وزارة التعليم العالي والبحث العلمي
Ministry Of High Education And Scientific Research
جامعـــة محمد البشيـــر الابراهيمـــي برج بوعريريج
University Of Mohamed El Bachir El Ibrahimi-BBA
كلية الحقوق و العلوم السياسيـــة
Faculty Of Law And Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في القانون

تخصص: قانون أعمال

الموسومة بـــ :

خصوصية التحقيق الجنائي في الجرائم الإلكترونية

من إعداد الطالبتين:

- العمري سلسبيل
- الحديدي هدى

إشراف الأستاذ:

د/ رفاف لخضر

لجنـــة المناقشـــــــة:

الاسم واللقب	الرتبـــــة	الصفة
الاستاذ رفاف لخضر	أستاذ محاضر قسم أ	مشرفا
الاستاذ زاوي رفيق	أستاذ محاضر قسم ب	رئيسا
الاستاذ سي حمدي عبد المومن	أستاذ محاضر قسم ب	ممتحنا

السنة الجامعيـــــة: 2021م/2022م

بِسمِ ٱللَّهِ ٱلرَّحمَٰنِ ٱلرَّحِيمِ

شكر و عرفان

الحمد لله رب العالمين، و أشهد أن لا إله إلا الله ولي الصالحين و أشهد أن سيدنا و نبينا محمد رسول الله خاتم الأنبياء و المرسلين.

في كلية القانون أنت لا تقرأ لتستعد إلى الامتحان أنت تقرا لتستعد إلى اليوم الذي تكون فيه أنت الفصل بين إنسان برئ وحبل المشنقة.

بداية نتقدم بجزيل الشكر و العرفان للدكتور و الأستاذ **رفاف لخضر** الذي تفضل علينا بالإشراف على هذا العمل المتواضع، و تحمله معنا مشقته فشجعنا و أفادنا بالشيء الكثير من إرشاداته و نصائحه القيمة و معاملته الطيبة التي تدل على رفعة أخلاقه كما نتقدم بالشكر لجميع من قدم لنا يد المساعدة و بالمآزرة و التشجيع.

و أخيرا نوجه تحية تقدير للأساتذة المناقشين على تفضلهم لقراءة و تقييم عملنا هذا.

و الله ولي التوفيق

إهداء:

الحمد الله الذي وفقني على إنهاء عملي هذا و كان خير عون لي.

إلى نبع المحبة و الإيثار، إلى ملحمة الحب و فرحة العمر أمي غاليتي.

إلى مثال التفاني و الأخلاق، المبجل و المحترم والدي العزيز.

إلى عضدي وحبيباتي أخواتي:مروة ،أنفال ،تسنيم، توبة.

إلى أختي التي لم تلدها أمي صديقتي و توأم روحي "هدى"

إلى من لم يبخلوا بمساعدتي و دعمي :الأساتذة ، الأصدقاء و الأخلاء .

إلى نفسي القوية التي كادحت و تحملت الصعاب لأجل هذا اليوم.

و كل من يحبني بصدق و إخلاص أهديكم خلاصة عملي و ثمرة جهدي المتواضع.

العمري سلسبيل

إهداء:

و أخيرا جاء اليوم الذي ترفع له القبعة احتراما لسنين مضت بجهد ليس بهين.

اهدي فرحة تخرجي لكل روح كلفت نفسها بالدعاء لي و لم تقل سوى خيرا...

إلى من علمتني أن العطاء ليس له حدود أمي الغالية...

إلى الشمعة التي أنارت طريقي دائما أبي الغالي...

إلى عائلتي أخوتي الأعزاء " صلاح الدين ، إبراهيم ، محمد "

إلى أختي توأم روحي "ملك" كنتم عونا لي في مسيرتي دمتم لي...

إلى بنت الجزائر التي كانت بمقام الأخت و الصديقة الأقرب لي " سلسبيل ".

إلى نفسي التي صبرت لأجل هذا اليوم. إلى وطني الحبيب "الأردن – فلسطين ".

الحديدي هدى

يعد التطور التكنولوجي مهم في العصر الحديث حيث سهل الحياة للبشرية و سهل الكثير من الخدمات و الأعمال حيث انتشر على نطاق واسع في كافة الدول ، و نتيجة ذلك التطور أصبح الحاسوب و الانترنت شرطا أساسي في المجتمع لدخول عصر العولمة ،إلا أنه و رغم فوائده القيمة انتشر نوع جديد من الجرائم المختلفة عن الجرائم التقليدية من حيث الاختصاص و إجراءات التحقيق ووسائل الإثبات حيث عرفت بشدة خطورتها لصعوبة التحقيق فيها فالمجرم غير ظاهر في الواقع حيث يستطيع رؤية المعلومات صوتا و صورة عبر الإنترنت و في أي مكان في العالم فيسمح له باستغلال هذه الشبكة و إرتكاب جريمة و هذا يعتبر خطر يهدد المجتمع و العالم ككل عرفت الجريمة الالكترونية على أنها سلوك غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالكتروني و التي تتجول عن طريقه لكن البعض يعتقد أن سرقة جهاز الكمبيوتر أو كسره يعد جريمة إليكترونية و هذا غير صحيح فالجرائم الالكترونية يتم النص عليها حصرا في القانون، فقد ورد النص في المعاهدة مجلس أوروبا لمكافحة الجرائم الالكترونية (معاهدة بوداسيث) سنة 2001 على أربع مجموعات من الجرائم الالكترونية هي الجرائم التي تقع ضد سلام المعلومات و البرامج و خصوصياتها و توافرها و الجرائم المتصلة بالكمبيوتر و الجرائم المتصلة بالمحتوى و الجرائم المتصلة بانتهاك حقوق الملكية الفكرية و الحقوق الملحقة بها.

لا جدال في اعتبار أن الجرائم الالكترونية من أخطر الجرائم على الإطلاق و تأتي في مقدمة الأشكال الجديدة الجريمة المنظمة و خطورة هذه الجرائم نابعة من طبيعتها المعقدة من حيث ذاتية أركانها و حداثة أساليب ارتكابها فهي جريمة تقنية سهلة الارتكاب إنشاء في الخفاء في بيئة إليكترونية افتراضية و هذا ما أدى بنا إلى التطرق إلى هذا الموضوع.

أهمية الدراسة :

تتجلى أهمية الموضوع باعتباره من الموضوعات الحديثة و المعاصرة و المهمة في إطار البحوث كالأكاديمي و القانوني، كما أنه يفتح المجال لأبحاث مستقبلية تتناوله من زوايا مختلفة حيث يمكن الاستفادة منه على أرض الواقع و محاولة تقديم حلول ممكنة لمكافحة هذه الجريمة. كما تساهم في إضافة معلومات يمكن وضعها في المكتبة القانونية في مجال التحقيق الجنائي في الجرائم الالكترونية.

أهداف الدراسة :

•جذب الانتباه و التركيز على موضوع خصوصية التحقيق الجنائي في الجرائم الإلكترونية و هذا يعود لتطور الثروة الإلكترونية بشكل رهيب و سريع و هذا ما أدى إلى تطور الإجرام المعلوماتي حيث أصبح يرتكب بطريقة يصعب اكتشافها .

• معالجة هذا الموضوع لتعلقه بالوسائل الحديثة و ذلك كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النوع من الجرائم.

• زيادة و إثراء الكم المعرفي في هذا المجال لكونه أساسي .

أسباب اختيار الموضوع :

لقد كان اختيارنا لهذا الموضوع " خصوصية التحقيق الجنائي في الجرائم الإلكترونية " رغبة شخصية ملحة منا ، أولا لأهميته لكونه حديث و معاصر و السبب الرئيسي هو

أننا شاهدنا الجرائم الإلكترونية جرت في كافة المجتمعات العربية و الغربية بمختلف مواقع التواصل من ابتزاز و تشهير و سرقة الكترونية و منها انتحال شخصيات وهمية بغرض الإيذاء و افتعال الضرر لهذا كان من الضروري التطرق إليه من خلال موضوعنا للتسهيل و نشر الوعي .

إشكالية الدراسة:

إن البحث في التحقيق الجنائي في الجريمة الإلكترونية يثير الكثير من الجدل نظرا لكونه حديثو معاصر. و على هذا الأساس نتوصل إلى طرح إشكالية بحثنا و التي تتمثل في :

• هل خصوصية التحقيق الجنائي في الجرائم الإلكترونية كفيلة في مواجهة الخطر الناتج عنها ؟

للإجابة عن هذه الإشكالية الجوهرية لابد بالبحث في بعض التساؤلات التي تتفرع عنها و التي من بينها:

• فيما يتمثل مفهوم الجرائم الإلكترونية و ما هي أهم أجهزتها ؟

• كيف تتم الإجراءات المتعلقة بالتحقيق الجنائي في الجرائم الإلكترونية و ما هي الحلول التي تم تبنيها؟

منهج الدراسة : لدراسة موضوعنا اتبعنا **المنهج الوصفي** من خلال معالجة مختلف جوانبه كما اعتمدنا على **المنهج التحليلي** من أجل تحليل مختلف النصوص القانونية المتعلقة به.

صعوبات الدراسة:

لقد واجهنا في إعداد موضوعنا هذا العديد من الصعوبات و على رأسها :

• قلة المراجع القانونية المختصة في القانون الجزائري .

• صعوبة الحصول على مراجع أجنبية رغم جلوسنا لساعات طويلة وراء الانترنت للبحث عنها .

• يعتبر موضوع الجريمة الإلكترونية من المواضيع الطويلة و المتشبعة و هذا ما استدعى منا التطرق غلى كافة جوانبه القانونية.

تقسيم الدراسة:

للإجابة عن الإشكالية الرئيسية و تساؤلاتها الفرعية اعتمدنا في هذه الدراسة خطة بحث ثابتة و متوازنة تنقسم إلى فصلين، حيث تناولنا في الفصل الأول ماهية الجرائم الإلكترونية ،أركانها و دوافع المجرم إلى ارتكابها. كما كان من المهم التطرق إلى الأجهزة .أما في الفصل الثاني فقد تطرقنا إلى الإجراءات و صعوبات التحقيق الجنائي في الجرائم الإلكترونية وكذا الحلول المقترحة لذلك.

الفصل الأول: ماهية الجريمة الإلكترونية ،أركانها ،دوافعها و أجهزة مكافحتها

الفصل الأول:.....ماهية الجريمة الإلكترونية ،أركانها ،دوافعها و أجهزة مكافحتها

مما لاشك فيه أن الثورة المعلوماتية سهلت الحياة البشرية إلا أنه رغم إيجابياتها نتج عنها نوع جديد من الجرائم المتميزة عن الجرائم التقليدية و التي تتمثل في الجرائم الالكترونية و هذه الأخيرة تنعكس خصوصيتها على إجراءات التحقيق الجنائي ، إلا أن البعض يعتقد أن الجرائم الالكترونية هي التي يتم فيها سرقة جهاز الكومبيوتر و هذا خطأ و على هذا الأساس لجأنا إلى التحدث عن ماهية الجريمة الإلكترونية و دوافع المجرم إلى ارتكابها

المبحث الأول: ماهية الجرائم الإلكترونية و دوافع ارتكابها

إن الجريمة الإلكترونية هي من الظواهر الحديثة و ذلك لارتباطها بتكنولوجيا حديثة تتمثل في تكنولوجيا المعلومات و الاتصالات و قد أحاط بتعرف الجريمة الإلكترونية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف لها إلا أنه لا يوجد تعريف محدد و متفق عليه بين الفقهاء و على هذا الأساس تحدثنا في المطلب الأول عن تعريف الجريمة الإلكترونية التي وضعها مختلف الفقهاء و في المطلب الثاني خصصناه لأركان الجريمة الإلكترونية و عن دوافع ارتكابها في المطلب الثالث.

المطلب الأول: مفهوم الجريمة الالكترونية و أركانها

الفرع الأول :تعريف الجريمة الالكترونية :

تناولنا في هذا الجزء عدة تعريفات للجريمة الإلكترونية حيث تعددت محاولات الفقهاء في تعريف جرائم الانترنت ومنها:

- « هي ذلك النوع من الجرائم التي تتطلب الماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات،لارتكابها أو التحقيق فيها ومقاضاة فاعليها[1]»

- « إنها الجرائم التي لا تعرف الحدود الجغرافية،والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة[1].

[1] منير و ممدوح محمد الجنبيهي ، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي ، الأزاريطة –الاسكندرية 2005 ط2 ص179.

– وفي تعريف أخر «كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها[2]»

– كما إنها الجرائم الناشئة عن استعمال التواصل بين الشبكات

– **التعـــريف الأكـــاديمي :**

كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ، ترتبت عنه خسارة تلتحق بالصحية أو مكسب يحققه الجاني ، كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية على :

1– على ما تكون المعلوماتية موضوعا للاعتداء (عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية).

2– عندما تكون المعلوماتية أداة ووسيلة للاعتداء (عندما يستخدم الجاني أو جهاز معلوماتي لتنفيذ جريمته) [3].

– **التعريف القـــانوني :**

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات

---

[1] نفس المرجع السابق ص 13

[2] محمد أمين أحمد الشواكية –جرائم الحاسوب و الانترنت ص 10.

3 المقدم عز الدين عز الدين ، الاطار القانوني الوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية ، بسكرة في 16/11/2015

غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث .[1]

وهي أيضا «تلك الجرائم العابرة للحدود والتي تقع على شبكة الانترنت أو بواسطتها من قبل شخص على دراية فائقة بها » .

والباحث يؤيد هذا التعريف الأخير ،لأنه يبرز خصائص جرائم الانترنت إلا انه من الأفضل عدم تحديد هذه الجرائم بأنها عابرة للحدود .لأنها من الممكن أن تكون جرائم داخلية أو دولية أو ذات بعد دولي كما سنرى لاحقا لذلك نرى أن يكون تعريف جرائم الانترنت بأنها :تلك الجرائم التي تقع على شبكة الانترنت أو بواسطتها من قبل شخص ذو معرفة تقنية.

الفرع الثاني : أركان الجريمة الإلكترونية

إن للجريمة الإلكترونية أركان ثلاثة وتتمثل في الركن الشرعي وهو الصفة غير المشروعة للفعل ، وتتمثل قاعدة التحريم و العقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

1 قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 صادر بتاريخ 16/08/2009 ،ص 5

و الاتصال ومكافحتها . أما الركن المادي يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي , وأخيرا الركن المعنوي وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ . كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني (المجرم الإلكتروني) وبهذا المعنى يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي ، أما المجني عليه يكون في الغالب الأعم شخص معنوي ، كالبنوك والشركات وغيرها من المنظمات والهيئات التي تعتمد في إنجاز أعمالها على الحاسب الآلي , علما أن للجريمة الإلكترونية محلا يتمثل في المعلومات ، الأجهزة ، الأشخاص أو الجهات.[1]

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

إن فئات مرتكبي الجرائم الإلكترونية تختلف عن مرتكبي الجرائم التقليدية، فالدافع هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة و الشفقة و البغضاء و الانتقام. و للجريمة الإلكترونية عدة دوافع لارتكابها ،فبعضها شخصية أو مادية و البعض الآخر يرجع لدوافع خارجية و التي يكون مصدرها الرغبة الإجرامية . و نوجز أهم الدوافع في مايلي:

[1] عبد الله دغش العجمي ، المشكلات العملية والقانونية للجرائم الإلكترونية ، دراسة مقارنة ، رسالة مكملة للحصول على درجة الماجستير في القانون العام ، جامعة الشرق الأوسط ، 2014 ، ص من 26 إلى 36

أولا :السعي إلى تحقيق الكسب المالي

حيث تستهدف أكثر الجرائم المعلوماتية إدخال تعديل على عناصر الذمة المالية، و طمع الاستيلاء على المال دافعها و بريق المكسب السريع محركها. و حجم الربح الكبير الممكن تحقيقه من بعضها، خاصة غش الحاسب الالكتروني، أو الاحتيال المرتبط بالحاسب، من أجل اختلاس المال. و غالبا ما يكون الدافع لارتكاب هذا النوع من الجرائم هو وقوع الجاني في مشاكل مادية و عم القدرة على تسديد ديونه المستحقة، أو مشاكل عائلية تعود لعدم توفر المال الكافي، أو القيام بأعمال المراهنة أو القمار أو من أجل شراء المخدرات. و هذا ما يؤدي بالجاني للقيام بعمليات التلاعب بالأنظمة المعلوماتية للبنوك أو المؤسسات المالية و ذلك باختراق الأنظمة المعلوماتية لها واكتشاف فجواتها للأمنية من أجل الخروج من هذه المآزق[1] .

ثانيا :الرغبة في الانتقام و إلحاق الضرر

يتعرض العاملون في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ، لضغوطات نفسية ناجمة عن ضغط العمل و المشكلات المالية ، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح مما يدفع بعض العاملين لارتكاب جرائم الحاسب الإلكتروني و تحديدا جرائم إتلاف البيانات ،و البرامج ، و زرع الفيروسات باعثها الانتقام من المنشأة أو رب العمل أو أحد الزملاء[2].

---

[1]غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية كلية الحقوق ، لبنان ،2004 ،ص158،157

[2]محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية)جرائم الكمبيوتر والانترنت،(الطبعة الأولى، المكتبة العصرية للنشر والتوزيع ،مصر، ،2010ص 51

ثالثا: الرغبة في قهر النظام و التفوق على تعقيد وسائل التقنية

قد يكون الدافع إلى ارتكاب جرائم الحاسب الإلكتروني الرغبة في قهر النظام و تخطي الحواجز حوله ، أكثر من رغبة الحصول على الربح ، و يتجسد ذلك في نسبة معتبرة من جرائم الحاسب الالكتروني خاصة ما يعرف بأنشطة الـ(hackers) – المتطفلين الدخيلين على بعد –[1] و الاستخدام غير المصرح به لنظام الحاسب ، و اختراق مواقع الانترنت و مرتكبي هذه الجرائم (شغف الآلة) دائما يحاولوا إيجاد الوسيلة إلى التفوق عليها . و يتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم الحاسب ، الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب و شبكات المعلومات ، و لإظهار تفوقهم على وسائل التكنولوجيا الحديثة.

رابعا : الرغبة في التعليم

هناك من يرتكب جرائم الحاسوب ، من أجل الحصول على الجديد من المعلومات و سير أغوار هذه التقنية متسارعة النمو و التطور . و هؤلاء الأشخاص يقومون بالبحث و اكتشاف الأنظمة و العمل من خلال الجماعة و تعليم بعضهم ، و يفضل هؤلاء القراصنة مجهولين اكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة و يكرس البعض الآخر كل وقته في تعلم كيفية اختراق المواقع الممنوعة و التقنيات الأمنية لأنظمة الحاسوبية .

[1] محمد على العريان – الجرائم المعلوماتية – سنة 2004 – دار الجامعة الجديدة للنشر – ص 65

يرى هؤلاء المجرمون أن جميع المعلومات المفيدة يجب أن تتاح حرية نسخها و الاطلاع عليها ، إلا أنهم يقرون بضرورة إغلاق بعض نظم المعلومات السرية التي تخص الأفراد [1].

و بالتالي يتضح أن المكسب المادي ليس دائما دافعهم على ارتكاب تلك الجريمة.

خامسا: المنافسة

محاولات الشركات المنافسة الحصول على معلومات تقنية أو أسرار تكنولوجية أو معلومات عن البنوك و المعاملات المالية كالأسهم و السندات المتعامل بها في البورصات العالمية ، و ذلك بواسطة أشخاص ذوي خبرة في الجريمة الإلكترونية مؤجرين على ذلك ن هذا النوع من الجرائم شائع في الجريمة الإلكترونية ، حيث يقوم هذا المختص بالجانب الفني من المشروع الإجرامي و آخر من المحيط أو خارج المؤسسة المجني عليها ، فيقوم بتغطية و التستر على عمليات التلاعب و تحويل المكاسب المادية [2]، و عادة ما يقومون بالتصنت على الأنظمة و تبادل المعلومات بصفة منتظمة حول أنشطتهم ، و ينتشر هذا الدافع نتيجة الوقوع تحت تهديد أو ضغط من الغير في مجالات الأعمال التجارية و الخاصة بالتجسس و المنافسة.

[1] عبد العال الديربي الجرائم الإلكترونية المركز القومي للاصدارات القانونية –القاهرة–2012 ص 48

[2] عفيفي كامل جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية دار نشر منشورات الحلبي الحقوقية 2003 ص32

سادسا: التهديد الأمني

بعض الجرائم الإلكترونية يكون سببها السياسة كتهديد الأمن الوطني و العسكري ، و ذلك بمحاولات لاختراق شبكات حكومية و الحصول على معلومات عسكرية لمختلف الدول في أنحاء العالم ، و هذا ما اوجد التجسس الإلكتروني و الإرهاب الإلكتروني و كذلك الحرب الإلكترونية كما هو حال الدول المتقدمة إلكترونيا.

سابعا: الدوافع الأخرى

لا تعتبر الدوافع السابق ذكرها هي الوحيدة بل إن هناك دوافع أخرى تدفع بالمجرم المعلوماتي إلى ارتكاب الجريمة الإلكترونية ، فمثلا تعتبر الدوافع السياسية و الاقتصادية من أهم المحفزات إلى ارتكاب هذا السلوك الإجرامي ، و ترتكب عن طريق شبكة الإنترنت بشكل شبه دائم . كما يعتبر التسابق الفضائي و العسكري الحاصل بين الدول دافعا لارتكاب الجريمة الإلكترونية ، و كذلك مناهضة العولمة قد تكون أحد أسباب ارتكاب هذا الفعل الإجرامي.

و أخيرا يمكننا القول أن الفعل الواحد قد يعكس دوافع متعددة و خاصة و قد تتداخل و تشترك هذه الدوافع من أجل الوصول إلى هدف واحد.

المبحث الثاني: أجهزة التحقيق في الجرائم الإلكترونية

المطلب الأول: الهيئات المكلفة بالتحقيق في الجرائم الإلكترونية

الفرع الأول: الهيئات القضائية الجزائية المختصة

يعتبر إنشاء هيئات قضائية جزائية متخصصة توجها جديدا لتطويق نطاق الجرائم الخطيرة و من بينها الجرائم المعلوماتية.

أولا: إنشاء الهيئات القضائية الجزائية المتخصصة

نشأت هيئات قضائية جزائية متخصصة منذ تعديل قانون الإجراءات الجزائية الجزائري بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري .

باستقراء نص المادة 37 و 40 منه ، يتضح أن المشرع الجزائري خروجا عن القواعد العامة للاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق و المحددة بـ :

- مكان وقوع الجريمة.
- محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيه .
- المكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى و لو حصل هذا القبض لسبب آخر.

فقد أجاز المشرع بموجب الفترة الثانية من المادة 37 قانون الإجراءات الجزائية تمديد اختصاص وكيل الجمهورية في جرائم محددة على سبيل الحصر و من بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات إلى دائرة محاكم أخرى محددة عن طريق التنظيم ، و هو نفسه بالنسبة لتمديد اختصاص قاضي التحقيق بموجب الفقرة الثانية من المادة 40 قانون الإجراءات الجزائية .

كما نصت الفقرة الأخيرة من المادة 329 من قانون الإجراءات الجزائية الجزائري ، على تمديد الاختصاص المحلي للمحكمة في الجرائم المحددة على سبيل الحصر و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

و ما يفسر خروج المشرع عن معايير الاختصاص الأصلي[1] في الجرائم المعلوماتية هو:

•اتساع مكان ارتكاب الجرائم المعلوماتية خارج حدود الاختصاص الإقليمي التقليدي ، و انتشار الأعمال المكونة هذه الجرائم داخل و خارج حدود الدولة .

• التمسك بالمعايير الأصلية للاختصاص يشكل عائقا أمام مواجهة الجرائم المعلوماتية.

• الطبيعة الخاصة لهذه الجرائم.

[1] كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11،العدد01. ، ص0211 ، سنة21

و قد حدد المشرع سنة 2006 ، بموجب المرسوم التنفيذي رقم 06-348 تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق حيث يمتد الاختصاص المحلي لمحكمة سيدس محمد و محكمة قسنطينة و محكمة ورقلة و محكمة وهران و وكلاء الجمهورية و قضاة التحقيق في هذه المحاكم ، إلى محاكم المجالس القضائية التابعة لمختلف ولايات الوطن (58 ولاية) حسب الجهة[1].

و ما يعاب على المشرع الجزائري في مسالة تمديد الاختصاص أنه لجأ إلى ذلك إلا أنه لم يستحدث أساما متخصصة و لا تشكيلة خاصة لدى الجهات القضائية و لا قضاة متخصصين في الجرائم المحددة حصرا في هذه المواد و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، عكس ما ذهب إليه القانون الفرنسي في المادة 106-75 من قانون الإجراءات الجزائية الفرنسي أن المحاكم ذات الاختصاص الموسع تشمل على فرع للنيابة و تشكيلات للتحقيق و المحاكمة متخصصة بالنظر في الجرائم محل الاختصاص الذي وضح أنه تمديد الاختصاص للمحاكم لا يخص إلا القضاة المعينين في فروع متخصصة في حين أن قانون 04-14 جاء عاما حيث جعل من تمديد الاختصاص لكل القضاة الموجودين في المحاكم ذات الاختصاص الموسع[2].

---

[1] أنظر المادة 0-0-2-1المرسوم التنفيذي رقم ،22-022المؤرخ في 1أكتو ر ،0222يتضمن تمديد الاختصاص المحلي لبع المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد ،20الصادرة في 2أكتو ر ،0222ص .

[2] د. كريمة علة مرجع سابق ص132

ثانيا: توسيع صلاحيات ضباط الشرطة القضائية

تجدر الإشارة أن المادة 16 من قانون الإجراءات الجزائية الجزائري عالجت مسألة تمديد اختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني فيما يتعلق بالبحث و معاينة جرائم محددة بنص المادة و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و أجازت المادة 47 التفتيش و المعاينة و الحجز في هذه الجرائم في أي ساعة من النهار و الليل بإذن من وكيل الجمهورية كما يجوز لقاضي التحقيق بالتفتيش و الحجز ليلا أو نهارا في كامل التراب الوطني ، أو يأمر ضباط الشرطة القضائية المتخصصين بذلك.

كما مكن المشرع الجزائري بموجب المادة 51 من نفس القانون ، تمديد آجال التوقيف للنظر مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات ، و هنا لابد من مراعاة ضمانات المتهم خلال مرحلة التوقيف النظر.

الفرع الثاني: الهيئات غير القضائية

تتمثل الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتية في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، إضافة إلى السلطة الوطنية لمعالجة المعطيات ذات طابع شخصي ، و وكالة أمن الأنظمة المعلوماتية .

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

1- مفهوم الهيئة

في سبيل ضمان فعالية التحقيق أنشأ المشرع الجزائري بموجب المادة 13 من القانون 09-04 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، و ترك تحديد تشكيلها و تنظيمها و كيفيات سيرها عن طريق التنظيم ، حيث نظمت وفقا لعدة مراسيم بداية بالمرسوم الرئاسي 16-261 المؤرخ في 8 أكتوبر 2015 [1]، الذي عرف الهيئة بموجب المادة 02 منه على أنها : سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع لدى الوزير المكلف بالعدل ثم جاء المرسوم الرئاسي 19-172 المؤرخ 6 يونيو 2019[2] و أعاد تعريف الهيئة بموجب المادة 02 منه على أنها : مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني ، و اعيد تنظيم الهيئة من جديد بموجب المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020 [3]، حيث عرفت الهيئة بأنها سلطة إدارية

---

1 مرسوم رئاسي رقم ،11-021مؤرخ في 2اكتو ر ،2011يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد ،10الصادرة بتاريخ 2اكتو ر ،2011ص 1.

2 مرسوم رئاسي رقم ،10-100مؤرخ في 2جوان ،2010يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها و كيفيات سيرها، ج ر، عدد ،00الصادرة بتاريخ 0جوان ،2010ص21.

3 مرسوم رئاسي رقم ،02-120مؤرخ في 10جويلية ،2020يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد ،22الصادرة بتاريخ 12جويلية ،2020ص05.

مستقلة تتمتع بالشخصية المعنوية و الاستقلالية المالية ، توضع تحت سلطة رئيس الجمهورية .

و ما يلاحظ أنه وقع تعديل فيما يخص الجهة الوصية حيث أصبحت الهيئة توضع تحت سلطة رئيس الجمهورية ، بعدما كانت توضع تحت سلطة وزارة العدل سنة 2015 ، و لدى وزارة الدفاع الوطني سنة 2019 ، كما تم استرجاع مصطلح سلطة إدارية مستقلة كما كان سابقا في المرسوم الرئاسي 16-2061 ن و ذلك بعدما استعمل مصطلح مؤسسة عمومية ذات طابع إداري في المرسوم الرئاسي 13-172 عندما وضعت تحت سلطة وزارة الدفاع الوطني .

و موقف المشرع الجزائري اتجاه هذه السلطة الجديدة كان يسوده الغموض فلم يسلم بمبدأ استقلاليتها بسهولة رغم نصه على تمتعها بالاستقلالية الإدارية و المالية ، إذ أنه لم يوفر الأدوات القانونية التي تأكد ذلك ، فلم تكن رؤيته واضحة اتجاه مفهوم السلطة الإدارية المستقلة ، فالمصطلح يثير إشكالات قانونية عديدة و يحمل في طياته ما يشبه التناقض بين صفة السلطة الإدارية التي تتمتع بالتبعية و تخضع لرقابة رئاسية أو وصاية و إلى رقابة القضاء الإداري و بين صفة استقلالية [1].

و ما نلاحظه أن المرسوم الرئاسي لسنة 2019 غير المصطلح من سلطة إدارية مستقلة إلى مؤسسة عمومية ذات طابع إداري عندما ألحق الهيئة بوزارة الدفاع

[1] سلطان عمار، السلطات الادارية المستقلة في الجزائر، مجلة جيل للأبحاث القانونية المعمقة، العدد 33، 2010، ص53

باعتبارها وزارة سياسية تتنافى وصفة الاستقلالية التي تتمتع بها الهيئة ، و حسن فعل بتعديل المصطلح في المرسوم الأخير لسنة 2020، باعتبار الهيئة في ميدان الضبط الإداري أين يستعمل مصطلح سلطة أو هيئة مستقلة ، و تتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بالشخصية المعنوية و الاستقلال المالي ، و بوضع الهيئة تحت سلطة رئاسة الجمهورية فالهيئة هي امتداد للسلطة التنفيذية و باعتبار رئيس الجمهورية هو رئيس السلطة التنفيذية فهو المتحكم في هذه الهيئات .

2- مقر الهيئة :

كان مقر الهيئة مقتصر في مدينة الجزائر في المرسوم الرئاسي لسنة 2015 ، ثم أضيفت إمكانية تمديد مقر الهيئة إلى مكان آخر من التراب الوطني بموجب المرسوم الرئاسي لسنة 2019 ، و أبقى المرسوم الرئاسي لسنة 2020 على أن مقر الهيئة كأصل عام يحدد بمدينة الجزائر مع إمكانية نقل المقر إلى أي مكان آخر على تراب الوطني ، و يكمن الاختلاف بين المادة 03 في المرسومين الأخيرين أن نقل مقر الهيئة في مرسوم 2019 كان بموجب قرار من وزير الدفاع الوطني ، و أصبح نقل مقر الهيئة إلى كامل التراب الوطني بموجب المرسوم الرئاسي الأخير يتم بموجب مرسوم رئاسي.

3- مهام الهيئة : أبقى المرسوم الرئاسي لسنة 2020 على مهام الهيئة تحت رقابة السلطة القضائية و المتمثلة في[1] :

•اقتراح عناصر الإستراتجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

• تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

• مساعدة السلطات القضائية المختصة و مصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، لاسيما من خلال جمع المعلومات و التزويد بها و من خلال الخبرات القضائية .

• ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و المساس بأمن الدولة .

•تجميع و تسجيل و حفظ المعطيات الرقمية للأنظمة المعلوماتية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية[2] .

[1]أنظر المادة 04 من المرسوم الرئاسي 02-183 ، ص05و06

[2] مقال بعنوان" إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، الأربعاء 14 ديسمبر 2016، وكالة الأنباء الجزائرية، على الموقع الالكتروني www.aps.dz/sante.science

•السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية و تطوير تبادل المعلومات و التعاون على المستوى الدولي في مجال اختصاصها.

•تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

•المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام و الاتصال.

•المساهمة في تعيين المعايير القانونية في مجال اختصاص الهيئة [1] .

4- تنظيم الهيئة:

وضع المرسوم الرئاسي لسنة 2020 كل من مجلس التوجيه ومديرية عامة، تحت السلطة المباشرة لرئيس الجمهورية، و يقدمان له عرضا عن نشاطاتهما[2].

مجلس التوجيه : أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة لمجلس التوجيه بموجب المرسوم الرئاسي لسنة 2019 ، غير أنه عدل التشكيلة برئاسة و رئيس الجمهورية و يمكنه أن يفوض مثله ، حيث يتشكل مجلس التوجيه من الوزير المكلف بالعدل ، و الوزير المكلف بالداخلية، الوزير المكلف

[1] المواد 2 و 3 من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53، 8 أكتوبر 2015، ص ص 16-17

[2] المادة 05 من المرسوم الرئاسي 02-183 ،ص06

بالمواصلات السلكية و اللاسلكية و قام المرسوم بإضافة كل من المدير العام للأمن الداخلي و قائد الدرك الوطني و المدير العام للأمن الوطني و ممثل عن رئاسة الجمهورية و ممثل عن وزارة الدفاع الوطني و يعين رئيس الجمهورية ممثلي رئاسة الجمهورية و وزارة الدفاع الوطني .

و أضافت المادة 08 منه أن اجتماع مجلس التوجيه في دورة عادية مرتين في السنة ، بناء على استدعاء من رئيسه ، و يمكنه أن يجتمع في دورة غير عادية ، كلما كان ذلك ضروريا ، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة .

المديرية العامة: يديرها مدير عام، تعيينه أو إنهاء المهام يكون بموجب مرسوم رئاسي.

أسندت للمديرية العامة نفس الصلاحيات المنصوص عليها في مرسوم 2019 ، غير أن الاختلاف يكمن في أن المرسوم الجديد جعل من صلاحيات المديرية العامة مقيدة بموجب موافقة مجلس التوجيه ، على مشروع ميزانية الهيئة و إعداد و تنفيذ برنامج عمل الهيئة ، و وجوب رفع التقرير السنوي لنشاطات الهيئة لمصادقة مجلس التوجيه .

كما أضاف مصطلح " الهوية " و أبقى على نفس الصلاحية المنصوص عليها في المرسوم السابق ، حيث أن من بين صلاحيات المديرية العامة تبادل المعلومات

من مثيلاتها في الخارج بغرض تجميع كل المعطيات المتعلقة بتحديد مكان و هوية مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و التعرف عليهم ، كذلك إعادة عبارة مراقبة أنشطة هياكل الهيئة[1] .

كذلك أعيدت صياغة أسماء المديريات و المصالح التابعة للمديرية العامة، حيث تضم الهيئة[2]:

- **مديرية للمراقبة الوقائية و اليقظة الالكترونية:** حيث أضافت المادة 15 صلاحية اليقظة الالكترونية في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و سبب تغير المصطلح الذي كان في المرسوم الرئاسي لسنة 2019 " مديرية تقنية ".

- **مصلحة الدراسات و التلخيص:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 19 منه.

- **مصلحة التعاون و اليقظة الالكترونية:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 20 منه.

5- سير الهيئة : أضاف المرسوم الرئاسي الأخير المواد من 21 إلى 30 تنظم كيفية سير الهيئة و أهم ما جاء في هذه المواد:

[1] المادة 10 من المرسوم الرئاسي 02-183 ، ص 07

[2] المادة 11 من المرسوم الرئاسي 02-183 ، ص07

– إضافة صلاحية مهمة للهيئة حيث تكلف حصريا بمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في الحين ، و القيام بإجراءات التفتيش و الحجز داخل المنظومة المعلوماتية .

– إمكانية طلب أي وثيقة أو معلومة ضرورية لإنجاز مهامها من أي جهاز أو مؤسسة أو مصلحة.

– إمكانية طلب المساعدة من الوزارات المعنية للأعوان العموميين المختصين في مجال تكنولوجيات الإعلام و الاتصال.

– وجوب المحافظة على السر المهني .

– استعمال الوسائل و التجهيزات الالكترونية أو استيراد أو اقتناء أو حيازة لا يكون إلا من طرف الهيئة في حدود اختصاصها. أو عند الاقتضاء سلطة ضبط الاتصالات السلكية و اللاسلكية ، و المؤسسة العمومية المكلفة بشبكات الاتصالات .

– تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علم الجهات المختصة بأنه يحوز أو يستعمل وسائل و تجهيزات موجهة لمراقبة الاتصالات الالكترونية.

ثانيا : السلطة الوطنية لحماية المعطيات ذات طابع شخصي

1– استحداث المشرع الجزائري بموجب القانون 18–07 سلطة وطنية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي و هي عبارة عن سلطة إدارية مستقلة

تتمتع بالشخصية المعنوية و بالاستقلال المالي و الإداري تضمن عدم انطواء استعمال تكنولوجيات الإعلام و الاتصال على أي أخطار تجاه حقوق الأشخاص و الحريات العامة و الحياة الخاصة . توضع لدى رئيس الجمهورية و ذلك بهدف حماية المعطيات .

2- المهام المسندة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

- تلقي التصريحات المسبقة المتعلقة بمعالجة المعطيات ذات الطابع الشخصي : حيث تضمنت المواد من 13 إلى 16 من القانون كل ما يخص إجراء التصريح الذي يجب أن يودع مسبقا لدى السلطة الوطنية ، و باستقرار نص للمادة 13 من القانون نجد أن طريق تقديم التصريح المسبق يكون بأي شكل من الأشكال ، حيث يمكن تقديمه الكترونيا ، و يسلم وصل إيداع أو يرسل فورا بالطريق الالكتروني في مدة محددة بـ 48 ساعة .

- إخضاع المعالجة لنظام الترخيص: و قد تضمنت المواد من 17 إلى 21 كل ما يخص نظام الترخيص، حيث لابد للسلطة الوطنية إذا تبين لها أن المعالجة محل التصريح تتضمن أخطارا ظاهرة على احترام و حماية الحياة الخاصة و الحريات و الحقوق الأساسية للأشخاص. كذلك تمنح السلطة الوطنية الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا شروط محددة قانونا . كما نقوم بنشر التراخيص الممنوحة و الآراء المدلى بها في السجل الوطني.

– الإعلام و تقديم الاستشارات و الاقتراحات اللازمة : حيث تسهر السلطة على إعلام الأشخاص المعنيين و المسؤولين عن المعالجة بحقوقهم و واجباتهم . و تسهر على تقديم الاستشارات للأشخاص و الكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي ، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة . كما تختص بتقديم أي اقتراح من شأنه تبسيط و تحسين الإطار التشريعي و التنظيمي ، لمعالجة هذه المعطيات.

– إصدار أوامر: حيث تأمر بالتعييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، كما تأمر بإغلاق معطيات أو سحبها أو إتلافها.

– تطوير علاقات التعاون مع السلطة الأجنبية المماثلة : و يشترط في ذلك مراعاة مبدأ المعاملة بالمثل

– وضع معايير و قواعد السلوك و الأخلاقيات التي تخضع لها معالجة المعطيات، بالإضافة إلى إصدار عقوبات إدارية وفقا لأحكام المادة 46.

– تختص بالإعلام الفوري للنائب العام المختص ، في حالة معاينة وقائع تحتمل الوصف الجزائي .

– إعداد تقرير سنوي: حيث تقوم السلطة الوطنية بإعداد التقرير السنوي حول نشاطاتها، و ترفعه إلى رئيس الجمهورية.

لقد اشترط القانون 18-07 الموافقة المسبقة من الشخص الطبيعي الذي تكون المعطيات ذات الطابع الشخصي المتعلقة به محل معالجة ، و له الحق في التراجع عم موافقته في أي وقت ، كما لا يمكن اطلاع الغير على المعطيات محل المعالجة إلا بع الموافقة المسبقة منه ، و إذا كان عديم أو ناقص الأهلية تكون الموافقة وفق القواعد المقررة قانونا[1].

و لا يمكن القيام بالمعالجة للمعطيات ذات الطابع الشخصي المتعلقة بالطفل إلا بعد حصول موافقة من ممثله الشرعي ، أو بترخيص من القاضي المختص[2].

و يخرج عن مجال تطبيق هذا القانون كل من المعطيات ذات الطابع الشخصي: سواء المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، شرط عدم إحالتها للغير أو نشرها أو المحصل عليها و المعالجة لمصلحة الدفاع و الأمن الوطنيين. أو المعالجة لأغراض الوقاية من الجرائم و متابعة مرتكبيها و قمعها كذلك المحتوية في قواعد البيانات القضائية التي تخضع إلى النص الذي أحدثت بموجبه و إلى أحكام المادة 10 من القانون 18-07 .و تجدر الإشارة أنه لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم و العقوبات و تدابير الأمن، إلا من قبل السلطة القضائية و السلطة العمومية و الأشخاص المعنوية المسيرة لمصلحة عمومية، و مساعدي العدالة في إطار اختصاصاتهم القانونية. كما يجب

[1] المادة 07 من القانون 18-07

[2] المادة 08 من القانون 18-07

تحديد المسؤول عن المعالجة و الغاية منها و الأشخاص المعنيين بها ، و الغير الذي يمكنه الاطلاع على المعلومات و مصدرها و الإجراءات الواجب اتخاذها لضمان سلامة المعالجة[1] .

ثالثا : وكالة أمن الأنظمة المعلوماتية

استحداث منظومة وطنية لأمن الأنظمة المعلوماتية توضع لدى وزارة الدفاع ، و التي تتكون من المجلس الوطني لأمن الأنظمة المعلوماتية التي من بين مهامها إجراء التحقيقات الرقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية[2].

و تعتبر وكالة أمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلال المالي، يقع مقرها في مدينة الجزائر.

سير الوكالة :

تدير الوكالة لجنة توجيه و تزود بلجنة علمية ، و تتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية و مديريات و مصالح تقنية و إدارية موضوعة تحت سلطة المدير العام الذي يسير بدوره الوكالة و يسهر على تنسيق تنفيذ

[1] المادة 10 من القانون 18-07

[2] مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 ،يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04 الصادر فيفي 26 جانفي 2020 ص05

الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية و تنفيذ المخططات و البرامج المسطرة من قبل لجنة التوجيه.

المطلب الثاني: الوحدات المكلفة بالتحقيق في الجرائم الإلكترونية

إن الأجهزة التابعة للأمن و الدرك الوطني تسهر على المواجهة التنظيمية للجرائم الإلكترونية بشكل عمودي كل في مجال اختصاصه.

الفرع الأول: وحدات الدرك الوطني

تلعب مؤسسة الدرك الوطني دور فعال في مواجهة الجرائم المعلوماتية و تطويق نطاق الجرائم المعلوماتية من خلال استحداثها لتقنيات خاصة، و إنشاء و حدات خاصة.

أولا : المعهد الوطني للأدلة الجنائية و علم الإجرام INCC /GN

هو جهاز تابع للدرك الوطني أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183[1] يتكون من 11 دائرة متخصصة في عدة مجالات تضمن الخبرة و التكوين و التعليم و تقديم المساعدات التقنية و البحوث و الدراسات و التحاليل في عالم الإجرام.

[1] مرسوم رئاسي 04-183 المؤرخ في 2004/06/26 يتضمن احداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني و تحديد قانونه الأساسي ، الجريدة الرسمية عدد 41 الصادرة في 2004/06/27 ص 18

حيث تكلف دائرة الإعلام الآلي و الإلكترونيك بمعالجة تحليل و تقديم كل دليل إلكتروني و تماثلي للعدالة ، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تعيين المعارف، التقنيات و الطرق المستعملة في مختلف الخبرات العلمية.

و لإنجاز المهام المنوطة بها تنقسم الدائرة إلى ثلاثة مخابر و كل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات و ضمان نزاهة و شرعية الدليل:

1- مخبر الإعلام الآلي : يختص بتحليل و معالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش) ، كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية.

2-مخبر الفيديو: يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، كما يعمل على تحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات، و مقارنة الأوجه شرعية الصور و الفيديو.

3- مخبر الصوت: يختص بمعرفة و تحديد المتكلم، و تحديد شرعية التسجيلات الصوتية، و يعمل على تحسين نوعية إشارة الصوت بنزع التشويش و تعديل السرعة[1].

1عرض مقدم من طرف : هواري عياش ، المعهد الوطني للأدلة الجنائية ، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر

ثانيا: مركز الوقاية من جرائم المعلوماتية و مكافحتها CPLCIC/GN

و هو مركز تابع لأجهزة الدرك الوطني بدأ عمله منذ سنة 2004، و الذي يكلف بمهمتين رئيسيتين:

المهمة الأولى: قبلية تتعلق بالتدقيق و الوقاية.

المهمة الثانية : بعدية تتعلق بردع الجرائم الماسة بالطفولة .

و حديثا أنشأ مكتب خاص بحماية الأحداث عبر الانترنت بغرض تقديم الدعم التقني للوحدات الإقليمية في التحري و جمع الأدلة الجنائية.

في 2017 عالج المركز 100 جريمة تتعلق بالأطفال و المراهقين ، و 20 جريمة مالية ، حيث أن الجرائم المالية مازلت محدودة لأن التجارة الإلكترونية و الدفع الإلكتروني مازال في بدايته ، و يتوقع زيادة هذا النوع من الجرائم خلال السنوات المقبلة بعد تعميم التجارة الإلكترونية ، مما يتطلب الاستعداد لمواجهة من الجرائم المتعلقة بالتجارة الإلكترونية عن طريق إنشاء مكتب خاص بالجريمة الاقتصادية و مختلف تحديات الفضاء السبراني ، و هذا يستدعي إطار قانوني متكامل من الجوانب العلمية و التقنية و ذلك عن طريق تكوين مختصين في الجرائم المعلوماتية في كل مجالاتها[1].

[1] مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة :95 بالمائة من الجرائم الالكترونية تم حلها بنجاح، موقع الاذاعة الجزائرية، 2019/05/25 على الساعة 15:34

ثالثا : المصلحة المركزية للتحريات الجنائية SCIC/GN

تعد المصلحة المركزية للتحريات الجنائية مصلحة تابعة لأجهزة الدرك الوطني تقوم بالتحقيق التقني و العملي ، و يبقى إجراء التحقيق في الجرائم الإلكترونية ليس بالأمر السهل ، باعتبار أن هذا النوع من الجرائم المعاصرة لا يعترف بحدود المكان و الزمان ، كما أن إجراءات جمع الأدلة و تحديد هوية مرتكبي هذه الجرائم أو المشبه بهم تبقى معقدة في ظل التكنولوجيات الحديثة .

و جدير بالذكر أن المحققين على مستوى المحلي من فصائل الأبحاث التي تشمل محققي جرائم الإعلام الآلي، يختصون بالتحقيق و مقاربة تقنية أولية[1]. و هو كذلك بالنسبة لخلايا الشرطة العلمية و التقنية على المستوى المحلي.

الفرع الثاني: وحدات الأمن الوطني

تتولى المديرية العامة للأمن الوطني التحقيق في الجرائم الإلكترونية عن طريق قسمين يشمل القسم الأول المخابر ، و يشمل القسم الثاني الفرق ، و في سبيل نجاعة التحقيق لها دور فعال في مواجهة الجرائم الإلكترونية.

[1] عرض مقدم من طرف : عز الدين ، المعهد الوطني للأدلة الجنائية ، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر

أولا: المخابر

يوجد مخبر مركزي للشرطة العلمية في الجزائر العاصمة، و مخبر جهوي في قسنطينة و وهران و قد استحدثت أقسام متخصصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة إلكترونية قصد استخراج و تتبع ما من شأنه أن يفيد في التحقيق و يساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع، و أهم الأجهزة المستغلة من طرف هذه الأقسام:

1. أدوات التخزين الرقمية (أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة).
2. أجهزة الكمبيوتر و لواحقها[1].

و حسب المعطيات الإحصائية لدائرة الأدلة الرقمية و الآثار التكنولوجية التابعة لمخبر الأدلة الجنائية بقسنطينة ووهران [2]، فقد شهد سنة 2014 ما يقارب 250 قضية محل تحقيق، أبرزها قضيتين تتعلق بالإنابة القضائية الدولية عن طريق مكتب الإنتربول أقدم فيهما شابين من ولاية قسنطينة بالاعتداء و تعطيل نظام معلوماتي خاص بموقع وزارة الخارجية الكويتية ، و القيام بالاحتيال الالكتروني على أهداف بالولايات المتحدة الأمريكية ، و سجل الثلاثي الأول سنة 2005، 60 قضية تتعلق أغلبها بسوء استخدام

[1] حملاوي عبد الرحمان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر ص8

2 وتجدر الإشارة أن هناك مخابر أخرء قيد الانجاز في ورقلة، بشار، تمنراست

مواقع التواصل الاجتماعي من خلال قضايا المساس بالأشخاص في صورة الابتزاز، القذف و التشهير ...[1]

ثانيا : وجود فرقة على مستوى كل أمن ولاية

في سبيل ضمان فاعلية التحقيق في مواجهة الجرائم المعلوماتية تم إنشاء ما يعرف بالمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، و هي مصلحة تابعة لمديرية الشرطة القضائية مقرها على مستوى الجزائر العاصمة، ثم أنشأت خلايا تابعة للفرق الاقتصادية و المالية على مستوى أمن الولايات، تشمل خلية مكافحة الجرائم الإلكترونية ، ثم مع تطور الجرائم و اعتماد Modem و 3G ، تم ترقية الخلية لتصبح فرقة في حد ذاتها ، حيث أصبحت مستقلة و تابعة للفرق الولائية للشرطة القضائية، و توجد فرق على مستوى 58 ولاية.

و كمثال عن بعض الإحصائيات على مستوى الفرق ، كانت القضايا المنجزة من خلال فرقة مكافحة الجرائم المعلوماتية في أمن ولاية قالمة تقدر بـ 153 قضية منجزة خلال الثلاث سنوات الأخيرة و الموضحة في الجدول التالي :

1 حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية،جامعة باتنة 01،2016 ،ص .181

السنة	عدد القضايا المنجزة	عدد المتورطين	
		الراشدين	الأحداث
2018	40	40	00
2019	55	56	05
2020 إلى غاية نوفمبر	58	67	01
المجموع	153	163	06

جدول يوضح مثالا عن الإحصائيات المتعلقة بالجرائم الإلكترونية خلال السنوات الأخيرة

(مقدم من طرف أمن باتنة)

و ما يلاحظ من خلال ذلك أن القضايا في تزايد من عام لآخر ، خاصة في السنوات الأخيرة ، كما تختلف الفئات العمرية للمتورطين في الجريمة بين بالغين و أحداث، و لعل السبب في ارتفاع معدل الجريمة المعلوماتية يرجع إلى عدة عوامل ، من بينها: الانفتاح على العالم الافتراضي ، إغفال الأولياء عن مراقبة الطفل القصر، التأثيرات السلبية لمواقع التواصل الاجتماعي، الانفلات الأخلاقي و غيرها من العوامل الاقتصادية و الاجتماعية.

و أغلب القضايا المعالجة في الفرقة تتعلق بمواقع التواصل الاجتماعي خاصة "الفايسبوك "، في قضايا المساس بحرمة الحياة الخاصة للأشخاص، و السب و الشتم و التهديد، و قضايا النصب و الاحتيال[1].

ثالثا : دور المديرية العامة للأمن الوطني في مواجهة الجرائم الالكترونية

للمديرية العامة للأمن الوطني دور أساسي في مواجهة الجرائم المعلوماتية و يتجلى ذلك من خلال دورها الوقائي و الردعي و التحسيسي.

حيث يتجلى الدور الوقائي من خلال عقد دورات افتراضية على مستوى شبكات المعلومات عموما و مواقع التواصل الاجتماعي خصوصا.

أما دورها الردعي يعتبر امتدادا لدورها الوقائي في حالة الإخلال بالنظام العام، أو في حالة منشورات هادمة تمس النظام العام كعرض أهزة حساسة أو ممنوعات للبيع عبر مواقع التواصل الاجتماعي، حيث يتم التدخل و تحديد هوية صاحب الحساب و اتخاذ الإجراءات القانونية في هذا الشأن مع انجاز ملف قضائي ضده.

زيادة على ذلك للمديرية العامة دور تحسيسي كالتنقل لمختلف المؤسسات التربوية و تنظيم نشاطات التحسيس حول سوء استعمال شبكات التواصل الاجتماعي أو سوء استخدام الانترنت ، و حماية الأطفال القصر من مخاطر الانترنت.

[1] وهو ما تم تسجيله في إطار زيارة ميدانية للفرقة المختصة بمكافحة الجرائم المعلوماتية على مستوى أمن ولاية قالمة

كما تعمل المديرية على تلقي الشكاوي التي قد تكون مباشرة، أو غير مباشرة عن طريق إرسال النيابة العامة للقضية للتحقيق فيها.

أما على المستوى الدولي لم تغفل مديرية الأمن الوطني استغلال عضويتها الفعالة في الانتربول الذي يتيح لها مجالات للتبادل المعلوماتي و تسهيل الإجراءات القضائية المتعلقة بتسليم المجرمين، و كذا مباشرة الإنابة القضائية الدولية و نشر أوامر القبض للمبحوث عنهم دوليا[1].

و من خلال الهيكل التنظيمي للمكتب المركزي الوطني " انتربول الجزائر " يوجد مكتب الربط للانتربول لـ 58 ولاية، و استخدام قاعدة المعطيات 124/7 ، حيث يعمل جهاز 124/7 على تحديد المعلومات اللازمة حول الأشخاص و المركبات موضوع التحقيق.

[1] حملاوي عبد الرحمان، مرجع سابق، ص 09.

خلاصة الفصل الأول :من خلال التعرض إلى الإطار المفاهيمي لخصوصية الجريمة الإلكترونية وماهيتها يتضح لنا أن لهذا النمط من الجرائم طبيعة خاصة ومتميزة إذ بمجرد ملامسة الجاني للحاسب الآلي بغير منطق ووعي قد ترتكب أخطر الجرائم في بضعة ثواني دون التقاء الجاني والمجني عليه وهذا ما استدعى إنشاء أجهزة وهيئات لمكافحتها وهو الأمر الذي دفعنا للتساؤل حول إجراءات عمل هاته الهيئات و الصعوبات التي تواجهها و ما هي حلولها و هذا ما سنتطرق إليه في الفصل الثاني.

الفصل الثاني: إجراءات التحقيق في الإلكترونية

صعوباتها و الحلول المقترحة لذلك،

لم تكتفي التشريعات الحديثة بالحماية الموضوعية للحاسب الآلي و ذلك نظرا لخطورتها فهي تعتبر في الحقيقة عن ذبذبات إلكترونية افتراضية يسهل على الجاني القيام بعمل إجرامي عليها دون ترك آثار أو استغراقه لأداء هذا العمل وقتا طويلا وهو ما جعلها صعبة الاكتشاف والإثبات.مما أدي ذلك إلي ظهور مشكلات إجرائية في هذا النطاق ؛ حيث إن المحقق او ضابط شرطية قضائية أو القاضي نفسه في حيرة أمام هذه الجرائم نظرا لقصور التشريع الإجرائي خاصة وان هذه الجرائم حديثة ولا يمكن تطبيق النصوص التقليدية من جهة وعدم القدرة الكافية والفنية لرجال القانون لاكتسابها و من هنا بعد ما تطرقنا في الفصل الأول إلى التعريف بالجريمة الالكترونية و أجهزة التحقيق الجنائي في الجرائم الإلكترونية في مواجهتها وجب علينا الانتقال إلى فصل جديد نمس فيه أبرز إجراءات التحقيق الجنائي حيث خصصنا المبحث الأول لنتناول فيه الإجراءات و صعوبة التحقيق و في المبحث الثاني تطرقنا فيه الحلول القضائية في التحقيق.

المبحث الأول: إجراءات التحقيق في الجرائم الإلكترونية و الصعوبات التي تواجهها

التحقيق الجنائي في الجرائم الإلكترونية هو نشاط قانوني يتعلق بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الاستدلالات التي يتطلبها التحقيق والدعوى الجنائية ، فهو الضبط القضائي للجاني والدليل على إدانته أو براءته ، ودور المحقق يتلخص في تلقي البلاغ وجمع الاستدلالات ضد مرتكب الجريمة لجهات التحقيق القضائي بأدلة الإدانة . فإجراءات التحقيق القضائي تمر بثلاث مراحل هي : .

1- مرحلة جمع الاستدلالات بواسطة مأموري الضبطية القضائية المختصين بالبحث في الجرائم الالكترونية.

2- مرحلة التحقيق الابتدائي بمعرفة النيابة العامة أو قاضي التحقيق لتحريك الدعوى العمومية أو حفظ التحقيقات لعدم كفاية الأدلة .

3- مرحلة التحقيق النهائي والتي تكون خلال مرحلة المحاكمة[1].

إلا أن إجراءات التحقيق تعرف في بعض الأحيان معوقات وصعوبات نظرا لوقوع الجريمة الإلكترونية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم (serveurوالشبكات بمختلف أنواعها ، مما يجعل عملية الحصول على الدليل الإلكتروني ليس بالهين ، الأمر الذي يترك معه أجهزة البحث والتحري ترفع تحدي في تطبيق القواعد الإجرائية لأجل استخلاص الدليل ، وعليه أستعرض في المطلب الأول

[1] مصطفى محمد موسى – التحقيق الجنائي في الجرائم الإلكترونية – مطابع الشرطة – القاهرة – الطبعة الأولى 2009 ص 165

ماهية التحقيق في الجرائم الإلكترونية ، وفي المطلب الثاني الأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية .

المطلب الأول : ماهية التحقيق في الجريمة الإلكترونية

إن التحقيق كما يدل اسمه عليه هو استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة . وكما تم التنويه عنه أن الدعوى الجزائية تمر بمرحلتين . مرحلة التحقيق ومرحلة المحاكمة ، وتمر عملية التحقيق بمرحلتين أيضا ، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي . فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي ، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[1].

الفرع الأول : تعريف التحقيق و المحقق وخصائص كل منهما

أ- **تعريف التحقيق** :تعريف التحقيق في الجريمة الإلكترونية لا يختلف عنه في الجرائم الأخرى ،وعليه أتطرق إلى تعريفه لغة وقانونا ، ثم إلى تعريف المحقق الذي يشرف على إجراءات التحقيق .

أولا : لغة : التحقيق مأخوذ من حقق يحقق تحقيقا ، حقق الظن بالله صدقه ، الأمر أحكمه – مع فلان – في قضيته : أخذ رأيه فيها

1 سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجستير ، تخصص علوم جنائية ، جامعة الحاج لخضر باتنة ، السنة الجامعية 2012 – 2013 ص 102

ثانيا : تعريف التحقيق اصطلاحا : عرف التحقيق بمعناه العام أنه : اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها ،وعرف التحقيق على أنه مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة ، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا ، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة [1] وكذلك عرف التحقيق بأنه " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه أو عدم لزومها . وهناك نوعان من قسم التحقيق إلى[2]:

1- **التحقيق الجنائي العملي :** يقصد به جميع إجراءات التحقيق التي يباشرها المحقق الجنائي عند وقوع جريمة أو حادث ، توصلا إلى معرفة الحقيقة وقواعد أساسها التجارب العملية التي وصل إليها المحققون في تحقيق القضايا الهامة .

---

1 – عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي . مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، 2007 ص 2

2 –غسان مدحت الخبري ، الطب العدلي والتحري الجنائي ، دار الراية ، المملكة الأردنية ، ط 1 ، 2013 ، ص 17

2- **التحقيق الجنائي الفني** : ويرتكز على الأبحاث العلمية والتجارب الفنية التي يمكن تطبيقها لاكتشاف حقيقة الحوادث الجنائية والاهتداء إلى مرتكبيها وقد عرف أيضا بأنه " التحري والتدقيق في البحث تلمسا لمعرفة الجاني في جناية ارتكبت أو شرع في ارتكابها

ب- تعريف المحقق وخصائصه الفنية

أولا : تعريف المحقق

ذهب جانب من الفقه إلى تعريف المحقق بأنه : كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية ، وتحقيقها ويسهم بدوره في كشف غموضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة [1]

كما عرف البعض المحقق أو الباحث الجنائي بأنه " الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها ، وضبط مرتكبها والأدوات التي استعملت فيها " [2]

1 خالد ممدوح إبراهيم ، عن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الإسكندرية ، ط 1 ، 2009 ص 86

2 غسان مدحت الخيري ، الطب العدلي والتحري الجنائي ، دار الراية ، المملكة الأردنية ، ط 1 ، 2013 ، ص1

وعرف المحقق بأنه ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى علمه من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة[1]

أما المشرع الجزائري فقد وضع تعريفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي [2]

إن الجريمة الإلكترونية تنبع من التطور الفني الإلكتروني وهذا للاستخدام السيئ لبعض العاملين على أجهزة الحاسوب ، مما أضاف أعباء جديدة على أجهزة التحقيق ، لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها المحققون ولم يتعودوا عليها ، مما أدى إلى ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال ، وعليه فالتركيز هنا سوف ينصب على الخصائص الفنية التي تتسم بالحداثة والناتجة عن التطور الإنساني في مجال تقنية المعلومات والأنظمة الإلكترونية .

[1] خالد ممدوح إبراهيم ، المرجع السابق ص 86

2 الأمر رقم 56- 155 المؤرخ في 18 صفر عام 1385 الموافق 8 يونيو 1956 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم 5

ثانيا : الخصائص الفنية للمحقق :

ويمكن ذكر الخصائص الفنية للمحقق كما يلي [1]:

أ – أن يكون هدف المحقق دائما هو الوصول إلى الحقيقة : الشرط المتطلب لنجاح المحقق في أداء رسالته إيمانه بها ، وأن يكون هدفه الحقيقي الوصول إلى الحقيقة ، لا العدول عنها ، وهذا ليس بالأمر الهين ذلك أن أساس العدالة من صفات الله تعالى فإن أمن بها المحقق حينها لن يخل بواجباته مهما لاقى من الصعوبات ، وعلى المحقق أن يضل مدركا بأنه في حالة صراع دائم بينه وبين المجرم الإلكتروني فالأول ينشد للحقيقة والثاني يجتهد في تضليل العدالة وطمس الحقائق والأدلة .

ب– أن يكون لدى المحقق موهبة فن التحقيق : إن التحقيق الفني هو إبداع ، والتمكن من القدرة على التحليل ورفع الستار عن الحقيقة والغموض عن أي أمر ، أو أي قضية كانت .

أما فيما يتعلق بفن التحقيق في الجريمة الإلكترونية ليس قدرة المحقق على استجلاء مدى توافر أركان الجريمة المعروضة وعناصرها ، إنما هو قدرته أيضا على مناقشة الشهود لاستجلاء أقوالهم مما يكون قد شابها غموض ، ففي التحقيق في الجريمة الإلكترونية . لا يجب أن يكون المحقق مجرد آلة ميكانيكية تسجل فقط الأسئلة والأجوبة بل عليه توجيه الأسئلة للمتهم والشهود .

1 بختي فاطمة الزهراء – إجراءات التحقيق في الجريمة الإلكترونية – مذكرة لنيل شهادة الماستر– جامعة محمد بوضياف المسيلة ، السنة الجامعية 2013 – 2014 ص 43

ج – أن يكون المحقق سريع التصرف في إجراءات التحقيق : إن سرعة إنجاز التحقيق تحافظ على أدلة الجريمة وآثارها ، دون أن تمس أو تمحى ، ويمنع من ضياعها ، فالتأخير في إجراءات التحقيق قد يترتب عليه تعريض أدلة الجريمة ومعالمها لخطر الضياع ، فالسرعة في إجراء التحقيق الجنائي من الواجبات الضرورية لمساس ذلك بسلطة الدولة.

وكذا حقوق الناس وحرياتهم ، فسرعة التحقيق تؤدي إلى كشف حقيقة الجريمة دون أن يتمكن الجناة من طمس آثارها وأدلتها .

د– قوة الملاحظة وسرعة البديهة : ويقصد بها المعرفة الدقيقة لحقيقة أمر أدركته أحد الحواس عما يحيط به من ظروف ، كما يجب عليه معرفة الجوانب الفنية والتقنية لأجهزة الحاسب والإنترنيت التي تتعلق بالجريمة .

و– حياد المحقق أثناء إجراء التحقيق : يعتبر من أهم خصائص التحقيق ، فيجب أن يقوم بالتحقيق شخص غير متحيز يعنى بما يفيد الدفاع عنايته بأدلة الاتهام ، ولا تتحقق الحيدة التامة للمحقق إلا إذا استقلت سلطة التحقيق عن كل من سلطة الاتهام من ناحية وسلطة الحكم من ناحية أخرى ، فلا يجوز للنيابة المنوط بها توجيه الاتهام أن تحقق بعدل.

ي– المساواة في معاملة الحضور : القاعدة العامة بالنسبة للمحقق يلتزم بها هي المساواة في المعاملة ، حتى بالنسبة للمتهم الماثل أمامه فينبغي على المحقق المساواة بين المتهم والمجني عليه عند المثول أمامه .

هـ- الهدوء وضبط النفس : يوجد في الحياة كثيرا من ذوي النشاط الإجرامي يعملون على استفزاز المحقق لتشتيت أفكاره أو يدفعه للتعدي عليهم حتى يمكنهم تبرير اعتراضهم بارتكاب الواقعة وإبطالها بادعاء أنه وليد إكراه ، لذا يتوجب على المحقق بالإضافة إلى الهدوء إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية ، التي تدل على وقوع الجريمة الإلكترونية بتحريها في الأقراص المعدة لذلك ومنع حذفها .

كما يجب أن تتوافر في المحقق بعض الأمور ليقوم بعمله على أحسن وجه [1]:

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والإنترنت والتي تتعلق بالجريمة المرتكبة .

- وصول الإخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والإنترنت من الفنيين الذين يعملون على هذه الأجهزة.

- تشكيل فريق تحقيق فني ، وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش على مسرح الجريمة.

- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة ، وتخزينها في الأقراص المعدة لذلك ومنع حذفها.

[1] خالد عباد الحلبي ن اجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت –دار الثقافة للنشر والتوزيع عمان ط1 2011 ص 183و184

– البحث عن الأدوات المستخدمة في ارتكاب الجريمة ، وطرق الدخول على البرامج المحزنة ، وكيفية الحصول على الأرقام السرية والشفرات الفنية التي تمكنهم من الدخول إلى الحاسوب.

– وضع خطة عمل مع جميع أعضاء فريق التحقيق ، والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها .

ج- خصائص التحقيق في الجريمة الإلكترونية

الجرائم التي ترتكب بواسطة الحاسوب تنشأ في الخفاء وينصب الاعتداء فيا على معطيات الحاسوب المحزنة والمعلومات المنقولة غير نظم وشبكات المعلومات ، وعليه فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق ، وقبل التطرق إلى خصائص التحقيق في الجريمة الإلكترونية تجدر الإشارة لخصائص التحقيق عامة وهي كالأتي :

1- **السرية** : يقصد بسرية الإجراءات عدم الاطلاع عليا ، ويقصد بسرية التحقيق عدم علانيتها بالنسبة للغير ، وهم غير أطراف الدعوى العمومية فسرية التحقيق إذا تعني إجراء التحقيق في جو من الكتمان بالنسبة للجمهور [1]حيث أن حضور إجراءات التحقيق غير مسموح به للجمهور وذلك لحماية المتهم من الشهر الذي قد يصبه بسبب التحقيق الذي قد

[1] عبد الله أوهايبة ، شرح قانون الاجراءات الجزائية الجزائري، دار هومة الجزائر ط2 2011 ص 336

ينتهي بإصدار قرار أن لا وجه لإقامة الدعوى ولحماية الأدلة من العبث[1].

2- **التدوين** :لقد أوجب المشرع المختص بالتحقيق اصطحاب كاتب معه يرافقه في جميع إجراءاته و يدون المحاضر و يصادقان معا على جميع صفحات المحاضر بحيث يجري تدوين جميع إجراءات التحقيق و إثباتها كتابة في محضر رسمي يعد لذلك حتى يكون حجة في الإثبات.

الفرع الثاني : الإجراءات التي يباشرها قاضي التحقيق في الجريمة المعلوماتية .

لقد خص المشرع الجزائري قاضي التحقيق بسلطات واختصاصات واسعة في سبيل تحقيق الهدف من إسناد مهمة التحقيق إلى قاضي تحقيق مستقل عن جهة المتابعة وجهة الحكم ، وقد خولته المادة 68 ق.إ.ج سلطة اتخاذ أي إجراء يراه ضروريا للكشف عن الحقيقة ، كاستجواب المتهمين ، وسماع الشهود والتفتيش وإجراء الخبرات وغيرها من الاختصاصات .

وقد اتجهت ارادة المشرع إلى منحه سلطات جديدة لم يكن يتمتع بها في سبيل مواجهة الأنواع الجديدة من الجرائم المعلوماتية . وهو ما سنطرق إليه من خلال مايلي:

أولا : المعاينة في الجريمة المعلوماتية :

مع تزايد استخدام الكمبيوتر والإنترنت والشبكات الداخلية والخارجية تزايدت نسبة الجريمة المرتكبة باستخدام هذه التقنيات الجديدة ، سواء كانت هذه الجريمة تمت عبر

[1] بختي فاطمة مرجع سابق ص42

الكمبيوتر ، أم الجريمة تمت على الكمبيوتر .حيث أصبح قضاة التحقيق عاجزون على ضبط واستخلاص دليل إدانة في المجرم المعلوماتي .

ويتطلب مسرح الجريمة سواء كان ماديا أو معنويا (الكتروني) إجراءات خاصة تختلف عن الإجراءات التي سبق وقد عرضناها في مرحلة البحث والتحري عن الجريمة المعلوماتية وذلك باختلاف الجهة القضائية في هذه المرحلة ألا وهو قاضي التحقيق [1].

01 : الانتقال للمعاينة (انتقال قاضي التحقيق للمعاينة)

إن من أعمال قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من آثار وسماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم من المتهم أو من أطراف أخرى وهو ما قرره المشرع الجزائري في المادة 79 ق.ا.ج.ج .[2]

وتتم المعاينة في الجريمة المعلوماتية المرتكبة عبر الإنترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني .[3]

1 محمد حزيط . مذكرات في قانون الاجراءات الجزائية الجزائري ، مرجع سابق ، ص 59 .

2 انظر المادة 79 ق.إ.ج.ج

3 – عبد العالي الديري , محمد صادق اسماعيل . الجرائم الإلكترونية . مرجع سابق ، ص 264 .

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة .

وحتى يستطيع قاضي التحقيق أن ينتقل إلى عالم الفضاء الالكتروني لمعاينته ، عدة طرق تتمثل في :

- الانتقال إلى العالم الافتراضي من المكتب بالمحكمة من خلال الكمبيوتر الخاص به.
- اللجوء إلى مقهى الإنترنت . [1]
- يجوز له اللجوء إلى مقر عمل مزود خدمة الإنترنت server internet[2] . providerالذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة .

كما يستطيع قاضي التحقيق أيضا الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص .[3]

وبالتالي يتضح مما سبق أن هناك عوائق ومشكلة أمام القاضي التحقيق من خلال الانتقال إلى العالم الافتراضي ، حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة .[4]

---

1 خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية . مرجع سابق ، ص 156.

[2] يقصد مزود خدمة الإنترنت : هي الشركة التي توفر لعملائها إمكانية الوصول إلى الإنترنت

[3] – خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية . مرجع سابق ، ص 158

[4] – خالد عياد الحلبي ، إجراءات البحث والتحقيق في جرائم الكمبيوتر والانترنت . مرجع سابق ، 155 .

02 : الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة المعلوماتية :

يجب على المحقق الجنائي (قاضي التحقيق) قبل الانتقال إلى معاينة مسرح الجريمة المعلوماتي إتباع الخطوات التالية :

- توفير معلومات مسبقة عن مكان الجريمة ، ومالك المكان ، نوع وعدة أجهزة الكمبيوتر .
- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل .
- قطع التيار الكهربائي عن موقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شأنه التأثير على أو محو آثار الجريمة .
- إعداد فريق بحث من المختصين والفنيين [1].

03 : شروط صحة معاينة مسرح الجريمة :

حتى تعطى المعاينة ثمارها للكشف عن الغموض والتوصل إلى الجاني لابد أن يراعي قاضي التحقيق ما يلي :

1- سرعة الانتقال إلى مكان الجريمة : فور تلقي المحقق أو قاضي التحقيق البلاغ عن وقوع الجريمة

[1] نبيلة هروال ، الجوانب الإجرائية لجرائم الانترنت ، مرجع سابق ، ص 45.

من الجرائم المعلوماتية والتأكد من صحة الواقعة ، عليه أن ينتقل إلى مكانها ، وذلك ضمانا لعدم التغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه ، والحصول على شهادة الشهود .[1]

2- السيطرة على مكان وقوع الجريمة : بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة

من أجل معاينتها لابد من أن يتبع مجموعة من الإجراءات التالية :

- منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي تم العثور عليها في المسرح .
- التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة .
- التحفظ على كل ما له علاقة بالحادث من أشياء وأشخاص.
- إخطار الخبراء لرفع الآثار والبصمات [2].

ثانيا : التفتيش في الجريمة المعلوماتية : خولت المواد من 79 إلى 81 ق.ا.ج.ج لقاضي التحقيق الاختصاص ، الانتقال إلى منازل المتهمين أو المشتبه فيهم

1 على عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، ط 1 ، دار الجامعة الجديدة للطباعة والنشر : بيروت ، 1999 ، ص 85

[2] خالد ممدوح إبراهيم ، أن التحقيق الجنائي في رائم الالكترونية مرجع سابق ، ص 159 .

أو الذين بحوزتهم أشياء لها علاقة بالجريمة لتفتيشها والحصول على الأدوات المستعملة في الجريمة . [1]

وبالتالي نجد أن جميع الإجراءات الخاصة بالتفتيش في الجريمة المعلوماتية في مرحلة جمع الاستدلالات هي نفسها الإجراءات في مرحلة التحقيق القضائي مع بعض الاختلافات البسيطة المتعلقة بجهاز التحقيق(قاضي التحقيق) .

وحتى يكون التفتيش الذي يقوم به قاضي التحقيق سواء بنفسه (أو بواسطة ضابط الشرطة القضائية) لابد من احترام مجموعة من القيود والشروط الآتية بيانها : [2]

- وقوع الجريمة فعلا وان يتحصل على فائدة من وراء التفتيش من أجل كشف الحقيقة.
- أن يكون هناك اهتمام قائم ضد شخص معين من أجل القيام بعملية التفتيش.
- أن تكون الواقعة المرتكبة جناية أو جنحة .
- أن يكون المنزل أو المحل المراد تفتيشه معروفا ومحددا [3].

[1] أحمد شوقي الشلفاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري ، ص 240

[2] محمد حزيط . مذكرات في قانون الإجراءات الجزائية الجزائري مرجع سابق ، ص 118

[3] عبده جميل غصوب ، الوجيز في قانون الإجراءات الجزائية . ط 1 ، المؤسسة الجامعية للنشر والتوزيع : بيروت . 2011 ، ص 298

- لابد أن يتم التفتيش من قبل قاضي التحقيق وذلك بعد إخطار وكيل الجمهورية الذي يمكن مرافقته حيث يكون مصحوبا بكاتب التحقيق .

فإذا حصل التفتيش في منزل المتهم أو مسكن المتهم أو مسكن شخص آخر يشتبه أن يحوز أشياء لها علاقة بالجريمة فعلى قاضي التحقيق أن يقوم بهذه العملية بحضور المتهم أو صاحب المسكن فإن تعذر حضوره أو كان هاربا يتعين على قاضي التحقيق إحضار شاهدين لا يمتان بصلة للمتهم وذلك طبقا للمادة 82 ، 80 ق.ا.ج.ج [1](من الساعة الخامسة صباحا إلى الساعة الثامنة ليلا)[2] وغير أن قاضي التحقيق خرج عن القاعدة العامة في ميعاد التفتيش في الجرائم المعلوماتية حيث يجوز له القيام بعملية التفتيش ليلا أو نهارا طبقا لنص المادة 47 فقرة 4 ق. ا. ج . ج[3] .

ثالثا: الاستجواب والشهادة وضبط الأدلة في الجريمة المعلوماتية :

يقوم قاضي التحقيق في مجال الكشف والبحث والتحري عن الجريمة المعلوماتية وكشف الغموض عنها والقبض على فاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه ، ومن بينها :

- استجواب المتهم .
- سماع شهود (شاهد الكتروني) .
- ضبط الدليل الالكتروني .

---

[1] أنظر المادة 80 ، 82 ، 83 ق ، ج ج

[2] أنظر لمادة 47 ق.ا.ج. ج

[3] أنظر المادة 47 فقرة أخيرة ق.ا. ج . ج

وهو ما سنطرق إليه فيما يلي :

1- استجواب المتهم :

الاستجواب هو مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده ، وهو وسيلة تمحيص للتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات [1].

إذ اعتبر الاستجواب ذو طبيعة مزدوجة فهو أداة اتهام ووسيلة دفاع في آن واحد بحيث يسمح للمتهم أن يحاط بالتهم والوقائع المنسوبة إليه وبكل ما يوجد بالملف من أدلة التي تساعد على كشف براءته .[2]

ويختلف الاستجواب عن السؤال و أن الثاني لا يتطلب مناقشة المتهم في هويته ، ومدى خطورته ، اعمالا بالمواد .

- استجواب المتهم في الموضوع : أي مواجهة قاضي التحقيق المتهم بالتهم المنسوبة إليه ومناقشته فيها مناقشة تفصيلية ومواجهته بالأدلة القاطعة ضده ولابد أن يكون الاستجواب بحضور المحامي طبقا لنص المادة 57/110 ق.ا.ج.ج 101 ، 102 ق.ا. ج . ج .

[1] أحسن بوسقيعة . التحقيق الفضائي ، ص 45

[2] محمد حزيط . مذكرات في قانون الإجراءات الجزائية الجزائري ، ص 102

- الاستجواب الإجمالي للمتهم : يكون في مسائلة جنائية (جنايات) وهو إجراء وجوبي إذ تعلق التحقيق بقضية ذات طابع جنائي ، يهدف إلى تخليص الوقائع وإبراز الأدلة التي سبق جمعها .[1]

2- الشهادة الالكترونية :

إن مصطلح الشهادة الالكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق وسائل الكترونية أو رقمية من خلال شبكة الإنترنت[2] .

وقد أعطى قانون الإجراءات الجزائية لقاضي التحقيق الحرية في تحديد الأشخاص الذين يرى فائدة من سماع شهادتهم ، سواء كان هؤلاء الأشخاص قد ورد ذكرهم في البلاغ عن الجريمة أو الشكوى منها ، أو أي

شخص آخر ، وذلك تطبيقا للمواد 60 ، 88 ، 97 ، 110 ، ق.ا.ج. ج [3]

3- ضبط الدليل في مجال الجريمة المعلوماتية :

الضبط كقاعدة عامة لا يرد إلا على أشياء مادية ، فلا صعوبة في ذلك ، وبالتالي يضبط الدليل في الجريمة المعلوماتية على المكونات المادية للكمبيوتر ، فترفع البصمات مثلا وغيرها ، فلا صعوبة في ذلك . وإنما تكمن الصعوبة في ضبط الوسائل الفنية أو المعنوية المستخدمة في إتلاف البرامج .

---

[1] محمد حزيط ، المرجع نفسه ، ص 103

[2] عبد العالي الديري . محمد صادق اسماعيل الجرائم الاكترونية ، ص 313

[3] 2 أنظر المواد 60 ، 88 ، 97 ، 110 ، ق.ا.ج.ج

المطلب الثاني: صعوبات التحقيق في الجرائم المعلوماتية

يتسم التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائياً بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق ، بل يمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه وعلى المجتمع بفقدائه الثقة في أجهزة تنفيذ القانون غير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها ، وانعكاسها أيضا على المجرم نفسه ،[1]حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه ، الأمر الذي يعطيه ثقة كبيرة في ارتكابه المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشد ضرراً على المجتمع المحلي أو المجتمعات الأخرى [2].

ومن أهم المعوقات التي قد تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق فيها ، عوائق تتعلق بالجريمة وعوائق تتعلق بالجهات المتضررة ، وأخري تتعلق بجهات التحقيق ، وعوائق تتعلق بإجراءات الحصول على الدليل الإلكتروني ، ونتناولها بشيء من التفصيل على النحو التالي:

1 حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت رسالة دكتوراه حقوق عين شمس ، 2005، ص 399 وما بعدها

2 عبد الرحمن بحر : معوقات التحقيق في جرائم الإنترنت " دراسة مسحية على ضباط الشرطة بدولة البحرين ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، الرياض 1999، ص51

أولا : عوائق تتعلق بالجريمة المعلوماتية : [1]

من المعوقات المتعلقة بالجريمة المعلومانية :

1- خفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمة .

2- افتقاد أكثر الآثار التقليدية.

3- إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها

4- سهولة محو الدليل أو تدميره في زمن قصير جداً ، ومن الأمثلة على ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة .[2]

1 حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ، ص 407 وما بعدها

2 د . هشام . هشام محمد فريد رستم ، الجرائم المعلوماتية " أصول التحقيق الجنائي الفني ، مؤتمر القانون والكمبيوتر والإنترنت ، المنعقد بكلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة في الفترة من 1-2000 / 5 / 3 ، ص 430 .

وفي واقعة مماثلة حدثت وقائعها بدولة الإمارات العربية المتحدة تتمثل في قيام مشغل حاسب آلي بتهديد المؤسسة التي يعمل بها لتنفيذ مجموعة من المطالب ، وذلك بعد أن قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة ، وإزاء رفض المؤسسة الاستجابة لمطالبه أقدم على الانتحار مما سبب صعوبة بالغة في استرجاع البيانات التي كان قد حذفها [1].

فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا ، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها ، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده ، وبالتالي تنصله من مسئولية هذا الفعل وإرجاعه إلي خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة .

ناهيك عن الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها ، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والنصيحة . [2]بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بالإنترنت من قبل بعض الأطراف المعينة .[3]

---

1 خالد الستاني . – أمن المعلومات وتحليل المخاطر ، ورقة عمل مقدمة إلي ندوة فيروسات الحاسب التي عقدها معهد التنمية الإدارية بالمجمع الثقافي بإمارة أبو ظبي بدولة الإمارات العربية المتحدة في 23/9/1996 .

2 عبد الرحمن بحر : المرجع السابق ص 46

3 سليمان بن مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجستير – جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2003 ، ص 114 - Johm Eaton and Jeremy Smithers . This is it a Managers Guide to information Technology . London , Philip Allan , 1982. p 263 . 11

ثانياً : عوائق تتعلق بالجهات المتضررة

1- عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معوقات التحقيق .

2- كما يعد إغفال جانب التوعية لإرشاد المستخدمين إلي خطورتها معوق أخر ، وبالنظر إلى بعض

المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس أنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك على حساب الأمن. [1]

3- كما تعد التقنية المستخدمة في نظم المعلومات مجال استثمار ولذا تتسابق الشركات في تبسيط الإجراءات

وتسهيل استخدام البرامج والأجهزة وملحقاتها ، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني ، على سبيل المثال مستخدمو شبكة الإنترنت عبر مزودي الخدمة والبطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الإنترنت ، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة . [2]

1 باسم الحمادي ، إثبات جرائم الإنترنت صعب ، بحث منشور على شبكة الإنترنت بتاريخ 7 محرم 1423 هـ على موقع www.alrivadh.com، الرياض ، ص 14

2 عبد الرحمن بحر ، المرجع السابق ، ص 39

4- كما أن الأحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن ، [1]خوفاً من المجتمع المحيط

بهم وخشية الفضيحة يعد معرفا من معوقات التحقيق ، وقد يكون بهدف إخفاء الأسلوب الذي ارتقت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلاً

5- كما يكون الإحجام عن الإبلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضررة في

الظهور بمظهر مشين أمام الآخرين ، لأن تلك الجرائم ارتكبت ضدها ، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني ، [2]ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها .

كما توجد أسباب أخرى تحجم عن الإبلاغ عن هذه الجرائم من قبل الجهات المتضررة منها الحفاظ على سمعة المؤسسات ومصداقيتها.

6- أيضا قد تكون بعض هذه الجرائم محدودة الأثر ، مما يدفع بعدم الإبلاغ عنها ، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية، أو يقوم مجرم آخر بإرسال فيروس كمبيوتر إلي جهاز المستفيد ويكون

---

[1] .زكي أمين حسونه ، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي ، المؤتمر السادس للجمعية المصرية للقانون الجنائي ، ص TV476 .

2 طارق عبد الله الشدي ، آلية البناء لنظم المعلومات ، دار الوطن للطباعة والنشر ، الرياض 1423 هـ ، ص 210

هذا الفيروس محدود الأثر ، أو تقوم برامج الحماية من الفيروسات بالقضاء عليه .

7- قد يكون الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق

بالنظام المعلوماتي ، فقد يحرم الموظف في الجهة من خدمات معينة على الإنترنت أو قد يحرم من خدمات الإنترنت عموماً حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها ، وقد يكون سبب عدم الإبلاغ عن الجريمة ، عدم معرفة الصحية بوجود جريمة أصلاً ، وعدم القناعة إنها ممكن أن تحدث في مؤسسته.

ثالثاً : عوائق تتعلق بجهات التحقيق [1]

1- بعض هذه المعوقات ترجع إلى شخصية المحقق ، مثل التهيب من استخدام جهاز الكمبيوتر والتهيب

من استخدام الإنترنت ، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية

2- والبعض الآخر يتعلق بالنواحي الفنية ، كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ،

1 حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ، ص 409

ونقص المهارة في استخدام الكمبيوتر والإنترنت ، وعدم توفر المعرفة بأساليب ارتكاب الجرائم المعلوماتية ، وقلة الخبرة في مجال التحقيق في جرائم الكمبيوتر والإنترنت والمعرفة باللغة الإنجليزية ، [1]سيما وإن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم ، وليس هذا فحسب بل أختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات Acronymsوهي لغة جديدة ومتطورة.

كل هذا دفع بمعتادي الإجرام المعلوماتي أن يطلقوا على أنفسهم صفة النخبة ، وفي ذات الوقت يطلقون على رجال إنقاذ القانون صفة الضعفاء أو القاصرين . [2]

لأجل ذلك بدأت بعض الأجهزة الأمنية والقضائية في استقطاب المختصين في الكمبيوتر ليكونوا ضمن كوادرها ، كما جرى تدريب رجال الشرطة والقانون على استخدام الحاسب الآلي ، وعلى الرغم من ذلك فقد تكون تلك الأجهزة غير قادرة على مواكبة التطور السريع في الحاسب الآلي لعدة أسباب ، [3]كأن تكون الميزانيات المالية المرصودة لتدريب الكادر البشري في الأجهزة الحكومية لا تكفي لاستقطاب النخبة

1 سليمان بن مهجع العنزي ، المرجع السابق ، ص 119

2 د . محمد الأمين البشري : التحقيق في جرائم الحاسب الآلي ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة (1) 2000 / 5 / 3 م الطبعة الثالثة 2004 م ص 1070 – مشار إليه لدي : حسين بن سعيد بن سيف الغافري ، المرجع السابق ، ص 410

3 د . محمد أمين البشري ، المرجع السابق ، ص 1072

المتميزة في المجال المعوماتي خاصة وأن الشركات ومؤسسات القطاع الخاص تبذل المستحيل من أجل ضم هذه النخبة إليها .

وقد تكون أمام أجهزة الشرطة والنيابة مجالات متنوعة ينبغي تغطيتها بالدعم والعناية فهي ليست متفرغة تماماً للجرائم المعلوماتية وحدها ، ومن هنا كانت المناداة إلى إنشاء وحدة تحقيق خاصة بالجرائم المعلوماتية متفرغة لهذا النوع من الجرائم ، وقد يكون لحداثة هذا النوع من الجرائم وقلة المستكشف منها سبب وراء عدم اكتساب تلك الأجهزة خبرة التعامل معها ، ناهيك عن الأنتشار الواسع للكمبيوتر وتنوع برامجه وأنظمته مما يجعل حصر أساليب الجريمة المعلوماتية وصورها وأنماطها صعبا وبالتالي يتعذر معه تدريب المحققين .

إزاء ذلك يري البعض أنه من المستحسن أن توكل مهمة التحقيق في هذا النوع من الجرائم إلي بيوت الخبرة المتخصصة في هذا المجال لا سيما مع وجود شركات عالمـية متخصصة في تحقيق الجرائم المعلوماتية حققت النجاح في كثير من الحالات [1].

في حين أن جانب أخر يرى- وبحق- أن متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومية مسئوليتها تجاه اكتشاف كافة الجرائم ومن بينها الجرائم المعلوماتية وضبط الجناة فيها وتحقيق العدالة في حقهم .

1 حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت ، مرجع سابق ، ص 411 وما بعدها

كما ينبغي على تلك الأجهزة تحمل توفير الإمكانيات التقنية اللازمة للتحقيق في الجرائم المعلوماتية بالإضافة إلى الكوادر البشرية ذات الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في التحقيق .

ومن الممكن وحتى تكتمل قدرات تلك الأجهزة في هذا المجال أن يتم الاستعانة بالنخبة المتخصصة في مجال الكمبيوتر وتكنولوجيا المعلومات وكل ما يتعلق بها في جميع مراحل الدعوى الجنائية بدأ من اكتشاف الجريمة المعلوماتية وانتهاء بالتحقيق والمحاكمة.

و من أجل ذلك فإنه لا بد من إيجاد أسلوب خاص للتحقيق في ملم الجرائم أسلوب يجمع بين الخبرة الفنية والكفاءة المهنية ومن الممكن حيال ذلك إتباع الخطوات التالية: [1]

1- تبادل المعلومات بين المحقق وخبير الحاسب الآلي وذلك قبل البدء في التحقيق وأخذ أقوال الشهود

والمشتبه فيهم أو استجواب المتهمين ، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم . [2]

1 د . محمد الأمين البشري ، المرجع السابق ، ص 1073

[2] - United Nation . United Nation Manusl on the prevention and control of Computer - Related crime : Viennal 1999

ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلابها من الأشخاص، وكافة المصطلحات الحاسوبية يمكن استخدامها مع بيان معانيتها ليتم الاستفادة منها عند الضرورة.

2- يتم حصر النقاط المطلوب استجلابها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد

ذلك ترتيب تلك النقاط.

3- يتم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة

الفرعية أثناء الاستجواب وفق الكيفية التي يتم الاتفاق عليها مسبقاً قبل بدء التحقيق .

4- التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة

بالشاهد أو المتهم الذي تم التحقيق معه ، مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه

ولضمان نجاح التحقيق في الجرائم المعلوماتية فهناك بعض القواعد التي ينبغي مراعاتها أهمها :[1]

1- تنادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها أو أن الأدلة اللازمة لاكتشافها

[1] - Peter Tillers . Introduction to program on Artificial intelligence N.Y Yeshiva University Press . 1999. p117 .

وإثبات التهمة قد قضي عليها .

2- ضرورة مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها .

3- مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغيرها من الحقوق .

4- العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها .

5- مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدا ، وذلك حتى يتم تقديمها للمحكمة

وهي على حالتها التـ ضبطت عليها .

6- الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية ، سيما وأن هذا

التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق.

رابعاً : عوائق تتعلق بإجراءات الحصول على الدليل الإلكتروني

يجب علينا بحث بعض المشاكل التي تعيق الضابط المحقق في مثل تلك الجرائم وهي :

اعتبارات المعرفة الأساسية لكل من الضباط والمحقق لماهية الجرائم المعلوماتية وهل ما قام به يعد جريمة في قانون الدولة التي ينتمون إليها من عدمه ، وكذا قانون الدولة المتواجد بها المشتبه فيه الأمر الذي تنشأ عن مشكله أخري وهو كيفية الحصول علي الدليل عبر الحدود وربما يكون ذلك الدليل غير قائم بالفعل ، وكيفية اكتشاف الجريمة الطريقة التي تكتشف بها الجرائم ، وغالباً ما يحدث خلل وظيفي ما في الأجهزة أو المواقع الخاصة لموفري الخدمات ينتج عن ذلك الخلل الصحفي والتحقيق ، ويتم بعد ذلك اكتشاف الجريمة الأمر الذي يجد معه أن يكون لدي أعضاء النيابة الدراية الكافية لمعرفة البدء في التحقيقات ، وهذا ما نطلق عليه عبارة " الوضع المناسب والإشارة الصحيحة " فإذا لم تحدد الجريمة ولم يتم التحفظ علي الدليل فإن الأثر المباشر لهذا هو عدم وجود الجريمة .

ومن ثم يجب على أعضاء النيابة والضابط منذ فجر تفشي نبأ الجريمة الحفاظ علي الدليل وتقنية بالطرق المبينة سلفاً ، وذلك لأن الدليل الإلكتروني سهل التغير ويكون ذلك بالتعاون مع الجهات التي تقدم الخدمة بإجبارهم بوسيلة ما في الحفاظ علي الدليل وعدم البعثرة فيه وأن يتم تعيين بعض من المتخصصين تخول لهم سلطة الضبط والتفتيش في تتبع الدليل.

و لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول الأدلة التي تكفي لإثباتها ، وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة ، فإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق

المشاهدة والتتبع والمساعدة ، فإنه قد يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية . [1]

إلا أن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجاً أمنياً على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب ، فهم قد يزيدون من صعوبة إجراءات التفتيش التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلي البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال ، وقد يلجا هؤلاء المجرمون أيضاً إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم أفعالهم غير المشروعة. [2]

كذلك فإن هناك معوقات كثيرة قد تعترض الحصول على الأدلة بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية ، ومثال ذلك أنه قد يتعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلاً بحاسبات أخرى خارج الدولة ، ويكون تفتيش هذه الحاسبات ضرورية الإماطة اللثام عما تشتمله من جرائم . [3]

وليس بخف علينا أن الجرائم التي ترتكب في فضاء شبكة الإنترنت كما أنها تقع على المستوى الوطني ، فإنها قد ترتكب أيضاً المستوى الدولي ، وهذا يثير مشكلات

1 – حسين بن سعيد بن سيف الغافري ، المرجع السابق ، ص 413 .

2 د . هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، 1994 ، ص 22

3 أسامة أحمد و آخرون المرجع السابق ص 293

عديدة مثل تتبع الاتصالات الإلكترونية عن طرق سلطات التحقيق لأجل إقامة الدليل على الجرائم على التي ترتكب في مجال الإنترنت .

ولا شك في أن اختلاف التشريعات فيما بينها فيما يتعلق بشروط قبولها للأدلة وتنفيذ بعض الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود .[1]

فعلى الرغم من أن إرهاصات الثورة التكنولوجية في مجال الاتصال عن بعد قد أفرزت العديد من الجرائم ذات الطبيعة الخاصة ، فما زالت إجراءات البحث عن هذه الجرائم وضبطها تتم في إطار النصوص الإجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية التي تنص عليها القوانين العقابية ، [2]الأمر الذي سيترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المعلوماتية ذات الكيان المعنوي والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة ، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت ، كما هو الحال في شان جريمة غسل الأموال عبر الإنترنت ، فيتعذر تبعا لذلك اتخاذ إجراءات الدليل بالنسبة لها ، أو قد تلحق عدم المشروعية بهذه الإجراءات .

ولذلك نجد أن بعض الفقه في ألمانيا يشكك في إمكانية الدخول أنظمة تقنية المعلومات لدى الحاسبات الأخرى التي توجد بالخارج بغرض ضبط البيانات المخزنة بها لأنه بدون وجود أتفاق بين الدول المعينة بتنظيم ذلك ، فإن اتخاذ مثل هذا الإجراء

[1] جميل ع الباقي صغير ،الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ،دار النهضة العربية 2002 ص 76

[2] حسين بن سعيد بن سيف الغافري ، المرجع السابق ص414

يعد خرقا لسيادة كل دولة على إقليمها ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية .[1]

ويلاحظ في هذا المجال تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية ، وذلك لأن هذا التفتيش يتم – غالباً – على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات ، الأمر الذي قد يتجاوز النظام المعلوماتي المشتبه به إلى أنظمة أخرى مرتبطة ، نظرا لشيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول ولاشك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه قد يمس – في الصميم – حقوق الخصوصية المعلوماتية لأصحاب النظم المعلوماتية التي يمتد إليها التفتيش .

المبحث الثاني : سبل مواجهة الجرائم الإلكترونية في الشريعة الإسلامية والأنظمة الدولية

ويضم مطلبين :

المطلب الأول : سبل مواجهة الجرائم الإلكترونية في الشريعة الإسلامية .

المطلب الثاني : سبل مواجهة الجرائم الإلكترونية في الأنظمة الدولية .

[1] Mohrenschlager “ Manfred " : computer crimes and other crimes against information techmology in Germany . Rev. inter . De . Dr. Pen . 1993. P351

المطلب الأول : سبل مواجهة الجرائم الإلكترونية في الشريعة الإسلامية

من المسلم به أن الشريعة الإسلامية شريعة عامة لكل زمان ومكان ، وأن الناس مختلفون في ضبط نفوسهم ، فلابد من وجود عقاب رادع يضبط أصحاب النفوس الضعيفة من الوقع في الجرائم حتى يسلم المجتمع من الفساد ظاهراً وباطناً من أجل ذلك حاربت الشريعة الإسلامية الجرائم بشتى صورها ؛ لأن شريعة الإسلام تفترض أن الإنسان يجب أن يعيش من طريق شريف ، وأن يحيا على ثمرات كفاحه وجهده الخاص ، والشريعة الإسلامية لا تجعل أي فعل من الأفعال جريمة إلا ما فيه ضرر محقق للفرد والجماعة ، ويظهر هذا الضرر فيما يمس الدين ، أو العرض ، أو النفس ، أو النسل ، أو المال ، أو العقل ، وهذه الكليات مقصد مهم من مقاصد الشريعة الإسلامية التي شرعت من اجل الحفاظ عليها .

وقد تميزت الشريعة الإسلامية بمنهجها الفريد في مكافحة الجريمة واستئصالها من جذورها من خلال خطين متلازمين ومتوازنين وهما :

أولا : الجانب الوقائي :

ومن أهم ملامحه إصلاح الجاني ، وفتح أبواب التوبة أمامه على مصراعيها ، وعدم تيئيسه من رحمة الله ، وحثه على الإقلاع والندم ، وعدم التمادي في الباطل ، فالشريعة بداهة تكره الجريمة ، وتتوعد عليها بالنكال في الدنيا والآخرة وتهدد أقواماً

يرتكبونها سراً ثم يبرزون للناس وكأنهم أطهار شرفاء[1]. قال تعالى (ولا تجادل عن الذين يختانون أنفسهم إن الله لا يحب من كان خوانا أثيما يستخفون من الناس ولا يستخفون من الله وهو معهم إذ يبيتون ما لا يرضى من القول وكان الله بما يعملون محيطا) [2]

فدور الشريعة في الجانب الوقائي تجاه الجريمة لا يقتصر على وضع عقاب رادع للجاني فحسب ، بل تتخذ كل الإجراءات والتدابير التي من شأنها الحيلولة دون وقوع الجريمة ، فالتربية الإسلامية المستمرة بالحكمة والموعظة الحسنة ثم التوعية المستمرة بالجريمة وأخطارها من كافة الجهات المعيشية ، وأيضاً سد الأبواب والمنافذ التي تؤدي إلى اقتراف الجريمة .

ثانيا : الجانب العلاجي :

وهذا الجانب يلي الجانب الوقائي في مواجهة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة وبما أن الجريمة سلوك شاذ يهدد امن الأفراد و استقرار المجتمعات ويقوض أركان الدولة والبلاد فإن أحكام الشريعة الإسلامية الغراء بعدلها القويم ومبادئها الشاملة يدور حول صيانة الضرورات الأساسية التي لا يستطيع الإنسان أن يستغني عنها ويعيش بدونها ، فوضعت العقوبات الشرعية الزاجرة والأليمة لكل من يتعدى على هذه الضرورات الأساسية وينتهك حرمتها ، فوضعت لكل جريمة

1 هذا ديننا محمد الغزال ص 229– 3 حسان القاهرة 1395 هـ 1975 م

2 النساء 107 ـــ 108

من الجرائم العقوبات المناسبة للحد من ارتكاب هذه الجريمة ، كل هذه الخطوات تؤدي إلى مكافحة الجريمة وتقي المجتمع من أخطارها ، وبذلك فقد تكفلت التشريعات الجنائية الإسلامية على عاتقها عبء مكافحة الجريمة والتصدي لها ؛ حماية للمجتمع من أن يقع فريسة لها بمختلف أنوعها ، وهناك حقان متميزان ترعاهما الشريعة الإسلامية هما :

1- حق المخطئ في فرصة يتوب منها ، ويستأنف ملكاً أنظف .

2- ٢ - حق المجتمع في صيانة كيانه من نزوات العصيان وتخبطه الذي يصيب الأبرياء والغافلين .

والإسلام يرعى الحقين كليهما ، فأما حق المخطئ في التوبة ، فليس في الأرض دين ييسر المتاب للخاطئين ويدفعهم إليه دفعا كدين الإسلام ، ولكن ما العمل إذا تحول المرء إلى كلب مسعور ، فأصبح تركه حراً لا يزيده ألا ضراوة ، ولا يزيد المجتمع به إلا شقاوة ، إن عقاب مثل هذا لا مناص منه .[1]

إن مما لا شك فيه أن الشريعة الإسلامية أفردت لكل جريمة من الجرائم ، العقوبة التي تلائمها ، ونصت على الضوابط والشروط والأحكام التي تخص كل جريمة وعقوبتها وهذا في الجرائم والعقوبات التقليدية مثل جريمة القتل وعقوبتها القصاص أو الدية ، وجريمة الزنا وعقوبتها الحد –الرحم أو الجلد وجريمة السرقة

[1] هذا ديننا محمد الغزالي ص 154

وعقوبتها الحد القطع ، وجريمة الشرب وعقوبتها الحد الجلد وهكذا وكل جريمة لها عقوبة منصوص عليها فهي عقوبة حدية وكل جريمة لها عقوبة ليست منصوص عليها ، فهي عقوبة تعزيرية .

وهذه كلها جرائم تقليدية قديمة عرفها الفقه الإسلامي ووضع لها العقوبات الشرعية المقدرة – الحدود وغير المقدرة – التعزيرات– ، لكن في هذا العصر ظهرت جرائم كثيرة مرتبطة بالتقدم في جميع مجالات التقنية في مجال الحاسب الآلي والإنترنت ، فكان لزاماً على المشتغلين بالفقه الإسلامي أن يتعرفوا على هذا النوع من الجرائم ويضعوا له العقوبات التي تناسبه .

هذا ومما تجدر الإشارة إليه أن الحاسب الآلي لم يكن له أدبي تأثير في وصف الجريمة المرتكبة عن طريقه ، فجرائم النصب مثلا تأخذ هذه الصفة حتى لو ارتكب بطريق الانترنت مثلها في ذلك مثل جريمة النصب التي ترتكب بالطريقة التقليدية ، وكذلك جريمة السرقة ، والقذف ، وغيرها ، ولمزيد من الإيضاح في بيان مواجهة الشريعة الإسلامية للجريمة الإلكترونية ، يحسن التعرف على وصف بعض الجرائم وتطبيقاتها حتى يمكن معرفة مدى انطباق هذا الوصف على نفس الجريمة الواقعة بطريق الحاسب الآلي ، ولنأخذ مثلا جريمة السرقة ؛ لكونها من أخطر جرائم الحاسب الآلي والانترنت في هذا العصر ، وتطبق عليها أركان وشروط هذه الجريمة كما ذكرها الفقهاء في عصر تدوين الفقه ، ويمكن تصور جريمة السرقة في هذا العصر عن طريق الانترنت من خلال بطاقات الائتمان المسروقة ، فلو نظرنا في تعريف السرقة

وشروطها ، والعقوبات المقدرة لها في كتب الفقهاء و طبقناه على جريمة السرقة عبر الإنترنت لاستطعنا أن نقرر باطمئنان أن جريمة السرقة من خلال الإنترنت هي بذاتها جريمة السرقة التقليدية وبالتالي فالعقوبة المقررة لها شرعا هي نفس العقوبة المقررة لجريمة السرقة التقليدية . وها هو التفصيل على النحو التالي :

تعريف السرقة :

عرفها الحنفية بأنها : احذ العاقل البالغ نصاباً محرزاً ، أو ما قيمته نصاباً ملكاً للغير لا شبهة له فيه على وجه الخفية.[1]

وعرفها المالكية بقولهم : هي أخذ مال الغير مستترا من غير أن يؤتمن عليه[2].

وعرفها الشافعية بقولهم : هي أخذ المال خفية ظلماً من حرز بشروط[3].

وعرفها الحنابلة بقولهم : هي أخذ المال على وجه الخفية والاستتار ومنه استراق السمع ، و مسارقة النظر إذا كان يستخفى بذلك.[4]

شروط السرقة :

من التعاريف السابقة يمكن القول إنه يشترط لجعل هذا الفعل سرقة توجب القطع أن يتوافر فيه الشروط التالية :

---

[1] شرح فتح القدير للكمال من المسام الحنفي 120 / 5 ط دار إحياء التراث العربي

[2] بداية المشهد وقاية المقتصد لابن رشد 199 تحقيق أبو عبد الرحمن عبد الحكيم بن محمد ط المكية التوفيقية القاهرة

[3] حاشية قليوبي وعميرة 186/ 4 ط المعاهد الأزهرية

[4] الروض المربع شرح زاد المستقنع في اختصار المقنع للشيخ منصور بن يوسف البهومي 439 ، ط دار الفكر بيروت

1- أن يكون السارق مكلفا ، فإن كان صبياً أو مجنونا فلا حد عليه.[1]

2- أن يكون قد سرق مختاراً لا مكرها[2].

3- أن لا يكون السارق مضطراً لسد جوعته حيث لم يجد من الطعام الحلال شيئاً يأكله.[3]

4- أن يبلغ المسروق نصاباً ، والنصاب الذي تقطع به يد السارق وهو ربع دينار من الذهب ، أو ثلاثة دراهم من الفضة عند الجمهور خلافاً للحنفية حيث يرون أن مقدار النصاب دينار أو عشرة دراهم أو قيمة أحدهما[4]. ومنشأ الخلاف هو في تقدير ثمن المجن الذي قطع رسول الله – صلى الله عليه وسلم بسرقته يد السارق ، فالحنفية يقولون : كان ثمنه دينارا والجمهور يقولون كان منه دينار والأحاديث الصحيحة تشهد لقول الجمهور ومنها ما جاء عنه – صلى الله عليه وسلم – : (أنه قطع سارقا في محن قيمته ثلاثة دراهم)[5]

[1] لسن الحقائق الزيلعي 3/211 ، والقوانين الفقهية لابن جرى مي 259 ، وحاشية قليون وعميرة – 4/187 المعاهد الأزهرية

[2] حاشية قليون وسميرة 196

[3] الفقه الإسلامي وأدلته دا وهية الرحيلي 6/102 .

[4] بداية 663/2 و ما بعدهاالمجتهد ط المكتبية التوفيقية

[5] أخرجه مسلم في صحيحة كتاب الحدود باب حد السرقة ونصابها

5- أن لا يكون للسارق في المال الذي سرقه شبهة ملك ، فإن كان له فيه شبهة ملك ، فإنه لا يعد سارقا[1].

6- أن يكون المال المسروق قد سرق من حرزه وهذا الشرط متفق عليه عند جميع فقهاء الأمصار الذين تدور عليهم الفتوى.[2]

ثالثا :الجانب التطبيقي لمواجهة جريمة السرقة الإلكترونية في الشريعة الإسلامية

وإذا طبقنا هذه الشروط على السرقة عن طريق الانترنت باستخدام بطاقات الائتمان المسروقة يمكن أن يتضح توفر هذه الشروط في هذه الجريمة حيث إن هذه البطاقات تعد مالا .

ولعل هذا المثال يبين أن جرائم الانترنت يمكن تكييفها بحسب وصفها المدون في كتب الفقه ، وذلك بعد استعانة القاضي بالمتخصصين لشرح ما قد يرغب الاستفسار عنه أو توضيحه حول الأسلوب والطريقة التي تمت بها الجريمة عبر شبكة الإنترنت ؛ ليكون على دراية تامة بكافة التفاصيل التي يمكن من خلالها أن يصدر حكمه على المتهم .

هذا إذا سهل على المتخصصين في العلوم الشرعية إلحاق وصف الجريمة الإلكترونية بوصف الجريمة التقليدية فإنه والحالة هذه تأخذ هذه حكم تلك ، أما إذا لم يتمكن المفتون والقاضي من إلحاق وصف الجريمة الإلكترونية بوصف الجريمة

[1] الهداية 2/123 ، وبداية المجتهد 2/669 ، وحاشية قليوبي وعمره 4/188 ، والروض المربع ص 44

[2] بداية المجتهد 666/2

التقليدية لاختلال شرط من الشروط مثلا ، فإن ميدان العقوبة التعزيرية ميدان واسع لمواجهة هذه الجريمة ، يختار القاضي فيه ما هو مناسب وملائم لحال المحرم وجسامة ضرره ، وباعثه ، وزمانه ومكانه ، فالعقوبات التعزيرية : عقوبات غير مقدرة تحب حقاً لله أو لآدمي في كل معصية ليس فيها حد ولا كفارة [1]فهي كالحدود في الزجر والتأديب للأمة ، وإذا كانت العقوبة التعزيرية غير مقدرة فللحاكم أو القاضي أن يفرض العقوبة التي يراها مناسبة ، فقد تكون توبيخاً ، وقد تكون ضرباً ، وقد تكون حبساً ، وقد تكون مصادرة على ألا تبلغ حداً من الحدود عند جمهور الفقهاء [2]، خلافاً للحنفية والمالكية الذين يتوسعون في ميدان العقوبة التعزيرية حيث يرون أن العقوبة التعزيرية قد تصل في بعض الأحيان إلى القتل [3] .

ولهذا القول وجاهة بخاصة في مجال الجرائم الإلكترونية ، فهناك جرائم الكترونية بلغت من خطورتها مبلغاً يفوق بكثير جريمة القتل التي عقوبتها أشد عقوبة وهى القصاص ، فيكفي في وصف خطورتها أنها لا تعترف بالحدود بين الدول ولا حتى بين القارات ، فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة[4]وخلاصة

[1] الفقه الإسلامي وأدلته للدكتور وهبة الزحيلي 197 / 6 ط دار الفكر.

[2] نهاية المحتاج ٧/١٧٥ ، وحاشية الباجوري على ابن قاسم الغزي 2/234 ، والمغني 8/334 ، والساسة الشرعية لابن تيمية ص 146 ، ط دار علم الموائد النشر والتوزيع حده والطرق الحكمية لابن القيم 1/265 ، ط دار علم الفوائد النشر والتوزيع حده .

[3] رد المحتار على الدر المختار لابن عابدين 3/196 ، والشرح الكبير للدردير 4/255 ، والمغني لابن قدامه 8/334 ، ط المكتب الثقافي والعزيز في الشريعة الإسلامية لعبد العزير عامر في 322 ، وما بعدها ط دار الفكر العربي .

[4] الإجرام المعاصر محمد علي عبد ص 252 م أكاديمية نايف العربية للعلوم الأمنية ، الرياض 1419 هـ

القول إن الفقه الإسلامي واسع المجال في مواجهة الجرائم المستحدثة عبر الانترنت وغيره بفضل اجتهاد الفقهاء في استنباط الأحكام واستخدام القياس وإعمال القواعد الفقهية التي تعد ضوابط حاكمة لمواجهة الجريمة الالكترونية ومن بين هذه القواعد قاعدة الضرر يزال [1]، وقاعدة سد الذرائع [2]وقاعدة درء المفاسد مقدم على جلب المصالح [3]وغيرها .

المطلب الثاني : سبل مواجهة الجرائم الإلكترونية في الأنظمة الدولية

إن مواجهة الجرائم الإلكترونية قد لاقت اهتماماً عالمياً فقد عقدت المؤتمرات والندوات المختلفة ، وصدرت من خلالها قوانين وتشريعات تحرم من يقدم على ارتكاب هذه الجرائم ، وتعد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي ولانترنت حيث صدر قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها ، وجاءت الولايات المتحدة الأمريكية بعد السويد حيث شرعت قانونا خاصاً بحماية أنظمة الحاسب الآلي في الفترة من 1976- 1985 م ، وفي عام 1985 م حدد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي جرائم الحاسب الآلي الداخلية ، وجرائم الاستخدام غير المشروع عن بعد ، وجرائم التلاعب بالحاسب

[1] الأشباه والنظائر للسيوطي ص 83 ، ط دار الكتب العلمية بيروت .

[2] الموافقات للشاطي 4/163

[3] الأشباه والنظائر للسيوطي ص87

الآلي ، ودعم التعاملات الإجرامية ، وسرقة البرامج الجاهزة والمكونات المادية للحاسب ، وفي عام 1986 م صدر قانوناً تشريعياً عرف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة التطبيقية ، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ، ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي ، وقد حولت وزارة العدل الأمريكية في عام 2000 م خمسة جهات منها مكتب التحقيقات الفيدرالية (fb1) للتعامل مع جرائم الحاسب الآلي والانترنت [1].

ويلي الولايات المتحدة في الاهتمام بمواجهة الجرائم الإلكترونية مباشرة بريطانيا التي تأتي في المرتبة الثالثة بعد السويد وأمريكا فقد أقرت قانون مكافحة التزوير و التزييف عام 1981 م الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى [2]

وتحظى كندا بالتصنيف بين هذه الدولة التي أولت مواجهة الجرائم الإلكترونية عناية فائقة حيث عدلت في عام 1985 م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت ، كما شمل القانون الجديد تجديد عقوبات المخالفات الحاسوبية وجرائم التدمير ، أو الدخول غير المشروع لأنظمة الحاسب الآلي ، كما

[1] الجرائم المعلوماتية من منظور شرعي وقانون هشام عبد القادر بحث منشور بشبكة الانترنت بدون ترقيم صفحات .

[2] أمن المعلومات وجرائم الحاسب الآلي لعبد الرحمن عبد العزيز الشنيفي ص 108 ط الأولى الرياض

وضح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة الذي يخول المأمور متى ما حصل على أمر الضبط القضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها قضائيا[1].

وها هي الدنمارك قد سنت أول قوانينها الخاصة بجرائم الحاسب الآلي ولإنترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي ، أو التزوير ، أو أي كسب غير مشروع ، سواء للجاني أو لطرف ثالث ، أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها ، أو تعبيرها أو الاستفادة منها[2].

وكذلك اهتمت فرنسا بتطوير قوانينها الجنائية للتوافق المستجدات الإجرامية حيث أصدرت في عام 1988 م القانون الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها كما تم تعديل قانون العقوبات لديها عام 1994 م ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال[3].

كما توجد في هولندا واليابان والمجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والإنترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها ، وتعطي تلك

---

[1] المرجع السابق ص 243.

[2] أمن المعلومات وجرائم الحاسب الآلي 110

[3] الجرائم الناشئة عن استخدام الحاسب الآلي لأحمد حسام دار النهضة العربية القاهرة ، ص 391

القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي ، أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج ، كما تعطي الشاهد أيضاً الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما أدى ذلك إلى إدانته أو إدانة أحد أقاربه ، بل تذهب القوانين الجنائية المعمول بها في بولندا إلى أبعد من هذا حيث إنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم .

هذا وعلى مستوى الدول العربية نجد أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة التقليدية ، ومن ذلك مثلا أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات ، كما تم تطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار بحيث يمكن تطبيقها على بعض الجرائم المعلوماتية ، وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية .[1]

وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت ، وإن وجد نص قريب من الفعل المرتكب ، فإن العقوبة المنصوص عليها لا تتلاءم مع حجم الأضرار المترتبة على جريمة الإنترنت[2].

[1] المرجع السابق ص 104

[2] معوقات التحقيق في جرائم الإنترنت دراسة مسحية على ضباط الشرطة في دولة البحرين رسالة ماجستير منشورة لعبد الرحمن ابعد . أكادمية نايف العربية للعلوم الأمنية بالرياض السعودية 1440 هـ

وكذا معظم الدول العربية ومنها المملكة العربية السعودية ، ويمكن مواجهة جميع الدول لهذه الجرائم باتباع ما يلي :

1- التعاون الدولي في مجال مكافحة الجرائم 3 .

2- حجب المواقع الإباحية .

3- إنشاء إدارات جديدة بوزارة الداخلية مسئولة عن مواجهة هذه الجرائم .

4- تفعيل دور وسائل الإعلام في التوعية .

5- تطبيق شرع الله عز وجل لتطبيق العقوبات المناسبة لهذه الجرائم من خلال الحدود و التعازير .

خلاصة الفصل الثاني:

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها ، حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية حيث أن هناك بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية كالمعاينة على مسرح الجريمة مشتركا بين الجرائم المسرح التقليدي و الافتراضي وكذا التفتيش الالكتروني وضبط الدليل الرقمي والمستحدث إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية سنة 2006 التي تعرف بأساليب التحري حيث تعتبر كل هذه الإجراءات تطبق سواء كانت الجريمة معلوماتية التقليدية (قانون الإجراءات الجزائية) ومنها إجراءات لا تطبق إلا على الجرائم المعلوماتية وهي إجراءات المحاكمة التي يخص بها الأقطاب الجزائية المتخصصة بالإضافة إلى إجراءات خاصة جاء بها قانون 09/04.

كما أن الشريعة الإسلامية تركت الباب مفتوحاً لتجريم الجرائم المستحدثة تحت قواعد وضوابط فقهية واضحة ولو أن كل المجتمعات نظرت إلى الإسلام بهذه النظرة الشمولية ، العادلة لوجدوا فيه حلا لكل معضلة وسعدوا الجميع في ظل الإسلام وعدالته وسعة رحمته المستمدة من المشرع سبحانه وتعالى ، وأدركوا الفارق الكبير بين الإسلام وغيره من الأنظمة البشرية الأخرى التي ظهر عوارها ونقصها حتى عند الدول التي تدعي التقدم والتطور والحضارة وتسمح لنفسها بالريادة لهذه المجتمعات وهذا قلب

للحقائق ، ولو فطن المسلمون لمكانتهم ولإسلامهم لكانوا بحق هم القادة والسادة والأمل في ذلك كبير – بإذن من الله عزوجل.

الخاتمة

وبعد فقد انتهينا بفضل الله وحمده من إنجاز هذه الدراسة ، ولكن لا يزال يساورنا ذلك الخاطر من أن دراسة خصوصية التحقيق الجنائي في جرائم الإلكترونية هي دراسة واسعة وشاملة لمواضيع كثيرة ، وتحتاج إلى معالجة دقيقة ومتأنية ، بحيث لا نكتفي بمجرد التعليق وإلا كانت تكريساً للجمود الفكري ، ولا تلهث وراء التصورات مهما تعددت ، وهي في جميع الأحوال لا تخلو من إعمال الفكر ولا تستغني عن التأمل . ويعد ما سبق حصيلة جهد متواضع لدراسة خصوصية التحقيق الجنائي في الجرائم الإلكترونية التي ظهرت نتيجة التطور العلمي والتكنولوجي السريع ، وثورة المعلومات الهائلة ، والتي تعتبر بلا أدنى شك من الموضوعات المهمة التي باتت الحاجة إلى دراستها بصورة جيدة ومتأنية ، من قبل العاملين والباحثين والدارسين القانونيين من قضاة وأعضاء النيابة العامة ورجال الضابطة العدلية والمحامين وغيرهم من القانونيين ، لأن هناك جرائم مستجدة في السنوات القليلة الماضية ، وظهور أساليب وطرق جديدة في ارتكاب هذه الجرائم.

ملخص

تعد الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام والاتصال الحديثة ، فهي تختلف تماما عن الجرائم التقليدية ، في ذاتية أركانها و أساليب ارتكابها والبيئة الافتراضية و اللامادية التي ترد عليها و خصوصية مرتكبها ، مما جعلها ظاهرة غريبة عن لصوص القانون الجزائي التقليدي بشقيه الموضوعي و الإجرائي ، من ثمة فأية محاولة إخضاع هذا النمط الإجرامي الجديد لإجراءات التحقيق و الإثبات المألوفة سيؤدي حتما إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية ، ويندر عنه عقبات كثيرة أمام سلطات التحقيق حيث صاحب هذا التطور م الكبير و المتسارع ظهور بعض الممارسات أو الأفعال التي من شأنها المساس ببعض الأفراد والجماعات أو المساس بأمن الدولة ، فكان على التشريعات ومن بينها التشريع الجزائري مواكبة هذا التطور وسن قوانين لمكافحة هذه الأفعال وللوقاية منها ، وإعطائها وصف التجريم وتحديد صورها والعقوبات المقررة لها ، وهو ما قام به المشرع الجزائري من خلال القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات و القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها . بالإضافة إلى نصوص أخرى نجد أثرها في قانون الإجراءات الجزائية ، لذا كان هدف هذه الدراسة البحث في تحديد مفهوم الجريمة المعلوماتية من جهة ، والبحث في

نصوص التشريعات الجزائرية عن الأركان التي يعتد بها المشرع الجزائري لقيام هذه الجريمة.

Les délits électroniques constituent l'un des nouveaux schémas criminels produits par les technologies modernes de l'information et de la communication. Ils se distinguent totalement des délits traditionnels, par la subjectivité de leurs éléments, les modalités de leur perpétration, l'environnement virtuel et immatériel auquel ils répondent, et le respect de la vie privée. de leurs auteurs, ce qui en faisait un phénomène étrange pour les voleurs de la loi pénale traditionnelle, avec ses parties substantielles et procédurales, à partir de là, la tentative de soumettre ce nouveau schéma procédural aux procédures habituelles d'enquête et de preuve conduira inévitablement à une le non-respect des exigences du principe de légalité procédurale et de nombreux obstacles aux autorités d'enquête sont rares.

Cependant, ce développement technologique important et accéléré s'est accompagné de l'émergence de certaines pratiques ou actions qui porteraient préjudice à certains individus et groupes ou porteraient atteinte à la sécurité de l'État. La législation, y compris la législation algérienne, a dû suivre le rythme de cette évolution et promulguer des lois combattre ces actes et les prévenir, leur donner une description de l'incrimination et préciser ses formes et les peines prescrites, c'est ce qu'a fait le législateur algérien à travers la loi n°15-04 du 10 novembre 2004 portant modification du Code pénal et Loi n°09-04 du 05 août 2009 portant règles particulières de prévention et de répression des infractions liées aux technologies de l'information et de la communication. Outre d'autres textes, on retrouve leur impact sur le Code de procédure pénale, ainsi l'objectif de cette étude était de rechercher dans la définition de la notion de délit d'information d'une part, et de rechercher dans les textes de la législation algérienne sur les piliers sur laquelle le législateur algérien s'est appuyé pour établir ce crime.

المصادر والمراجع

القوانين:

1- قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 صادر بتاريخ 16/08/2009 ،

2- قانون رقم 18-07 المؤرخ في 10 جوان 1430 سنة 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ج ر.ع 34 .

الأوامر:

1- لأمر رقم 56- 155 المؤرخ في 18 صفر عام 1385 الموافق 8 يونيو 1956 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم

المراسيم:

1- مرسوم رئاسي 04-183 المؤرخ في 2004/06/26 يتضمن احداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني و تحديد قانونه الأساسي ، الجريدة الرسمية عدد 41 الصادرة في 2004/06/27

2- مرسوم رئاسي رقم ،10-100مؤرخ في 2جوان 2010 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها و كيفيات سيرها، ج ر، بتاريخ جوان 2010.

3- مرسوم رئاسي رقم ،021-11مؤرخ في 2اكتو ر ،0211يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد ،10الصادرة بتاريخ 2اكتوبر 2011

4- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53، 8 أكتوبر 2015.

5- مرسوم رئاسي رقم 05-20 المؤرخ في 20 جانفي 2020 ،يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04 الصادر فيفي 26 جانفي 2020

6- مرسوم رئاسي رقم ،120-02مؤرخ في 10جويلية ، 2020يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد ،22الصادرة بتاريخ 12جويلية 2020

7- مرسوم رئاسي رقم 20-183 المؤرخ في 13 يوليو 2020 يتضمن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال و مكافحتها، ج ر عدد 40 الصادرة 18 يوليو 2020

الكتب بالعربية

الكتب العامة

1- ابن تيمية نهاية المحتاج 7/175 ، وحاشية الباجوري على ابن قاسم الغزي 2/234 ، والمغني 8/334 ، والساسة الشرعية ، ط دار علم الموائد النشر والتوزيع

2- ابن رشد بداية المشهد وقاية المقتصد 199، تحقيق أبو عبد الرحمن عبد الحكيم بن محمد ط المكية التوفيقية القاهرة.

3- أحسن بوسقيعة. التحقيق الفضائي ط 10 دار هومة 2012.

4- شرح فتح القدير للكمال من المسام الحنفي 120 / 5 ط دار إحياء التراث العربي.

5- طارق عبد الله الشدي ، آلية البناء لنظم المعلومات ، دار الوطن للطباعة والنشر ، الرياض 1423 هـ

6- عبد العالي الديربي الجرائم الإلكترونية المركز القومي للاصدارات القانونية –القاهرة–2012

7- محمد الغزال هذا ديننا ص 229– 3حسان القاهرة 1395 هـ 1975 م.

8- محمد حزيط . مذكرات في قانون الاجراءات الجزائية الجزائري ط 08 دار هومة 2013.

9- محمد على العريان – الجرائم المعلوماتية – – دار الجامعة الجديدة للنشر –سنة 2004

10- منصور بن يوسف الروض المربع شرح زاد المستقنع في اختصار المقنع للشيخ البهومي 439 ، ط دار الفكر بيروت.

الكتب المتخصصة:

1- جميل ع الباقي صغير ،الجوانب الاجرائية للجرائم المتعلقة بالانترنت ،دار النهضة العربية.

2- خالد عباد الحلبي إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت –دار الثقافة للنشر والتوزيع عمان ط1 2011.

3- خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية،ط 1، دار الفكر الجامعي ، الاسكندرية ، 2009.

4- عبد الله أوهايبة ، شرح قانون الاجراءات الجزائية الجزائري، دار هومة الجزائر ط2 2011.

5- عبده جميل غصوب ، الوجيز في قانون الإجراءات الجزائية . ط 1 ، المؤسسة الجامعية للنشر والتوزيع : بيروت . 2011.

6- عفيفي كامل جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية دار نشر منشورات الحلبي الحقوقية 2003.

7- على عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، ط 1 ، دار الجامعة الجديدة للطباعة والنشر : بيروت ، .1999

8- محمد الأمين البشري : التحقيق في جرائم الحاسب الآلي ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة (1) 2000 / 5 / 3 م الطبعة الثالثة 2004 م.

9- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت)، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع ،مصر، ،2010.

10- مصطفى محمد موسى – التحقيق الجنائي في الجرائم الإلكترونية – مطابع الشرطة – القاهرة – الطبعة الأولى.

11- هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، 1994.

مذكرات تخرج :

1- بختي فاطمة الزهراء – إجراءات التحقيق في الجريمة الإلكترونية – مذكرة لنيل شهادة الماستر– جامعة محمد بوضياف المسيلة ، السنة الجامعية 2013 – 2014.

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

3- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية،جامعة باتنة ،2016.

4- سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجستير ، تخصص علوم جنائية ، جامعة الحاج لخضر باتنة ، السنة الجامعية 2012 – 2013.

5- سليمان بن مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجستير – جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2003.

6- عبد الرحمن بحر : معوقات التحقيق في جرائم الإنترنت " دراسة مسحية على ضباط الشرطة بدولة البحرين ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، الرياض 1999.

7- عبد الله دغش العجمي ، المشكلات العملية والقانونية للجرائم الإلكترونية ، دراسة مقارنة ، رسالة مكملة للحصول على درجة الماجستير في القانون العام ، جامعة الشرق الأوسط ، 2014.

8- عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي . مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، 2007.

9- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية كلية الحقوق ، لبنان ،2004.

المقالات

1- سلطان عمار، السلطات الادارية المستقلة في الجزائر، مجلة جيل للأبحاث القانونية المعمقة، العدد ،33 ،2010

2- مقال بعنوان" إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، الأربعاء 14 ديسمبر 2016، وكالة الأنباء الجزائرية، على الموقع الالكتروني www.aps.dz/sante.science

المداخلات :

1- حملاوي عبد الرحمان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر

2- زكي أمين حسونه ، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي ، المؤتمر السادس للجمعية المصرية للقانون الجنائي

3- عرض مقدم من طرف : عز الدين ، المعهد الوطني للأدلة الجنائية ، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، الملتقى الوطني حول

الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر

4- عرض مقدم من طرف : هواري عياش ، المعهد الوطني للأدلة الجنائية ، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ، يومي 17/16 نوفمبر 2015 بسكرة، الجزائر

5- عزالدين عزالدين ، الاطار القانوني الوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية ، بسكرة في 16/11/2015

6- مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الالكترونية تم حلها بنجاح، موقع الاذاعة الجزائرية، 2019/05/25 على الساعة 15:34

7- هشام محمد فريد رستم ، الجرائم المعلوماتية " أصول التحقيق الجنائي الفني ، مؤتمر القانون والكمبيوتر والإنترنت ، المنعقد بكلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة في الفترة من 1-2000 / 5 / 3

المصادر والمراجع باللغة الأجنبية:

1- Johm Eaton and Jeremy Smithers . This is it a Managers Guide to information Technology . London , Philip Allan , 1982.
2- Mohrenschlager “ Manfred " : computer crimes and other crimes against information techmology in Germany . Rev. inter . De . Dr. Pen . 1993.
3- Peter Tillers . Introduction to program on Artificial intelligence N.Y Yeshiva University Press . 1999
4- United Nation . United Nation Manusl on the prevention and control of Computer - Related crime : Viennal 1999

أهمية الدراسة	ا
أهداف الدراسة	ا
أسباب اختيار الموضوع	ا
إشكالية الدراسة	ب
منهج الدراسة	ب
صعوبات الدراسة	ج
تقسيم الدراسة	ج
مقدمة	
الفصل الأول: ماهية الجريمة الإلكترونية ،أركانها ،دوافعها و أجهزة مكافحتها	
تمهيد	01
المبحث الأول: ماهية الجرائم الإلكترونية و دوافع ارتكابها	02
المطلب الأول: مفهوم الجريمة الالكترونية و أركانها	02
الفرع الأول: تعريف الجريمة الالكترونية و أركانها	02
الفرع الثاني :أركان الجريمة الإلكترونية	04
المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية	05
أولا :السعي إلى تحقيق الكسب المالي	06
ثانيا :الرغبة في الانتقام و إلحاق الضرر	06
ثالثا: الرغبة في قهر النظام و التفوق على تعقيد وسائل التقنية	07
رابعا : الرغبة في التعليم	07
خامسا: المنافسة	08
سادسا: التهديد الأمني	09
سابعا: الدوافع الأخرى	09
المبحث الثاني: أجهزة التحقيق في الجرائم الإلكترونية	10
المطلب الأول: الهيئات المكلفة بالتحقيق في الجرائم الإلكترونية	10

الفرع الأول: الهيئات القضائية الجزائية المختصة	10
أولا: إنشاء الهيئات القضائية الجزائية المتخصصة	10
ثانيا: توسيع صلاحيات ضباط الشرطة القضائية	13
الفرع الثاني: الهيئات غير القضائية	13
أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال	14
1- مفهوم الهيئة	14
2- مقر الهيئة	16
3- مهام الهيئة	17
4- تنظيم الهيئة	18
5- سير الهيئة	20
ثانيا : السلطة الوطنية لحماية المعطيات ذات طابع شخصي	21
ثالثا : وكالة أمن الأنظمة المعلوماتية	25
سير الوكالة	25
المطلب الثاني: الوحدات المكلفة بالتحقيق في الجرائم الإلكترونية	26
الفرع الأول: وحدات الدرك الوطني	26
أولا : المعهد الوطني للأدلة الجنائية و علم الإجرام INCC /GN	26
ثانيا:مركز الوقاية من جرائم المعلوماتية و مكافحتها CPLCIC/GN	28
ثالثا : المصلحة المركزية للتحريات الجنائية SCIC/GN	29
الفرع الثاني: وحدات الأمن الوطني	29
أولا: المخابر	30
ثانيا : وجود فرقة على مستوى كل أمن ولاية	31
ثالثا :دور المديرية العامة للأمن الوطني في مواجهة الجرائم الالكترونية	33
خلاصة الفصل الأول	35

الفصل الثاني: إجراءات التحقيق في الإلكترونية ،صعوباتها و الحلول المقترحة لذلك	
تمهيد	36
المبحث الأول: إجراءات التحقيق في الجرائم الإلكترونية و الصعوبات التي تواجهها	37
المطلب الأول : ماهية التحقيق في الجريمة الإلكترونية	38
الفرع الأول : تعريف التحقيق و المحقق وخصائص كل منهما	38
أ– تعريف التحقيق	38
ب – تعريف المحقق وخصائصه الفنية	40
أولا : تعريف المحقق	40
ثانيا : الخصائص الفنية للمحقق	42
ج– خصائص التحقيق في الجريمة الإلكترونية	45
الفرع الثاني : الإجراءات التي يباشرها قاضي التحقيق في الجريمة المعلوماتية	46
أولا : المعاينة في الجريمة المعلوماتية	46
01 : الانتقال للمعاينة (انتقال قاضي التحقيق للمعاينة)	47
02:الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة المعلوماتية	49
03 : شروط صحة معاينة مسرح الجريمة	49
ثانيا : التفتيش في الجريمة المعلوماتية	50
ثالثا: الاستجواب والشهادة وضبط الأدلة في الجريمة المعلوماتية	52
01–استجواب المتهم	53
02–الشهادة الالكترونية	54
03–ضبط الدليل في مجال الجريمة المعلوماتية	54
المطلب الثاني: صعوبات التحقيق في الجرائم المعلوماتية	55
أولا : عوائق تتعلق بالجريمة المعلوماتية	56
ثانياً : عوائق تتعلق بالجهات المتضررة	58

ثالثاً : عوائق تتعلق بجهات التحقيق	60
رابعاً : عوائق تتعلق بإجراءات الحصول على الدليل الإلكتروني	65
المبحث الثاني :سبل مواجهة الجرائم الإلكترونية في الشريعة الإسلامية والأنظمة الدولية	69
المطلب الأول : سبل مواجهة الجرائم الإلكترونية في الشريعة الإسلامية	70
أولا : الجانب الوقائي	70
ثانيا : الجانب العلاجي	71
ثلثا:الجانب التطبيقي لمواجهة جريمة السرقة الإلكترونية في الشريعة الإسلامية	76
المطلب الثاني : سبل مواجهة الجرائم الإلكترونية في الأنظمة الدولية	78
خلاصة الفصل الثاني	83
الخاتمة	85
ملخص	86
المصادر و المراجع	
الفهرس	