وزارة التعليم العالي والبحث العلمي
جامعة الشهيد حمه لخضر . الوادي
كلية الحقوق والعلوم السياسية
قسم الحقوق

إجراءات التحري في الجرائم الإلكترونية

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر ل.م.د في الحقوق

تخصص: قانون قضائي مهني

إعداد الطالبان:

عماد يوسف

لزهر ضربان

لجنة المناقشة:

الاسم واللقب	المؤسسة	الصفة
العايبي سعيدة	جامعة الشهيد حمه لخضر . الوادي	رئيسا
جعفر عرارم	جامعة الشهيد حمه لخضر . الوادي	مشرفا ومقررا
عمامرة مباركة	جامعة الشهيد حمه لخضر . الوادي	مناقشا

السنة الجامعية: 2023/2022

وزارة التعليم العالي والبحث العلمي
جامعة الشهيد حمه لخضر . الوادي
كلية الحقوق والعلوم السياسية
قسم الحقوق

إجراءات التحري في الجرائم الإلكترونية

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر ل.م.د في الحقوق

تخصص: قانون قضائي مهني

إعداد الطالبان:

عماد يوسف

لزهر ضربان

لجنة المناقشة:

الاسم واللقب	المؤسسة	الصفة
العايبي سعيدة	جامعة الشهيد حمه لخضر . الوادي	رئيسا
جعفر عرارم	جامعة الشهيد حمه لخضر . الوادي	مشرفا ومقررا
عمامرة مباركة	جامعة الشهيد حمه لخضر . الوادي	مناقشا

السنة الجامعية: 2023/2022

بسم الله الرحمن الرحيم

وقل رب زدني علما

الإهداء

الحمد الله وكفي والصلاة علي الحبيب المصطفي

وأهله ومن وفي الحمد الله الذي وفقني في المسار الدراسي

وأنار لي طريق النجاح واهدي ثمرة عملي هدا :

إلي الوالدين الكريمين أطال الله في عمرهما وأدام لهما

الصحة والعفاف وهم من كانوا سندا ودعما لي في هده الحياة

والي زوجتي المساندة لي وأولادي (الصالح و رتيل) حفظهم الله

أخي ودم عروقي عثمان وعائلته وأبنائه (عقيلة النور و احمد) حفظهم الله

والي جميع أخواتي وردة ومسعودة ونادية وفهيمة كل منهم وعائلته

والتوأم (فاطمة وفاطمة)

وابن أختي عبد الحفيظ الذي هو بمثابة أخي الصغير أنار الله دربه ووفقه في

الحياة الدراسية

والي كل من كان لهم اثر في حياتي

عماد

الإهداء

بسم الله الرحمان الرحيم

"قل اعملوا فسيرى الله أعمالكم و رسوله و المؤمنون"

صدق الله العظيم.

الحمد لله الذي هداني بهديه وانار بصيرتي بنوره وبعد :

اهدي ثمرة جهدي هذا إلى من علمني معنى الإخلاص والوفاء إلى الذي علمني الكفاح والمثابرة ولولاه لما بلغت ان أشرب ينبوع العلم والمعرفة.

إلى الذي كبرني في طاعة الله وطلب العلم ولم يبخل عليا بشيء أبي العزيز"

عمر"

حفظه الله وأطال عمره .

إلى أروع من في الوجود إلى الصدر الحنون الذي يسعى حنانه وحبه الكون كله، إلى التي أدين لها بعمري إلى بحر الحنان الذي لا ينتهي إلى التي كان دعائها سندا لي إلى التي ترعرعت بين أحضانها ارتويت من ينبوع عطفها وحنانها إلى التي لها الفضل في تربيتي وتعليمي إلى شمعة التي تضئ حياتي أمي الغالية حفظها الله وباركها وأطال في عمرها .

إلى شريكة حياتي ونصفي الثاني الى من دفعني لإتمام دراستي

زوجتي العزيزة

إلى من قاسموني وشاركوني أفراحي وأحزاني

إخوتي الكرام

الزاهرا

الشكر و التقدير

قال رسول الله صل الله عليه وسلم ((من لم يشكر الناس لم يشكر الله ومن أهدي إليكم معروفا فكافئوه فإن لم تستطيعوا فأدعو له))

الحمد الله الذي وهبنا السداد ومنحنا 7الثبات وأعاننا علي إتمام هدا العمل بعد أن سافرنا لنضع النقاط علي الحروف ونكتشف ما وراء ستار العلم والمعرفة فها هي ثمار علمنا قد انبتت وحان قطفها هده الكلمات المبعثرة نهمس بها في أدان من سيفتح هده المذكرة لينهل معها ما يشاء ويشتهي يرفض ويبتغي .

هي أيضا كلمات شكر إلي كل من حثنا وغرس فينا الأمل والإرادة

إلي كل من الأساتد المشرف وجميع الأساتدة

إلي كل الزملاء والأصدقاء الأحباب

إلي جميع من ساعدنا من قريب أو بعيد

مـــــقـــــدمـــــــة

إن التطور المتسارع الذي يشهده العالم في ظل الثورة المعلوماتية الحديثة التي تلت الثورة الصناعية و التي فرضت الاعتماد على تقنيات تكنولوجية استعملها الإنسان في مجالات العمل والحياة فأصبح بذلك العالم عبارة عن قرية صغيرة يمكن التواصل بين مجتمعاته بلا حدود جغرافية و لا زمنية مما ترك آثاراً ايجابية وقفزة حضارية نوعية مست مختلف القطاعات واستطاعت أن تقدم خدمات جليلة للأمم والشعوب.

إلا أن هذا الجانب الايجابي للتكنولوجيا المعلوماتية أفرز معه بعض الانعكاسات السلبية التي تولدت نتيجة إساءة استخدام الأنظمة المعلوماتية ، واستغلالها على نحو غير شرعي قصد الإضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط و صور مستحدثة من الجرائم اصطلح الفقه على تسميتها بالجرائم المعلوماتية.

والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا، فهي أيضا معينة بالمكافحة فكان لا بد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجريمة المعلوماتية، ومنها إجراءات تطبق فقط على الجريمة المعلوماتية فقط، والتي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحته في القانون رقم 09/04 المؤرخ في أوت 2009.

1-أهمية البحث:

تكمن أهمية البحث أساسا في كون الجرائم الالكترونية جرائم جديدة، بالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات لتي لم تنل حقها من البحث والتحقيق والمحاكمة على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

بالإضافة إلى كون الجرائم الالكترونية حديثة النشأة، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال، والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات، إذ تجعل التعاملات معها صعبا ومعقدا، مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها.

2-أسباب اختيار الموضوع:

أ-الأسباب الذاتية :

*تكمن في اهتمامنا بمجال الجريمة الالكترونية ، وما يلقاها من جرائم، وكذا من إجراءات.

*أنه موضوع يستحق البحث ويثير الفضول.

*موضوع حيوي وجديد لأنه من الجرائم المستحدثة.

*رغبة وميول شخصي لدراسة الموضوع

ب-الأسباب الموضوعية:

*تسليط الضوء على الموضوع من خلال التعرف على مفهومه والوقوف على أسباب ارتكاب هذا النوع من الجرائم.

*التعمق في تفاصيل الجرائم المعلوماتية وما يحيط بها من اعتداء على نظم المعلوماتية ومعالجة الأنظمة الآلية وغيرها.

*التعمق في تفاصيل الجرائم المعلوماتية وما يحيط بها من اعتداء على نظم المعلوماتية ومعالجة الأنظمة الآلية وغيرها.

*التعرف على القواعد الإجرائية والجزاءات التأديبية المترتبة عن ارتكاب الجريمة الالكترونية.

ونظراً لحداثة الجرائم الالكترونية واتصالها بجانب تقني و فني بحث يتمثل في النظام المعلوماتي بشقيه المادي والمعنوي فقد اختلفت و تباينت الاجتهادات الفقهية في تعريف الجريمة الالكترونية وكذا حصر أنواعها وتحديد طبيعتها القانونية ، مما أصبح يشكل تحدياً أمام

القواعد القانونية التقليدية في مواجهة هذا النوع من الجرائم المرتبط بتكنولوجيا المعلومات ، ومن هذا المنطلق يمكن أن نطرح الإشكالية التالية:

ماهي الضوابط والإجراءات التي سنها المشرع الجزائري للكشف عن الجرائم الالكترونية؟

ولقد اعتمدنا في دراستنا على منهجين هما:

- **المنهج المقارن:** وذلك من خلال مقارنة المشرع الجزائري بالمشرعين الفرنسي والمصري وذلك بقدر ما تستدعيه طبيعة الدراسة، إذ لا تخلو أي دراسة قانونية في البحوث الجامعية على الاعتماد على المقارنة.
- **المنهج التحليلي:** من خلال تحليل بعض القرارات والأحكام القضائية والنصوص القانونية.

حيث قسم هذا البحث الى فصلين وكل فصل الى مبحثين وكل مبحث الى ثلاث مطالب.

ففي الفصل الاول تحدثنا عن الاطار المفاهيمي للجرائم الالكترونية والذي انبثق منه مبحثين ولكل مبحث ثلاث مطالب حيث تعنون المبحث الأول بمفهوم الجريمة الالكترونية وبدوه تجزء الى ثلاث مطالب حيث جاء في المطلب الأول تعريف الجريمة الالكترونية أما في المطلب الثاني فكان تحت عنوان خصائص الجريمة الالكترونية ، وفي مطلبه الثالث والاخير تمحور حول الطبيعة القانونية للجرائم الالكترونية أما المبحث الثاني فكان الاختصاص في الجرائم الالكترونية حيث ظم في مطلبه الأول تحديد مفهوم شروط الاختصاص في مسائل الجريمة الالكترونية، وفي مطلبه الثاني الإختصاص القضائي في الجريمة الإلكترونية، أما في المطلب الثالث فكان لقواعد الاختصاص في الجريمة الالكترونية ، ولا ننسى أيضا أنه تحت كل مطلب عنوانين فرعيين.

وبعد اتمامنا لهذا الفصل انتقلنا الى الفصل الثاني الذي تعنون الدليل الالكتروني للجرائم حيث اعتمدنا فيه كما جاء في الفصل الأول مبحثين ولكل واحد منهما ثلاث مطالب ، فجاء المبحث الأول بعنوان مفهوم الدليل الالكتروني وتضمن هذا الأخير في مطلبه الأول مفهوم تعريف الدليل الإلكتروني ما في المطلب الثاني فكان تحت أنواع وخصائص الدليل الإلكتروني، أما المطلب الثالث تمحور حول شروط قبول الدليل الإلكتروني، ونجد أيضا في المبحث الثاني

المعنون بإجراءات الحصول على الدليل الالكتروني حيث شمل هذا في المطلب الأول مبدأ مشروعية الدليل الالكتروني وفي المطلب الثاني الاجراءات التقليدية والحديثة للدليل الالكتروني وختمناه بمطلب ثالث تحت عنوان موقف التشريعات من الدليل الالكتروني .

حيث سبقتهم مقدمة عامة ضمت العناصر المنهجية للدراسة عناصر الإشكالية وتليهم خاتمة عامة ضمت تلخيص عام لما جاء في هذه الدراسة.

الـــفـــصـــل الأول:

الاطار المفاهيمي للجرائم الالـكـتـرونـيـة

تمهيد:

إن الجرائم الإلكترونية تشمل مجموعة واسعة من الأنشطة غير القانونية التي تتعامل مع التكنولوجيا الرقمية كما أن الإجراءات الجزائية تمتاز بمجموعة من المراحل بداية من مرحلة قبل وقوع الجريمة ثم مرحلة التحريات الأولية والتي تسمي بمرحلة جمع الاستدلالات والحقائق لتنتهي بمرحلة تحريك الدعوى والمبشرة فيها وتعد أهم مرحلة عندما يتعلق الأمر بالجرائم الإلكترونية، كما ان التحقيق الجيد والفعال يلعب دورًا حاسمًا في التمكن من تحديد المتسبب وجمع الأدلة اللازمة لإحالته للعدالة.

ومع تطور التكنولوجيا، أصبح التحقيق في الجرائم الإلكترونية تحديًا أكبر نظرًا للطبيعة الخفية والمتقدمة لهذا النوع من الجرائم. لذلك، تتطلب الجرائم الإلكترونية إجراءات تحقيق مختلفة ومتخصصة فيما يلي نستعرض أهم الإجراءات الإدارية للجرائم الالكترونية.

المبحث الأول: مفهوم الجريمة الالكترونية.

في هذا المبحث سنتطرق لتعريف الجريمة الالكترونية، كما سنحاول إعطائها خصائص تتميز بها عن غيرها من الجرائم التقليدية وأخيرا سوف نتعرض للطبيعة القانونية للجريمة الالكترونية، وذلك في المطالب الثلاث الآتية:

المطلب الأول: تعريف الجريمة الالكترونية:

تعريف الجريمة الالكترونية للجريمة الالكترونية مسميات كثيرة، فالبعض يطلق عليها اسم جرائم الحاسب الآلي.[1]

والبعض الأخر الجرائم المستحدثة أو جرائم الكمبيوتر أو الجرائم الإلكترونية.[2]

ونظراً لاختلاف وتعدد التسميات التي تطلق على هذا النوع من الأجرام، ونظراً لحداثته والذي ولد نتيجة التطور العالمي والتكنولوجي الهائل والمتسارع الذي تشهده البشرية.[3]

بالإضافة إلى الطبيعة الخاصة التي تتميز بها، فقد تنوعت التعريفات التي تناولت موضوع الجريمة الالكترونية، الأمر الذي انعكس على الصعوبة التي واجهتنا عند وضع تعريف جامع مانع للجريمة الالكترونية فقد ذهب البعض [4]إلى تعريف الجريمة الالكترونية بالاعتماد على الوسيلة التي يتم ارتكاب الجريمة من خلالها ألا وهي الحاسب الآلي: " هيا وهي الجرائم التي يتم ارتكابها عن طريق الحاسب الآلي.[5]

المطلب الثاني: خصائص الجريمة الالكترونية:

تتميز الجريمة الالكترونية بخصائص تميزها عن الجريمة التقليدية ونجد من أهمها:

1. الجريمة الالكترونية جريمة عابرة للحدود الجريمة:

الجريمة الالكترونية تتسم غالباً بالطابع دولي ، ذلك لأن الطابع العالمي لشبكة الإنترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط On line يُسهل ارتكاب الجريمة من دولة إلي دولة أخري ، فالجريمة الالكترونية لا تعترف بالحدود بين الدول والقارات

---

[1]محمد العجلوني، د. زياد مشاقبة، استخدامات حاسوبية في الإدارة، ط1، دار اليازوري – عمان – الأردن 2011، ص 14.

[2] محمد علي قطب، الجرائم المستحدثة وطرق مواجهتها، ط1، دار الفجر للنشر والتوزيع القاهرة، 2009، ص 131.

[3]بيل غيتس الالكترونية بعد الانترنت ترجمة عبد السلام رضوان، عالم المعرفة سلسلة كتب ثقافية شهرية يصدرها المجلس الوطني للثقافة والفنون والآداب – الكويت، يناير 1978، ص15.

[4]منير الجنبيهي، ممدوح الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي الإسكندرية، 2006، ص 13.

[5] عمرو عيسى ألفقي، الجرائم الالكترونية، المكتب الجامعي الحديث – الإسكندرية 2006، ص 85.

ولذلك فهي جريمة عابرة للقارات ، فهي تعتبر شكلاً جديداً من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة ، إذ يمكن من خلال النظام الالكتروني ارتكاب العديد من الجرائم مثل جرائم التعدي علي قواعد البيانات ، وتزوير وإتلاف المستندات الإلكترونية ، والاحتيال الالكتروني ، وسرقة بطاقات الائتمان ، والقرصنة ، وغسيل الأموال.

فالجريمة الالكترونية هي من نوع الجرائم التي يتم ارتكابها عن بعد on line عبر المسافات، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي الالكتروني في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء، وبالتالي لا تقف الجريمة الالكترونية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الإقليمية لدولة أخري مما يزيد من صعوبة اكتشافها.[1]

مفاد ما سبق أن الجرائم الالكترونية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، ومن الوجهة التقنية، بين الكمبيوتر أداة الجريمة وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه وبفعل سيادة تقنيات شبكات النظم والمعلومات، امتد خارج هذه الحدود – دون تغيير في الاحتياجات التقنية ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء.

ولمواجهة مثل هذه الجريمة مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وأن يكون هناك تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وإيجاد الحلول لمشكلاتها الأساسية.

2. صعوبة إثبات الجريمة الالكترونية:

فالجرائم الالكترونية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف، أو صعبة في تحديد مكان وقوعها أو مكان التعامل معها، بسبب اتساع نطاقها المكاني وضخامة البيانات، ترجع صعوبة إثبات الجريمة الالكترونية هي إلى عدة أمور منها:

[1] عبد الله حسين علي محمود، سرقة المعلومات المحزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة 2001،ص 351.

أ – أنها كجريمة لا تترك أي أثار مادية لها بعد ارتكابها، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير مرئية ولا توجد مستندات ورقية .

فهذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فهذه الجرائم لا تترك أثراً، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، فالجريمة الالكترونية من الجرائم المستحدثة التي لا تترك شهوداً يمكن استجوابهم ولا أدلة مادية يمكن فحصها، من هنا تأتى صعوبة الكشف عن هذه الجريمة.

ب – صعوبة الاحتفاظ الفني بدليل الجريمة الالكترونية [1]إذ لا يستطيع المجرم الالكتروني في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر، لذا فإن للمصادقة وسوء الحظ دوراً في اكتشافها يفوق دور أساليب التدقيق والرقابة ومعظم مرتكبيها الذين تم ضبطهم وفقا لما لاحظه أحد الخبراء في مجال الجريمة الالكترونية إما أنهم تصرفوا بغباء أو لم يستخدموا الأنظمة الالكترونية بمهارة.

ج – تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها، حيث تتطلب جرائم الكمبيوتر والإنترنت إلمام خاص بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو لملاحقتهم قضائياً.

لذلك يجد مأموري الضبط القضائي أحياناً أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فضلاً عن صعوبة إجراء التحريات السرية وتتبع مسار العمليات الإلكترونية العابرة للحدود.

أن رجال الشرطة ومأموري الضبط القضائي قد لا يتعاملون بمهارة واحتراف مع الدليل الإلكتروني المستمد من الجريمة الالكترونية، فقد يتسبب المحقق بدون قصد أو بطريق الخطأ في أتلاف الدليل الإلكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة، وقد يتجاهل المحقق الدليل الإلكتروني تماماً ظنا منه أنه غير مهم، أو لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو ملحقاته مثل الطابعة أو الماسح الضوئي.

[1] - John Eaton & Jermy smothers'. A managers Guide to information Technology, London, Philip Allan, 1982, p263.

ولذلك نري ضرورة عقد دورات تدريبية مشتركة بين رجال القضاء والنيابة العامة ورجال الشرطة والخبراء الفنيين مجتمعين معاً، وذلك بغرض معرفة كل جهة بطبيعة عمل الجهة الأخرى مما يحقق التعاون بين هذه الجهات وصولاً إلى أنسب الطرق القانونية لمكافحة الجرائم الالكترونية والإلكترونية.

د – تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها ومما يساعد من ازدياد عدم التعرف على مرتكبي الجرائم الإلكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم معلوماتية قبلها تجنباً للإساءة إلى السمعة وهز ثقة العملاء فيها، وكذلك إخفاء أسلوب ارتكاب الجريمة خوفاً من قيام آخرين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الأحجام عن إبلاغ السلطات المختصة عن الجريمة وهو ما يزيد فرص المجرم الالكتروني في الإفلات من العقاب.

هـ – تعتمد على الذكاء في ارتكابها، فالجريمة الالكترونية من النوع الذي يمكن أن نصفه بجرائم الذكاء بالإضافة إلى أنها ليست جريمة منظمة في الغالب، بل تتم على المستوي الفردي، وأهم دوافعها الطمع والجشع والانتقام، وأحياناً ترتكب بدافع إثبات الذات.

ذلك أن الإجرام الالكتروني هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم الالكتروني ذو مهارات تقنية عالية وإلمام بتكنولوجيا النظم الالكترونية.[1]

3. عدم وجود مفهوم مشترك للجريمة الالكترونية:

من خصائص الجريمة الالكترونية عدم وجود مفهوم مشترك لماهية الجريمة الالكترونية، وكذلك عدم وجود تعريف قانوني موحد لها ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة الالكترونية، ويرجع ذلك إلى أن عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة الالكترونية، أو لاختلاف مفهوم الجريمة تبعاً لاختلاف النظم القانونية.

كما أن التطور التكنولوجي نتج عنه تطور في طرق إثبات لجريمة والتعامل معها، فالجرائم العادية يسهل – غالباً – تحديد مكان ارتكابها، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند الجرائم الالكترونية، لكون الرسائل وملفات الكمبيوتر تنتقل من نظام معلوماتي إلى أخر في ثوان معدودة، كما انه لا يقف أمام فقال الملفات والمستندات والرسائل

[1] أحمد خليفه الملط، الجرائم المعلوماتية ، دار الفكر الجامعي 2005 ، ص 114.

عبر شبكة الإنترنت أية حدود دولية لو جغرافية، ونتيجة لذلك فإن تحديد أي محكمة تحدد أي قانون يطبق سوف يكون مشكلة بين الدول مما يستدعي التعاون بين دول العالم.

أن مشروعية الجريمة أمر نسبي من دولة إلى أخري، فمثلاً تجارة المخدرات في مصر محرمة نهائياً، بينما في الدول الإسكندنافية مصرح بها في حدود الاستعمال الشخصي فقط، بل أن مشروعية الجريمة قد تختلف داخل البلد الواحد، فمثلاً نجد داخل الولايات المتحدة الأمريكية أن العاب القمار عبر الإنترنت مسموح بها في ولاية لاس فيجاس بينما هي مجرمة قانوناً في ولاية نيويورك.

ولذلك يري البعض أنه في سبيل مكافحة الجريمة الالكترونية يجب أن تتحرك الدول المختلفة في محورين:

الأول: داخلي بحيث تتماشي قوانينها الداخلية من هذا الشكل الجديد من الجرائم.

والثاني: دولي عن طريق عقد الاتفاقيات الدولية، وهذا بالطبع يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق مبدأ ازدواجية التجريم، وحتى لا يستفاد مجرمو الالكترونية من عجز التشريعات الداخلية من جهة، وغياب المعاهدات الدولية التي تعالج سبل مواجهة هذه الجرائم من جهة أخري.[1]

4. وقوع الجريمة الالكترونية أثناء المعالجة الآلية للبيانات:

من خصائص الجريمة الالكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الالكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الالكترونية.[2]

والجريمة الالكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات.

---

[1] نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادي، دراسة نظرية وتطبيقية، القاهرة، مصر، 2004، ص55.

[2] خالد محمد كدفور المهيري،جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، دار الغرير للطباعة والنشر – دبي،2005، ص 135.

5. قلة الإبلاغ عن وقوع الجريمة الالكترونية:

لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة: والعدد الذي تم اكتشافه، هو رقم خطير. وبعبارة أخرى، الفجوة بين عند هذه الجرائم الحقيقي وبين ما تم اكتشافه فجوة كبيرة.

6. الجريمة الالكترونية جريمة مستحدثة:

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة ، فلا غرابة أن تعتبر الجرائم الالكترونية – سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تُسخر تلك الأجهزة في ارتكابها – من الجرائم المستحدثة ، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة ، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها ، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.

وعلى الرغم من المزايا والمنافع الإيجابية المرتبة على هذه العولمة وثورة المجتمع الإلكتروني، إلا إنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم من أبرزها جرائم غسيل الأموال، وتهريب المخدرات، واختراق قطاع الأعمال، والإفلاس بالتدليس والغش والفساد ورشوة الموظفين العموميين، وسرقة الملكيات الفكرية، والاتجار تكون عبر المشروع في الأسلحة وفي النساء والأطفال، والاتجار غير الأعضاء البشرية، وسرقة المقتنيات الفنية والثقافية، المشروع في والغش في التأمين والجرائم الالكترونية.

7.عدم كفاية التعاون الدولي في مجال الجرائم الالكترونية:

عدم وجود معاهدات دولية كافية للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر وديناميكية التحريات فيها وكفالة السرعة بها.

ويمثل مشروع الاتفاقية الأوروبية لجرائم الكمبيوتر في الوقت الحاضر المشروع الأكثر نضجا لموجهة جرائم الكمبيوتر بل وواحدا من أهم أدوات التعاون الدولي في هذا الحقل.

8.احتمال تعدد الأوصاف القانونية لمحل الجريمة الالكترونية: [1]

نظراً لأن النظام الالكتروني ذاته لا يتكون من طبيعة واحدة ، فهو يتكون من عناصر مادية وعناصر معنوية ، بما يسمح من إمكانية أن يكون موضوع الجريمة الالكترونية ذا طبعتين مختلفتين أحدهما يتمثل في الجاني المادي والأخر يتمثل في الجاني غير المادي ، وذلك ليس علي مكونات النظام ذاته بل يشمل ظهور المحل الواحد بمظهرين أحدهما مادي والثاني معنوي ، كما هو الحال بالنسبة للمعلومات فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الالكتروني أي أنها في حالة غير مادية ، والشكل الآخر أن تكون المعلومات متجسدة في صورة.

المطلب الثالث: الطبيعة القانونية للجرائم الالكترونية:

يحمي القانون الجنائي حق الملكية سواء كان محله عقاراً أو منقولا، وإن كانت ملكية المنقولات تحظى بالنصيب الأوفر من رعاية التشريع الجنائي. وجدير بالذكر أن الجرائم التي تقع اعتداء على ملكية المنقول تنقسم إلى طائفتين رئيستين: أحدهما تضم جرائم تكون الغاية منها الاستيلاء على مال الغير، والأخرى تشمل الجرائم التي تكون غايتها إتلاف مال الغير، ويدخل ضمن الطائفة الأولى جرائم السرقة والاحتيال وخيانة الأمانة.[2]

فإذا كان الاحتيال الالكتروني كما أسلفنا هو التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية، فإلى أي مدى تمثل المعلومات محلاً للاعتداء عليها من خلال جريمة الاحتيال؟

إن الإجابة على هذا التساؤل تقودنا بطبيعة الحال إلى الحديث أولاً عن الأساس القانوني لاعتبار المعلومات من المنقولات حتى نستطيع من خلال ذلك أن نتعرف على الطبيعة القانونية للاحتيال الالكتروني، وهنا ينبغي التمييز بين عدة حالات، نوجزها في الآتي:

الحالة الأولى: ويتمثل في قيام الجاني بالاستيلاء على أي من وسائط تخزين البيانات أو المعلومات أسطوانة مرنة Floppy Disk FD أسطوانة صلبة Hard Disk HD سواء داخلية أو خارجية، أو أسطوانة CDأو فلاش USP أو ذاكرة Memory ما يستحدث من وسائل تخزين البيانات، ففي هذه الحالة يتعلق الأمر بمال منقول باعتبار أن هذه الوسائط المدون عليها

[1] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية،1999، ص 42 وما بعدها.

[2] عمر السعيد رمضان، شرح قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، الطبعة الأولى، 1986، ص 407 .

معلومات تشكل ولا ريب مالاً منقولا، شأنهما في ذلك شأن المستندات التي يحميها تجريم السرقة والنصب وخيانة الأمانة.[1]

الحالة الثانية: فتمثل في قيام المتهم فقط بنسخ البيانات أو المعلومات سواء أكان هذا على جهاز الحاسب الآلي نفسه أو على أي من تلك الوسائط ومن ثم ترك المعلومات الأصلية كما هي بجهاز الكمبيوتر أو الحاسب الآلي أو الوسائط الأصلية التي تحوي تلك البيانات أو المعلومات، وظاهر هذا الأمر أن الجاني لم يقم بالاستيلاء على مال مادي منقول وإنما فقط استولى على تلك البيانات أو المعلومات. إلا انه لأهمية وخطورة هذه البيانات أو المعلومات تتجه التشريعات إلى توفير الحماية القانونية لها على الرغم من أنها من الأموال ذات الطابع المعنوي ما دامت هذه البيانات أو المعلومات مسجلة على دعامة وسائط مادية.

الحالة الثالثة: ويتمثل في حالة قيام الجاني بالاطلاع فقط على تلك البيانات أو المعلومات دون نسخها، هنا نجد أن التشريعات على اختلاف فيما بينها، ولعل ذلك راجع إلى اعتبار المعلومات منتمية تارة إلى المنقولات وتارة أخرى إلى الأفكار، وذلك على نحو ما نرى في القوانين المعمول بها في إنجلترا مثلاً، من حيث عدم اعتبار الاطلاع على المعلومات المسجلة بالحاسب الآلي مشكلاً لجريمة من جرائم الأموال قياساً بما هو مستقر بالنسبة للملفات الورقية واعتبار أن مجرد الاطلاع على تلك الملفات ثم تركها مكانها لا يشكل جريمة سرقة أو احتيال أو خيانة أمانة على أن هناك بعض التشريعات كما هو الحال في القانون الأمريكي وبعض القوانين الأوربية قد تدخلت ببعض النصوص الخاصة لحماية مثل هذا السلوك.

الحالة الرابعة: ويتمثل في حالة قيام المتهم بإجراء توصيلات بإحدى أجهزة الحاسوب للحصول على بيانات أو معلومات دون علم صاحب الحق في هذه المعلومات، وهنا يقتصر سلوك المتهم على التجسس على نظام الحاسب الآلي عن بعد دون إجراء توصيلات مادية إضافية، ومستعينا في ذلك بالوسائل الالكترونية المتقدمة التي توفرها شبكة الإنترنت وتكنولوجيا الاتصال الحديثة. ونلاحظ أن المتهم في هذا الأمر قد اقتصر نشاطه الإجرامي على مجرد التجسس وأنه لا يوجد نص يجرم التجسس إلا فيما يختص بأسرار الدولة العسكرية أو السياسية.

[1] غنام محمد غنام دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، مرجع سابق، ص 41.

إذن وفي ضوء ما يستنبط مما سبق – نجد أن المشاكل التي يثيرها الفته بخصوص تطبيق نص جريمة الاحتيال على الأفعال التي تتمثل في التلاعب في البيانات والمعلومات أو البرامج بهدف الحصول على مال أو أي شيء آخر ذا قيمة[1] حيث يرى البعض أن الهدف الرئيسي الذي يتحقق به الاحتيال في النظام الالكتروني هو المعلومات سواء أكانت صورة أولية كالبيانات أو في صورة يمكن الاستفادة منها كالمعلومات وجميعها من المعالجة آليا، التي تمثل وفق النظم الالكترونية أموالاً أو أصولاً وأن أكثر.

المبحث الثاني: الاختصاص في الجرائم الالكترونية.

وتعتبر شروط الاختصاص القضائي من مسائل النظام العام التي يمكن إثارتها في أي مرحلة كانت عليها الدعوى فتتعرض الإجراءات برمتها للبطلان في حال عدم استيفائها، وشروط الاختصاص في مسائل البحث والتحقيق نوعان اختصاص نوعي وآخر إقليمي محلي، فلا يمكن لمن يتولى أعمال البحث والتحقيق مباشرة أعماله وهو غير مختص نوعا، كما لا يمكن لمن يتولى الإجراءات نفسها وهو يتمتع بصفة الاختصاص النوعي ممارسة أعماله خارج نطاق اختصاصه الإقليمي.

المطلب الأول: تحديد مفهوم شروط الاختصاص في مسائل الجريمة الالكترونية:

إن المقصود بالاختصاص هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل أقاليمها، وتعد الجرائم الإلكترونية من أكثر الجرائم التي تطرح مسألة الاختصاص ذلك أن سلوك أو نشاط المجرم فيها لا يعترف بالحدود، فالعالم كله مرهون بمجرد نقرة بسيطة على لوحة المفاتيح جهاز الحاسوب، إذ أن الطبيعة التقنية العالية للنظم الالكترونية المرتبطة بشبكات الاتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة، الأمر الذي قد ينجم عنه تنازع في الاختصاص بين هذه الدول، فقد يحدث أن ترتكب الجريمة الإلكترونية في إقليم دولة معينة وتتحقق النتيجة في دولة أخرى فتتعدد القوانين التي يمكن أن تحكم هذه الجرائم بتعدد الدول ذا كان ٍ المرتبطة بها، وإذا كان الاختصاص على مستوى داخلي وطنيا فيتحدد سلفا بمعايير محددة في قانون الإجراءات الجزائية.

[1] محمد سامي الشواء ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1998، ص 132.

ان التحقيق هو مجموعة القواعد القانونية والفنية التي تبشرها السلطة المختصة لتمحيص الأدلة والكشف عن الحقيقة تتأتى الحقيقة في الجرائم الالكترونية بوجودها كأساس موضوع التحقيق المستحدث، وينبغي التطبيق السليم للقانون من خلال التقدير السليم للدليل المستمد من الجريمة واحترام قواعد الاختصاص وعدم تجاوز حدود الحيز المكاني والزماني خاصة عند عبور الجريمة حدود الدولة الواحدة، واحترام مختلف عناصر التحقيق، مع كفالة حقوق الأفراد لتحقيق توازن عادل بين ما تفرضه السلطة العامة من التزامات عادلة، مع مراعاة مبدأ الشرعية الإجرائية والحق فيه، أين يخضع الفرد لقيود تحد من حريته الخصوصية تحديا أمام سلطات التحري والتحقيق في الجرائم الالكترونية، كما أن قواعد إثبات الجرائم الالكترونية تعتبر مميزة وتعتبر إجراءات البحث والتحقيق من الإجراءات التي تمس بحقوق وحريات الأفراد، ولذلك فقد حرص المشرع الجزائري على إسنادها لجهة قضائية لأجل ضمان كفالة حقيقية لجملة الحقوق والحريات الفردية.

المطلب الثاني: الإختصاص القضائي في الجريمة الإلكترونية:

حظي الاختصاص القضائي المتعلق بالجرائم الإلكترونية بالكثير من الاهتمام والجدل لذلك سوف نحاول طرح أهم الإختصاصات في موضوع عبر الفروع الآتية:

الفرع الأول: اختصاص النيابة العامة في تحريك الدعوى العمومية في مجال الجرائم الإلكترونية في التشريع الجزائري:

يتعين التأكيد هنا بأن الأمر لا يخرج عن نطاق المادة الأولى من قانون الإجراءات الجزائية وفق استثناءات حددها هذا القانون نفسه، كما سوف ترى ومن الواضح أيضا إن دور النيابة العامة كما رسمته المادة 29 من قانون الإجراءات الجزائية الجزائري وكذا المادة 36 يكون قد توسع في ظل المستحدثات والتطور الحاصل في مجال الجرائم المنظمة والجرائم عابرة الحدود والجرائم الإلكترونية على الأخص.

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 09/01 و 14/04 وضع قواعد وأحكام خاصة لسلطة

المتابعة والاختصاص، الغرض منها هو مواجهتها، حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ومما يتعين الإشارة إليه أن تحريك الدعوى العمومية في جرائم الانترنت وتقديم الشكاوى بشأنها من قبل المتضررين بات محل اهتمام الهيئات الدولية، فبالإضافة إلى القرارات الصادرة عن الأمم المتحدة بخصوص الجرائم المتصلة بالكمبيوتر في توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد سنة 1994 بالبرازيل بشأن جرائم الكمبيوتر، والذي أبرز الوجود المركز العالمي للشكاوي الخاصة بجرائم الأنترنت، حيث يعتبر هذا المركز من أهم المؤسسات التي ظهرت إلى الوجود في مجال مجابهة جرائم الأنترنت الذي تأسس في الولايات المتحدة الأمريكية سنة 1999.

ومن هنا يتضح أن إختصاص النيابة العامة توسع مجاله ليمتد ويغطي نطاقات أخرى لم تكن مرخصة لها من قبل، إذ أن المادة 37 من ق.ا.ج.ج. بعد تعديله بموجب القانون رقم 04/14 المؤرخ في 10 نوفمبر 2004 وبعد أن كان إختصاص المحلي لوكيل الجمهورية محصورا في المجالات التالية:

- بمكان وقوع الجريمة.

- بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة بالمكان الذي تم في دائرته القبض على أحد الأشخاص المشار لهم ولو لسبب آخر.

- فإنه نص على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى في إطار جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بقوانين الصرف وذلك عن طريق التنظيم[1].

[1] ربيعة زيدان، الجريمة الالكترونية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة الجزائر، سنة 2011، ص ص 109 في 111.

كما جاء في نص المادة 37 ق ا ج ج وبصدور المرسوم التنفيذي رقم 06/348 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[1] ليكون بذلك قد شمل الاختصاص المحلي للنيابة العامة كل ربوع الوطني في ما يخص الجرائم المعلوماتية، علما أن المحاكم التي تم تمديد اختصاصها أصطلح على تسميتها في التشريع الجزائري بالأقطاب أو محكمة القطب.

والنيابة مجال إختصاص واسع جدا في إطار البحث والتحري عن الجرائم الإلكترونية ومنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور كما هو منصوص عليه في المادة 65 مكرر 5 من ق ا ج ج وسوف يأتي شرحه، وهذا بالإضافة إلى استعمال التقنيات المخزنة وكذا حجز هذه المعطيات هذا فضلا عن اتخاذ التدابير الملائمة والتحفظية في إطار المساعدات الدولية المتبادلة في مجال الجريمة المعلوماتية.

الفرع الثاني: الاختصاص المحلي لقاضي التحقيق في جرائم الإلكترونية:

من المعلوم أن المشرع الجزائري سار بوتيرة متسارعة على خطى التشريعات العالمية ، في إطار مواكبة التطور الحاصل في مضمار القانون لمجابهة التطور الحاصل في مجال الإجرام بصوره الحديثة لا سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2] وفي هذا الاتجاه جاء تعديل قانون الإجراءات الجزائية بموجب القانون رقم 04/014 المؤرخ في 10/11/2004 ومس التعديل المادة 40 من قانون ا ج ج لتصبح كما يلي :

"يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر"[3].

[1] المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلى لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.
[2] ربيعة زيدان، مرجع سابق، ص 113 و 114.
[3] المادة 40 من ق.ا.ج.ج. المعدل بموجب القانون رقم 014/04 المؤرخ في 2004/11/10.

يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

ومن الملاحظ أن تمديد اختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة للنيابة العامة بأحكام المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 وقد حددت المادة الأولى من المرسوم المشار له مجال الإختصاص المحلي الممدد في النطاق الأقطاب القضائية المحددة في المواد 2، 3، 4، 5 من نفس المرسوم في الجرائم المذكورة سابقا وما يهمنا في الموضوع هو ما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الثالث: الصلاحيات المكانية للضبطية القضائية في الجرائم المعلوماتية:

من الواضح أن المشرع الجزائري يكون قد سارع إلى تدارك النقص وسد الفراغ القائم بخصوص مجلات التحقيق الابتدائي إثر التطور الذي عرفته الجريمة لاسيما بأشكالها الحديثة كما هو الحال في الجرائم الإلكترونية لذلك جاءت تعديلات قانون الإجراءات الجزائية المتعاقبة لاسيما التعديل الذي جاء به القانون 06/22 المؤرخ في 20/12/2006 والذي مدد من صلاحيات الضبطية القضائية ووسع دائرة اختصاصها ودعمه في ذلك القانون رقم 09/04 المؤرخ في 05/08/2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها كما سوف نرى[1].

أناط القانون الجزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات تماشيا مع المبدأ الدستوري المتعارف عليه " لا جريمة ولا عقوبة إلا بنص"[2]، وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي، ويتضح من نص المادة 12 قانون ا ج ج أن مناط البحث عن الجرائم بالنسبة الضبطية القضائية ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم فإذا ما ابتدأ التحقيق القضائي تقلص دورها، لينحصر في تنفيذ

[1] ربيعة زيدان، مرجع سابق، ص 155.
[2] المادة 01 من قانون العقوبات الجزائري .

طلبات جهات التحقيق القضائي وإنجاز ما توجه إليهم من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي.

المطلب الثالث: قواعد الاختصاص في الجريمة الالكترونية:

الاختصاص هو السلطة التي يقرها القانون للقضاء في أن ينظر في دعاوى من نوع معين[1].

وبالنظر لطبيعة وخصائص الجريمة الالكترونية فليس لها مقر ثابت أو دولة معينة بل تنتشر في كل دول العالم، وليست لها أية هيئة أو جهة تشرف عليها ومسؤولية عنها مما يترتب عن ذلك عدم وجود قانون جنائي محدد أو موحد يحكم الجريمة بل بالعكس هناك العديد من القوانين الجنائية بتعدد الدول والأنظمة القانونية و ذلك يرجع أساسا لارتباط القانون الجنائي بالسيادة الوطنية.

ومن هنا تكمن الإشكالية في أن بعض السلوكيات والأفعال مجرمة في بعض الدول ومباحة في دول أخرى وفي أغلب الدول لا توجد نصوص تنظم هذه السلوكيات.

ان القاعدة العامة المطبقة في أغلب الدول هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يطبق على كافة الجرائم التي تقع في تراب الدولة بغض النظر عن جنسية فاعلها أو مرتكبها، ومع هذا فإن تطور الإجرام وتوسعه إلى دول العالم تطلب وجود اتفاقيات دولية لتسليم المجرمين، غير أن غالبية الدول لا تسلم رعاياها وفق لمبدأ السيادة من جهة، ومن جهة أخرى التعارض مع مبدأ أساسي في القانون الجنائي وهو عدم جواز محاكمة لشخص عن فعل واحد أكثر من مرة.

[1] محمود نجيب حسني، شرح قانون الإجراءات الجزائية، دار النهضة العربية 2002، ص 723.

الفرع الأول: مبدأ الاختصاص الإقليمي والشخصي:

أولا: مبدأ الاختصاص الإقليمي:

تأخذ أغلب التشريعات الوضعية بهذا المبدأ على غرار المشرع الجزائري في المادة 03 من قانون العقوبات التي تنص" يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية".

كما أخذ بهذا المبدأ المشرع الفرنسي في المادة 113 ف 02 من قانون العقوبات الجديد التي تنص (يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية وتعتبر قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم"[1].

و يعني هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل القطر الوطني بغض النظر عن جنسية مرتكبيها أو المجني عليه و ينعقد الاختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة.

كما أن هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للجريمة ولو كان الفعل غير معاقب عليه في بلد المنشأ الأصلي أي بداية السلوك الإجرامي، ومن ثم تنقل البيانات والمعلومات بين العديد من الدول وبمجرد اقتراف أحدى سلوكيات الجريمة في القطر الوطني ينعقد الاختصاص للقاضي الوطني، ومن ثم يجب تطبيق قانون العقوبات الوطني كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل القطر لأن العبرة بمكان وقوع الجريمة.

غير إن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة الجريمة الالكترونية وهذا بالنظر لطبيعتها و خصائص التي تميزها عن الجريمة التقليدية وخصوصا صعوبة تحديد مكان وقوعها وارتكباها بدقة وكذا زمان حدوثها.

كما أن هذا المبدأ يجد صعوبة في تطبيقه في قانون العقوبات الفرنسي حيث تنص المادة 113 ف 05 (يطبق القانون الفرنسي على كل من ارتكب فعلا في إقليم الجمهورية

[1] VIDAL (G), Cours de droit criminal et de science penitenterntniaire 8eme ed,mis a jour par Magnol, libraie Arthur .Rousseau, paris, 1935,N 0 1,p1071

يجعله شريكا في جناية أو جنحة وقعت بالخارج إذا كانت الجناية أو الجنحة معاقبا عليها في القانون الفرنسي والقانون الأجنبي و كانت ثابتة بمقتضى حكم نهائي من القضاء الأجنبي).

وعليه وبناء على نص المادة أعلاه فإنه لكي يسأل الشريك يجب توافر ما يلي:

– أن يكون الفعل مجرما في البلد المنشأ – الفعلي الأصلي–

– أن يصدر حكم الإدانة عن الفاعل الأصلي في البلد المنشأ.

وعليه فإن تطبيق هذا النص يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي، لأنه شرط أولي لعقد الاختصاص للقاضي الوطني، لأن ذلك يترتب عليه معرفة ما إذا كان الفعل مباحا أو مجرما في ذلك البلد.

وأخيرا نقول أن مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية وهذا المبدأ يبدوا أنه غير ملائما للجريمة الالكترونية، وهذا بالنظر لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها وتحديد مكان وزمان وقوعها بدقة.

ثانيا: مبدأ الاختصاص الشخصي:

يأخذ هذا المبدأ وجهان وجه إيجابي ووجه سلبي وسنحاول توضيح ذلك كما يلي:

الوجه الإيجابي : ويعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها.

الوجه السلبي: ويعني تطبيق القانون الجنائي على كل جريمة يكون فيها المجني عليه ينتمي إلى جنسية الدولة ولو كان الجاني أجنبيا وارتكب الفعل خارج إقليم الدولة[1].

والمشرع الجزائري على غرار باقي التشريعات لا يعترف بمبدأ الشخصية في وجه السلبي لأن جنسية المجني عليه ليست محل اعتبار في تطبيق القانون الجنائي من حيث المكان.

وعلى العكس من ذلك يأخذ المشرع الجزائري بمبدأ الشخصية في شقه الإيجابي وهو ما نصت عليه المادتين 582 – 583 من قانون الإجراءات الجزائية.

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنيت ، دار النهضة العربية، الإسكندرية، 2002، ص 55.

غير أن هذا المبدأ وردت عليه قيود بصفة عامة و بالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج بل يجب علم النيابة العامة بها، كما أنه لا يجوز محاكمة الشخص على نفس الفعل الواحد مرتين وهذه الإجراءات طويلة ومكلفة وتقيد تطبيق مبدأ الاختصاص الشخصي.

والملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف عن جنسيته، وهذه المعلومات تعد صعبة وعسيرة في جرائم الانترنت أين يستعمل التشفير والأسماء المستعارة بالإضافة إلى اللغة الصعبة والمعقدة في كشفها والتعامل معها.

كما أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة ومعقدة ومكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام الصادرة في الخارج.

وكذلك من مخاطر تطبيق القانون الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت أنه قد يؤدي إلى المساس بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة وهو إحدى المبادئ الأساسية للقانون الجنائي.

وعلى العكس من ذلك إذا لم يكن القانون الوطني مختص بنظر للواقعة فتثار الإشكالية بالنسبة للمضرور من الجريمة الذي يجب عليه التنقل إلى الدولة حيث ارتكب الفعل لرفع دعواه المدنية[1].

والأخطر من ذلك أن يكون الفعل غير معاقب عليه في هذه الدولة ولذلك نري بأنه يجب أن يكون هناك قانون جنائي دولي على غرار القانون الدولي الخاص ليطبق على جرائم الالكترونية.

[1] جمال محمود الكردي: المحكمة المختصة والقانون الواجب التطبيق بشان دعاوى المسؤولية والتعويض عن مضار التلوث البيئة العابرة للحدود ، ط 01 ، دار النهضة العربية، الإسكندرية 2003، ص132

الفرع الثاني: مبدأ الاختصاص العيني والعالمي:

أولا: مبدأ الاختصاص العيني:

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها، ويرجع هذا المبدأ إلى المساس بسيادة الدولة[1].

وحقها في الدفاع عن جميع صور الاعتداء على مصالحها الحيوية والأساسية ولو وقعت تلك الجرائم خارج إقليمها.

وعلى هذا الأساس يمكن أن يطبق هذا المبدأ على جرائم الالكترونية إذا كانت تمس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية ولو ارتكبت من قبل أجانب وخارج إقليم الدولة.

وعلى هذا الأساس يمكن أن يطبق هذا المبدأ على جرائم الالكترونية إذا كانت تمس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية ولو ارتكبت من قبل أجانب وخارج إقليم الدولة.

غير أن هذا المبدأ في الواقع يصادف العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص الجريمة الالكترونية حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع الأنظمة القانونية في العالم واختلافها مما يترتب عليه البطء والتعقيد وطول مدة الإجراءات.

ثانيا: مبدأ الاختصاص العالمي:

يطبق وفقا لهذا المبدأ القانون الجنائي على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني[2].

[1] مأمون محمد سلامة: شرح قانون العقوبات القسم العام، ط 03، دار النهضة العربية، الاسكندرية، 2002، ص 75.

[2] محمود نجيب حسني ، المرجع السابق، ص 140.

وهذا المبدأ يعطي لقانون العقوبات مجال متسعا يشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة أو احد سلوكياتها ولا بجنسية مرتكبها ولا بطبيعة الجريمة ومساسها بالسيادة والمصالح الوطنية.

وإنما يتطلب فقط القبض على الجاني في إقليم الدولة ليعطي للقانون الجنائي الوطني الاختصاص، وهذا المبدأ يتلائم كثيرا وطبيعة الجريمة الالكترونية رغم ما يطرحه من تنازع حاد بين التشريعات الجنائية في الدول.

وعليه فانه يمكننا القول:

بأن أهمية هذا المبدأ ومدى ملائمته للجريمة الالكترونية مستمدة من خطورتها من جهة، ومن طبيعتها من جهة أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة، وفي فترات زمنية قصيرة جدا، وهذا المبدأ – أي العالمية – يبقى عاجزا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي جاد وسريع ، وكذا وجوب إعداد تشريعات وطنية لتجريم الظاهرة، ومنها إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاة لجنسيته أو مكان وقوع الفعل الإجرامي.

والملاحظ أن اغلب التشريعات الوضعية ومنها المشرع الجزائري لم ينص على هذا المبدأ بالرغم من أهميته خصوصا في مجال الجريمة الالكترونية، ونرى وجوب النص عليه عند إعداد قانون خاص بمعالجة الجريمة الالكترونية وجرائم الكمبيوتر والانترنت، وهذا بالرغم من أن الاتفاقيات الدولية تركز بل وتعول عليه كثيرا في هذا المجال خصوص اتفاقية بودابست 2001 لمكافحة الجريمة الالكترونية وكذا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة الالكترونية 2003 في المادة 26.

كما أن الفقه يرى بوجوب الأخذ به على غرار جريمة القرصنة في القانون الدولي الجنائي[1].

[1] محمود نجيب حسني ، المرجع السابق، ص 141.

ونحن نعتقد أن الجريمة الالكترونية لا تقل أهمية عن جريمة القرصنة كونها تهدد أمن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة العنكبوتية مما يهدد الاقتصاد العالمي يشهد وتيرة متصاعدة خصوص في المجال المالي والبنكي، وعليه أصبح من الضروري الاخذ بهذا المبدأ ومعاقبة الجاني في أي إقليم يتم فيه القبض عليه دون مراعاة لجنسيته أو مكان ارتكاب جريمته لارتكابه جريمة عالمية.

خلاصة الفصل الأول

يمكن القول في هذا السياق أن وجود نظام قانوني للجرائم الالكترونية في كل دولة فرضته عدة متغيرات يأتي في صدراتها عدم القدرة على مجابهة ومواجهة المخاطر والأضرار الناتجة عن الحماية التقنية المحدودة المقررة لأنظمة المعلوماتية، ولكن الصعوبة لا تزال تطرح في كل مره حتى مع وجود نظام تجريمي لردع الانتهاكات المرتبطة باستخدام أنظمة المعلومات والاتصال خاصة مع ازدياد وتنوع تقنيات توظيفها، وبذلك أصبحت العلاقة طردية بالضرورة بين تطور أنظمة المعلوماتية من جهة والاجرام المعلوماتي من جهة أخرى.

الفصل الثاني:

الدليل الالكتروني للجرائم

تمهيد:

ان الطبيعة الفنية والتقنية الناجمة عن الجرائم المعلوماتية نتج عنها في مجال الإثبات الجنائي نوع جديد من الأدلة يطلق عليه الدليل الرقمي أو الدليل الإلكتروني ، وقد اعتدت به المحاكم في بعض النظم القانونية المقارنة ، سواء من حيث قيمته القانونية أو من حيث حجيته في الإثبات ، حيث اعتمدت هذه النظم القانونية مبدأ التنظير الوظيفي أو المعادل الوظيفي equivalence function، حيث ساوت في الإثبات الجنائي بين الدليل التقليدي والدليل الإلكتروني.

المبحث الأول: مفهوم الدليل الالكتروني.

لدليل الرقمي أو الدليل الإلكتروني هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة.

المطلب الأول: تعريف الدليل الإلكتروني:

عرف القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات الدليل الرقمي بأنه: " أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة " .

كما عرف الدليل الإلكتروني أيضاً بأنه " هو المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون " [1].

فكلما كان هناك مزج في موضوع الدليل ، الفكرة أو المعلومة أو الصورة أو كبيانات Data... الخ ، بالمعالجة الآلية للمعلومات فإنه يعد هنا دليلاً الكترونياً[2].

ويستخلص من التعريفات السابقة أن الدليل الإلكتروني هو " أي معلومات يتم استخلاصها من أجهزة الكمبيوتر أو غيرها من الأجهزة التي تعتمد علي التقنية الرقمية في تشغيلها ، وبشكل يمكن قراءته أو تفسيره من أشخاص لديهم مهارات في إعادة تشكيل المعلومات، بمساعدة من برامج الكمبيوتر.

---

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

[2] Anabda Giet- Analysis of the police and criminal evidence act sec. 69/ computer generated evidence- WEB journal of Current Legal issues UK, 1996 Issue 1, P.1. Available on-line in june 2008 at Http://webicli.nci.ac.uk/1996/issuel/hocy.html

المطلب الثاني: أنواع وخصائص الدليل الإلكتروني:

سنتناول في هذا المطلب أنواع الدليل الرقمي والأشكال التي يبدو عليها كدليل ، ثم نتناول خصائص الدليل الالكتروني ليكون دليلا لإثباتها ، وذلك على النحو التالي:

أولا: أنواع وأشكال الدليل الالكتروني:

أ: أنواع الدليل الإلكتروني:

الدليل الإلكتروني يمكن تقسيمه إلى ثلاثة أنواع وهي كالتالي :

1 – السجلات المحفوظة في الكمبيوتر: وهي الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت.

2– السجلات التي تم إنشاؤها بواسطة الكمبيوتر: وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الآلي ATM .

3– السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الكمبيوتر: ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل مثل Excel ، ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها.

ب: أشكال الدليل الإلكتروني: يتخذ الدليل الرقمي ثلاثة أشكال رئيسة هي: الصور الرقمية والتسجيلات الصوتية ، والنصوص المكتوبة ، ونتناول هذه الأشكال على النحو التالي:

1– الصور الرقمية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية ، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصور التقليدية.

2–التسجيلات الصوتية: وهى التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية ، وتشمل المحادثات الصوتية على الانترنت والهاتف المحمول ، أو غير ذلك من الأجهزة المشابهة التي قد تظهر في المستقبل.

3– النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الالكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الكمبيوتر، وغير ذلك من الأجهزة الالكترونية.

ثانيا: خصائص الدليل الالكتروني:

للوصول إلى الحكم على مدى حجية الدليل الإلكتروني والاستناد عليه في بناء الأحكام القضائية لا بد من معرفة أهم خصائصه، ومن خلالها وبالنظر إلى مدى قابلية هاته الخصائص في وقوع الإثبات تظهر مدى حجية الدليل الإلكتروني أو الرقمي.

يمتاز الدليل الإلكتروني عن غيره من الأدلة بعدة خصائص، وذلك لكونه من بيئة رقمية متطورة بطبيعتها، وتتمثل مميزاته وخصائصه في الآتي[1]:

1- كونه دليلا علميا:

يتكون هذا الدليل من مجموعة من البيانات والأرقام ذات الطبيعة الإلكترونية غير الملموسة، والتي تتطور وفق التطور العلمي، وفي الوقت نفسه تكون موافقة لما وصل إليه العلم، فلا يتعارض مضمونها مع القواعد العلمية الاساسية.

2- كونه دليلا تقنيا:

طبيعة الدليل الإلكتروني الرقمية تجعل من إدراكها يتطلب معالجتها تقنيا، وذلك بالاستعانة بالوسائل والأجهزة وأدوات الحواسيب الآلية، وباستخدام أنظمة معالجة حاسوبية، ليتم من خلالها تحويل بياناته الأساسية إلى معلومات يمكن استخدامها كدليل للإثبات.

3 كونه قابلا للنسخ:

يتميز الدليل الرقمي مهما كان نوعه وحجمه بسهولة نسخه، مع الحفاظ على القيمة المادية والعلمية في كافة النسخ، وهذه الخاصية لا تتوفر في غيره من الأدلة وهذا يشكل ضمانا في الحفاظ عليه، وقلة نسبة ضياع الدليل أو تلفه.

4- كونه سهل التخزين:

الدليل الإلكتروني سهل التخزين مهما بلغ حجمه الرقمي، وذلك نظرا لتطور الأجهزة والحواسيب الرقمية، بحيث يمكن تخزين الفيديوهات والملفات الكثيرة في شريحة تخزين صغيرة جدا، وهذا يساهم في تسهيل عملية استخدامه والرجوع إليه وقت الحاجة.

من خلال الخصائص الأساسية للدليل الإلكتروني والتي تم ذكرها أعلاه يتبين أن هذا النوع من الأدلة له درجة من الموثوقية تجعل منه حجة ومرجعا للإثبات ومستندا للأحكام، ولكن

[1] حميد بلهادي حجية الدليل الرقمي في الإثبات الجنائي مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة الجزائر، المجلد التاسع، العدد الأول، 2019م، ص 19-21.

هاته الحجية التي تم إدراكها من خلال ما يتميز به ليست مبنية على الخصائص فقط، بل لها قيود وضوابط، بحيث أن الدليل الإلكتروني لا يُقبل إلا بتوافر جملة من الشروط، وهذا ما سيتم تفصيله في المبحث الموالي.

كما تجدر الإشارة إلى أن حجية الدليل الإلكتروني ترتبط بنظام الإثبات المعتمد، فهناك أنظمة لالا تعترف بأي دليل لم ينص عليه القانون.

المطلب الثالث: شروط قبول الدليل الإلكتروني:

إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث ، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة[1].

وإذا كانت الأدلة المتحصلة عن الوسائل الإلكترونية قد توجس منها كل من رجال القضاء والفقه خيفة من عدم تعبيرها عن الحقيقة ، نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتحريف أو التغيير والأخطاء المتعددة ، فإنه ذلك قد تطلب وجوب توافر مجموعة من الشروط التي قد تضفي عليها المصداقية ، ومن ثم اقترابها نحو الحقيقة وقبولها كاملة إثبات في المواد الجنائية[2].

الفرع الأول : الشروط الواجب توافرها في الدليل الإلكتروني :

لقبول الأدلة الإلكترونية كأساس تقوم عليه الحقيقة في الدعاوى الجنائية ، سواء أكان الحكم الصادر فيها بالإدانة أم بالبراءة ، فإنه يلزم أن تتوافر فيها الشروط الآتية :

1- يجب أن تكون هذه الأدلة يقينية :

وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات ، ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو

---

[1] طارق محمد الجملي ، الدليل الرقمي في مجال الاثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية والقانون المنعقد في الفترة (28-2009/10/29) تنظمه أكادمية الدراسات العليا طرابلس ، ص 8 .

[2] حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ، رسالة دكتوراه - حقوق عين شمس - 2005 ، ص 485 وما بعدها .

إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع للسلطة التقديرية للقاضي الجنائي ، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال.

والقاضي الجنائي يستطيع أن يصل إلي يقينيه الأدلة والمخرجات السالف ذكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها ، وكذلك عن طريق المعرفة العقلية عن طريق ما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويحبب أن يصدر حكمه استناداً إليها[1].

2- أن يكون الدليل الإلكتروني ذي علاقة بموضوع الجريمة :

هذا الشرط يشار إليه في قانون الإثبات الفيدرالي الأمريكي بمبدأ العلاقة الكاشفة The principal of Relevance ، حيث يتطلب القانون الأمريكي ضرورة أن يكون هناك علاقة من نوع ما بين الدليل وبين الواقعة محل الدعوي (المادة 401)[2].

وشرط ثبوت العلاقة الكاشفة في الدليل الإلكتروني يتطلب شرط أخر وهو مطابقة الدليل الإلكتروني المستخرج من الكمبيوتر للأصل الموجود بداخله ، بحيث لا يكون هناك ثمة إدعاء أو دفع بأن البيانات غير صحيحة بسبب عدم دقة عمل الكمبيوتر ، وهو ما اشترطه القانون الإنجليزي بشأن الشرطة واثبات الأدلة الجنائية لسنه 1984.

3- يتعين مناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة[3] :

فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم . ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب أم كانت بيانات مدرجة في حاملات أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلاً للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة[4] .

ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استناداً إلى علم شخصي له.

---

[1] هلالي عبد اللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، دار النهضة العربية ، 1997 ، ص 91.

[2] عمر أبو بكر بن يونس ، المرجع السابق ، ص 992.

[3] حسين بن سعيد بن سيف الغافري، المرجع السابق ، ص 476 .

[4] هلالي عبد اللاه أحمد حجية المخرجات، مرجع سابق ، ص 104.

4- يجب أن تكون الأدلة المتحصلة من الوسائل الإلكترونية مشروعة:

تعرف المشروعية بأنها " التوافق والتقيد بأحكام القانون في إطار ومضمونه العام ، فتى تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة وبالتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته "[1].

فمشروعية الإثبات الجنائي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريقة غير مشروعة ، فحرية القاضي الجنائي في الإثبات لا تعني أن يجري البحث عن الدليل بأية طريقة كائنة ما كانت ، بل أن هذا البحث مقيد باحترام حقوق الدفاع وقيم العدالة[2].

كما ان شرعية الإثبات تستلزم عدم قبول أي دليل يكون حمله إلي القضاء أو إقامته أمامه قد جاء بالمخالفة للقانون أو لحقوق الدفاع ، أي ضرورة ارتكاز الدليل على إجراءات مشروعية سواء أكانت تلك الإجراءات قد صدرت من قبل القاضي بصورة مباشرة أم غير مباشرة، أم من قبل المتهم عند استجوابه واعترافه ، أم من قبل المتهم عند استجوابه واعترافه، أم من قبل الغير بعد بالقبض عليه واستجوابه أم تفتيشه أم تفتيش مسكنه أم ممارسة أي عمل من أعمال الخبرة الفنية.

فمشروعية الدليل تتطلب صدقه في مضمونه ، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث الحصول عليه.

الفرع الثاني : تقدير أدلة الإثبات:

تذهب التشريعات المقارنة إلي قبول مصادر المعلومات الخاصة بأجهزة الكمبيوتر أو المتحصل عليها من أنظمته مثل مخرجات نظام المعالجة الآلية للبيانات والبيانات المكتوبة على شاشته ، والبيانات المسجلة على دعائم ممغنطة أو المخزنة داخل نظام المعالجة كأدلة يقوم عليها الإثبات الجنائي [3].

---

[1] نبيل إسماعيل عمر: قاعدة عدم قضاء القاضي بعلمه الشخصي، المجلة العربية للدراسات الأمني ، المجلد الأول، العدد الأول ، 1989، الرياض ، ص 115.

[2] محمد زكي أبو عامر ، قانون العقوبات ، دار المطبوعات الجامعية ، 1986، ص 116 .

[3] هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي، مرجع سابق، ص 212 وما بعدها.

وهذه الأدلة المتحصلة من الوسائل الإلكترونية تخضع للسلطة التقديرية للقاضي الجنائي، فإن استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد اقتناعه ويعول عليها في الحكم الذي ينتهي إليه[1].

ولذلك يمكن القول بأن المخرجات المتحصلة من الوسائل الإلكترونية لا تمثل مشكلة في النظام اللاتيني ، حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع [2]،

ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإلكترونية والتي هي عبارة عن إشارات الكترونية ونبضات ممغنطة، يمثل مشكلة أمام القضاء في هذا النظام، إذا لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتوالدة منها ووضع أيديهم عليها ، وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية [3].

ولقد صدر في إنجلترا قانون للإثبات الجنائي في سنة 1984 وعمل به بدءاً من عام 1986 وقد نصت المادة 68 منه على أن يقبل الإثبات بالمحررات التي تتعلق بأي غرض من الأغراض إذا توافرت شروط معينة وهي:

1- أن يكون المحرر عبارة عن سجل أو جزء من سجل يعده الشخص بموجب واجب يقع على عاتقه ليثبت فيه معلومات مقدمه إليه من شخص آخر.

2 – يمكن قبول افتراض توافر علمه الشخصي بالأمور المتعلقة بها المعلومات.

3- ألا يكون الشخص التي تستقي منه المعلومات متاح وجوده أو ممكنا تعيينه أو تتبعه أو يكون غير متوقع منه تذكر الأمور المتعلقة بالمعلومات.

4 – يمكن قبول إفتراض توافر علمه الشخصي بالأمور المتعلقة بها المعلومات.

ولقد نصت المادة 69 من ذات هذا القانون على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الاعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة ، ويجب كذلك أن يكون الحاسب الناتج منه المخرج الإلكتروني يعمل بكفاءة وبصورة سليمة[4].

---

[1] Alan M. Gahtan, Electronic Evidence. Thomas Canada Limited, 1999, p.37.

[2] هلالي عبد اللاه أحمد ، المرجع السابق ، ص 82.

[3] هشام رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، 1994 ، ص172.

[4] هلالي عبد اللاه أحمد ، المرجع السابق ، ص 53.

ولذلك، فإن السؤال الذي يطرح نفسه بالنظر إلي هذه الآثار التي ترتبت على ثورة الاتصالات عن بعد ، هل ستشهد نظاماً للإثبات الجنائي قد تفرزه أيضا هذه الثورة بحيث يعتمد الإثبات الجنائي على الأدلة العلمية الإلكترونية وتتقيد بالتالي سلطة القاضي في الإقتناع؟

يمكن القول بأن التطور العلمي قد يؤثر بلا شك على نظام الاقناع القضائي، فقد يعلى هذا التطور من تقارير الخبراء[1]، بالنظر الى كثرة المسائل الفنية البحتة التي سوف تفرزها تطبيقات ثورة الاتصالات عن بعد، فهذا التطور قد يزيد من دور الخبرة في المسائل الجنائية، بالنظر إلي أن الكثير من الجرائم التي ترتكب كنتيجة لهذه الثورة ستقع على مسائل إلكترونية ذات طبيعة فنية معقدة ، أو قد تستخدم هذه الوسائل في ارتكابها، وبالنظر إلي تطور مجالات الخبرة فإنه سوف تتسع مجالات اللجوء إليها.

كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها ، أيضا فقد يعلو شأن الإثبات بالقرائن كنتيجة لاتساع مجال الإثبات بها نتيجة تطور العلوم ، ولقد أصبح هذا الأمر جلياً واضحاً في الإثبات بالبصمة الوراثية ، وبصمة الصوت، وبصمة قزحية العين[2].

فالقضاء قد قبل الإثبات بالأدلة المتحصلة عنها عن طريق الرادار التصوري، السينومومتر، كاميرات الفيديو مسجلات الصوت الوسائل الإلكترونية في التصنت[3] .

المبحث الثاني: إجراءات الحصول على الدليل الالكتروني.

وحتى يكون استخلاص الدليل الإلكتروني قانونياً ومنتجاً لآثاره القانونية كدليل يقره القضاء، فيجب أن يتوافر في عملية التفتيش عن ذلك الدليل مجموعة من الشروط والتي تتمثل في: أن يكون هذا التفتيش يصاحبه إذن بإجرائه من الجهات المختصة والمعنية بإصدار هذا الإذن، أو أن يكون قد تم حال قيام حالة التلبس.

المطلب الأول: الاجراءات التقليدية للدليل الالكتروني:

وهذا الإجراء يتبع ما يخص الفاعل للجريمة من خلال آثاره الإلكترونية، وهذا الإجراء يتم البدء في سلوكه أثناء قيام المحقق بإجراء المعاينة، وباستخدام آليات البحث عن الدليل

[1] جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي ، مرجع سابق، ص 22.

[2] . Thierry Care Catherine Ginestet: Droiut Penal- Procedure - Penale: Dallozed.2000. P.248

[3] Gaston stefani- Georges Levasseur- Bernard Bouloc: Droit Penal General 17 ed 2000 Dalloz, .P.34

الإلكتروني فيما تم إجراؤه وتخزينه على الجهاز أو الشبكة من تسجيلات تخص إرسال أو استقبال رسائل إلكترونية، أو السجلات الخاصة بما أجراه من محادثات.

الفرع الاول: التفتيش وضبط الادلة:

يعتبر التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر والغرض منه هو ضبط كل ما يفيد في كشف الحقيقة عن الجريمة التي يجري التحقيق أو جمع الاستدلالات بشأنها ومعنى ضبطها هو ضعها تحت يد السلطة العامة للتحفظ عليها إلى حين انتهاء الإجراءات في الدعوى الجنائية[1].

الفقرة الأولى: التفتيش يختلف التفتيش في الجرائم المعلوماتية عن التفتيش المعروف في الجرائم التقليدية، ويرجع ذلك لعدة اعتبارات.

أولا: تعريف التفتيش:

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في مكان يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة[2].

والتفتيش هو التنقيب في وعاء السر بقصد ضبط ما يفيد من معلومات في كشف الحقيقة، وهو كشف نقاب السرية عما تحويه نظم الحاسوب من خفايا ونوايا إجرامية، وبالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة"، وهذا المعنى لا يتقيد بالكيان المادي للحاسوب والأجهزة الملحقة به بل يشمل كذلك كيانه المنطقي من شبكات أو أنظمة وبرمجيات[3].

إذا فالتفتيش ليس غاية في حد ذاته، وإنما وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في كشف الحقيقة[4].

---

[1] فرج عنواني هليل، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، مصر، 2006 ص 622 .

[2] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر 2013، ص 143.

[3] علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب والإنترنت دراسة مقارنة عالم الكتب الحديثة، الأردن2004، ص 28.

[4] أشرف عبد القادر قنديل،الإثبات الجنائي في الجريمة الإلكترونية،دار الجامعة الجديدة، الإسكندرية، مصر، 2015 ص140.

ثانيا: شروط التفتيش:

للتفتيش شروط موضوعية وأخرى شكلية، سنعرضها على النحو التالي:

1-الشروط الموضوعية للتفتيش: ويمكن تقسيمها إلى شرطين أساسيين هما السبب والمحل.

*** سبب التفتيش في البيئة المعلوماتية:** وهو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[1] ، ويتمثل في:

- توافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره[2].

- محل التفتيش في البيئة المعلوماتية ويتمثل محل التفتيش في الجريمة المعلوماتية في المكونات المادية والمعنوية للحاسوب وكذا شبكات الاتصال الخاصة به، ويستوي أن يكون محل التفتيش بحوزة شخص معين أو موجود في مكان ما كالمسكن أو المكتب[3].

2- الشروط الشكلية للتفتيش:

- أن يتم تفتيش النظم المعلوماتية بأسلوب الكتروني من قبل الأجهزة القائمة بالتحقيق.

- كما ينبغي في نهاية التفتيش تحرير محضر للتفتيش يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ويشترط أن يكون المحضر مكتوبا باللغة الرسمية[4].

ثالثا: مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

كما أن له شبكات software ومكونات منطقية hardware يتكون النظام المعلوماتي من مكونات مادية اتصالات بعدية سلكية ولاسلكية سواء على المستوى المحلي أو على المستوى الدولي[5]

---

[1] نبيلة هية هروال، الجوانب الاجرامية لجرائم الانترنت في مرحلة جمع الاستدلالت، دار الفكر الجامعي، الاسكندرية، مصر، 2007، ص 229.

[2] عبد العال الدريبي ومحمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت المركز القومي للإصدارات القانونية، الطبعة الأولى،القاهرة، مصر 2012 ص305.

[3] خالد عباد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، 2011 ، ص 154.

[4] أشرف عبد القادر قنديل، المرجع السابق، ص 151.

[5] عائشة بن قارة مصطفى حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، ص 88.

1- تفتيش المكونات المادية للحاسوب:

بخصوص تفتيش المكونات المادية للحاسوب لا توجد صعوبة في ذلك، لأنه يرد على عناصر مادية لا خلاف للقانون فيها، فتطبق بشأنه القواعد التقليدية للتفتيش، لكن الأخذ بعين الاعتبار القواعد الخاصة بضبط هذه الأجهزة الحساسيتها وإمكانية تعريضها للتلف، كما تطبق على إجراء التفتيش الضمانات المقررة قانونا[1].

2- تفتيش المكونات المنطقية للحاسوب:

إن التساؤل يثور حول إمكانية اعتبار تفتيش المكونات المنطقية للحاسب الآلي نوعا من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي. وقد انقسم الفقه في هذا الشأن إلى اتجاهين:

الاتجاه الأول: تتجمد فكرة هذا الرأي في عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية. إذ أن التفتيش يقتصر مفهومه على أشياء ذات حيز مادي ملموس.

الاتجاه الثاني: يرى أنصار هذا الاتجاه أن برامج الحاسوب يمكن أن تطبق عليها خصائص وسمات المادة، وهو ما يجعلها تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامجا أو تطبيقات حاسوبية مستندين في ذلك إلى أن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين مثل البايت (byte) والميغابايت MB^2.

وبخصوص موقف المشرع الجزائري فهو يتضح جليا من خلال القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حينما أجاز صراحة بموجب نص المادة 5 منه تفتيش المنظومات المعلوماتية[3].

---

[1] فاروق خلف الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015 كلية الحقوق، بسكرة، الجزائر، ص 3.

[2] نعيم سعيداني، المرجع السابق، ص 146.

[3] طبقا للمادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، الدخول بغرض التفتيش إلى منظمة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

الفقرة الثانية: ضبط الدليل الإلكتروني:

إن الأدلة الرقمية المضبوطة أثناء عملية التفتيش لها أهمية كبيرة في إثبات الواقعة الجرمية ونسبتها لمرتكبها من عدمها و بالتالي الحكم عليه بالإدانة أو البراءة.

أولا: مفهوم ضبط الأدلة:

سنتناول في هذا العصر تعريف ضبط الدليل وأنواع الأدلة القابلة للضبط.

1- تعريف ضبط الأدلة:

يعتبر ضبط الأشياء أثرا من آثار المعاينة والتفتيش باعتبارهما يؤديان إلى جمع الأدلة المادية وأدوات ارتكاب الجرائم، وبيان مدلولاتها من أجل الاستفادة منها في إثبات الوقائع الجنائية ونسبتها إلى مرتكبه، فضبط الأدلة إذا لا يخرج عن كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وقد يرد الضبط على منقولا أو عقارا ويستوي أن يكون الشيء المضبوط مملوكا للمتهم أو لغيره[1].

2- الأدلة القابلة للضبط:

توجد العديد من أدلة الاثبات القابلة للضبط في مجال الجرائم المعلوماتية، ومن أهم هذه الأدلة نذكر ما يلي:

- المخرجات الورقية والمستندات التي تفيد الكشف عن الجريمة.
- أجهزة الحاسوب الآلي وملحقاتها مثل وحدات المعالجة المركزية أجهزة لوحة المفاتيح وغيرها.
- البطائق الممغنطة وبطائق الائتمان والمواد المستعملة في إعدادها حيث تعتبر من قرائن الإثبات[2].

ثانيا: مدى قابلية جرائم الحاسوب لضبط أدلتها :

وتفرق في ذلك بين حالتين:

1- ضبط الأدلة المادية للجريمة:

لا يثار أي إشكال بشأن ضبط الأدلة المادية التي تفيد في كشف الحقيقية سواء كانت أجهزة حاسوب أو ملحقاته أو غيرها من الأشياء المنقولة، أما العقارات التي تحتوي على أجهزة

[1] عبد العال الدريبي، المرجع السابق، ص 320.

[2] ضياء علي أحمد نعمان، موسوعة التشريعات الالكترونية المدنية والجنائية، المطبعة والوراقة الوطنية، 2009، ص 374.

الحاسوب وشبكاته فيتم التحفظ على ما تشتمل عليه الجريمة المعلوماتية، عن طريق وضع الأختام على هذه الأماكن وتعيين السلطة المختصة حارسا عليها[1].

2 – ضبط المكونات المنطقية للحاسوب:

لقد سمح المشرع الجزائري للمحقق بحجز معطيات الحاسب الآلي، مع إمكانية نسخها إذا لم يكن هنالك داعي لحجز المنظومة المعلوماتية برمتها، بالإضافة إلى ذلك منحه سلطة استعمال الوسائل التقنية لتشكيل أو إعادة تشكيل هذه المعطيات ثم حجزها ووضع الأختام عليها، طبقا لقانون الإجراءات الجزائية وفي حالة تعذر حجز هذه الأدلة لأسباب تقنية يتعين على السلطات المختصة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات ومنع الإطلاع عليها، وذلك بتكليف أشخاص مؤهلين في هذا المجال[2]، وهو الأمر الذي تناوله المشرع بالنص في المادة 6 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الثاني: المعاينة والخبرة:

إن التعامل في الجريمة المعلوماتية يتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والخبرة من بين إجراءات التحقيق، والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية.

الفقرة الأولى: مفهوم الانتقال والمعاينة:

لم تحدد أغلب التشريعات المقصود بالانتقال والمعاينة ومنها المشرع الجزائري الأمر الذي دعا بالفقه للتصدي لتعريفهما، حيث يعتبر الانتقال عملا هاما من أعمال التحقيق يتم بقصد. الأدلة وفحصها لكشف حقيقة الجريمة ويتطلب ذلك أن ينتقل المحقق من مقر عمله إلى مكان آخر قد يكون مسرح الجريمة لإجراء جمع عمل من أعمال التحقيق، حيث يتم الانتقال بهدف إجراء معاينة أو بهدف القيام بعمل آخر كالتفتيش والضبط وسماع أقوال الشهود في

[1] علي حسن محمد طوالبة، المرجع السابق، ص 142.

[2] أمال، حابت الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، ورقة بحثية مقدمة الأعمال المنتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر ، ص 17.

بعض الأحوال[1] ، أما فيما يخص المعاينة فهناك عدة تعاريف لها، فيقصد بها: رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته ومعرفة كل ما يلزم لكشف الحقيقة[2] في حين عرفها جانب آخر من الفقه تعريف أكثر دقة بأنها مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها[3].

الأصل في المعاينة أنها إجراء من إجراءات التحقيق، ولهذا في غير حالات التلبس المنصوص عليها في القانون يجب أن تقوم بها سلطة التحقيق بنفسها، أو تنتدب مأمور الضبط للقيام بذلك[4] ويقتضي ذلك تحرير محضر بها عن طريق كاتب، لأنها من الإجراءات التي تستلزم من المحقق تفرغا ذهنيا، وتتبع في شانها أيضا جميع القواعد التي تحكم إجراءات المحاكمة من إخطار الخصوم بمكان المعاينة وزمانها ليتمكنوا من الحضور أثناء إجراءها[5] كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة، سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[6].

للمعاينة أهمية كبيرة في كشف غموض العديد من الجرائم التقليدية، إلا أن دورها في كشف غموض الجرائم الإلكترونية، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها لمرتكبها ليس بالدرجة نفسها من الأهمية مقارنة بالجريمة الإلكترونية وذلك لأسباب عدة منها:

-إن عن عدد كبير من الأفراد يكونوا قد ترددوا على مسرح الجريمة خلال الفترة التي تتوسط عادة بين ارتكاب الجريمة واكتشافها، و هذا ما يفتح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو محو بعضها، وهو ما يثير الشك على الدليل المستنبط من المعاينة[7].

استطاعة الجاني من التلاعب في البيانات عن بعد أو محوها عن طريق قيامه بالتدخل من خلال وحدة طرفية، لذلك نص كل من المشرع الجزائري في المادة 43 من قانون

---

[1]خالد ممدوح إبراهيم إبرام العقد الإلكتروني، ط 2،دار الفكر الجامعي، أمام كلية الحقوق –الاسكندرية، ص 156.

[2]عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، لبنان، (دس، ن) ص 303

[3]علي عدنان القيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1 المكتب 94 الجامعي الحديث، مصر، 2012، ص 22.

[4]محمد علي الجمال، التقاط الدليل المادي من مسرح الجريمة، مجلة الدراسات العليا، العدد الثاني، يناير 2000 ص 190.

[5]جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001، ص 27.

[6]جلال ،ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 456.

[7]عبد الله حسين علي محمود، مرجع سبق ذكره، ص ص 365-366.

الإجراءات الجزائية الجزائري [1]، والمشرع الفرنسي من خلال المادة 1/55 من قانون الإجراءات الجنائية الفرنسي[2] ، جزائيات جنائية على كل من يقوم بإجراء أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب أو وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات قبل قيام سلطة التحقيق بإجراء المعاينة وذلك حرصاً منهما على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ و إن كانت أحكام هذه النصوص تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي على خلاف معاينة المكونات غير المادية لأنها تتطلب إجراءات خاصة[3].

أولا: الانتقال والمعاينة على مسرح الجريمة الإلكترونية:

تتم معاينة الجريمة الإلكترونية بالانتقال إلى مسرح الجريمة الإلكترونية وينبغي التعامل مع هذا المسرح على أنه مسرحان هما:

***مسرح تقليدي:** يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية للحاسوب وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، فقد يترك الجاني آثارا كالبصمات وبعض المتعلقات الشخصية أو وسائط تخزين رقمية .

***مسرح افتراضي:** يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت وفي ذاكرة الأقراص الصلبة للحاسوب غير أن الانتقال لا يتم بالضرورة عبر العالم المادي وإنما عبر العالم الافتراضي (cuber space) . وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الجريمة الإلكترونية كما يأتي [4].

– يمكن لضابط الشرطة القضائية اللجوء إلى مقهى الانترنت.

---

[1] تنص المادة 43 من قانون الإجراءات الجزائية الجزائري يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، –وإلا عوقب بغرامة 200 إلى 1000 دج.

غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغيرات أو نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليهم.

[2] Article 55 DU (cppf)

[3] عائشة بن قارة مصطفى المرجع السابق، ص 82.

[4] نبيلة هبة هروال، المرجع السابق، ص 218.

– يمكن الضابط الشرطة القضائية اللجوء على مزود خدمة الانترنتinternet server provide الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة[1].

ونتيجة لاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعاملا خاصا معه ويكون ذلك من خلال إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية أبرزها:

– توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها فنيا[2].

– إعداد خريطة للموقع المتوقع الإغارة عليه والتأكيد من تأمين وصلاحية الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة[3].

– إعداد فريق متخصص من الخبراء ورجال الأمن والضباط وإعطائهم الوقت الكافي للاستعداد فنيا عن طريق وضع خطة عملية لضبط أدلة الجريمة وقت معاينتها [4].

تأمين عدم انقطاع التيار الكهربائي المفاجئ لأن ذلك يتسبب في محو المعلومات من الذاكرة وبالتالي ضياع كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة[5].

ثانيا: الإجراءات التي يتعين إتباعها عند إجراء المعاينة:

– تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسوب وملحقاته مع مراعاة تسجيل وقت وتاريخ ومكان النقاط كل صورة[6].

---

[1] عمر أبو بكر بن يونس، الإثبات الجنائي عبر الإنترنت ، دار الفكر للنشر والتوزيع، 2013، ص 06.

[2] هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2015، ص186.

[3] نبيلة هبة هروال، المرجع السابق، ص 219.

[4] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الابتدائي في الجرائم الالكترونية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجمالية، عمان، الأردن، 2010، ص 216.

[5] عبد الفتاح بيومي حجازي، المرجع السابق، ص 217.

[6] خالد ممدوح إبراهيم، المرجع السابق، ص 172.

– عدم نقل أي مادة معلوماتية من مكان وقوع الجريمة إلا بعد إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي قد تؤدي إلى فقد البيانات المخزنة[1].

– ربط الأقراص الكومبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها، مما يتيح للمحققين قراءة بياناتها من دون تغييرها.

– قصر مباشرة المعاينة على المحققين الذين تتوافر الكفاءة العملية والخبرة التقنية في مجال المعلوماتية واسترجاع المعلومات والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحتويها مسرح الجريمة الإلكترونية[2].

وعلى ضوء ما تقدم يمكن القول بعدم كفاية المعاينة كإجراء تقليدي للإحاطة بكافة جوانب مسرح الجريمة الإلكترونية نظرا لمميزات الدليل الإلكتروني، فهو غير مرئي كما يسهل على المجرم محوه أو بتعديله بضغطة زر وفي جزء من الثانية وهو جالس وراء حاسوبه، لذا لنجاح المعاينة لابد من توفير فريق متخصص من ضباط الشرطة القضائية لديهم معرفة متميزة بالمعلوماتية عموما وبنظمها خصوصا وكيفية تشغيلها ووسائلها، وتقنيات إساءة استعمالها من قبل مستخدميها ولا يتأتى ذلك إلا بتكوينهم وتدريبهم وتجديد معارفهم قصد حصولهم على المهارات اللازمة في مجال الكشف عن الجرائم المستحدثة[3].

الفقرة الثانية: الخبرة التقنية في العالم الافتراضي:

الخبرة القضائية عموما هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين[4] عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر سواء لدى المحقق أو القاضي، وفي هذا

---

[1] عبد العال الدريبي محمد صادق إسماعيل، المرجع السابق، ص 296.

[2] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، مكتب الآلات الحديثة، مصر، 1994.

[3] يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم ، تخصص قانون خاص جامعة باجي مختار، عنابة 2016، ص 226.

[4] أمال عثمان الخبرة في المسالة الجنائية، رسالة دكتوراه كلية الحقوق جامعة القاهرة 1964. 68 وما بعدها. أنظر أيضا: عادل حافظ غانم، الخبرة في مجال الاثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968، ص 19 وما بعدها.

المجال نتطرق أولا إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية بصفة عامة، ثم نتناول ثانيا الجوانب الفنية التي تحكم إنجاز الخبرة التقنية المتعلقة بإثبات الجريمة الإلكترونية.

أولا: القواعد القانونية التي تحكم الخبرة القضائية:

وسنتناول من خلالها مفهوم الخبرة القضائية طرق اختيار الخبراء، وواجبات الخبير التقني وذلك من خلال النقاط التالية:

1 – مفهوم الخبرة القضائية:

*** تعريف الخبرة:**

يقصد بالخبرة: مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه[1].

كما يعرف الخبير الإلكتروني بأنه الشخص الذي تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة .[2]

*** طرق اختيار الخبراء:**

إذا كانت الاستعانة بالخبير في الجرائم التقليدية أمر بالغ الأهمية في إثبات الجريمة، فإن الاستعانة به في مجال إثبات الجرائم الإلكترونية يعد أمرا متطلبا و ضروريا بسبب التطور التقني السريع في مجال تقنية المعلومات، إذ لا يكشف غموض الجريمة إلا من طرف شخص على درجة كبيرة من العلم والدراية في مجال تخصصه[3] ، حيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة كما تحدد الأوضاع التي يجري فيها قيد الخبراء أو شطبهم بقرار من وزير العدل.

وقد ترك المشرع لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين بحسب المادة 147 من قانون الإجراءات الجزائية الجزائري.

---

[1] صغير يوسف الجريمة المرتكبة عبر الانترنت ماجستير منشورة، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص 88.

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الاثبات الجنائي بالأدل الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007،، ص 24.

[3] David forest et gautier kaufman, droit de l'informatique goaline éditeur, extenso edition, France, ,2010, p79.

وكذلك لم يحدد المشرع طبيعة من يقوم بالخبرة سواء كان شخصا طبيعيا، أو معنويا كمؤسسة متخصصة تعمل في مجال الحاسوب الذين يتم اللجوء إليهم خاصة في مجال الدليل الإلكتروني باعتبار أن هذا النوع من المؤسسات يملك موارد مادية من برامج و أجهزة حديثة وموارد بشرية من مهندسين متخصصين في الحاسوب والانترنت[1].

* **واجبات الخبير التقني:** له عدة واجبات تتمثل في:

- **حلف اليمين:** أوجب المشرع الجزائري لضمان صحة تقرير الخبير ونيل ثقة أطراف الدعوى، أن يحلف اليمين[2] قبل البدء في انجاز الخبرة.

- **إنجاز الخبير لأعمال الخبرة بنفسه:** لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر أو حكم الندب، وأن يستجيب للطلبات التي يقدمها أطراف الخصومة مثل: سماع أي شخص – قادر على إعطاء معلومات فنية[3].

- **الخضوع للرقابة القضائية:** يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه وأن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير هو مساعد للقاضي ومعاون فني لا أكثر[4].

- **إيداع الخبرة التقنية:** بعد انتهاء الخبير من أعماله التي كلف بها يقوم بإيداع الخبرة التقنية خلال المدة المحددة في أمر أو حكم الندب، وأن يقدم نتائج ما قام به من أبحاث فإن خال ذلك جاز للقاضي استبداله بغيره، كما يمكن أن يتخذ في حق الخبير الذي ثبت وقوع إهمال منه إجراءات تأديبية قد تصل إلى شطب اسمه من جداول الخبراء بقرار من الوزير.

المطلب الثاني: الإجراءات الحديثة للدليل الالكتروني:

تطرقنا في المطلب السابق على الاجراءات التقليدية ، فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة، وهذا ما قام به المشرع الجزائري من خلال التعديلات

---

[1] عائشة بن قارة مصطفى المرجع السابق، ص ص 141 142.

[2] حيث تنص المادة 145 من قانون الإجراءات الجزائية على يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية بيانها، أقسم بالله العظيم أن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص و أن أبدي رأي بكل نزاهة و استقلال ولا يجدد هذا القسم ما دام الخبير مقيدا في الجدول.....

[3] المادة 152 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[4] .Michaud le juge d'instruction et l'expert, R. S. c. 1975.p791

المتتالية لأحكام قانون الإجراءات الجزائية، وذلك بإدراج قواعد إجرائية جزائية جديدة وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد[1].

الفرع الاول: التسرب:

استحدث المشرع الجزائري إجراء التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التي تنص على: "عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية في المواد أدناه".

يلاحظ من خلال التعريف السابق أن التسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو الشريك[2].

والتسرب كغيره من الإجراءات الحديثة له ضوابط وشروط شكلية وأخرى موضوعية حتى يعتد به:

أولا: الضوابط الشكلية: تتعلق بما يلي:

1- تحرير التقرير:

يلزم ضابط الشرطة القضائية المكلف بعملية التنسيق بتحرير تقرير كتابي يتضمن بيان مفصل عن جميع العناصر المتعلقة بالعملية[3]، ويجب أن يذكر في التقرير ووفق الترتيب الزمني جميع المعلومات ذات الصلة كالأفعال التي استدعت حدوث عملية التسرب، وكذا تحديد هوية العناصر المشتبه تورطهم في الجريمة (أسمائهم و ألقابهم)، تحديد الكيفيات التي تم بها مخادعة الجناة، فيجب ذكر جميع العمليات منذ بداية التسرب حتى نهايته.

[1] يزيد بوحليط، المرجع السابق، ص 248

[2] سارة قادري، المرجع السابق، ص 42.

[3] أنظر المادة 65 مكرر 13 من قانون الإجراءات الجزائية الجزائري.

2 – الحصول على إذن بالتسرب:

تنص المادة (65) مكرر (11) من (ق.إ.ج) على : عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65) مكرر (5) أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب ضمن الشروط المبينة أدناه ، وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق، ومنه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا.

كما يجب أن يكون الإذن مكتوباً، وهذا وفق نص المادة (65) مكرر (15) التي تنص على: يجب أن يكون الإذن المسلم تطبيقا للمادة (65) مكرر (11) أعلاه، مكتوبا ... وذلك تحت طائلة البطلان ذلك أن الأصل. في العمل الإجرائي هو الكتابة وفقا لنص المادتين (138–139) من (ق.إ.ج) ، كما يشترط ذكر اسم الضابط المشرف، وهو ما نصت عليه المادة (65) مكرر (15) بقولها : يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا ... وذلك تحت طائلة البطلان، تذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته..."

3– مدة التسرب:

حددتها المادة (65) مكرر(15/3) حيث تنص على "..... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر ..... غير أنه ومراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة ضمن نفس الشروط الشكلية والزمنية السابقة، وحفاظا على حياة العون المتسرب من الخطر إضافة إلى الأشخاص المسخرين، أجاز المشرع للقاضي الذي رخص بعملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها، وذلك إذا وصل إلى علمه أن معلومات تفيد باحتمال كشف العملية من طرف المجموعة الإجرامية[1].

4 – إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية:

وذلك للحفاظ على السرية المطلوبة لنجاح عملية التي التسرب والتي حصرها المشرع بين القاضي الأمر بها (وكيل الجمهورية أو قاضي التحقيق)، وضابط الشرطة القضائية

[1] عبد المجيد حجازي، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص 60.

المشرف على العملية وكذا العون المتسرب. بعد الانتهاء من عملية التسرب يجب إيداع رخصة التسرب في ملف الإجراءات وهذا وفقا لنص المادة (65) مكرر (15/6) التي تنص على .... تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

ثانيا: الضوابط الموضوعية:

تتمثل الضوابط الموضوعية لعملية التسرب في شرطين رئيسيين هما:

1- التسبيب:

يعتبر التسبيب أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[1]، وهذا طبقا لنص المادة (65) مكرر (15/1) التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان..."

2- نوع الجريمة:

وقد حصرتها المادة (65) مكرر (5) من (ق.إ.ج) في سبعة أنواع هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد[2]. وعليه يجب أن تكون الجريمة جناية أو جنحة.

الفرع الثاني: اعتراض المراسلات والتقاط الصور وتسجيل الأصوات:

ومن خلال هذا الفرع سنقوم بتعريف كل من اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وكذا الضوابط التي تحكمهم وحجية الدليل الإلكتروني في التشريعين المصري والامريكي.

أولا: مفهوم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات:

وهنا سنتطرق لمفهوم لكل واحدة منهم على حدى.

---

[1] سيدهم سيدي محمد، محاضرة جول التسرب حسب تعديل قانون الإجراءات الجزائية محكمة فرندة مجلس القضاء تيارت في 20 / 03 / 2008، ص 03.

[2] أحسن بوسقيعة، التحقيق القضائي، دار ،هومة، ط2، الجزائر ، 2009، ص 114.

1: تعريف اعتراض المراسلات:

يقصد باعتراض المراسلات على أنه الإجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث وتتم بواسطة الوسائل السلكية واللاسلكية"[1].

من جانب آخر نجد المشرع الجزائري لم يعرف بإجراء اعتراض المراسلات بل اكتفى بوضع بتنظيم لهذه العملية بموجب المادة (65) مكرر 5 من قانون الإجراءات الجزائية التي تنص على "إذا اقتضت ضروريات التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

– وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو بسرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو النقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص..."

باعتبار المشرع الجزائري لم يتطرق إلى تحديد مفهوم اعتراض المراسلات فهل يقصد بها التنصت الهاتفي أم مجرد الاطلاع عليها ؟ أو يمتد إلى أكثر من ذلك من خلال ضبط كل ما له علاقة بوسائل المواصلات السلكية واللاسلكية؟

2: تعريف التقاط الصور:

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، غير أنه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذا الإجراء، وإنما نص على مجال تطبيقه وتوضيح إجراءات القيام بذلك، يقوم هذا الإجراء أساسا على استخدام الكاميرات، أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل

[1] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2014، ص 32.

مادي على اعتبار أن عدسة الكاميرا أصبحت من الأساليب العالمية والمطلوبة الإثبات الحالة بما تنقله من صور حية لحادثة معينة[1].

لقد شاع اليوم استخدام كاميرات رقمية بغرض المراقبة في الأماكن العامة والخاصة كالبنوك والمطارات وماكينات الصرف الآلي والمحلات والمستشفيات ... الخ قصد ضبط الجرائم وإثباتها[2] ويكون الاطلاع على صور هذه الكاميرات في حالات وقوع الجرائم بأمر من المحكمة، ولاشك أن ذلك يثير قضايا تتعلق بالخصوصية الشخصية. لذا يرى جانب من الفقه أن تركيب هذه الكاميرات يكون في الأماكن العامة فقط 3 بترخيص قانوني[3].

وعليه يربط هذا الإجراء الشخص أو الأشخاص في مكان واحد وفي وقت واحد، خاصة في ظل التطور التكنولوجي الرقمي الذي يسمح بالتصوير ليلا وبجودة عالية من خلال الكاميرا ذات العدسات فائقة التكبير والتي تستخدم أيضا الأشعة تحت الحمراء بما يمكن ضابط الشرطة القضائية من التقاط الصور الثابتة أو المتحركة للمشتبه فيه خلال جميع مراحل البحث والتحري[4].

3: تعريف تسجيل الأصوات:

يعرف التسجيل الصوتي بأنه: النقل المباشر والآلي للموجات الصوتية من مصادره بنبراتها ومميزاتها الفردية وخواصها الذاتية، بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه. كما تتم هذه العملية باستخدام وسائل تقنية خاصة لها صلة مباشرة بنوعيها السلكية واللاسلكية والتي من خلالها يتم بث الكلام المتفوه وتثبيته واستغلاله في التحريات، وهو إجراء تحقيقي تأمره به السلطة القضائية خلسة وينتهك سرية الأحاديث الخاصة بغية الحصول على دليل غير مادي للجريمة.

---

[1] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط صور والتسرب كالاجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة 1 الجزائر، العدد 33 جوان 2010.

[2] سارة قادري، المرجع السابق، ص 39.

[3] عبد الفتاح بيومي حجازي، المرجع السابق، ص 782.

[4] شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس لبنان. طاء 2011، ص 154.

إلا أن المشرع الجزائري لم ينص في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي مثل ما لم ينص على تعريف اعتراض المراسلات كما رأينا سابقا، إنما أشار لها في نص المادة (65) مكرر في الفقرة المعنيين من أجل التقاط وتثبيت وبث تسجيل الكلام المتفوه به بصفة وضع الترتيبات التقنية دون موافقة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية.

وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى جنائية حركتها السلطات القضائية قصد الوصول إلى الحقيقة، كما لا تعتبر أدلة واستغلال التسجيل الذي لا يتضمن اعتداء على حق من تم تسجيل صوته أو حديثه، كما هو الشأن في حالة تسجيل الأحاديث الإذاعية أو التلفزيونية أو الصحفية.

ثانيا: الضوابط التي تحكم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات:

حدد المشرع الجزائري من خلال قانون الإجراءات الجزائية شروط للقيام بهذا الإجراءات كونها تشكل انتهاكا لحرمة الحياة الخاصة للأفراد واعتداء على سرية مراسلاتهم واتصالاتهم.

1: الشروط الشكلية:

تتعلق بالضوابط الشكلية بإجرائيين هما :

* الحصول على إذن من طرف وكيل الجمهورية لابد من ضابط الشرطة القضائية الذي يباشر هذا الإجراء في عملية التحري والبحث أن يكون مستندا في ذلك على إذن من وكيل الجمهورية يخوله اللجوء إلى إجراء التقاط الصور واعتراض المراسلات وتسجيل الأصوات، وكذلك يمكن لضابط الشرطة القضائية أن يحصل على الإذن من طرف قاضي التحقيق المختص إذا كانت القضية معروضة عليه[1] ، وفي حالة قيام ضابط الشرطة القضائية بممارسة الإجراء دون إذن، فإن إجراءه الذي قام به يقع تحت طائلة البطلان.

ويشترط في الإذن أن يكون مكتوبا، ويتضمن عمل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم وكذا الأماكن المقصودة سواء كانت عامة

[1] أنظر: المادة 65 مكرر 5 من القانون رقم 05-22 المؤرخ في 20-12-2006 ، المعدل والمتمم لقانون الإجراءات، الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية عند 84 المؤرخة في 24 ديسمبر 2006.

أو خاصة وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، يسلم الإذن مكتوبا لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق[1].

* تحرير محضر عن العملية باعتبار محاضر الشرطة القضائية لها حجية في الإثبات، وجب على ضابط الشرطة القضائية الذي قام بإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات أن يقوم بتحرير محضر موقع عليه من طرفه يسرد فيه بالتفصيل العمليات التي قام بها[2].

أما مضمون المراسلات المسجلة والصور الملتقطة، فيقوم ضابط الشرطة بنسخ محتواها في محضر يودع بملف الإجراءات، أما إذا كانت تلك المراسلات أو الاتصالات بلغة أجنبية فيتم تسخير مترجم لترجمتها[3].

تتم عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65) مكرر (8)[4].

2: الضوابط الموضوعية:

تتعلق هذه الضوابط بنشوء الحق في اللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، وتتمثل هذه الضوابط في:

– أن يكون الإجراء من أجل التحري والكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

–غاية المراقبة وضرورتها، عبر المشرع الجزائري عن المصطلح بلفظة: إذا اقتضت ضرورة التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض

[1] أنظر : المادة 65 مكرر 5 من القانون رقم 06–22، المعدل والمتمم لقانون الإجراءات الجزائية.

[2] أنظر المادة 65 مكرر 9 من القانون رقم 06–22 المعدل والمتمم لقانون الإجراءات الجزائية.

[3] انظر: المادة 65 مكرر 10 من القانون رقم 06–22 المعدل والمتمم لقانون الإجراءات الجزائية.

[4] حيث تنص المادة 65 مكرر 8 من قانون الإجراءات الجزائية على: يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالعمليات المذكورة في المادة 65 مكرر 5 أعلاه.

الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد..."، وهذا حسب المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري.

– الجهة المكلفة بهذه العملية باعتبارها تمس بحرمة الحياة الخاصة، لا يقوم بها إلا ضابط الشرطة القضائية.

3: ضوابط التنفيذ :

تتعلق بكيفيات المراقبة ونتائجها والأدلة الناجمة عنها، لذا سمح المشرع من خلال نص المادة (65) مكرر 5 الفقرة (4) لضابط الشرطة القضائية الدخول إلى المكان المعني دون احترام الشروط الواردة في المادة 47 من قانون الإجراءات الجزائية وذلك باستخدام الترتيبات التقنية حيث نصت الفقرة الثانية من المادة 65 مكرر 05 على أن النيابة العامة يمكنها منح الإذن لضابط الشرطة القضائية لوضع الترتيبات التقنية، التي يتم عن طريقها التصنت على المحادثات وتسجيلها والتقاط الصور دون الحاجة إلى موافقة المشتبه فيه[1].

وفي حالة اكتشاف جرائم أخرى غير تلك التي يتم التحقيق فيها والواردة في الإذن فيمكن التحري بشأنها ولا يكون ذلك سببا في بطلان الإجراءات وهذا حسب أحكام المادة 65 مكرر 6 من قانون الإجراءات الجزائية الجزائري.

ثالثا : حجية الدليل الإلكتروني:

يثير حكم مخرجات الكمبيوتر في مجال الإثبات مسألتين هامتين هما مدى استيفاء هذه المخرجات لمتطلبات الدليل الكتابي ، ومدى حجيتها في مجال الإثبات الجنائي.

ولما هدف العملية الإثباتية هو إفراز دليل صحيح يعول عليه القاضي الجنائي في أحكامه، لذلك يتم البحث في مدى حجية تلك المخرجات وفقا لما قرره المشرع المصري في مجال الإثبات مع المقارنة بالتشريع الأمريكي وفقاً لما يلي .

1–حجية الدليل الإلكتروني في التشريع المصري:

جاء نص المادة (11) القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات بشأن الأدلة الرقمية على أنه " يكون للأدلة المستمدة أو المستخرجة من الاجهزة أو المعدات أو الوسائط أو الدعامات الالكترونية ، أو النظام المعلوماتي أو من برامج الكمبيوتر ، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الاثبات الجنائي

[1] انظر المادة 65 مكرر 5 من قانون الاجراءات الجزائية الجزائري.

متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية. ومفاد المادة سالفة الذكر أن المشرع المصري قد ساوي في الحجية بين الأدلة الرقمية وبين الأدلة الجنائية المادية التقليدية ، بشرط توافر الشروط الفنية المتطلبة لذلك.

وجديراً بالذكر أن التشريع المصري أتخذ نهج التشريعات اللاتينية المتمثلة في القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الإيطالي والإسباني وقوانين أمريكا اللاتينية[1].

2- حجية الدليل الإلكتروني في التشريع الأمريكي :

حسم المشرع الأمريكي حجية الدليل الإلكتروني بالنص عليه صراحة في القوانين الخاصة بالولايات المتحدة الأمريكية حيث نص قانون الحاسب الآلي لسنة 1984 الصادر في ولاية أيوا (IOWA) على أن مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي المخزنة بداخله.

المطلب الثالث: موقف التشريعات من الدليل الالكتروني:

فمن خلال هذا المبحث سنتطرق الى ثلاث مواقف ثلاث تشريعات وهم المشرع المصري وكذا المشرع المصري وفي الاخير المشرع الفرنسي.

الفرع الأول: موقف المشرع الجزائري من الدليل الالكتروني:

لم تفرد تشريعات الدول المنتمية للنظام اللاتيني كفرنسا وغيرها من الدول المتأثرة بها ومنها الجزائر، نصوص خاصة بقبول الدليل الإلكتروني، وهذا على أساس استنادها لمبدأ حرية الإثبات في المواد الجنائية تطبيقا لنظام الإثبات الحر. حيث نصت المادة (212) من (ق.إ.ج) على: يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه من جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات، مما لا يدع للشك في تطبيقها أمام كل الجهات القضائية الجزائية وبالتالي اعتمد المشرع الجزائري نظام الإثبات الحر كأصل ونظام الإثبات المقيد كاستثناء[2].

[1] أيمن عبد الحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، بدون ناشر ، 2005 ص 190.

[2] يزيد بوحليط، المرجع السابق، ص 288.

الفرع الثاني: موقف المشرع المصري من الدليل الالكتروني:

لم نلمس إقرار المشرع المصري حماية جنائية شاملة للاتصالات الشخصية الالكترونية، حيث اقتصرت الحماية الخاصة للاتصالات الالكترونية على تلك المتعلقة بالأحوال المدنية فقط دون غيرها لنص المادة 74 من قانون الأحوال المدنية على أنه " مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين يعاقب بالحبس ... كل من اطلع أو شرع في الاطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها... أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون وفقا للإجراءات المنصوص عليها فيه (المادة (13/1)، فإذا وقعت الجريمة على البيانات أو المعلومات أو الإحصاءات المجمعة وهى تلك تشتمل عليها السجلات والدفاتر الإلكترونية السابق ذكرها "سرا قوميا " التي لا يجوز الإطلاع عليها أو نشرها إلا المصلحة قومية أو علمية وبإذن كتابي من مدير مصلحة الأحوال المدنية أو من ينيبه (المادة 13 في فقرتها الثانية تكون العقوبة السجن ..... وتكون العقوبة الإشغال الشاقة المؤبدة إذا وقعت\ الجريمة في زمن الحرب .". دون أن نلمس نصا آخر يفهم من صياغته شموله لنوعي الاتصالات الالكترونية والتقليدية.

الفرع الثالث: موقف المشرع الفرنسي من الدليل الالكتروني:

نصت المادة 432 عقوبات فرنسي على معاقبة كل شخص عام أو مكلف بخدمة عامة بالحبس ثلاث سنوات والغرامة اذا قام أو سهل أو أمر عند مباشرته لعمله أو بمناسبته وفى غير الحالات المقررة قانونا باختلاس أو الغاء أو فض المراسلات أو كشف محتواها. كما نص في الفقرة الثانية بمعاقبة كل شخص عام أو مكلف بخدمة عامة اذا قام أو أمر أو سهل أثناء مباشرته لعمله أو بمناسبته وفي غير الحالات المقررة قانونا بالتقاط أو اختلاس مراسلات تتم أو تنقل أو تحمل بطريق الاتصالات وكذلك استعمالها وفض محتواها[1].

[1] عبد الفتاح بيومى، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي ، دار الكتب والوثائق القومية القاهرة ، 2009 ، ص 171.

خلاصة الفصل الثاني

ويعتمد هذا النظام على نظام الإثبات يتقيد بها القاضي الجنائي ، بل ترك حرية الإثبات الأطراف الخصومة في أن يقدموا ما يرون أنه مناسب الاقتناع القاضي الذي الإثبات تكون عقيدته من أي دليل يطرح أمامه، وله يقدر القيمة الإقناعية لكل منهما حسبما تتكشف لوجدانه، حيث لا سلطان عليه في ذلك إلا ضميره .

ويتضح من خلال ذلك أن القاضي له مطلق الحرية في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها ما دام كانت هذه الطرق مشروعة ، ويقوم بتقدير كل دليل طرح أمامه، لأن مبدأ الحرية والاقتناع لدى القاضي في تقدير الأدلة قائم ، وله أن يستمدها من أي مصدر يطمئن إليه دون أن يملى عليه المشرع حجية معينة أو يلزمه بإتباع وسائل محددة للكشف عن الحقيقة كقاعدة عامة.

ويبين القاضي الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه وإذا كان تقديره لا يخضع لرقابة النقض ، إذ ليس لها أن تراقبه في تقديره إلا أن لها أن تراقب صحة الأسباب التي استدل بها على هذا الاقتناع.

ولعل من أهم ما يبرر هذا المبدأ الذي خوله القانون للقاضي الجنائي هو ظهور الأدلة العلمية، مثل تلك الأدلة المستمدة من الطب الشرعي والتحاليل وتحقيق الشخصية ومضاهاة الخطوط ، ويلاحظ أن هذه الأمور لا يقبل أي قيود بشأنها عند تعويل القاضي عليها لتكوين عقيدته.

ويعد من أوضح النماذج لذلك القضية التي نظرت أمام محكمة أمن الدولة العليا والمتهم فيها أحد الأشخاص بالتخابر مع دولة إسرائيل، وقد تم تأجيل القضية لحين إحضار الديسكات ووحدات التخزين الداخلية بالكمبيوتر الخاص بالمتهم لتفريغ محتوياتها ، ولا شك أنه يعتبر دليلاً هاماً في القضية تعترف به المحكمة ، وقد يكون أساساً في تكوين عقيدة القاضي في حكمه.

خـــاتـــمـــة

خـــاتـــمـــة

أن دراسة موضوع الجريمة الالكترونية في ظل التشريع الجزائري تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة، بدأت في الظهور والانتشار في معظم المجتمعات من بينها الجزائر، ونظرا لارتباطها بتكنولوجيا متطورة أدت إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها.

ولا شك أن لقانون رقم 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، وتعديل قانون العقوبات بموجب قانون رقم 04/15 كانت لها أهمية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري.

كما أن هذا التعديل بعد قفزة في مجال التشريع كونه واكب التشريعات المقارنة بتجسيده معظم أحكام الاتفاقية الدولية للإجرام المعلوماتي من خلال تجريم الأفعال الدخول والبقاء غير المشروع داخل النظام المعلوماتي وتشديد العقوبة، إذ ترتب على ذلك مساس بالمعطيات أو نظام التشغيل للمنظومة المعلوماتية، المساس بالمعطيات أو تغييرها، استخدام المعطيات كوسيلة لارتكاب الجرائم المعلوماتية، حيازة وإفشاء ونشر واستعمال المعطيات المحصلة من هذه الجرائم، تجريم المساس بنظام التشغيل على أساس اعتبار المعطيات المعلوماتية من خلال الفقرة ج من المادة الثانية من قانون 09-04 تشمل برامج التشغيل.

كما يتضح لنا أن الثورة المعلوماتية فاقت الجهود و المحاولات التي بذلها رجال الفقه في ضبط تعريف جامع للجريمة الالكترونية نظرا لخصوصيتها وتميزها عن الجرائم التقليدية، كما فاقت كذلك اجتهادات المشرعين و رجال القضاء، فالقاضي مقيد عند نظره في الدعوى بمبدأ شرعية الجرائم و العقوبات وبالتالي لا يستطيع تجريم أفعال لم ينصص عليها التشريع صراحة حتى ولو كانت تشكل انتهاكاً لحقوق الغير وحرياتهم.

وتجدر الإشارة إلى أنه لا يكفي أن يتم مواكبة نصوص تشريعية للتشريعات المقارنة بدون تجسيدها من الناحية التطبيقية، إذ يجب العمل على تكوين فرق من الضبطية القضائية وقضاة متخصصين في هذا النوع من الجرائم ومدها بكافة الوسائل المادية والتقنية اللازمة لأداء عملها، من هنا يمكن أن نستخلص النتائج التالية:

* نشر الوعي لدى الهيئات والشركات وحتى المواطنين الذين قد تتعرض أنظمتهم المعلوماتية للانتهاك بضرورة التبليغ و الكشف عن هذه الجرائم، لأن التستر و الكتمان يؤثر سلباً في السياسة التي يمكن أن تضعها الدولة لمكافحتها.

*إذا سلمنا بخصوصية الجرائم المعلوماتية و تميزها عن الجرائم التقليدية سواء من حيث التقنيات و الوسائل المستعملة في ارتكابها أو من حيث السمات التي تميز مرتكبيها (المجرم المعلوماتي)، فإنه بات من الضروري العمل على ضبط و توحيد المصطلحات لتسهيل مهمة القضاء.

* ضرورة تفعيل التعاون الدولي لمواجهة الجرائم المعلوماتية و الحد منها، وذلك من خلال الدخول في اتفاقيات ومعاهدات جديدة تنص على تبادل الخبرات و المعلومات.

*بحكم أن الجريمة المعلوماتية جريمة متعدية الحدود فإنه من الضروري تدخل المشرع الجزائي الوطني والدولي لاستحداث نصوص قانونية مستقلة من شأنها تحقيق الردع العام والخاص لأن الاعتماد على النصوص التقليدية وتعديلاتها أثبت فشلها أمام الثورة المعلوماتية التي فاقت كل الجهود.

التوصيات:

بعض التوصيات العامة لإجراءات التحري في الجرائم الإلكترونية:

*الإبلاغ الفوري: في حالة ارتكاب جريمة إلكترونية، يجب على الضحية أو المؤسسة المتضررة إبلاغ الجهات الأمنية المختصة فورًا. يجب الاحتفاظ بأدلة الجريمة مثل الرسائل، والصور، والتسجيلات، والسجلات الرقمية.

*تأمين الأدلة: يجب تأمين الأدلة الرقمية بشكل آمن ومحمي لمنع التلاعب أو الحذف أو التغيير. يمكن القيام بذلك عن طريق إنشاء نسخ احتياطية للبيانات المهمة وتخزينها في مكان آمن.

*التعاون مع الجهات الأمنية: يجب تقديم التعاون الكامل للجهات الأمنية أثناء التحقيق في الجريمة الإلكترونية. يمكن تقديم المعلومات والأدلة المتاحة والتعاون في إجراءات جمع الأدلة الإلكترونية.

*استشارة خبراء الأمن الإلكتروني: في حالة جرائم إلكترونية معقدة، قد تحتاج إلى استشارة خبراء الأمن الإلكتروني لتحديد سبب الهجوم وتقديم المشورة في استعادة الأدلة وتحليلها.

*الحفاظ على السرية والخصوصية: يجب التأكد من اتخاذ الإجراءات اللازمة لحماية السرية والخصوصية أثناء التحقيق في الجريمة الإلكترونية. يجب اتباع الإجراءات القانونية والأخلاقية للتعامل مع المعلومات الشخصية والبيانات الرقمية.

*التحقق الفني: يمكن الاستعانة بشركات أمن البيانات والشركات المتخصصة في التحقق الفني لتحديد مصدر الاختراق وتقديم تقرير.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: بالغة العربية:

1-النصوص القانونية:

أ- الدستور:

1-دستور 28 نوفمبر 1996، المنشور بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996، ج ر عدد 76، الصادرة في 08 ديسمبر 1996، المتمم بالقانون رقم 02-03 المؤرخ في 10 أفريل 2002، ج ر عدد 25، الصادرة في 14 أفريل 2002، المعدل بموجب القانون رقم 1908 المؤرخ في 15 نوفمبر 2008، ج ر عدد 63، الصادرة في 16 نوفمبر 2008، المعدل والمتمم بموجب القانون رقم 16-01 المؤرخ في 26 جمادى الأولى 1437 الموافق ل 6 مارس 2016، الصادرة في 27 جمادى الأولى 1437 الموافقل 7 مارس 2016، ج ر عدد 14، المعدل والمتمم بموجب المرسوم الرئاسي رقم 20-251 المؤرخ في 27 عام 1442 الموافق ل 15 سبتمبر 2020 يتضمن استدعاء الهيئة الانتخابية للاستفتاء المتعلق بمشروع تعديل الدستور.

ب- النصوص التشريعية:

1-القانون رقم 05-22 المؤرخ في 20-12-2006 ، المعدل والمتمم لقانون الإجراءات الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية عند 84 المؤرخة في 24 ديسمبر 2006.

2-القانون رقم 02-15 المؤرخ في 23جويلية 2015 ، المعدل والمتمم لقانون الإجراءات الجزائية.

3-الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم.

4-القانون 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

5- قانون الاجراءات الجزائية المعدل بموجب القانون رقم 014/04 المؤرخ في 2004/11/10.

6- المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلى لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

2-الكتب:

1-أحسن بوسقيعة، التحقيق القضائي، دار ،هومة، ط2، الجزائر ، 2009.

2-أحمد خليفه الملط، الجرائم المعلوماتية ، دار الفكر الجامعي 2005.

3-احمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، دار النهضة العربية، القاهرة 1985.

4-أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

5-أيمن عبد الحفيظ ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية ، بدون ناشر، 2005.

6-جلال، ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.

7- جمال محمود الكردي: المحكمة المختصة والقانون الواجب التطبيق بشان دعاوى المسؤولية والتعويض عن مضار التلوث البيئة العابرة للحدود ، ط 01 ، دار النهضة العربية، الإسكندرية 2003.

8-جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001.

9- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنيت ، دار النهضة العربية، الإسكندرية، 2002،

10-خالد عباد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، 2011.

11-خالد محمد كدفور المهيري، جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية، دار الغرير للطباعة والنشر - دبي،2005.

12-خالد ممدوح إبراهيم إبرام العقد الإلكتروني، ط 2،دار الفكر الجامعي، أمام كلية الحقوق - الاسكندرية.

13- ربيعة زيدان، الجريمة الالكترونية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة الجزائر، سنة 2011.

14-سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية،1999.

15-شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس لبنان. طاء 2011.

16-صغير يوسف الجريمة المرتكبة عبر الانترنت ماجستير منشورة، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر، 2013.

17-ضياء علي أحمد النعمان، موسوعة التشريعات الالكترونية المدنية والجنائية، المطبعة والوراقة الوطنية، 2009،

18-عائشة بن قارة مصطفى حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية.

19-عبد العال الدريبي ومحمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر 2012.

20-عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الابتدائي في الجرائم الالكترونية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجمالية، عمان، الأردن، 2010.

21-عبد الله حسين علي محمود، سرقة المعلومات المحزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة 2001.

22-عبد المجيد حجازي، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012.

23-عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

24-عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، لبنان، (دس، ن) .

25-علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب والإنترنت دراسة مقارنة عالم الكتب الحديثة، الأردن 2004.

26-علي عدنان الفيل إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1 المكتب 94الجامعي الحديث، مصر، 2012.

27-عمر أبو بكر بن يونس، الإثبات الجنائي عبر الإنترنت ، دار الفكر للنشر والتوزيع، 2013.

28-عمر السعيد رمضان، شرح قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، الطبعة الأولى، 1986.

29-عمرو عيسى ألفقي، الجرائم الالكترونية، المكتب الجامعي الحديث – الإسكندرية 2006.

30-غنام محمد غنام دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت.

31-فرج عنواني هليل، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، مصر، 2006.

32-محمد العجلوني، د. زياد مشاقبة، استخدامات حاسوبية في الإدارة، ط1، دار اليازوري – عمان – الأردن 2011.

33-محمد سامي الشواء ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1998.

34-محمد زكي أبو عامر ، قانون العقوبات ، دار المطبوعات الجامعية ، 1986.

35-محمد علي قطب، الجرائم المستحدثة وطرق مواجهتها، ط1، دار الفجر للنشر والتوزيع القاهرة، 2009.

36- محمود نجيب حسني، شرح قانون الإجراءات الجزائية، دار النهضة العربية 2002.

37-منير الجنبيهي، ممدوح الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي الإسكندرية، 2006.

38- نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادي، دراسة نظرية وتطبيقية، القاهرة، مصر، 2004.

39- نبيل غيتس الالكترونية بعد الانترنت ترجمة عبد السلام رضوان، عالم المعرفة سلسلة كتب ثقافية شهرية يصدرها المجلس الوطني للثقافة والفنون والآداب – الكويت، يناير 1978.

40- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2007.

41- مأمون محمد سلامة: شرح قانون العقوبات القسم العام، ط 03، دار النهضة العربية، الاسكندرية، 2002.

42-هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2015.

43-هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، مكتب الآلات الحديثة، مصر، 1994.

44-هلالي عبد اللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، دار النهضة العربية، 1997.

3- المقالات:

1-أمال ،حابت الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، ورقة بحثية مقدمة الأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر.

2-حميد بلهادي حجية الدليل الرقمي في الإثبات الجنائي مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة الجزائر، المجلد التاسع، العدد الأول، 2019م.

3-سيدهم سيدي محمد، محاضرة جول التسرب حسب تعديل قانون الإجراءات الجزائية محكمة فرندة مجلس القضاء تيارت في 20 / 03 / 2008.

4-طارق محمد الجملي ، الدليل الرقمي في مجال الاثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية والقانون المنعقد في الفترة (28-2009/10/29) تنظمه أكادمية الدراسات العليا طرابلس .

5-عادل حافظ غانم، الخبرة في مجال الاثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968.

6-فاروق خلف الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015 كلية الحقوق، بسكرة، الجزائر.

7-فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط صور والتسرب كالاجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة 1 الجزائر، العدد 33 جوان 2010.

8-محمد علي الجمال، التقاط الدليل المادي من مسرح الجريمة، مجلة الدراسات العليا، العدد الثاني، يناير 2000.

9-نبيل إسماعيل عمر، قاعدة عدم قضاء القاضي بعلمه الشخصي، المجلة العربية للدراسات الأمني ، المجلد الأول، العدد الأول ، 1989، الرياض.

4- الرسائل والمذكرات الجامعية:

أ- الرسائل:

1-أمال عثمان الخبرة في المسالة الجنائية، رسالة دكتوراه كلية الحقوق جامعة القاهرة 1964.

حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت ، رسالة دكتوراه، حقوق عين شمس – 2005.

2-يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم ، تخصص قانون خاص جامعة باجي مختار، عنابة 2016.

ب- المذكرات:

1-سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2014.

2-نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر 2013.

ثانيا: باللغة الفرنسية:

1-Alan M. Gahtan, Electronic Evidence. Thomas Canada Limited, 1999.
2-Anabda Giet- Analysis of the police and criminal evidence act sec 69/computer generated evidence- WEB journal of Current Legal issuesUK, 1996 Issue 1.
3-David forest et gautier kaufman, droit de l'informatique goaline éditeur, extenso edition, France, .2010.
4-Gaston stefani- Georges Levasseur- Bernard Bouloc: Droit Penal General 17 ed 2000 Dalloz.
5-John Eaton & Jermy smothers'. A managers Guide to information Technology, London, Philip Allan, 1982.
6-Michaud le juge d'instruction et l'expert, R. S. c. 1975
7-Thierry Care Catherine Ginestet: Droiut Penal- Procedure - Penale: Dallozed.2000.
8- VIDAL (G), Cours de droit criminal et de science penitenterntniaire 8eme ed,mis a jour par Magnol, libraie Arthur Rousseau, paris, 1935.

ثالثا: المواقع الالكترونية:

1-الموقع الإلكتروني : www.arablawinfo.com.

الـــمـــــــلاحـــــــق

جامعة حمه لخضر
كلية الحقوق والعلوم السياسية
قسم الحقوق
تخصص ماستر قانون قضائي مهني

تقرير تربص ميداني بأمن ولاية الوادي

من اعداد الطلبة:

- يوسف عماد
- لزهر ضربان

تحت اشراف:

ضباط امن الولاية

السنة الجامعية 2023/2022

نحن طالبان سنة ثانية ماستر قانون قضائي مهني، المشرفين على التخرج وبعد استلامنا للترخيص الممنوح من طرف رئيس قسم الحقوق كلية الحقوق والعلوم السياسية بجامعة حمه لخضر بالوادي.

الهدف من الترخيص هو الاستفادة من التسهيلات المختلفة سواء من الهيئات العمومية أو الخاصة بما فيها القضائية والأمنية وذلك من اجل إنجاح التربص المكلفين يه الذي قمنا به في أمن ولاية الوادي بمكتب الجرائم المعلوماتية البحث والتحري.

وقد كانت مدة التربص الممنوحة من 2023/05/02 إلى غاية 2023/05/15 بحيث كانت مدة كافية لجمع المعلومات اللازمة لتجسيد العمل المكلفين به.

وقد تجسد عملنا على النحو التالي:

1/ الحضور إلى مقر امن الشرطة للولاية الوادي مكتب الجرائم المعلوماتية.

2/ التواصل مع الضباط المكلفين بالبحث والتحري في الجرائم المعلوماتية.

أولا: الحضور إلى مقر الأمن:

قمنا بالتوجه إلى مقر أمن الشرطة لولاية الوادي وعليه في باب الدخول وجدنا عون الشرطة بعد طرحه لنا سؤال ماذا تريدون وليه قدمنا له ترخيص الممنوح لنا، وبالتالي وجهنا إلى مكتب الاستقبال.

وهذا الاخير بعدما فصحنا له اننا طالبة ماستر مشرفين على التخرج وأبرزنا له الترخيص وبدوره وجهنا أيضا إلى مكتب الجرائم المعلوماتية بمقر الأمن الشرطة، وصعدنا إلى المكتب وطلبنا الاستئذان للدخول وقد حفونا باستقبال من قبل ضباط الشرطة وقدمنا له هويتنا الشخصية والتعريف بنا والعمل من أجله.

ثانيا: التواصل مع ضباط الشرطة مكتب الجرائم المعلوماتية:

بعد التعريف الخاص بنا والعمل الذي جئنا من اجله، فقد ادلينا مقدمون على مذكرة تخرج بعنوان اجراءات البحث والتحري في الجرائم الالكترونية بحيث أن ضابط الشرطة أفتتح بتحية السلام المتبادلة من الطرفين وفي مقدمة الكلام استفتح المادة الاولى من قانون العقوبات " لا جرعة ولا عقوبة أو تدابير امن بغير قانون" وعلى آثر هذه الجرائم فإن اجراءات التحري الخاصة تسقط على 6 قضايا وهي كالآتي:

- قضايا المخدرات
- قضايا الارهاب
- قضايا المساس بأنظمة المعالجة للمعطيات
- قضايا تبييض الأموال
- قضايا العابرة للحدود الوطنية

- قضايا الفساد

واما اساليب التحري الخاصة فهي التسرب والتنصت والتقاط الصور واعتراض المراسلات فهي تدخل في الجرائم الالكترونية

وقد بين لنا من هم الذين يتمتعون بالضبطية القضائية من خلال ما صب في نص المادة 15 من قانون الاجراءات الجزائية ضباط الدرك الوطني محافظ الشرطة وضباط الشرطة وذو الرتب في الدرك.

وقانون العقوبات في المادة 394، قانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وفيها حدد المدة القانونية الشخص الذي أقدم على الجرم بالحبس والغرامة المالية ،بحيث أن ضباط الشرطة القضائية في المادة 17 من قانون الإجراءات الجزائية بتلقي الشكاوى والبلاغات لإجراء التحقيق الابتدائي لهم في الجريمة الالكترونية لان الشرطة القضائية يقومون بتحقيق ابتدائي في حين الوكيل الجمهورية يسمى تحقيق أولي كما أن الشرطة القضائية أي الضبطية ,وأي إجراء يقدمون عليه لابد أن يقيده وذلك حسب المادة 18 من قانون الإجراءات الجزائية وفي الجرائم الالكترونية عندما تقع أو يتلقى ضباط الشرطة القضائية شكاوي أو بلاغات فلابد لهم من إجراءات متبعة وهي كالتالي :

- محضر سماع الضحية.
- محضر سماع المشتبه فيه.
- محضر تفتيش مسكن.
- محضر حجز وجرد.
- محضر إذن بالتفتيش الالكتروني.
- محضر التفتيش الالكتروني.
- شهادة ميلاد.
- استمارة المعلومات.
- في الأخير تقرير الإجمالي.

وقد تطرقنا في التربص إلى كيفية معالجة قضية إجراء التفتيش الالكتروني وتتجلي في سماع على محضر وبوقع فيه المشتبه ع فيه وعليه

فـان ضبـاط الشرطة يقـومون بإخطـار وكيـل الجمهوريـة وهـذا الإخطـار لا بـد له أن يكـون تقـرير مكتـوب وبعـدها يقومـون بإجـراء التحـري مـن وسـائل تقنيـة المتـاحة مـن قبـل جهـاز الأمـن الوطنـي

الـذي يقـوم بإجـراء حول المعطيـات التقنيـة المرتبة بالحسـاب تـم استخراجه مـن رقـم هاتف المرتبطـة بالحسـاب وضبـاط الشرطة القضـائية في الإجـراء تسخيـره تكليـف وكـالة الاتصـال تـابع للرقـم الحسـاب المشتبـه به و ذلك حسب المـادة 49 مـن قانون الإجراءات الجزائية الجزائـري والتعـرف علـى هويـة الشخص وتعـد الجـرائم الالكترونية جريمـة تلبس بهـا وفـي هـذا اللحظـة استصـدار بتفتيش هـاتف نقـال وتحـرير محضـر تفتيش مسكن إلى أخر إجراء الـذي تطرقنا إليـه سـابقا.

وقـد عالجنا فـي المكتـب قضيـة حساب بحيث أن مـن كان يستخـدم رقم حساب ع وينشر بعض المنشـورات التـي في محل المشتبه وعليـه فـان ضباط الشرطـة بالقسـم رودهم إلى الأخـذ بإجراء التحـري حـول هـذا الأخيـر ومن بعـد اخـذ الأذن مـن وكيـل الجمهـورية بـإذن التفتيـش المسكـن تبين ان مـن هـو الذي يستخـدم رقـم الهاتف ع وإنشـاء حسـاب دون علمـه .وان س ابن ع وتعـد الجريمـة الالكترونية في الوقـت الحـالي هي جريمة التي تتماشى مع العصر الحديث .

كما عالجنا قضية الضحية س الذي تعرض موقع التواصل الاجتماعي الفايسبوك إلى قرصنة من طرف ص والذي بدوره كان يقوم ببعض الاشياء المنافية وعليه اقدم س بتقديم شكوى على مستوى امن ولاية الوادي الذي أدلى أنه تعرض موقعه إلى القرصنة، وقد بشر رجال الأمن بالتحقيق في الجريمة الالكترونية وذلك باتباع الاجراءات التحري بتتبع رقم الهاتف والموقع الذي يستعمل فيه شبكة الاتصال وليس من شريحة الهاتف وقد ضبط ص من طرف رجال الأمن وبدورهم أقدم على توقيفه في الحال وحرروا محضر سماع المتهم وبدور رجال الأمن اخطار وكيل الجمهورية من اجل تسخيرة لتفتيش المنزل والذي كان فيه المتهم ص يستعمل جهاز الحاسوب.

لأن في التشريع الجزائري الذي يستعمل جهاز الحاسوب أو الهاتف فهو في حالة تلبس بالجرم الذي أقدم عليه.

بعد محضر السماع والتحقيق للمتهم بوضعه رهن الحبس المؤقت، لابد من عرضه على الطبيب لإتمام الإجراءات اللازمة بعد التحقيق الابتدائي من طرف ضباط الشرطة ويتم توجيهه لجهة التحقيق الأولي الذي يشرف عليها قاضي التحقيق ويسمى التحقيق الأولي لإثبات الجرم الذي أقدم عليه هذا الأخير، ليأخذ العقوبة المناسبة له.

- جريمة القذف عبر مواقع التواصل الاجتماعي هي جريمة عمدية ولذلك لابد من توفر القصد الجنائي وهو القصد العام حيث لا يتطلب القانون قصدا خاصا لها، وبتوافر القصد الجنائي وهو علم الجاني بان الوقائع التي سندها ولو كانت صادقة لا أوجبت عقاب لأسندت إليه ومع ذلك اتجهت ارادته الى اذاعة هذه الوقائع وعناصر والقصد الجنائي : وهي العلم والارادة.

- **نماذج من القذف:**

- قذف الهيئات: نصت عليه المادة 296 من قانون العقوبات الجزائري.
- قذف السلطات الدولة الثلاثة:

1-القذف الموجه لرئيس الجمهورية نص المادة 144 مكرر من قانون العقوبات الجزائري في صورة العلنية.

2-القذف الموجه إلى الرسول صلى الله عليه وسلم: نص المادة 144 مكرر2 من قانون العقوبات الجزائري.

3-القذف الموجه للسلطات الدولة الثلاثة عبر مواقع التواصل الاجتماعي:

- السلطة التنفيذية دستور 2020.
- السلطة التشريعية دستور 2020.
- السلطة القضائية دستور 2020.

- قذف المؤسسات العسكرية والهيئات العمومية والنظامية

- قذف المؤسسات العسكرية: وهو ما نصت عليه المادة 30 من دستور 2020 في جعله قضاء استثنائي.
- الهيئات العمومية والنظامية: وهو ما نصت عليه المادة 146 من قانون العقوبات

تعد جرائم التواصل الاجتماعي وخاصة الفايسبوك من اكبر الجرائم المنتشرة في الوقت الحالي وهي تعد أحدث الجرائم المتطورة تماشيا مع العصر الذي نعيش فيه اليوم.

الـــــفـــــهـــــرس

الفـــهـــــــرس

المحتويات	الصفحة
الإهداء	
الشكر والتقدير	
مقدمة	**أ–د**
الفصل الأول: الاطار المفاهيمي للجرائم الالكترونية	
تمهيد	**6**
المبحث الأول: مفهوم الجريمة الالكترونية	**7**
المطلب الأول: تعريف الجريمة الالكترونية	**7**
المطلب الثاني: خصائص الجريمة الالكترونية	**7**
المطلب الثالث: الطبيعة القانونية للجرائم الالكترونية	**13**
المبحث الثاني: الاختصاص في الجرائم الالكترونية	**15**
المطلب الأول: تحديد مفهوم شروط الاختصاص في مسائل الجريمة الالكترونية	**15**
المطلب الثاني: الإختصاص القضائي في الجريمة الإلكترونية	**16**
الفرع الأول: اختصاص النيابة العامة في تحريك الدعوى العمومية في مجال الجرائم الإلكترونية في التشريع الجزائري	**16**
الفرع الثاني : الاختصاص المحلي لقاضي التحقيق في جرائم الإلكترونية	**18**
الفرع الثالث: الصلاحيات المكانية للضبطية القضائية في الجرائم المعلوماتية	**19**
المطلب الثالث: قواعد الاختصاص في الجريمة الالكترونية	**20**
الفرع الأول: مبدأ الاختصاص الإقليمي والشخصي	**21**
الفرع الثاني: مبدأ الاختصاص العيني والعالمي	**24**
خلاصة الفصل	**27**
الفصل الثاني: الدليل الالكتروني للجرائم	
تمهيد	**29**

المبحث الأول: مفهوم الدليل الالكتروني	**30**
المطلب الأول: تعريف الدليل الإلكتروني	**30**
المطلب الثاني: أنواع وخصائص الدليل الإلكتروني	**31**
المطلب الثالث: شروط قبول الدليل الإلكتروني	**33**
الفرع الأول : الشروط الواجب توافرها في الدليل الإلكتروني	**33**
الفرع الثاني : تقدير أدلة الإثبات	**35**
المبحث الثاني: إجراءات الحصول على الدليل الالكتروني	**37**
المطلب الأول: الاجراءات التقليدية للدليل الالكتروني	**37**
الفرع الأول: التفتيش وضبط الادلة	**38**
الفرع الثاني: المعاينة والخبرة	**42**
المطلب الثاني: الاجراءات الحديثة للدليل الالكتروني	**48**
الفرع الأول: التسرب	**49**
الفرع الثاني: اعتراض المراسلات والتقاط الصور وتسجيل الاصوات	**51**
المطلب الثالث: موقف التشريعات من الدليل الالكتروني	**57**
الفرع الاول: موقف المشرع الجزائري من الدليل الالكتروني	**57**
الفرع الثاني: موقف المشرع المصري من الدليل الالكتروني	**58**
الفرع الثالث: موقف المشرع الفرنسي من الدليل الالكتروني	**58**
خلاصة الفصل	**59**
خاتمة	**61**
قائمة مراجع	**/**
الملاحق	**/**
الفهرس	**/**

ملخص:

إن إجراءات البحث والتحقيق في الجنائي العام هي الأساس في البحث والتحقيق في جرائم الالكترونية تماما كما هو الحال في باقي الجرائم الأخرى، أما عناصر البحث والتحقيق الجنائي الأخرى من عملية وفنية وغيرها فإن استخدامها يتوقف على ظروف كل جريمة، فلما اعتمد المشرع الجزائري نصوصا لتجريم الأفعال الواقعة في الوسط الإلكتروني والمستخدم فيها الأجهزة الإلكترونية وكل ما يمس المعالجة الألية للمعطيات بمفهوم الجريمة الإلكترونية مما استدعى المشرع الجزائري الى ادخال مجموعة من التعديلات على كل من قانون العقوبات وقانون الاجراءات الجزائية كما استحدث القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، اضافة الى القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية والقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الكلمات المفتاحية:

الجريمة الإلكترونية / الدليل الإلكتروني / الجنائي / التحري.

Abstract:

The procedures of research and investigation of the general criminal are the basis for the research and investigation of electronic crimes just as in other crimes, but the elements of research and criminal investigation of the general criminal process and other, its use depends on the circumstances of each crime. when the Algerian legislator adopted texts to criminalize the acts in the electronic environment and the use of electronic devices and all that affects the automated treatment of data in the concept of cybercrime, which necessitated the Algerian legislator to introduce a set of amendments to all amendments to all From the Penal Code and the Penal Procedure Act, Act 09.04 on special rules for the prevention and control of crimes related to information and communication technologies was introduced, in addition to Law 18.04 on the General Rules of Mail and Electronic Communications, and Law 18.07 on the.

Key words:

Electronic crime / Electronic guide / Criminal / Investigate.