة للتجديد لمدة أربع (04) أشهر أخرى كلما دعت الضرورة لذلك.

- ان تودع الرخصة اي الاذن في ملف الاجراءات بعد الانتهاء من عملية التسرب[1].

ولقد أجاز المشرع وفقا لنص المادة (65 مكرر18) الاتي نصها: يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهد عن العملية.[2]وبالتالي فإن ضابط الشرطة القضائية اجاز اعتباره شاهد دون سواه غير انه وفي كل الاحوال غير أنه وفي كل الأحوال فإن الأشكال يظل قائما بالنسبة للوصول إلى الدليل الجنائي في الجريمة الالكترونية وما يصاحب ذلك من صعوبة كبيرة ويضاف إلى ذلك ما يشيره الإختصاص القضائي والقانون الواجب التطبيق من صعوبات جمة.

ثانيا: اعتراض المراسلات السلكية واللاسلكية وتسجيل الاصوات والتقاط الصور:

هذه الإجراءات وظفها المشرع من المادة 65 مكرر5 الى المادة 65 مكرر10 ق إ ج ج، سنقوم بتوضيح كل عنصر على التوالي:

1. اعتراض المرسلات: المقصود بإجراء اعتراض المرسلات اعتراض أو تسجيل أو نسخ المراسلات الي تتم عن طريق قنوات أو وسائل الاتصال السلكية او اللاسلكية وهته المراسلات عبارة عن بيانات قابلة للإنتاج، التوزيع، التخزين، الاستقبال والعرض.

2. تسجيل الأصوات: في هذه العملية يتم وضع الترتيبات التقنية وأجهزة التنصت المختلفة دون موافقة المعنيين من أجل التقاط ونسخ وبث وتسجيل الكلام المتفوه، بصفة خاصة، أو يسربه من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، وإخفائها لتلقي أحاديث تفيد في تجلي الحقيقة وتسجيلها.[3]

[1] زيبحةزيدان ,المرجع السابق ,ص171
[2] راجع المادة 65 مكرر 18 ق ا ج ج
[3]

ثالثا . المراقبة الالكترونية :

هذا الاجراء مستحدث بموجب المادة 03 من قانون 09/04المتضمن لقواعد الخاصة للوقاية من جرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها، اجاز تبعا لمستلزمات التحريات والتحقيقات القضائية المتبعة في اطار هذا النوع من الجرائم ، اللجوء الى وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها[1].

1 مفهوم المراقبة الالكترونية:

من خلال القانون رقم 09/04 لم يعرف المشرع الجزائري اجراء المراقبة الالكترونية بل ترك امر تعريفها للفقه فعرفها الفقه على انها " عمل أمنى أساسي له نظام معلومات الكتروني، يقوم فيه المراقب بكسر القاف بمراقبة المراقب بفتح القاف بواسطة اجهزة الكترونية وعبر شبكة الانترنت، لتحقيق غرض محدد افراغ النتيجة في ملف الكتروني وتحرير تقارير النتيجة "

.3 بناءا على التعريف السابق يمكن القول ان المراقبة الالكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها المراقب الكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذو كفاءة وتقنية عالية[2].

.4 والى جانب امكانية القيام بإجراء مراقبة الاتصالات الالكترونية في إطار التحقيقات والتحريات القضائية من اجل الوصول الى ادلة لم يكن بالمقدور الوصول اليها لولا استعمال هذه الوسيلة بالإضافة انه يمكن استغلال تقنية للعمل في بيئة الرقابة من اجل الوقاية من احتمال وقوع الجرائم خطيرة من شانها تهديد امن الدولة وهو ما قررته المادة 4من القانون

[1]بن بادرة عبد الحليم ـاجراءات البحث والتحري عن الجريمة المعلوماتية ـمجلة الحقوق والعلوم الانسانية العدد 23 الجلد 2 ص 86

[2]طاهري عبد المطلب الاثبات الجنائي بالأدلة الرقمية مذكرة نيل شهادة ماستر تخصص قانون جنائي ص 23

04/09 السابق الذكر التي مفادها انه يمكن القيام بهذا الاجراء للوقاية من الافعال الموصوفة بجرائم الارهاب والتخريب والجرائم الماسة بأمن الدولة[1].

ـ شروط المراقبة الالكترونية:

.5 حدد المشرع الجزائري شروط اللجوء الى تقنية المراقبة الالكترونية، وهي ان يتم تنفيذ هذه العملية تحت سلطة القضاء وبإذن مكتوب من السلطة القضائية المختصة، زيادة على ذلك ان تكون هناك ضرورة تتطلب هذا الاجراء وذلك عندما يكون من الصعب الوصول الى نتيجة تهم مجريات التحري او التحقيق دون اللجوء الى المراقبة الالكترونية .وهو ما نصت عليه المادة 04 من القانون 04/09[2] .

المطلب الثاني: وسائل جمع الأدلة الجنائية الرقمية

عند القيام بالتحقيق في جريمة ما ،فانه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة ،وقواعد فنية تحقق الشرعية وسهولة الوصول الى الجاني ، حيث ان الجرائم المعلوماتية طابعها الخاص المميز لها فان التحقيق فيها يحتاج الى معرفة تامة وادراك لوسائل وقوع الجريمة وبالتالي حل لغزها والوصول الى الجاني سنتعرف على هذه الوسائل والطرق والتي تتمثل في وسائل اجرائية ووسائل مادية.

الفرع الاول: الوسائل المادية:

وهي الادوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ اجراءات واساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبيها ونذكر منها :

أولا ــ . عناوينIP والبريد الالكتروني وبرامج المحادثة:

[1]بن بادرة عبد الحليم نفس المرجع ص 86
[2]طاهري عبد المطلب ـ المرجع السابق ص 24

عنوان الانترنتInternet Protocol Adresse هو المسئول عن تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها الى اهدافها وهو يشبه الى حد كبير عنوان البريد العادي ، حيث يتيح للموجهات والشبكات المعنية نقل السالة وهو يوجد بكل جهاز مرتبط بالأنترنت ويتكون من اربع اجزاء كل جز ء من اربع خانات كحد اقصى خانات فيكون المجموع اثنا عشر كحد اقصى حيث يشير الجزء الاول من اليسار الى المنطقة الجغرافية والجزء الثاني لمزود الخدمة والثالث لمجموعة الحاسبات الالية المرتبطة والرابع يحدد جهاز الحاسبة الالكترونية الذي تم الاتصال منه.

وفي حالة وجود أي مشكلة او اية اعمال تخريبيه فان اول ما يجب ان يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الاعمال الغير قانونية ويمكن لمزود خدمة الانترنت ان يراقب المشترك كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي ان تراقبه ايضا اذ ما توافرت لديها اجهزة وبرامج خاصة لذلك.

هذا وتوجد العديد من الطرق يمكن من خلالها معرفة العنوان الخاص بجهاز الحاسبة الالكترونية في حالة الاتصال المباشر على سبيل المثال ما يستخدم في حالة العمل على نظام التشغيل (Windows) حيث يتم كتابة(WINPCFG (في امر التشغيل ليظهر مربع الحوار يبين فيه عنوان IP مع ملاحظة ان عنوان الانترنت قد يتغير مع كل اتصال بشبكة الانترنت[1]

2. البروكسي: يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تتضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الامن وتوفير خدمات الذاكرة الجاهزة وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث في صفحة ما ضمن الذاكرة المحلية المتوفرة فيتحقق البروكسي فيما اذ

[1]سليمان بن مهجع العنزي ' وسائل التحقيق في جرائم نظام المعلومات , رسالة ماجيستر في العلوم الشرطية , جامعة الامير نايف العربية للعلوم الامنية , الرياض , 2003ص 99/98

كانت هذه الصفحة قد جرى تنزيلها من قبل فيقوم بإعادة ارسالها الى المستخدم بدون الحاجة الى ارسال الطلب الى شبكة العالمية. ام انه لم يتم تنزيلها من قبل من قبل فيتم ارسال الطلب الى الشبكة العالمية ' وفي هذه الاخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP ومن اهم مزايا مزود البر وكسي أن ذاكرة المتوفرة لديه يمكن ان تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الاثبات عن طريق فحص تلك العمليات المحفوظة بها التي تخص المتهم والمجودة عند مزود الخدمة[1].

ثالثا ــ برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها الى المستخدم الذي تم اختراق جهازه ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوانIP التي تمت من خلاله عملية الاختراق واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، وارقام داخلها ومخارجها على شبكة الانترنت والمعلومات الأخرى ومن الامثلة على هذه البرامج برنامج hack tracer vl .2 à وهو يتكون من معلومات اساسية تقدم للمستخدم بيان شامل بعمليات الاختراق الي تعرض له جهازه[2].

رابعا: نظام كشف الاختراق:

وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على اجهزة الحاسبة الالكترونية او الشبكة مع تحليلها بحثا عن اي اشارة قد تدل على وجود مشكلة قد تهدد امن الحاسبة الكترونية او الشبكة.

وهذا من خلال مراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الاحداث فور وقوعها في جهاز الحاسبة الالكترونية او الشبكة ومقارنة نتائج تحليل بمجموعة من الصفات المشتركة للاعتداءات على الانظمة الحاسوبية والتي يطلق عليها اهل الاختصاص مصطلح

[1]علي عدنان الفيل ـ اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية دار الكتب والوثائق القومية 2012 ص 70/
[2]علي عدنان نفس الرجع ص71'(

توقيع وفي حالة اكتشاف النظام وجود احد هذه التواقيع يقوم بإنذار مدير النظام بشكل وهذا ما يساعد فريق التحقيق معرفة مرتكبي الجريمة[1].

خامسا: أدوات فحص ومراقبة الشبكات:

هذه الادوات تستخدم في فحص بتوكول الانترنت لعرفة ما قد يصيب الشبكة من مشاكل ، ومعرفة العمليات التي تتعرض لها ’، ومن هذه الادوات:

1. أداة:(ARA) ووظيفتها تحديد مكان الحاسبة الالكترونية فيزيائيا على الشبكة[2]

2. برنامج(visuaul Route s.2a) هو عبارة عن برنامج يلتقط أي عملية فحص عمليات ضد الشبكة ،فيقوم بتقديم اجوبة تبين المعلومات التي حدث فيها مسح ، والمناطق التي مر فيها الهجوم ،وبعد معرفة عنوان IP او اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

3. اداة :(TRACER)تستخدم هذه الاداة في الاساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها اذ انه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف ، ولكن يمكن ايضا من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها[3].

الفرع الثاني: الوسائل الاجرائية :

ويقصد بها الاجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

---

[2]د حسين بن سعد الغافري , التحقيق وجمع في الجرائم المتعلقة بشبكة الانترنت , بحث منشورعلى شبكة الانترنت , موقع والبحوث www. Minshaw.com.

[3]حسين بن سعد الغافري المرجع السابق ص

أولا: اقتفاء الاثر: من اخطر ما يخشاه مجرم نظم المعلومات تقصي ارتكابه للجريمة ،فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنابتها العديد من النصائح اولاها نصيحة هي قم بمسح اثارك فلو لم يقم المخترق بمسح اثاره فمن المؤكد انه سوف يتم القبض عليه حتى وان كانت عملية الاختراق قد تمت بشكل سليم . ويمكن تقصي الاثر بطرق عدة سواء عن طريق البريد الالكتروني تم استقباله او عن طريق تتبع الاثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

ثانيا: الاطلاع على عمليات النظام المعلوماتي واسلوب حمايته: ينبغي على المحقق وهو بصدد التحقيق في الجرائم المعلوماتية الاطلاع على كافة النظام المعلوماتي من مكوناته وشبكاته، كذلك الاطلاع على قاعدة بيانته وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والاجراءات وتصنيف الموارد العامة، ومدى مزامنة الاجهزة ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور. ويتأكد هنا قائد فريق التحقيق على الامور التالية اثناء تعاملهم مع الادلة الرقمية على وجه الخصوص:

1عدم القيام باي عمل من شانه احداث تعديل او تغير اي دليل

2. عدم تنفيذ اية برامج على الحواسيب الموجودة في موقع الجريمة خصوصا البرامج ذات الصلة بأنظمة التشغيل

3. ضرورة عمل نسخة مطابقة للأقراص الصلبة ومن ثم عمل الفحوصات الجنائية على هذه النسخة فقط، سواء تم ذلك داخل مسرح الجريمة او خارجها فيجب عمل نسخة لكامل القرص الصلب وعلى مستوى البت bit وهي اصغر وحدة لقياس كم البيانات الرقمية بحيث تظل النسخة الاولى دون ان تطالها التعديلات[1].

[1]علي عدنان المرجع السابق ص76

المبحث الثاني: السلطة التقديرية للقاضي في تقييم دليل الاثبات في الجريمة المعلوماتية:

تتطلب الجرائم الإلكترونية والجرائم المعلوماتية تحليلًا دقيقًا للبيانات الرقمية والأدلة الإلكترونية المستخدمة لإثباتها. وتشكل هذه الأدلة التي تقدم في القضايا الجنائية الإلكترونية تحديات جديدة للنظام القضائي، خاصة فيما يتعلق بتقييم الدليل الرقمي وتحديد صحته وقوته في إثبات الجريمة. ويعتبر القاضي الجزائي المسؤول الأساسي عن تقييم الدليل الرقمي وتحديد صحته ومدى قدرته على إثبات الجريمة المعلوماتية. وبالتالي، فإن سلطة القاضي الجزائي في تقييم الدليل الرقمي تعتبر محورية في العملية القضائية، حيث يتحتم عليه اتخاذ القرار النهائي بشأن صحة الدليل وإثبات الجريمة المزعومة. ومن المهم أن يكون لدى القاضي الجزائي فهم عميق للتقنيات الرقمية وأساليب جمع البيانات الرقمية وتحليلها. كما يجب عليه أن يلتزم بالمعايير والإرشادات المحددة لتقييم الدليل الرقمي، والتي يمكن أن تشمل التحقق من مصدر الدليل وصحته وتوافق البيانات وغيرها من الجوانب المتعلقة بالدليل.

وهذا ما سنتطرق اليه من خلال دراسة حرية القاضي الجنائي بالاقتناع الدليل في المطلب الاول وحدود سلطته التقديرية في المطلب الثاني.

المطلب الاول: حرية القاضي الجنائي بالاقتناع بالدليل:

يتمثل هذا المبدأ في أن القاضي يجب أن يقوم بتقييم الأدلة والحجج المقدمة أمامه بشكل مستقل وموضوعي، وأن يصدر حكمه بناءً على اقتناعه الشخصي دون تأثر بأي ضغوط أو تأثيرات خارجي .

وفي سياق الجرائم المعلوماتية، يلعب دور مبدأ الاقتناع الشخصي للقاضي دوراً مهماً في تحقيق العدالة وتطبيق القانون على الجانيين، حيث يتعين على القاضي في هذا الصدد أن

يتمكن من فهم الدلائل الإلكترونية والحجج المتعلقة بالجريمة المعلوماتية بشكل كامل، وأن يتمكن من تحليلها وتقيمها بشكل موضوعي ودوم تحيز. وبالتالي يمكن القول إن مبدأ الاقتناع الشخصي للقاضي يعتبر من العوامل الحاسمة التي تؤثر على نتيجة المحاكمة في الجرائم المعلوماتية، حيث يتمثل دور القاضي في تحقيق العدالة من خلال تطبيق القانون بشكل صحيح وموضوعي، لكن نظرا لطبيعة الدليل الالكتروني وما يحتويه على معلومات متعددة يصعب فهمها وتقييمها هذا ما يؤثر بشكل كبير على مجرى الحكم ونتيجة القضية، لذلك جعل المشرع الجزائري كغيره من التشريعات ضوابط قانونية تحكم هذا المبدأ وشروط لقبول الأدلة الرقمية كدليل إثبات في الجريمة الالكترونية.

وهذا ما سنتعرض له في هذا المطلب من خلال التعريج على مفهوم مبدأ الاقتناع الشخصي للقاضي في الفرع الأول وضوابط القانونية لهذا المبدأ في الفرع الثاني ثم نطاق تطبيقه في الفرع الثالث.

الفرع الأول: مفهوم مبدأ الاقتناع الشخصي للقاضي ونطاق تطبيقه

أولا: تعريف مبدأ الاقتناع الشخصي للقاضي

ان من المبادئ الأساسية التي يقوم عليها نظام الإثبات الجزائي هو مبدأ الاقتناع الشخصي للقاضي ،وهو ما استقرت عليه اغلب التشريعات الجزائية ،نظرا لخصوصية التي يتميز بها القانون الجزائي عن القانون المدني [1] ،وقد تعددت الآراء حول تعريف الاقتناع الشخصي للقاضي الجزائي نذكر منها:

تعريف الدكتور محمد زكي ان الاقتناع الشخصي للقاضي ما يتوفر لدى القاضي من الادلة الوضعية ما يكفي لتسبيب ادانة بالتسليم بثبوت الوقائع كما اثبتها في حكمه وينسبها الى

[1]عبد رزاق خامرة ـ عبد القادر حباس ـ حدود حرية مبدا الاقتناع الشخصي للقاضي ـ مجلة الاجتهاد للدراسات القانونية والاقتصادية العدد 10سنة 2021 تاريخ النشر 2021/05/21 ص730

المتهم ،اي انه اعتقاد قائم على ادلة موضوعية او يقين قائم على تسبيب لا على اسباب شخصية[1]

كما عرفه الدكتور عبد الله بن صالح الراشد "بانه تلك الحالة الذهنية او النفسية او ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة لم تحدث امام بصره بصورة عامة"

ومن خلال هذه التعريفات، فان مدلول الاقتناع الشخصي للقاضي الجنائي هو تلك الحرية المعترف بها القاضي الجنائي في تكوينه عقيدته بما يستقر في ضميره وذلك من خلال حريته في تقدير ما يعرض عليه من ادلة ووقائع في الدعوى لتقرير الحكم المناسب اما بالبراءة او الادانة.

وتظهر أهمية الاقتناع الشخصي للقاضي الجزائي فيما يترتب عليه من نتائج والمتمثلة في الدور الايجابي للقاضي وحريته في الاستعانة بالوسائل والأدلة المعروضة في ملف الواقعة ،وفي تقديرها بكل حرية وتكوين اقتناعه منها مجتمعة ومتساندة وتسبيب الحكم الذي ينتهي اليه[2] .

وبالنسبة للمشرع الجزائري فقد نص عليه صراحة وبوضوح في المادة 307 من ق.ا.ج على أنه لا يجب على القضاة تقديم حساب عن الوسائل التي استندوا إليها في تكوين اقتناعهم داو فرض عليهم قواعد يجب اتباعها لتقييم دليل معين بشكل كامل أو كافٍ.،و تشير المادة إلى أن القضاة يجب أن يتساءلوا في صمت عن تأثير الأدلة على إدراكهم للوقائع، وعن أي تأثير قد يكون لوجهات نظر المتهم أو دفاعه عن نفسه على إدراكهم. .

[1]د. محمد زكي ابو عامر نظرية الاثبات الجنائي الفنية للطباعة والنشر اسكندرية ـ مصر ص135

[2]انظر .عبد الرزاق خامرة عبد القدر حباس نفس المرجع ص 732

وتتضمن هذه المادة أيضًا سؤالًا وحيدًا ومهمًا للقضاة، وهو "هل لديكم اقتناع شخصي"، والذي يعكس مسؤوليتهم الأساسية في تقييم الأدلة واتخاذ قراراتهم بشأن الإدانة أو البراءة. ويتعين على القضاة أن يتصرفوا بنزاهة وإخلاص، وأن يتجنبوا أي تأثيرات خارجية على قراراته

ثانيا: نطاق تطبيق مبدا الاقناع الشخصي للقاضي :

لقد ثار الجدل حول تطبيق مبدأ الاقتناع القضائي في القضاء ومراحل الدعوى الجنائية فبالنسبة لطبيعة القضاء، فإن تطبيق هذا المبدأ يمتد إلى جميع أنواع المحاكم الجنائية، سواء كانت محاكم جنايات أو جنح أو مخالفات على الرغم من عدم وجود تحديد واضح لذلك في القانون الجزائري بالنسبة لمحكمة الجنح. بخلاف المشرع الفرنسي الذي نص عليها في المواد 353 بالنسبة لتطبيق هذا المبدأ امام محكمة الجنايات وم 427 بالنسبة لمحكمة الجنح وبالنسبة للمحكمة المخالفات م 536. وبالنسبة لمراحل الدعوى الجنائية، فإن مبدأ الاقتناع القضائي يمتد أيضًا ليشمل مرحلة التحقيق الابتدائي، ويطبق أمام قضاة التحقيق والاحالة، الذين يقدرون مدى كفاية الأدلة دون الخضوع لقواعد معينة أو لرقابة محكمة العليا، ولكنهم يخضعون في ذلك إلى ضمائرهم واقتناعهم الذاتي. أما قضاة الحكم فيقدرون الأدلة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة، وبذلك يمكن القول بأن القضاء يسعى إلى ترجيح الترجيح في الظن أو توكيد اليقين. ويترتب على ذلك أن الشك في مرحلة الاتهام يفسر ضد مصلحة المتهم، بينما يكون في صالحه في مرحلة الحكم[1].

ثانيا: الاستثناءات الواردة على مبدا الاقتناع الشخصي للقاضي الجزائي.

[1] عائشة مصطفى بن قارة المرجع السابق ص244

رغم ان المشرع منح الحرية للقضي الجزائي في تقدير او قبوله الا ان هناك استثناءات واردة على هذا المبدأ حيث قيد المشرع فيها حرية القاضي وان يحتكم بالقانون في هذه الحالات الاتية

. المحاضر ذات الحجية الان يثبت عكسها وهي التي نصت عليها المادة 400 والمادة 218 من ق.ا.ج وهي محاضر ضباط الشرطة القضائية واعوانهم والموظفين واعوانهم في اطار وظيفتهم المنوط لهم بعض اعمال الضبط القضائي تكون لها حجية مالم يثبت عكسها بالكتابة والشهود مالم ينص القانون خلاف ذلك[1].

_المحاضر التي لها حجية اثبات ولا يثبت عكسها الا بتزوير هذه المحاضر اكثر تقيد للقاضي فلا يمكن دحضها الا بالتزوير وهي محاضر محررة من طرف المفتشية العمل وهذا ما اكدته المحكمة العليا في قرارها الصادر بتاريخ 7\01\1984 .والمحاضر الجمركية وهذا ما نصت عليه المادة 241 من قانون الجمارك.

.–القرائن القانونية وهي نوعان قرائن قانونية قطعية كقرينة العلم بالقانون بعد نشره مباشرة في الجريدة الرسمية م 78 من دستور 2020.

وهناك القرينة القانونية البسيطة لها حجية نسبية مثل قرينة البراءة والتي نص عليها المشرع في المادة 41 من الدستور[2] .

المسائل التي تحتاج الى ادلة اثبات خاصة كجريمة الزنا المنصوص عليها في المادة 339 ق.ا.ج وجريمة السرقة في حالة سكر. فالقاضي هنا مقيد بأدلة معينة لإثبات هذه الجرائم[3]

[1]بتصرف.عبد الرزاق خامرة حباس عبد القادر استثناءات الواردة على مبدا الاقتناع الشخصي للقاضي في التشريع الجزائري ـ مجلة الحقوق والعلوم الانسانية المجلد 15 العدد 02 تاريخ النشر 2022/06/15 ص 167

[2]بتصرف ابو طعيمة أسماء ـ جمعي نعيمة ـ الاقتناع الشخصي للقاضي مذكرة لنيل شهادة الماستر تخصص علم الاجرام وعلوم جنائية جامعة عبد الحميد بن باديس ـ مستغانم 2012/2011ص 63

[3]بتصرف **ابو طعيمة اسماء جمعي نعيمة** نفس المرجع ص62ص 69

- اثبات المسائل الغير جزائية المتعلقة بالدعوى أي المسائل الفرعية المتعلقة بجريمة ما كمسائل التجارية او الادارية او غيرها من مسائل غير جنائية فان قاضي الفرع يفصل فيها.

الفرع الثاني: الضوابط التي تحكم مبدا الاقتناع الشخصي للقاضي.

للقاضي سلطة تقدير وحرية الاقتناع بالدليل المعروض أمامه وهذا من خلال المادة 212 من ق ا ج التي جاءت بمبدأ الاقتناع الشخصي للقاضي إلا انه ألزمه بمجموعة من الإجراءات لإضفاء المشروعية على حكمه ،والتي من شانها تامين الوصول بالحكم الى الحقيقة الواقعية بطريق صحيح ومن اهم هذه الضوابط نذكر العناصر التالية:

أ ولا: مشروعية الدليل :

وهو الحرص على مشروعية اجراءات البحث وجمع الادلة ومدى مشروعية الوسائل المتبعة في الاثبات الجنائي وقد كرس الدستور هذ القاعدة الشرعية الاجرائية في المادة 39 والمادة 40 منه 1996[1] والتي تركز على حرمة حياة المواطنين الخاصة، وعدم التعدي عليها وتتمثل مشروعية الدليل في الاجراءات التالية:

1_1 صحة الاجراءات الإجراءات للحصول على دليل:

اشترط المشرع ضرورة احترام حقوق المتهمين والمشتبه بهم في جمع الادلة المتعلقة بجرائمهم ويجب ان يتم ذلك بواسطة اشخاص مؤهلين وفقا للقواعد الاجرائية الواردة في القانون ،ويجب على القاضي ان يعتمد فقط على الادلة التي تم الحصول عليها بطريقة قانونية .ولا يمكن الاعتماد على ادلة تم الحصول عليها بواسطة وسائل غير مشروعة كسرقة محل او التجسس او غيره.

1_2 مدى مشروعية بعض الوسائل العلمية في الاثبات الجنائي:

[1] قانون 03/02 المؤرخ في 27/محرم 14423 الموافق 04/10/ 2002 يتضمن تعديل الدستوري

بالإضافة الى وجوب صحة الاجراءات التي يستند اليها القاضي في حكمه، لا يمكن للقاضي ان يعتمد في حكمه على طرق ولم يقر او لم يعترف بها العلم على سبيل اليقين وتتعارض مع الحريات الفردية للأشخاص مثل استخدام العلاج بالتنويم المغناطيسي، او عقاقير الحقيقة او جهاز كشف الكذب وغيره والتي من شانها ان تحدث تأثيرات فسيولوجية. فالفقه والقضاء يرفضون هذه الطرق كوسائل لإثبات لجريمة وبالتالي يتم استبعاد وقبول وتقدير الادلة المتحصلة منها[1]

بالإضافة الى صحة الاجراءات ومدى مشروعية الدليل لابد على القضاة ايضا احترام مبدا النزاهة والتي ترتبط بالقيم والاخلاق وترتكز على العدالة والانصاف الاساسية للنظام القضائي .

للحرص على احترام هذا المبدأ وضع المشرع في م 65 ف 2 من ق ا.ج حودا لعملية التسرب فحظر على ضابط الشرطة القضائية او عون متسرب من القيام بأفعال من شانها ان تشكل على تحريض ارتكاب الجرائم بغرض الحصول على دليل ضدهم[2].

2قيمة الدليل الغير مشروع في الاثبات:

بالنسبة لقيمة دليلا لغير مشروع في الاثبات في حالة الحكم بالإدانة فهذا متفق عليه بعدم الاخذ به لكن، الاشكال يثور في حالة ما إذا كان الدليل الغير شروع يؤدي الى براءة الشخص، حيث انقسمت الراء حول ذلك الى ثلاثة اتجاهات:

الاتجاه الاول: يرون ان الاصل في الانسان البراءة ولا تحتاج المحكمة لإثباتها بل كال ما تحتاجه هو التشكيك في ادانته بالإضافة الى ان بطلان دليل الادانة الذي تولد عن اجراء غير مشروع انما شرع لضمان حرية المتهم فلا يجوز ان ينقلب وبالا عليه.

[1]بتصرف عبد الرزاق خامرة : عبد القادر حباس حدود مبدا الاقتناع الشخصي للقاضي ص739 ص740

[2] غرس الله كريمة ضوابط حرية القاضي الجزائي في الاقتناع مجلة الاقللعلووم مجلد 8 العدد 2 جامعة البشير الابراهيمي برج بوعريريج 2023 ص48

الاتجاه الثاني: انتقد اصحاب هذا الراي الاتجاه السابق وحجتهم في ذلك انه لا يحق للقضاء ان يقرر قاعدة ا لغاية تبرر الوسيلة كمبدأ قانوني صحيح وإذا بلا اعتمدنا يصبح التزوير وشهادة الزور كلها أمور مشروعة لإثبات البراءة وهذا كلام يرفضه كل عاقل.

الاتجاه الثالث: وهو اتجاه توفيقي اذ انه فرق بين ما اذ كانت الوسيلة الحصول على الدليل تعد في حد ذاتها جريمة ام انها مجرد مخالفة لقواعد الاجراءات، فاذا كان الدليل متحصل من جريمة فانه لا يمكن انن يعتد به. اما إذا كانت وسيلة الحصول على الدليل مجرد مخالفة للإجراءات فيمكن الاستناد اليه في تبرئة المتهم فالبطلان يشوب الوسيلة التوصل الى دليل ولا يصح ان يضار المتهم بسبب لا دخل له فيه[1] .

ثانيا: تسبيب الحكم.

ان تسبيب الحكم الجزائي يقيد القاضي بتأسيس اقتناعه ويخضع للمحمة العليا التي يمكنها الغاء الاحكام المقترنة بعيب انعدام التسبيب فهو حق لأطراف الدعوى لمعرفة الاسباب التي ادت الى الحكم حقهم ويجب على المحكمة ان تقوم الادلة بناء على الجزم واليقين ليس على الاحتمال او الترجيح وان تحرص على صحة الاسباب التي استدل بها القاضي على قناعته ، وقد اصدرت المحكمة العليا عدة قرارات بالنقض لأنها مشوبة بعيب عدم التأسيس . فالقاضي الجزائري يتحمل مسؤولية كبيرة في تسبيب حكمه حيث يحب عليه الاقتناع والاقناع بالأدلة التي تم عرضها امامه[2].

ثالثا . تــساند الادلة :

حتى يكون الاقتناع الشخصي للقاضي صحيح يجب ان يكون مبناه ادلة متناسقة فيما بينها وغير متعارضة وتؤدي مجتمعة

[1]بتصرف. نصر الدين مروك ,المرجع السابق ,ص523ص524ص525
[2]بتصرف عميمر عبد القادر ,المرجع السابق ص 146

الى نتائج مستخلصة منها، فاذا كان هناك تناقض او التخاذل في الادلة يؤدي الى اقصائها. ولذلك فان القاضي ملزم بإيراد الادلة التي اعتمد عليها في مضمون تلك الأدلة وهذا ما سنوضحه في النقاط التالية:

1. بيان الأدلة و مضمونها:

معناه انه متى سند القاضي الى دليل من أدلة الإثبات لإدانة المتهم وجب عليه إن يتعرض إلى أسباب الحكم وما يتضمنه هذا الدليل، فلا يقتصر للإشارة إلى أدلة اثبات دون مضمونها فقد نص ق. ا.ج في م314ف 1 وف 6 و م 379 على وجوب بيان مؤدى الأدلة بيانا كافيا. هذا ولا تكوم المحكمة مطالبة ببيان مؤدى الدليل إلا إذا استندت إليه في حكمها بالإدانة أما إذا لم يستند إليه فإنها غير مكلفة بان تذكره. وترجع الاسباب في ذلك لتمكن الجهات القضائية التي لها الحق في المراقبة الاحكام ومدى مطابقتها للقانون[1] .

2 .انعدام الغموض والابهام :

ان الغموض والابهام قد يشوب ادلة الاثبات لعدم ايراد القاضي لمضمون الادلة او الغموض الذي يعتري تدليله لثبوت الوقائع او نفيها والتي تتعلق بتوافر اركان الجريمة او ضروفها ومن صور ابهام الحكم ان تعرض للمحكمة عدة روايات غير متجانسة دون ان يظهر في الحكم باي رواية اجذ القاضي. فالقاضي ملزم ان ينسب احكامه صفة واضحة ،وذلك كي تستطيع المحمة العليا مراقبتها على وجه صحيح.

3 . انعدام التناقض: تشترط المحكمة في الادلة التي تستند الحكم ان تكون خالية من التناقضات التي تنفي بعضها البعض حتى لا تصبح المحكمة غير قادرة على تحديد الحقيقة واصدار قرار مناسب .وعدم الاعتماد على ادلة متناقضي بدون تفسير واضح لهذا الاختلاف التضاد. على سبيل المثال يمكن ان يحدث تناقض بين دليلين في ملف القضية مما يتطلب

[1]نصر دين مروك , المرجع السابق , ص 645

تفسيرا واضحا للتناقض قبل اتخاذ القرار. تناقض الاسباب والمنطوق او بين شهادة شاهد واخر وتقرير الطب الشرعي. مما يجعل القضية أكثر تعقيدا ويتطلب التحقق من الادلة بشكل دقيق قبل اصدار الحكم[1].

رابعا: عدم حكم القاضي على علمه الشخصي :

ان القاعدة العامة في الاثبات تلزم القاضي الا يحم بمقتضى معلوماته الشخصية في الدعوى او بناءا على ماراه بنفسه او سمعه او حققه ي غير مجلس القضاء وبدون حضور الخصوم والسبب في ذلك ان هذه المعلومات لم تعرض في الجلسة ولم تتح فرصة مناقشاتها. لذلك يجدر بالقاضي الذي توافرت لديه معلومات خاصة عن الدعوى ان يتنحى عن نظرا بعد اعمال اجراءات الرد ويمكن للقاضي ان يدلي في هذه الحالة بأقواله كشاهد.

اما المعلومات العامة عن الاشياء بصفة عامة فغير محظور الحكم بمقتضاه او كذلك يجوز للقاضي ان يستند في حكمه الى راي يقول به العلم او العرف شريطة الا يستند الى راي محل خلاف علمي[2].

خامسا: ان يخضع اقتناع القاضي للعقل والمنطق

يلتزم القاضي بمقتضى بهذا الشرط ، بان يبني اقتناعه على عملية عقلية منطقية تقوم على الاستقراء والاستنباط ينتهي في ختامها الى نتيجة معينة .

فالقاضي حر في ان يعتقد قيمة الادلة المطروحة امامه ولكنه لا يملك التحكم في هذا الاعتقاد فاليقين المطلوب عند الاقتناع ليس اليقين الشخصي للقاضي وانما اليقين القضائي الذي يصل اليه القاضي بناءا على العقل والمنطق.

ولضمان الوصول إلى هذه النتيجة يكون من خلال الاستعانة بالخبراء في المسائل المتطلبة للخبرة فلا تبدي المحكمة رأيها

[1]بتصرف شترة كريمة المرجع السابق ص 44
[2]نصر دين مروك المرجع السابق بتصرف ص 642 ص643

دون الاستعانة بخبير

المطلب الثاني: حجية الدليل الرقمي في اثبات الجرائم الالكترونية:

بما ان للقاضي حرية في قبول الدليل والاقتناع به وفقا لما خول له القانون من ضوابط و قيود لهذا المبدأ ننتقل الآن إلى مسالة تقدير هذا الدليل وحجيته امام القضاء للحكم به والاستناد عليه.

ويقصد بالحجية هي وصف ثابت يحكم الشرع يلحق مضمون الحكم القضائي او الامر القضائي فيه ويكون غير قابل للمناقشة فيه مرة اخرى [1].

وبما اننا في مجال الجريمة الإلكترونية فالأمر يتعلق أكثر بالدليل الرقمي وهذا الاخير لما له من خصوصية تجعله محيطا بمجموعة من ضمانات ووسائل التوثيق تجعله منه دليل دقيق إلا أن هذا لا يمنع من أن يتعرض الدليل الالكتروني للعبث به وتزويره او المسح. وهذا ما أدى إلى اختلاف الفقهاء حول حجية الدليل الرقمي في الإثبات ماذا كانت نسبية او مطلقة؟

سنجيب على هذا التساؤل في هذا المطلب من خلال التطرق الى حجية الدليل الرقمي من الجانب الفقهي في الفرع الاول ثم شروط قبول الدليل الرقمي كحجية في الاثبات في الفرع الثاني وموقف المشرع الجزائري ازاء الدليل الرقمي في مجال جرائم المعلوماتية الفرع الثالث.

الفرع الاول: الآراء الفقهية حول حجية الدليل الرقمي.

لقد ثار النقاش والجدال حول حجية الدليل الإلكتروني في اثبات الجريمة المعلوماتية وهذا نظر لطبيعة هذا الدليل وما يتميز به من خصائص عن باقي الأدلة فا انقسمت الآراء حول حجية الدليل الرقمي في الإثبات الى ثلاثة اتجاهات:

الاتجاه الاول: الحجية المطلقة للدليل:

[1] نور الهدى محمودي حجية الاداة ف اثبات الجريمة المعلوماتية مجلة الباحث للدراسات الاكاديمية العدد 11 جوان 2017 ص918

يرى أصحاب هذا الاتجاه أن دقة وموضوعية الدليل الرقمي والطبيعة الخاصة التي يتسم بها هذا الدليل وهي طبيعة علمية بحتة تجعل القاضي عاجزا عن مناقشة باعتباره وسيلة اثبات تساهم في تقليص سلطته التقديرية وهو ما يؤثر بصورة مباشرة في تكوين اقتناعه الشخصي ويصل الى حد الغائه في بعض الحالات، وهو ما يجعل القاضي امام خيارين اما ان يلغي اقتناعه الشخصي او يسلم بالدليل الرقمي.

الاتجاه الثاني: الحجية النسبية للدليل الرقمي:

تثور فكرة الشك في مصداقية الدليل الرقمي كدليل الجزائي وهو امر لا يتعلق بمضمون الدليل الرقمي في حد ذاته، وانما بعوامل مستقلة عنه تؤثر في مصداقيته لهذا يجب التثبت من الدليل الرقمي من حيث العيوب واخضاعه للتقييم الفني لتفادي تلك العيوب التي تشوبه، ويتم ذلك عن طريق وسائل الفنية من طبيعة هذا الدليل تمكن من فحصه لتأكد من سلامته وصحة الاجراءات المتبعة في الحصول عليه. كمان الدليل الرقمي لا يغني عن الاعتماد على طرق تقليدية للإثبات لان الدليل الرقمي في غالب الاحيان يستعان به في الاثبات ووقوع الجريمة وليس في اسنادها للمتهم او نفيها[1].

اما فيما يتعلق بحجية الدليل الرقمي الناتج عن الخبرة التقنية فانقسم الفقهاء الى ثلاثة اتجاهات:

الاتجاه الاول: يرى أنصار هذا الاتجاه ضرورة تقييد القاضي الجنائي بتقارير الخبير ويتزعم هذا الاتجاه الفقيه" انريكو فيري "والفقيه "جارو " بحيث يرون الزامية ان يتقيد القاضي براي الخبرة وان فكرة او مبدا القاضي خبير الخبراء ء لا يمكن تحقيقها الا إذا تم تكوين القضاة تكوينا في هذا المجال. ويرون ان من الصعب قبول فكرة ان يطرح القاضي تقرير الخبير جانبا فتمكن الخبير من تخصصه والمامه به يجعل تقدير تقريره ليس من صلاحيات القاضي.

[1]محمد عميمر المرجع السابق ص 144

الاتجاه الثاني: برى اصحاب هذا المبدأ ان القاضي لا يقيده راي الخبراء لان القاضي له سلطة مطلقة وحرية كاملة في تقدير الادلة المعروضة عليه ومنها خبرة القضائية المتعلقة بالدليل الرقمي، وان دور الخبير يقتصر على ابداء رايه الفني بخصوص مسالة فنضي. تتعلق بالنزاع المطروح امام القاضي وهو ما يؤكد ان راي الخبير ليس حكما وانما راي استشاري لا يتقيد به القاضي .

الا ان هذه السلطة الممنوحة تحكمها قيود تعين القاضي ' ومن بين الضوابط التي وضعها الفقهاء لهذا الغرض وهي عبارة عن اسئلة نذكرها: هل رعيت القوانين والمبادئ التي تحكم اعمال الخبرة مراعاة دقيقة؟ هل كانت استنتاجات وخلاصة رأي الخبير والأسانيد التي تدعم رأيه مبررة ومسببة تسبيبا كافيا؟[1]

الاتجاه الثالث: وهو راي توفيقي بين الاتجاهين السابقين من خلال التمييز بين مسالتين تتمثل الاولى في القيمة العلمية القاطعة للدليل العلمي ، والمسالة الثانية تتمثل في الظروف التي وجد فيها الدليل لان هذا الامر ليس في مقدوره وهو ما دفعه للاستعانة بالخبير في هذا المجال الان القاضي الان القاضي يمكنه الذهاب الى امر اخر وهو مناقشة الظروف والملابسات التي وجد فيها هذا الدليل والتي في نطاق سلطته التقديرية.

الفرع الثاني: شروط قبول دليل الرقمي دليلا لا ثبات الجريمة المعلوماتية.

بالإضافة الا مشروعية الدليل التي سبق ان تطرقنا اليها والضوابط التي تقيد القاضي لقبوله هذا الدليل ان الدليل الرقمي يخضع في الاصل الى تقد ير القاضي شانه شان بقية الادلة ومنه يكون اقتناعه الشخصي والا ان تقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل باعتبار عمليته وموضوعتيه وحيادته، وانما يمكنه مناقشة الظروف والملابسات التي وجد فيها الدليل.

[1] عميمر عبد القادر المرجع السابق ص 146

أولا ـ القيمة القاطعة للدليل الرقمي :

ان القيمة العلمية للدليل الرقمي من المسائل التي تخرج عن اطار معارف القاضي ومناقشة الحقائق العلمية الثابتة لا يدخل ضمن المهام المنوط بالقاضي وانما يختص به اهل الخبرة ، فهنا ينحصر دور القاضي بشأنه في مراعاة مدى توافر الشروط القانونية فيه من عدمها فاذا توافرت فانه يأخذ به واذا لم تتوافر يستبعده [1] .حيث قد يتعرض الدليل الإلكتروني للعبث والتلاعب به وهو امر لا يمكن للشخص العادي اكتشافه والانتباه له وبالتالي التشكيك في الدليل الرقمي لا يعود على مضمونه وإنما على العوامل مستقلة عنه ولكنها تؤثر في حجيته كدليل اثبات وهو م افرض اللجوء الى استعمال وسيلة فنية من سلا مته وصحة اجراءات الحصول عليه وهذا عن طريق سلامة الاجراءات الوسائل التالية:

1. تقييم الدليل العلمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه: للتأكد من سلامة الاجراءات التبعة للحصول على الدليل الرقمي يمكن اعتماد عدة طرق من بينها :

ـاختبارات داو بورت: حيث يتم اخضاع الاداة المستخدمة في الحصول على دليل الرقمي لعدة تجارب للتأكد من دقتها وذلك باتباع اختبارين رئيسين :

أ. اختبار السلبيات الزائفة: ومفادها ان تخضع الأداة الى اختبار يبن مدى قدرتها على عر كافة البيانات المتعلقة بالدليل الرقمي.

ب . اختبار الايجابيات الزائفة: يتم عن طريق اخضاع الاداة الى اختبار فني يمكن من خلاله التأكد من ان هذه اداة لا تعرض بيانات اضافية جديدة.

2ـــ تقييم الدليل الرقمي من حيث سلامته من العبث: من اهم المعايير المعتمدة لإثبات مصداقيته ويمكن التأكد من هذا من خلال العديد من الوسائل منها طريقة التحليل التناظري،

[1]محمد حمدان عاشولر ' اساليب التحقيق والبحث الجنائي ,اكاديمية فلسطين للعلوم الامنية , فلسطين 2010 ص283

حيث تتمم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بنظام المعالجة الالية للمعطيات فبهذا يتم التأكد من مدى حصول عبث في النسخة المستخرجة ام لا.

كما ان هناك طريقة الدليل المحايد، وهو دليل محايد لا علاقة له بموضوع الجريمة ولكنه يساهم في التأكيد من مدى سلامة الدليل الرقمي المقصود من حيث عدم الحصول على تعديل او تغيير في نظام المعالجة الالية للمعطيات .

من خلال ما تقدم يمكن القول ان التشكيك في سلامة الدليل الرقمي بسبب قابليته للعبث والخطأ في اجراءات الحصول عليه هي مسالة فنية لا يمكن للقاضي ان يقطع في شانها براي حاسم ويعود ذلك لأهل الاختصاص. اذ ان سلطة القاضي في رد الدليل استنادا لفكرة الشك يلزم اعمالها ان يكون هناك ما يرقى لمستوى التشكيك في الدليل وهو ما لا يستطيع القاضي الجزم به ما توافرت في هذا الدليل من شروط السلامة ، فيقتصر دوره على بحث صلة الدليل بالجريمة لان بحث مصداقية هذا الدليل هي من صميم عمل الخبير وليس على القاضي سوى القبول بهذا الدليل وهذا بحكم طبيعته الفنية يمثل اخبارا صادقا عن الواقع[1] .

ثانيا ـ منا قشة الظروف والملابسات التي وجد فيها الدليل:

ان وجود الدليل الرقمي في قضية مطروحة على قاضي الجزائي لا يعني انه ملزم بالحكم بموجبه مباشرة بل ينظر من حيث الظروف والملابسات التي وجد فيها وأحاطت به فإذا تعارض هذا الدليل مع ظروف الواقعة ومدى انطباقه على الوقائع ونسبته الى المتهم هنا يطبق قاعدة الشك يفسر لصالح المتهم ويستبعد الدليل .

الفرع الثالث: القيمة القانونية لدليل الرقمي لدى المشرع الجزائري:

[1] عميمر عبد القادر المرجع السابق ص152

لقد سيطر على نظام الاثبات الجنائي في قانون الاجراءات الجزائية الجزائري مبدا حرية القاضي في الاقتناع ذلك ان نص المادة 212 منه تنص على جواز الاثبات الجرائم باي طريق من طرق الاثبات ماعدا الاحوال التي ينص فيها القانون على غير ذلك والقاضي يصدر حكمه تبعا لاقتناعه الخاص ولا يوجد نص يقيد الاثبات الجنائي في الجرائم المعلوماتية فتخضع بذلك للقواعد العامة في الاثبات .

وبالنظر الى طبيعة الخاصة التي تتميز بها الادلة المتحصلة من الوسائل الإلكترونية وما قد يصاحب الحصول عليها من تلاعب او عبث بالدليل قد يسبب العديد من المشكلات ولذلك فان هذه المشكلات التي تثيرها هذه الادلة تتحد في كيفية ضمان هذه مصداقية الادلة ومدى تعبيرها عن الحقيقة. فهذه الادلة الرقمية تخضع لسلطة التقديرية للقاضي الجزائي فان استراح اليها ضميره وكانت كافية ومنطقية فيمكنه ان يستمد اقتناعه ويسبب حكمه بناءا عليها.

فالمشرع الجزائري لم يضع اي نصوص قانونية صريحة بهذا الخصوص حيث تم الاستناد الى م 212 من ق ا ج السابق ذكرها، الانه ادر كان هذا لا يكفي لوحده وليواكب التطور الحاصل وضع القانون رقم 04/15 المؤرخ في 10 نوفمبر 2004المتمم والمعد ل للقانون 66/ 156 المتضمن قانون العقوبات والذي اقر في القسم السابع مكرر منه تحت عنوان "المساس بأنظمة المعالجة الالية للمعطيات " وكان هذا القانون كنتيجة حتمية لثورة تقنية المعلومات التي مست مصالح غير التي يحميها قانون العقوبات فقد تطرق المشرع الى تجريم افعال المساس بأنظمة المعالجة الالية للمعطيات حيث تضمن هذا التعديل ثمانية مواد من394 مكرر الى 394مكرر 7اين تناول المشرع فيها حماية سرية وسلامة المعلومات .

بعدها تدخل المشرع الجزائري لحماية التعاملات الرقمية حين وضع قانون 09/ 04المتضمن قواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والإتصال ومكافحتها ، من خلال هذا القانون ادرج طريقة ضبط الادلة الرقمية والتي تتخذ صورتين ،

الصورة الاولى تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على ان تكون هذه المعطيات مهيأة بشكل يجعلها قابلة لحجزها ووضعها في احراز حسب ما هو مقرر في قواعد تحريز الادلة الجنائية عموما الانه نظرا لطبيعته الخاصة فانه يخضع لبعض الاجراءات الخاصة التي تحافظ عليه وتحميه من العبث ، وهذا ما اشارت اليه المادة السادسة من القانون 09/04 والتي تلزم السلطات المعنية بعملية الضبط الدليل الرقمي ان تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية[1].

[1]نور الهدى محمودي المرجع السابق ص 922/ص923

خلاصة

بالنسبة لهذا الفصل تناولنا اجراءات ووسائل استخلاص الدليل الرقمي في المبحث الاول والتي تمثل في اجراءات التقليدية والمعتادة في كشف باقي الجرائم وبحكم عدم كفايتها لإثبات الجريمة الالكترونية لوحدها بحكم طبيعة هذا الدليل حيث تطرقنا الى الاجراءات المستحدثة والوسائل الفنية التي تساعد في جمع وتحليل هذا النوع من الأدلة و موقف المشرع الجزائري من خلاله نصوصه القانونية التي جاءت ببعض الاجراءات المستحدثة .اما المبحث الثاني بينا السلطة التقديرية للقاضي الجزائي في تقيم هذه الأدلة من خلال حرية القاضي فالقبول والاقتناع بالدليل الرقمي والضوابط التي تحكمه ثم التطرق الى حجية الدليل الرقمي في الاثبات من خلال الاء الفقهية حوله والخروج منها بجملة شروط لقبول الدليل الرقمي او الالكتروني كدليل اثبات وفي الختام موقف المشرع الجزائري ازاء قبوله كدليل اثبات وصور هذا القبول من خلال النصوص التشريعية التي جاء بها.

خاتمة

لقد حاولنا من خلال هذه الدراسة ان تعالج موضوع ذو أهمية على الصعيدين التشريعي والعلمي فقد تعرضنا إلى مفهوم الجريمة الالكترونية من خلال تناول العديد من التعاريف والخصائص ، كما تطرقنا لجانب من التقسيم النوعي للجريمة المعلوماتية وكذا الاركان التي تقوم عليها هذه الجرائم كغيرها من الجرائم مع بيان موقف المشرع الجزائري اتجاهها مبدئيا ،ثم قمنا بمعالجة صلب الموضوع المتمثل في الدليل الرقمي باعتباره الأداة الاساسية في اثبات الجريمة المعلوماتية .لاعتبار ان الادلة التقليدية غير كافية لوحدها في اثبات هذا النوع من الجرائم ، فهو دليل مستخلص من اجهزة الحاسب الآلي وملحقاته او شبكة الانترنت او اي جهاز اخر له آلية المعالجة او تخزين المعلومات كما ان الدليل الجنائي الرقمي ذو طبيعة فنية تقنية بحتة ،واستخراجه يتطلب طرق واساليب حديثة قائمة على علوم الحاسب الآلي ونظرا لهذا ادرك المشرع الجزائري اهمية هذا النوع من الادلة فعمل على استحداث قواعد اجرائية جديدة ،تتماشى مع خصوصية الجريمة المعلوماتية وادلتها.

وعلى الرغم من القيمة العلمية التي يتمتع بها الدليل الرقمي الا انه يخضع للاقتناع الشخصي للقاضي كغيره من الادلة الجنائية الاخرى، وهذاالإمكانية العبث به او حتى ازالته.

وبناءا على ماسبق تطلب الأمر ان نتقدم بنتائج واقتراحات مما توصلنا اليه من خلال هذا المجهود المتواضع الذي قمنا به.

النتائج:

-لا يوجد الى حد الان اجماع فقهي على تعريف موحد للجريمة المعلوماتية وهذ اراجع للتطور المستمر لهذه الجريمة.

قيام المشرع الجزائري بمعالجة الجرائم المعلوماتية من خلال تعديل قانون العقوبات التمثل في قانون 04/15 المؤرخ في 10 نوفمبر 2004المتمم والمعد ل للقانون 166/15 ولم يخصها بقانون خاص يعالج فيه مختلف انواع الجرائم.

– صعوبة اثبات هذه الجرائم تكمن في طبيعتها ولما تتميز به من خصائص وما يتعلق بادلتها التي تشكل عائق أمام القضاء باعتبارها تستوجب هياكل مادية وبشرية متخصصة في المجال الرقمي.

– هناك صعوبة تكتنف الدليل الجنائي الرقمي من حيث طرق الحصول عليه ومن حيث طبيعته فالحصول عليه قد يحتاج الى القيام بالعديد من العمليات الفنية والعلمية المعقدة اضافة الى التكاليف المالية الباهظة للحصول على وسائل اكتشافه.

– ان التشريع الجزائري لم يعرف الدليل الجنائي الرقمي وذلك بسب أنه يعتمد على نظام الاثبات الحر الذي لا يفرض على القاضي على أدلة جنائية معينة ،زيادة على ذلك يعتبر هذا النوع من الادلة مثلها مثل باقي الادلة الجنائية الأخرى ، تخضع لسلطة التقديرية للقاضي.

إقتراحات:.

– على المشرع الجزائري استحداث قانون جزائي خاص بالجريمة المعلوماتية

– ضرورة تدريب وتأهيل افراد الضبطية القضائية والعاملين في أجهزة القضاء

_. ان اجهزة العدالة الجنائية لم تعد قادرة وحدها على اثبات هذا النوع من الجرائم انكما أصبح من الضروري ان تساند هذه الاجهزة جهات خاصة وتكون عونا لها كأجهزة شرطة متخصصة للبحث والتحري والخب راء لقد حاولنا من خلال هذه الدراسة ان تعالج موضوع ذو أهمية على الصعيدين التشريعي والعلمي فقد تعرضنا إلى مفهوم الجريمة الالكترونية من خلال تناول العديد من التعاريف والخصائص ، كما تطرقنا لجانب من التقسيم النوعي للجريمة المعلوماتية وكذا الاركان التي تقوم عليها هذه الجرائم كغيرها من الجرائم مع بيان موقف المشرع الجزائري اتجاهها مبدئيا ،ثم قمنا بمعالجة صلب الموضوع المتمثل في الدليل الرقمي باعتباره الأداةالاساسية في اثبات الجريمة المعلوماتية .لاعتبار ان الادلة التقليدية

غير كافية لوحدها في اثبات هذا النوع من الجرائم، فهو دليل مستخلص من اجهزة الحاسب الآلي وملحقاته او شبكة الانترنت او اي جهاز اخر له آلية المعالجة او تخزين المعلومات كما ان الدليل الجنائي الرقمي ذو طبيعة فنية تقنية بحثة ،واستخراجه يتطلب طرق واساليب حديثة قائمة على علوم الحاسب الآلي ونظرا لهذا ادرك المشرع الجزائري اهمية هذا النوع من الادلة فعمل على استحداث قواعد اجرائية جديدة ،تتماشى مع خصوصية الجريمة المعلوماتية وادلتها.

وعلى الرغم من القيمة العلمية التي يتمتع بها الدليل الرقمي الا انه يخضع للاقتناع الشخصي للقاضي كغيره من الادلة الجنائية الاخرى، وهذاإمكانية العبث به او حتى ازالته.

وبناءا على ماسبق تطلب الأمر ان نتقدم بنتائج واقتراحات مما توصلنا اليه من خلال هذا المجهود المتواضع الذي قمنا به.

قائـمـة المـراجـع والمصادر

LES REFERENCES

قائمة المصادر والمراجع:

أ . المصادر:

_ القران الكريم

– دستور 1996 القانون 03. 02 المؤرخ في 27 محرم 1423 الموافق ل 10 ابريل 2002

القوانين

1القانون رقم 04/15 المؤرخ 10/نومبر 2004 المتضمن قانون العقوبات المعدل والمتمم لامر 55/156 المؤرخ 8يونيو 1966 الجريدة الرسمية العدد 71 سنة 2004

2القانون رقم 04م09 المؤرخ في 14 شعبان 1430 موافق 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 74 2009

ب المراجع:

1. الكتب

أخمد خليفة الملط . الجرائم المعلوماتية ط 2 دار الفكر الجامعي . الاسكندرية 2006

2ابن منظور لسان العرب . الطبعة الثالثة . دار الصادر المجلد الحادي عشر ، لبنان

امير فرج الله . الاثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها . الطبعة الاولى الناشر مكتبة الوفاء الاسكندرية مصر 2006

3بالمكي نجاة السياسة الجنائية لمكافحة الجرائم المعلوماتية . منشورات دار الخلدونية الجزائر 2017

.4شيخ سناء ادله الاثبات المكتوبة التقليدية والإلكترونية في الفانون الجزائري النشر الجامعي الجديد . دار نشر لطباعة . توزيع تلمسان الجزائر 2021

رستم هشام محمد فريد، الجوانب الاجرائية للجرائم المعلوماتية ،مكتبة الآلات الحديثة ،ط 1 اسيوط ،مصر 1996 ،ص16

عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ،ط1 بدون نشر– زيبحة زيدان الجريمة المعلوماتية في التشريع الجزائري دار الهدى عين مليلة الجزائر 2011

عائشة بن مصطفى حجية الدليل الالكتروني في مجال الاثبات الجنائي: دار الجامعة الجديدة الاسكندرية 2010

عميمر عبد القادر . التحديات القانونية . لإثبات الجريمة المعلوماتية النشر الجامعي تلمسان الجزائر 2021

عبد الفتاح بيومي مبادئ الإجراءات في جرائم الكمبيوتر والانترنت

عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ،دار الكتب القديمة ،مصر ،2007،

عبد الفتاح بيومي حجاي . الجريمة في عصر العولمة . ط 1 دار الفكر الجامعي مصر 2008

عفيف–ي كامل . جرائم الكمبيوتر وحقوق المؤلف والمصنفات . منشورات الحلبي الحقوقية بيروت لبنان 2003

عفيفي كامل عفيفي ،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ،ط1 بدون نشر

علي عدنان الفيل . اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية دار الكتب والوثائق القومية 2012

علي عبد القادر القهوجي . الحماية الجنائية لبرامج الحاسب الالي منشأة المعارف . اسكندرية مصر 1999

غنية باطلي . الجريمة الالكترونية . منشورات الدار الجزائرية 2016

. محمد حمدان عاشولر ' اساليب التحقيق والبحث الجنائي ، أكاديمية فلسطين للعلوم الامنية ، فلسطين 2010

2. د. محمد زكي ابو عامر نظرية الاثبات الجنائي الفنية للطباعة والنشر اسكندرية . مصر

ممدوح عبد المطلب البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر دار الكتب القانونية، مصر

منير محمد الجنبيهي –جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي ،الاسكندرية ،2005،

نصر دين مروك . محاضرات في الإثبات الجنائي . الجزء الثاني ت دار هومة للطباعة والنشر والتوزيع . بوزريعة الجزائر 2004

نهلا عبد القادر المومني . الجرائم المعلوماتية ط1 دار الثقافة للنشر والتوزيع الاردن 2008

هدى حامد قشقوش جرائم الحاسب الالكتروني في التشريع المقارن دار النهضة العربية القاهرة 1992 ص 99

المذكرات :

رسالة ماجيستر:

عبد الله دغش العجمي المشكلات العملية والقانونية للجرائم الالكترونية . مذكرة لنيل درجة الماجيستر قانون عام جامعة الشرق الأوسط الكويت

محمد بن نصير محمد السرحاني مهارات التحقيق الجنائي الفني في الجرائم الحاسوب والانترنت رسالة ماجيستر جامعة نايف العربية للعلوم الأمنية 2004 .

مذكرات الماستر

ابو طعيمة أسماء . جمعي نعيمة . الاقتناع الشخصي للقاضي مذكرة لنيل شهادة الماستر تخصص علم الاجرام وعلوم جنائية جامعة عبد الحميد بن باديس . مستغانم 2012/2011

الهام بولطامين الاثبات الجنائي في المجال الالكتروني مذكرة مكملة لنيل شهادة الماستر جامعة العربي بن مهيدي . ام البواقي 2018/2017

بلعيد منصورية النظام الاجرائي للجريمة المعلوماتية في التشريع الجزائري ،مذكرة لنيل شهادة الماستر ،كلية الحقوق والعلوم السياسية ،جامعة عبد الحميد بن باديس مستغانم ،2020،

1بلعلمي جليلة، مزري صالح، الدليل الرقمي والاثبات الجنائي، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، جامعة قاصدي مرباح ورقلة، 2022، ص 08

طاهري عبد المطلب الاثبات الجنائي بالأدلة الرقمية مذكرة نيل شهادة ماستر تخصص قانون جنائي جامعة المسيلة 2014/2015

1بن زرت اسيا إثبات الجريمة المعلوماتية في التشريع الجزائري مذكرة لنيل شهادة ماستر تخص قانون جنائي وعلوم جنائية جامعة عبد بن باديس مستغانم، 2019

ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر جامعة العربي بن مهيدي ام الب واقي2016

شهرا زاد حجييه الدليل الإلكتروني في مجتال الاثبات الجنائي . مذكرة لنيل شهادة ماستر قانون جنائي اجنائي للأعمال جامعة العربي بن مهيدي . ام البواقي 2017/2016

لعاقل فريال ،الجريمة المعلوماتية في ظل التشريع الجزائري ،مذكرة لنيل شهادة الماستر ،في القانون العام ،تخصص القانون الجنائي و العلوم الجنائية ،جامعة آكلي محند اولحاج ،البويرة ،2015

بن بادرة عبد الحليم اجراءات البحث والتحري عن الجريمة المعلوماتية جامعة غرداية مجلة

جواحي عبد الستار جرائم الحاسوب . مذكر لنيل شهادة ماستر . تخصص شريعة وقانون كلية العلوم الإجتماعية والانسانية جامعة حمى لخضر الوادي 2015/2014

عمار حشمان ،مذكرة :الجريمة المعلوماتية في التشريع الجزائري ،مذكرة لنيل الماستر كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ،جامعة قاصدي مرباح –ورقلة – 2018– 2019

عبد الكريم شيباني ،الحماية الاجرائية والموضوعية للجريمة المعلوماتية ،مذكرة لنيل شهادة ماستر ،كلية الحقوق والعلوم السياسية ،جامعة الطاهر مولاي ،سعيدة ،2016،2015،

عمار حشمان ،مذكرة :الجريمة المعلوماتية في التشريع الجزائري ،مذكرة لنيل الماستر كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ،جامعة قاصدي مرباح –ورقلة – 2018– 2019

المقالات

علي عبد الله اجراءات استخلاص الدليل الرقمي مجلة دفاتر البحوث العلمية المجلد 9 العدد 1 الناشرحليم رامي، اجراءات استخلاص الدليل الرقمي في الجرائم المعلوماتية، جامعة البليدة، الجزائر، دفاتر البحوث العلمية ،المجلد،09،العدد 01 ،2023

غرس الله كريمة ضوابط حرية القاضي الجزائي في الاقتناع مجلة الآفاق للعلوم ،المجلد 08،العدد و02 ،جامعة البشير الابراهيمي ، برج بوعريريج ،2023

بن بادرة عبد الحليم اجراءات البحث والتحري عن الجريمة المعلوماتية مجلة الحقوق والعلوم الانسانية العدد 23 الجلد 2

سليمان بن مهجع العنزي ' وسائل التحقيق في جرائم نظام المعلومات ، رسالة ماجيستر في العلوم الشرطية ، جامعة الامير نايف العربية للعلوم الامنية ، الرياض ، 2003

نور الهدى محمودي حجية الادلة الرقمية في ا اثبات الجريمة المعلوماتية . مجلة الباحث للدراسات الأكاديمية العدد 11 جوان 2017

.عبد الرزاق خامرة حباس عبد القادر استثناءات الواردة على مبدا الاقتناع الشخصي للقاضي في التشريع الجزائري . مجلة الحقوق والعلوم الانسانية المجلد 15 العدد 02 تاريخ النشر 2022/06/15

1. عبد رزاق خامرة . عبد القادر حباس . حدود حرية مبدا الاقتناع الشخصي للقاضي . مجلة الاجتهاد للدراسات القانونية والاقتصادية العدد 10سنة 2021 تاريخ النشر 2021/05/21

محاضرات

بن فردية محمد محاضرات . لدليل الجنائي الرقمي وحجيته امام القضاء الجزائي. كلية الحق والعلوم السياسية جامعة بجاية. الجزائر

د. مازن خلف . محاضرة بعنوان /تقسيمات الادلة الجنائية جامعة المستنصرية 2017_2015

لبحوث العلمية.

د حسين بن سعد الغافري ، التحقيق وجمع في الجرائم المتعلقة بشبكة الانترنت ، بحث منشورعلى شبكة الانترنت ، موقع والبحوث.www. Minshaw.com

المواقع الالكترونية

www .Noor Book.com

www.asjp.ceriste https:

الفهرس

الرقم	العنوان	الصفحة
01	الشكر والعرفان	I
02	الاهداء	II
03	قائمة المحتويات	III
04	قائمة المختصرات	IV
	الفصل الأول أساسيات حول اثبات الجريمة المعلوماتية	
05	تمهيد	15
06	المبحث الأول: مفهوم الجريمة المعلوماتية واساسها القانوني	16
07	المطلب الأول: ماهية الجريمة الالكترونية وخصائصها	16
08	الفرع الأول: تعريف الجريمة الالكترونية	17
09	الفرع الثاني: خصائص الجريمة المعلوماتية	23
10	المطلب الثاني: أركان الجريمة الإلكترونية	33
11	الفرع الأول: الركن الشرعي	33
12	الفرع الثاني: الركن المادي	35
13	الفرع الثالث: الركن المعنوي	38
14	المبحث الثاني: الإطار المفاهيمي لدليل اثبات جرائم المعلوماتية	41
15	المطلب الأول: مفهوم دليل الاثبات في الجرائم المعلوماتية	41
16	الفرع الأول: المفهوم العام لدليل الاثبات الجنائي	43
17	الفرع الثاني: تعريف الدليل الرقمي	45
18	الفرع الثالث: خصائص الدليل الرقمي	46
19	المطلب الثاني: تقسيمات الدليل الرقمي	49
20	الفرع الأول: أنواع الأدلة الجنائية	49
21	الفرع الثاني: أنواع الدليل الرقمي	55
22	الفرع الثالث: صور الدليل الرقمي	57

23	خلاصة الفصل الأول	59
	الفصل الثاني: الأحكام الإجرائية لأدلة اثبات الجرائم المعلوماتية	
24	تمهيد	61
25	المبحث الأول: إجراءات استخلاص الدليل الرقمي	62
26	المطلب الأول: إجراءات جمع الدليل الإلكتروني	62
27	الفرع الأول: إجراءات استخلاص الدليل الرقمي التقليدية	62
28	الفرع الثاني: الوسائل المستحدثة لاستخلاص الدليل المعلوماتي	73
29	المطلب الثاني: وسائل جمع الأدلة الجنائية الرقمية	78
30	الفرع الأول: الوسائل المادية	78
31	الفرع الثاني: الوسائل الاجرائية	81
32	المبحث الثاني: السلطة التقديرية للقاضي في تقييم دليل الاثبات في الجذعية المعلوماتية	83
33	المطلب الأول: حرية القاضي الجنائي بالاقتناع بالدليل	83
34	الفرع الأول: مفهوم مبدأ الاقتناع الشخصي للقاضي ونطاق تطبيقه	84
35	الفرع الثاني: الضوابط التي تحكم مبدأ الاقتناع الشخصي للقاضي	88
36	المطلب الثاني: حجية الدليل الرقمي في اثبات الجرائم الالكترونية	93

37	الفرع الأول: الآراء الفقهية حول حجية الدليل الرقمي	93
38	الفرع الثاني: شروط قبول الدليل الرقمي دليلا لإثبات الحرية المعلوماتية	95
39	الفرع الثالث: القيمة القانونية للدليل الرقمي لدى المرشح الجزائري	98
40	خلاصة الفصل الثانـــــي:	100

ملخص

ملخص:

من خلال هذه المذكرة حاولنا الالمام بأساسيات اثبات الجريمة المعلوماتية بالتطرق الى تعاريفها وخصائصها اضافة الى اركانها واسس قيامها ثم تعمقنا أكثر في ادلة اثباتها وهذا ب تعريف الدليل الجنائي بصفة عامة والدليل الرقمي بصفة خاصة باعتباره اداة اساسية في اثبات الجريمة المعل وتصنيفه من بين الادلة الجنائية والتطرق الى تقسيماته وصوره هذا بالنسبة لما تناولناه في للفصل الاول اما بالنسبة للفصل الثاني حاولنا ايضاح اجراءات استخلاص الدليل الرقمي المتمثلة في إجراءات حديثة وتقليدية. وفي الاخير بينا حجية الدليل الرقمي في الاثبات وسلطة تقديرية للقاضي الجزائي في قبول هذا الدليل كدليل اثبات

الكلمات المفتاحية:الجريمة المعلوماتية . الدليل الرقمي، حجية الدليل الرقمي، الاقتناع الشخصي للقاضي، الاثبات الجنائي، الاجراءات المستحدثة.

Abstract*:*

Through this note, we tried to get acquainted with the basics of proving informational crime by addressing its definitions and characteristics, in addition to its pillars and foundations, then we delved more into the evidence of its establishment, and this is by defining criminal evidence in general and digital evidence in particular as a basic tool in proving the crime and classifying it among the forensic evidence and addressing Its divisions and images are in relation to what we discussed in the first chapter. As for the second chapter, we tried to clarify the procedures for extracting the digital evidence represented by modern and traditional procedures. Finally, we showed the authoritativeness of the digital evidence in proof and the discretionary power of the criminal judge to accept this evidence as proof.

Keywords: information crime - digital evidence, authenticity of digital evidence, personal conviction of the judge, criminal evidence, updated procedures.

Résumé*:*

A travers cette note, nous avons tenté de nous familiariser avec les bases de la preuve du crime informationnel en abordant ses définitions et caractéristiques, en plus de ses piliers et fondements, puis nous nous sommes penchés davantage sur les preuves de son établissement, et ceci en définissant la preuve pénale en preuves générales et numériques en particulier comme outil de base pour prouver le crime et le classer parmi les preuves médico-légales et aborder Ses divisions et ses images sont en relation avec ce que nous avons discuté dans le premier chapitre.Quant au deuxième chapitre, nous avons essayé de clarifier le procédures d'extraction des preuves numériques représentées par les procédures modernes et traditionnelles. Enfin, nous avons montré l'autorité de la preuve numérique dans la preuve et le pouvoir discrétionnaire du juge pénal d'accepter cette preuve comme preuve.

Mots-clés : crime d'information - preuve numérique, authenticité de la preuve numérique, conviction personnelle du juge, preuve pénale, procédures mises à jour.