وزارة التعليم العالي و البحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed El Bachir El Ibrahimi – BBA –
كلية الحقوق و العلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص : قانون الإعلام الآلي و الأنترنيت

الموسومة بـ :

التحقيـــق فـــــــــــي الجريمـــــــة الإلكترونيـــــــــة

إعداد الطالبة
بوبعاية ابتســـام

إشراف الدكتورة
هـــــودة دكدوك

بحضور لجنة المناقشة المكونة من السادة الأعضاء

الاسم و اللقب	الرتبة	الصفة
حمـــزة عياش	أستاذ محاضر أ	رئيســـــــا
دكدوك هـــودة	أستاذ محاضر ب	مشرفا و مقررا
مراد عجيـــري	أستاذ مساعـد أ	مناقشـــــــا

2022-2021

شكـــــر و عرفـــــــان

في البداية

الحمد لله عز وجل الذي أعطانا القوة و الصبر على اتمام هذا العمل العلمي المتواضع

ثم

أتوجه بجزيل الشكر و الإمتنان إلى الأستاذة **''دكدوك هودة''** لقبولها الإشراف على هذه المذكرة، إذ لم تبخل علي بإرشاداتها و توجيهاتها القيمة، و التي شجعتني و وقفت وراء هذا العمل

و

إلى رمز العلم و العمل الأستاذة **''سعاد قيرة''** على نصائحها الهادفة

كما أشكر أعضاء اللجنة الموقرة أساتذتي المحترمين

إهـــــداء

أهدي هذا العمل إلى من أوصانا الرحمن عليها

(وَقُل رَّبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا)

إلى من أحمل اسمه بكل فخر ...

إلى روح أبي الطاهرة، تغمده الله برحمته و أدخل فسيح جناته ...

إلى والدتي العظيمة حفظها الله و رعاها برعايته ... منبع الحنان ...

إليك يا أمي يا من تسكن الجنة تحت قدميها ...

حفظك الله يا أمي الغالية ...

إلى رفيقة دربي و سندي في الحياة أختي "سعـــــاد" ...

إلى إخوتي، أحبتي، الذين شاركوني حلو الحياة و مرها ...

"ميلود – عثمان – نبيل" تاج رأسي و ظهري الذي لا يميل ...

إلى أخوتي سعيدة و مليكة و أبنائهم كل واحد باسمه ...

إلى زوجات أخوتي و أبنائهم حفظهم الله و رعاهم من كل شر ...

"آية – أمينة – محمد – مهدي – عبد القهار – زكية – رقية" ...

إلى كل من وسعه قلبي و لم تسعه سطور مذكرتي ...

إلى كل من ساعدني في عملي ...

إلى جميع الزملاء و الأصدقاء ...

الفهـــــرس

العنـــــــوان	الصفحــة
شكر و عرفان	
إهداء	
مقدمـــة	**أ – د**
الفصل الأول : ماهية التحقيق الجنائي في الجريمة الإلكترونية	
المبحث الأول : الإطار المفاهيمي للتحقيق الجنائي في الجرائم الالكترونية	**8**
المطلب الأول : ماهية الجريمة الإلكترونية	**9**
الفرع الأول : تعريف الجريمة الالكترونية	**9**
الفرع الثاني : خصائص الجريمة الالكترونية	**15**
المطلب الثاني : ماهية التحقيق الجنائي	**18**
الفرع الأول : تعريف التحقيق الجنائي	**19**
الفرع الثاني : خصائص التحقيق و المحققين في الجريمة الالكترونية	**20**
المبحث الثاني : الأجهزة المكلفة بالبحث و التحري عن الجرائم الإلكترونية	**31**
المطلب الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال	**31**
الفرع الأول : التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال	**32**
الفرع الثاني : مهام و اختصاصات الهيئة الوطنية للوقاية من المتصلة بتكنولوجيا الاعلام و الاتصال	**33**
المطلب الثاني : الوحدات التابعة لسلك الأمن الوطني و الدرك الوطني	**35**
الفرع الأول : الوحدات التابعة لسلك الأمن الوطني	**35**
الفرع الثاني : الوحدات التابعة لسلك الدرك الوطني	**36**
الفصل الثاني : آليات التحقيق في الجرائم الإلكترونية	
المبحث الأول : إجراءات التحقيق في الحصول على الدليل الإلكتروني	**40**
المطلب الأول : القواعد الإجرائية التقليدية في الحصول على الدليل الإلكتروني	**41**
الفرع الأول : التفتيش و ضبط الأدلة	**41**
الفرع الثاني : المعاينـــة	**43**
الفرع الثالث : الخبـــرة	**44**
المطلب الثاني : القواعد الإجرائية الحديثة في الحصول على الدليل الإلكتروني	**46**
الفرع الأول : التسرب الإلكتروني	**46**
الفرع الثاني : اعتراض المراسلات و المراقبة الإلكترونية	**47**
المبحث الثاني : القيمة القانونية للدليل الالكتروني	**50**
المطلب الأول : مشروعية الدليل الإلكتروني	**50**
الفرع الأول : ماهية الدليل الإلكتروني	**51**
الفرع الثاني : ماهية الدليل الإلكتروني	**53**
الفرع الثالث : مشروعية الدليل الإلكتروني في التحصيل	**57**
المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي	**58**
الفرع الأول : شروط اكتساب الدليل الإلكتروني حجية الإثبات الجنائي	**59**
الفرع الثاني : موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجنائي	**62**
خاتمـــة	**66**
قائمة المراجع و المصادر	

مقدمـــــــة

مقدمـــــة

دخل العالم في السنوات الأخيرة مرحلة جديدة من التطور الفكري و المعرفي الهائل و الغير معهود، و ذلك بفضل التطور العلمي في مجال تكنولوجيا الإعلام و الاتصال، و هذا ما وفر مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة الاقتصادية، الاجتماعية، الثقافية، و العلمية. ولا شك أن هذه الثورة المعلوماتية الهائلة قد انعكست بصورة ايجابية على كثير من جوانب الحياة المعاصرة بسبب ما توفره من الوقت و الجهد و التكلفة عن الانسان، و تجعل حياته اليومية أكثر سهولة حيث أصبح جهاز الكمبيوتر وسيلة لا يمكن الاستغناء عنها في حياتنا اليومية.

و بالرغم من هذه المزايا الهائلة التي تحققت و التي هي بصدد التحقق كل يوم بفضل التطور العلمي على جميع الأصعدة و في شتى الميادين، إلا أن هذه الثورة التكنولوجية صاحبتها جملة من الانعكاسات السلبية و الخطيرة جراء الاستخدام المفرط لهذه التقنية، فأصبحت تستخدم في خدمات غير مشروعة و أصبحت محلا لارتكاب الجرائم حيث أدى لبروز ظاهرة إجرامية حديثة في العالم الافتراضي سميت "بالجريمة الالكترونية"، و التي تعد من أخطر و أعقد الجرائم على الإطلاق.[1] فهي جريمة سرية تقنية سهلة الارتكاب تنشأ في الخفاء و في بيئة إلكترونية إفتراضية، و هي كل فعل يرتكب باستخدام الحاسب الآلي و شبكة الأنترنيت، و مرتكبو هذه الجريمة يتمتعون بالذكاء و بمهارات و خبرات تقنية عالية، و هم أشخاص غير عدوانيين و لا يتمتعون بالعنف، و تميزت الجريمة الالكترونية بعدة خصائص تميزها عن الجريمة التقليدية، فهي جريمة عابرة للحدود و تتم عبر شبكة إتصال لا متناهية غير مجسدة و غير مرئية و غير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، كما

[1] عادل يوسف عبد النبي الشكري، **الجريمة المعلوماتية و أزمة الشرعية الجزائرية**، كلية القانون، جامعة الكوفة، العدد 7، 2008، ص 112

أنها جريمة صعبة الإثبات و الإكتشاف،[1] ذلك أن إثبات هذه الجريمة يحيط به الكثير من الصعوبات لأن مرتكبها لا يترك أثرا خارجيا فيصعب إيجاد دليل مادي.

لا تخلوا الجريمة الإلكترونية من الأركان الثلاثة المتواجدة و المتشابهة في الجريمة التقليدية، فهي تقوم بالركن الشرعي و هو الصفة الغير مشروعة للفعل الذي يقوم به الجاني، بالإضافة إلى الركن المادي و هو كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، و ينقسم الركن المادي في الجريمة المادية إلى ثلاثة عناصر، السلوك الإجرامي، النتيجة الإجرامية، و العلاقة السببية. أما الركن المعنوي في الجريمة المرتكبة عبر الأنترنيت مجسد في الإرادة الجرمية لدى الفاعل و توجيه هذه الإرادة للقيام بعمل غير مشروع جرمه القانون، فهي تعتبر جريمة قصدية عمدية تتطلب العلم و الإرادة.

إن التمييز بين الجرائم الإلكترونية و الجرائم التقليدية إجرائيا سواء من حيث الاختصاص أو إجراءات التحقيق أو وسائل الإثبات هام جدا، فالتحقيق في الجرائم الالكترونية تختص به نيابة متخصصة وفق إجراءات و قواعد إثبات خاصة يساعدها في ذلك ضابذة قضائية متخصصة بالجرائم الإلكترونية، على عكس الجرائم التقليدية التي تختص بالتحقيق فيها النيابة العامة يساعدها في ذلك ضابطة قضائية ذات اختصاص عام وفقا لقواعد التحقيق و الإثبات التقليدية.

تتبع أهمية الدراسة إلى أهمية الموضوع، فالتحقيق في الجرائم الإلكترونية و كيفية ضبط الأدلة الرقمية و جمعها من الموضوعات المستحدثة و المتطورة و ذلك بتعميق المعرفة في مجال التحقيق و الإجراءات القانونية الصحيحة الواجب اتباعها من قبل السلطات القضائية المختصة في كشف هذه الجرائم.

[1] صغير يوسف، مرجع سابق، ص 14

تهدف هذه الدراسة إلى تسهيل إجراءات التحقيق و ملائمة السياسات وصولا إلى تحقيق فعال في الجرائم الإلكترونية، و كذلك تهدف الدراسة إلى فحص و تحديد العوامل المؤثرة في الوصول إلى تحقيق جنائي ناجح و التغلب على الصعوبات و المعضلات التي تعترض طريقه.

ما يكتنف هذا الموضوع من صعوبات ترجع في الأساس إلى حداثة الموضوع وما يتسم به من صبغة علمية بحتة جديدة و غريبة في تصورنا عن رجال القانون، إذ لم ينل حظه بعد من البحث و التمحيص على مستوى الفقه الجنائي، كما أن معظم الدراسات و الأبحاث القانونية التي تناولت الجريمة الإلكترونية تركز على الجانب الموضوعي فقط ما نتج عنه ندرة و قلة المراجع و المؤلفات التي تعرضت للجانب الإجرائي، و هذا ما أثار اهتمامنا لهذا البحث.

من هنا نطرح الإشكالية التالية :

- **ما مدى خصوصية التحقيق الجنائي في الجريمة الإلكترونية ؟**

و نظرا لخصوصية الموضوع و طبيعته القانونية التي تفرض علينا المنهج المتبع، فقد اخترنا منهجا يلم بدراسة الموضوع من كل جوانبه و هو المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية ذات الصلة بالموضوع، و الرجوع إلى رسائل و بحوث و مراجع قانونية و جمع الحقائق و البيانات و وضعها في البحث.

و من الدراسات السابقة التي تناولت موضوع التحقيق في الجريمة الإلكترونية، و من خلال عملية البحث التي قمنا بها عبر المراجع المتعلقة بالموضوع، و نظرا لحداثته، فقد وجدنا رسالة دكتوراه للطالب سعيد على نعيم المعنونة "بآليات البحث و التحقيق في الجرائم المعلوماتية"، و كذلك رسالة ماجيستير للطالب أدهم باسم البغدادي "وسائل البحث

و التحري في الجرائم الإلكترونية"، و أطروحة ماجيستير للطالب صغير يوسف تحت عنوان "الجريمة المرتكبة عبر الأنترنيت"، و كذلك رسالة ماجيستير عبد الله بن حسين آل حجراف القحطاني بعنوان "تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية".

إن الهدف الرئيسي من وراء هذه الدراسة هو تزايد استخدام الحاسوب و الأنترنيت و ظهور و نمو التجارة الإلكترونية الدولية، فإن هدفها الرئيسي هو تنظيم التجارة الدولية و حمايتها من الأعمال غير المشروعة و تجنب الاحتيال و الغش و سرقة المعلومات من أجل استقرار التعامل و شعور الناس بالثقة و الإطمئنان، أي أن الجرائم المرتبطة بالحاسوب و الأنترنيت تدخل في عدد الجرائم المنظمة التي لها صفة الاستمرارية، و كذلذ يمكن أن ترتكب بشكل فردي مما يوجب توفير الحماية الجنائية لها و إدراج نصوص قانونية تجرمها في قانون العقوبات، و الإجراءات القانونية الصحيحة الواجب اتباعها من قبل النيابة العامة و الضوابط العدلية في كشف جريمة الحاسوب و الأنترنيت و آليات الإثبات الجنائي على المتهم المقترف لهذه الجرائم و الطرق الفنية التي تقوم بها السلطة المختصة بالتحقيق في كشف الجريمة، و قم تم تقسيم البحث إلى فصلين :

يتضمن الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية، إذ يحتوي على مبحثين، المبحث الأول ماهية الجريمة الإلكترونية، أما المبحث الثاني فيتضمن الأجهزة المكلفة بالبحث و التحري عن الجرائم الإلكترونية.

أما الفصل الثاني فقد تم تخصيصه لدراسة آليات التحقيق في الجرائم الإلكترونية، و بدوره يحتوي على مبحثين، تضمن المبحث الأول إجراءات التحقيق في الحصول على الدليل الإلكتروني، و المبحث الثاني تضمن القيمة القانونية للدليل الإلكتروني في مجال الإثبات الإلكتروني

الفصل الأول

ماهية التحقيق الجنائي في الجريـــمة الإلكترونيـــة

تمهيد

تعد الجرائم الالكترونية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة الكثر من الغموض، لأجل ذلك فقد بدا لنا أنه و قبل الخوض في الاجراءات التي تنطبق على الجرائم الالكترونية أن ننوه على جانب من القواعد الموضوعية لهذه الظاهرة الإجرامية، إذ يجب الإلمام بماهية الجرائم الالكترونية و طبيعتها و إظهار موضوعها و خصائصها، و هذا حتما في منظورنا يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة من طرف القائمين على مكافحتها.

و على ضوء ذلك، سيتم تقسيم هذا الفصل إلى الإطار المفاهيمي للتحقيق الجنائي في الجرائم الإلكترونية و الأجهزة المكلفة به، أما المبحث الثاني سيكون تحت عنوان الأجهزة المكلفة بالبحث عن الجريمة الالكترونية.

المبحث الأول : الإطار المفاهيمي للتحقيق الجنائي في الجرائم الإلكترونية

للتحقيق أهمية في إثبات وقوع الجرائم و إقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها، و هو كما يدل عليه اسمه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم بعد جمع الأدلة القائمة على الجريمة، و من يقوم بالتحقيق هم الضبطية القضائية و القضاة وفقا لإجراءات البحث و التحري المحددة وفقا لقانون الإجراءات الجزائية، و لكي نتعرف على التحقيق الجنائي، نتطرق أولا بالتعرف على الجريمة الإلكترونية ثم نتناول التحقيق و هذا ما سنقدمه في هذا المبحث.[1]

[1] صغير يوسف، مرجع سابق، ص 7

المطلب الأول : ماهية الجريمة الإلكترونية

الفرع الأول : تعريف الجريمة الإلكترونية

تعد الجرائم المعلوماتية من الجرائم المستحدثة و التي ظهرت في عصرنا الحديث، و السبب يعود إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة الكمبيوتر و شبكات الأنترنيت و المواقع الالكترونية.[1]

أولا : التعريف الواسع للجريمة الإلكترونية

إزاء الانتقادات التي وجهت إلى الاتجاه الاول، حاول الفقهاء تعريف الجريمة الإلكترونية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق للتصدي لظاهرة الإجرام الإلكتروني.[2]

و على عكس الاتجاه السابق، فإن أنصار هذا الاتجاه يذهبون إلى توسيع مفهوم الجريمة الإلكترونية، حيث يرى الفقيهان (Credo/Michel) بأنها تشمل استخدام الحاسب كاداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد هذه الجريمة لتشمل الاعتداءات المادية سواء كان هذا الاعتداء على الحاسوب ذاته، أو المعدات المتصلة به، و كذلك الاستخدام غير المشروع لبطاقات الإئتمان، و انتهاك ماكينات الحسابات الآلية بما يتضمنه من شبكات

[1] عديلة مراد، مراد عبدلي، **الجريمة الالكترونية في التشريع الجزائري**، مذكرة لنيل شهادة ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، 2021، ص 14

[2] أدهم باسم نمر البغدادي، **وسائل البحث و التحري عن الجرائم الالكترونية**، رسالة ماجيستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص ص 7-8

تمويل الحسابات المالية بطريقة إلكترونية و تزييف المكونات المادية و المعنوية للحاسوب، بل و سرقة الحاسوب في حد ذاته أو مكون من مكوناته.[1]

تناول رأي آخر من الفقه تعريف الجريمة الإلكترونية بأنها "عمل أو إمتناع يأتيه الانسان إضرار بمكونات الحاسوب و شبكات الاتصال الخاصة به التي يحميها قانون العقوبات و يفرض لها عقابا".

عرفت في إطار المنظمة الأوروبية للتعاون و التنمية الاقتصادية بانها "عمل أو امتناع من شأنه أن يؤدي إلى الإعتداء على الأموال المادية و المعنوية[2] يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية"، و جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين المنعقدة في فيينا سنة 2000 تعريف الجريمة الإلكترونية كما يلي :

"يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، و الجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".

لاشك أن هذا الاتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسوب الآلي في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا، لا يمكن إعطاؤها وصف الجريمة

[1] عادل يوسف عبد النبي الشكري، **الجريمة المعلوماتية و أزمة الشرعية الجزائرية**، كلية القانون، جامعة الكوفة، العدد 7، 2008، ص ص 112-113

[2] عديلة مراد، عبدلي مروان، مرجع سابق، ص 15

الإلكترونية على سلوك الفاعل لمجرد أن الحاسب أو أحد مكوناتها المادية كانت محلا لفعل الإختلاس.[1]

ثانيا : التعريف الضيق للجريمة الإلكترونية

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية التي تتطلب قدرا كبيرا من المعرفة التقنية و أن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية.

من التعريفات التي وضعها أنصار هذا الاتجاه أيضا ما ذهب إليه الفقيه (Merwe) حيث يرى أن الجريمة الإلكترونية هي الفعل الغير مشروع الذي يدخل في ارتكابه الحاسب الآلي، أو هي الفعل الإجرامي الذي يستخدم في ارتكابه الحاسب الآلي كأداة رئيسة أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات، و عرفها آخرون بأنها "الجرائم التي تلعب فيها بيانات الكمبيوتر و البرامج المعلوماتية[2] دورا هاما أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسة".

فيما ذهب الفقيه (Rosbalt) على أنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تغييرها أو حذفها أو التي تحول عن طريقه".

[1] مرجع نفسه، ص 16

[2] عبد الحكيم مولاي ابراهيم، **الجرائم الالكترونية**، مجلة الحقوق و العلوم الانسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الثاني، العدد 23، 2015، ص 213

حسب الدكتورة (هدى فشقوش) هي "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات أو هي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات".

عرفها كل من (A. Hard/Laster.R.Tott) بانها "تلك الجرائم التي قد يكون قد حدث في مراحل ارتكابها بعض العمليات الفعلية داخل الحاسوب"، و بمعنى آخر هي التي يكون الحاسب الآلي فيها دورا إيجابيا أكثر من سلبيته.

ما يؤخذ على التعريفات السابقة أنها جاءت قاصرة على الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة و البعض الآخر ركز على وسيلة ارتكابها و البعض الآخر على معيار النتيجة.[1]

ثالثا : تعريف الجريمة الإلكترونية في التشريع الجزائري و التشريعات المقارنة

أولا : تعريف المشرع الجزائري للجريمة الإلكترونية

تبنى المشرع الجزائري للدلالة على الجريمة الالكترونية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الإعتداء على هذا النظام، فإذا تخلف هذا الشرط الأولي لا يكون هناك مجال لهذا البحث.[2]

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة تحقيقه، فضلا عن أنه تعبير يخضع للتطورات السريعة و المتلاحقة

[1] صغير يوسف، مرجع سابق، ص 8

[2] عيدة بلعايد، **خصوصية التحقيق في الجريمة المعلوماتية**، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية، جامعة مولاي طاهر، سكيكدة، العدد 06، 2011، ص 132

في مجال فن الحسابات الآلية، لذلك فالمشرع الجزائري على غرار التشريع الفرنسي، لم يعرف نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من الفقه و القضاء.[1]

ثانيا : تعريف الجريمة الإلكترونية في التشريعات المقارنة

أ. تعريف الجريمة الإلكترونية لدى بعض التشريعات العربية

اختلفت التشريعات العربية في تعريف الجريمة الإلكترونية، و مع النمو المتسارع لاستخدام شبكة الأنترنيت ظهرت أنماط من جرائم مستنبطة على هذا النوع من الإجرام مما أدى إلى تنوع التعاريف بشأن هذه الجريمة المستحدثة.

1. تعريف المشرع المصري

بالعودة للمشرع المصري، نجده لم يقم بتعريف الجريمة بل ترك مسألة تعريف الجريمة الإلكترونية للفقه، و بالتالي اختلف الفقهاء في تعريفها، فهناك من عرفها من الزاوية التقنية أو الفنية على أساس انها "عمل أو امتناع يأتي أضرار بمكونات الحاسب الآلي و شبكات الاتصال الخاصة به التي يحميها قانون العقوبات و يفرض لها عقابا".

فهي تنشأ عن استخدام غير مشروع لتقنية المعلوماتية و يهدف إلى الإعتداء على الأموال أو الأشياء المعنوية.[2]

كما يعرفها البعض الآخر من الفقهاء على أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو

[1] مرجع نفسه، ص ص 133-134

[2] بوشعرة أمينة، موساوي سهام، **الإطار القانوني للجريمة الالكترونية**، مذكرة ماستر، جامعة عبد الرحمن ميرة، بجاية، 2018، ص 9

الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة و إساءة استخدام المخرجات".

2. تعريف المشرع السعودي

عرف المشرع السعودي الجريمة الإلكترونية من خلال نظام مكافحة جرائم المعلوماتية بأنها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[1]، فبالتالي، فالجريمة الإلكترونية بحسب هذه المادة عن "عبارة عن سلوك إجرامي يستخدم فيه الحاسب الآلي أو شبكة المعلوماتية كوسيلة لحدوث هذا النوع المستجد من الجرائم، كما نجد أن نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية عرف من جهته الجريمة الإلكترونية على غرار بعض التشريعات العربية التي تركت مسألة تعريفها للفقه كالمشرع الجزائري و المشرع المصري، و من جهة أخرى قام هذا النظام بتحديد أنواع الجرائم المعلوماتية و العقوبات المقررة عليها.

ب. تعريف الجريمة الإلكترونية في بعض التشريعات الأخرى

لا يوجد مصطلح موحد للدلالة على الجريمة الإلكترونية، و إنما فقد تعددت التعاريف بشأنها، لذا نقتصر بعرض جهود كل من فرنسا و الولايات المتحدة الأمريكية في مجال تعريف هذا النوع المستجد من الجرائم.

1. تعريف المشرع الفرنسي للجريمة الإلكترونية

المشرع الفرنسي لم يعرف بدوره الجريمة الإلكترونية، و إنما نص على تجريم بعض الأفعال المساهمة في حدوثها ضمن نصوص قانونية، ترك مسألة تعريف الجريمة الإلكترونية للفقه، لذا ذهب الفقهاء في تعريف الجريمة الإلكترونية في مذاهب شتى، و وضعوا تعريفات مختلفة، و من الفقه الفرنسي،

[1] مرجع نفسه، ص 10

يعرف الفقيه (Masse) جريمة الكمبيوتر بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".[1]

كما يعرفها الفقيهان الفرنسيان (Vinaut/Stane) بانها "مجموعة من الأفعال المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب".

و نجد أن المشرع الفرنسي قام بإدراج الفصل الثالث من قانون العقوبات الفرنسي تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" للدلالة على الجريمة الإلكترونية، و يظهر ذلك في تجريمه لبعض الأفعال المساهمة في حدوث الجريمة الإلكترونية، كتجريمه لفعل البقاء و الدخول بطريقة الغش إلى نظام المعالجة الآلية للمعطيات، و بالتاي فالمشرع الفرنسي لم يعرف الجريمة الإلكترونية بل اكتفى بتجريم بعض الأفعال التي تساهم في حدوث الجريمة الإلكترونية.[2]

2. تعريف المشرع الأمريكي للجريمة الإلكترونية

يتبنى الخبير الأمريكي (Parker) مفهوما واسعا للجريمة الإلكترونية، حيث يشير إلى أنها "كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".[3]

الفرع الثاني : خصائص الجريمة الإلكترونية

تعتبر الجريمة المرتكبة عبر الأنترنيت من بين الجرائم المستخدثة التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجرائم التقليدية و التي ترتكب في العالم المادي، و لذلك تتميز بخصائص و سمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها

[1] بوشعيرة أمينة، موساوي سهام، مرجع سابق، ص 11

[2] عادل يوسف عبد النبي شكري، مرجع سابق، ص 115

[3] عديلة مراد، عبدلي مروان، مرجع سابق، ص 17

العالم من قبل، و سوف نسرد هذه الخصائص التي ميزت الجريمة الإلكترونية عبر الأنترنيت على النحو التالي :

أولا : جريمة عابرة للقارات

من أهم الخصائص التي تميز الجريمة الإلكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الأنترنيت و تقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد بسبب السرعة الهائلة في تنفيذها، فيمكن أن تقع الجريمة في دولة من طرف الجاني و المجني عليه في دولة أخرى في وقت يسير جدا.[1]

و من أهم القضايا التي أكدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة "الايدز" و تتلخص وقائعها عام 1989 حيث قام أحد الأشخاص المدعو "جوزيف بيب" بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح بمرض نقص المناعة المكتسبة،[2] إلا أنها كانت في الحقيقة تحتوي على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يطلب الفاعل من خلالها مبلغ مالي يرسل إلى عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد الفيروس، و في 03 فيفري 1990 تم إلقاء القبض عليه، و تثير خاصية عالمية الجريمة الإلكترونية عدة آثار قانونية أهمها القانون الواجب التطبيق عليها و القضاء المختص بها.[3]

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة، الطبعة الأولى، عمان، 2008، ص 50

[2] عادل يوسف، مرجع سابق، ص 114

[3] عادل يوسف، مرجع نفسه، ص ص 115-116

لذا بات من الضروري ايجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام اتفاقيات دولية خاصة بتسليم المجرمين و الوسائل الكفيلة بمكافحة هذا النوع من الجرائم.[1]

ثانيا : صعوبة إثبات و إكتشاف الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية جريمة مستحدثة تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي.

على اعتبار هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء كان في تجميدها أو في إدخالها إلى الحاسوب المرتبط بشبكة المعلومات و لغرض الحصول على معلومات معينة و قد ترتكب هذه الجرائم في معالجة الكلمات أو النصوص، و تمكن المستخدم من تحرير الوثائق و النصوص على الحاسوب مع إمكانية التصحيح و التعديل و المسح و التخزين و الاسترجاع و الطباعة.[2]

فإن إثبات هذه الجريمة يحيط به الكثير من الصعوبات و التي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا بحيث يصعب ايجاد دليل مادي يدين مرتكب الجريمة كون أمر طمس الدليل و محوه كليا من قبل الفاعل في غاية السهولة و في زمن قصير جدا، و من يتعذر عليه إن لم يكن مستحيلا ملاحقة و كشف شخصيته خاصة في حالة تفتيش الشبكات، كما قد تكون البيانات المراد البحث عنها مشفرة ولا يعرف شفرة دخوله إلا أحد العاملين على الشبكة، و هنا تتأثر مسألة مدى مشروعية إجباره على فك الشفرة، كما يصعب أيضا ملاحقة مرتكبي الجرائم الإلكترونية الذين

[1] عبد الحكيم مولاي ابراهيم، مرجع سابق، ص 214

[2] نهلا عبد القادر المومني، مرجع سابق، ص 53

يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه.

ثالثا : الجريمة الإلكترونية جريمة مستحدثة

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطار جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم الإلكترونية من الجرائم المستحدثة حيث أن التقدم التكنولوجي الذي تحقق خلا السنوات القليلة المالضية جعل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته و إمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها.

رابعا : خصوصية مرتكب الجريمة الإلكترونية

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن خصائص المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي و معرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف في الجرائم الإلكترونية فهي جرائم فنية تقنية في الغالب، و مرتكبوها غالبا ما يكونون من ذوي الاختصاص في مجال تقنية المعلومات الإلكترونية، فيتمتع مجرموها بقدر لا يستهان به من المهارة بتقنيات الحاسوب و الأنترنيت فيعتبر إجرام الأنترنيت إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يصل إلى العنف.[1]

المطلب الثاني : ماهية التحقيق الجنائي في الجرائم الإلكترونية

يقصد بالتحقيق مجموعة الإجراءات التي تباشرها الجهة المكلفة بالتحقيق لدى وقوع الجريمة بغاية البحث و التنقيب عن الأدلة التي تفيد في الكشف عن الحقيقة

[1] بوشعرة أمينة، موساوي سهام، مرجع سابق، ص 20

باعتبارها جريمة ذات خصائص و طبيعة خاصة، هذا ما يجعل التحقيق الجنائي فيها مختلف عن التحقيق الجنائي في الجرائم العادية إذ يكون التحقيق في الجريمة المعلوماتية تحقيقا جنائيا معلوماتيا بإعتبار مسرح و محيط هذه الأخيرة هو الفضاء الإلكتروني و البيانات التقنية.[1]

الفرع الأول : تعريف التحقيق الجنائي المعلوماتي

يعرف التحقيق الجنائي بأنه العلم الذي يضم مجموعة من الإجراءات النظرية و العملية التي يقوم بها محققو هيئة التحقيق و الإدعاء العام بما يوصلهم لكشف الجريمة المعلوماتية و توفير الأدلة الرقمية ضد مرتكبيها و تقديمهم للعدالة لمحاكمتهم.[2]

يشكل التحقيق الجنائي المعلوماتي في البيئة المعلوماتية تحديا كبيرا للدول بالنظر إلى طبيعة هذا التحقيق و طبيعة هذه الجرائم المعلوماتية، ففي الولايات المتحدة الأمريكية تم إنشاء شرطة Web police كمركز لتلقي الشكاوى في جرائم الأنرتنيت، أما على المستوى الوطني، أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة، إذ يحتوي على مخبر خلية الإعلام بالإضافة إلى مخبرين جهويين بكل من وهران و قسنطينة، كما توجد على مستوى المركز فرق متخصصة في التحقيق في الجريمة المعلوماتية بالتنسيق مع المخابر السابق ذكرها، كما يوجد بالمعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي قسم الإعلام و الإكترونيك يختص في هذا النوع من الجرائم.[3]

---

[1] فلاح عبد القادر، آيت عبد المالك نادية، **التحقيق الجنائي في الجرائم الالكترونية و اثباتها في التشريع الجزائري**، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، جامعة الجيلاني بونعامة، خميس مليانة، مجلد 04، العدد 02، 2019، ص 1964

[2] خالد ممدوح ابراهيم،**فن التحقيق الجنائي في الجرائم الالكترونية**، دار الفكر الجامعي، الاسكندرية، 2010، ص 18

[3] عيدة بلعايد، مرجع سابق، ص 137

و يمكن تعريف التحقيق الجنائي بأنه "مجموعة من الإجراءات القانونية المتخذة للتنقيب و الكشف عن الجريمة المعلوماتية و مرتكبيها في الفضاء الرقمي بالإستعانة بالخبراء التقنيين في ميادين الإعلام الآلي لغاية الحصول على أدلة رقمية"، كما يمكن تعريفه بأنه مجموعة من الإجراءات التي تستهدف التنقيب و الكشف عن الأدلة في شأن الجريمة التي ارتكبت ثم مدى كفايتها لإحالة المتهم على المحاكمة، يقوم به المحقق و هو شخص عهد إليه القانون سلطة اتخاذ كافة الإجراءات القانونية و الوسائل المشروعة فيما يصل إلى عمله من جرائم بهدف الكشف عنها و ضبط فاعلها و تقديمه للمحاكمة.

و يتميز التحقيق في الجريمة الإلكترونية بمجموعة من الصفات و هي[1] :

- **السرية :** و هي عدم إطلاع الغير على مجريات التحقيق وفقا لما نصت عليه امادة 11 من قانون الإجراءات الجزائية.
- **التدوين :** تدون جميع إجراءات التحقيق في محاضر و يصادق عليها في محضر رسمي حتى تكون حجة في الإثبات.
- **وضع خطة التحقيق :** بحيث تبدأ مهمة المحقق بجمع الاستدلالات و في الجريمة الإلكترونية يساعد المحقق في أعمال التحقيق فريق مؤهل.[2]

الفرع الثاني : خصائص التحقيق و المحققين في الجريمة الإلكترونية

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات مرحلة هامة في سبيل البحث و التحري عن الجرائم، و تبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية لأنها تعد حجر الزاوية الذي سيتم عليه على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات و أدلة رقمية في المرحلة التي تعقب ارتكاب

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 19

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1695

الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها، و السبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم، ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوده القائمين على تعقبه و الممزوج بالإحباط و الإعجاب معا.[1]

أولا : خصائص التحقيق في الجريمة المعلوماتية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة و راسخة بدونها ما كان ليتمتع التحقيق تلك الصفة.

و هذه القواعد إما قانونية و إما فنية، فالأولى لها صفة الثبات التشريعي لا يملك التحقيق إزاءها شيئا سوى الخضوع و الامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته و فطنته و مهارته الكثير،[2] ذلك أن الفكر البشري المتعلق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق الجنائي، و بالتالي فإن أسلوب التحقيق و فكر المحقق الجنائي يجب أن يتغير و يتطور أيضا و ذلك كنتيجة طبيعية لمواجهة فكر المجرم المعلوماتي.

ثانيا : منهج أو أسلوب التحقيق الابتدائي في الجريمة الالكترونية

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق و التي تؤدي إلى اكتشاف الجريمة و معرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة، و تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي، و الهدف من التحقيق الابتدائي هو التأكد

[1] سعيداني نعيم، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجنائي**، مذكرة ماجيستير، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 109

[2] خالد ممدوح ابراهيم، مرجع سابق، ص 56

أولا من وقوع جريمة يعاقب عليها القانون، و من ثمة معرفة هذا النوع من الجرائم و من هو الجاني و من هو المجني عليه، و كذا معرفة وقوعها و ما هي الوسائل التي استعملت في ارتكابها، ز يكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيق يختلف عن غيره بالنسبة للجرائم الأخرى.[1]

1. وضع خطة عمل التحقيق

يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة الإلكترونية بوضع خطة العمل على ضوء المعلومات المتوافرة لديه، و تحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق و ذلك على النحو الآتي :

- وضع الخطة المناسبة و التي لا تبدأ إلا بعد معاينة مسرح الجريمة و التعرف على أنظمة الحماية تحديد مصادر الخطأ، التخطيط الفني للتحقيق و ذلك من أجل الوصول إلى أفضل الطرق و الأساليب للتعامل مع هذه الجرائم بالتفصيل و الوضوح، و أبضا عمل دراسة وافية و جادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها و ناقشها العاملون في فريق التحقيق، و تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم و عملهم و تقليل الآثار السلبية و الإسراع في إنجاز العمل و هو ما يؤدي إلى ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة و التي من شأنها التقليل من الأخطاء الفردية التي تنتج عن قلة الخبرة أو نقص المعرفة، و بالتالي تساعد على ايجاد درجة جيدة من التقييد بالمستوى المطلوب مع ضمان أن الخطوات التي

[1] سعيداني نعيم، مرجع سابق، ص 11

يقوم بها المحقق خلا جميع مراحل التحقيق تسير ضمن الضوابط التشريعية و تقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة.[1]

- و يجب أن ترتكز خطة العمل على مجموعة البنود الأساسية التي يتم الارتكاز عليها أثناء تنفيذ الخطة، و هي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم و تحديد النقاط التي يجب استضاحها معهم و تقدير مدى الحاجة إلى الاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الملابسات المحيطة بالوقائع ذلك ان من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل و منها [2]:
  - ✓ مدى أهمية الأجهزة و الشبكات المتضررة لعمل المنظمة.
  - ✓ مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها
  - ✓ مستوى الإختراق الأمني التي تسبب فيها الجاني.
- ثم بعد ذلك وضع الأسلوب الأمثل للتفتيش و ذلك من خلال وضع نوع الأدلة التي يريد فيق التحقيق البحث عنها.

2. تشكيل فريق التحقيق

إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده حتى و لو كانت المضبوطات هي مجرد حاسب شخص واحد، و لذلك فإنه يفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق و العثور على الأدلة.[3]

---

[1] سعيداني نعيم، مرجع سابق، ص 111

[2] خالد ممدوح، مرجع سابق، ص 57

[3] عبد الله حسين محمد، **اجراءات جمع الأدلة في الجريمة المعلوماتية**، مؤتمر الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، 2003، ص 612

و يجب أن يتشكل فريق التحقيق من فنيين و أخصائيين ذوي خبرة في مجال الحاسوب و الأنترنيت، و بمتازون بمهارات في التحقيق الجنائي بشكل عام و التحقيق الالكتروني بشكل خاص، لهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب و الأنترنيت ليتمكنوا من فك التعقيدات التي تفرضها ظروف و ملابسات كل جريمة.[1]

و إن أسلوب عمل كل فريق يستخدم في التحقيق كثير من أنواع الجرائم، إلا أنه يأخذ عملية خاصة في الجرائم المعلوماتية لما تتطلبه من مهارات فنية و خبرات متنوعة قد لا تتوافر لدى المحققين، و بذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا، و من الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من :

- المحقق الرئيسي و يكون ممن لهم خبرة في التحقيق الجنائي.
- خبراء الحاسوب و شبكات الأنترنيت الذين يعرفون ظروف الحادث و كيفية التعامل مع هذه الجرائم.
- خبراء الضبط و تحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء ضبط الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء الرسم و البصمات و الرسم التخطيطي.

و في هذا الإطار، نجد أن المشرع الجزائري قد أشار إلى إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المختصين في مجال الحاسوب و النظم المعلوماتية، و من الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة

[1] عبد الله حسين محمد، مرجع سابق، ص 613

لحماية المعطيات المعلوماتية و ذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها و تزويدها بالمعلومات الضرورية لذلك.[1]

ثالثا : العناصر الأساسية للتحقيق الابتدائي في مجال المعلوماتية

و نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة و المحددة التي تثبت وقوع الجريمة و تحدد شخصية مرتكبها، و هناك إجراءات و احتياطات يتعين على الضبطية القضية مراعاتها قبل البدء في عمليات التحقيق الابتدائي و إجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي.[2]

1. الاجراءات التي يجب مراعاتها قبل البدء في التحقيق

و يمكن أن نسرد الأهم منها كالآتي :

- تحديد نظام المعالجة الآلية للمعطيات، فهو كمبيوتر معزول أو متصل بشبكة الأنترنيت، مع وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها و دور كل منهم، فإذا وقعت الجريمة على الشبكة فإنه يجب حرص طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الإختراق من عدمه، و هل هناك حواسب آلية خارج هذه المشكلة و لها إمكانية الإتصال بهم أم لا؟

[1] **المادة 05 الفقرة الأخيرة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها** المؤرخ في 5 أوت 2009، الجريدة الرسمية، العدد 47

[2] مصطفى عبد الباقي، **التحقيق في الجريمة الإلكترونية و إثباتها**، كلية الحقوق و الإدارة العامة، جامعة بيزيت، رام الله، فلسطين، المجلد 45، العدد 4، 2018، ص 286

- مراعاة صعوبة إبقاء الدليل فترة طويلة في الجريمة المعلوماتية، و أيضا مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة التي ارتكبها، و كذلك فصل خطوط الهاتف حتى لا يتسنى للجاني استخدامها و التحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق.
- إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر و كذا الشفرات في حالة وجودها، و تصوير الأجهزة المستهدفة التي وقعت بها أو عليها الجريمة من الأمام و الخلف لإثبات أنها تعمل، و كذا للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.[1]

2. الإجراءات التي يجب مراعاتها أثناء التحقيق

عند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب، فإنه على رجال الضبطية القضائية و برفقتهم الخبراء الذين يستعينون بهم مراعاة ما يلي [2]:

- عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها و التأكد من دقة النسخ عن طريق الأمر (Disk comp) مع نزع غطاء الحاسب الآلي المستهدف و التأكد من عدم وجود أقراص صلبة إضافية، و أن يكون الهدف من نسخ محتوى الأسطوانة و الأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة و

[1] سعيداني نعيم، مرجع سابق، ص 113

[2] مرجع نفسه، ص 134

التي يمكن استعادتها من سلة المهملات، مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضعت على أزرار معينة مثل (Shift delete) وقت واحد لا يمكن استعادتها، و كذا من أجل معرفة الملفات المخفية المخزنة في ذاكرة الحاسوب، مع العمل على فحص البرامج و تطبيقاتها مثل البرامج الحسابية التي تطون قد استخدمت في جريمة اختلاس معلوماتي، و العمل على فحص العلاقة بين برامج التطبيقات و الملفات، خاصة تلك التي تتعلق بدخول المعلومات و خروجها و أيضا حفظ المعدات و الأجهزة التي تضبط بطريقة فنية و سليمة.

رابعا : خصائص المحققين المعلوماتيين

أمام التطور التكنولوجي الذي صاحب الجريمة المعلوماتية، فإن المتخصصين بالتحقيق بهذا النوع من الإجرام المستحدث يختلفون عن أولئك المختصين بضبط الجرائم التقليدية من حيث خصائص و طريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية و إنما يعتمد على البناء العلمي و التكنولوجي و هم يتولون مهمة البحث و التحري عن الجرائم المعلوماتية و كشف النقاب عنها، و إن كان قد سبق و أن طرحنا خصائص الجريمة المعلوماتية و كذا خصائص المجرم المعلوماتي فإنه في اعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفر عليها من يتصدى لمهمة البحث و التحري عن هذا النوع من الجرائم و المجرمين.[1]

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 56

خامسا : الخصائص الفنية للمحقق في الجريمة المعلوماتية

تلعب الأجهزة الأمنية دورا أساسيا في صيانة أمن المجتمع و ذلك إما القيام بدور وقائي يهدف إلى منع ارتكاب الجريمة و الحيلولة دون وقوعها و تقليل فرص اقترافها، و إما القيام بدور قضائي في ضبط الجرائم و مرتكبيها بعد حدوثها.

و لقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها رجال الضبطية القضائية و لم يتعودوا عليها ما يستلزم ضرورة توفير الإمكانات و المهارات المطلوبة في هذا المجال.[1]

و المشكلة الأساسية التي تواجه المحققين في جرائم تنظيم المعلومات هي خلفية المحقق نفسه، فمتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة و لكنهم ليسوا مدربين على تفهم دوافع الجريمة و جميع الأدلة لتقديم المتهم للمحاكمة، بينما المحققون ذو الخلفية القانونية قد تكون لهم الخبرة الواسعة في التحقيق و لكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم، إذ يلزم المحقق قبل مباشرة عملية التحقيق أن يكون على دراية بالعديد من الجوانب الفنية نذكر منها [2]:

- معرفة الجوانب الفنية و التقنية لأجهزة الحاسوب و الأنترنيت و التي تتعلق بالجريمة المرتكبة، ذلك لأن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف و تدمير الدليل على اعتبار أن

[1] مصطفى عبد الباقي، مرجع سابق، ص 287

[2] عيدة بلعابد، مرجع سابق، ص 138

جهله لأساليب ارتكاب الجريمة المعلوماتية يجعله في الكثير من الأحيان يقع في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها.[1]

- اتباع الإجراءات الصحيحة أو المشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة و تخزينها في الأقراص المعدة لذلك و منع حذفها و الحرص على عدم تعريض وسائط التخزين لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكرويف، كما يجب على المحق معرفة آلية عمل تشكيلات الحاسوب و الأنترنيت، كما يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات و ما يمكن أن تحتويه من معطيات، و معرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات، كما أن فهم المحقق لأساليب و تقنيات الأمن و المعلوماتية و الحاسوب لوظائفها و أسلوب عملها و طرق استخدامها عاملا مساعدا له عند قراءته للتقارير الجنائية التي يعدها خبير الحاسوب و التي تعتبر من أهم الوثائق التي يرجع إليها المحقق و يعتمد عليها في تحقيقه.

سادسا : تأهيل و تدريب المحقق المعلوماتي

في مكافحة الجرائم المعلوماتية بصفة عامة لابد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، و يمتد هذا التدريب و التأهيل إلى العاملين بأجهزة الضبطية القضائية.[2]

[1] سعيداني نعيم، مرجع سابق، ص 115

[2] محمد الأمين البشرى، مرجع سابق، ص 22

و قد تنبهت الدول إلى هذا الأمر و ظهر الاهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة و معاملة المجرمين، و منها ما جاء في القاعدة 1/22 من قواعد بيكين التي أكدت على الحاجة إلى التخصص المهني و التدريب.[1]

و لهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة و تنفذ بطرق ذكية، و ليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب و النظم المعلوماتية، و لكن لابد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسوب الآلي و حسن استغلالهم في كشف الجرائم و جمع الادلة، كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة و التدابير اللازمة لتأمين الادلة و المعلومات الممغنطة بصورة علمية و سليمة.

و يرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعاة عناصر أساسية تتمثل في شخص المتدرب و منهج الدورة التدريبية، و صفة و أسلوب التدريب.

و يجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة أو الأساليب التي تتعلق بالكشف عنها و كيفية إثباتها و معاينتها و التحفظ عليها و كيفية فحصها فحصا فنيا.

و قد كان هناك من يرى أن صعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن بعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال، لكن الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد و المجتمع و يضعها تحت رحمة هذه الشركات التي يكون همها تحقيق الربح المادي على حساب إظهار الحقيقة، فضلا عن

[1] ختاد ممدوح ابراهيم، مرجع سابق، ص 64

الإخلال بمبدأ سرية التحقيق لو تعلق التحقيق بجرائم عرض الأشخاص و أسرارهم الشخصية أو تعلق الأمر بأن الدولة.[1]

المبحث الثاني : الأجهزة المكلفة بالبحث و التحري عن الجرائم الإلكترونية

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية أو من أعضاء النيابة العامة أو قضاة التحقيق و يلحق بالتحقيق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطة القضائية الذي يخول لهم القانون مهمة جمع الاستدلالات عن المشتبه بهم.

سنحاول من خلال هذا المبحث أن نستعرض أبرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية حيث سنتناول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال في المطلب الأول، إضافة إلى الوحدات التابعة للأمن الوطني و التابعة لقيادة الدرك الأوطني في المطلب الثاني.[2]

المطلب الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

نص المشرع الجزائري في المادة 13 من القانون 09-04 على ضرورة إنشاء هيئة ذات وظيفة تنسيقية تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم و

[1] محمد الأمين البشرى، مرجع سابق، ص 25

[2] بوضياف اسمهان، **الجريمة الالكترونية و الاجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018، ص 366

تتولى تنشيط و تنسيق عملية الوقاية من الجرائم الإلكترونية و كذلك مصاحبة السلطات القضائية في التحريات التي يجريها بشأن هذه الجرائم.[1]

الفرع الأول : التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

تعرف حسب أحكام المواد من 01 إلى 04 من القانون 09-04 بأنها "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع لدى الوزير المكلف بالعدل و يقع مقرها بالجزائر العاصمة"، و أنشأت الهيئة الوطنية بالجزائر بموجب المادة 13 من القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاتصال و الإعلام و مكافحتها[2]، و تحديدا في نص المادة 13، لكنه ترك أمر تشكيل الهيئة و تنظيمها و كيفية سيرها للتنظيم الصادر بموجب المرسوم الرئاسي 261/15[3]

تعد الهيئة سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف و مراقبة لجنة يترأسها وزير العدل و تضم أساسا أعضاء من الحكومة معنيين بالموضوع، و مسؤولي مصالح الأمن، و قاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء و تضم الهيئة قضاة و ضباط و أعوان من الشرطة القضائية التابعين لمضالح الاستعلام

[1] **القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها** المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009، الجريدة الرسمية، العدد 47 صادر في 16 أوت 2009، ص 8

[2] مولاي ابراهيم عبد الحكيم، **الجرائم الالكترونية**، مجلة الحقوق و العلوم الانسانية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 23، المجلد الثاني، 2015، ص 220

[3] **المرسوم الرئاسي رقم 261/15 مؤرخ في 8 أكتوبر 2015 يحدد تشكيلة و تنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها**، الجريدة الرسمية، عدد 53 بتاريخ 8 أكتوبر 2015

العسكرية و الدرك و الأمن الوطنيين، وفقا لقانون الإجراءات الجزائية تكلف بتجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية، و ضمان المراقبة و الوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات و الجرائم الأخرى تحت سلطة القاضي المختص.[1]

الفرع الثاني : مهام و اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

أولا : مهامها

تنص المادة 14 من نفس القانون على أنه تتولى الهيئة المذكورة في المادة 13 خصوصا مجموعة من المهام نذكر منها :

1. الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

تكون اجراءات الوقاية بتوعية مستعملي تكنولوجيات الإعلام و الاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها و هم يتصفحون أو يستعملون هذه التكنولوجيات و من أهم هذه الجرائم التجسس على الاتصالات و الرسائل الالكترونية، التلاعب بحسابات العملاء[2] ... الخ

2. مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

بحسب المادة 14 من القانون 09-04 فهناك نوعان من المكافحة تقوم بها هذه الهيئة :

[1] عديلة مراد، عبدلي مروان، مرجع سابق، ص 78

[2] القانون 09-04 السالف الذكر

- مساعدة السلطة القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، تقديم المساعدة لمصالح الأمن و الدرك الوطنيين و لجميع إدارات و مصالح الدولة المركزية (المديريات العامة المحتلفة).

3. تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و تحديد مكان تواجدهم

تقوم الهيئة على المستوى الوطني بتنشيط و تنسيق الأعمال التحضيرية الضرورية و من ثم تشاركها مع المنظمات (الهيئات) المماثلة على مستوى الدول بدون المساس بتطبيق الاتفاقيات الدولية و مبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات و المصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية و كذلك التعرف على الفاعلين و أماكن تواجدهم.[1]

ثانيا : اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

بينة الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261 المهام التي تكلف بها الهيئة على سبيل الحصر و الهدف منها هو الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و أبرز مهامها :

[1] بوضياف اسمهان، مرجع سابق، ص 369

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،[1]
- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،
- مساعدة السلطة القضائية و مصالح الشرطة القضائية في مجال مكافحة المعلوماتية من خلال التزويد بمعلومات و الخبرات القضائية و ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية التي تمس بأمن الدولة و ذلك تحت سلطة القاضي المختص و باستثناء أي هيئات وطنية أخرى،
- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

المطلب الثاني : الوحدات التابعة لسلك الأمن و الدرك الوطني

توجد لدى مديرية الأمن الوطني و الدرك الوطني لتنفيذ مهامها في مجال الحفاظ على الأمن و النظام العام مجموعة من الوحدات التي سنذكرها في هذا المطلب.

الفرع الأول : الوحدات التابعة لسلك الأمن الوطني

أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة و مخبريين جهويين بكل من قسنطينة و وهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي و فرق متخصصة مهمتها التحقيق و الكشف على جرائم

[1] المرسوم الرئاسي رقم 15-261 السالف الذكر

الأنترنيت، بالإضافة لانشائها ثلاث مخابر على مستوى بشار، ورقلة، و تمنراست، قيد الانجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن.[1]

كما ينظم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة و وهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية و الآثار التكنولوجية"، و التي تضم ثلاث أقسام، و هي :

- قسم استغلال الرقمية الناتجة عن الحواسيب و الشبكات.[2]
- قسم استغلال الأدلة الناتجة عن الهةاتف النقالة.
- قسم تحليل الأصوات، و ذلك بالإستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية.

الفرع الثاني : الوحدات التابعة لسلك الدرك الوطني

تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية و علم الإجرام الكائن مقره ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام و الألكترونيك الذي يختص بالتحقيق و الكشف عن الجرائم الإلكترونية، و أيضا بواسطة مديرية الأمن العمومي و الاستغلال و المصلحة المركزية للتحريات الجنائية و هي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الالكترونية و ذلك بتحليل الدعامات الالكترونية، و انجاز المقاربات الهاتفية و تحسين التسجيلات الصوتية و الفيديو و الصورة و ذلك لتسهيل استغلالها، بالإضافة إلى مراكز الرقابة على جرائم

[1] سعيد علي نعيم، آليات البحث و التحري من الجرائم المعلوماتية في القانون الجزائر، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، قسم الحقوق، 2012-2013، ص 107

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1696

الإعلام الآلي و الجرائم المعلوماتية و مكافحتها ببئر مراد رايس التابع لمديرية الأمن العمومية للدرك الوطني و هو قيد الإنشاء.[1]

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن و النظام العام و محاربة الجريمة بكافة أنواعها وحدات متنوعة و عديدة على مستوى القيادة العامة أو على مستوى القيادات الجهوية و المحلية نذكر منها :

- المصالح و المراكز العلمية و التقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.[2]

[1] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1696

[2] سعيد علي نعيم، مرجع سابق، ص 107

الفصل الثانـــــي

آليات التحقيق في الجرائـــم الإلكترونيـــــة

تمهيد

إن طبيعة الجرائم الالكترونية بعناصرها و وسائل ارتكابها قد تدفع المشرع الجزائي إلى إعادة النظر في الكثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الإثبات، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من طبيعة الكترونية، و هو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء و مدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف و الأخطاء، و كذا مصداقيته و مشروعيته.

و قد تم تقسيم هذا الفصل إلى مبحثين، المبحث الأول تحت عنوان "اجراءات التحقيق في الحصول على الدليل الالكتروني"، أما المبحث الثاني فيتمثل في "القواعد الاجرائية في الحصول على الدليل الالكتروني".

المبحث الأول : اجراءات التحقيق في الحصول على الدليل الرقمي

إن التطور التقني الذي لحق نظام المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير الكثير من المفاهيم السائدة حول إجراءات و طرق الحصول عليها، و هو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية فضلا عن استحداث قواعد إجرائية أخرى تتلائم مع طبيعة البيئة التقنية، فتطور الإثبات و وسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، و هو الأمر الذي سوف نعالجه من حيث بحث القواعد الإجرائية التقليدية و إلى أي مدى يمكن الاستناد عليها في الحصول على الدليل الرقمي

في المطلب الأول، ثم نعرض القواعد الإجرائية الحديثة في استخلاص الدليل الإلكتروني في المطلب الثاني.

المطلب الأول : القواعد الإجرائية التقليدية في الحصول على الدليل الإلكتروني

مما لاشك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها التفتيش و ضبط الأشياء و الخبرة و المعاينة سنتطرق لها في هذا المطلب

الفرع الأول : التفتيش و ضبط الأدلة

أولا : التفتيش

لم يورد المشرع الجزائري تعريفا خاصا و دقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق و أحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة من جهة، و خطورته فيما يترتب عنه من مساس لحرية الأشخاص و بكرامتهم من جهة أخرى،[1] و خير دليل على ذك اهتمام الدستور الجزائري بأهمية هذا الإجراء من خلال نص المادة 40 منه و التي تنص على ما يلي "فلا تفتيش إلا بمقتضى القانون و في إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

كما نصت المادة 1/5 من القانون 09-04 المتضمن لقواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها "يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 212

إلى : منظومة معلوماتية أو جزء منها و كذا المعطيات المخزنة فيها و منظومة تخزين المعلوماتية".[1]

و يمكن تعريف التفتيش بأنه ذلك الإجراء الذي يدخل ضمن اجراءات التحقيق الابتدائي أو القضائي ولا يمكن أن يقوم به سوى النيابة و قاضي التحقيق.[2]

أ. القواعد الموضوعية لتفتيش الحاسوب

و تلخص هذه القواعد كالآتي :

- وقوع جريمة إلكترونية
- توافر أدلة إلكترونية قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الجريمة.
- أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية و المعنوية و شبكات الاتصال الخاصة به.

ب. القواعد الشكلية لتفتيش نظام الحاسوب

تتضمن عدة قواعد نذكر منها مايلي :

- أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش.
- أن يكون التفتيش مسبقا.
- تكوين فريق تفتيش يتضمن خبراء و فنيين و متخصصين بالحاسوب و الأنظمة الإلكترونية.[3]

[1] القانون 09-04 السالف ذكره، ص 6

[2] مصطفى عبد الباقي، **التحقيق في الجريمة الالكترونية و اثباتها**، كلية الحقوق و الإدارة العامة، جامعة بيرزيت، رام الله، فلسطين، المجلد 4، العدد 4، 2018، ص 289

[3] عيدة بلعابد، مرجع سابق، ص 143

ثانيا : الضبط

يتمثل الضبط في العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها و التحفظ عليها، و يعتبر الضبط هو الهدف من التفتيش و النتيجة المباشرة و المستهدفة و لذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق بشأن التفتيش و يؤدي بطلان التفتيش إلى بطلان الضبط.

يختلف الضبط في الجريمة المعلوماتية عن ضبط الجرائم الأخرى من حيث المحل لأن اجريمة الالكترونية يرد فيها الضبط على الأشياء ذات طبيعة معنوية من حيث البيانات و المراسلات و الاتصالات الالكترونية و على الأشياء ذات الطبيعة المادية كالكمبيوتر و ملحقاته و الأقراص الصلبة الخارجية و المرنة.[1]

الفرع الثاني : المعاينـــــة

المعاينة من أهم مراحل التحقيق في الجرائم المستحدثة نظرا لما يمكن أن توفره من أدلة اثبات للجريمة و تزداد أهميتها في اثبات الجرائم الالكترونية عبر الأنترنيت في أنها تقوم على معاينة جملة من البرمجيات أو الأقراص و كل ما يتعلق بجهاز الحاسب الآلي و ذلك راجع إلى الطبيعة الخاصة للمعاينة في هذا المجال، و بالتالي جوهر المعاينة هو الملاحظة و فحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة لإثبات حالته و التحفظ على كل ما يفيد من الأشياء في كشف الحقيقة، و يجوز اللجوء إلى المعاينة في كافة الجرائم.[2]

إلا أن أن أغلبية التشريعات بما فيها التشريع الجزائري يقتصر عن الجنايات و الجنح الهامة بحيث تعد إجراء وجوبيا في الجنايات و جوازيا في الجنح، و هي قد تتم في

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 221

[2] عيدة بلعابد، مرجع سابق، ص 140

مكان عام أو خاص، فإذا كانت في مكان عام، مأمور الضبط القضائي لا يحتاج إلى إذن أو ندب سلطة تحقيق بإجرائها، أما إذا كانت بمكان خاص، لابد لصحتها إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

لتحقيق المعاينة لابد من مراعاة خطوات و إرشادات محددة منها :

- تصوير الكمبيوتر و ما يتصل به من أجهزة و ملحقات مع تشغيل وقت التقاط الصور.
- عدم إجراء أي نقل للمعلومات من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محز و اتلاف البيانات المسجلة.[1]
- التحفظ على سلة المهملات من أورق ممزقة و أوراق مستعملة و الشرائط و الأقراص الممغنطة و الغير سليمة لفحصها و رفع البصمات.
- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة.
- جعل المعاينة الإلكترونية سرية و مقتصرة على فئة الباحثين و المحققين ذو الكفاءة العالية و الخبرة الفنية.

الفرع الثالث : الخبرة

تعتبر الاستعانة بالخبراء من بين الإجرءات التي يلجأ إليها القضاء و سلطات التحقيق على حد سواء و ذلك ما استعصى عليهم الأمر و من بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الالكترونية حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية و خبرة في مجال الالكترونيات.

[1] عيدة بلعابد، مرجع سابق، ص 141

أولا : أنواع الخبراء الالكترونيين

الخبير في الجريمة الالكترونية هو الفني المتخصص و صاحب خبرة في التقنية الالكترونية و شبكاتها، و يطون قد رأى أو سمع أو أدرك بحواسه معلومات هامة لازمة للدخول في نظام المعالجة الآلية الرقمية للبيانات إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الإلكتروني داخله، و يعتبر خبراء الكترونييون كل من :

- المبرمجون
- المحللون و هم الأشخاص الذين يضعون خطوات العمل و يقومون بتجميع بيانات نظام معينة.
- مهندسو الصيانة و الاتصالات
- مشغلو الحاسوب الآلي
- مدير النظام المعلوماتي.[1]

ثانيا : أهمية الخبرة في البحث عن الدليل الإلكتروني

تكون أهمية الخبرة في الأدلة التي تقدمها لجهة التحقيق و القضاء و لسائر السلطات المختصة بالدعوى الجزائية لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد 143 إلى 156 من قانون الإجراءات الجزائية و اعتبرها من اجراءات البحث عن الدليل حيث نصت المادة 143 على أنه "لجهات التحقيق أو الحكم عندما تتعرض لها مسألة ذات طابع فني أن تأمر بندي خبير إما من تلقاء نفسها أو بناء على طلب النيابة العامة و إما بطلب من الخصوم".[2]

[1] صغير يوسف، مرجع سابق، ص 89

[2] **القانون رقم 66-155 مؤرخ في 8 يونيو 1966 المعدل و المتمم لقانون الإجراءات الجزائية، الجريدةالرسمية، العدد 48 المعدل و المتمم للأمر 15-02** المؤرخ في 23 جويلية 2015، العدد 40

كما أشار المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها أنه "يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنطومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لانجاز مهمتها".[1]

المطلب الثاني : القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني

كان لتطور أساليب ارتكاب الجريمة الالكترونية منحنى تصاعدي بين الجرائم المرتكبة في الجزائر، و هو ما فرض على المشرع الاعتماد على قواعد اجرائية خاصة في سبيل مكافحة الجريمة الالكترونية و هو ما جاء به القانون 06-22 المؤرخ في ديسمبر 2006 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 08 يوليو 1966 و المتضمن لقانون الإجراءات الجزائية.

الفرع الأول : التسرب الإلكتروني

لقد تطرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية بعد تعديله بقانون 22/06 و التي تنص على "يقصد بالتسرب قيام ضابط أو عون شرطة قضائية، تحت مسؤولية ضابط الشرطة القضائية المكلفة بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض بهوية مستعارة و أن يرتكب عند الضرورة الأفعال المذكورة في المادة 69 مكرر

[1] القانون 09-04 السالف الذكر

14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم".[1]

فالتسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه في أنهم ارتكبوا الجريمة بإظهار أنه ساهم معهم أو شريك، و يستعمل الضابط أو العون هوية مستعارة إذا ما ارتبط بأحد هذه الجرائم :

- جرائم المخدرات
- الجريمة المنظمة العابرة للحدود
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات
- جرائم تبييض الأموال
- الجرائم الموصوفة بأفعال إرهابية
- الجرائم المتعلقة بالتشريع الخاص بالصرف و جرائم الفساد.[2]

الفرع الثاني : إعتراض المراسلات و المراقبة الالكترونية

أولا : مفهوم اعتراض المراسلات

استحدث بموجب المادة 65 مكرر إلى 65 مكرر 10 من قانون الإجراءات الجزائية إمكانية قاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي و تحت إشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية و وضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القبام بإلتقاط و تثبيت و تسجيل و بحث في سرية و في أي مكان عام عن طريق وسائل

[1] **المادة 65 مكرر 5 من قانون الإجراءات الجزائية أمر رقم 66-156 مؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية**، الجريدة الرسمية، عدد 84 معدل و متمم وفقا للقانون 22/06 المؤرخ في 20 جويلية 2006

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1698

الاتصال السلكية و اللاسلطية و وضع ترتيبات تقنية دون مراقبة المعنيين من أجل التقاط الصور و تثبيت و بحث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة.[1]

و هذا ما جاء به القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها في المادة 2 من الفقرة "و" في تعريفه للاتصلات الالكترونية على انها تراسل أو ارسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بأي وسيلة كانت.

و تجدر الإشارة في هذا الصدد إلى أن المراسلات التي يمكن اعتراضها يجب أن تتم بالخصوصية و لكي تكون كذلك يلزم أن يتوافر فيها عنصران أساسيان هما :

- عنصر موضوعي يتعلق بموضوع و مضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخص و سري.
- عنصر شخصي و المراد به إرادة المرسل في تحديد المرسل إليه و رغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة.

و عند توفر هذان العنصران في الرسالة، فإنها تتصف بالمراسلة الخاصة التي لها خصوصيتها و سريتها المحمية قانونا ولا أهمية لشكل الرسالة أو طريق نقلها و توصيلها للمرسل إليه، ولا يجوز لضباط الشرطة القضائية اللجوء إلى اعتراض المراسلات إلا بعد أن الحصول على إذن مكتوب و مسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

[1] المادة 65 مكرر، قانون سالف الذكر من قانون الإجراءات الجزائية

ثانيا : المراقبة الإلكترونية

تعد الرقابة على الاتصالات الالكترونية أو كما يطلق عليها بمصطلح "المراقبة الالكترونية للاتصالات" من أهم مصادر التحري التي يستعان بها في التقصي على مختلف الجرائم بما في ذلك الجرائم المتصلة بالتكنولوجيات الحديثة، خاصة في ظل لجوء الجناة إلى وسائل التقنية الحديثة للتصال في تنفيذ مخططاتهم الاجرامية و التواصل فيما بينهم، كما تعد مراقبة الاتصالات الالكترونية مصدرا للأدلة الرقمية.[1]

أ. مفهوم مراقبة الاتصالات الإلكترونية

نجد أن المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الالكترونية لكن بعض التشريع قد قامت بتعريفها مثل التشريع الأمريكي الذي عرفها على أساس أنها "عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز الكتروني أو أي جهاز آخر".[2]

إلا أنه يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر خلسة و تنتهك فيه سرية الأحاديث الخاصة، تأمر السلطة القضائية في الشكل المحدد قانون يهدف الحصول على دليل غير مادي للجريمة المعلوماتية و يتضمن من ناحية استراق السمع في الأحاديث و من ناحية أخرى حفظه بواسطة أجهزة متخصصة في ذلك.[3]

بينما في القانون 09-04 في المادة 3 منه قد حدد كيفية مراقبة الاتصالات على النحو الآتي "مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات و التحريات أو

[1] عبيدة بلعابد، مرجع سابق، ص 145

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1699

[3] بوشعرة أمينة، موساوي سهام، **الإطار القانوني للجريمة الالكترونية**، مذكرة ماستر، جامعة عبد الرحمن ميرة، بجاية، كلية الحقوق و العلوم السياسية، قسم القانون الخاص، 2017-2018، ص 82

التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية".[1]

و بالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء و في الحالات المحددة حصريا في المادة 04 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال.

المبحث الثاني : القيمة القانونية للدليل الإلكتروني

لقد أثارت مسألة الدليل الرقمي الكثير من التساؤلات حول تعبيره أو عدم تعبيره عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليه من التزييف و التحريف و العبث، و هو ما يثير مسألة مشروعية الأخذ به إذ يشترط في الدليل الجنائي بشكل عام أن يكون مشروعا من خيث وجوده و من حيث الحصول عليه.

إن مجرد وجود دليل يثبت وقوع الجريمة و نسبيتها إلى شخص معين لا يكفي أن يكون دليل إثبات، إذ يجب أن تكون لهذه الأدلة قيمة قانونية و قيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين، الأولى مشروعية الدليل و الثانية هي حجية الدليل المراد إثباته.

المطلب الأول : مشروعية الدليل الإلكتروني

تعرف المشروعية بأنها التوافق و التقيد بأحكام القانون في إطاره و مضمونها العام، فهي تهدف إلى تقرير ضمانة أساسية و جدية للأفراد لحماية حقوقهم و حريتهم

[1] المادة 04 من القانون 09-04 السالف الذكر، ص 6

الشخصية ضد تعسف السلطة و من التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي و بنفس القدر تحقيق حماية مماثلة للفرد ذاته.[1]

لذلك فإنه لصحة الإجراءات التي تقوم بها جهة التحقيق أن لا تخل بمبدأ المشروعية من أجل الحصول على دليل صحيح و سليم يستند عليه القضاء في أحكامه، و الحقيقة أن مشروعية الدليل الإلكتروني هي مشروعية الوجود و مشروعية الحصول.[2]

الفرع الأول : ماهية الدليل الإلكتروني

أولا : تعريف الدليل الالكتروني

تعددت التعريفات الاصطلاحية للدليل الرقمي و ان كانت في مجملها تجتمع في نقطة محددة تتعلق بالبيئة الإلكترونية لهذا الدليل الحديث،[3] فالدليل الرقمي هو الدليل المأخوذ من أجهزة الكمبيوتر في شكل موجات و نبضات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها بواسطة برامج تطبيقات و تكنولوجيات خاصة، و هي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الرسوم من أجل اعتماده أمام أجهزة تطبيق القانون.[4]

كما يعرف بأنه الدليل الذي يجد له أساسا في العالم الافتراضي و يقود إلى الجريمة أو تلك المعلومات التي يقبلها المنطق و العقل و يعتمدها العلم و يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أحهزة الحاسب

[1] عبد الله بن حسين آل حجراف القحطاني، **تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية**، رسالة ماجيستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014، ص 55

[2] سعيداني نعيم، مرجع سابق، ص 207

[3] عبد الله بن حسين آل حجراف القحطاني، مرجع نفسه، ص 56

[4] محمد الأمين البشرى،**التحقيق في الجرائم المستحدثة**، جامعة نايف العربية للعلوم الأمنية، الرياض،2004،ص 3

الآلي و ملحقاتها و شبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بالجريمة أو المجني عليه.[1]

كما يمكن تعريف الدليل الرقمي بأنه ذلك الدليل الذي يتضمن بيانات إلكترونية مخزنة بالحاسب الآلي و لها وجود في الوسط الإفتراضي و التي من خلالها يتم الكشف عن الجريمة أو إثبات العلاقة بين حدوث الجريمة و فاعلها.

ثانيا : خصائص الدليل الإلكتروني

يتميز الدليل الرقمي بمجموعة من الخصائص تميزه عن باقي الأدلة الجنائية، تتمثل هذه الأخيرة فيما يلي [2]:

1. **الدليل الرقمي دليل علمي و تقني**

يتكون الدليل الرقمي في أساسه من مجموعة من البيانات و المعلومات ذات صبغة الكترونية غير ملموسة يتم إدراكها بواسطة أجهزة و معدات و أدوات محاسبات الآلية و الاستعانة بنظم برامجية حاسبية، و هذا ما يجعل الدليل الرقمي من الأدلة العلمية و التقنية الحديثة نظرا لبنيته التقنية في المجال الافتراضي كما أنه دليل يعتمد على التقنيات بالدرجة الأولى.[3]

2. **الدليل الرقمي ذو طبيعة متطورة**

فهو يمتاز بتطور تلقائي تبعا تطور البيئة الرقمية التي تعتمد أساسا على التجدد، و يرجع هذا إلى تطور الثورة التكنولوجية خاصة في مجال الاتصالات و أجهزة التواصل.[4]

[1] عبيدة بلعابد، مرجع سابق، ص 153

[2] سعيداني نعيم، مرجع سابق، ص 208

[3] عبيدة بلعابد، مرجع نفسه، ص 154

[4] مرجع نفسه، ص 155

3. صعوبة اتلاف الدليل الرقمي

قد يتعرض الدليل الرقمي إلى عملية اتلاف سواء بصفة كلية أو جزئية و هذا من خلال عملية المسح، غير أنه و بالرغم من هذا فإن اتلافه لا يمنع من غعادة استرجاع محتوى الدليل الرقمي من ذاكرة الحاسب الآلي أو بالاستعانة بنسخ منه.[1]

ثالثا : تقسيمات الدليل الإلكتروني

لم يتطرق أغلب فقهاء القانون الجنائي إلى دراسة شاملة و دقيقة للأدلة الجنائية الرقمية نظرا لحداثة هذا النوع من الأدلة و بيئته التي تمتاز بالتطور المستمر، و بالرغم من ذلك، نشير إلى محاولة فقهية قسمت الدليل الرقمي إلى أربعة تقسيمات هي [2]:

- الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي و شبكاتها، تعتبر هذه الأخيرة مستخرجات برامج الحاسب الآلي.
- الأدلة الرقمية الخاصة بالأنترنيت.
- الأدلة الرقمية الخاصة ببروتوكولات نبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

الفرع الثاني : مشروعية الدليل الإلكتروني في الوجود

تقتضي مشروعية وجود الدليل الالكتروني أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الاثبات الجنائي، و يقصد بمشروعية الوجود أن يكون الدليل معترفا به، بمعنى أن يكون القانون مجيز للقاضي الاستناد عليه و الاستدلال به لتكوين عقيدته و قناعته للحكم بالإدانة أو البراءة، و لعل المعيار الذي يتحدد على أساسه موقف القوانين

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

[2] مصطفى عبد الباقي، مرجع سابق، ص 292

فيها يتعلق بسلطة القاضي الجزائري في قبول الدليل الالكتروني، تتمثل في نظام الاثبات السائد في الدولة إذ يختلف النظام القانوني في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات و هناك ثلاث فئات سنتناولها في هذا الفرع.

أولا : نظام الإثبات المقيد

و فيه يقوم المشرع بتحديد سلفا و بشكل حصري الأدلة التي يجوز للقاضي قبولها و الاستعانة بها في الإثبات، و كذا تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها، في حين لا يكون للقاضي الجزائي في هذا النظام[1] أي دور في تقدير الأدلة أو البحث عنها، و إنما يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته و توفره على الشروط التي حددها القانون و في حالة انتقاء الشروط التي يتطلبها القانون في الدليل فإن القاضي لا يسمح له الحكم بإدانة حتى ولو تكونت لديه قناعة يقينية بارتكاب المتهم للجريمة المنسوبة إليه.[2]

و من هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين، الأول يتمثل في الدور الايجابي للمشرع في عملية الإثبات لكونه الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة او باستبعاد أدلة أخرى، أو باخضاع كل دليل شروط معينة، و لكونه يحدد القيمة الاقناعية لكل دليل بأن يضفي الحجية الدامغة على بعض الأدلة، و الحجية النسبية على بعضها الآخر، أما المبدأ الثاني فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات اذ يلتزم التزاما صارما بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقد سلطته في الحكم بما يتفق مع

[1] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1701

[2] مرجع نفسه، ص 1702

الوقائع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالعبد في طاعته لنصوص القانون.[1]

ثانيا : نظام الإثبات الحر

و هو نظام يسود فيه مبدأ حرية الإثبات، إذ لا يحدد فيه المشرع طرقا معينة لإثباتها ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجزائي الذي يكون له دور ايجابي في البحث عن الأدلة المناسبة و تقدير قيمتها الثبوتية حسب اقتناعه بها، فلا يلزمه القانون بالاستناد على أدلة معينة لتكوين قناعته فله أن يبني هذه القناعة على أي دليل يقدم في الدعوى و إن لم يكن منصوصا عليه، بل أن المشرع في مثل هذا النظام لا يختص بالنص على أدلة الإثبات، فكل الأدلة تساوي قيمتها في نظر المشرع، و القاضي هو الذي يختار من بين ما يطرح عليه من أدلة ما يراه مفيدا للوصول إلى الحقيقة، و هو في ذلك يتمتع بمطلق الحرية في قبول الدليل أو طرحه جانبا إذا لم يطمئن إليه، دون أن يكون مطالبا بتبيين اقتناعه.[2]

و يجد هذا النظام مبرراته في كون الإثبات في المسائل الجزائية لا ينصب على وقائع مادية أو نفسية خاصة بالجريمة ولا ينصب على تصرفات قانونية يتفق معها قيام المشرع سلفا بتحديد وسائل اثباتها و مدى الحجية التي تتمتع بها كل منها، كما أن الإثبات ينصرف إلى وقائع إجرامية غالبا ما يعمد الجناة بقدر المستطاع إلى إزالة و محو آثارها، الأمر الذي يحتم تحويل القضاء كافة الوسائل المتاحة و الممكنة لكشف الجريمة و تقصي الحقيقة.[3]

---

[1] نداء نائل فايز المصري، **خصوصية الجرائم المعلوماتية**، جامعة النجاح الوطنية، كلية الدراسات العليا، رسالة ماجيستير، فلسطين، 2017، ص 95

[2] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1703

[3] براهيمي جمال، **آليات التحقيق في الجريمة الإلكترونية**، جامعة مولود معمري، تيزي وزو، 2018، ص 139

و على عكس نظام الإثبات المقيد، فإن فلسفة هذا النظام ترتكز على مبدأين مختلفان هما :

الأول : يتمثل في الدور السلبي للمشرع في عملية الإثبات و من خلاله يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا و هو ما يفتح المجال لأن تكون جميع الأدلة مقبولة وفقا لتقدير القاضي و ليس المشرع.

أما الميدأ الثاني : فهو الدور الايجابي للقاضي الجزائي في الإثبات، و يبدو ذلك من ناحيتين : الأولى من خلال الحرية المطلقة التي يتمتع بها القاضي الجزائي في اثبات حقيقة الجريمة بكافة طرق الإثبات و سلطته الواسعة في اتخاذ جميع التدابير، و من ناحية أخرى فنظام الإثبات الحر يمنح للقاضي الجزائي سلطة تقديرية كبيرة في قبول الأدلة، و موازنتها و تقدير قيمتها التدليلية معتمدا على ثقافته و خبرته القانونية.

ثالثا : نظام الإثبات المختلط

و هو نظام وسط بين نظام الإثبات المقيد و نظام الإثبات الحر، و فيه تم التصدي للإنتقادات الموجهة لنظام الإثبات الحر حول خشية تعسف القاضي الجزائي و خروجه عن جادة الصواب، و ذلك بأن حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه.[1]

و اعتبارا لما سبق، نستنتج بأن مسألة مشروعية الدليل الالكتروني في الوجود تثور بالدرجة الأولى في الأنظمة القانونية التي تتبنى نظام الاثبات المقيد إذ لا يمكن في ظلها الاعتراف للدليل الالكتروني بآية قيمة اثباتية ما لم ينص عليه القانون صراحة ضمن

[1] براهيمي جمال، مرجع سابق، ص 142

قائمة أدلة الإثبات المقبولة و من ثم لا يجوز للقاضي الجزائي أن يستند إليه لتكوين قناعته مهما توافرت فيه شروط اليقين.[1]

و في هذا الصدد نجد المشرع الجزائري و كغيره من التشريعات المنتمية إلى نظام الإثبات الحر لم يفرد نصوصا خاصة تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل بما في ذلك الدليل الالكتروني.

الفرع الثالث : مشروعية الدليل الإلكتروني في التحصيل

من الضروري أن يتم رسم ضوابط و أطر معينة، يتعين أن تمارس في نطاقها عملية البحث عن الأدلة و تحصيلها و التحقيق فيها بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائه و هو الوصول إلى الحقيقة الفعلية في الدعوى و هو الهدف الأسمى لقانون الإجراءات الجزائية و يعني مبدأ مشروعية الحصول على الدليل الإلكتروني بما يتضمنه من مفاهيم الكترونية، ضرورة اتفاق الإجراءات مع القواعد القانونية و الأنظمة المتبعة[2] في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا يقتصر فقط على مجرد المطابقة مع القواعد القانونية، بل يجب أن تراعي المبادئ السامية لحقوق الإنسان و قواعد النظام و حسب الآداب في المجتمع.[3]

و يشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، و ذلك يقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن و نحن نبحث عن مشروعية الدليل الإلكتروني، فإننا نقتصر على ما يثير جمع الدليل الإلكتروني من حيث مشروعية

[1] براهيمي جمال، مرجع سابق، ص 143

[2] خالد عياد الحلبي، **إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنيت**، دار الثقافة للنشر و التوزيع، عمان، ص 235

[3] مرجع نفسه، ص 239

الحصول عليه يتركز بشكل أساسي في إجراءات التفتيش للبحث عن هذا الدليل و ذلك يتم بنقطتين رئيسيتين :

- صفة القائم بالتفتيش
- مدى مشروعية التفتيش عن الدليل الإلكتروني و في ضبطه في الوسط الافتراضي.

من المقرر أن الإدانة في أي جريمة لابد أن تكون مبنية على أدلة مشروعة في الحصول عليها وفق قواعد الأخلاق و النزاهة، و احترام القانون من طرف الجهة المتخصصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية،[1] ولا يكون إلا إذا تم التفتيش عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء و إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية، فلا يعتد بقيمته مهما كانت دلالته الحقيقية و ذلك لعدم مشروعيته، و على هذا الأساس فإن إجراءات جمع الأدلة الإلكترونية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، و بالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة عليها بالإدانة في المواد الجنائية.[2]

المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي

إن مجرد الحصول على الدليل الالكتروني و تقديمه للقضاء لا يكفي للاعتماد عليه كدليل للإدانة إذ أن الطبيعة الفنية الخاصة بالدليل الالكتروني تمكن من العبث، فضلا عن ذلك، فإن نسبة الخطأ في اجراءات الحصول على دليل صادق في الإبلاغ

[1] خالد عياد الحلبي، مرجع سابق، ص 239

[2] مرجع نفسه، ص 240

عن الحقيقة فتبدو عادية في مثل هذا النوع من الأدلة، لذلك تثور فكرة الشك في مصداقيتها كأدلة الاثبات الجنائي.[1]

الفرع الأول : حجية الدليل الالكتروني في الإثبات الجنائي

إن مسألة تقييم الدليل الجنائي في إثبات الوقائع الججرمية مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها.

أولا : تقييم الدليل الإلكتروني من حيث سلامته من التزوير

يمكن التأكد من سلامة الدليل الالكتروني من العبث بعدة طرق، مذكر منها :

- فكرة التحليل التخاطري الرقمي و التي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، و من ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، و يستعان في ذلك باستخدام الحاسوب الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في مضمون الدليل الرقمي، و هذا العلم يستعان به أيضا في كشف مدى التلاعب بمضمون هذا الدليل.[2]
- استخدام عمليات حسابية خاصة تسمى الخوارزميات و يلحق إلى هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي و في حالة العبث بالنسخة الأصلية بالإمكان التأكد من سلامة الدليل الرقمي من التحريف و التغيير باستعمال هذه العمليات الحسابية.[3]

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

[2] ياسين بن عمر، **المعالجة القانونية الإلكترونية في القانون الجزائري و التشريعات المقارنة**، جامعة باتنة، مجلة العلوم القانونية و السياسية، مجلد 10، العدد 3، 2019، ص 720

[3] خالد عياد الحلبي، مرجع نفسه، ص 249

- استعمال الدليل المحايد و هو نوع من الأدلة الرقمية للمخزون في البيئة الافتراضية لا علاقة لخ بموضوع الجريمة، و لكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في نظام الحاسوب، و لاشك أن الخبرة التفقنية تمثل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي، فإذا كان للخبرة التقنية أهمية كبرى في مجال استخلاص الدليل الرقمي، فإن لها ذات الدور في بحث مصداقيته و تقبمه من حيث عدم حصول أي عبث عليه، فنقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم عليه كواجب قضائي أن يستعين في هذه المسائل بوسائل الخبرة كنهج، ليس من أجل استيفاء الدليل فحسب، بل كذلك لبحث مصداقيته في مجال المعالجة الآلية للمعلومات و تحقيق اليقينية لهذا الدليل.[1]

ثانيا : تقييم الدليل الالكتروني من حيث السلامة الفنية للاجراءات المتبعة في الحصول عليه

سبق الحديث على أن الدليل الرقمي يتم الحصول عليه بإتباع جملة من الإجراءات الفنية و التي من الممكن أن يعتريها خطأ يشكك في سلامة نتائجها الأمر الذي يحتم إخضاعها إلى اختبارات كوسيلة للتأكد من سلامة هذه الإجراءات من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات و يتبع في ذلك مجموعة من الخطوات :

- إخضاع الأدة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج، و يكون ذلك باتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأدلة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي و في نفس الوقت لن تضاف إليها أي بيانات جديدة و هو ما قد يعطي النتائج المقدمة مصداقية

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

في التدليل على الوقائع، و يتمثل هذان الاختباران في : اختبار السلبيات الزائفة و مفاده أن تخضع الأدلة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، و أنه لم يتم إغفال معطيات مهمة عنه، أما الاختبار الثاني و الذي يجرى باختبار الايجابيات الزائفة مفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي للاختبار يمكن من التأكد من أن هذه الاداة لا تعرض معطيات إضافية جديدة.[1]

- الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ بينت الدراسات العلمية و البحوث المنشورة في مجال تقنية المعلومات بالطرق السليمة التي يجب اتباعها في الحصول على الدليل الرقمي و في المقابل، بينت تلك الدراسات أيضا الأداوت المشكوك في كفاءتها و هو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأداوت.[2]

من خلال ما تقدم، يمكن الوقوف على سلامة الدليل الإلكتروني، فإذا توافرت في الدليل الالكتروني الشروط العامة لما يمكن أن يمثل أساسا لتأكيد الثقة فيه، فإنه يبدو و من غير المعقول أن يعيد القاضي تقييم هذا الدليل و طرحه من جديد على البحث، فإن الدليل الالكتروني بوصفه دليلا علميا، فإن دلالته قاطعة شأن الواقعة المستشهد به منها، فإذا سلمنا سابقة إمكانية التشكيك في سلامة الدليل الالكتروني بسبب قابليته للعبث و نسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم و إن لم يقطع به أهل الاختصاص.[3]

[1] خالد عياد الحلبي، مرجع سابق، ص 251

[2] ياسين بن عمر، مرجع سابق، ص 721

[3] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1701

إذا توافرت في الدليل الاكتروني الشروط السابقة بخصوص سلامته من العبث و الخطأ، فإن هذا الدليل لا يمكن رده استناد السلطة القاضي التقديرية اذا سلطة القاضي في رد الدليل استنادا لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، و هو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة بحيث بقتصر دور القاضي على بحث صلة الدليل بالجريمة، و لاشك أن الخبرة تحتل في هذه الحلة دورا مهما في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث الدليل هي من صميم الخبرة لا القاضي.[1]

الفرع الثاني : موقف المشرع الجزائري من الدليل الالكتروني في الإثبات الجنائي

إن من واجب القاضي الجنائي سواء كان قاضي التحقيق أو غرفة الاتهام أو المحكمة الجزائية أن تقيم الدليل على المتهم ولا يجوز أن يحاكم المتهم و يدان بمجرد وجود قرائن بل لابد أن تكون هذه الدلائل مكملة لبقية الأدلة المادية الأخرى، كما يجب أن تتسم إجراءات جمع الادلة بالمشروعية و ذلك احتراما للحرية الشخصية للمتهم باعتباره بريئا إلى أن تثبت إدانته بحكم.[2]

إن الاثبات الجنائي هو كل ما يؤدي إلى كشف الجريمة و إقامة الدليل على وقوعها و التأكد من أن المتهم هو مرتكب الجريمة بالفعل و وجود الدليل على ذلك، و يعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة و كشف الجريمة و نسبتها إلى المتهم، و قد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في

[1] فلاح عبد القادر، آيت عبد المالك نادية، مرجع سابق، ص 1702

[2] ياسين بن عمر، مرجع سابق، ص 721

مجال الإثبات الجنائي فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منها و قد سبق الإشارة إليهما.

تنتمي الجزائر إلى مجموعة الدول التي تتبنى نظام الإثبات الحر في مجال الإثبات الجنائي، فهي تساير النظم اللاتينية كفرنسا و بلجيكا و الأردن و سوريا، و هو الأمر الذي كرسته المادة 212 من قانون الاجراءات الجزائية التي جاء في نصها على أن "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص بها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه".[1]

إن قرار المشرع الجزائري للحرية في تقديم الأدلة المقنعة لشخص القاضي الموضوع هو لتعزيز اثبات قرينة البراءة، و تعزيز لممارسة حقوق الدفاع الفردية، غير أن هذا الإطلاق بدون تحديد و تخصيص يعد قصورا تشريعيا واضحا، فلا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الالكتروني هو دليل من نوع خاص شأنه شأن الجرائم الالكترونية، فغياب أدنى نص قانوني في هذا الشأن يؤدي إلى ظهور إشكالات متعلقة بطبيعة الأدلة المقدمة أمام الجهات القضائية بحيث يمكن[2] لهذه الأخيرة و في حال عدم إلمامها بتقنية المعلوماتية دحض هذا الدليل و عدم الاعتداد به، و لو كان حائزا على القوة التشريعية و تتوفر كافة شروط الصحة و كذلك العكس.

أما بالنسبة لسلطة القاضي الجزائري في تقدير الدليل الإلكتروني، فإن المادة العلمية للدليل الالكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف

[1] المادة 12 من قانون الإجراءات الجزائية

[2] بوبكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012، ص 507

فقهي، إن هناك من يرى أن ادليل العلمي و منه الدليل الالكتروني له قوته الثبوتية الملزمة حتى للقاضي مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، و هناك من يرى بأن مبدأ حرية القاضي في الامتناع يجب أن يبسط سلطتع على كل الأدلة دون استثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تصديرها يعد بمثابة الرجوع إلى مذهب الاثبات القانوني المقيد، و المشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأية طريقة من طرق الإثبات ما عدا الجرائم التي يتطلب إثباتها دليلا معينا و منح القاضي الجزائي سلطة تقدير الدليل و الحرية في تكوين قناعته من أي دليل يطمئن عليه.[1]

[1] بوبكر رشيدة، مرجع سابق، ص 508

خاتمـــــة

خاتمـــــة

بعد استعراضنا بالبحث و الدراسة لموضوع خصوصية التحقيق في الجرائم الإلكترونية، اتضح لنا جليا مدى التحول الذي مس مجلات البحث في مجال العلوم الجنائية، فقد تأثرت هذه الأخيرة بالتطور الجنائي و بالخصوص بتطبيقات التقنيات الإلكترونية، فقد حاولنا من خلال كل ما استعرضناه إضفاء الطابع الفني و التقني بالقدر المستطاع إلى الطابع القانوني للبحث، و ذلك من خلال الاعتماد على مزيج من المصطلحات القانونية و العلمية و الإلكترونية و ذلك بغرض إبراز مدى تقدم البحوث في المجال القانوني الجنائي و خصوصا في مجال الإجراءات الجنائية المتعلقة بأعمال البحث و التحقيق، فطبيعة الجريمة المعلوماتية تفرض نمط تحقيق مختلف عن نمط التحقيق المعتاد في الجرائم العادية، فتختلف بذلك الوسائل و يكون وجود خبير في الإعلام الآلي في عملية التحقيق الجنائي لما له من كفاءة و دراية بعالم المعلوماتية في الفضاء الإلكتروني هذا من جهة، و من جهة أخرى، ما يبرر اللجوء إلى إجراءات تحقيقية خاصة في هذا النوع من الجرائم هو طبيعة الدليل في إثبات قيام الجريمة و نسبها لفاعل محدد، و هنا تكون الأدلة الرقمية الدليل المناسب لذلك، و على ضوء الإشكالية التي أظهرتها الدراسة خلصت الإجابة عنها في جملة من النتائج.

النتائج المستخلصة في موضوع البحث

- التحقيق الجنائي المعلوماتي هو مجموعة من الإجراءات القانونية المتكاملة تهدف إلى التنقيب و البحث عن الأدلة الرقمية لإثبات الجريمة المعلوماتية و الوصول إلى مرتكبيها.
- التحقيق الجنائي المعلوماتي يعتمد على التخطيط الاستراتيجي المسبق و التخطيط التكتيكي مع التحديد لخطة عمل مسبقة.

- محل التحقيق الجنائي المعلوماتي هو المعلومات و البيانات المتواجدة بالبيئة الإلكترونية.
- يواجه التحقيق الجنائي المعلوماتي صعوبات قد ترجع إلى طبيعة الجريمة المعلوماتية أو إلى الجهات المتضررة أو إلى جهات التحقيق.
- الدليل الرقمي وسيلة أمثل لإثبات الجريمة المعلوماتية و معرفة مرتكبيها.
- المعاينة الإلكترونية، التفتيش الإلكتروني، المراقبة الإلكترونية، و الضبط الالكتروني، هي إجراءات تحقيقية للحصول على الدليل الرقمي.
- يقترن نجاح إجراءات البحث و التحقيق في الجرائم المعلوماتية بمدى براعة و فعالية و جاهزية الجهات المختصة بمباشرة الإجراءات لتتبع الأدلة الإلكترونية، و تحصيلها و حفظها بغرض عرضها على الجهات المختصة بتقديرها.
- لاحظنا على المستوى القانوني و التشريعي مدى الاهتمام الذي توليه الدول و الحكومات لهذا المجال من خلال التحديات المستمرة و المتوالية للنصوص العقابية و القانونية بشكل متناسق مع تطور الأساليب الإجرامية.

و من خلال الملاحظات السابقة فإنه بدى لنا تقديم جملة من التوصيات التي نرى أنه من الممكن أن تساهم في مواجهة تحديات الموضوع قيد الدراسة، و التي تتمثل فيما يلي :

- استحداث نصوص قانونية متلائمة مع مستوى التطور الذي آلت إليه التقنية الإلكترونية.
- حث ضحايا الجرائم الإلكترونية على التبليغ.
- تعديل قانون الإجراءات الجزائية على وجه الاستعجال من خلال إدراج قسم خاص بأعمال البحث و التحقيق في الجرائم الإلكترونية.

- إبرام اتفاقيات تعاون داخلية بين القضاة و مهندسي الإعلام الآلي من أجل إثراء المعرفة الفكرية في ميدان المعلوماتية.
- بالرغم من اهتمام المشرع الجزائري بالجريمة الإلكترونية و بالعقوبات المقررة لها (09-04) لا يكفي لمواجهة الإنتشار الرهيب لهذه الجرائم، بل يجب إصدار قانون خاص بها و تشديد العقوبات على مرتكبيها.

قائمة المراجع و المصادر

قائمة المراجع و المصادر

أ. الكتب

1. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، دار الحامد للنشر و التوزيع، الأردن، 2014

2. خالد عياد الحلي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنيت، دار الثقافة و النشر و التوزيع، عمان، الطبعة الأولى

3. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، 2010

ب. المقالات و المنشورات

1. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، العدد 7، 2008

2. عبد الحكيم مولاي ابراهيم، الجرائم الالكترونية، مجلة الحقوق و العلوم الانسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الثاني، العدد 23، 2015

3. رشيدة بوبكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري، المقارن منشورات الحلبي الحقوقية، الطبعة الأولى، 2012

4. بوضياف اسمهان، الجريمة الإلكترونية و الاجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018

5. عيدة بلعايد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية، جامعة مولاي الطاهر، سكبكدة، العدد 06، 2011

6. فلاح عبد القادر، آيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، جامعة الجيلالي بونعامة، خميس مليانة، مجلد 04، العدد 02، 2019
7. عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، 2003

ج. الأطروحات و الرسائل

رسائل الماجيستير

1. نهلا عبد القادر المومني، الجرائم المعلوماتية، رسالة ماجيستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر و التوزيع، 1429 هـ - 2008، الطبعة الأولى، الإصدار الأول، 2008
2. أدهم باسم نمر البغدادي، وسائل البحث و التحري عن الجرائم الإلكترونية، رسالة ماجيستير، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018
3. سعيد علي نعيم، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري، رسالة ماجيستير، جامعة الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، قسم الحقوق، 2012-2013
4. نداء نائل، فايز المصري، خصوصية الجرائم المعلوماتية، جامعة النجاح الوطنية، رسالة ماجيستير، نابلس، فلسطين، 2017
5. صغير يوسف، الجريمة الالكترونية المرتكبة عبر الأنترنيت، رسالة ماجيستير، جامعة مولود معمري، تيزي وزو، 2013

6. سعيداني تميم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجنائي، رسالة ماجيستير، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012

أطروحات الدكتوراه

1. براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، 2018

مذكرات الماستر

1. عديلة مراد، عبدلي مروان، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، 2021
2. بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية، مذكرة ماستر، جامعة عبد الرحمن ميرة، بجاية، 2018

د. القوانين و المراسيم

1. القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبة، العدد 47، الصادر بتاريخ 25 شعبان 1430 المؤرخ في 16 أوت 2009
2. القانون 06-22 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر 2006، الجريدة الرسمية

للجمهورية الجزائرية الديمقراطية الشعبية، العدد 84 الصادر في 4 ذي الحجة عام 1427 الموافق لـ 24 ديسمبر 2006

3. المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 53

الملخص

الجرائم الالكترونية من الأنماط الاجرامية الجديدة التي أفرزتها تكنولوجيات الاعلام و الاتصال الحديثة، فهي تختلف تماما عن الجرائم التقليدية.

و لقد الدراسة في هذا المجال معطيات قانونية و أخرى فنية و تقنية نظرا لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الأنترنيت و العلوم القانونية الإجرائية، و لذلك فقد عالجنا في إطار فصلين مختلف الجوانب المتصلة بالموضوع، حيث تناولنا تعريف الجريمة الإلكترونية من النواحي الفقهية و القانونية و خصائصها، ثم تطرقنا إلى تعريف التحقيق الجنائي و خصائصه و كذا خصائص المحققين في التحقيق، و كذا استعراض الهيئات الخاصة المكلفة باجراءات البحث و التحقيق بشأن الجرائم الالكترونية، و قد ركزنا في هذا المجال حول الهيئات المكلفة بالبحث و التحقيق المنتمية إلى مختلف الهيئات كالأمنية في صورة مصالح الشرطة و الدرك.

و في الأخير ختمنا بحثنا بمجموعة من النتائج التي تفيد في الإجابة على الإشكالية، مع تحصيل مجموعة من التوصيات القانونية التي من شأنها دعم آليات البحث و التحقيق في الجرائم الالكترونية.

الكلمات المفتاحية : الجرائم الالكترونية، التحقيق الجنائي الالكتروني، الاثبات الجنائي الالكتروني، الأمن السيبراني

Résumé

Les infractions électroniques sont l'un des nouveaux types de la criminalité engendré par les technologies modernes de l'information et de la communication qui se diffère des infractions classique.

L'étude inclus dans ces données sur le terrain juridique et d'autres techniques et des technologies en raison de la nature du sujet qui est le point d'intersection entre les systèmes scientifique de la procédure de l'informatique et de l'information juridique, on a donc traité avec sous deux aspects différents pertinents de sujet.

La définition du crime électronique a tous les égards, y compris la jurisprudence et juridique et ces caractéristiques de l'enquête criminelle et ses enquêteurs, et nous avons réservé les différent organes propres procédures couteuses de recherche et enquête sur crimes électroniques que nous avons concentré notre étude dans ce domaine autour des organismes chargés de la recherche et d'enquêtes appartenant à divers organismes à la fois sécurité de la police et la gendarmerie.

Et enfin, nous avons terminé notre recherche avec des ensembles de résultats qui aident à répondre au problème, avec la collection d'une série de recommandations juridiques qui soutiendraient de recherche et d'interrogations juridiques qui soutiendraient les mécanismes de recherche d'investigation des crimes cybernétique.

Mots clés : Cybercriminalité, Enquête criminelle électronique, Preuve criminelle électronique, Cyber-sécurité.