وزارة التعليم العالي و البحث العلمي

جامعة العربي التبسي – تبسة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

التخصص:قانون جنائي

مذكرة مقدمة لنيل شهادة ماستر «ل.م.د"

إجراءات البحث و التحري في الجرائم المعلوماتية

دفعـــة: 2021/2020

إعداد الطالبة:

حنان حفافصة

إشراف الأستاذ :

د. قحقاح وليد

أعضاء لجنة المناقشة

الأستاذ	الرتبة	الجامعة الأصلية	الصفة
د. عثماني عز الدين	أستاذ محاضر – أ -	جامعة العربي التبسي	رئيسا
د. قحقاح وليد	أستاذ محاضر – ب -	جامعة العربي التبسي	مشرفا ومقررا
د. فرحي ربيعة	أستاذ محاضر – ب -	جامعة العربي التبسي	ممتحنا

السنة الجامعية 2021/2020

إجراءات البحث و التحري عن الجرائم المعلوماتية

وزارة التعليم العالي و البحث العلمي

جامعة العربي التبسي – تبسة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

التخصص:قانون جنائي

مذكرة مقدمة لنيل شهادة ماستر "ل.م.د"

دفعـــة: 2021/2020

إعداد الطالبة :
حنان حفافصة

إشراف الأستاذ :
د . قحقاح وليد

الأستاذ	الرتبة	الجامعة الأصلية	الصفة
د. عثماني عز الدين	أستاذ محاضر – أ -	جامعة العربي التبسي	رئيسا
د. قحقاح وليد	أستاذ محاضر – ب -	جامعة العربي التبسي	مشرفا و مقررا
د. فرحي ربيعة	أستاذ محاضر – ب -	جامعة العربي التبسي	ممتحنا

السنة الجامعية 2021/2020

شكر و عرفان

الكلية لا تتحمل ما جاء في هذه المذكرة من آراء

إهـــــداء

أشكر الله في المقام تعالى سبحانه وتعالى على فضله وتوفيقه لإنجاز هذا العمل، كما وأشكر جامعة العربي التبسي" كلية الحقوق" على احتضانها لي أثناء مشواري الدراسي، وأتقدم بالشكر الخالص والاحترام للأستاذ المشرف " قحقاح وليد" الذي تقبل الإشراف على هذه المذكرة ولم يبخل عليا بنصائحه، وأوجه شكري لكل من أعانني في هذه المذكرة، كما وأتقدم بالشكر مسبقا لأعضاء لجنة المناقشة بقبولها مناقشة هذه المذكرة.

بعد الحمد لله أهدي ثمرة جهدي إلى من جعل الله الجنة تحت أقدامها

إلى أعز من قدم لي الأمل والتحفيز إلى قرة عيني ونور حياتي التي ألهمتني الصبر وبثت في الأمل والقناعة والتي كافحت وقدمت لي العزم لأكمل مشواري الدراسي، إلى نبع الحنان وقدوتي "أمي الغالية"

إلى من كانو لي سندا وحثوني على المثابرة والإجتهاد والثقة بالنفس ودفعوني لأواصل وأتذوق طعم النجاح "أختاي "أحلام" " خولة"

إلى من لا تحلو الحياة بدونهم وأرى السعادة بأعينهم إخوتي "أيمن" عبد النور"معتز"

إلى من جمعني بهم القدر في الدراسةفأحببتهم وأحبوني "صديقاتي وزميلاتي"

إلى من وسعتهم ذاكرتي ولم تسعهم مذكرتي أهديكم ثمرة جهدي المتواضع.

مقدمة

مقدمة

نشهد اليوم تطورات عظمى إقتحمتجميع المجالات ولاسيما المجال العلمي الذي يهتم بالمعلومات وتكنولوجيا الإتصال،ويعود الفضل فيها إلى الثورة المعلوماتية الهائلة التيانعكست على مستويات التقدم التقني والعلمي على العديد من جوانب الحياة المعاصرة، وهذا بفضل ماقدمته الحضارة الإنسانية من ابتكارات جعل من هذه الأخيرة سبب لتسهيل متطلبات الحياة، ولعل من أعظم هذه الإبتكاراتأصبح الحديث اليوم عن ما يسمى بالحاسوب، فهذا الأخير كان له الدور الفعال في إحداث تغيير شامل على جميع ميادين الحياة العصرية، بحيث أصبح هذا الإبتكار ليس حكرا فقط على الدول المتقدمة بل وحتي تبلوره في الدول النامية، مما زاد من أهمية هذه التكنولوجيا إذ عرفت بما يسمى بعصر المعلومات، فالعصر الحديث جعلها من ضروريات التقدم الإنساني والمحرك الأساسي لها في مختلف مجالات الحياة، وهذه التقنية قد إنعكست بشكل إيجابي على ما قدمته للإنسان جعلت الحياة أمامه مبسطة مما زاد إستعمالهابشكل مفرط في كل القطاعات العامة والخاصة، إذ لم يعد من السهولة الإفراط فيها أو انجاز نشاطاتهم دون الإستعانة على هذه التقنيات الحديثة التي أضحت المحور الأساسي في سير الحياة في شتى المجالات.

ألا أن هذا التقدم الذي تحقق بفضل تقنيات وسائل تكنولوجيا الاعلام والإتصال و الإستخدامالمتنامى لهذه التنقنياتإنعكس في نفس الوقت على بعض الجوانب السلبية التي خولت لفتح آفاق غامضةإنعكست سلبا على أمن وإستقرار المجتمع، نتيجة لسوء إستخدام هذه التقنية وإستغلالها بطرق غير شرعية تأدي للإضرار بمصالح الأفراد والجماعات،أدي إلى ظهور نمط جديد من الإجرام، هذا الأخير ينتمي إلى جرائم تقنية المعلومات أو ما يسمىبالجرائم المعلوماتية، هذه الأخيرة تعتبر من أخطر وأفتك الجرائم مقارنة بغيرها.

إن طبيعة هذه الجريمة وتطورها بشكل سريع جعلها جريمة ذو طابع خاص ذلك راجع إلى إنفرادها بمجموعة من السمات والخصائص سواء من ناحية الجريمة نفسها أو مرتكبيها، فهذا النوع من الجرائم له جانب خاص مقارنة بنظيره من الجرائم التقليدية، إذ له

خاصية تنطبع على المجرمين الذينيباشرون هذه الجريمة فأصبح يطلق عليه بالمجرم المعلومات، لأن مرتكبيها ذو فئات مميزة لهم علم ودراية على نحو عالي بالتقنيات الحديثة، وإمتلاكهم أدوات المعرفة الفنية مما سهل عليهم الإندماج في مجال المعالجة الآلية للمعطيات، التي جعلتهم يتمركزون في المقام الأول في مجال الإجرام المعلوماتي

أهمية البحث:

يكمن أهمية موضوع " إجراءات البحث والتحري عن الجرائم المعلوماتية" ،في أنه من المواضيع الجديدة في ميدان الجرائم كون أن الجريمة المعلوماتية جريمة مستحدثة مواكبة للتطور في المجال التكنولوجي للإعلام والإتصال،إضافة لما تتميز به من صبغة علمية وتقنية جديدة برزت في مهارة التحقيق بشكل تقني وفني ،إذ أنالقواعدالتقليديةفيالإثباتالجزائيأضحتقاصرةأوغيركافيةأوغيرملائمةفيكشفبعضالجرائموإثب

اتها؛لذابدأالاهتمامبالأدلةالرقميةالتيأصبحت بلور في إستكشاف الأدلة وصولا للحقيقة المرادة، وكذلك لما تتسم به من إجراءات البحث والتحقيق في هذا النوع من الجرائم خلافا للجرائم التقليدية.

فمع بروز أساليبإجراميةبتقنياتجديدة، صادفها تطورالتقنياتالحديثةلإكتشاف الجريمة من مرحلة البحث والتحقيق وصولا للدليل الكاشف عن الحقيقة،بإستخدام أجهزةوأدوات متطورة ومتصلة بتكنولوجيا الإعلام والإتصال.

من خلال بيان كافة الجوانب الخاصة بالجريمة المعلوماتية وتدارك الطبيعة المميز التي تميزها عن الجرائم الأخري من خلال تطرقه لأحدث الوسائل التكنولوجية والعلمية،وذلك من خلال التعرف على مفهوم وخصائص وأركان هذه الجريمة وكدلك الأشخاص الذين يشكلون أطرافا فيها والبواعث التي جعلتهم يرتكبون هذه الجريمة.

أهداف الدراسة:

يتجسد الهدف من هذه الدراسة لتحقيق مجموعة من الأهداف البحثية تتمثل فيما يلي:

- الإسهام في وضع حلول للوصول للحقيقة في ظل إرتكاب هذا النوع من الجرائم وهذا نتيجة حداثة الموضوع وصعوبة التحري فيه.

- معرفة الإجراءات الحديثة التي كان لها الريادة في تسهيل عملية التحقيق في الجريمة المعلوماتية.

- خصوصية الدليل الرقمي في الجريمة المعلوماتية بإعتباره دليل فني يختلف بإختلاف البيئة التي أرتكبت فيه الجريمة.

- إثراء مكتبتنا المركزية بإضافة مرجع جديد وإن كان متواضعا لا يصل لقيمة الكتب والمراجع الموجودة

أسباب إختيار الموضوع:

يمكن رد الأسباب التي جعلتنا نبحث في هذا الموضوع إلى أسباب ذاتية وأخرى موضوعية.

فالأسباب الذاتية تتمثل في ميولي الشخصي إلى دراسة الجوانب التي تخص الجريمة المعلوماتية وبالتاليالغوص في ما يطرحه هذا الموضوع من إجراءات مستحدثة في متابعة الجرائم المعلوماتية.

أما الأسباب الموضوعية فترجع إلى كونه يندرج ضمن تخصصي فهو من المواضيع النادرة والذي أصبح موضوع يتماشى مع الواقع الذي نعيشه

إشكالية الموضوع:

تكمن إشكالية البحث في الإجراءات المتبعة للتصديللجريمة المعلوماتية، بحيث أن موضوع الجرائم المعلوماتية عامة يثير العديد من التساؤلات والإشكاليات إنطلاقا من ماهية هذه الجريمة إلى كيفية مباشرة التحري والتحقيق فيها وصولا للحقيقة البحتة،ولتدارك هذه الحقيقة فإن المشرع قام بإستحداث طرقا إجرائية في سبيل البحث والتحري عن هذا النوع من الجرائم.

وبناءا على ماسبق ذكره إرتأينا إلى ضبط إشكالية موضوع بحثنا, على النحو التالي:

ماهي طبيعة القواعد الإجرائية المتبعة في البحث والتحقيق في الجرائم المعلوماتية؟

منهج الدراسة:

وقد إتبعت في هذا البحث المنهج الوصفي منخلالوصف طبيعة هذه الجريمة وتبيان سيمات الأطراف وخصوصية التحقيق فيها، ووصف المفاهيم العامةالخاصةبالإجراءاتالمتبعةللبحثوالتحقيقفيالجرائمالمعلوماتية لاستخلاصالدليل كذلك وصف المفاهيم المتبعة في إستخلاص طبيعة هذا الدليل في مجال الإثبات .

والمنهجالتحليليمنخلال عرض أهمالإجراءات القانونيةالتيتتبع لمواجهة الجريمة المعلوماتية،ومناقشة وتحليل هذه الإجراءات الفنية الحديثةبشكلمنالتفصيل للتصدي لهذا النوع من الجرائم المستحدثة، إضافة لتحليل الطبيعة الخاصة للدليل الرقمي.

كذلك إستندنا للمنهج المقارن وذلك للطبيعة الإستثنائية للجريمة المعلوماتية، من خلال تبلور أجهزتها في مختلف التشريعات المقارنة .

الدراسات السابقة:

ومن أهم الدراسات السابقة في موضوعنا والتي إستفدنا منها:

- أطروحة تخرج لنيل شهادة الدكتوراه موسومة بعنوان التحقيق الجنائي في الجرائم الإلكترونية للطالب براهيمي جمال، جامعة مولود معمري ،تيزي وزو سنة 2019/2018.

- أطروحة تخرج لنيل شهادة الماجستير موسومة بعنوان أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري للطالب سعيداني نعيم، جامعة الحاج لخضر، باتنة سنة 2013/20112.

- أطروحة لنيل شهادة الماجستير موسومة بعنوان آليات مكافحة تكنولوجيات الاعلام والاتصال في ضوء القانون رقم 04/09 للطالبة أحمد مسعود مريم، جامعة قاصدي مرباحي، ورقلة سنة 2013/2012.

تقسيم الدراسة:

بناءا على ماتقدم وللإجابة عن إشكالية أعلاهإرتأينا لتقسيم موضوع الدراسة إلى خطة ثنائية تحتوي على فصلين وكل فصل إلى مبحثين وكل مبحث إلى مطلبين بحيث إشتمل الفصل الأول الأحكام المتعلقة بالجريمة المعلوماتية، وتناولنا من خلال المبحث الأول الطبيعة القانونية للجريمة المعلوماتية، والمبحث الثاني خصصناه إلى خصوصية البحث والتحقيق في الجرائم المعلوماتية ، اما الفصل الثاني فقد عالجنا فيه الآليات الإجرائية للتحري عن الدليل في الجريمة المعلوماتية وإشتمل بدوره على مبحثين الأول تضمن طبيعة الدليل الرقمي في الجريمة المعلوماتية، والمبحث الثاني على إجراءات التحري داخل المنظومة المعلوماتية.

وختما أنهينا موضوع بحثنا بمجموعة من النتائج التي نأمل الاستفادة منها.

الفصل الأول:

لقد غزا العالم تطور ملحوظ في مجال تقنية المعلومات على شتى الميادين في الحياة المعاصرة ولكن بالرغم من المزايا الهائلة إلا أن هده الثورة التكنولوجية انعكست في المقابل بجملة من الانعكاسات السلبية الخطيرة نتيجة لاستخدامها بطريقة غير مشروعة الأمر الذي أدي إلى ظهور جرائم لها علاقة بالمجال وهي كما يعرف بالجريمة المعلوماتية ونظرا لحداثة هده الجريمة فقد إختلف الفقهاء في وضع تعريف موحد لها وكذلك إتسمت بمجموعة خصائص وعرفت مجموعة مجرمين لهم دوافع لإرتكاب هده المجموعة كذلك لهده الجريمة دليل مناسب لإثباتها وهدا ماسأحاول التطرق إليه في هذا الفصل من حيثالطبيعة القانونيةللجريمة المعلوماتية من حيث المفهوم وأطراف الخاصة بالجريمة بالإضافة إلى الدوافع المؤدية لإرتكاب الجريمة وهذا في المبحث الأول، ثم سنتطرق إلىخصوصية البحث والتحري في الجريمة المعلوماتية من خلال تناول الاجهزة المكلفة بالبحث في القوانين المقارنة وفي التشريع الجزائري و خصائص التحقيق والمحقق في هذه الجريمة في المبحث الثاني.

المبحث الأول: الطبيعة القانونية للجريمة المعلوماتية

من خلال هدا المبحث سأحاول التعرض إلى التعاريف المختلفة للجريمة المعلوماتية و الأركان التي ترتكز عليها وبيان الدوافع المؤدية لارتكابها نظرا لطبيعتها الخاصة، بإعتبارها تقع في العالم الافتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس وذلك من خلال مفهوم الجريمة المعلوماتية في المطلب الأول، ثم يليه التطرق لأطراف هذه الجريمة ودوافع إرتكاب الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا وإتساعا مما أسفر عن ذلك تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية أو كما يقال الإلكترونية فلفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية فكلما كان البحث منصبا على الجرائم التي ترتكب ضد النظام الإلكتروني كلما انطبق التعريف على محل الإلكترونية بأنها الجريمة المرتكبة وأن الفعل المرتكب بواسطتها يشكل إعتداءا على النظام المعلوماتي كما للجريمة المعلوماتية أركان لا تقوم الجريمة إلا بتوافرها وهذا ما تطرقنا إليه في هذا المطلب، بحيث تناولنا التعريف في الفرع الأول ثم الأركان في الفرع الثاني يليه الخصائص في الفرع الثالث،

الفرعالأول:تعريف الجريمة المعلوماتية

تعتبر الجريمة الالكترونية من الظواهر الحديثة لإرتباطها بتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعري ف محدد بل أن بعض الفقهاء ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل

هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني[1]، ولقد ذهب الفقهاء في تعريف الجريمة المعلوماتية لمذاهب شتى ووضعوا تعريفات مختلفة فاختلفت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن تقنية المعلوماتية من الوجهة التقنية وحتى من الوجهة القانونية ومنه فبتعدد هذه التعريفات وإختلافها بحسب الدراسة القانونية التي تتناولها.

وفي سبيل ذلك فإن الفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية وهذه التعاريف لا تخرج عن أحد الإتجاهين أولهما يضيق مفهومها والثاني يوسعه.[2]

أولا: يذهب أنصار هذا الاتجاه لحصر الجريمة المعلوماتية وتضييقها ومن التعريفات التي وضعها أنصار هذا الاتجاه: " أن الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخري[3]"، وفي هذا الاتجاه أيضا عرفها الفقيه " DAVID THOMSON" أنها جريمة يكون متطلبا لاقترافها أن تتوافر لدي فاعلها معرفة بتقنية الحاسوب[4]، ومن هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة بالعلم بتكنولوجيا الحاسبات.

كذلك عرفها جانب من الفقه بالنظر لمعيار نتيجة الإعتداء إذ يرى الأستاذ "MASSE"أن الجريمة المعلوماتية هي تلك الإعتدات التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" ،كما يرى الأستاذ "TREDMANE" أن الجريمة المعلوماتية تشمل تشملأي جريمة ضد المال، مرتبطة بإستخدام المعالجة الآلية للمعطيات".

كما عرف الأستاذ PARKER"، "الجريمة المعلوماتية بأنها كل فعل إجرامي متعمد مهما كانت صلته بالمعلوماتية تنشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".

وهناك جانب آخر أخذ في تعريفه للجريمة المعلوماتية بمعيار موضوع الجريمة وذلك كما ذهب إليه الفقيه ROSENBLATTبأن الجريمة المعلوماتية هي" نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه"[5].

1-خالد ممدوح، امن الجريمة الإلكترونية، الدار الجامعية، الاسكندرية، 2008، ص41

2-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لحضر،باتنة، كلية الحقوق والعلوم السياسية، 2013/2012، ص26.

3- حمزة بن عقون السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية تخصص علم الإجرام والعقاب جامعة باتنة 2012/2011، ص13.

4-رشيدة بوكر جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية الطبعة الأولى

5-حمزة بن عقون، المرجع السابق ص14.

ومنه فإنه يؤخذ من هذه التعريفات السابقة أنها جاءت قاصرة بالإلمام بأوجه ظاهرة الإجرام المعلوماتي فالبعض من الفقهاء ركزوا على معبار لموضوع والبعض الأخر على وسيلة إرتكابها والبعض الأخر على معيار النتيجة.

ثانيا: حاول بعض الفقهاء وضع تعريف موسع لتفادي القصور التي شابت تعريفات الإتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي، ومنه يرى فريق من الفقهاء ضرورة توسيع من مفهوم الإجرام المعلوماتية وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا وذلك بإستخدام شبكات الأنترنيت من خال غرف الدردشة و إختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعي بهدف إلحاق الضرر بالفرد أو مجموعة من الأفراد، وحتي دولة من الدول قد تكون ضمن الإستهداف الحربي أو الاقتصادي أو الإضرار بمسمعتها أو العكس ويبقا لهدف واحد وهو الكشف عن قضايا متستر عليها، أو نشر معلومات لفائدة طرف أو أطراف من باب التسرب[1].

ودائما حسب هذا الإتجاه فيرى البعض أن هذه لجريمة هي كل فعل ضار يستخدم من قبل الفاعل الذي يفترض أن لديه معرفة بتقنية النظام الحاسوبي للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة[2].

وكذلك في نفس الإتجاه عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا[3]،وهناك إتجاه فقهي آخر عرفها بالقول أن الجرائم المعلوماتية كل سلوك غبر مشروع وغير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها.

أما بالنسبة للتعريف القانوني للجريمة المعلوماتية فقد إصطلحاللمشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وعرفها بموجب أحكام المادة 02 من القانون 04/09،على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة من قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومةمعلوماتية أو نظام الاتصالات الإلكترونية"[4]، من هنا نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إإلى 394 مكرر 07[5]،وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية.

1-سميرة بيطام الجريمة الإلكترونية وتقنية الإجرام المستحدث ص04/01، 2016/11/30.
2-كامل فريد السالك،الجريمة المعلوماتية ندوة التنمية ومجتمع المعلوماتية، حلب،23/21 تشرين الأول،2000، بدون صفحة.
3-خالد عباد الحلبي،إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت،الطبعة الأولى،دار الثقافة.
4-القانون 04/09،الصادر في 5أوت 2009 يتضمن القواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر، العدد 47.
5-القانون رقم 15/04، الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66، الصادر في 08جوان 1966، المتضمن قانونالعقوبات،ج ر العدد 71.

وحسب المشرع الجزائري فإنهقد تتحقق الجريمة المعلوماتية بمجرد أن ترتكب الجريمة، أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف شامل لعدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[1]،ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسرب أسئلة الباكالوريا لسنة 2016،كذلك قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية.

فبصفة عامةفالجريمة المعلوماتية هي كل فعل ضار يأتيه الفرد أو الجماعة يعتبر جرما يرتكب منظما إستخدام الحاسب الآلى، أو الشبكة المعلوماتية بطريقة منافية لأحكام هذا النظام التقني وهو نظام مكافحة الجريمة المعلوماتية ويكون لهذا الفعل أثر ضار على الغير.

الفرع الثاني: أركان الجريمة المعلوماتية

تتمثل أركان الجريمة المعلوماتية مثل الجريمة العادية في الركن الشرعي والمادي والمعنوي

- أولا: الركن الشرعي للجريمة المعلوماتية

هو ركن يضع نص لتجريم هذا الفعل فالقاعدة القانونية أنه" لا جريمة ولا عقوبة إلا بنص" ومنه فالجريمة هي نتيجة أفعال مادية صادرة عن إنسان هذه الأفعال تختلف من شخص لأخر،وهذاماجعل المشرع يتدخل لتجريم هذه الأفعال الضارة، وبموجب نص قانوني يحدد فيه الفعل الضار أو الجرم والعقوبة المقررة لإرتكابها[2].ومنه فهو الصفة الغير مشروعة للفعل وتتمثل قاعدة التجريم والعقاب كما قلنا سابقا من خلال ماورد عليه في القانون المتضمن القواعد الخاصة، للوقاية من الجرائم المتصلة بتكنولوجيا اللإعلاموالإتصال ومكافحتها.

- ثانيا: الركن المادي

ويتمثل في كيان الجريمة الذي يظهر في العالم الخارجي، يتكون الركن المادي من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقيق النتيجة كالتبليغ عن الجريمة قبل تحقيق نتيجتها مثلا: إنشاء موقع إبتزازشخص معين بصوره الشخصية دون تسريب هذه الصورعلى الشبكة، ومنه فهو نشاط يبادر به الجاني للإعتداء على الفرد أو المجتمع، عن طريق التقنية المعلوماتيةمما يدفع النظام للتدخل ومعاقبة الفاعل عما صدر منه من إجرام.

1- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2011/2010، ص 14-16.

2- أحسن بوسقيعة،الوجيز في القانون الجزائي العام، دار هومة، الجزائر،ط10، 2011،ص27.

- ثالثا: الركن المعنوي

ويتمثل إرتكاب الفعل المجرم من الجاني المعلوماتي بإرادة فعلية ورغبة وعن إدراك تام بالنتيجة المرادة وعواقبها، ويتضح هذا الركن للجريمة المعلوماتية من خلال توضيح الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.

الفرع الثالث: خصائص الجريمة المعلوماتية

الجريمة المعلوماتية لها سيمات تميزها عن غيرها من الجرائم لاسيما التقليدية منها سنحاول عرض أهم الخصائص فيما يلي:

- الجريمة المعلوماتية عابرة للحدود بحيث أنه بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تعيق نقل المعلومات عبر الدول المختلفة، إذ أن الجريمة هنا لا تعترف بالحدود بين الدول، وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين الدول والعالم كافة[1]، ومنه فقدرة تقنية المعلومات على إختصار المسافات بين أنحاء العالم إنعكست على طبيعة الأعمال الإجرامية التي يقوم بها المجرمون وهو مايعني أن مسرح الجريمة لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد دون القيام بأي مجهود نتيجة التباعد الجغرافي واختلاف المواقيت بين الجاني والمجني عليه.

- ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات وتجهيزات الحاسب الآلى بمعنى تتم بواسطة المكونات المادية للحاسوب HARDWARE، ومكونات البرمجيات SOFTWARE.

- يقوم بها مجرم ذو طبيعة خاصة وإمكانيات خاصة، يستخدم في إرتكاب جريمته للموارد المعرفية والأساليب الإحترافية وذو خبرة عالية في مجال التقنية المعلوماتية.

- صعوبة الحصول على دليل مادي في مثل هذه الجرائم، بحيث يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطاتهم الجرمية عن طريق تلاعبهم بالبيانات، كما يسهل تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ماقورنت حالات إكتشاف الجريمة على ضوء مايتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم إكتشافها بالمصادفة بعد وقت طويل من إرتكابها، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو إقتحام

1-خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولي ص23.

وإنما هي معلومات وبيانات تغير أو تعدل أوتمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الألي[1]، إذ أنه من السهولة إتلاف الادلة من قبل الجناة.

- الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص إضرارا بالمجني عليه،وغالبامايشارك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب و الأنترنيت ويقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أومن خارج المؤسسة المجني عليه لتغطية عملية التلاعب وتحوبل المكاسب[2].

المطلب الثاني: أطراف ودوافع إرتكاب الجريمة المعلوماتية

بإعتبار الجريمة وليدة المجتمع فقد كان لها الأثر البالغ في تمييز مرتكبيها، وبالتالي فالجريمة المعلوماتية لم تندمج بالتقنية الآلية فحسب بل كان لها الدور في تصنيف مرتكبيها عن غيرها من المجرمين العاديين، كونها تشكل جانب جديد في حياتنا فقد جلبت شكلا جديدا من المجرمين، ومنه فقد اصطلح على تسميتهم بمجرمي المعلوماتية، ذلك راجع كون أن مرتكبي الجريمة المعلوماتية يتسمون بالذكاء والدراية في التعامل في مجال الآلية للمعطيات والمعارف التقنية، وإذا كنا أمام جرم معلوماتي فيجب أن نلتفت إلى المجرم المعلوماتي من حيث سماته وأصناف الطوائف التي تميزه من غيره من المجرمين وهذا ما سنتطرق إليه في الفرع الأول، الذي كان وراء تحقيق السلوك الإجرامي وكون هذا الجرم يستهدف شخص معين وهو الضحية فهو أيضا يعتبر طرفا في الجريمة المعلوماتية،ومنه فمن الطبيعي أيضا أن نجد الإختلاف في الأسباب والعوامل التي تدفع المجرم لإرتكاب الفعل الغير مشروع ، فهو يختلف من جريمة لأخرى أما الهدف فهو تحقيق النتيجة التي أصرف إليها القصد الجنائي أو الإعتداء على الحق الذي يحميه قانون العقوبات، وبالنسبة للجريمة المعلوماتية، فثمة دوافع عديدة تحرك الجناة لإرتكاب أفعال الاعتداء المختلفة وهذا ما سنتطرق إليه في الفرع الثاني.

الفرعالأول: أطراف الجريمة المعلوماتية

تتكون أطراف هذه الجريمة من صنفين أساسين وهما المجرم المعلوماتي والضحية (المجني عليه)، فقد تنوعت الدراسات التي تحدد المجرم المعلوماتي وشخصيته والأفعال الإجرامية التي يقوم بها، ويعد الأستاذ BARKER واحد من أهم الباحثين الذين خصصوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة، بحيث يرى أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة ، إلا أنه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه.

أولا: الجاني في الجريمة المعلوماتية (المجرم المعلوماتي).

1- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية أزمة الشرعية الإجرائية، جامعة كوفة، كلية الحقوق ص112.
2- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص القانون الجنائي، جامعة محمد خيضر، بسكرة، 2014/2013، ص18

يتميز بصفات معينة تميزه عن غيره من المجرمين، إذ جعلته محل العديد من الأبحاث والدراسات من قبل باحثون، بحيث اختلفت الخصائص إلا أنها تندرج ضمن جوانب مشتركة، ومن أهم هذه الصفات:

-1-التخصصوالمهارة والذكاء: فالجريمة تحتاج إلى خبرة قوامها التعليم والتدريب المتخصص، نظرا إلى تمكن المجرم من تنفيذ جريمته بمهارة وخفة كونه متخصصا في مجال التقنية الإلكترونية، إذ يمتلك هذا المجرم من المهارات ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب[1]. بحيث أن المهارة التي يتميز بها المجرم المعلوماتي تمكنه من تكوين تصور كامل لجريمته، أذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من تفشل مخططاته أو الكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى تمهيد ارتكابه لجريمته بالتعرف على المحيط الذي تدور فيه وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانية نجاحها وإحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها[2]،فتتجلى صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في إرتكابه للجريمة، فالسلوك الإجرامي ينشأ من صفة التدمير الناعمة (SABOTAGE SOFT)[3].

-2-التخطيطوالتنظيم: المحكم لتحقيق النتيجة المراد تحقيقها من قبل المجرم المعلوماتي، بحيث أن الجريمة المعلوماتية يقوم بها عادة مجموعة من الأفراد أو مجموعات صغيرة التي تحدد لكل شخص دورا يقوم به، حتى يتم العمل بنظام محكم دون الوقوع في صعوبات تعيق من النشاط الإجرامي المراد إنجازه، بحيث يتم تقاسم الأشغال بصورة دقيقة ومتسلسة مثلا: من يقوم بنسخ برامج الحاسب الآلى إلى من يقوم بتعديلها. وغالبا ما يكون متضمنا فيها متخصصا في الحاسب الآليقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة امجني عليه لتغطية التلاعبولتحويل المكاسب إليه.

-3-مجرم إجتماعي متكيف اجتماعيا: فالمجرم يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسة دون أي عائق في حياته اليومية[4]، فالمجرم المعلوماتي لا يضع نفسه في العداء السافر مع المجتمع الذي يحيط به بل أنه إنسان متكيف اجتماعيا، ذلك أنه أصلا مرتفع الذكاء ويساعده في ذلك عملية التكييف، ومماالذكاء في رأي الكثيرين سوى القدرة على التكيف، ولا يعني ذلك التقلل من شأن المجرم المعلوماتي بل خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه.

1- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنيت، دار النشر مكتبة الوفاء القانونية،الإسكندرية،ط1، سنة2011، ص54.

2- نائلة محمد فريد قورة، المرجع السابق،ص58.

3- سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص51.

4- مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية. 2012، العدد21، ص12.

-4-المجرم المعلوماتي يبرر إرتكاب جريمته، إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم، بحيث أن فاعلها يفرق بين الإضرار بالأشخاص الذين يعدون غاية في اللاأخلاقية، وبين المؤسسات أو الجهة التي يكون في مقدورها تحمل تلاعبهم، ولعب التباعد وعدم وجود إحتكاك بالأشخاص دورا في تسهيل القيام بالفعل الغير مشروع.

-5-مجرم ذو مهارات عالية، هذه الأخيرة تؤهله للتبلور في مجال التقنية الإلكترونية، إذ له من القدرات والمهارات مايؤهله لأن يوظف مهاراته في الإختراق والسرقة والنصب والإعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.

-6-التطورفيالسلوك الإجرامي، بحيث أن وجود المجرم الإلكتروني في جماعة إجرامية يساعد على خفة إكتسابه المهارة التقنية من أدنى الحدود إلى أعلى درجات في المهارة التقنية المتمثلة في إثبات قدرته على القيام بجريمته بأسلوب متقون.

وبناءا علما تطرقنا له فيمكن تصنيف المجرم المعلوماتي إلى طوائف محددة يمكن حصرها فيما يلي:

-1-صغارنوابغ المعلوماتية (PRANKSTERS): وهي مجموعات صغار السن كما يسمى التي تميل للتحدي الفكري غالبا ما يكونون في مرحلة المراهقة، ولكن بالرغم كم صغر سنهم إلا أن لهم قدرات على إقتحام كافة أنواع الأنظمة المعلوماتية، فهذه الفئة تعتبر أن ما تقوم به لا يعتبر جريمة كونهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع، كما يمكن لهذه الفئة أن تتحول إلى فئة قراصنة بعد تطور خبراتهم ومهاراتهم فيتم استئجارهم والتلاعب بهم في أعمال ذات أهداف إجرامية.

-2- فئة القراصنة: وهي طائفة المجرمين البالغين أو المخربين وتندرج ضمن نوعين من المجرمين وهي الهاكرز والكراكز، فالهاكرز هو شخص يقوم بإنشاء أو تعديل البرمجيات أو العتاد الحاسوبي، وغالبا لا تكون لديهم دوافع حاقدة فالباعث الأساسي لديهم هو الإستمتاع باللعب والمزاح أو إكتساب الخبرة باستخدام هذه التقنية لإثبات قدراتهم، كذلك لدينا بما يسمى الكراكر وهو المقتحم، من أبرز سيمانهم أنهم متخصصين في مجال التقنية الإلكترونية، أي أنهم يتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية وإدراك واسع للتقنية الإلكترونية تمكنهم من الهيمنة الكاملة في البيئة المعالجة لآلية المعطيات[1]، مما جعل الهاكرز يستعين بالكراكر إذا ما صادفته أي نوع من أنواع الحماية.

-3- فئة المحترفين: وهي من أخطرالفئات في مجال التقنية لأن هدفها هوالنيةلإرتكاب الفعل الإجرامي، وهذا هو مصدر الخطورة كون أن الأضرار التي تنجم عن هذه الأفعال تعكس ميولا إجراميا بنسبة بالغة من الضرر، تنبئ عن رغبتها في إحداث التخريب، فإعتداءاتهم تهدف أساسا إلى تحقيق الكسب المادي لهم وللجماعات التي كلغتهم وسخرتهم لإرتكاب الجرائم الماسة بالتقنية المعلومات،كما تهدف إعتداءات بعضهم إلى

1-سمية مزغيش، المرجع السابق،ص22-23.

تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، فنيتهم لتحقيق ميولات إجرامية هي ماجعلتهم أكثر خطورة من الأصناف سابقة الذكر.

-4- فئة الحاقدون: هذه الفئة تكون نيتها الإنتقام من شخص معين، أو من صاحب العمل. أو من منشأة معينة، ولهذا فقد يكونون من مستخدمي النظام أو مشتركين بالنظام، فالمنتمي لهذه الفئة لا يتسم بالتقنية الإخترافية، إلا أنه يكون لديه إستراتيجية لتتبع الفعل الذي ينوي إرتكابه، بحيث يستخدم تقنيات الفيروسات والبرامج الخبيثة وتعطيل النظام أو الموقع المستهدف والمراد إختراقه، وهم الطائفة الأسهل من حيث الكشف عن أعمالهم ذلك لتوفر العوامل المساعدة على معرفة ذلك.

ثانيا: المجني عليه في الجريمة المعلوماتية (الضحية).

فكما يمكن أن ترتكب الجريمة المعلوماتية من شخص طبيعي أو معنوي، فإن المجني عليه في تلك الجرائم قد يكون كذلك شخصا طبيعيا أو معنويا،مع أن غالبية هذه الجرائم تقع على شخص معنوي،فالضحية هنا كل شخص أصابه ضرر مادي أو معنوي نتيجة الإستخدام غير المشروع لتقنية المعلومات، وقد يتمثل في شخص عام ممثلا في مؤسسة الدولة وهيآتها، وقد يكون خاصا ممثلا في الأشخاص الطبيعية أو المعنوية، ومنه فإن الضحايا في لجريم المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية من مجرد كونهم أشخاصا عادية إلى مؤسسات مالية أو عسكرية أوقطاعات حكومية، ومنه فإنمايستهدفه المجرم المعلوماتي لإنجاز عمله هو الإلمام بالمعلومات المراد بها تحقيق فعله الإجرامي، بحيث أن المعلومات أضحت في الوقت الحاضر من أهم المصالح المستهدفة بعد الأموال، وخصوصا إذا كانت هذه المعلومات مهمة وتخدم مصالح المجرم، وكان هدف المجرم الحصول على مقابل، ويلاحظ أهمن الصعوبة تقدير حجم الجريمة المعلوماتية بتحديد الضحايا بأكمل وجه، ومما يجدر الإشارة إليه في هذا الصدد هو دور المجني عليه في كبح الجريمة المعلوماتية، إذ يفضل الأغلبية في الإبقاء على مالحقهم مناعتداء سرا، وبعبارة أخرى ميلهم للتكتم عما لحقهم من أضرارجراء الجريمة المعلوماتية يكمن في رغبتهم في الحفاظ على مكانتهم الاجتماعية، أو حماية لمركزهم المالي وثقة العملاء بهم، كون أن أكثر مايحرص عليه القائمون على هذه المؤسسات هو السمعة المالية للمؤسسة، لذا فهم يفضلون تحمل الخسائر على عدم رغبتهم في الكشف عن الاختراقات التي لحقتهم بسبب هذه الجرائم، حتي لاينظر لضعف تدابير الحماية لديهم، فتسبب ضعف الثقة بالمؤسسة وبالتالي عزوف العملاء عنها[1].

كذلك فبتعدد المتضررين من الجريمة المعلوماتية فمرتكبي هذه الأخيرة تستهدف فئات معينة كالمؤسسات المالية والجهات الحكومية، الأشخاص الطبيعيون، مقدمي الخدمات الوسيطة في نطاق شبك الأنترنيت، وغيرهم من الأشخاص الذين تستهدفهم الجريمة المعلوماتية، كذلك نذكر بإيجازأهم ما يمكن ذكره عن المعلومات التي يتحصل عليها المجرم المعلوماتي بطريقة غير شرعية وهي:

1- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص61.

- المعلومات المالية:لمرتبطة بالمركز المالي والحسابي والإداري وانتقال الأموالوالاستثمارات[1].

-المعلومات التجارية :خصوصا في ما يتعلق بالتجارة الالكترونية وعمليات التجسس والقرصنة الحاصلة عليها[2].

- المعلومات الشخصية: المرتبطة بخصوصية الأشخاص الطبيعية أو المعنوية كالشركات والمستشفيات وأقسام الشرطة، والأحزاب والنقابات وغيرها، سواء كانتمخزنة بذاكرة الحاسوب أم مدخلة في بنوك المعلومات، إذ يتم تشويشها وإظهارها على غير حقيقتها[3]، ويدخل في هذا النوع بما يتعلق بأسرارالدولة والمشاريع المرتبطة بالتسليح الحربي، والتي تعد هذه الأخيرة أكثر عرضة للإعتداء من غيرها.

الفرع الثاني: دوافع إرتكاب الجريمة المعلوماتية

مما لا شك فيه أن مرتكبي الجريمة الالكترونية تختلف عن الأفعال الإجرامية التقليدية لذا من الطبيعي أن نجد نفس الاختلاف في أسباب وعوامل الدافعة لإرتكاب الفعل غبر المشروع، ومايجدر ذكره أن الجريمة مهما اختلفت وتنوعت تسميتها فهي في الأخير ستتشكل من عناصر رئيسية لتشجع المجرم على إرتكابها وهي: اما باعث معين، أم هدف الضحية، الفرصة المواتية، غياب عيون الأمن[4]، فالجريمة المعلوماتية لاتخرج عن بواعث لها نفس المراد إما تحقيق الربح وكسب المال، وثانيا الرغبة في الدخول إلى الأنظمة المعلوماتية للحسابات الآلية والمعلومات التي تحتويها بدافع المتعة والتسلية، أو إثبات الخبرة التقنية دون المساس بالأنظمة، وأخيرا الرغبة في الإضرار بهذه الأنظمة،ومنه فإن الفقه قسم هذه الدوافع إلى نوعين دوافع شخصية و أخرى خارجية.

أولا: الدوافع الشخصية.

وقد تكون دوافع الشخصية لدي المجرم المعلوماتي إما دوافع مادية وإما دوافع ذهنية.

-1-الدوافع المادية: يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لإقتراف الجريمة المعلوماتية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها ويدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتبس الفرص ويسعى للإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون ترك أثرا وراءه، فيعمد الجاني رغبة منه في تحقيق الثراء والكسب المادي للتلاعب بأنظمة المعالجة الآلية للبنوك والؤسسات المالية إن كان أحد موظفيها، أو إختراق النظم المعالجة الآلية لها من خلال إكتشافها لفجواتها الأمنية، فيعمل على إستغلالها وبرمجتها لتحويل مبالغ مالية

1- توفيق شمبور وآخرون، السرية المصرفية، أبحاث ومناقشات الندوة التي نظمها اتحاد المصارف العربية، لبنان، 1993، ص82.

2- هدى حامد قشقوش، الحماية الجنائي للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000، ص18/06.

3- طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، دار صادر للمنشورات الحقوقية، ط1، بيروت، 2001، ص150،

4- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الأسكندرية، 2005، ص126.

لحسابه أو لجساب شركائه، أولحساب من يعمل لحسابهم إن كان من خارج المؤسسة، كما يمكن الحصول على المكاسب المادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة SECURITEINFORMATIQUE،وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل إختلاس أموال، و23%من أجل سرقة معلومات ، و19%أفعال إتلاف،و15%الإستعمالالغير مشروع للحاسوب لأجل تحقيق منافع شخصية.

وفي حقيقة الأمر أنه في حال نجاح المجرم المعلوماتي في إرتكاب جريمته المعلوماتية فإن ذلك يدر عليه أرباحا كبيرة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة إقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدي الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية، ومؤسسات صحية وجامعات التي أظهرت حجم الخسائرالناجمة عن الجرائم المعلوماتية، فقد تبين أن 85% من المشاركين في الدراسة تعرضوا لإختراقات للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الإعتداءات[1]، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي وإثبات المقدرة.

-2-دوافع ذهنية: غالبا مايكون الدافع لدي مرتكب الجرائم المعلوماتية هو الرغبة في إتلاف الذات دون أن يكون له نوايا خادعة، ويرجع دلك لوجود عجز في التقنية التي تترك القرصة لمشيدي برامج النظام المعلوماتي، لإرتكاب الجرائم وعليه فإنه يرى البعض أن الدافع إلى إرتكاب الجرائم المعلوماتية يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، إلا أنه في الحقيقة نيته تحقيق الربح دافعا أكثر تحريكا لجرائم الحاسوب من الرغبة في قهر النظام.

ثانيا: الدوافع الخارجية.

إن تأثر الإنسان من بعض المواقف يجعله في حالة إستسلام تام لكثير من المؤثرات والدوافع الخارجية، التي تدفعه لإرتكاب بعض الجرائم الإلكترونية، وذلك نتيجة لوجوده في البيئة المعالجة الآلية للمعلومات، ومع توافر هذه المؤثرات، فإن الأمر حتما سيأدي إلى إرتكابه للجريمة الإلكترونيةو غما بدافع الانتقام أو الجنون أو بدافع التعاون والتواطئ على الأضرار والتهديد ويمكن إبراز أهم هذه الدوافع كالتالي:

-1- دافع الإنتقام: يعد هذا الدافع من أخطر أنواع الدوافع التي تدفع الشخص لإرتكاب الجريمة، فقد يتوفر هذا الدافع نتيجة فصل الموظف من عمله،أوتخطيه من الحوافز أو

1- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012 ص61/60.

الترقيات، قد يكون الإنتقام مؤثر في إرتكاب جرائم إلحاق الضرر برب العمل ،ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشئات بحيث بعد رحيله من المنشأة بعد أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشأة، ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، ويتعرضون لنحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، ومن طبيعة علاقات العمل المنفردة في حالات معينة، هذه الأمور قد تدفع النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لإرتكاب جرائم الحاسوب، بعثها الإنتقام من منشأة أو رب العمل [1]، وثال ذلكأن الانتقام دفع بمحاسب للتلاعب بالبرامج المعلوماتية بحيث جعلها تخفي كل بيانات الحساب الخاصة بديون الشركة التي يعمل بها بعد رحيله بستة أشهر.

-2دافع التعاون والتواطؤ: هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا مايحدث بتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو المؤسسة التي يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة مايمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منظمة حول أنشطتهم.[2]

واذا كانت هذه أبرز الدوافع لإرتكاب الجريمة الالكترونية، مع ذلك فهي ليست ثابتة ومعتمدة لدي الفقهاء والباحثين لأن السلوك الاجرامي والدوافع لارتكاب الجريمة الالكترونيةقد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلىتدميرها أو على الأقل حيازتهاللقيام بعملية الابتزاز والحصول على الأموال، لذلك فان هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد لدي كل جريمة دوافع جديدة، بل كثيرا مانجد الجريمة الواحدة لها دوافع متعددة خاصة ماأذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.[3]

المبحثالثاني:خصوصية البحث والتحقيق في الجريمة المعلوماتية

تعد الجرائم المعلوماتية من أشد الجرائم خطورة وإضرارا بالفرد والمجتمع، لاسيما لما باتت تشكله من خطر يمس بأمن الدولة كذلك، الأمر الذي دفع معظم التشريعات سواء على التشريعات المقارنة أو على المستوي الدولي والإقليمي أو في التشريع الجزائري، بالنظر في جانب التصدي إلى مكافحة هذا النوع من الجرائمفكثرة الإستنزافالمستمر للجرائم المعلوماتية أدى إلى ضرورة تطوير أجهزة الضبط القضائي تتلاءم مع التطورالحاصل في هذه الجريمة ووضع سبل وإجراءات للتصدي إلى النتيجة الحاصلة، بحيث أن هذه الاجراءات تعد جوهر الكشف عن هذا النوع من الجرائم ومتابعة مرتكبيها، وهذا ما سنستعرضه في المطلب الأول،وهذه الاجراءات تمر بما يسمى بمرحلة البحث والتحقيق بحيث أن الاولى تنظم التحريات التي تناط بها الضبطية القضائية التي تتجسد في

1- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، 2018، ص40.
2- سعيداني نعيم. المرجع السابق، ص62.
3- سعيداني نعيم، المرجع السابق، ص62.

الشرطة القضائية وأعوان الضبط القضائي، أما التحقيق تكمن في الاجراءات التي تجرى بعد توجيه الاتهام إلى شخص متهم يبادر معه التحقيق في جرم إرتكبه،فالتحقيق هو اجراء من اهم الإجراءات التي تتخذ بعد وقوع الجريمة لما لهو من أهمية في التثبت من حقيقة وقوعها وإقامة الاسناد المادي على مرتكبيها باذلة الاثبات على اختلاف أنواعها وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول الى ادلة ادانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة ومن خلال دراستنا هنا فالتحقيق كإجراء قانوني عام يختلف بمفهومه وخصوصيته في ضبط الجرائم من خلال دراستنا في نطاق هذا النوع المستحدث من الجرائم المعلوماتية، ولذلك فقد تطرقنا غلى مفهوم وخصوصية التحقيق في المطلب الثاني.

المطلبالأول:الأجهزة المخولة بالبحث والتحري في الجريمة المعلوماتية

إذا كان التحقيق يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه وان يحاول بكل الجهد الممكن ان يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة فان التحقيق في البيئة الالكترونية يستوجب بالإضافة الى كل هذا تطويرا لأساليبه وتكليف أجهزة مختصة لممارسته من اجل مسايرة حركة الجريمة وتطور أساليب ارتكابه، اذ لا تكمن هده الأجهزة على المستوى الوطني فقط بل هناك أجهزة متخصصة على المستوى الدولي و الإقليمي أيضا، وهذا ما سنتطرق إليه في هذا المطلب بحيث سنستعرض أجهزة المتخصصة على المستوي الداخلي في بعض البلدان الأجنبية والعربية ثم نعرج الدراسة للأجهزة المختصة في الجزائر في الفرع الأول، ويليه التطرق إلى الأجهزة المختصة على المستوي الدولي ثم الإقليمي وهذا في الفرع الثاني.

الفرع الأول: الأجهزة المكلفة بالبحث والتحري على المستوى الداخلي

لقد تعددت الأجهزة المكلفة في نطاق مكافحة الجرائم المعلوماتية، اي كان على المستوى الداخلي في التشريعات المقارنة أو الوطني(التشريع الجزائري)، انه بالنظر الى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية ذهبت اغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة الى ان تعهد بمسالة البحث والتحري عن هذا النوع من الجرائم لأجهزة متخصصة لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستخدم من الاجرام وسوف نحاول ان نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نصب الموضع على الوضع في بلادنا[1].

أولا: الأجهزة المختصة في متابعة الجريمة المعلوماتية في التشريعات المقارنة

-1- الأجهزة المختصة في الدول الأجنبية: كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة اذا ان مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية

1-سعيداني نعيم، المرجع السابق، ص104/103.

وبمدى توفر الإمكانات المادية الازمة لإنشاء هذه الأجهزة على سبيل المثال في هذا الصدد الدول التالية

أ- الولايات المتحدة الامريكية : قامت الولايات المتحدة الامريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها:

- شرطة الواب web police: وتعتبر نقطة مراقبة على الانترنت إضافة الى انها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة والبحث عن الأدلة ضدهم وتقديمهم الى المحاكمة[1].

- مركز تلقي شكاوى جرائم الانترنت: والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي في سنة 2003 تم دمج مركز شكاوى الاحتيال عبر الإنترنت مع هذا المركز ويعمل مركز بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الانترنت اين يقوم الشاكي بملىء استمارة الكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل.

- قسم جرائم الحاسوب والاتصال: وتتألف من مجموعة من قضاة النيابة العامة ممن تلقو تدريبات مكثفة على نظم المعالجة الالية للبيانات وتم منحهم صلاحيات واسعة في مجال جرائم المعلوماتية والعدوان على حقوق الملكية الفكرية

- المركز الوطني لحماية البنية التحتية التابع: للمباحث الفدرالية الامريكية وقد حدد هذا المركز البنى التحتية التي تعتب هدفا للهجومات والاعتداءات عب الانترنت وعلى راسها شبكات الاتصالات.

كذلك نجد في اسرائيل جهاز المرصاد: جهاز الاستخبارات من جهة ويتبع مكتب رئيس الوزراء، ويتولى إدارة شبكات التجسس وتجنيد وزرع العملاء في جميع أنحاء العالم.

واضافة الى هذه الأجهزة يوجد أيضا في الولايات المتحدة الامريكية وحدة متخصصة بمكافحة الاجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والانترنت ومن مستشارين قانونيين[2].

ب - في بريطانيا : قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث العلمي والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني وقد بدات هذه الوحدة نشاطها عام 2001.

1- جميلعبدالباقيالصغيرالجوانبالإجرائيةللجرائمالمتعلقةبالأنترنات،المرجعالسابق .ص77

2- نبيلة هبة محمد هروال، الجوانب الاجرائية لجرائم الانترنات في مرحلة جمع الاستدلالات، ط1، دار الفكر الجامعي الاسكندرية، ص54.

ت ـ في فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكر من هذه الأجهزة القسم الوطني لقمع جرائم المساس بالأموال والأشخاص: ويتكون هذا القسم من مختصين في التحقيق بجرائم العالم الافتراضي وقد بدا هذا القسم مهامه عام 1997[1]، كذلك المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات والاتصالات: ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية وقد تم إنشاؤه في عام 2000/05/15.

ج ـ في الصين: قامت السلطات في هذا البلد ببرمجة وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم القوة المضادة للهكرة وهي تختص برقابة المعلومات التي تسمح لمواطنيها الدخول اليها عبر الانترنت.

واما على المستوى العربي فنجدها لم تقف مكتوفة الايدي امام خطر الجرائم المعلوماتية فقد قامت بعض الدول العربية بإنشاء أجهزة متخصصة لمكافحة هده الجرائم ونذكر على سبيل المثال

د ـ في مصر: قامت وزارة الداخلية في مصر بأنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرض لها على النحو التالي:

ـ إدارة مكافحة جرائم الحسابات وشبكات المعلومات: أنشئت هذه الإدارة بموجب قرار وزاري وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الامن العام التابعة لوزارة الداخلية وتضم ثلاث اقسام رئيسية هي :قسم التامين وقسم الوزارات الداخلية وتضم ثلاثة اقسام رئيسية هي قسم العمليات قسم التامين وقسم البحوث والمساعدات الفنية وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية فهي تتكون من ضباط متخصصين في مجال تكنلوجيا الحسابات والشبكات وتختص بمكافحة جرائم الانترنت على مختلف أنواعها[2].

ـ قسم مكافحة جرائم الحسابات وشبكات المعلومات: وقد أنشئ هدا القسم بالإدارة العامة للبحث الجنائي بمديرية القاهرة ويتبع إدارة المعلومات والحاسب الالي ويخضع من حيث الاشراف الفني للإدارة مكافحة جرائم الحاسبات وشبكة المعلومات ويختص بعمليات تامين ورقابة نظم وشبكات المعلومات لمنع وقوع اية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.

ه. المملكةالعربيةالسعودية :حيثصدرفيعام1428نظاممكافحةالجرائمالمعلوماتية بوضعالعقوباتلمرتكبيهاوأسندهذاالنظامإلىوزارةالداخليةمسؤوليةتنفيذهذاالنظام والذييهدفإلىوضعمعاييرقانونيةوتنظيميةلمكافحةجرائمالمعلوماتوالحاسبالآلي

1- سعيداني نعيم، المرجع السابق، ص105.
2- سعيداني نعيم، المرجع السابق، ص106.

والإنترنتمنخلالتحديدالجرائمذاتالصلةواتخاذإجراءاتتأديبيةمقابلكلجريمةأو إنتهاك[1].انتهاك يقومبابتزازبصوريحصلهكرألقتأجهزةالأمنفيالمملكةالعربيةالسعوديةعلى عليهامنخلالعملياتاختراقإلكترونيةكمين،2010كماأوضحتدراسةأجرتها شركةالخليجللحاسباتأندولالخليجالعربيةتعتبرأحدالأهدافالرئيسةللجرائم الإلكترونية[2].

ثانيا: الأجهزة المختصة بالبحث والتحري في التشريع الجزائري

ومن أجل التصدي للجريمة المعلوماتية إتجهت لوضع هيئات وأجهزة خاصة من أجل المباشرة في البحث والتحري فيها نذكرها في ما يلي:

-1- الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: انشأت بموجب القانون 04/09 نصت عليه المادة 13 المؤرخ في 05 أوت 2009[3]، ويقصد بها جرائم المساس بأنظمة معالجة الآلية للمعطيات أو أي جريمة أخري ترتكب بسهولة بواسطة منظومة معلوماتية أو نظام الاتصالات الالكترونيةومن مهام هذه الهيئة :

أ- تفعيل التعاون القضائي للسلطات القضائية ومصالح الشرطة القضائية في التحريات بشأن الجرائم المعلوماتية المادة 04 من القانون السالف الذكر، بما في ذلك تجميع الخبرات القضائية لتنشيط وتنسيق عملات المكافحة ضد الفاعلين المشتركين في ارتكاب الجرم على المستوى الوطني، من خلال القيام بإذن منى السلطات القضائية بجميع إجراءات التحري دون المساس بإختصاص باقي الهيئات المختصة بمكافحة جرائم مختلفة منصوص عليها في القانون، كذلك تقديم مساعدات لمصالح الأمن والدرك الوطني ومصالح الدولة، بالإضافة إلى التدخل الفوري تلقائيا لتقديم المساعدات بعد موافقة السلطات المختصة، وكذلك المباشرة بالبحث الميداني في وقائع مرتبطة بتحقيق تقوم به السلطات نصت عليه المادة 04 من قانون 04/09.

هناك الحالات التي تسمح بمراقبة الاتصالات الالكترونية لأغراض وقائية كالوقاية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بادن النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.

والوقاية من اعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة او الدفاع الوطني او المصالح الاستراتيجية للاقتصاد الوطني بادن السلطة القضائية المختصة

1- فيصلحسنحامد،التحدياتالتيتواجهالأجهزةالأمنيةفيالمملكةالعربيةالسعودية،المجلة العربيةللدراساتالأمنيةوالتدريب،العدد 63 الرياض، 2015 ،ص174

2- فيصل حسن حامد. المرجع السابق. ص173.

3- نصت المادة على" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته يحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم" الق 04/09، المؤرخ في 05 أوت 2009،الجريدة الرسمية العدد 47، ص08.

ب.التبادل مع نظير لها في الخارج قصد جمع المعطيات المفيدة في التعرف غلى الجناة وتحديد مكان تواجدهم[1]، كذلك السماح بمراقبة الاتصالات الالكترونية لصد الخطر الذي يمس بالمجتمع أو أمن الدولة، كجرائم الارهاب وتشكيل عصابات اجرامية... أو الوقاية من بوادر إجرامية تهدد مؤسسات الدولة في أي مجال كان أو الدفاع الوطني للبلاد.

- حيث أنه على مستوى جهاز الشرطة فقد انشات المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين بكل من قسنطينة ووهران تحتوي هذه المخابر على فروع تقنية من بينها خلية الاعلام الالي بالإضافة الى انه يوجد على مستوى مراكز الامن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر[2].

- اما على مستوى الدرك الوطني فانه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الاجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الاعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية بالإضافة الى مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية ومكافحتها الذي يوجه إلى التنبه لسلامة الانظمة المعلوماتية ومنع الخطر عنها، ببئر مراد رايس والتابع لمديرية الامن العمومي للدرك الوطني.

-2- الهيئات القضائية الجزائية المتخصصة: انشئت بموجب القانون 14/04 المؤرخ في 10نوفمبر2004 المعدل للقانون الإجراءات الجزائية .

أ. تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الالية للمعطيات طبقا للمواد 37– 329-40 قانون إجراءات الجزائية[3].

اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06المؤرخ في2006/01/05

إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام الاتصال بالمرتكبة في الخارج حتى ولو كان مرتكبيها اجنبيا ادا كانت تستهدف مؤسسات الدولة او الدفاع الوطني المادة 15 من القانون رقم 04/09.

ب. توسيع صلاحية الضبطية القضائية: عند معاينة الجرائم الماسة بأنظمة المعالجة الالية كما يمكن تمديد الاختصاص المحلى على كامل الإقليم الوطني المادة 16 قانون إجراءات جزائيةكما يمكن تفتيش المحلات السكنية في كل ساعة من ساعات الليل والنهار بادن من وكيل الجمهورية حسب المادة47 قانون الإجراءات الجزائية.

1- أحمد مسعود مريم، آليات مكافحة تكنولوجيات الاعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير، جامعة قاصدي مرباحي، ورقلة، كلية الحقوق، تخصص قانون جنائي، 2013/2012، ص46.

2- سعيداني نعيم، المرجع السابق الذكر، ص107.

3- مولود ديدان، قانون الاجراءات الجزائية، الأمر 02/11، دار بلقيس ، الجزائر، ص18.

أساليب التحري الخاصة:اعتراض المرسلات الالكترونية المادة65 مكرر5 قانون إجراءات الجزائية المدرجة بموجب القانون 06-22المؤرخ في2006/12/20

التسرب المادة65 مكرر11من قانون الإجراءات الجزئية

تفتيش المنظومة المعلوماتية المادة 5 من القانون رقم04/09

- حجز المعطيات المعلوماتية المادة 6 رقم04/09

- نسخ المعطيات على دعامة تخزين الكترونية.

- إمكانية منع الوصول الى معطيات تحتويها المنظومة.

- منع الاطلاع على المعطيات التي تشكل محتواها جرائم.

وفي كل جميع أنواع التحقيق هذه يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزئية وهو الامر الذي يفهم صراحة من خلال استقراء نص المادتين 38 و12 ومن قانون الاجراءات الجزائية الجزئية الواردتين في الباب الأول من هذا القانون تحت عنوان في البحث والتحري عن الجرائم حيث تنص المادة 12ف3 انه يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وتنص في نفس الوقت المادة 38من نفس القانون انه يناط بقاضي التحقيق إجراءات البحث والتحري في الجرائم المعلوماتية.

وعليه فانه يمكن القول ان إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان اوليا ام ابتدائيا وبهذا المفهوم فان إجراءات البحث والتحري يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولى بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

الفرع الثاني: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي

سبق وان أسلفنا الذكر بان الجرائم المعلوماتية تتميز بانها عابرة للحدود الوطنية يمكن ان يتعدى أثرها عدة دول لذلك لابد من وجود تعاون دولي من اجل مكافحة هذا النوع من الاجرام ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن ان يحقق أهدافه لا قبل الشرطة الإقليمية بتحقيقها ومن ابرز هده الأجهزة في مجال مكافحة الجرائم المعلوماتية على هدا الصعيد ندكر ما يلي:

أولا: على المستوى الدولي

المنظمة الدولية للشرطة الجنائية الانتربول من اهم الأجهزة على المستوى الدولي لمكافحة الاجرام بصفة عامة ومنها الجرائم المعلوماتية وتهدف هذه المنظمة الدولية الى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من اجل مكافحة

الجريمة ذات الطابع العالمي بما في ذلك الطابع العالمي بما في ذلك الاجرام المرتبط بالمعلوماتية[1] وتستخدم هده المنظمة لتحقيق أهدافها وسيلتين :

1- تجمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف

2- التعاون في ملاحقة المجرمين الفارين والقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم،

وتعمل المنظمة الدولية للشرطة الجنائية في مجال المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحي في قضايا الجرائم المعلوماتية من خلال خلق فرق عمل وورشات تكوين ولقد انشات هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الاجرام وكيفية التدريب على مكافحته

ثانيا: الأجهزة على مستوى الإقليمي

الشرطة الأوربية او الأورروبول: وهو جهاز على مستوى الاتحاد الأوروبي تم إنشاؤه في لكسمبورغومقره في مدينة لاهاي بهولندا تملك الوكالة قرابة 700 موظف في مقرها الرئيسي، ليكون حلقة وصل بين أجهزة الشرطة للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الاجراء المعلوماتي ويهدف هذا الجهاز الى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتيةوبمبادرة من الشرطة القضائية الفرنسية تم انشاء جهاز على مستوى الاورروبول أطلق عليه اسم ICROS (internet crime repporting online system)

الاوروجست: EUROJUST **وهو** جهاز يعمل على المستوى الأوربي الى جانب الاوروبول في مجال مكافحة جميع أنواع الجرائم تم إنشاؤه عام 2002 وينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوربي او دولة عضو مع أخرى من غير الاتحاد الأوربي ويعد الاوروجيست وحدة للتعاون القضائي مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية[2] .

المطلب الثاني: خصوصية التحقيق والمحقق في الجريمة المعلوماتية

للتحقيق أهمية في إثبات وقوع الجرائم وإقامة الدليل على مرتكبيها بأدلة الإثبات علىاختلاف أنواعها، وهوكما يدل عليه اسمها استجلاء الحقيقة لغرض الوصول لإدانة

1- سعيداني نعيم، المرجع السابق، ص107.
2-سعيداني نعيم، المرجع السابق، ص108.

المتهممن عدمه بعد جمع الأدلة القائمة على الجريمة ومن يقوم بالتحقيق هما الضبطية القضائيةوقضاة وفقإجراءات البحث والتحري المحددة وفقا لقانون الإجرءات الجزائية.وعليه سنعالج هذا المطلب من حيث سيمات التحقيق والمحقق الالكتروني في الجرائم المعلوماتية.لقد تعددت تعريفات رجال الفقه في تعريف التحقيق فمنهم من عرفه بأنه العلم الذي يرشد المحقق إلى كيفية السير في التحقيق من بدايته إلى نهايته ويعلمه كيف يكشف الجرائم الغامضة بتتبع اثر الجاني إذا فر من وجه القضاء للقبض عليه وينال ما يستحق من جزاء.[1]إذا كان التحقيق يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه وأنيحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلةوالتنقيب عنها وصولا لإظهار الحقيقة، إلا أن هذا التحقيق يجد أمامه عوائق مما يحدث عرقلة في السير في مقتضيات الجريمة وبالتالي صعوبة إكتشاف الحقيقة، ومن هذا المطلب تطرقنا إلى خصوصية التحقيق في الفرع الأول، ثم صعوبات التي تواجهه في الفرع الثاني.

الفرع الأول: خصوصية التحقيق في الجريمة المعلوماتية.

تعد مرحلة التحقيق مرحلة حاسمة في آليات البحث والتحري عن الجرائم،لأنه تعد المنبع الأساسي الذي سيتم علي أساسه مباشرة الدعوى، إذ أنه يعد من أهم الإجراءات التي تأتي بعد وقوع الجريمة، وبما أن التحقيق من مهام المحقق الجنائي سنتناول تعريف التحقيق وخصائصه ثم تعريف المحقق في الجريمة المعلوماتية.

أولا :تعريف التحقيق في الجريمة الإلكترونية

عرف التحقيق على أنه: " إتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها[2]".

كذلك عرف التحقيق بأنه " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه أو عدم لزومها[3]".

فالتحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى ،فلهقواعد ثابتة وراسخة بدونها ماكان ليتمتع التحقيق بتلك الصفة وهذه القواعد إما قانونية وإما فنية، فالأولى له صفة الثبات التشريعي لايملك المحقق إزاءه اشيئا سوى الخضوع والامتثال لها أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير[4].

1-مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط1، مطابع الشرطة، مصر، 2008، ص165.
2- عمر بن إبراهيم بن خماد العمر، إجراءات الشهادة في مرحلتي الإستدلال والتحقيق الإبتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2007، ص22.
3- حسن الجوخندار، التحقيق الإبتدائي في أصول المحاكمات الجزائية، دار الثقافة، عمان، ط1، 2008، ص11.
4- سعيداني نعيم، المرجع السابق، ص108.

فالتحقيق هو إجراء يتم بواسطة المحقق لإزالة اللغز عن الجريمة محل التحقيق، وصولا للحقيقة المرادة، وتكون بواسطة أسلوب من أساليب البحث والتحقيق كالتفتيش أو ضبط الأدلة..."

بالإضافة للخصائص التي يتميز بها التحقيق في أي جريمة و فإن التحقيق في الجرائم المعلوماتية له ميزات نذكرها :

أ ـ وضع خطة عمل التحقيق : يبدأ المحقق عند تجميع الإستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني للقيام بمساعدته في أعمال التحقيق [1].

ب ـ إتباع منهج أو أسلوب التحقيق الإبتدائي في الجريمة المعلوماتية: التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى إكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهرات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي[2] .

ج . تشكيل فريق للتحقيق: إن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية، لما تطلبه من مهارات وخبرات متنوعة قد لا تتوافر لدي المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العلمية غالبا مايتكون فريق التحقيق من :

ـ خبراء الحاسوب وشبكات الانترنت الذين يعرفون ظروف الحادثة و التعامل مع هذه الجرائم

ـ خبراء الضبط وتحرير الأدلة الرقمية بأمور تفتيش الحاسوب.

ـ خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

ـ خبراء التصوير والبصمات والرسم التحطيطي [3].

فهنا نجد ان المشرع الجزائري قد أشار لإمكانية الإستعانة بالخبراء المتخصصين الذين لديهم دراية وكفاءة ذات مستوي في مجال الحاسوب والنظام المعلوماتي من قبل جهات التحقيق[4].

1- محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في الجرائم الحاسوب والأنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياضو 2004، ص72.

2- سعيداني نعيم، المرجع السابق، ص108.

3- عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص613.

4- المادة05، من الق 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المعدل والمتتمم 2019.

د ـ إتباع إجراءات قبل وأثناء التحقيق، فقبل التحقيق هناك تدابير يجب الإستعانة بها كتحديد نوع المعالجة الأولية للمعطيات، السرعة في رصد حفظ الدليل خوفا من تدخل الجاني لإتلاف المعلومات المحفوظة للكشف عن الحقيقة...،أما أثناء التحقيق فتتجلى في

ـ عمل نسخة من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ

ـ نزع غطاء الحاسب الآلى المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

ـ العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

ـ حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة

ـ العمل على فحص تطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس المعلومات.

ـ أن يكون الهدف من النسخ محتوي الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات الممسوحة، وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.[1]

ثانيا: خصائص المحقق في الجريمة المعلوماتية

أمام التطور التقني والتكنولوجي الذي صاحب الجريمةالمعلوماتية ،فإن المتخصصينبالتحقيق في هذ االنوع من الجرائم المستحدثة يختلف عن المختصين ضبطالجرائمالتقليدية من حيث الخصائص وطريقة التكوين ،ذلك أن التحقيق في هذه الجرائم لا يعتمد على لغة الجسد،إنما يعتمد على بلورة العلم والتكنولوجيا وإتصافهم بالدراية والذكاء الفارط كون مهامهم يرتبط بمجال التقنية الإلكترونية أثناء آدائهم مهمة البحث والتحري عن الجرائم المعلوماتية والكشف عنها.

يعرف المحقق أنه الشخص القائم بأعمال إجراءات التحقيق الجنائي، بحيث عرف أنه" كل من عهد إليهالقانون بتحري التحقيق في البلاغات والحوادث الجنائية، ويساهم بدوره في كشف غموضهاوصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريهاالمحكمة"[2].

كما عرفه البعض أنه كل شخص يقوم بعمل من أعمال التحري و التحقيقوالبحث عن الأدلة لتقديمها كدليل سواءا للبراءة أو الإدانة أمام القضاء وذلك للكشف عن مرتكبيها وصولا للحقيقة وسد الإبهام اذي يتدارك الجريمة.

1- سعيداني نعيم، المرجع السابق، ص114.
2- خالد ممدوح إبراهيم، المرجع السابق، ص87.

أما المشرع الجزائري فقد وضع تعريفا لقاضي التحقيق في المادة 68 من ق الإج الج حيث تنص على" يقوم قاضي التحقيق وفقا للقانون بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإتهام وأدلة النفي"

إضافة إلى الخصائص التي تميز المحققين في الجرائم التقليدية، فإن المحقق الجنائي في الجريمة المعلوماتية يتميز بسيمات تميزه عن غيره من المحققين في الجرائم الأخري وهي ما يلى:

أ- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعقب الجريمةالمرتكبة.

ب. وصولا الاخبار تو البلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنييناالذين يعملون على هذه الأجهزة.

ج - إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلةالإلكترونيةالتي تدل على وقوع الجريمة، وتخزينها في الأقارص المعدة لذلك ومنع حذفها، فالتأخير في حفظ الأدلة قد يعرضها للفقدان والضياع مما يسسبب التأخير في إجراءات التحقيق.

د - حياد المحقق أثناء إجراء التحقيق يعتبر من الخصائص الهامة، فيجب أن يقوم بالتحقيق شخص غير متحيز يعني بما يقيد الدفاع عنايته بأدلة الإتهام، ولا تتحقق الحيد التامة إلا إذا استقلت سلطة التحيق عن كل من سلطة الإتهام من ناحية وسلطة الحكم من ناحية أخري، فلا يجوز للنيابة المنوط بها توجيه الاتهام أن تحقق بعدل [1].

و- قوة الملاحظة والمهارةأثناء البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول إلى البرامج المخزنةوكيفية الحصول على الأرقام السرية والشفارات التي تمكنهم من الدخول إلى الحاسوب.

ي - وضع خطة عمل مع جميع أعضاء فريق التحقيق، والتشاور معهم لمعرفة جميعالجوانب الفنية للجريمة التي يجري التحقيق بشأنها.

و- الإلزام بالسرية والكتمان وذلك للحفاظ على مقتضيات القضية، الجريمة والسير في الجريمة طبقا لإجراءات صحيحة.

الفرع الثاني: صعوبات التحقيق في الجرائم المعلوماتية

يتصف التحقيق في الجرائم المعلوماتية في الجرائم المعلوماتية بالعديد من المعوقات والصعوبات، فنظرا لكون الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاسي الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها، أدت إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية التي نظمت مسألة

1- فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار النمطبوعات الجامعية، الاسكندرية، 2006، ص56.

إستخلاص الدليل الرقمي، وتضعف قيمتها في مكافحة هذا النوع من الجرائم وتؤثر على عملية التحقيق وتؤدي بها للخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في أجهزة التحقيق، بل وتنعكس على المجرم نفسه حيث يشعر أن الجهات الأمنية غير قادرة على إكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الامر الذي يعطيه ثقة أكبر في إرتكاب المزيد من هذه الجرائم[1] .

لذلك ظهرت معيقات ترتبط بالتحقيق كتن لها الأثر البالغ في عملية الكشف عن الحقيقة، ومن بين هذه المعيقات نذكرها:

أ- قلة خبرة القائمين في هذه الجرائم: فهناك مايتعلق بشخصية المحقق مثل الهيبة من استخدام الكمبيوتر والانترنت، وهناك مايتعلق بالنواحي الفنية و لنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، وعدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية وقلة الخبرة في هذا المجال والمعرفة باللغة الإنجليزية، خاصة وأن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة تشكل الطابع المميز لمحادثاتهم [2].

ب- وقد يكون لحداثة هذا النوع من الجرائم وقلة المستكشف منها وراء عدم اكتساب تلك الأجهزة خبرة التعامل معها، ناهيك عن الإنتشار الواسع للكمبيوتر وتنوع برامجه وأنظمته مما يجعل حصر أساليب الجريمة المعلوماتية وصورها وأنماطها صعبا وبالتالي يتعذر معه تدريب المحققين[3] .

ج- كذلك من الصعوبات التي تعيق التحقيق في مجال الجريمة المعلوماتية والمرتبطة بالدليل الرقمي هي سهولة محو هذا الدليل أو تدميره في زمن قصير جدا، فإرتباط الجريمة المعلوماتية بالبيئة التقنية إنعكس على طبيعة الدليل المترتب عنها من حيث أن أمر ظمسه ومحوه من قبل الفاعل أمرا في في غاية السهولة، إذ بإمكان المستخدم الذي يتحكم في المعلومات أن يستعمل نظاما معلوماتيا من أجل محو تلك المعلومات التي تعد موضوعا للتنقيب الجنائي وبالتالي تدمير كل الأدلة، فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها بحيث لا يمكن السلطات من كشف الحقيقة، وإذا ماعلمت بها لا تستطيع إقامة الدليل ضده [4].

د- كذلك صعوبة الوصول إلى الدليل والتعرف على هذا الدليل و حمايته من الفقدان يضع إشكالا في عملية التحقيق وبالتالي صعوبة الوصول للحقيقة.

1- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، ص 119
2- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص69.
3- خالد ممدوح ابراهيم، نفس المرجع، ص70-71.
4- سعيداني نعيم، المرجع السابق، ص186.

ملخص الفصل:

في نهاية هذا الفصل، يتبين لنا أن موضوع الدراسة فيه كان متمحور حول نوع من الجرائم المستحدثةالتي ترتكب في بيئة إلكترونية بواسطة نظام الحاسوب أو الشبكة الحاسوبية وهي الجريمة المعلوماتية أو كما يقال الجريمة الإلكترونية، بحيث تحدثنا عن مفهوم الجريمة المعلوماتية من خلال عرض التعريف والأركان والخصائص التي تميزها عن الجرائم التقليدية، كونها جريمة مستحدثة تعتمد على نظام تقنية المعلومات، كما أن مرتكبي هذا النوع من الجرائم لهم دراية ومهارة في مجال هذه التقنية مما جعل لهم سيمات خاصة تميزهم عن غيرهم من المجرمين في الجرائم الأخري، بالإضافة للأسباب التي دفعتهم لإرتكاب هذه الجريمة.

وبسبب إرتفاع نسبة الإجرام الإلكتروني نتيجة إقتحام مجال التقنية الإلكترونية في كافة ميادين الحياة قمنا بتسليط الدراسة حول خصوصية البحث والتحقيق في الجريمة المعلوماتية، وذلك من خلال تصدي المجتمع الدولي لهذه الجريمة بتكليف أجهزة تتلاءم وطبيعتها بمكافحة الجرائم المعلوماتية سواء في التشريعات المقارنة أو على المستوي الدولي أو الإقليمي التي تكفلت بوضع آليات للتصدي لهذا النوع من الجرائم، فالتشريع الجزائري أيضا أعطي إهتمام لمواجهة هذه الجريمة المستحدثة من خلال وضع قوانين في مجال الإتصال والمعلومات كقانون 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بالإعلام والإتصال ومكافحتها، إذ أنه من الضرورة الإستعانة بهذه الأجهزة للتصدي لظاهرة الإجرام المعلوماتي، بسبب إرتفاع نسبة الإجرام، وهذه الأجهزة تواكب جهات أمنية متخصصة للتحقيق فيها يكونون ذو خبرة وكفاءة في هذا المجال. وفي بعض الأحيان فقصور تقنية التحقيق أو نقص في أدلة الإثبات يصعب على القائمين بالتحقيق كشف لغز القضية التي يحققون فيها في البيئة الإلكترونية مما يعيق السير في الإجراءات فنكون أمام معيقات تواجه البحث والتحقيق في هذا النوع من الجرائم.

الفصل الثاني

تختلف البيئة التي ترتكب فيها الجريمةالإلكترونية من وسط مادي محسوس الى وسط معنوي او ما يعرف بالوسط الافتراضي وعليه فإن البحث عن ادلة الاثبات في اطار ما يتوافق ويتناسب مع الطبيعةالتقنية لهذه الجرائم ووسائل ارتكابها لا يكون مجديا الا اذا كان مدعما من قبل التقنية ذاتها وهو ما استتبع ظهور طائفه جديده من الأدلة تتفق وطبيعة الوسط الذي ارتكب فيه الجريمةالإلكترونية وهي الأدلةالرقمية او بما يسمى الأدلةالإلكترونية.

فالدليل الرقمي ناشئ عن بيئة رقميه يصدر عن جرائم حديثه ويكون مرتبطا بتكنولوجيات وسائل الاتصال وشبكه الرابط الحديثة فانه من الضروري ان يكون اي تعريف لهذا النمط من الأدلة متسما بما يسمح باستعادة مع سائر الجرائم المرتكبةبالتقنية ام مبتكره التعامل مع المعلومات،ونظر لتزايد الجرائم المعلوماتيةنتيجة الاستخدام المفرط لتقنية المعلومات في مختلف مجالات الحياه العامة فإن ذلك ادى الى اتساع نطاق الدليل الالكتروني إذ اصبحت الأجهزةالإلكترونية من حواسب هواتف ذكيه كاميرا وشبكه الاتصالات الرقمية تشكل مستودعا مهما للمعلومات والبيانات التي من شانها ان تدعم جهود تحقيق العدالةالجنائية.

وعليه سلطنا الدراسة على طبيعة القانونية للدليل الرقمي من خلال مفهومه ومشروعيته وحجيته في الإثبات في المبحث الاول.

ونظر الخصائص المميزةو الاستثنائية التي تتمتع بها هذه الفئه من الأدلة من طبيعة فنيه او تقنيه وسهولة إخفائها أو التلاعب بها وسرعةمحوها من مسرح الجريمة فان اجهزة القضاء وجدت نفسها امام تحديات قانونيه وعلميه جديده لهذه الأدلةالإلكترونيةالمنتشرة في البيئةالافتراضية واساليب البحث والتحري عنها وكيفيه التعامل معها وهو ما دفع فقه الجنائي الى التدخل لرفع الابهام عن هذه المسالة من خلال تحديد نمط الأساليب الفنية للوصوللأدلةالإلكترونية ونطاقها وخصوصياتها من خلال الأساليب التقليدية والحديثةهذا ما سنوضحه بالتفصيل في المبحث الثاني.

المبحث الاول:طبيعة الدليل الرقمي في الجرائم المعلوماتية

ان تقييم اي نظام قانوني لا يمكن ان يصل الى نتائج صحيحه الا اذا توفر لدى المقاوم تصورا واضحا لذلك النظام شيء فرع عن تصوره، ولد فأننا سنتطلع في هذه الدراسة الى نظام الأدلةالرقمية انهم من الواجب ان نتناول هذا النوع من الأدلة بالتعريف وما هي عليه ولذلك سنه تناول في هذا المبحث مفهوم الدليل التعريف والانواع وقيمه القانونية من حيث المشروعية وحجيه هذا الدليل الرقمي

وعليه ففي مجال التعامل مع الأدلةالجنائية فان جهات البحث والتحري مقبله على الانتقال من مرحله التعامل مع الأدلةالمادية من الملموسةالمعلومة المصادر الى مرحله التعامل مع الأدلةالرقميةالإلكترونيةالمنتشرة في العالم الافتراضي المجهولة المصادر الى مرحله التعامل مع الأدلةالرقميةالإلكترونيةالمنتشرة في العالم الافتراضي المجهولة

المصادر وهو الامر الذي يثير لا محال الى وضع حلول في تحديد طبيعة الدليل الالكتروني التي تميزه عن الأدلةالتقليدية وذلك من خلال وضع تعريف وخصائص وأنواع ثم بيان قيمته في القضاء الجنائي من حيث الحجيه والمشروعية وهذا ما عرضناه في المطلب الأول.

من القواعد المستقرة في مجال الاثبات الجنائي ان القاضي لا يمكنه ان يقضي بعلمه الشخص فإحاطته بوقائع الدعوة يجب ان يتم من خلال ما يطرح عليه من ادله ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوة وعدد لهذه الأهمية التي يتمتع بها الدليل عموما حظى باهتمام في مختلف الأنظمةالقانونية من حيث تحديد شروط مشروعيته وتقدير قيمه الإثباتية وهذا ما تناولناه في المطلب الثاني.

المطلب الاول: مفهوم الدليل الرقمي

إن للتطور المستمر واللامتناهي للتكنولوجيا والمعلومات والاتصال حال دون وضع تعريف فقه شامله وشامل لمفهوم دليل الالكتروني خشيه حصر نطاقه داخل اطار تجريمي محدد قد يضربه خاصة في ظل التطور المستمر للتقنيةالإلكترونية،فالدليل الالكتروني ناشئ عن بيئة رقميه يصدر عن جرائم حديثه ويكون مرتبطا بتكنولوجيات وسائل الاتصال وشبكه الرابط الحديثة فانه من الضروري ان يكون اي تعريف لهذا النمط من الأدلة متسما ب مما يسمح باستعادة مع سائر الجرائم المرتكبةبالتقنية ام مبتكره التعامل مع المعلومات، وعليه فقد تطرقنا لتعريف الدليل في الفرع الأولو ثم الأنواع في الفرع الثاني، يليه المميزات في الفرع الثالث،

الفرع الأول: تعريف الدليل الإلكتروني

عرفته المنظمة العالميةلدليل الكمبيوتر IOCE في اكتوبر 2001 بانه المعلومات ذات القيمةالمحتملةوالمخزنةأو المنقولة في صورة رقمية وكان قد عرفته في مارس 2000 بانه المعلومات المخزنة او المنقولة في شكل ثنائيوالتي يمكن الاعتماد عليها امام المحكمة.[1]

كان يعرف الدليل الالكتروني بانه الدليل المأخوذ من اجهزه الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية او كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور او الاصوات والاشكال والرسوم وذلك من اجل الربط بين

1- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص213.

الجريمة والمجرم المجني عليهوبشكل قانوني يمكن الأخذ به امام اجهزه انقاذ وتطبيق القانون.[1]

كما عرف بانه الدليل الذي يجد له اساس في العالم الافتراضي ويقود للجريمة فهو ذلك الجزء المؤسس على الاستعانة بتقنيةالمعالجةالتقنية للمعلومات والذي يؤدي الى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة باستعماله تكنولوجيات الاعلام والاتصال.[2]

كما عرفه البعض الاخر بانه الدليل المأخوذ من اجهزه الحاسب الالي ويكون في شكل مجالات مغناطيسيه او كهربائية ممكن تجميعها وتحليلها باستخدام برنامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده امام القضاء في حين عرفه الاخر بانه دليل الذي يوجد له اساس في العالم الافتراضي ويقود الى الجريمة

فقد عرفه البعض بأنه " ذلك الدليل المأخوذ من اجهزة الحاسب الآلي ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية او كهربائية يمكن جمعها أو تحليلها باستخدامبرامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل علمي يمكن اعتماده امام القضاء الجنائي".[3]

يؤخذ من هذه التعريفات انه يتم حصرهاالأدلةالإلكترونيةفي تلك التي تستخرج من اجهزة الاعلام الآلي وملحقاتها دون سواها من الوسائل التقنيةالإلكترونية الاخرى التي تعتمد المعالجة الالية للمعلومات كالهواتف النقالة والبطاقات الذكية والتي يمكن ان تكون مصدرا مهما للأدلةالإلكترونية.

كذلك عرفه أنه "مكون رقمي لتقديم معلومات في لأشكال متنوعة، كالنصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، للربط بين الجريمة والمجرم والمجني عليه، بشكل قانوني يمكن الأخذ به أمام أجهزة إنقاذ تطبيق القانون".[4]

فمن جهة نجد أن التعريفات قد حصرت الأدلة الإلكترونية في أجهزة الحاسب الآلي وملحقاته، إلا أنه نجد أن هناك نظم أخرى مدمجة بالحواسب كالهواتف المحمولة والبطاقات الذكية والمساعد الرقمي الشخصي.[5]

الفرعالثاني: مميزات الدليل الرقمي

1- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دون طبعة، دار الكتب القانونية، مصر، 2006، ص88.

2- أحمد مسعود مريم، آليات مكافحة تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير، جامعة قاصدي مرباح، ورقلة، كلية الحقوق، تخصص قانون جنائي،2013/2012، ص69.

3- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص88.

4- عبد الناصر محمد محمود فرقي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، جامعة نايف للعلوم الأمنية، الرياض، س2007، ص130.

5- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، س2010، ص55.

الدليل الرقمي يستثني بخصائص تصنفه عن غيره من الأدلة فالتطورالمستمر لهذا الدليل جعل الفقه الجنائي يحدد سمات وخصائص التي ويتميز بها الدليل الالكتروني من غير من الأدلةالتقليدية وهي كالتالي:

أ- الدليل الرقمي دليل علمي: يتصف الدليل الالكتروني بانه علمي لأنه مشكل من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي،وان ما يسرى على الدليل العلمي يسري على الدليل الالكتروني[1].

ب-الدليل الرقمي من طبيعةتقنية: إن الطبيعة التقنية للدليلتقضيانيكونهناكتوافقبينالدليلالمرصودوبينالبيئةالتييعيشفيهافلاتنتجالتقنيةسكيناليتمبهاكتشافالقاتل، أو اعترافامكتوباوموالافيجريمة الروشة،أوبصمةأصبعوانما ماتنتجهاالتقنيةهونبضاترقميةتشكلقيمتهافيامكانيةتعاملهامعالقطعالصلبةالتيتشكلالحاسوبعلىأيةشاكلةيكونعليها،ومثلهذاالامريجعلنانقررانهلاوجودللدليلالرقميخارج بيئةالتقنيةوأنهلكيتكونهناكدليلرقمييجبانيكونمستوحىاومستنبطامنالبيئةالرقميةاوالتقنية[2]، وهي في إطار الجرائم المعلوماتية ممثلة في العالم الافتراضي هو العالم الكامن في اجهزة الحاسب والخوادم والمضيفات وشبكات التي يتم تداول الحركة فيه عبرها. فالأدلة الجنائية الإلكترونية هي أدلة علمية تستمد مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية بواسطة أجهزة وبرامج تقنية، فالدليل الإلكتروني يعد من طائفة ما يعرف بالأدلة المستمدة من الآلة.[3]

ت-صعوبة التخلص من الدليل الالكتروني: تعد هذه الخاصية أهم ميزة يتمتع بها الدليل الإلكتروني من غيره من الأدلةالمادية، واذا كان من السهل جدا التخلص من الأدلةالمادية نهائيا دون امكانية استعادتها كالوثائق والأشرطة بتمزيقها او حرقها او بصمات الاصابع بمسحها من موضعها كما يمكنالتخلص من الشهود بقتلهم او تهديدهم بعدم الادلاء بالشهادة، فأما بالنسبة للأدلة الرقمية فالحال دون ذلك[4]، بحيث يمكن استرجاعها بعد محوها واصلاحها بعد اتلافها واظهارها بعد اخفائها وذلك بتوافرأدوات البرمجيات ذات الطبيعةالرقميةأنشأت لإسترداد البيانات أو الملفات التي تم حذفها أو إلغاؤها.

كما يعتبر نشاط الجاني في محو الدليل دليلا ضده، فبمحاولته إخفاء هذا الدليل يمكن استخلاصها كدليل إدانة ضده[5].

1-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، ص977.

2-سعيداني نعيم، المرجع السابق، ص127.

3- طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، بحث مقدم للمؤتمر المغاربي الأول حول المعلوماتية، المنعقد في 2009/10/28، الأكاديمية للدراسات العليا، طرابلس.

4-عمر محمد أبو بكر بن يونس، المرجع السابق، ص982.

5- فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملاتالتجارية والمدنية، ط1، دار الفكر والقانون، مصر، س2010، ص655.

ث-الدليل الرقمي متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية إلبا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات والملقمات والخوادم، وقد يكون بيانات مفهومة كما لوكان وثيقة معدة بنظام المعالجة الآلية[1] .

ج- الدليل الرقمي يمتاز بطبيعة ديناميكية فائقة السرعة، تنتقل عبر شبكات الإتصال من مكان لآخر متعدية لحدود ازمان والمكان[2].فاتساع مجال الدليل الإلكتروني يسهل من تبادل المعرفة بسرعة عالية النسبة في جل أنحاء العالم مما يساعد على الإستدلال على الجناة في وقت قصير.

د- الدليل الرقمي قابل للنسخ: إذ أنه يمكن إستخراج نسخ مطابقة للأصل ذات قيمة علمية، بحيث أن هذه الخاصية لا تتوافر في الأدلة الجنائية التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف، والتغيير، عن طريق نسخ طبق الأصل من الدليل[3].

الفرع الثالث: أنواع الدليل الرقميوأشكاله

وللدليل أنواع وأشكال تميزه عن باقي الأدلة وسندرجها في كالآتي:

أولا: أنواع الدليل الرقمي

تختلف الجريمةالمعلوماتية عن الجريمةالتقليدية الاولى تتم في بيئة غير ماديه عبر نظام حساب الي او شبكه معلوماتية دوليةنتيجة بحيث يمكن العبث في بيانات الحاسب او برامجها ويمكن محور في زمن قياسي اغاني وديع مراد بما يصعب الحصول على دليل مادي في مثل هذه الجرائم فنلاحظ ان هناك تقسيم أخذت به وزاره العدل الأمريكية سنه 2002 بحيث يمكن تقسيم الدليل الإلكتروني إلى ما يلي:

1. السجلات المحفوظة في الحاسوب: وهي الوثائق المكتوبةوالمحفوظة مثل رسائل البريد الالكتروني الذي يعتبر صندوق تتواجد به كل رسائل صاحب البريد التي سبق له إرسالها، والملغاة وغيرها والتي يحتوي عليها البريد الإلكتروني[4]، وهناك أيضا ملفات برنامج معالجه الكلمات ورسائل غرفالمحادثة على الانترنت كالدردشات،

1- سعيداني نعيم، المرجع السابق، ص128.
2- عبد الناصر محمد محمود فرقي، محمد عبيد سيف المسماري، المرجع السابق، ص15.
3- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط1، آسيوط مصر،1999، ص36.
4- مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر والتوزيع، الجزائر، ص59.

2. السجلات التي تم انشائها بواسطة الحاسوب: وتعتبر مخرجات برامج الحاسوب أي أن الحاسوب هو الذي يصدرها، وبالتالي لم يتم لمسها من قبل أشخاصمثل سجلات الهاتف وفواتير اجهزه السحب الالي(ATM)
3. السجلات التي جزء منها تم حفظه بالإدخال وجزء اخر تم انشاءه بواسطةالحاسوب، كأوراق العمل المالية التي تحتوي على مدخلات ثم تقييمها لبرامج عمل مثل:EXCELومن ثم تمت معالجته من خلال برامج بإجراءالعمليات الحسابية عليها[1].

كذلك صنفت الأدلة الإلكترونية إلى أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون وسيلة إثبات وهي كالتالي:

أ- الأدلة التيأعدتلتكون وسيلةإثبات

- السجلات التي تم انشاؤها بواسطة حاسوب تلقائيا وتعتبر هذهالسجلات من مخرجات الحاسوب التي لم يساهم الافراد في انشائها مثل سجلات الهاتف وفواتير البطاقات البنكية[2].
- السجلات التي جزء منها تم حفظهبالإدخالوجزئها الآخر تم انشاءه بواسطة الجهاز مثل البيانات التي يتم إدخالها إلى جهاز الحاسب وتتم معالجتها من خلال برنامج خاص.[3]

ب- الأدلة التي لم تعد لتكون وسيلة إثبات

هذا النوع من الأدلة نشأ دون إرادة الشخص بمعنى أنها أي أثر يتركه الجاني دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الادلة بالبصمة الرقمية أو الاثار المعلوماتيةالرقمية وهي تتجسس في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الإتصالات التي تمت من خلال النظام المعلوماتي وشبكة الإتصالات.

وتبدو اهمية التمييز بين هذين نوعين من الأدلةالإلكترونية فيكون أن النوع الاول قد اعدليكون كوسيلة إثبات بعض الوقائع التي يتضمنها،لذلك فإن عادة ما يعتمد إلى حفظه للإحتجاج به لاحقا وهو ما يقلل إمكانيه فقدانه وسهل الحصول عليه، بينما النوع الثاني من الأدلة الرقمية فلكونه لم يعد ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تفيد في الكشف عن الجريمة و مرتكبها ويكون الحصول عليه باتباع تقنيات خاصه لا تخلو من الصعوبة والتعقيد، وهو على العكس من نوع الاول لم يعد ليحفظ مما يجعلهعرضة للفقدان بسهولة.[4]

1- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق، ص14.
2- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011، ص234.
3- أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015، ص21.
4- سعيداني نعيم، المرجع السابق، ص 134/133.

ومنه فالتنوع في الدليل الإلكتروني مفاده أنه لا توجد وسيلة واحدة للحصول عليه، وإنما هي متعددة وفي جميع الحالات يبقى الدليل إلكترونيا حتي وإن إتخذ هيئة أخرى، وعليه فإن إعتراف القانون لهذا النوع من الأدلة يكون مؤسسا على الطابع الافتراضي الذي يبني أساسه على الدليل الإلكتروني، فإنه لا بد من إتخاذ مسلك الإفتراض بإعتبار هذا الدليل دليلا أصليا، نتيجة لنقص توافر الإمكانيات الإلكترونية في المحاكم الجنائية التي تنظر في هذا النوع من الأدلة[1].

ثانيا: أشكال الدليل الرقمي

أ- أدلة إلكترونية مرئية: (الصورة الرقمية) وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تكون الصورة إما في شكل ورقي أو في شكل مرئي بإستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة وأكثر تطورا للصورة التقليدية.[2]

ب- أدلة إلكترونية صوتية: وتشمل جميع التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الأنترنت[3].

ت- أدلة إلكترونية مكتوبة: وتشمل كل المخطوطات والنصوص التي يتم كتابتها من طرف المستخدم بواسطة الأجهزة الإلكترونية الرقمية كالمراسلات عبر البريد الإلكتروني أو الهاتف النقال، والتي تم إدخالها عن معالجة البيانات في وحدة المعالجة المركزية أو مختلف ملفات برامج معالجة الكلمات، ومثل هذا النوع من الادلة يمكن أن نجدها في مختلف وسائل التخزين الإلكتروني كالأقراص الممغنطة الصلبة والمرنة والأشرطة المغناطيسية.[4]

المطلب الثاني: القيمة القانونية للدليل الرقمي في الجرائم المعلوماتية

وترتكز عملية الاثبات الجنائي للجرائم المعلوماتية على الدليل الالكتروني بإعتباره الوسيلة الأساسية لإثبات مثل هذا النوع من الجرائم. وعليه فهو يمتاز بقيمة قانونية بحتة في مجال الإثبات الجنائي، ففي سبيل الحصول على هذا الدليل أقر المشرع مشروعية الحصول عليه وهذا ما درسناه في الفرع الأول بالإضافة إلى حجيته في الإثبات وهذا ما تناولناه في الفرع الثاني.

الفرع الأول: مشروعية الدليل الرقمي

يعد الدليل من الأدلة التي اقرها المشرع وعليه فقد تطرقنا لمشروعيته في الوجود ومشروعيته في التحصل عليه.

أولا: المقصود بمشروعية وجود الدليل الرقمي

1- عائشة بن قارة مصطفى، المرجع السابق، ص77.
2- ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية عبر جرائم الكمبيوتر، مركز شرطة دبي، 2005، ص9.
3- سعيداني نعيم، المرجع السابق، 132.
4- براهمي جمال، ص128.

يقصدبمشروعيةالوجودأنيكونالدليلالجنائيالرقميمعترفابه،بمعنىأنالقانونيجيزللقاضيالا ستنادإليهلتكوينعقيدتهللحكمبالإدانة[1]،ويتحددموقفالقوانينمنمشروعيةوجودالدليلالجنائيالرقميب حسبطبيعةنظامالإثباتالسائدفيالدولة.

ومنه فتتجلي أنظمة الإثبات في الدليل الرقمي فيما يلي:

أ - نظام الإثبات المقيد: وفيه يقوم المشرع بتحديد أدلة الإثبات حصرا وكذا القوة الإثباتية لكل دليل من الأدلة بناءا على قناعة المشرع بها. وهو ما يعترف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، فتحدد للقاضي الأدلة التي يجوز له قبولها واللجوء إليها في الإثبات ولا سبيل للاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات[2].

فدور القاضي يقتصر على مراعات تطبيق القانون من حيث توافر الدليل، فإذا لم يتوفر الدليل فإنه لا يجوز له الحكم بالإدانة المقررة حتى ولو لديه إقتناع شخصي بأن المتهم المتمثل أمامه هو الشخص الذي ارتكب الجريمة[3].

ومن المسائل التي إنتقدت في هذا النظام، قيامه بتقنين نصوص قانونية سلفا رغم أن اليقين مسألة يطرحها الواقع ترتبط بالظروف الخاصة والمتغيرة لكل قضية وتترك لقاضي الموضوع[4].

ومنه يمكن القول أن غالبية التشريعات في ظل نظام الإثبات أخذت بهذا النظام، نظرا لقوته الثبوتية في الدليل الجنائي

ب - نظام الإثبات الحر: وهو نظام يسود فيه مبدأ حرية الإثبات، إذ لا يحدد فيه المشرع طرقا معينة للإثبات ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجزائي اذي يكون له دور إيجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب اقتناعه بها[5].

وعلية فإن نظام الإثبات الحر يكرس مبدأ حرية القاضي في الإقتناع، بمعني أن القاضي حر في تكوين عقيدته من أي دليل يراه يقينا ويقتنع به[6].

ويجدهذاالنظاممبرراتهفيكونالإثباتفيالمسائلالجزائيةلاينصبالإعلى

وقائعماديةأونفسيةخاصةبالجريمةولاينصبعلىتصرفاتقانونيةيتفقمعهاقيام

1- خالد عياد الحلبي، المرجع السابق، ص235/236.
2- سعيداني نعيم، المرجع السابق، ص208.
3- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، س 1999، ص34/35.
4- هلالي عبد أللاه أحمد، النظرية العامة للإثبات، دار النهضة العربية للنشر، القاهرة، ص95/96.
5- عفيفي كامل عفيفي، جرائمالكمبيوتروحقوقالمؤلفوالمصنفاتالفنيةودورالشرطةوالقانون،دراسةمقارنة،منشوراتالحلبي،دمشق، 2007 مرجع سابق، ص379.
6- محمد مرواني، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول،ديوان المطبوعات الجامعية للنشر، الجزائر، س1999.

المشرعسلفابتحديدوسائلإثباتهاومددالحجيةالتيتتمتعبهاكلمنها،كماأنالإثبات

ينصرفإلىوقائعإجراميةغالباماتعمدالجناةبقدرالمستطاعإلى إزالةومحوآثارها،

الأمرالذييحتمتحويلالقضاءكافةالوسائلالمتاحةوالممكنةلكشفالجريمةوتقصي الحقيقة.[1]

أمابالنسبةللنظمالقانونيةالتيتعتمدنظاماالإثباتالحركماهوالحالعليهفيالق
الجالمادة212منقانونالإج الج والقانون الفرنسي المادة427قانون الإج الج الفرنسي
فإنهلاتثورمشكلةمشروعيةالدليلالرقميمنحيثالوجود،على
اعتبارأنالمشرعلايعتمدسياسةالنصعلىقائمةلأدلةالإثباتفالأساسهوحريةالأدلة،لذلك
فمسألةقبولالدليلالرقميلاينالمنهاسوىمدىإقتناعالقاضيبهإذاكانهذاالنوعمن
الأدلةيمكنإخضاعهلتقديرالقاضيوهوماسوفنتناولهلاحقاعندالحديثعلىحجيةالدليلالرقمي.[2]

وفيهذاالصددفإنالمشرعالجزائريوكغيرهمنالتشريعاتالمنتميةإلىالنظامالإثباتالحرلانجدهق
دأفردنصوصاخاصةتحظرعلىالقاضيمقدماقبولأوعدمقبولأيدليلبمافيذلك
الدليلالرقمي،وهوأمرمنطقيطالماأنالمشرعالجزائرييستندلمبدأحريةالإثباتحيثلم يتضمن
قانون 04/09 المتضمنالقواعدالخاصةبالوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلام
والاتصالومكافحتهاأيةأوضاعخاصةوتركالأمرللقواعدالعامة،ومنهاأنالأصلفيالأدلة
مشروعيةوجودهاومنثمفإنالدليلالرقميسيكونمشروعامنحيثالوجودإصطحابا
للأصل،ومنجهةأخرىفإنهوطبقالمبدأالشرعيةالإجرائية فلايكونالدليلمقبولافيعملية
الإثباتإلاإذاكانمشروعاذلكأنالقاضيلايقدرإلاالدليلالمقبولولايكونكذلكإلاإذا
كانمشروعاباأنتمالبحثعنهوالحصولعليهوفقالطرقمشروعة.[3]

ثانيا: مشروعية الحصول على الدليل الرقمي

يقصدبمشروعيةالتحصيل،أنتتمعمليةالبحثعندليلالإدانةوتقديمهللقضاءمنطرفالقائمينبالتـ
حقيقوفقاللقواعدوالإجراءاتالتيرسمهاالقانونلذلك،فمشروعية
الدليلإذاتتطلبصدقهفيمضمونه،وأنيكونهذاالمضمونقدتمالحصولعليهبطرق
مشروعةتدلّعلىالأمانةوالنزاهة، فمتىكانالأمركذلك كانتالمشروعيةحدافاصلا
بينحقالدولةفيتوقيعالعقابلضمانأمنواستقرارالمجتمعوبينحقالأفرادفيضمان
حقوقهموحرياتالأساسية.[4]

إنهمنالمقررأنالإدانةفيأي
جريمةلابدوأنتكونمبنيةعلىأدلةمشروعةتمالحصولعليهاوفققواعدالأخلاقوالنزاهة

1- عفيفي كامل عفيفي، المرجع السابق، ص380/379
2- سعيداني نعيم، المرجع السابق، ص 210/209.
3- سعيداني نعيم، المرجع السابق، ص 210.
4- براهمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الدكتوراه، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، س2018، ص 145/144.

واحترامالقانونمنطرفالجهةالمختصةبجمعالدليلالجزائيبمايتضمنهمنأدلةمستخرجةمن وسائلإلكترونية،ولايكونمشروعاإلاإذاأجربالتنقيبعنهأوالحصولعليهأوكانتعملية تقديمهإلىالقضاءأوإقامتهأمامهبالطرقالتيرسمهاالقانون،فمتىماتمالحصولعلىالدليل خارجهذهالقواعدالقانونيةفلايعتدبقيمتهمهماكانتدلالتهالحقيقيةوذلكلعدممشروعيته، وعلىهذاالأساسفإنإجراءاتجمعالأدلةالرقميةالمتحصلةمنالوسائلالإلكترونيةإذاخالفت القواعدالإجرائيةالتيتنظمكيفيةالحصولعليهافإنهاتكونباطلة،وبالتاليبطلانالدليلالمستمدمنهاولا تصلحلأنتكونأدلةتبنىعليهاالإدانةفيالموادالجنائية.[1]

فدائماماتقترنالحديثعنمشروعيةالحصولعلىالأدلةالجنائيةبوجوبحماية

واحترامحقوقالإنسان،علىاعتبارأنجميعالإجراءاتالقانونيةالتيتستهدفالحصولعلىالأدلةالـ جنائيةتمسبحقوقالأفرادوحرياتهم،ومنبينهذهالحقوقالحقفي الخصوصية،لذافإناتخاذإجراءالمراقبةالالكترونيةأواعتراضالمراسلاتيمثلدونأدنىشكلاعتداءع لىالحياةالخاصة،هذاالذيجعلهاموضوعاهتمامكبيرمنقبلالإعلاناتوالمواثيقالدولية.[2]

فمشروعيةالدليلبصفةعامةشرطاساسيللوصولالىاليقينالقضائيعندالادانة،ولا يحولدونذلكانتكونأدلةالادانةواضحةوصارخةمادامتهذهالأدلةمشبوهةولايتسممصدرهابالنزا هةواحترامالقانون،ومعيارمشروعيةالادلةيكمنفياحترامضماناتالحرية الشخصيةالتينصعليهاالقانونلاحترامحريةالفردبوصفهبريئا إلىانتثبتادانتهبحكم بات.[3]

الفرع الثاني: حجية الدليل الرقمي في مجال الإثبات

يقصدبحجيةالدليلالالكترونيمايتمتعبهمنالقوةالاستدلاليةفيكشفالحقيقة

وصدقنسبةالفعلالإجراميإلىشخصمعينأوكذبه.[4]ولايشترطأنيكونالدليلالذييستندإليهالقا ضيصريحادالاعلىالواقعةالمرادإثباتهابل يكفيأنيكونإستخلاصهاإستنتاجامنالظروفوالقرائنوترتيبالنتائجعلىالمقدماتوأدلة الدعوىتخضعفيكلالأحوالللتقديرالقاضيمادامهذاالدليلغيرمقطوعبصحته[5]. ومقابلذلكلاينبغيأنيفهممنحريةالقاضيفيالاقتناعالتحكمالمطلقفيالأمورالقضاءكيفماشاءوفقالأ هوائهومزاجهالشخصي،إنماهومطالبةبتحريالمنطقالدقيقفيتفكيرهالذيقادهإلىاقتناعهواستلهامعق يدته،وألايكونتفكيرههذاقدجافىالأصولالمسلم بهافيالاستدلالالقضائي.[6]

ولاشكأنتطبيقذلكعلىالدليلالالكترونيقديثيرعدةصعوبات،فالقاضي

1- سعيداني نعيم، المرجع السابق، ص210.
2- خالد عياد الحلبي، المرجع السابق، ص238.
3- أحمد فتحي سرور، الوسيط في قانون الإج ج، دار النهضة العربية، القاهرة 1985، ص292.
4- ياسرمحمدالكومىمحمودأبوحطب،الحمايةالجنائيةوالأمنيةللتوقيعالإلكتروني،منشاة المعارف، الإسكندرية، س2014، ص303.
5- سعيداني نعيم، المرجع السابق، ص213.
6- جميلعبدالباقيالصغير،أدلةالإثباتالجنائيوالتكنولوجيةالحديثة،دار النهضةالعربية،القاهرة، ص2002 ، ص13.

الجزائيبثقافتهالقانونيةوعدمكفاءتهالفنيةفيمجالالمعلوماتيةلايمكنهإدراكالحقائقالمتعلقةبأصالةالدليلالالكتروني،فضلاعنتمتعهذاالدليلفيقوتهالتدليليةبقيمةاثباتيةقدتصلإلىحداليقينشأنهفيذلكشأنالأدلةالعلميةعموما،ناهيكعنالطبيعةالفنيةالخاصةبالدليلالالكترونيوالتيتمكنمنالعبثبمضمونهبسهولةعلىنحويحرف الحقيقةدونأنيكونبمقدورغيرالمتخصصإدراكذلك.[1]

ولذلك فإنناسوف نعرضماهيالشروطالتييجبأنيتوافرعليها الدليلالرقمي لكونهيعبر عن حقائق علمية بحتة، ثمنبيندورذلكفي تكوينالاقتناعالشخصيللقاضيالجزائي.

أولا: شروط إكتساب الدليل الرقمي

إنمبدأالقناعةالوجدانيةيخولالقاضيالجزائيحريةكاملةوسلطةواسعةفي تقدير الأدلةالتيتطرحأمامهفيالدعوى،بمافيهاالأدلةالرقمية،واستخلاص اقتناعهمنهذاالدليلأوذاك،وبأيةوسيلةيراهاموصلةإلىالحقيقة،شرطأن يصدرالقاضيحكمهعناقتناع يقينيبالأدلة،وبخاصةالأدلةالمتحصلةمن الحاسبالآليومخرجاتهالإلكترونية،فسلطةالقاضيالجزائيفيتقدير الأدلةمقيدة بضرورةأنيؤسسقناعتهعلىأدلةقاطعةوحاسمة؛لأنالأحكامالجزائيةلاتبنى علىالشكأوالتخمينبلعلىالجزمواليقين، والوصولإلىيقينيةالدليلالرقمي يتمعنطريقمايستنتجهالقاضيبمختلفوسائلإدراكهمنخلالمعاينتهلهذا الدليل،ومايطبعهذاهنمنتصوراتذاتدرجةثقةعاليةمنالتوكيدعنطريق التحليلوالاستنتاجوالربطبينالوقائع.[2]

ولذلك فإن مصداقيةالدليلالالكترونيمرتبطاأساسابعناصر مستقلة، بحيث أنه يتطلب شروط في الدليل الرقمي وهذا من أجل تحقق المصداقية في الدليل وصولا للحقيقة سواءا بالبراءة أو الإدانة.

أ- وجوب يقينية الأدلة الرقمية:

يشترطفيالأدلةالإلكترونيةأنتكونغيرقابلةللظنأوالترجيححتييشيدعليها الحكمبالإدانة،لأنهلامجاللدحضقرينةالبراءةأوافتراضعكسهاإلاعندبلوغاقتناعالقاضيحدالجزم واليقين[3]. ويمكنالتوصلإلىذلكمنخلالمايعرضمنالأدلةالرقميةعلىإختلافأشكالها التيتتوافرعنطريقالوصولالمباشرإليهاأوبمجردعرضهاكمخرجاتعلىشاشةالحاسوب، ويستطيعالقاضيمنخلالمايعرضعليهمنمخرجاتإلكترونيةرقميةومايطبعهذهمتهمن تصوراتواحتمالاتبالنسبةلهاأنيحددقوتهاالاستدلاليةعلىصدقنسبةالجريمةالمعلوماتيةإلى شخصمعينمنعدمه،وكذاالوصولإلىيقينيةهذهالمخرجاتعنطريقالمعرفةالحسيةالتي

1- أحمد يوسف الطحطاوي، المرجع السابق، ص233.

2- طارقأحمدماهرزغلول،شرحقانونالإج الجعماني،الجزءالثاني، المحاكمةوطرقالطعنفي الأحكام، ط 1،دارالكتابالجامعي، س 2016، ص222.

3- علي حسين محمد الطوالبة، ص190،مشروعيةالدليلالرقميالمستمدمنالتفتيش الجنائي، س2009 ، بحثمنشورعلىموقعالانترنتالتالي :

www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc

تدركها الحواس منخلال معاينتها لهذه المخرجات وفحصها، وكذا عن طريق المعرفة العقلية من خلال ما يقوم به من إستقراء وإستنتاج ليصل إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه إستنادا إليها[1].

نظر اللطبيعة التقنية التي يتميز بها الدليل الجنائي تم وضع قواعد محددة من طرف

مختصين تحكم يقينيتها، وذلك بواسطة استعمال وسائل فنية من طبيعة هذا الدليل تمكن من فحصها والتأكد من سلامتها وصحة الإجراءات المتبعة في الحصول عليه[2].

1. **تقييم الدليل الجنائي الرقمي من حيث سلامته من العبث**: إن الطبيعة التقنية للدليل الالكتروني تجعله في الغالب عرضة للشكوك الظنون في سلامته، وذلك راجع إلى إمكانية تعرضه للعبث والخروج به عن الحقيقة، فقد يقدم هذا الدليل ليعبر عن واقعة معينة صنع خصيصا من أجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث، على نحو يمكن القول معه أن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة التقنية التي تقدم للقضاء، فالتقنية الحديثة تمكّن من العبث بالدليل الالكتروني بالتقنية ذاتها بسهولة ويسر ليظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.[3]

ويمكن التأكد من سلامة الدليل الرقمي من نوع العبث به بعدة طرق من حيث:

- تقنية التحليل التناظري الرقمي: وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم يتم التأكد من مدى حصول العبث في النسخة المستخرجة أملا[4]، ويستعان في ذلك باستخدام علم الكومبيوتر الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون كينونة الدليل الرقمي، وهذا العلم يستعان به أيضا في كشف مدى التلاعب بمضمون هذا الدليل.
- إستخدام عمليات حسابية خاصة تسمى الخوارزميات ويلجؤ إليه هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي، أو في حالة أن العبث قد وقع على النسخة الأصلية إذ بالأمكان التأكد من سلامة الدليل الرقمي من التبديل والتحريف والتغيير بإستعمال هذه العمليات الحسابية.[5]
- إستعمال الدليل لا محاي دو هو نوع من الأدلة الرقمية المخزونة في البيئة الإفتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود في عدم وقوعه عديل أو تغيير في نظام الحاسوب.[6]

1- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص91 .

2- خالد عياد الحلبي، المرجع السابق، ص249.

3 - Ammar.(D) « preuve et vraisemblance، contribution a l'étude de la preuvetechnologique » RTD Civ، juillet-septembre، 1993، p 499.

4- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، مرجع سابق، ص27

5- سعيداني نعيم، المرجع السابق، ص217.

6- ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد بدبي في الفترة من 12/10 ماي 2003، ص2246/2247.

2. **تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه:**
إذا كانت نسبة الخطأ الفني في الحصول على الدليل الالكتروني ضئيلة جدا باعتباره تطبيقا من تطبيقات الدليل العلمي الدقيقة كما أسلفنا الذكر، فذلك لا يعني أنها منعدمة تماما، إنما يظل الوقوع في الخطأ ممكنا أثناء استخلاصه.[1]

ومن أجل تفادي مثل هذه الأخطاء يمكن تبني بعض الخطوات والتطبيقات للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الالكتروني أهمها:

-
إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج: ويكون ذلك بإتباع إختبارين أساسيين تتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي وفي ذات الوقت لم تضف إليها أي بيانات جديد، وهو ما قد يعطي للنتائج المقدمة مصداقية في التدليل على الواقع[2]. بحيث أن هذان الإختبارات يتجسدان فيما يلي:

أ- إختبار السلبيات الزائفة: وفيه يتم إخضاع الأداة المستخدمة في الحصول على الدليل للاختبار بينما مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الالكتروني دون إغفال أية بيانات مهمة عنه.

ب- إختبار الإيجابيات الزائفة: ومفاده إخضاع الأداة المستخدمة في الحصول على الدليل الالكتروني لاختبار فني يمكننا من التأكد من أنها لا تعرض بيانات إضافية جديدة[3].

- الإستعانة بأدوات ذات جودة عالية:
هناك دراسات وبحوث علمية متخصصة في مجال التقنية المعلوماتية حددت الأدوات السليمة التي يجب إتباعها في سبيل الحصول على الدليل الالكتروني، وفي المقابل بينت كذلك الأدوات المشكوك في كفاءتها وحثت على اجتنابها، وعليه فاختيار أية أداة من هذه الأدوات من شأنها أن يؤثر على مصداقية المخرجات المستمدة منها.[4]

وعليه يمكننا القول بأنه إذا سلمنا سابقا بإمكانية التشكيك في سلامة الدليل الالكتروني بسبب قابليته للعبث نسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع فيها برأي حاسم إنما يقطع بها أهل الاختصاص، لذلك فإذا توافرت في الدليل الالكتروني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية.[5]

فمما سبق نستطيع القول إن القاضي الجزائي إذا قرر سلامة الدليل الرقمي، وان استخلاصه كان منسجما مع المنطق والواقعة وملابساتها، فإنه يستطيع بناء قناعته على هذا الدليل، شرط أن تتوفر فيه الضمانات السابق ذكرها، والتي جسدها القانون لكي يكون الاقتناع القضائي صائباً.

---

1 - Ammar (D)، op.cit.، p 500.

2- سعيداني نعيم، المرجع السابق، ص218.

3 - بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن، مرجع سابق، ص501،

4- طارق محمد الجملي، المرجع السابق، ص28.

5- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص182.

ب- وجوب مناقشة الأدلة الرقمية:

إنتحققشرطسلامةالدليلالالكترونيمنالعبثوسلامتهمنالخطأفيإجراءات التحصيلوحدهلايكفيلاكتسابهحجيةدامغةفيالإثبات،بللابدأيضامنمناقشةهذا الدليلبصفةعلانيةفيجلسةالمحاكمةوفقالمبدأأساسيفيالإجراءاتالجزائيةهومبدأ الشفويةوالمواجهة.[1]

إنحريةالدليلالجنائي مشروطةبأنيكونالدليلالذييستندإليهالقاضيقدطرحتمناقشتهبالجلسة،ويكونكذلك متكاملهأصلثابتفيأوراقالقضيةالمطروحةعلىالقاضي، وهومايجعلهذه الأدلةمتاحة للخصوملكييتمكنكلخصممنإعدادددفاعهفإنكانالدليلفيصالحهيدافعنه وإنكان ضدهيشكفيهويضعفه،ولايمكنللقاضيحينئذأنيؤسساقتناعهإلاعلىالعناصرالإثباتيةالتي طرحتفيجلساتالمحكمة وخضعتلحريةمناقشةأطرافالدعوى[2].كمالايجوزللقاضيالجزائيأنيبنياقتناعهعلى رأيالغير،إلاإذاكانمنالخبراء والفنييناللذيناستشارهموفقاللقانون وارتاحضميرهلرأيهم فقررالاستنادإليهضمنباقيالأدلةالقائمةفيأوراقالدعوىالمعروضةعليه.[3]

ويترتبعلىذلكعدمجوازاقتناعالقاضيمنمعلوماتشخصيةحصلعليهاخارج الجلسةأوفيغيرنطاقالمرافعاتوالمناقشاتالتيجرتفيها،وإلايكونبذلكقدجمع فيشخصهصفتينمتعارضتينهماصفةالشاهدوصفةالقاضي،ممايبعثالحرجفي نفسيةالخصومويعيقهمعنمناقشةشهادتهوالردعليهابحرية،لاناعتمادهعلىعلمه الشخصييجعلهعرضةللتهموالشبهاتوهوالأمرالذييجبأنيتنزهالقضاءعنه عموما.[4]

كمالايجوزللقاضيالجزائيأنيبنياقتناعهعلى رأيالغير،إلاإذاكانمنالخبراءوالفنييناللذيناستشارهموفقاللقانونوارتاحضميرهلرأيهمفقررالاستناد إليهضمنباقي الأدلةالقائمةفيأوراقالدعوىالمعروضةعليه.[5]

انقاعدةوجوبمناقشةالدليلالجزائيسواءكاندليلاتقليديااممكانناتجاعنالحاسبالآليتعتبرضمانا تمهمةواكيدةللعدالةحتىلايحكمالقاضيالجزائيفيالجرائمالمعلوماتيةبمعلوماتهالشخصيةاوبناءا على رأيالغير.[6]

وعلى هديماسبقفإنهناكمنيذهبإلىالإعتقادبأنهبمقدارإتساعمساحةالأدلةالعلميةبمقدارمايكونإنكماشوت ضاؤلدورالقاضيالجزائيفيالتقدير،خاصةأمامغياب

1- سليمان أحمد فضل، ص37.
2- سعيداني نعيم، المرجع السابق، ص219.
3- علي محمود علي حمودة، الأدلةالمحصلةمنالوسائلالإلكترونية فيإطار نظريةالإثباتلجنائي، بحثمقدمإلىالمؤتمرالعلميالاولحول الجوانبالقانونيةوالأمنيةللعملياتالإلكترونية،دبي،الإمارات العربيةالمتحدة،س2003، ص120.
4 -براهمي جمال، المرجع السابق، ص158.
5- عليمحمودعليحمودة،مرجعسابق،ص120.
6- راشدبنحمدالبلوشي، ورقةعملحولالدليلفيالجريمةالمعلوماتية،مقدمةالىالمؤتمر الدوليحول (حمايةالمعلوماتوالخصوصيةفيقانونالانترنت) برعايةالجمعيةالدولية لمكافحةالاجرامبفرنسا، س2008، ص20.

الثقافةالمعلوماتيةللقاضيوقديستتبعذلكبالقولأنالتطور العلميمنشأنهأنيطغىعلىنظام الإقتناعالقضائيولايبقىللقاضيسوىالإذعانلرأيالخبراء المختصينوناًيتقديرمنجانبه فمثلهذاالأمريدفعنإلىالبحثمدىتأثير القيمةالعلميةللدليلالرقميعلىمبدأإقتناعالقاضي الجزائي.[1]

ثانيا: أثر القيمة العلمية للدليل في تكوين قناعة القاضي الجزائي

إن حرية القاضي الجنائي بصفة عامة هي مايتمتع به القاضي الجنائي من إختيار النشاط الذهني الذي يسلكه بغية الوصول إلى حل ما يطرح عليه من قضايا.[2]

وعلىذلكفانهيكوننللقاضيالحريةفيتقديركافةالادلةالمطروحةعليهفيالدعوىوله من هذا التقديران يستفي هذه القناعة من أي دليل يطمئنناليه، ولا يلزمه المشرع بحجته المسبقة، كما له طرح الأدلة التي لا يطمئن عليها، وله في النهاية سلطة التنسيق بين الأدلة المعروضة عليه.[3]

فإذاكانللقاضيفيالدليلسلطةتقديريةواسعةفياللجوءإلىالخبرةوتقديرقيمتهاالإثباتية انطلاقامنمبدأحريةالإثباتفيالموادالجزائيةوالذيتولدعنهمبدأالقاضيخبيرالخبراءفإن ذلكمقتصرعلىمايمكنللقاضيأنيبتفيهلوحده،أماالمسائلذاتالصبغةالفنيةالبحتةفلا يجوزللقاضيأنيحلنفسهفيهامحلالخبيرولايمكنهطرحرأيهإلاالأسبابسائغةومقبولة،إذ يذهبفيهذاالصددإتجاهعريضمنالفقهالجنائيإلىالقولأنالأدلةالرقميةتتمتعبحجيةقاطعة فيالدلالةعلىالوقائعالتيتتضمنها،وأنهيمكنالتغلبعلىمشكلةالتشكيكفيمصداقيتهامن خلالإخضاعهالإختباراتتمكنمنالتأكدمنصحتهاوسلامتها،وأنهلايجبالخلطبينالشك الذييشوبالدليلالرقميبسببإمكانيةالعبثبهأولوجودخطأفيالحصولعليه،وبينالقيمة الإقناعيةلهذاالدليل.[4]

وخلافالماذهبإليهالاتجاهالفقهيالأول،هناكمنيربأنمبدأحريةالقاضي فيالاقتناعيجبأنيبسطسلطانهعلىكلالأدلةدوناستثناءبمافيهاالدليل الالكتروني،معبرينبأنإعطاءالدليلالالكترونيقوةثبوتيةمطلقةلايستطيعالقاضي مناقشتهاأوتقديرهايعدبمثابةرجوعإلىالوراء إلىنظامالإثباتالمقيد.[5]

ومؤدىذلكأنهالا
تصلحفيذاتهاكدليلوحيدفيالإثباتالجنائي،وأنهإذاكانيتعينعلىالقاضيالإستعانةبأهل الخبرة في المسائل الفنيةالبحتةواستطلاع رأيهمفيمايتعلقهذهالمسائل[6]، فإن ذلك

1- سعيداني نعيم، المرجع السابق، ص220.
2- محمد علي الكيك، السلطة التقديرية للقاضي الجنائي، دار المطبوعات الجامعية، مصر، س2007، ص28.
3- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، ط1، دار الثقافة للنشر والتوزيع، الاردن، س2006،ص94.
4- سعيداني نعيم، المرجع السابق، ص221.
5- براهمي جمال، المرجع السابق، ص164.
6- سعيداني نعيم، المرجع السابق، ص222.

لايعنيالتخليعنحقهفيمناقشةوموازنةنتائجالخبرةواستبعادهاإنرأىفيذلكتحقيق العدالة،لانهذايدخلفينطاقتقديرهالذاتيومنصميموظيفتهالقضائية.[1]

ويظلالقاضيهوالمسيطرعلىهذهالحقيقةلأنهمنخلالسلطته التقديريةيستطيعأنيفسرالشكلصالحالمتهم،وأنيستبعدالأدلةالتييتمالحصولعليهابطرق غيرمشروعة.[2]

المبحث الثاني: إجراءات التحري داخل المنظومة المعلوماتية

يعد التوصل للدليل في الجرائم المعلوماتية من الصعوبات التي تواجه عملية التحري في الكشف عن الغموض الذي يتلبسها، وعليه فهي تتطلب وسائل للتحقيق فيها تكون ذات كفاءة لإيجاد الدليل.

فرغم عدم إكتفاءالأساليبالتقليديةلإجراءاتجمعالأدلةمنأجلمباشرةتحقيقناجحفيمجالالجرائمالمعلوماتية وصولا للحقيقة إلا انه يمكن إستخلاص الدليل منها في بعض الأحيان وعليه فقد تطرقنا إلى الإجراءات التقليدية في الجرائم المعلوماتية في المبحث الأول.

وفضلاعنإستحداثقواعدإجرائيةأخرىتتلاءممعطبيعةالبيئةالتقنيةفتطويرالإثباتوسائلهأم رفيغايةالأهميةللتصديلهذاالنوعالجديدمنالإجرام وعليه فإلى جانب الإستدلال بالوسائل التقليدية للتحقيق في هذا النوع من الجرائم فقد قام المشرع بوضع أساليب حديثة وهذا نظرا لطبيعتها التيتتطلبتقنياتجديدةللبحثعنالجانيوالوصوللدليل بسهولة وعدم فقدان الدليل المتحصل عليه.

فهذه الوسائل كانت لها الصدارة في تسهيل إيجاد الدليل وبذلك لإزالة اللبس عن الجريمة المرتكبة وعليه فقد تطرقنا إلى أهم الأساليب الحديثة في المبحث الثاني.

المطلبالأول: القواعد الإجرائية التقليدية لجمع الدليل الرقمي

إن الأساليب التقليدية تصنف من بين الأساليب المشتركة بين الجرائم التقليدية والجرائم الحديثة وذلك لكونها تشتركإيجاد الإجابةعلىالأسئلةالمشهورةلدىالمحققبهدفكشفالحقيقة ولذلك فقد تناولنا مفهوم المعاينة كإجراء تقليدي في الفرع الأول، يليه التفتيش الإلكتروني وضبط الدليل في الفرع الثاني، ثم الخبرة في الفرع الثالث.

الفرع الأول: المعاينة التقنية

تعد المعاينة من الإجراءات المشتركة بين الجرائم التقليدية والجرائم المعلوماتية لما لها أهمية تساعد على التوصل للدليل المراد ويقصد بالمعاينة هو:

1- أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، مرجع سابق،ص205.
2- بوكر رشيدة، المرجع السابق، ص508.

أولا: تعريف المعاينة

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من اتلافها أو محوها أو تعديلها وهي من إجراءات التحقيق الابتدائي ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، وتظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لبيان مدى صحتها في الاثبات فليس الحال كذلك بالنسبة للجرائم المعلوماتية، حيث نادرا ما يتخلف عن ارتكابها آثار مادية وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها.[1]

كذلك فالمعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعني تستلزم الإنتقال لي محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة والأصل بالجريمة ان إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة ورائها، كذلك هناك بعض الحالات التي توجب على النيابة الإنتقال فورا إلى مسرح الجريمة وهي حالة الإخطار بجناية ملتبس بها.[2]

كذلك فقد أشارت الإجراءات الجزائية الجزائري لهذا الإجراء وهذا في المادة 79 من نفس القانون بقولها" يجوز للقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة....."

ثانيا: أهمية المعاينة

تظهر أهمية المعاينة في أنها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بل ما يحتويه هذا الموقع من تفضيلات سواء تعلقت هذه التفضيلات بمكانه أو بوصفه من الداخل أو الآثار الموجودة به، والتي تنقلها بالجريمة وإجمالا كل ما يمكن جهات الشرطة والقضاء من تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها.[3]

وللمعاينة أهمية بارزة في مجال التحقيق الجنائيوكشف الحقيقة في الجرائم سواء كانت في نطاق الجرائم التقليدية أو الجرائم المعلوماتية،لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة السلطات ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون إنحياز أو تعديل أو نقصان[4]. بحيث أنها تقوم بتأكيد أو نفي الجريمة كذلك فهي تساعد

1- هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، مكتب الآلات الحديثة، مصر، 2002، ص39.
2- عبد الفتاح بيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي الإسكندرية، ط1، سنة 2006،ص237.
3- نبيلة هبة هروال، المرجع السابق، ص216.
4- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودر الشرطة والقانون، دار النهضة العربية، القاهرة، سنة2013، ص44.

القاضي في تدارك قناعته، وتساعد على معرفة الطريقة الإجرامية التي إعتمدها الجاني في إرتكاب جرمه.

تتم المعاينة في مثل هذه الجرائم كأي معاينة في جريمة أخرى إلا أنها تختلف من حيث طبيعة الجريمة المعلوماتية المرتكبة:

فلدينا معاينة الجرائم الواقعة على المكونات المادية للجهاز: تتم امعاينة في الجهاز الآلي كشاشة العرض ومفاتيح التشغيل والاقراص وغيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي لا تثير أي مشكلة بحيث يمكن لظابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

معاينة الجرائم الواقعة عن المكونات غير المادية أو بواسطتها: وهي برامج الجهاز وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينات أوائدتها وهذه الصعوبات يمكن تخليصها فب ما يلي:

نقص وقلة الآثار المادية التي تقع على المكونات غير المادية للجهاز

تردد عدد كبير منة الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة، والتي غالبا ماتكون طويلة، وذلك بين إقتراف الجريمة والكشف عنها.[1]

وللمعاينة في جرائم الانترنت والحاسوب أشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على أن هناك طرقا عامة تتوافق مع طبيعة الإتصال بالانترنت أو الوسيلة التي تستخدم مثلا: وسيلة تصوير شاشة الحاسوب IMPRESSION DE CAPTURES DECRAN والتي تكون بواسطة آلة تصوير تقليدية أو عن طريق إستخدام برمجة حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة وهذا مايصلح غليه تجميد مخارجات الشاشة FROZEN وغيرها.[2]

وللمعاينة إجراءات وقواعد أثناء السير في معاينة مسرح الجريمة المعلوماتية نذكرها بإيجاز:

- عند العثور على عينات أو أجهزة أو دعائم التخزين (كأقراص اسطوانية أو بطاقات ذاكرة...) يجب تسجيل الحالة التي وجدت فيها وموضع المكان التي عثر عليها، ووضعها في أكياس بغرض حمايتها من التلف أو الفقدان أو الكسر.

- تحرير الأوراق المطبوعة على الحاسب الآلى والتي عثر عليها في مسرح الجريمة ووضعها بأكياس حسب إحالتها، ويمكن إعادة الطباعة إذا كان الجهاز في حالة

1- ماجد ياقوت، أصول التحقيق، دراسة مقارنة، ط3، منشأة المعارف، الاسكندرية ص70.
2- نبيلة هبة هروال، المرجع السابق، ص218.

تشغيل وتحرير هذه الاوراق التي تمت طباعتها، بالاضافة غلى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم إستخدامها لحظة دخول مسرح الجريمة[1].

- لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة الإختصاص، من قبل ضابط الشرطة القضائية، وهذا مانصته المادة 42 من ق الإج الج،وعليه فالإخطار يكون مسبوقا بتأكيد ضباط الشرطة القضائية من وقوع الجريمة سواء بإستعمال الكتابة أو الهاتف أو أي وسيلة متداول عليها.

- أجاز المشرع الجزائري بالرجوع إلى المادة 47 من ق الإج الج إجراء المعاينة في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار أو اللي دون تأخير هذه الإجراءات[2]، وهذا بناءا على إذن مسبق من قبل وكيل الجمهورية.

- يجوز الاستعانة بأشخاص مؤهلين أي خبراء في المسائل العلمية والتقنية، من قبل الشرطة القضائية، إذ يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم إلى أجهزة و أنظمة لإكتشاف الحقيقة من بين هذه البرمجيات نذكر منها: أجهزة عالية الجودة على التحليل وتخزين المعطيات، اللجوء لإستخدام تقنيات التخفي وبرامج التتبع وهذا لتسهيل الإيقاع بالأشخاص المشتبه فيهم وتحديد مكان تواجدهم، كذلك نسخ مختلف البرامج المساعدة على(التشفير وفك التشفير وبرامج كسر كلمات المرور وبرامج الحماية من الإختراقات وبرامج أسترجاع الملفات المحذوفة...)

الفرعالثاني: التفتيش الإلكتروني وضبط الدليل

قديتطلبالتحقيقتفتيششخصالمتهمأومنزلهأوغيرهأومنزلهلضبطالأشياءالمتعلقةبالجريمة ،والتفتيشكإجراءمنإجراءاتالتحقيقالابتدائيهوفيالأصلمناختصاصسلطةالتحقيق،المتمثلةفيقاضيالتحقيقوالنيابةالعامةباختلاف التشريعات.[3]

وأنضبطالأدلةهوالنتيجةالطبيعيةالتييننتهيإليهاالتفتيشوالتييتمالحصولعليهاأثناءه.وعلىذلك فإنهيتضحلناأنهذينالإجرائينماهماإلاوسيلةللإثباتالمادي،ذلكأنالتفتيشيستهدفضبطأشياءماديةتساعدفيإثباتوقوعالجريمةوإسنادهاإلىالمتهمالمنسوبإليهإرتكابهاوكما أنرجالالضبطيةالقضائيةقدتعودوافيالجرائمالتقليديةعلىضبطإلاالأشياءالمادية.[4]

أولا: إجراءات التفتيش في البيئة الرقمية

يقصدبمحلالتفتيش،المستودعالذييحتفظفيهالمرءبالأشياءالماديةالتيتتضمنسرهوخصوصيته،والسر الذييحميهالقانونهوذلكالذييودعفيمحللهحرمة،كالمسكنأوسيارةأورسائل،بالتاليفم

1- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 200، ص122.
2- المواد 47 و 49 من ق الإج ج .
3- براهيمي جمال، المرجع السابق، ص13.
4- سعيداني نعيم، مرجع سابق، ص143.

حلالتفتيشقديكونأحدالمواقعالمذكورةمعمراعاةالإجراءاتوالشروطالقانونيةالمقررةلكلموقععلد حدة.[1]

ويتضمن محل تفتيشالمكوناتالماديةوالمعنوية لنظامالمعالجةالآلية وتكون كالتالي:

-1-تفتيشالمكوناتالماديةلنظامالمعالجةالآلية:

إنالدخوللمكوناتالماديةللحاسببحثاعمايتصلبجريمةمعلوماتيةللكشفعنمرتكبيهالاخلافيه بينالفقهاءطالماتموفقاللإجراءاتالقانونيةالمقررة،فانكانتفيمكانخاصكمسكنالمتهمكانلهاحكمهف لايجوزتفتيشهاإلافيحالاتيجوزفيهاتفتيشمسكنهبنفسالضماناتالمقررةقانونافيالتشريعاتالمختلفة وإنكانتفيمكان عامكالمقاهيالشوارعكانلهاحكمه.[2]

فإذاكانتموجودةفيمكانخاصكمسكنالمتهمأوأحدملحقاتهكانلهحكمه،بحيثلايجوزتفتيشهاإ لافيالحالاتالتييجوزفيهاتفتيش
المساكنوملحقاتهاوبالإجراءاتوالضماناتالمقررةقانونافيالتشريعاتالمختلفةلذلك.[3]

ويجب
التمييزداخلالمكانالخاصبينماإذاكانتمكوناتالحاسبمنعزلةأممتصلةبحواسيبأوأجهزةمتواجدةفيم كانآخركمسكنالغير، إذ أنه
فيهذهالحالةيجبعلىالمحققمراعاةالقيودالضماناتالتييشترطهاالقانونلتفتيشهذهالأماكن.[4]

وعليهيتبينأنتفتيشالمكوناتالماديةلجهاز الحاسبوملحقاتهمثللوحةالمفاتيحأوالشاشةأوالطبا عةأوغيرهامنالأشياءالماديةالمحسوسة،لايثيرأيةمشاكلإجرائيةأمامسلطاتالاستدلال،إذيسريع ليهمايسريعلىتفتيشالأشياءوالأدواتالماديةالأخرىمنشروطوضمانات،كمراعاةوقتالتفتيش،الإذن بالتفتيش،الأشخاصالقائمينبالتفتيش،والأشخاصالمطلوبحضورهمعندالتفتيش،معمراعاةالاختصاصالمكانيوعدمفضالأوراقالمحرزة .
كماأنأجهزةالقضاءالمخوللهاالقيامبإجراءالتفتيشسواءبصفةأصليةأواستثنائيةيمكنهاتفتيشالمكو ناتالماديةفيالجريمةالالكترونيةدونالحاجةإلىأنتكونمتخصصةفيالجوانبالتقنية،مثلهامثلغيرهام ن المكوناتالماديةالأخرى.[5]

-2-تفتيش المكونات المعنوية لنظام المعالجة الآلية:

إذاكانالأمرقدإنتهىبنا إلىصلاحيةالمكوناتالماديةللنظامالمعلوماتيةكمحليرد عليهاالتفتيش،فإ نإمتدادذلكإلىالمكوناتهغيرالماديةهومحلجدلكبيرحولمدىصلاحيتهاالأنتكونموضوعاللتفتيشتمهيد الضبطالأدلة.فالخلافحاصلفيمسألةأنالتفتيشالتحقيقيوسيلةللبحثعنالأدلةالمادية،إذهوإجراءيسعد

1- براهيمي جمال، المرجع االسابق، ص 14
2-طارقإبراهيمالدسوقيعطية،الأمنالمعلوماتيفيالنظامالقانونيلحمايةالمعلوماتيةدونطبعة،دارالجامعة الجديدة،مصر،ص397.
3- خالدممدوحإبراهيم،فنالتحقيقالجنائيفيالجرائمالالكترونية،دارالفكرالجامعي،إسكندرية،س 2009،ص195
4 -أحمدبنزايدجوهرالحسنالمهدي،تفتيشالحاسبالآليوضماناتالمتهم،مذكرةلنيلدرجةماجستيرفيالقانون كليةالحقوق،جامعةالقاهرة، س2009، ص118.
5- فايزمحمدراجحغلاب،الجرائمالمعلوماتيةفيالقانونالجزائريواليمني،أطروحةلنيلشهادةالدكتوراهفيالقانون، فرعالقانونالجنائيوالعلومالجنائية،كليةالحقوق،جامعةالجزائر1، الجزائر، س2011، ص309.

إلىضبطالأدلةالمتعلقةبالجريمةلتقديمهاإلىالمحكمةالمختصةكدليلإدانة،لذلكيثورالشكوالتساؤل حولإمكانيةإعتبارالبحثعنأدلةالجريمةالمعلوماتيةفينطاقنظمالحاسوبنوعامنالتفتيشبإعتبارأنالبيانااتالإلكترونيةأوالبرامجفيحدذاتهاليسلهامظهرماديمحسوسفيالمحيطالخارجيويستشعرالفقهصعوبةالمسألةنظرالغيابالطبيعةالماديةللمعلوماتفي ذاتهامجردةمندعامتهاالمادية.[1]

ويتضحموقفالمشرعالجزائري من خلال نصالمادة 05قانون04/09علىجوازتفتيشالمنظومة المعلوماتية من قبل السلطات القضائية،وإلىجانبذلك قامالمشرعالفرنسيبتعديلالنصوصالتيتحكمالتفتيشوأضافعبارة" المعطياتالمعلوماتية "وهذا في نص المادة94منقانونالإجراءاتالجزائيةبموجبالمادة42 من قانون الإج الج.

-3-مدىقابليةشبكاتالمعلوماتالمتصلةبالحاسبالآليللتفتيش:

يقصدبالشبكةالمعلوماتية،اتصالجهازينأوأكثرمنأجهزةالحاسبالآلياتصالاسلكياأولاسلكيا أوبواسطةالأقمارالصناعية،وقدتكونهذهالأجهزةمرتبطةبعضهاالبعضفيموقعواحدفيطلقعليهاا لشبكةالمحلية،أوموزعةعلىعدةأماكنمتفرقةيتمربطهاعنطريقخطوطالهاتفأوالمجالالمغناطيسي فتسمىالشبكةالممتدةأوشبكة الأنترنت.

لذلكيثيرإخضاعشبكاتالمعلوماتالمتصلةبالحاسبالآليلعمليةالتفتيشصعوباتكبيرة،تتعلقبالد رجةالأولىبالطبيعةالتكنولوجيةالرقميةالتيتسمحبتوزيعالمعلوماتالتيتحتويأدلةعبرشبكاتحاسوب يةفيأماكنمجهولةوبعيدةتماماعنالموقعالماديللتفتيش،فقديكونالموقعالفعليلهذهالمعلوماتداخلاختصاصقضائيآخرفيإقليمدولةواحدةأوفيإقليمدولةأوعدةدولأخرى،وهومايزيدالأمرتعقيداباعتبار الشبكةالمعلوماتيةممتدةعبرأرجاءالعالم.[2]

لذلكيثارالتساؤلحولأثرتفتيشالأنظمةالمعلوماتيةالمتصلةبالنظامالمأذونبتفتيشهإذاتواجدت فيدوائرإختصاصمختلفة[3].ونستطيعأننميزفيهذهالصورةبينإحتماليننعلىالنحوالتالي:

أ-

اتصالالحاسبالمتهمبحاسبآليآخرأومنظومةمعلوماتيةمتواجدةفيموقعآخرداخلإقليمالدولةنفسها:

تتحققهذهالفرضيةحينمايقومالمتهمبتحويلعبرالانترنتمعلوماتأوبيانات

متعلقةبجريمةإلكترونيةمنحاسبهإلىحاسبأومنظومةمعلوماتيةمملوكةللغيرمتواجدةفيمكا نآخروتخزينهافيها،ففيهذهالحالةتواجهسلطاتالتحقيقمشكلةتجاوزالاختصاصالمكانيمنناحية،و الاعتداءعلىحرمةخصوصيةالغيرمنناحيةأخرى،لاسيمافيالدولالعربيةالتيلمتفصلقوانينهاالإج رائيةفيهذهالمسألةبعد.[4]

1- عبدالعظيموزير،شرحقانونالعقوباتالقسمالخاصجرائمالإعتداءعلىالأموالط1،دارالنهضةالعربيةالقاهرة،س1993، ص43.

2 - عادلعبداللهخميسالمعمري، التفتيشفيالجرائمالمعلوماتية،مجلةالفكرالشرطي، مجلد 22،العدد86، صادر عنمركزبحوثالشرطة،القيادةالعامةلشرطةالشارقة،الإماراتالعربيةالمتحدة،س2013، ص262.

3- سعيداني نعيم، المرجع السابق، ص149.

4 - جميلعبدالباقيالصغير،أدلةالإثباتالجنائيوالتكنولوجياالحديثة،دارالنهضةالعربية، س2001، ص113.

والملاحظ أنالمشرعالجزائريقام بتفادي مسألةتفتيشالمنظومةالمعلوماتيةعنبعدبصفةنهائية،حينماوسّعفيالتعديلالأخيرلقانونالإجراءاتالجزائيةاختصاصاتضباطالشرطةالقضائيةفيمجالالتحقيقعنالجرائمالالكترونية،وأجازإمكانيةقيامهذهالسلطاتبالتفتيشفيأيوقتمنالليلوالنهار،وفيأيمكانعلىامتدادكافةالترابالوطن وهذا ماجاء في نص المادة 47 من قانون الإج الج.

ب-إتصالالحاسبالمشتبهفيهأوالمتهمبحاسبآخر أو منظومة معلوماتية موجودةفيإقليم دولة أخرى:

وهنامنالمتصورطبقالهذاالإحتمالأنيقوممرتكبوالجرائمبتخزينبياناتهمفيأنظمةمعلوماتيةخارجالدولةعنطريقشبكاتالإتصالالبعيدة بهدفعرقلةسلطاتالتحقيق في جمع الأدلة.[1]

وفيمثلهذهالحالةتواجهسلطاتالتحقيقمشكلةكبيرةتتمثلفيمدىجوازتمديدهاإجراءاتالبحثوالتفتيشإلىخارجالإقليمالجغرافيللدولةالتيصدرمنجهتهاالمختصةالإذنبالتفتيشوالدخولفيالمجالالجغرافيلدولةأخرى،وهومايسميبالتفتيشالعابرللحدود.[2]

ثانيا: ضبط الدليل الرقمي

يعتبر الضبطمنإجراءاتجمعالأدلة،وهو النتيجةالطبيعيةالتييُنتهيإليهاالتفتيش

والأثر المباشر الذييسفر عنه،ويقصدبهوضعاليدّعلىالأشياءالمتعلقةبجريمةوقعتوالتيتفيدفي كشفالحقيقةعنهاعنمرتكبيها،ووضعهافيأحرازمختومةولتقدمإلىالجهةالقضائيةالمختصةكدليل لإثبات.[3]

وتحصيلالأدلةفيالجرائمالالكترونيةقديرتبطبعناصرماديةكجهازالحاسبالآليوملحقاته،الأقراصالصلبة،الأقراصالأشرطةالممغنطة،الطباعة،البرامجاللينةوالمراشد،البطاقاتالممغنطةوبطاقاتالائتمانوالمعداتالمستعملةفيشبكةالانترنتمثلالمودم،ففيهذهالحالةفلايطرحضبطهذهالمكوناتالماديةأيإشكالقانونيأوعمليلإمكانيةإخضاعهاالإجراءاتالضبطوالتحريزالتقليدية، وقديرتبطالدليلالالكترونيبالمكوناتالمعنويةللحاسب،كمختلفالبرامجوالبياناتالمعالجةآلياوالمراسلاتوالاتصالاتالالكترونيةالتييجريتبادلهاعبرشبكةالانترنتوالبريدالالكتروني،وهناتثير الطبيع

1- عبداللهحليسعليمحمود،إجراءاتجمعالأدلةفيمجالسرقةالمعلوماتبحثمنشورعلىموقع: www.arablawinfo.com.

2- حسينبنسعيدبنسيفالغافري،السياسةالجنائيةفيمواجهةجرائمالانترنت،رسالةلنيلشهادةالدكتوراهفيالقانون،كليةالحقوق،جامعةعينالشمس،القاهرة، 2005 ،ص376

3 -خالدعياد الحلبي،إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنت،دار الثقافةللنشروالتوزيع،عمان، س2011، ص170.

عةالمجردةلهذهالمكوناتجدلافقهياواختلافاتشريعياكبيراحولمدىإمكانيةضبطهاوفقالقواعدالضبطالمألوفة،معالعلمأنالضبطبمفهومهذهالأخيرةلايردإلاعلىالأشياءالمادية.[1]

1-أنواع الأدلة:

إنالغايةمنالتفتيشهوضبطشيءيتعلقبالجريمةويفيدالتحقيقالجاريبشأنهاسواءأكانهذاالشيء أدواتإستعملتفيإرتكابالجريمةأوشيئانتجعنهاأوغيرذلكممايفيدفيكشفالحقيقة.والضبطفيمجالالجرائمالإلكترونيةيتصلبضبطالمكوناتالماديةلأنظمةالحاسوب،ضبطالمكوناتالمعنويةوالبرمجيات،وكذاضبطالمعطياتالتيتتناقلأويجريتبادلهافينطاقشبكةالمعلوماتالتيترتبطالحواسيبومايتصلبها
وعلىهذاالأساسفإنمنالأشياءالتييتمضبطهاوالتحفظعليهافيالجرائمالمعلوماتيةوالتيلهاقيمةفيإثباتتلكالجرائمونسبتهاإلىالمتهم.[2]

ضبطجهازالكومبيوترولحقاته ":
ذلكأنضبطهأمرمهمجداللقولبأنالجريمةالواقعةهيجريمةمعلوماتيةأنها
مرتبطةبالمكانوالشخصالحائزعلىالجهاز
ولأجهزةالكومبيوترأنواعمختلفةالأمرالذييتطلبفيضابطالشرطةالقضائيةالمعرفةالكافيةالتيتؤهلهللتعاملمعهوالتعرفعلىمواصفاتهبسرعة.

- ضبطالمعداتالمستعملةفيشبكةالأنترناتوأهمهاوهي المودم MODEMالوسيلةالتيتمكنأجهزةالكومبيوترمنالإتصالببعضهاالبعضعبرخطوطالهاتف.

-وسائطالتخزينالمتحركةكالأقراصالمدمجة) أقراصالليزر (والأقراصالمرنةوالأشرطة المغناطيسية.

ضبط البرمجيات Software:
فإذاكانالدليلالرقميينشأبإستخدامبرنامجخاصفإنضبطالأقراصالخاصةبتثبيتوتنصيبهذاالبرنامجأمرفيغايةالأهميةعندفحصالدليل.

-
ضبطالبريدالإلكترونيوالذييحتويعلىبرامجمتخصصةلكتابةوإرسالوإستعراضوتخزينالرسائلالإلكترونية،وهذهالرسائللايختلفالتعاملمعهاعنالتعاملمعالرسالةالورقية،إذبمقدورالمستخدمأنيطرحهاجانباأويردعليهاأوينقلهاإلىشخصآخرأو يحفظ بهافيملفخاص،لذلكفالمحققالذييريدضبطالرسائلالإلكترونية الخاص به ثم يشغل برامجالبريدالإلكترونيفيجهازحاسوبهثممراجعةقائمةالرسائلليلتقطمنبينهاالرسالةالمطلوبة.

2-إجراءاتضبطالدليلالرقمي

من أهم الإجراءات التي تم تداركها لضبط الدليل هي:

1- عبدالفتاحبيوميحجازي، مبادئالإجراءاتالجنائيةفيجرائمالكمبيوترالانترنت،دارالفكرالجامعي،الإسكندرية،س. 2006 ، ص218.
2- سعيداني نعيم، المرجع السابق، ص160.

-
استخراجنسخاحتياطيةمندعائمالبياناتوالمعطياتالمضبوطةوالعملعليهالتفاديالمساسبالدليلالأصلي.

-عدمطويالقرصلتفاديتلفهوتحطمهوفقدانالمعلوماتالمسجلةفيه.

- تأمينالبرامجالمعلوماتيةالمضبوطةفنياقبلتشغيلها.

- مراعاةظروفالحرارةوالرطوبةالمناسبةفيأماكنتخزينالأقراصوالأشرطةالممغنطة المحرزة تكوندرجةالرطوبة80/20،وأنتتراوحدرجةالحرارةفيهابين32/4 درجة،معتفاديتعريضهاللأضواءأولأيسائلمنالسوائل،معالعلمأنهفيمثلهذهالظروفيمكنأنتصلمدةصلاحيةتخزينهذهالأقراصإلىثلاثسنواتدونأنيصيبهاتلفأوتعديلأوتحول.[1]

1- حساممحمدنبيلالشنراقي،الجرائمالمعلوماتية-دراسةتطبيقيةمقارنةعلىجرائمالاعتداءعلىالتوقيعالالكتروني،دارالكتبالقانونية،القاهرة، 2013 ،ص525

الفرعالثالث: الخبرة التقنية في إثبات الجرائم المعلوماتية

أدىالتطورالتقنيالهائلفيعالمتكنولوجياالإعلاموالاتصالإلىاحداثتغيير كبيرفيالمفاهيمالمتعلقةبالدليلالجنائي،مماأدىبدورهإلىتعاظمدورالإثباتالعلمي للدليلوإعلانانضماماالخبرةالتقنيةإلىعالمالخبرةالقضائية،وأصبحتالاستعانةبخبراء مختصينلفحصالأدلةالتقنيةوتقويمعمليةالإثباتالرقميوتحليلالجريمةالالكترونيةأمرا ملحالايمكنالاستغناءعنه.[1]

تعتبرالخبرةمنأهمالإجراءاتالتيتتخذللتنقيبعنالأدلةالتيتساعدعنالكشف عن الجريمةالإلكترونيةكونالجريمةالإلكترونيةتترتكببوسائلمستحدثةومعقدةيصعب التعاملمعها.

والخبرةهيالوسيلةلتحديدالتفسيرالفنيللأدلةأوالدلائلبالاستعانةبالمعلومات،فهيفيالحقيقةليستدليلامستقلاعنالقوليأوالدليلالمادي،إنماهيتقييمفنيلهذاالدليلوالعنصرالمميزللخبرةعنغيرهامن إجراءاتالإثباتكالمعاينة،الشهادةوالتفتيش.[2]

ممالاشكفيهأنالخبرةالتقنيةباعتبارهامنإجراءاتالتحقيقتخضعلضوابط قانونية وكذلك فنية سنجسدها كالآتي:

أولا: الضوابط القانونية الذي تحكم الخبرة القضائية في الجرائم المعلوماتية.

1- عبدالناصرمحمدمحمودفرغلي،الإثباتالجنائيبالأدلةالرقميةمنالناحيتينالقانونيةوالفنية، دراسةمقدمة للمؤتمرالعربيالأولللعلومالأدلةالجنائيةوالطبالشرعي،المنظمبالرياض،فيالفترةالممتدةبين 12 و 14 نوفمبر، س2008،ص24.

2- عبد الفتاح بيومي حجازي، المرجع السابق، ص321.

وتتجسدفيتلكالضوابطالقانونيةالمنصوصعليهافيقانونالإجراءاتالجزائيةكاختيارالخبراء ،واجباتوالتزاماتالخبير،الحلفاليمين،وخضوعهللرقابةالقضائية.

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

وقد عرفها البعض انها الإستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوينعقيدته على نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه.

والخبير هو كل شخص لديه دراية خاصة بمسألة من المسائل قد يستدعي التحقيق فحصها ويستلزم ذلك كفاء خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستعين بالخبيركما هو الحال مثلا في تقرير الصفةالتشريحية في جرائم القتل او تحليل المادةالمطعونة في جرائم التسمم او فحص خط جريمة التزوير.[1]

أ-أهمية الخبرة في البحث عن الدليل الرقمي

تكمنأهميةالخبرةفيأنهاتنيرالطريقلجهةالتحقيقوالقضاءولسائرالسلطاتالمختصةبالدعوىالجزائية،لذلكفقداهتمالمشرعالجزائريبتنظيمأعمالالخبرةمنالمواد143 إلى 156منقانونالإجراءاتالجزائيةوإعتبارهامنإجراءاتالبحثعنالدليلحيثنصتالمادة143أنهلجهاتالتحقيقأوالحكمعندماتعرضلهامسألةذاتطابعفنيأنتأمربندبخبيرإمامنتلقاءنفسهاأوبناءعلىطلبمنالنيابة العامةوإمابطلبمنالخصوم.[2]

وللخبرةالفنيةدوركبيرفيإثباتالجريمةالإلكترونية،لأنهاتنيرالدربلسلطاتالتحقيقوالقضاءو سائرالجهاتالمختصةبالدعوىالجزائيةللوصولإلىالحقيقةوتحقيقالعدالةالجنائية[3]،وقدتزايدتالحاجةإلىالخبرةالفنيةللتحقيقعنالجرائمالالكترونيفيالآونةالأخيرةنظرا للتحولاتالتكنولوجياالتيمستوسائلالإعلاموالاتصال،اذتعددتأنواعونماذجالحواسيبوشبكاتالاتصالبينها،وأصبحتالعلوموالتقنياتالمتعلقةبهاتنتميإلىتخصصاتعلميةوفنيةدقيقةومتشعبة،والتطوراتفيمجالهاسريعةومتلاحقةلدرجةقديصعبعلىالمتخصصتتبعهاواستيعابها . بليمكنالقولانهلايوجدحتىالآنخبيريملكمعرفةمتعمقةفيسائرأنواعالحاسباتوبرامجهاوشبكاتها،أوقادرعلىالتعاملمعكافةأنماطالجرائمالتيتقععليهاأوترتكببواسطته لذلكتركالمشرعللمحقق الحرية الكاملةوفيأيةمرحلةمنمراحلالتحقيقندبأيخبيريأنسفيهالكفاءةالفنية اللازمة للاستعانةبخبرته.[4]

ب-شروط صحة الخبرة.

1- عبدالناصرمحمدمحمود فرغليومحمدعبيدسيفسعيدالغافري،المرجعالسابق .ص24.
2- سعيداني نعيم، المرجع السابق، ص166.
3- بوكر رشيدة، المرجع السابق، ص424.
4- براهمي جمال، المرجع السابق، ص69.

1-اختيار هالخبير منجدو لالخبراء :
الأصلأنيختار الخبراءحسبالتخصصمنالجداو لالتيتعدهاالمجالسالقضائيةبعداستطلاع لرأيالنيابةالعامة،ولكناستثناءفيحالةعدمتوفر الخبرةالمطلوبةفيجداو لالخبراءيجوز لجهاتالتحقيقأنتختار بقرار مسببخبراءليسوامقيدينفيأيمنهذهالجداو لكماانعمليةاختبار الخبير أمر امتروكالجهاتالتحقيق،فبمفهومنصالمادة147منقانون الإج الج الج مثلاللقاضيأنيندبخبير اواحداأوخبراءمتعددينحسبالحاجة،ولاتهمطبيعةالخبير سواءكانشخصا طبيعياأوشخصامعنوياكمؤسسةمتخصصةتعملفيمجالالخبرةالتقنية.[1]

2- حلف اليمين القانونية:
حيثيجبلصحةتقرير الخبير أداءاليمينلحملالخبير علىالصدقو الأمانةفيعملهو بثالطمأنينةفيآر ائهالتيقدمها،سواءبالنسبةلتقدير القاضيأولثقةبقيةأطر افالدعوى،ولذلكلايغنيعنهذاالإجراءأيةضمانة أخرىمنالضمانات[2]،ولعلالعبرةمنحلفالخبير هيحملهعلىالصدقو الأمانةفيعمله،وبثالطمأنينةفينتائجخبرتهالتييقدمهاسواءبالنسبةلتقدير القاضيأو الثقةبقيةأطر افالقضية.[3]

و أماالشروطالمتعلقةبتقرير الخبرةفإنالخبير بعدإنتهائهمنأبحاثهو فحوصاتهيعدتقرير ايضمنهخلاصةماتوصلإليهمننتائج،بعدتطبيقالأسسو القواعدالعلميةالفنيةعلىالمسألةمحلالبحثو إنكانالمشرعلميوجبإتباعشكلمعينفيتقرير الخبرةفقديكونشفويا وقديكونكتابيا وفقالماتحدده طبيعةالمأمورية لكنالواقعالعمليأثبتأنمايتمفيالغالبالأعمهو أنيطلبمنالخبير إيداعتقرير هكتابة،سيماإذاماكانتالمسألةموضوعالخبرةتتطلبإجراءأبحاثو تجاربو فحوصاتعلميةو عمليةو معملية .
و غالباماير فقالخبير بالتقرير ملحقاإيضاحيابالصور حتييسهلعلىجهةالتحقيقفهمالخبرةو علىجهةالحكمتكوينعقيدتهاو إقتناعهاالذاتيبالدليل.[4]

ويشترطأيضافيمايتعلقبتقرير الخبرةأنيقومالخبير بإيداعتقرير خبرتهخلالالمدةالمحددةلهفيأمر أوحكمالندب،فإنلميودعتقرير هخلالهذهالمدةجاز للقاضيإستبدالهبغير همالميقدمالخبير طلبابتمديدهذهالمهلةوذلكنظر الماتتسمبهالإجراءاتالجزائيةمنطابعالسرعةسيماإذاتعلقالأمر بالجريمةالمعلوماتية.[5]

ثانيا: الضوابط الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية

-أ- مهام الخبير: بالرجوع للطبيعة الفنية والعلمية للخبير فإن الجدير بالذكر أن عمل الخبير يتمحور حول مايلي:

1- بوكر رشيدة، المرجع اسابق، ص426.
2- أحمد أبو قاسم،الدليلالجنائيالماديودور هفيإثباتجرائمالحدودو القصاص،المركز العربيللدراسات الأمنيةو التدريب،الرياض،س 1993، ص377.
3
عبدالناصر محمدمحمودو عبيدسيفسعيدالمسماري،الإثباتالجنائيبالأدلةالرقميةمنالناحيتينالقانونيةو الفنية،دراسةتطبيقيةمقارنة،بحثمقدمللمؤتمر العربيالأولللعلومالأدلةالجنائيةو الطبالشرعي،المنعقدبالرياض، س2007، ص24.
4- عبدالناصر محمدمحمودفرغليو محمدعبيدسيفسعيدالمسماري،المرجعالسابق.ص27.
5- سعيداني نعيم، المرجع السابق، ص169.

-
الإلمامبتركيبالحاسبوصناعتهوطرازهونظمتشغيلهالرئيسيةوالفرعيةوالأجهزةالطرفيةالملحقةبهوكلماتالمرورأوالسرورموزالتشفير.

-
طبيعةالبيئةالتييعملفيظلهاالحاسبمنحيثتنظيمومدىتركيزأوتوزيعهلالمعالجةالآليةوتحديدأماكنالتخزينوالوسائلالمستخدمةفيذلك.

-
القدرةعلىأداءالمهامدونأنيترتبعلىذلكإعطابأوتدميرالأدلةالمتحصلةمنالوسائلالإلكترونية.

-
التمكنمننقلالأدلةالإثباتغيرالمرئيةوتحويلهاإلىأدلةمقروءةأوالمحافظةعلىدعامتهالحينالقيامبأعمالالخبرةبغيرأنيلحقهاتدميرأوإتلاف،معإثباتأنالمخرجاتالورقيةلهذهالأدلةتطابقماهومسجلعلىدعائمهاالممغنطة.[1]

بالإضافةإلىضرورةإلمامالخبيرأيضا بنظمالحاسبالآليبمكوناتهالماديةوالبرامجية عن طريق:

- معرفتهلوسائلوطرقفحصنظامالحاسبالآليكبرامجكشفوإزالةللفيروساتوبرامج

- إسترجاعالبياناتوالمعلوماتوإصلاحالتالفوإظهارالمخفيمنها.

- معرفتهلوسائلنسخالبرامجوالملفاتوعملنسخمنالقرصالصلبطبقالأصل.

- معرفتهلكيفيةالربطبينالدليلالماديوالدليلالرقميفيالوقائعمحلالبحث.

ولاينجحالخبيرالمعلوماتيفيأدائهلمهامهالمنوطةبهوإتمامهللمأموريةالمكلفبهاإنلميكنلديهذاالقدرمنالمتطلباتالفنية.[2]

كذلك
للخبيرالمعلوماتيفيسبيلتحريالحقيقةأنيقومبكلمايمكنهمنالتوصلإليها،وهوفيإطارالقيامبعملهلهأنيستخدمالأساليبالعلميةالتييقومعليهاتخصصهولايسللمحكمةأنترفضتلكالأساليبماليمكنرفضهالهامسببابشكلمنطقي[3].

تشملخطواتاشتقاقالدليلالالكترونيوالتيتتمثلفيخطواتماقبلالتشغيلوالفحصوخطواتالتشغيل[4]، وتتمل فيما يلي:

1- سعيداني نعيم، المرجع السابق، ص170.
2- سعيداني نعيم، المرجع السابق، ص170.
3- خالد ممدوح إبراهيم، ص301.
4- عبدالفتاحبيوميحجازي .الاثباتفيجرائمالكمبيوترو الانترنت .دارالكتبالقانونية .مصر، س2003، ص187

-1-
مرحلةتجميعالمعلوماتالمخزنةلدىالطرفمقدمالخدمةمنخلالتتبعالحاسباتالخادمةالتيدخلفيهاالمجرمالمعلوماتي.[1]

-2-
مرحلةالمراقبةويتمذلكبطرقمختلفةأهمهااستخدامبرامجمراقبةيمكنتحميلهاللبحثعنالمعلوماتالمشتبهفيهاوحصروتسجيلبياناتكلدخولوخروجبالموقع.

-3-
المرحلةفحصالنظامالمعلوماتيالمشتبهفيهبعدضبطهمنطرفجهاتالتحقيقبمكوناتهالماديةوالمعنوية لإشتقاقالدليلوتقديمهلجهاتالتحقيقوتقريرمدىوقوعالجريمةبإستخدامالنظامالمضبوطمنعدمه.[2]

-ب-
تقنياتانجازالخبرةالالكترونية:لقدوضعتوزارةالعدلالأمريكيةإطارا عمليانموذجيايحددالتقنياتا لأساسيةالتييتعينعلىالخبيرالالكترونيإتباعهالجمعالأدلةالرقمية،فحصهاوتحليلها،ومنثمكتابةالنتائجالمتوصلإليهافيالتقرير[3]،والتييمكنتلخيصهافيمايلي:

-1-تقنياتماقبلالتشغيلوالفحص:

- التأكدمنصلاحيةوحداتنظامالأجهزةالالكترونيةالمتعلقةبالجريمةللتشغيل.

-التحققمنمطابقةمحتوياتإحرازالمضبوطاتلماهومدونعليها.

-تسجيلوتوثيقمعطياتوحداتالمكوناتالمضبوطة،كالنوعوالطرازوالرقمالتسلسلي.[4]

-2-تقنياتالتشغيلوالفحص:

- إستكمالتسجيلباقيمعطياتالوحداتمنخلالقراءاتالجهاز.

-

عملنسخةمنكلوسائطالتخزينالمضبوطةوعلىرأسهاالقرصالصلبلإجراءعمليةالفحصالمبدئيعلىهذهالنسخةلحمايةالأصلمنأيفقدأوتلفأوتدميرسواءعنسوءالإستخدامأولوجودفيروساتأوقنابلبرمجية.

-

تحديدأنواعوأسماءالمجموعاتالبرامجية(كبرامجالنظامبرامجالتشغيل،برامجالتطبيقاتوبرامج الإتصالات،وماإذاكانهناكبرامجأخرىذاتدلالةبموضوعالجريمة.

1- خالدممدوحإبراهيم ، فنالتحقيقالجنائيفيالجرائمالالكترونية.المرجعنفسه، ص300.
2- سعيدلني نعيم، المرجع السابق، ص171.
3- براهيمي جمال، المرجع السابقو ص76.
4- غازيعبدالرحمنهيانالرشيد،الحمايةالقانونيةمنجرائمالمعلوماتية،رسالةلنيلدرجةدكتوراه فيالقانون،كلية الحقوق،الجامعةالإسلاميةفيلبنان،بيروت، س2004، ص530.

- إظهار الملفات المخبأة و النصوص المخفية داخل الصور.

- إسترجاع الملفات التي تم محوها من الأصل وذلك بإستخدام أحد برامج إستعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة.

- تخزين هذه الملفات أو المعطيات و عمل نسخ أخر بطبق الأصل من الأسطوانة أو القرص المحتوية لها و لفحصها عن طريق تطبيق الخطوات السالفة الذكر.

- إعداد قائمة يجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها، مع إجراء مراجعة لكل صورة تم حفظ بها في القرص الصلب لحاسوب آخر للتأكد من سلامة القائمة.

- تحويل الدليل الرقمي إلى هيأة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها أو وضعها في أي وعاء آخر حسب نوع المعطيات و المعلومات المكونة للدليل.[1]

إضافة لذلك يعتمد الخبير في شرح ملابسات الجريمة الالكترونية و استخلاص الدليل الرقمي الذي يساعد على الكشف عن المجرم الالكتروني بجملة من الوسائل العلمية، و التي تتمثل في الغالب أدوات فنية تستخدم في بيئة نظام المعلومات[2]، نذكرها في ما يلي:

1- بروتوكول الأنترنات: و هو المسؤول عن ترسل حزم البيانات عبر شبكة الأنترنات و توجيهها إلى أهدافها، و هو يوجد بكل جهاز مرتبط بالأنترنت و يتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، و الجزء الثاني لمزود الخدمة، و الثالث مجموعة الحاسبات المرتبطة، و الرابع يحدد الكومبيوتر الذي تم الإتصال منه، مع ملاحظة أن عنوان الـ IP قد يتغير في كل إتصال بشبكة الأنترنت.

2- نظام البروكسي PROXY:
يعمل هذا النظام كوسيط بين الشبكة و مستخدميها بحيث يضمن مقدما الخدمة توفير خدمات الذاكرة الجاهزة، و تقوم فكرة البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تتريلها من قبل في وقت مبكر إرسالها إلى المستخدم دون حاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تتريلها من قبل في وقت مبكر إرسال الطلب إلى الشبكة العالمية، و من أهم مزايا هذا النظام أن الذاكرة المتوفرة و هنا يستخدم البروكسي أحد عناوين لديه يمكن أن تتحفظ بتلك العمليات التي تم تعليها مما يجعل دور هقوي في الإثبات عن طريق فحص تلك العمليات المحفوظة.

3- برنامج الدمج و فك الدمج pkzip :
و يستخدم هذا البرنامج لفك دمج البرامج، عادة لفك البرامج التي قام المجرم الالكتروني بدمجها قصد التع

1- عبد الناصر محمد محمود فرغلي و عبيد سيف سعيد المسماري، المرجع السابق، ص35.
2- براهيمي جمال، المرجع السابق، ص78.

رفعلىطبيعةالبياناتالتييحتويهاوتحليلها،ودمجالبرامجهيتقنيةعاليةيستعملهاالمجرمالالكترونيلإ خفاءمعلوماتمعينةلايمكنالاطلاععليهاإلابعدفكالدمج.[1]

4- برنامجTrace route : يتمعادةادراجهذاالبرنامجضمننظمتشغيلالحاسب الرئيسية،ويعتبرذاأهميةبالغةفيالكشفالجنائي،إذيحددبدقةالأجهزةالالكترونيةالتياشتركتفينقلالبـ ياناتعلىالانترنتبتحديدمساراتهاوصولاإلىالمرسلإليه،كمايمكنهأنيستدعويحيطبالملفاتالتيتمالو جإليهاوكافةعملياتالاختراقوالعبورأوالتجاوزخلالالإعدادللجريمة،وكافةالمعلوماتالمتعلقةبد خولأشخاصمواقعمعينةوتحديدمساراتتنقلاتهمفيهاالىغايةخروجهمنهذهالمواقع،وعليهفكلهذ هالمساراتتتضمنعادةآثارأوأدلةرقميةيمكنالاستدلالبهاعلىالجريمة.[2]

5- أنظمةكشفالاختراقIDS :
يكمندورهذهالفئةمنالبرامجفيمراقبةالعملياتالتيتحدثعلىالأجهزةالالكترونيةالمرتبطةبشبكةالانـ ترنتوتسجيلهافوروقوعهافيسجلاتخاصةداخلهذهالأجهزة.[3]

المطلب الثاني: القواعد الإجرائية الحديثة لجمع الدليل الرقمي

وعلىضوءماتقدم،كانلزاماعلىالمشرعالتدخلبقواعدإجرائيةجديدةأكثرفعاليةتحملمعهاطر قاإجرائيةمدعمةمنقبلالتقنيةذاتها،يمكنللجهاتالمكلفةبالبحثوالتحريعنالجريمةالالكترونيةالاعتـ مادعليهافيالكشفعنالمجرمالمعلوماتيوالوصولإلىالدليلالإثباتفيهابسرعةوسهولة، ومنه فقد تناولنا في هذا المطلب أهم الإجراءات المستحدثة لإستخلاص الدليل الرقمي وهي التسرب، وإعتراض المراسلات، والمراقبة الإلكترونية.

الفرع الأول: التسرب

تعتبرالجريمةالمعلوماتيةمنبينالجرائمالتييمكنفيهاللجوءإلىإجراءالتسربإذااقتضتذلكالضـ رورياتالتحريأوالتحقيقبشأنها، إذ هوتقنيةحديثةفيالتحريوالتحققعن بعض الجرائمفقدحددالمشرعالجزائرينطاقهذاالإجراءبالجرائمالمذكورةعلىسبيلالحصرفيالمادة 65 مكرر5منقانون الإج والتيمنبينهاالجرائمالماسةبأنظمةالمعالجةالآليةالمعطيات.

أولا: مفهوم التسرب

1- حسنطاهرداود،جرائمنظمالمعلومات،الطبعةالأولى،أكاديميةنايفالعربيةللعلومالأمنية،الرياض،س2000، ص230.
2- ممدوحعبدالحميدعبدالمطلب،مرجعسابق، ص15.
3- محمدبننصيرالسرحاني،مهاراتالتحقيقالجنائيالفنيفيجرائمالحاسوبوالانترنت "دراسة مسحيةعلى ضباطالشرطةبالمنطقة الشرقية " رسالةلنيلدرجةماجستيرفيالعلومالشرطية،كليةالدراساتالعليا،جامعةنايفالعربية للعلومالأمنية،الرياض، س004، ص84.

والتسربهوقيامضابطأوعونالشرطةالقضائيةتحتمسؤوليةضابطالشرطةالقضائيةالمكلفبتنسيقالعمليةبمراقبةالمشتبهفيارتكابهمجنايةأوجنحةبإيهامهمأنه فاعلمعهمأوشريك،ويمكنتجسيدعمليةالتسربفيالجرائمالالكترونيةكاشتاركضابط أوعونالشرطةفيمحادثاتغرفالدردشةأوحلقاتالنقاشحولدعارةالأطفال،أويدور حولقيامأحدهمباختراقشبكاتأوبثفيروسات،فيتخذالمتسربأسماءمستعارةويحاول الاستفادةحولكيفيةاقتحامالهاكرلموقعماحتىيتمكنوامناكتشافوضبط الجرائم.[1]

ويلاحظمنخلالماسبقذكرهأنالتسربعمليةمعقدةتتطلبأنيدخلالعونالمكلفبالعمليةفيإتصالبالأشخاصالمشتبهفيهمويربطمعهمعلاقاتمنأجلتحقيقالهدفالنهائيمنالعملية،وتتطلبعلىالخصوصالمشاركةالمباشرةفينشاطالخليةالإجراميةالتيتسربإليها.وعلىهديذلكفإنالتسربيرتكزعلىمبدئين:

-
المبدأالعاميستندعلىتقديمصورةعلىالوسطالمرادالتسربفيه،ويستوجبذلكمعرفةعموماتعنهذاالوسطمعتوثيقهذهالمعطيات.

-
والمبدأالخاصالذييستندعلىتعميقالتحريعنهذاالوسطونشاطاتهومميزاتهووسائلهوطبيعةالأشخاصالمنتمينإليه،ليتمبعدذلكدراسةالوظيفةالعملياتيةفيهذاالمجالبتوفيرالوسائلالبشريةوالتقنيةاللازمة.[2]

ثانيا: شروط التسرب

مناجلانتتمعمليةالتسرب بإتقان وسهولةمواكبة لمتابعةالجريمةالمعلوماتية،فقدأحاطهاالمشروعبجملةمنالشروط الشكلية والموضوعية نذكرها فيما يلي:

-أ-الشروط الشكلية: وتتجسد هذه الشروط فيما يلي:

- لابدأنيكون الإذن بالتسرب مكتوباوإلاكانهذاالإجراءباطلا،لأنالأصلفيالعملالإجرائيالكتابة، وهذا مانصته المادة 65 من قانون الإج الج،

-
ذكراسمالضابطالذيتتمعمليةالتسربتحتمسؤوليتهاوعونالشرطةالقضائيةباعتبارهمساعداله.

-
بالإضافةإلىتحديدالمدةالمطلوبةفيعمليةالتسربوالتييجبألاتتجاوزأربعةأشهرويمكنأنتجددحسبمقـ

1- خالدممدوحإبراهيم،فنالتحقيقالجنائيفيالجرائمالإلكترونية،مرجعسابق،ص316.
2- سعيداني نعيم، المرجع السابق، ص 175.

تضياتالتحريو التحقيقضمننفسالشروطالشكليةو الزمنية،وفينفسالوقتأجاز القانونللقاضيالذيأذن بها هذاالإجراءأنيأمرفيأيوقتيوقفهقبلإنقضاءالمدةالمحددة.[1].

-ب-الشروط الموضوعية: وتتمثل هذه الشروط في:

- الأولشرطالتسبيب،تضمنتهالمادة 65 مكرر 15 قانون الإج الج ،ويتمثلفيالمبرراتو الحججالتيأقنعتالجهاتالقضائيةالمختصةلمنحالإذنباجراءالتسرب،وكذاالدوا فعو الأسبابالتيجعلتضابطالشرطةالقضائيةيلجأإلىهذهالعمليةالمتمثلةعادةفيضرورةالتحقيقو التي تكونضمنموضوعطلبهالإذن.

- الثاني شرط تحديدنوعالجريمةو التييجبألاتخرجعنالجرائمالتيحددهاعلىسبيلالحصر في المادة65مكرر05 من نفس القانون فيسبعةأنواعوهي ": جرائمالمخدرات،الجريمةالمنظمةالعابرةللوطنية،جرائمتبيضالأموال،الجرائمالإرهابية،جر ائمالفساد،الجرائمالمتعلقةبالتشريعالخاصبالصرفو الجرائمالماسةبأنظمةالمعالجةالآليةللمعطي ات.

الفرع الثاني: إعتراض المراسلات

وتعد وسيلة من الوسائل الحديثة التي يستدل بها للوصول للدليل المتاح ويقصد بها:

اولا: مفهوم إعتراض المراسلاتاستحدثالمشرعالجزائرييموجبالقانونرقم 22/06، المؤرخ في 2006/12/20 المعدلو المتمملقانونالإجراءاتالجزائيةمنخلالالفصلالرابعالبابالثانيمنالكتابالأولتحتعنوانا عترا ضالمراسلاتوتسجيلالأصواتو التقاطالصور،وقدضمنهستة مواد المادة 65 مكرر5 إلى مكرر10،وتناولمنخلالهاالمقصودبهذاالإجراءوضماناتاستخدامه،وتتمثلفياعتراضكلالمراسلاتالتيتتمعنطريقوسائل الاتصالالسلكيةو اللاسلكيةالتييقصدبهاالتنصتالتيليفونيو هيتقنيةيتممنخلالها الاعتراضعنطريقربطخطهاتفيلشخصمامعاللجوءإلىتسجيلالمكالماتفي أشرطةممغنطة.[2]

و هذامايؤكدهالقانون04/09، المادة 02،فيتعريفهللإتصالاتالإلكترونيةعلىأنهاأنتراسلأو إرسالأو إستقبالعلاماتأو إشاراتأو كتاباتأو صورأو أصواتأو معلوماتمختلفةبواسطةأيوسيلةإلكترونية.

وبغضالنظرعنطبيعةالمراسلاتالسلكيةو اللاسلكيةفعمليةالاعتراضأو المراقبةتتمبواسط ةترتيباتتقنيةسريةيتموضعهادونعلمأوموافقةالمعنيين[3]،وذلكلغرضالتصنتو التقاطوتثبيتوبثوتسد

1- سعيداني نعيم، نفس المرجع، ص176.

2- شيخناجية،أساليبالبحثو التحريالمستحدثة فيقانون رقم 22/06، المعدلو المتمملقانونالاجراءاتالجزائية،المجلةالنقديةللعلومالسياسية،كليةالحقوقو العلوم السياسية،جامعةمولود معمري،تيزيوزو، 2013، ص294.

3- مصطفىمحمدموسى،المراقبةالالكترونيةعبرشبكةالانترنت،دراسةمقارنةبينالمراقبة الأمنيةالتقليديةو الالكترونية،الكتابالخامس،دارالكتبو الوثائقالقومية المصرية،القاهرة، 2003 ص180.

جيلالبياناتالمرسلةأوالمحادثاتالتيأجراهاالمشتبهفيهبصفةخاصةأوسريةفيأماكنخاصةأوعمومية،ومنثماستعمالهاكدليللمواجهةالمتهم.[1]

ولعلمنأهمالمراسلاتالالكترونيةالتييهتمالقائمينبالتحقيقبإخضاعهالعمليةالاعتراضوالمراقبةوالتيتمثلمصدراغنيالأدلةإثباتالجرائمالالكترونية،المراسلاتعبرالبريدالالكتروني،كونهذهالتقنيةمنأكثرالوسائلالحديثةاستخداماللاتصالعبرالانترنتومجالاخصباللربطبينالأشخاصفيمختلفأنحاءالعالمبسرعةفائقةودون
حواجز،فهوبمثابةنظامتبادلالرسائلوالصوروغيرهامنالموادالقابلةللإدخالالرقميفيصندوقالرسالة،أوالقابلةللتحميلالرقميبصفتهاملحقاتبالرسالة،كمايستخدمكمستودعلحفظالمستنداتوالأوراقوالمراسلاتالتيتتممعالجتهارقميافيصندوقخاصوشخصيللمستخدمولايمكنالدخولإليهبسهولةلأنهمحاطبحمايةفنية.[2]

وتجدرالإشارةفيهذاالصدد،الىأنالمراسلاتالتيتصلحلأنتكونمحلالإجراء الاعتراضأوالمراقبةلابدأنتتسمبالسريةوالخصوصية،ولا يكون هذاالأمرإلابتوفرهاعلىعنصرينجوهرين،يتعلقالأولبموضوعوفحوىالمراسلةفيحدذاتهاعندمايتضمنمعلوماتأوأفكارشخصيةوسريةفيماتخبربه،أماالعنصرالثانيفهوشخصييتعلقبإرادةالمرسلفيتحديدالمرسلإليهورغبتهفيعدمالسماحللغيربالاطلاععلىمضمونالمراسلة.[3]

ثانيا: شروط وضمانات المقررة لإعتراض المراسلات

يعدأسلوبإعتراضالمراسلات من الأساليب التي كشف الحقيقة وتزيل الغموض بالنسبة للجرائمالغامضةكالمتعلقةبالجرائمالمعلوماتية،فهويجسد إنتهاكالحرمةالحياةالخاصة الأفرادوإعتداءعلىسريةمراسلاتهموإتصالاتهمالتي أقرها لهم القانون، ولذلك فقد خصها المشرع بشروط لحماية أفرادها وتتمثل هذه الشروط فيما يلي:

-أ-الحصول على إذن السلطة القضائية: طبقاللمادة65مكرر05من قانون الإج الج، فإنه فإنهلايمكنلأي ضابط منالشرطةالقضائيةاللجوءإلىإجراءاعتراضالمراسلاتإلابعدأنيحصلعلىإذنمكتوبومسببمنطرفوكيلالجمهوريةأوقاضيالتحقيقفيحالةفتحتحقيققضائي،فالسلطةالقضائيةهيوحدهاالمختصةبإصدارهذاالإذنوهومايعدضمانةلازمةلمشروعيةهذاالإجراء.[4]

ولايكون الحصولعلىالإذنالمذكورةأعلاه لإتمامعمليةاعتراضالمراسلاتأوالمراقبة كافي بالغرض، بللابدأن تباشر هذهالعملياتتحتالرقابةالمباشرةللسلطاتالتيأذنتبها،وذلكمنخلالقيامضابطالشرطةالقضائيةالمأذونلهبإحاطتهاعلمابكلخطواتوتطورات

1- زيبحةزيدان،الجريمةالمعلوماتيةفيالتشريعالجزائريوالدولي،دارالهدى،الجزائر،س2011،ص157.
2- زيبحةزيدان،مرجعسابق،ص159.
3 - FERAL-SCHUHL Christiane « cyber droit- le droit a l'épreuve de l'internet »06 éme éditionDalloz، 2011/2012، p 999.
4- المادة 65 مكرر 05 من قانون الإج الج.

عملية الاعتراض و المراقبة و إخبارها بشكل دوري و مستمر عن عمليات و ضع الترتيبات التقنية لهذا الغرض، ساعة بداية و انتهاء هذه العمليات، علما أنه يرتبك لذلك في محاضر تقنية.[1]

و الجدير بالذكر هنا هو أنها لم تجانب إمكانية القيام بمراقبة الاتصالات الالكترونية في إطار التحريات و التحقيقات القضائية منا جلا لوصول لأدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء، فقد أجاز المشرع الجزائري كذلك تطويع هذه التقنية لغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما قررته المادة الرابعة من القانون 04/09، و هنا يصبح مفهوم الضرورة الملحة التي تستدعي القيام بإجراءات المراقبة الالكترونية مبهما و غير واضح، خاصة إذا تعلق الأمر بالجرائم التي تهدد النظام العام لان مصطلح النظام العام غير محدد المعالم و قد تنجر عنه إخلالات كبيرة منشأنها المساس بحرية الأفراد.[2]

-ب- تحديد طبيعة ومدة إعتراض المراسلات:

و التي ينبغي أن تتكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية، و إذا اكتشفت جرائم أخرى غير تلك الواردة ذكرها في الإذن فلا تبطل الإجراءات العارضة[3]، كذلك الجرائم المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة و الاقتصاد الوطني من القانون 04/09 المادة 04.

بالإضافة إلى أن المشرع إستوجب تحديد مدة الإعتراض و ذلك ما نصت عليه المادة 65 من قانون الإج ج، بحيث لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدر الإذن و فق المقتضيات لتحري و التحقيق.

الفرع الثالث: المراقبة الإلكترونية وحفظ المعطيات

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستعان بها في البحث و التقصي عن الجرائم سواء تلك التقليدية أو المستحدثة كجرائم الانترنت و هي ما يعرف بمراقبة الالكترونية.[4]

أولا: المقصود بالمراقبة الإلكترونية

المشرع الجزائري فلم يتطرق إلى تحديد ما المقصود بمراقبة الاتصالات الالكترونية إكتفى بذلك تحديد مفهوم الاتصالات الالكترونية فحسب، غير أن الفقه قد تصدى إلى هذه المهمة حيث عرف إجراء المراقبة الالكترونية على أنها مراقبة شبكة الاتصالات، أو هو عمل قانوني الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع المعطيات و معلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعتها يرتبط بالزمن لتحقيق غرض أمني

1- المادة 65 مكرر 09 من نفس القانون أعلاه.
2- براهيمي جمال، المرجع السابق، ص97.
3- المادة 65 مكرر 06 من قانون الإج الج.
4- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص197.

غرضأخروالملاحظأنالتقنيةهناهيالتقنيةالالكترونية التيهيمجموعةمنالبيانات الداخلةوفقالبرنامجموضوعمسبقاللحصولعلىالنتائجالمطلوبة.[1]

ويعتبرتكريسالمشرعلإجراءالمراقبةالإلكترونيةللإتصالاتخطوةجريئةمنهعلىإعتبارأنه ذاالإجراءيعدمنأخطرالإجراءاتفيإطارالنظامالإجرائيعبرالعالمالإفتراضيلكونهيمسمباشرةخصوصياتالإنسان، وذلكبالرغممنأنالبعضمنالفقهيرىأنالمراقبةلاتزالمحلنظرفيالقانونمنحيثضرورةالإلتزامبماهو مقررفيالقوانينوالضماناتالدستوريةللحقفيالخصوصية.[2]

شروط المراقبة الإلكترونية:

أحاطالمشرعهذاالإجراءبإعتبارهوسيلة إجرائيةللحصولعلىالدليلالرقميفيمجالالجريمةالمعلوماتيةبمجموعةمنالشروطأهمها:

-أنيتمتنفيذهذاالإجراءتحتسلطةالقضاءوبإذنمنه،وهوماكرستهالمادةالرابعةمن القانونالمتضمنالوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلامو الإتصالبنصهاعلىأنهلايجوز إجراءعملياتالمراقبةإلابإذنمنالسلطةالقضائيةالمختصة.

-أنتكونهناكضرورةتتطلبهذاالإجراءوتتحققهذهالضرورةعندمايكونمنالصعب الوصولإلىنتيجةتهممجرياتالتحريأوالتحقيقدونااللجوءإلىالمراقبةالإلكترونيةوهوماأكد عليهالمشرعفيالفقرةج" "منالمادةالرابعةفي القانون 09/04[3].

ثانيا: حفظ المعطيات

يقصد بالحفظعلىالمعطياتالالكترونيةبأنهتقيامممزوديخدماتالاتصالبتجميعالمعطياتالمعلوماتيةالتيتقومب التعرفعلىمستعمليالخدمةوحفظهاوحيازتهافيأرشيف،وذلكبوضعهافيترتيبمعينوالاحتفاظبهافيا لمستقبلقصدتمكينجهاتالاستدلالمن الاستفادةمنهاواستعمالهالأغراضالتحقيق.[4]

ويقصدبمزوميالخدماتأيكيانعاماوخاصيقدملمستعمليخدماتهاالقدرةعلىالاتصالبواسطةمنظومةمعلوماتيةاونظاماتصالاتوأيكياناخريقومبمعالجةاوتخزينمعطياتمعلوماتيةلفائدةخدمةالاتصالالمذكورةاومستعمليها.[5]

وينبغيالتنويهفيهذاالإطارإلىأنعمليةالحفظهنالاتخصكلالمعطياتالالكترونيةبمختلفنماذجه ،إنماتخصمعطياتالمرورفقطأوكمايسميهاالبعضحركةالسير،التيعرفتهاالمادةالأولىفقرة" د "

1- مصطفىموسى،المراقبةالالكترونيةعبرشبكةالانترنت، دراسةمقارنةبينالمراقبةالأمنية التقليدية،دارالكتب، والوثائقالقوميةالمصرية،ط1 ،مصر،س2000،ص205.

2- سعيداني نعيم، المرجع السابق، ص184.

3 سعيداني نعيم، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، س2013، ص 185.

4- بوكر رشيدة، المرجع السابق، ص448.

5- المادة12، من الق 04/09.

مناتفاقيةبودابستبأنها: "
صنفمنبياناتالحاسبالتيتشكلمحلالنظامقانونيمحدد،إذيتمتوالدهذهالمعطياتمنالحواسيبعبرتسلسل حركةالاتصالاتلتحديدمسلكالاتصالاتمنمصدرهاإلىالجهةالمقصودة.وعرفهاكذلكالمشرعالجزائريفيالمادة(02) الفقرةالأخيرةمنالقانونرقم 04/09بأنها "
أيةمعطياتمتعلقةبالاتصالاتعنطريقمنظومةمعلوماتيةتنتجهاهذهالأخيرةباعتبارهاجزءافيحلقة الاتصالات،توضّحمصدرالاتصال،الوجهةالمرسلة
إليها،والطريقالذييسلكه،ووقتوتاريخوحجومدةالاتصالونوعالخدمة".[1]

ومنبينمعطياتالمرورالتييتنبغيعلىمقدميالخدماتالتحفظعليهابطلبمن السلطاتالقضائيةالمختصةلأغراضالتحقيق، هي:

- المعطياتالتيتسمحبالتعرفعلىمستعمليالخدمة.

-
المعطياتالمتعلقةبالتجهيزاتالطرفيةالمستعملةللاتصال:كرقمالتسلسليلجهازالاتصال،ونوعه.

- الخصائصالتقنيةوكذاتاريخووقتومدةالاتصال.

-المعطياتالمتعلقةبالخدماتالتكميليةالمطلوبةأوالمستعملةومقدميها.

- المعطياتالتيتسمحبالتعرفعلىالمرسلوالمرسلإليهم:
كأرقامالهاتفمثلااوعناوينبروتوكولالانترنت،تحديدمكانهم.[2]

وعليه فعند
إرتباطمعطياتالمرورباكثرمنمقدمخدمةفالحفظالعاجللهذهالمعطياتيتممنخلالهمجميعا،سواءبناء علىأمرمنفصللكلمقدمخدمةعلىانفراد
أوأمرواحديشملهمجميعايتمإخطارهمبهبالتعاقب،أوبناءعلىأمريضمّكلمقدميالخدمات،ثميطلبمن كلمقدميخدمةيصلهالأمربالحفظ،أنيقومبإخطارمنيليه بفحوىهذاالأمر.[3]

1- براهيمي جمال، المرجع السابق، ص102.
2- براهيمي جمال، نفس المرجع، ص103.
3- هلاليعبدأللاهأحمد،الجوانبالموضوعيةوالإجرائيةلجرائمالمعلوماتية.،مرجعسابق،ص208

ملخص الفصل:

في نهاية هذا الفصل، يتبين لنا أن موضوع الدراسة فيه كان متمحور حول الطبيعة القانونية للدليلفي الجرائم المعلوماتية الذي يتم استخلاصهمنالبيئةالالكترونيةوالرقمية،إذ أن النظمالقانونيةتدرجهذا الدليل كأداةإثباتلهاقيمةقانونيةوحجيةفيالإثبات بحيث قمنا بعرض مفهوم هذا الدليل وأثر القيمة القانونية له، وعليه توصلنا أن عملية الإثبات الجنائي للجرائم المعلوماتية ترتكز على وجود الدليل الرقمي بإعتباره الوسيلة الرئيسية المعمول بها في هذا النوع من الجرائم،وهذا الدليل الرقمي يتمتع بدورإيجابي من حيثتقديرالقيمةالقانونيةله وخضوعهللسلطةالتقديرية من قبل القاضي الجنائي،شأنهفيذلكشأنباقيالأدلة التقليدية،

بالإضافةإلى
الإجراءاتالعامةالتيتخضعلهاالجرائمالمعلوماتيةوالتيتشتركفيهامعالجرائمالتقليدية نوعاما، فقد قام المشرعبتوسيعنطاقتطبيقإجراءاتالتحقيقالتقليدية إلى إجراءات تكون متطورة وتتناسب في التحقيق فيالجرائمالمعلوماتية والتي تم النص عليها في قانون الإج الج، بالإضافة إلى القانون 04/09 المتضمنالقواعدالخاصةللوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالومكافحته.

وعليه سلطنا الضوء في المبحث الثاني على أهم الإجراءات البحث والتحري داخل المنظومة المعلوماتية بحيث قسمناها إلىإجراءاتتقليدية تتجسد في المعاينة االتقنية،التفتيش الإلكتروني وضبط الدليل، والخبرة، يليه الإجراءات المستحدثة وهي التسرب وإعتراض المراسلات والمراقبة الإلكترونية،

بحيث أن هذه الوسائل كان لها الريادة في المساهمة في الكشف عن الحقيقة في الجرائم المعلوماتية والمشكلات التيتواجهعمليةالبحثوالتحقيق فيها.

الخاتمة

الخاتمة:

أمام التطور التكنولوجي الذي يعيشه العالم اليوم فقد أدى ذلك إلى ظهور ما يعرف بالإجرام المعلوماتي، وهذا نتيجة الإستخدام السلبي للمعلوماتية فهذه الأخيرة كان لها الأثر البالغ في إحداث عدة أضرار مست بأمن الدولة ومؤسساتها وحرية الأفراد من جهة أخرى.

ولأن الحماية الفنية لازمة لتدارك هذا النوع من الجرائم المستحدث، وأن التحقيق في الجريمة المعلوماتية يعتمد على الذكاء والفطنة بالبحث عن الدليل لإثبات الجريمة عموما فإنه كان لزاما تخصيص أجهزة مكلفة بالبحث والتحري فيها وهذا ما شرعته التشريعات المقارنة إضافة إلى المشرع الجزائري.

وبالحديث عن الآليات الإجرائي للتحري عن الدليلفيالجريمةالمعلوماتية، فطبيعة هذا الدليل الرقمي يكمن في أنه ذوقيمةقانونية أمام التحقيق في الجرائم الإلكترونية،التيتتوقففعلىمنبرين
أساسيتين،الأولىهيمشروعيةالدليل،والثانيةهيحجيتهعلىالوقائعالمراإثباتها،
واستخلصنا أيضاأنمسألةقبولالدليلالالكترونيإنماتخضعلمنطقتقديرالقاضيالجزائي،الذييتمتعبد ورايجابيفيمناقشةالقيمةالقانونيةللدليلالالكترونيقبلأنيطمئنإليه.

وإجتنابا
لإفلاتالمجرمالمعلوماتيمنالمتابعةالجزائيةوالعقاب،بادرالمشرعفيالكثيرمنالدولإلىإعادةالنظر فيبعضالقواعدالإجرائيةالمتعلقةباستخلاصالدليلكالتفتيش والضبطوجعلهاصائغةالاستعمالفيم جالالبيئةالرقميةالإلكترونية،فضلاعناستحداثقواعدإجرائيةأخرىتتلاءممعالطبيعةالخاصةالتيي تميزبهاهذاالنوعمنالجرائم،كالمراقبةالإلكترونيةواعتراضالمراسلاتوالتسربالالكتروني،وهو ماأقدمعليهالمشرعالجزائريمنخلال قانون الإجراءات الجزائية، والقانون 04/09 المتعلق بالقواعدالخاصةبالوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالومكافحتها.

وتوصلنا في الاخير الى مجموعة من النتائج والتوصيات سنبينها في مايلى:

النتائج:

ومن خلال موضوعنا توصلنا لمجموعة من النتائج وهي:

- توصلنا إلى التطور التكنولوجي لعب دورا في تبلور نوع جديد من الجرائم المستحدثة التي تنفرد بخصوصية عن غيرها من الجرائم وهي الجرائم المعلوماتية.

- توصلنا إلى الجريمة المعلوماتية لها طبيعة خاصة تميزها ومرتكبيها، وأن دوافع ارتكاب هذه الجريمة تختلف منمنشخصلأخر،فقدتكوندوافعشخصيةهدفهاتحقيقمصلحةخاصة،وقدتكونخارجيةبهدفالانتقام
.

- توصلت أن خصوصية هذا النوع من الجرائم جعل من التشريعات الداخلية والعالمية للإلتفاف لوضع أجهزة مكلفة بالتحقيق في هذا النوع المستحدث من الجرائم.

-
منأهممميزاتجرائمالاعتداءعلىنظمالمعالجةالآليةللمعطيات،أنهاتنصبعلىمحلمننوعخاصيختلف تماماعلىمحلالجرائمالتقليديةفهذهالجرائمتستهدفالمساس بالمعلومات.

- إلى ان قاضي التحقيق أثناء تحقيقه في الجرائم المعلوماتية يجب عليه أن يستثني بمجموعة من المؤهلات التي تجعله يقوم بعمله بمنبر سليم.

- إلى أنالقاضيالجزائي يتمتعبدورإيجابيمنحيثتقديرهالقيمةالقانونيةللدليلالرقميوخضوعهللسلطةالتقديرية.

-توصلت إلى أن هناك إجراءات مشتركة مابين الجرائم التقليدية والجرائم المعلوماتية كالمعاينة على مسرح الجريمة.

- توجد معوقات تمسالتحقيق بالنسبةللجرائمالإلكترونية،والمرتبطة بالدليل الرقمي هي سهولة محو هذا الدليل أو تدميره في زمن قصير جدا،وذلك بإستخدام استخداماالتقنيةالعلميةفيإخفائهأوإتلافهوقديتمذلكطريقالتشفيروكلماتالمرورالسريةواستخداماال برامجالفيروسية.

التوصيات:

توصلنا إلى مجموعة من الإقتراحات نوجزها في مايلي:

- فعلىالرغممنانتشارالوسائلالإلكترونيةفيهذهالدول،إلاأنالكثيرمنتشريعاتهالمتمسها هذا الإنتشار، كان من الأفضل مديدالتعديللكيتقوىعلىحماية القانونية الشاملةلمصالح الدولة والمؤسسات وحرية الأفراد جراء الصعوبات التوصل للتصدي لإنقاص ظاهرة الإجرام المعلوماتي.

- دعوة المشرع الجزائري إلى تخصيص تشريع مستقل يتضمن الطبيعة الخاصة للجريمة المعلوماتية ووضع إجراءات تتناسق مع طبيعة هذا النمط من الجرائم.

- إعادة النظر في وضع قانون خاص متعلق بعقوبات تتلاءم والجريمة المعلوماتية، وهذا لإزالة القصور والنقص الناجم عن تدارك هذه الجريمة.

- بماأنالمجرماالمعلوماتييعتمدبالدرجةالأولىعلىوسائل تقنيةالحديثةولانالإجراءاتالتقليديةيبادرها نقص فيمكافحةهذهالجرائمفينبغيعلىالمشرعوضعإجراءاتحديثة اخريتعتمدعلىذاتالوسائلالمستخدمةفيالجريمةللكشفعنهاوتتبع مرتكبيها.

- تدريسمواد تنص علىالأنظمةالمعلوماتيةوالجرائمالتيقد تتفرعمنهابشكلرسمي فيكلياتالحقوقوالمعاهدالقضائية.

قائمة المصادر والمراجع

أولا: قائمة المصادر

القوانين:

1. الأمر رقم 155/66 مؤرخ في 08 يونيو1966 يتضمن قانون الإجراءات الجزائية، معدل ومتتمم لاسيما بالقانون 07/17 المؤرخ في 27 مارس سنة2017.
2. القانون رقم 15/04، الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66، الصادر في 08جوان 1966، المتضمن قانونالعقوبات،ج ر العدد 71.
3. القانون 04/09،الصادر في5 أوت 2009 يتضمن القواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر، العدد 47

ثانيا: قائمة المراجع

الكتب:

4. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر،ط10، سنة2011.
5. أحمد أبو قاسم،الدليلالجنائيالماديودورهفيإثباتجرائمالحدودوالقصاص،المركز العربيللدراسات الأمنيةوالتدريب،الرياض، سنة1993 .
6. أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة،سنة 2015.
7. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنيت، دار النشر مكتبة الوفاء القانونية ،الإسكندرية ،طبعة1، سنة2011.
8. جميلعبدالباقيالصغير،أدلةالإثباتالجنائيوالتكنولوجيةالحديثة،دار النهضةالعربية،القاهرة، سنة2002 .
9. حساممحمدنبيلالشنراقي،الجرائمالمعلوماتية- دراستةتطبيقيةمقارنةعلىجرائمالاعتداءعلىالتوقيعالالكتروني، دارالكتبالقانونية،القاهرة، 2013 .
10. حسن الجوخندار، التحقيق الإبتدائي في أصول المحاكمات الجزائية، دار الثقافة، عمان، ط1، 2008.
11. حسنطاهرداود،جرائمنظمالمعلومات،الطبعةالأولى،أكاديميةنايفالعربيةللعلوم الأمنية،الرياض،س2000.
12. حسينبنسعيدبنسيفالغافري،السياسةالجنائيةفيمواجهةجرائمالانترنت،رسالةلنيل شهادةالدكتورارهفيالقانون،كليةالحقوق،جامعةعينالشمس،القاهرة، 2005 .
13. خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، 2018،
14. خالدعياد الحلبي،إجراءاتالتحريوالتحقيقفيجرائمالحاسوبوالانترنت،دارالثقافةللنشروالتوزيع،عمان، س2011.

15. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011.
16. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولي
17. خالدممدوحإبراهيم،فنالتحقيقالجنائيفيالجرائمالالكترونية،دارالفكرالجامعي،إسكندرية،س 2009
18. رشيدة بوكر جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية الطبعة الأولى, سنة2012.
19. زيبحةزيدان،الجريمةالمعلوماتيةفيالتشريعالجزائريوالدولي،دارالهدى،الجزائر،س2011،
20. شيخناجية،أساليبالبحثوالتحريالمستحدثة فيقانون رقم 22/06، المعدلوالمتممللقانونالاجراءاتالجزائية،المجلةالنقديةللعلومالسياسية،كليةالحقوقوالعلوم السياسية،جامعةمولود معمري،تيزيوزو،سنة2013,
21. طارقإبراهيمالدسوقيعطية،الأمنالمعلوماتيفيالنظامالقانونيلحمايةالمعلوماتيةدونطبعة،دارالجامعة الجديدة،مصر.
22. طارقأحمدماهرزغلول،شرحقانونالإج الجعماني،الجزءالثاني، المحاكمةوطرقالطعنفي الأحكام، طبعة 1،دارالكتابالجامعي، سنة2016.
23. طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، دار صادر للمنشورات الحقوقية، ط1، بيروت، 2001.
24. عادلعبداللهخميسالمعمري، التفتيشفيالجارئمالمعلوماتية،مجلةالفكرالشرطي، مجلد 22،العدد86، صادر عنمركزبحوثالشرطة،القيادةالعامةلشرطةالشارقة،الإماراتالعربيةالمتحدة،سنة 2013.
25. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، سنة 2010.
26. عبدالعظيموزير،شرحقانونالعقوباتالقسمالخاصجرائمالإعتداءعلىالأموالط1، دارالنهضةالعربيةالقاهرة، سنة1993.
27. عبدالفتاحبيوميحجازي .الاثباتفيجرائمالكمبيوترو الانترنت .دارالكتبالقانونية . مصر، سنة2003.
28. عبدالفتاحبيوميحجازي، مبادئالإجراءاتالجنائيةفيجرائمالكمبيوترو الانترنت،دارالفكرالجامعي،الإسكندرية، س. 2006 .
29. عبد الفتاح بيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي الإسكندرية، ط1، سنة 2006.
30. عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، سنة2003.

31. عبدالناصرمحمدمحمودفرغلي،الإثباتالجنائيبالأدلةالرقميةمنالناحيتينالقانونية والفنية، دراسةمقدمة للمؤتمرالعربيالأوللعلومالأدلةالجنائيةوالطبالشرعي،المنظمبالرياض،فيالفترةالممتدة بين 12 و 14 نوفمبر، سنة2008.
32. عفيفي كامل عفيفي، جرائمالكمبيوتروحقوقالمؤلفوالمصنفاتالفنيةودورالشرطةوالقانون،دراسةمقارنة،منشوراتالحلبي،دمشق،2007 .
33. علي حسين محمد الطوالبة، ص190،مشروعيةالدليلالرقميالمستمدمنالتفتيش الجنائي، س2009 .
34. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت،
35. غازيعبدالرحمنهيانالرشيد،الحمايةالقانونيةمنجرائمالمعلوماتية،رسالةلنيلدرجةدكتوراه فيالقانون،كلية الحقوق،الجامعةالإسلاميةفيلبنان،بيروت، س2004،
36. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، طبعة01، دار الثقافة للنشر والتوزيع، الاردن, سنة2006.
37. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات التجارية والمدنية، ط1، دار الفكر والقانون، مصر، سنة2010،
38. فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار النمطبوعات الجامعية، الاسكندرية، سنة2006.
39. فيصلحسنحامد،التحدياتالتيتواجهالأجهزةالأمنيةفيالمملكةالعربيةالسعودية،المجلة العربيةللدراساتالأمنيةوالتدريب،العدد 63 الرياض،سنة 2015.
40. كامل فريد السالك، الجريمة المعلوماتية ندوة التنمية ومجتمع المعلوماتية، حلب،23/21 تشرين الأول, سنة 2000.
41. ماجد ياقوت، أصول التحقيق، دراسة مقارنة، ط3، منشأة المعارف، الاسكندرية
42. محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، طبعة 1، دار الثقافة للنشر والتوزيع، عمان, سنة 2000.
43. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة،سنة 1994.
44. محمد علي الكيك، السلطة التقديرية للقاضي الجنائي، دار المطبوعات الجامعية، مصر، سنة2007.
45. محمد مرواني، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، ديوان المطبوعات الجامعية للنشر، الجزائر, سنة1999.
46. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ط1، مطابع الشرطة، مصر, سنة 2008.
47. ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية عبر جرائم الكمبيوتر، مركز شرطة دبي, سنة 2005.
48. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دون طبعة، دار الكتب القانونية، مصر. سنة 2006.

49. مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر والتوزيع، الجزائر،دون سنة النشر.
50. مولود ديدان، قانون الاجراءات الجزائية، الأمر 02/11، دار بلقيس ، الجزائر،
51. نبيلة هبة محمد هروال، الجوانب الاجرائية لجرائم الانترنات في مرحلة جمع الاستدلالات، ط1، دار الفكر الجامعي الاسكندرية،
52. هدى حامد قشقوش، الحماية الجنائي للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000،.
53. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط1، آسيوط مصر، 1999.
54. هلالي عبد أللاه أحمد، النظرية العامة للإثبات، دار النهضة العربية للنشر، القاهرة.
55. ياسرمحمدالكومىمحمودأبوحطب،الحمايةالجنائيةوالأمنيةللتوقيعالإلكتروني، منشاة المعارف، الإسكندرية، سنة2014.

ثالثا: الرسائل والمذكرات

أ- المذكرات

1. أحمدبنزايدجوهرالحسنالمهدي،تفتيشالحاسبالآليوضماناتالمتهم،مذكرةلنيلدرجةماجستيرفيالقانون كليةالحقوق،جامعةالقاهرة، سنة2009
2. أحمد مسعود مريم، آليات مكافحة تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير، جامعة قاصدي مرباح، ورقلة، كلية الحقوق، تخصص قانون جنائي،سنة 2013.
3. براهيمي جمال, التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الدكتوراه، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، سنة2018.
4. حمزة بن عقون السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية تخصص علم الإجرام والعقاب جامعة باتنة, سنة 2012.
5. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لحضر،باتنة، كلية الحقوق والعلوم السياسية، سنة 2013.
6. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، سنة2011.
7. عمر بن إبراهيم بن خماد العمر، إجراءات الشهادة في مرحلتي الإستدلال والتحقيق الإبتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، سنة 2007.

8. فايزمحمداراجحغلاب،الجرائمالمعلوماتيةفيالقانونالجزائريواليمني،أطروحةلنيلشهادةالدكتوراهفيالقانون،
فرعالقانونالجنائيوالعلومالجنائية،كليةالحقوق،جامعةالجزائر1، الجزائر، س2011
9. محمدبننصيرالسرحاني،مهاراتالتحقيقالجنائيالفنيفيجرائمالحاسوبوالانترنت "دراسة مسحيةعلى ضباطالشرطةبالمنطقة الشرقية " رسالةلنيلدرجةماجستيرفيالعلومالشرطية،كليةالدراساتالعليا،جامعةنايفالعربية للعلومالأمنية،الرياض، سنة 2004.
10. محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في الجرائم الحاسوب والأنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض , سنة2004.

ب- الرسائل العلمية:

1. توفيق شمبور وآخرون، السرية المصرفية، أبحاث ومناقشات الندوة التي نظمها اتحاد المصارف العربية، لبنان،سنة 1993.
2. راشدبنحمدالبلوشي، ورقةعملحولالدليلفيالجريمةالمعلوماتية،مقدمةالىالمؤتمر الدوليحول (حمايةالمعلوماتوالخصوصيةفيقانونالانترنت) برعايةالجمعيةالدولية لمكافحةالاجرامبفرنسا، سنة2008.
3. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، بحث مقدم للمؤتمر المغاربي الأول حول المعلوماتية، المنعقد في 2009/10/28، الأكاديمية للدراسات العليا، طرابلس.
4. عبد الناصر محمد محمود فرقي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، جامعة نايف للعلوم الأمنية، الرياض، سنة2007.
5. علي محمود علي حمودة، الأدلةالمحصلةمنالوسائلالإلكترونية فيإطار نظريةالإثباتلجنائي، بحثمقدمإلىالمؤتمرالعلميالاولحول الجوانبالقانونيةوالأمنيةللعملياتالإلكترونية،دبي،الإمارات العربيةالمتحدة،سنة2003.
6. مصطفىمحمدموسى،المراقبةالالكترونيةعبرشبكةالانترنت،دراسةمقارنةبينالمراقبة الأمنيةالتقليديةوالالكترونية،الكتابالخامس،دارالكتبوالوثائقالقوميةالمصرية،القاهرة، 2003.
7. ممدوحعبدالحميدعبدالمطلب،زبيدةمحمدجاسموعبداللهعبدالعزيز،نموذجمقترحلقواعد اعتمادالدليل الرقميللإثباتفيالجرائمعبر الكمبيوتر،مؤتمرالأعمالالمصرفيةالإلكترونيةبينالشريعةوالقانون،المجلدالخامس، المنعقدبدبيفيالفترةمن 12/10 ماي 2003.

الفهرس

الفهرس

ملخص المذكرة

خلاصة الموضوع

تعدالجرائمالالكترونيةمنالأنماطالإجرامية الجديدةالتيأفرزتهاتكنولوجياتالإعلام والاتصالالحديثة،فهيتختلفتماماعنباقي الجرائمالتقليدية،في طبيعتها المتميزة أنماط أو أركانها والأجهزة المخولة بالتحقيق فيها إذ لم تكتفيالتشريعاتالمقارنةوالتشريعالجزائريبتجريمأعمالالإلكترونيةوقانون العقوباتوقانونالإجراءاتوالقوانينالخاصةوالمتعلقةبهابلأقرتأجهزةخاصةلمتابعتها ومكافحتها، بلإضافةأن إختلافأساليبارتكابها لوجودها في بيئة رقمية أدت لإرساء طابع خاص لإستحداث إجراءات للبحث والتحري عن هذه الجرائم، ورغمالخطورة البالغة لهذه الجريمة وتأثيرها السلبي في المجتمع التي أثارت جدلا حولاعتباركل شخصمعنيبالأخطاروالعواقبالتييخلفها عن إرتكابه لهذاالسلوكالإجرامي فهي لمتتخلفعن التصديلهاوكافحتهابأحدثالوسائل التقنية.

Summary

Information crimes are one of the new types of criminal offences created by modern information and communication technologies. They are quite different in nature from other minor crimes. The types of elements and the bodies authorized to investigate them are distinct.

Despite the extreme seriousness of this crime and its negative impact on society, which has given rise to debate about the fact that everyone is concerned with the dangers and consequences of such criminal behavior, it has not failed to respond to and combat it by the latest technical means.