جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

البحث والتحري حول الجريمة المعلوماتية في التشريع الجزائري

مذكرة لنيل شهادة الماستر في العلوم القانونية
تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبتين:
- مسعودة سولاف تواتي
- حفيظة بلحديد

إشراف الأستاذ:
د/ صغير يوسف

لجنة المناقشة

الأستاذ(ة) د/خليفي سمير.....رئيسا
الأستاذ(ة): د/ صغير يوسف: أستاذ مساعد قسم "أ".....مشرفا ومقررا
الأستاذ(ة): د/ قاسة عبد الرحمان.....ممتحنا

السنة الجامعية: 2022/2021

الإهداء:

أهدي هذا العمل المتواضع إلى من أوصاني بهما ربي برا وإحسانا، إلى

العزيزين أمي وأبي أطال الله في عمرهما.

وإلى أخواتي وكل أساتذتي

وإلى جميع أصدقائي.

مسعودة سولاف تواتي

الإهداء:

أهدي ثمرة جهدي هذا إلى الوالدين الكريميّن أبي العزيز رحمه الله وأمي العزيزة أطال الله في عمرها، وإلى زوجي العزيز وإلى أبنائي أحمد، أنيس آية الرحمان.

إخواني وأخواتي وزملائي في العمل.

حفيظة بلحديد

كلمة شكر

نشكر الله سبحانه وتعالى، ابتداء واعترافا بالفضل والجميل نتوجه بالشكر الجزيل إلى أستاذنا المشرف"يوسف صغير" الذي أشرف على هذا العمل وتتبعنا فيه بالنصائح و الإرشادات، وأخذ بأيدينا أثناء إنجازه خطوة بخطوة إلى أن تم واكتمل بحمد الله، فجزاه الله كل خير.

مسعودة سولاف تواتي

حفيظة بلحديد

قائمة المختصرات

باللغة العربية :

ق.ا.ج.ج : قانون إجراءات الجزائية الجزائري

د.س.ن : دون سنة النشر

د.ب.ن : دون بلد النشر

ط: طبعة

ص : صفحة

ص ص: من صفحة إلى صفحة

باللغة الأجنبية

FBI : federal bureau of Investigation .

UsDoJ : département de la justice des ETAS-UNIS.

IP : internet protocol.

مقدمـــــة

إن مجال الجريمة متطور على الدوام تطور الحياة وأساليبها وظروفها، فالجرائم التي كانت ترتكب في العصور الأولى غير التي ارتكبت في العصور التي ما بعدها لاختلاف نمط الحياة وحاجات الإنسان، ففي الماضي كان يسعى إلى ضمان بقائه عن طريق الصراع من أجل البقاء، وبعد التطور الحاصل في المجتمعات تطورت تطلعات الإنسان بتطور مجالات الحياة، وكذلك بتطور واختلاف الزمان والمكان.

حيث في الماضي كانت ترتكب جرائم تقليدية معهودة وضعت لها قوانين وقواعد تحكمها، كما سلط لها المشرع عقوبات ملائمة لطبيعتها وجسامتها كجرائم السرقة والقتل والتهريب والاختطاف على سبيل المثال وكان المشرع قد عالج هذه الجرائم بنصوص تجريمية وأخرى إجرائية من أجل الوصول إلى كشف الحقائق ومعاقبة الجاني.

و لقد أثار البحث عن هذه الجرائم مشاكل وصعوبات في استخلاص الأدلة التي تثبت وقوعها وتدين مرتكبيها كونها تختلف عن الأدلة التقليدية في الجرائمالعادية من حيث خصائصها وأنواعها وسبل جمعها ووسط ارتكابها وحتى صفات مرتكبيها، كما يثير الدليل الإلكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي وفقدان الآثار التقليدية للجريمة المعلوماتية، بالإضافة إلى صعوبات متعلقة بسلطات الاستدلال والتحقيق من حيث إحجامهم عن الإبلاغ حرصا على ثقة العملاء أو لصعوبة اكتشافها من قبل الأشخاص العاديين، فضلا عن نقص خبرة سلطات الاستدلال والتحقيق.[1]

أثارت الجريمة المعلوماتية العديد من المشكلات في نطاق قانون الإجراءات بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها ، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي ، وكذلك يثير تساؤلات عديدة حول مشروعية وجود الدليل الإلكتروني ومشروعية الحصول عليه وأدلة الإدانة ذات نوعية مختلفة.

[1]) **نايري عائشة**، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية ، جامعة احمد دراية، أدرار 2016-2017، ص1.

فهي معنوية الطبيعة كسجلات الحاسوب ومعلومات الدخول والنفاذ والبرمجيات، وقد أثارت أمام القضاء مشكلات من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية، إذا فإن البعد الإجرائي لجرائم الحاسوب والانترنيت ينطوي على تحديات ومشكلات عناوينها الرئيسية.

تأثرت الجريمة بالتقدم العلمي والتكنولوجي المعاصر وبرزت أساليب إجرامية بتقنيات لم تكن معروفة من قبل، وطُوعت التقنيات الحديثة لارتكاب الجريمة في مراحلها المختلفة من تخطيط وإعداد وتنفيذ وتحليل وتمويه لإفلات من العدالة فاستخدمت الأجهزة والأدوات والتقنيات الحديثة في ارتكاب الجرائم التي تميزت بالعنف و من الطبيعي أن يصاحب التقدم العلمي ظهور أنماط من الجريمة لم تتضمنها التشريعات العقابية القائمة.

وتبدو النصوص الجزائية قاصدة عن ملاحقتها ذلك أن التشريع وليد الحاجة لذا لم تتطرق التشريعات العربية إلى الجرائم المعلوماتية إلا نادرا، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية لم تتعدَ العقد الواحد وإن كان دخوله إليها قد بدأ قبل ذلك بفترة طويلة نسبيا، وتكمن صعوبة التعامل مع الجرائم المعلوماتية في صعوبة إجراء التفتيش القانوني، فإذا كانت الجريمة واقعة على المكونات المادية للكومبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجرائم واقعة على برامج الحاسب وبيانتاه فإن الصعوبات تظهر على اعتبار أنه بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر.[1]

أسباب اختيار الموضوع:

من أهم أسباب اختيار الموضوع مايلي: إن البحث والتحري في الجرائم المعلوماتية موضوع مستجد، فالبحث في فعالية هذه الإجراءات وتقدير مدى مساسها بحقوق الأفراد ممن شاءت

[1]) **بخي فاطمة الزهراء**، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق،تخصص قانون جنائي، جامعة المسيلة2013-2014

أقدارهم أن تتخذ هذه الإجراءات في حقهم دون أن يثبت عليهم بعد ذنب جنائي ارتكبوه، أو الغير الذي لا تربطه أي رابطة بالجريمة يعتبر نقطة البداية للخوض في تنظيمها وبيان ضوابطها، فهذ الإجراءات لم تحظَ بعد الاستقرار في مسائلها على النحو الذي حظيت به إجراءات التحري التقليدية هذا الذي دفعنا لاختيار الموضوع .

أهمية الموضوع:

يعد موضوع هذا البحث من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي، ونظرا لحداثة الجرائم المعلوماتية واتصالها بجانب تقني وفني بحث يمثل في النظام المعلوماتي بشقيه المادي والمعنوي، وما يزيد الموضوع أهمية هو خطورة هذه الجريمة وانتشارها بسرعة رهيبة وعجز القوانين التقليدية على مواكبة هذه السرعة.

هدف هذه الدراسة:

ينبع الهدف من هذه الدراسة من محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن حداثة الجرائم المعلوماتية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها

وبالتالي فالإشكالية المطروحة مع معالجة هذا الموضوع تتمثل في: كيف نظّم المشرع الجزائري آليات البحث والتحري لمعالجة الجريمة المعلوماتية في التشريع الجزائري ؟

وللإجابة على هذه الإشكالية قسمنا البحث إلى فصلين اعتمدنا في ذلك على المنهج التحليلي في دراستي هذه، لتبيان كل من مفهوم الجريمة المعلوماتية والتحقيق والاستدلال، ومناقشة الإجراءات المتخذة للتصدي لهاته الجريمة المستحدثة.

الفصل الأول بعنوان الاستدلال والتحقيق حول الجريمة المعلوماتية، حيث عالجت **الاستدلال في المبحث الأول منه والذي قسمنا إلى مطلبين، خصصت المطلب الأول لدراسة تلقي البلاغات والشكاوى، والاستجواب وسماع الشهود حول الجريمة المعلوماتية كمطلب ثانٍ.**

أما المبحث الثاني من هذا الفصل فقد تناولنا فيه التحقيق في الجريمة المعلوماتيةمن حيث الأجهزة المكلفة بالبحث والتحري كمطلب أول، والمطلب الثاني ذكرت فيه خصائص التحقيق والمحقق، أما المطلب الثالث منه تناولنا فيه الدليل المناسب لإثبات الجريمة المعلوماتية.

الفصل الثاني بعنوان: آليات البحث والتحري حول الجريمة المعلوماتية.

بينت في المبحث الأول منه إجراءات الحصول على أدلة إثبات الجرائم المعلوماتية فيما يتمثل في الاجراءات التقليدية، والمبحث الثاني لهذا الفصل تناولت فيه عقبات البحث والتحري حول الجريمة المعلوماتية حيث تكلمت عن العقبات التقنية كمطلب أول، وعقبات متعلقة بالجاني والضحية وسلطات الاستدلال البشرية في المطلب الثاني، أما المطلب الثالث تحدثت عن العقبات المتعلقة بجهات التحقيق

الفصل الأول:

الاستدلال والتحقيق حول الجريمة المعلوماتي

إن الجريمة ظاهرة اجتماعية مرتبطة ارتباطا بأعضاء المجتمع وعاداتهم وتقاليدهم، لذا نجد أن الجريمة تتطور بسرعة وفق متغيرات معينة، وتتجاوز غالبا سرعة حركة المجتمع، وخاصة في هذا العالم الذي أصبحت فيه المجتمعات مفتوحة على مساحات واسعة، وهي بذلك تتعرض للمؤثرات التي لا تحدها حدود في ظل ما يعرف بالعولمة، وسبب ذلك هو تداخل المجتمعات الذي فرضه التطور التكنولوجي، وهذا الأخير يدعو إلى متابعة المستجدات التي تطرأ على الجريمة في موضوعها وإجراءاتها فكلما تطورت الجريمة بأساليبها وطرقها كلما لزم الأمر تطوير سبل مكافحتها لتلك الجرائم والتحقيق فيها.

يعد الاستدلال والتحقيق الجنائي من الأنشطة الأمنية التي تأتي في مقدمة محاولات المواجهة لتلك الظواهر الإجرامية عن طريق العلوم والتكنولوجيا الحديثة، ولا شك أن القواعد والإجراءات القانونية للتحقيق تبدأ من تلقي البلاغ عن وقوع الجريمة مرورا بالإجراءات التي يتخذها المحقق من أجل الكشف عن غموضها وضبط الفاعل وإسناد الاتهام إليه شريطة أن يكون ذلك وفقا للقانون الذي يحدد ويضبط هذه الإجراءات ومن هنا سنتطرق إلى الاستدلال حول الجريمة المعلوماتية في المبحث الأول، والتحقيق حول الجريمة المعلوماتية في المبحث الثاني.

المبحث الأول: الاستدلال حول الجريمة المعلوماتية.

تتجسد أول طرق مكافحة الجرائم المعلوماتية في الاستدلال الذي يتضمن الاستجواب وسماع الشهود وتلقي البلاغات والشكاوى.

المطلب الأول: تلقي البلاغات والشكاوى

تتسم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأنها خفية ومستترة في أغلبها، فالضحية لا يلحظها رغم أنها قد تقع أثناء وجوده على الشبكة لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، الأمر الذي يجعل من وقعها تحت وصف التلبس أمرا نادرا –إن لم نقل مستحيلا–[1].

إن تقديم البلاغ يشكل أهمية بالغة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نظرا للطابع الخفي الذي تتميز به هذه الطائفة من الجرائم من جهة، ومن جهة أخرى للإحجام عن الإبلاغ عنها خاصة في مجتمع الأعمال، فتحجم أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك عن الكشف حتى بين موظفيها عما تعرضت له من اعتداء، وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.

وعليه سأتناول البلاغ والشكوى عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في الفرع الأول، أما الفرع الثاني أخصصه لآليات التبليغ عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الأول: البلاغ والشكوى في الجرائم المعلوماتية:

تظل هذه الجرائم مستترة عادة–مالم يتم التبليغ عنها إلى الجهات المختصة بتحريك الدعوى العمومية والتحقيق فيها، حسب القوانين والأنظمة المعمول بها.

---

[1])_**عبد المؤمن بن صغير**، الطبيعة الخاصة للجريمة المرتكبة عبر الإنترينت في التشريع الجزائري والمقارن، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بتاريخ 16و17 نوفمبر2015، كلية الحقوق،جامعة بسكرة، صفحة 08.

ويعد الإبلاغ عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حقا لكل شخص علم بها، ولم يكن متضررا منها أو ذا مصلحة فيها ، ولا يترتب على عدم القيام به أية مسؤولية جزائية، إلا في جرائم معينة يوجب القانون التبليغ عنها،وإلى جانب البلاغات يتلقى ضباط الشرطة القضائية الشكاوى من المتضرر من الجريمة أو نائبه القانوني[1].

وفي هذا الصدد نصت الفقرة الأولى من المادة 17 المعدلة بموجب الأمر 15-02 من قانون الإجراءات الجزائية على أنه:"يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية".[2]

ولمعرفة كيفية الإبلاغ عن هذه الجرائم يستوجب التطرق إلى البلاغ (أولا) ومن ثم التعرض إلى الشكوى(ثانيا)

أولا: البلاغ في الجرائم المعلوماتية:

لدراسة البلاغ عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يتعين تعريف البلاغ والتطرق إلى صعوبات تلقي البلاغ في هذا النوع من الجرائم.

1-تعريف البلاغ: يتم البلاغ بكافة السبل التي توصل المعلومات إلى الجهات المختصة بالبحث والتحري والتحقيق، فقد يتم كتابيا أو شفويا بمعرفة المجني عليه أوّ أحد الشهود أو ممن يبلغ عن جريمته، ويصطلح على البلاغ في هاتين الحالتين بال"بلاغ المادي" وقد يقدم بواسطة البريد أو الهاتف أو الصحف وهذا ما يصطلح عليه بالبلاغ المعنوي ، أو يقدم عبر الإنترنيت ويسمى

[1])_**محمد الأمين البشري**،التحقيق في جرائم الحاسب الآلي والأنترينت، المجلة العربية للدراسات الأمنية، العدد الثلاثون، أكاديمية نايف العربية للعلوم الأمنية،2000، صفحة 349.

[2])-انظر الى المادة 17 من قانون الاجراءت الجزائية .

بالبلاغ الرقمي، وهنا يرى البعض أنه يمكن إرسال البلاغ عبر رسالة البريد الإلكتروني لشبكة الإنترنيت للجهة المختصة[1].

ويقدم البلاغ لضابط الشرطة القضائية من شخص معلوم أو غير معلوم الشخصية، ويجب على ضباط الشرطة القضائية في الحالتين ولا سيما الأولى منها تناول البلاغ بجدية كاملة.

وحتى يكون البلاغ وافيا لا بد أن تتوفر فيه العناصر التالية: نوع الحادثة، وتحديد المجني عليه، ووقت وقوع الجريمة، وبيان الأسباب و الدوافع لارتكاب الجريمة وتحديد الشخص المتهم[2].

ويستحب أن يكون المبلغ في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على درجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب، حتى يتمكن من تقديم معلومات تصف الحادث بالشكل الذي يمكن معه لضباط الشرطة القضائية من مباشرة البحث والتحري عنها، إذ تعين عليه أن يقدم وصفا علميا محددا للنشاط الإجرامي مع بيان الأسماء واللغات والبرامج وأنواع الأجهزة المستخدمة وأماكنها قدر المستطاع[3]، وهو ما يستزم أن يكون متلقي البلاغات على قدر من المعرفة بتكنولوجيات الإعلام والاتصال، حتى يتمكن من مناقشة المبلِّغ في الكثير من جوانب الجريمة محل البلاغ.

2-صعوبات تلقي البلاغ في الجرائم المتصلة بتكنولوجيات الإعلاموالاتصال:

ترجع أسباب صعوبة البلاغ في هذا النوع من الجرائم إلى أن الأشخاص والمؤسسات والشركات تحاول درء الأثر السلبي للإبلاغ حرصا على ثقة العملاء، كما أن آثار هذه الجرائم

[1])**سليمان أحمد محمد فضل**، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية(الإنترنت)، رسالة دكتوراه من كليات الدراسات العليا بأكاديمية الشرطة، القاهرة،2007، ص277.

[2])**خالد حازم إبراهيم**، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية(الإنترنت)، دراسة مقارنة ، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع د. ب. ن نوفمبر 2014، ص212.

[3]**محمد الأمين البشري**، مرجع سابق، ص355.

وأدلتها لا يظهر في أغلب الحالات، وإذا ظهرت فلا يستوضحها إلا متخصص في الحاسب الآلي وتقنيات المعلوماتـ الذي يملك معرفة بنظم الاتصالات وشبكة الإنترنيت، وهو ما قد لا يتوافر في ضحايا هذه الجريمة.

كما يرجع سبب عدم الإبلاغ عن هذه الجرائم من طرف المجني عليه وأفراد المجتمع عموما إلى شكهم في قدرة الجهات الشرطية في التعامل مع التقنيات الحديثة في هذا الشأن والوصول إلى الجناة، هذا من جهة ومن جهة أخرى قد يرجع عدم الإبلاغ عن هذه الجرائم إلى عدم دراية أفراد المجتمع بأن هذه الوقائع مُجرّمة أو أن عادات وتقاليد المجتمع لا تتفق مع الإبلاغ عن هذه الجريمة[1]

وبالتالييجب تطوير ثقافة تكنولوجيات الإعلام والاتصال وسط رجال الأمن وربط تلك الثقافة بالثقافة الأمنية التقليدية لكي تكفل للأجهزة الأمنية نجاحا في مواكبة ظاهرة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ثانيا: الشكوى في الجرائم المعلوماتية:

إلى جانب البلاغات، يتلقى ضباط الشرطة القضائية الشكاوى من المتضررين من الجريمة، وهو الأمر الذي يتطلب التطرق إلى تعريف الشكوى ومن ثم معرفة أحكامها في الجرائم المعلوماتية.

1-تعريف الشكوى:

يقصد بالشكوى "البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة حظر المشرع تحريكها قبل تقديمها[2]، أي أن هناك بعض الجرائم حددها المشرع على سبيل الحصر، لا يمكن تحريك

[1])_**خالد حازم إبراهيم**، المرجع السابق، ص212.

[2])**أحمد شوقي الشلفاني**، مبادئ الإجراءات الجنائية في التشريع الجزائري، جزء1، طبعة3، ديوان المطبوعات الجامعية-الجزائر، 2003، ص41.

الدعوى العمومية فيها إلا بعد تقديم شكوى من قبل المجني عليه أو وكيله الخاص[1]ومن بين هذه الجرائم ما يرتكب عن طريق تكنولوجيات الإعلام والاتصال كجريمة النصب المعلوماتي، فهل يا ترى تختلف أحكام الشكوى فيها؟

2-أحكام الشكوى في الجرائم المعلوماتية:

لا تختلف أحكام الشكوى في الجرائم التقليدية عن تلك المطلوبة في الجرائم التي ترتكب عن طريق منظومة معلوماتية ، إذ لا يجوز للجهات المختصة تحريك الدعوى العمومية في تلك الجرائم إلا بعد تقديم شكوى من المجني عليه أو المتضرر منها أو من وكيله الخاص ضد المتهم.

ونظرا لصعوبة تحديد الشخص الجاني أو المتهم في هذا النوع من الجرائم، فإنه يذهب البعض إلى ترتيب المسؤولية على مزود الدخول أو خدمات الإنترنت عن تلك الجرائم مستندين في ذلك على مبدأ افتراض مسؤولية الغير[2]، وهذا ما جعل موضوع الشكوى في هذه الجزائم محل جدل قانوي، وخصوصاإذا علمنا أن تقديم الشكوى من قبل المجني عليه قد يوجه إلى السلطات العامة ضد مزودي خدمات الأنترنت دون حاجة إلى متابعة التحريات لمعرفة الجاني الحقيقي.

غير أنه من جانبنا أرى أنه بالرغم من انتشار الأسماء المستعارة أو التخفي أو انتحال الشخصية عبر الأنترنت، إلا أنه يمكن من خلال تحديد مسار الأنترنت معرفة الحاسوب الذي تم من خلال ارتكاب الفعل المجرم والوصول إلى الجاني وبالتالي توجيه الشكوى ضده وليس ضد مزود خدمات الأنترنت.

---

[1])_**حبيباتي بثينة**، الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، اطروحة لنيل شهادة الدكتوراه ل.م.د في القانون العام، تخصص قانون جنائي وعلوم الاجرام، كلية الحقوق و العلوم السياسية ، جامعة الجزائر1، 2020، ص278.

[2]**نبيلة هبة هروال**، جرائم الانترنت، دراسة مقارنة، أطروحة الدكتوراه، جامعة ابي بكر بلقايد، تلمسان،2013-2014 ص192.

كما أن الإشكال الثاني المطروح يتعلق بمدى قبول الشكوىإذا كان المجني عليه قد تعرض إلى نصب من الجاني في الوقت الذي كان يستخدم فيه اسما مستعارا عبر الانترنيت؟

تضارب الآراء حول الإجابة عن هذا الإشكال، إذ يتجه رأي قبول شكوى المجني عليه عندما يكون في حالة تخفي دون أية عوائق في هذا الإطار، وهناك من يرى إجازة ذلك في حالة واحدة، وهي حالة إذا ما كان الغرض من الاستعارة مشروعا[1].

وحسب ظننا أن الرأي الثاني هو الأقرب إلى الصواب حيث يمكن للجهات المختصة قبول الشكوى المقدمة من الشخص المتضرر في حالة استخدام اسم لغرض مشروع.

الفرعالثاني : آليات التبليغ عن الجرائم المعلوماتية:

ساهمت شبكة الإنترنيت كوسيلة بالغة الأهمية في تطوير الاتصال بين أفراد ومؤسسات المجتمع، وتطور معها نظام تقديم البلاغ عبر التوجه موقع خاص بالبلاغات وكتابة بيانات الجريمة ثم بثه إلى الجهات المختصة كما هو الحال في موقع المباحث الفيدراليةFbi، وكذلك إدارة العادل الأمريكية USDOJ، وموقع شرطة دبي... إلى غيرها من المواقع التي تخص الضبط القضائي المختص بتلقي البلاغات.

إلا أن الإشكال الذي يمكن أن يطرح في هذا المقام يتعلق بالقيمة القانونية لمثل هذه التبليغات الرقمية أو الإلكترونية، وبمدى قبول الضبطية القضائية مثل هذا النوع من التبليغات؟

وعليه سأتعرض فيما يلي إلى دراسة البلاغ عن الجرائم المعلوماتية(أولا) ثم أتعرض إلى الضوابط الفنية للتصرف في البلاغ الرقمي(ثانيا).

أولا: الإخطار عن الجرائم المعلوماتية:

الجدير بالذكر أن التبليغ عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لا يختلف عما هو الحال في مجال الجرائم التقليدية، وإن كان يتمتع بنوع من الخصوصية تتماشى بطبيعة هذه الجرائم، فالبلاغ في هذه الحالة قد يتم عن طريق شبكة الأنترنت أو ما يسمى بالبلاغ

[1] **عمر محمد أبو بكر بن يونس**، المرجع سابق، ص836.

الرقمي أو الإلكتروني، وذلك إما عن طريق إرسال رسالة إلكترونية أو عن طريق ملء بيانات الاستمارة الرقمية.

1-الإخطار عن طريق رسالة إلكترونية:

تتمثل هذه الطريقة في كتابة رسالة إلكترونية تتضمن الإبلاغ غن جريمة متصلة بتكنولوجيات الإعلام والاتصال، وإرسالها إلى عنوان البريد الإلكتروني العائد لأحد الجهات المختصة بالبحث والتحري لإبلاغها عن نشر فيروسات تخريبية عبر شبكة الإنترنت أو وجود صفحات أو مواقع غير مشروعة كإرسال رسالة تتضمن التبليغ عن وجود موقع منشور فيه صور للاستغلال الجنسي للأطفال إلى عنوان البريد الإلكتروني للدرك الوطني الفرنسي Judiviaire@gendarmeriedefense-gouv.fr باعتباره الجهة المختصة بالتحري والتحقيق عن تلك الجرائم في فرنسا أو إلى موقع شرطة إدارة مكافحة جرائم الحاسبات وشبكات المعلومات المخصص لتلقي البلاغات والشكاوى في مصر.[1]

2-الإخطار عن طريق ملء استمارة رقمية:

يتم التبليغ عن طريق ملء بيانات الاستمارة الرقمية التي تكون متواجدة عادة على المواقع الإلكترونية المخصصة لتلقي تلك البلاغات والشكاوى، كتلك التي يوفرها موقع مركز الشكاوى الخاصة بجرائم الأنترنت C3[2] أو البوابة الرسمية للإبلاغ عن المحتوى غير المشروع للأنترنت في فرنسا[3] أو تلك المتوفرة على موقع وزارة الداخلية السعودية.

---

[1])_**نبيلة هبة هروال**، ، مرجع سابق، ص182-181

[2] _)الموقع الرسمي لمركز الشكاوى الخاصة بجرائم الأنترنت:https://comlaint-ic3.gov/default.aspx تاريخ الدخول 2019/01/03

[3])_https://www.intenet-signalement-gouv.fr/portalweb/planets/signalerEtap choix Type contenu!input action.

date de consultation:07/06/2017

ويستوجب لملء تلك الاستمارة التوضيح والتدقيق في المعلومات المحصل عليها لتسهيل عملية التأكد من قبل الجهات المختصة.

ثانيا: الضوابط الفنية للتصرف في البلاغ الرقمي:

تؤثر دقة تلقي البلاغ في هذه الجرائم في مساعدة رجال الضبط القضائي لوضع التصور المبدئي لخطة التعامل مع الواقعة المرتكبة من حيث التجهيزات والانتقال إلى مسرح الجريمة والخطة التي سوف يتم التعامل بمقتضاها في الكشف عن تفاصيل الواقعة.

وتحديد نوع الخبرة المتطلبة للعمل في الواقعة ورجال البحث المفترض انتقالهم لمحل الواقعة وأدوارهم في إجراء المعاينة لمحل الواقعة[1] وما يجب التأكيد عليه أن جهة تلقي البلاغ يجب عليها أن تحرص على أن يقوم المُبَلِغ بالخطوات التالية:

-تجهيز قائمة بأسماء العاملين في المؤسسة ممن لهم علاقة بالأجهزة المتضررة، أو علاقة بأي مشروع للأجهزة المتضررة.

-تجهيز نسخة احتياطية من بيانات الأجهزة المتضررة.

-التأكيد على عدم تبليغ أي شخص بالجريمة الواقعة[(2)]

كما هناك العديد من الأسئلة الاسترشادية التي يتعين على ضابط الشرطة القضائية طرحها على المجني عليه قبل الانتقال لمسرح الجريمة الرقمي، كمثال:*هل يوجد لدى المبلغ نظام IDSاوفي حالة وجوده فيتم التساؤل على مصدره؟

*هل من متابعين للواقعة محل الفحص؟

*هل الجاني الذي قام بالاعتداء ما زال على خط الاتصال بالشبكة؟...؟

[1] **خالد حازم إبراهيم**، مرجع سابق، ص 215-216.

[2] **خالد عياد الحلبي**، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، طبعة1، دار الثقافة، عمان، 2011، ص195.

المطلب الثاني : الاستجواب والشهادة حول الجريمة المعلوماتية.

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

-استجواب المتهم.

-سماع الشهود(شاهد إلكتروني)

وهو فيما سنتطرق إليه فيما يلي:

الفرع الأول: 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 في طريق من طرق تقصي الحقيقة ومصدر من مصادر الإثبات وليس وسيلة إثبات [1].

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

ويختلف الاستجواب عن السؤال وأن الثاني لا يتطلب مناقشة المتهم في هويته ومدى خطورته إعمالا بالمواد.

-استجواب المتهم في الموضوع: أي مواجهة قاضي التحقيق المتهم بالتهم المنسوبة إليه ومناقشته فيها مناقشة تفصيلية ومواجهته بالأدلة القاطعة ضده ولا بد أن يكون الاستجواب

[1] _)**أحسن بوسقيعة**، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربيوية،2002 الجزائر، ص45

[2] _)**محمد حزيط**، قاضي التحقيق في النظام القضائي الجزائري، دار هومة،ط2، الجزائر، 2010، ص102.

بحضور المحامي طبقا لنص المادة 110/57 ق ا ج ج 101، 102 قانون إجراءات جزائية جزائري[1].

-الاستجواب الإجمالي للمتهم: يكون في مساءلة جنائية (جنايات) وهو إجراء وجوبي إذ تعلق التحقيق بقضية ذات طابع جنائي، يهدف إلى تخليص الوقائع وإبراز الأدلة التي سبق جمعها[2].

أ-القواعد التي يلتزم بها المحقق في الاستجواب:

يعتبر الاستجواب إجراء من الإجراءات العامة في التحقيق لأن نجاح المحقق في إسناد الواقعة إلى الجاني واعترافه بارتكابها، وحتى يكون الاستجواب صحيحا لا بد أن يتضمن مجموعة من الإجراءات وهو ما سنتناوله بالتفصيل في ما يلي:

1-القواعد التي يلتزم بها المحقق قبل إجراء الاستجواب:

قبل أن يقوم المحقق بإجراء الاستجواب والمواجهة عليه أن يستعد لها وذلك باتباع القواعد العامة التالية:

-الإلمام الكامل بفهم أقوال الشهود وسائر المتهمين أن يحدد النقاط الجوهرية التي سيتم إيضاحها من المتهم[3].

-فهم فحوى التقارير الفنية التي وضعها الخبراء عن نتائج عملهم في الآثار المستخلصة،

-وضع خطة لنفسه يسير عليها في استجواب المتهم

2-القواعد التي يلتزم بها المحقق الجنائي عند البدء في الاستجواب :

على المحقق عند البدء في الاستجواب أن براعي اتخاذ واتباع القواعد التالية :

[1])_ نظر المواد 110/57، 101، 102ق.أ.ج.ج.

[2])_**محمد حزيط**، مرجع سابق، ص103.

[3])_**خالد ممدوح إبراهيم**،فن التحقيق الجنائي فيا لجرائم الإلكترونية،دارالفكرالجامعي،ط2009،01،ص243.

-إذا أعلن المتهم عن محاميه لا بد من دعوة المحامي لحضور الاستجواب.

-تفتيش المتهم.

-عدم إكراه المتهم على الاعتراف بأي شكل من أشكال التعذيب.

الفرع الثاني: الشهادة الإلكترونية(سماع الشهود)(شاهد إلكتروني):

أ-الشهادة الإلكترونية : إن مصطلح الشهادة الإلكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد تتم مثلا عن طريق وسائل إلكترونية أو رقمية من خلال شبكة الأنترنت.[1]

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[2].

أما بالنسبة لجميع الحكام وضوابط الأشخاص الذين يراد سماعهم في مجال الجريمة المعلوماتية فقد تطرقنا إليها سابقا.

يختلف الشاهد في الجريمة المعلوماتية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية، وقد عرف الشاهد الإلكتروني بأنه:"الشخص الفني ذو الخبرة والتخصص في تقنية وعلوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات ويمكن القول أن الشاهد الإلكتروني هو كل من:

[1])_(**عبد العالي الديري**، محمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي للإصدارات القانونية، القاهرة، ص313.

[2])_انظر المواد 60-88-97-110 ق ا ج ج.

أ-مشغلو الحاسب الآلي: هو ذلك الشخص المسؤول عن تشغيل الجهاز و المعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات واستخراجها كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح[1].

ب-خبراء البرمجة: هم الأشخاص المتخصصون في كتابة أوامرالبرامج وينقسمون إلى فئتين: الأولى هم مخططو برامج التطبيقات والثانية هم مخططو برامج النظم.

ج-المحللون: هم الأشخاص الذين يحللون الخطوات، ويقومون بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن الذي يمكن ميكنتها بواسطة الحاسوب.

د-مهندسو الصيانة والاتصالات: هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.

هـ-مديرو النظُم: هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية.[2]

المبحث الثاني: التحقيق حول الجريمة المعلوماتية:

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

والثابت أن الدعوى تمر بمرحلتين: مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى هي

[1])_ **خالد ممدوح ابراهيم**، مرجع سابق، ص263-264.

[2])**بخي فاطمة الزهراء**، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية حقوق وعلوم سياسية، جامعة المسيلة، 2013،2014، ص69-70

جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي[1] والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[2] وإننا نؤيد الرأي والاتجاه، الذي يقسم التحقيق إلى:

-تحقيق أولي والذي أناط به رجال الضبطية القضائية.

-تحقيق قضائي ونياط به رجال القضاء وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي ويكون في مرحلة المحاكمة من طرف قضاة الحكم، وفي مل جميع أنواع التحقيق هذه يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراء البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 12و38 من قانون الإجراءات الجزائية الواردتين في الباب الأول من هذا القانون تحت عنوان "في البحث والتحري عن الجرائم" حيث تنص المادة 12 الفقرة 3 أنه"يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..." وتنص في نفس الوقت المادة 38 من نفس القانون أنه"يناط بقاضي التحقيق إجراءات البحث والتحري[3].

1-حسب المادة 15 من ق ا ج:يتمتع بصفة ضابط الشرطة القضائية..."

-رؤساء البلديات، ضباط الدرك الوطني ...التابعين للمصانع العسكرية"

2-يبدو لنا أن المشرع لا يفرق بين التحقيق الأولي والتحقيق الابتدائي وذلك من خلال نص المادة 63 من قانون ا ج التي تنص على أن ضباط الشرطة القضائية يقومون بالتحقيقات

---

1)_حسب المادة 15 من ق ا ج: يتمتع بصفة ضابط الشرطة القضائية..."

-رؤساء البلديات، ضباط الدرك الوطني... التابعين للمصالح العسكرية

2)_يبدو لنا أن المشرع لا يفرق بين التحقيق الأولي والتحقيق الابتدائي، وذلك من خلال نص المادة 63 من قانون ا ج التي تنص على أن ضباط الشرطة القضائية يقومون بالتحقيقات الابتدائية..."، وفي نفس الوقت تنص المادة 66 الواردة في الباب المتعلق بالأحكام الخاصة بقضايا التحقيق على أن التحقيق الابتدائي في الجنايات وجوبي وهو بذلك يعتبر أن التحقيق الذي يمارسه سواء رجال الضبطية القضائية أم قضاة التحقيق يعد تحقيقا ابتدائيا على حد سواء.

3)_انظر للمواد 12-38 ق.إ.ج.ج.

الابتدائية..." وفي نفس الوقت تنص المادة 66 الواردة في الباب المتعلق بالأحكام الخاصة بقضايا التحقيق على أن التحقيق الابتدائي في الجنايات وجوبي وهو بذلك يعتبر أن التحقيق الذي يمارسه سواء رجال الضبطية القضائية أم قضاة التحقيق يعد تحقيقا ابتدائيا على حد السواء.

وعليه فإنه يمكن القول أن إجراء البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة.

المطلب الأول: الأجهزة المكلفة بالبحث والتحري حول الجريمة المعلوماتية.

لقد كان للتزايد المستمر للجرائم المعلوماتية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدثة تتولى مهمة التحري عن جرائم العالم الافتراضي وكشف النقاب عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها مثلا شرطة الأنترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا، وسوف نستعرض أهم هذه الأجهزة سواء على المستوى الداخلي أو الدولي وكذلك كما يلي:

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المعلوماتية:

نص المشروع الجزائري في المادة 13 من القانون 09-04[1] على ضرورة إنشاء هيئة ذات وظيفة تنسيقي، تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم، وتتولى تنشيط وتنسيق عملية الوقاية من الجرائم الإلكترونية، وكذلك مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي يجريها بشأن هذه الجرائم.

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المعلوماتية:

تعرف حسب أحكام المواد من 01 إلى 04 من القانون 09-04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة.

ثانيا: مقام الهيئة الوطنية للوقاية من الجرائم المعلوماتية:

تنص المادة 14 من نفس القانون على أنه" تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة ات الإعلام والاتصال ومكافحتها.

-مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بالإعلام والاتصال بما في ذلك تجميع المعلومات.

-تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بالإعلام والاتصال وتحديد مكان تواجدهم.

[1])_المرسوم رقم 09-04 المؤرخ في 08 غشت 2009 يتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 ، بتاريخ 5 غشت، 2009

ثالثا:اختصاصات الهيئة الوطنية للوقاية من الجرائم المعلوماتية.

بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261([1])المهام الأساسية التي تكلف بها الهيئة وهي على سبيل الحصر:

الهدف منها هو الوقاية من الجرائم المعلوماتية ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي:([2])

-اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة ات الإعلام والاتصال.

-تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة ات الإعلام والاتصال ومكافحتها .

-مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

-ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية الماسّة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

-تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

-السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

[1])_المرسوم الرئاسي رقم15-261 مؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53،الصادر بتاريخ 08 أكتوبر 2015.

–تطوير التعاون مع المؤسسات والهيئات الوطنية المعينة بالجرائم المتصلة ات الإعلام والاتصال.

الفرعالثاني:الوحدات التابعة لسلك الأمن الوطني والدرك الوطني.

توجد لدى مديرية الأمن الوطني والدرك الوطني لتنفيذ مهامه في مجال الحفاظ لى الأمن والنظام العام مجموعة من الوحدات نذكر منها:

أولا:الوحدات التابعة لسلك الأمن الوطني:

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدوليوالوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[1].

وقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجرائم المعلوماتية تعمل بالتنسيق مع هذه المخابر[2]

ثانيا: الوحدات التابعة للدرك الوطني الجزائري:

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها:

---

[1] **ربيعي حسين**، آليات البحث والتحري في الجرائم المعلوماتية، أطروحة دكتوراه علوم، جامعة باتنة، كلية الحقوق و العلوم السياسية،2015–2016 ، ص182.

[2])_**سعيداني نعيم**، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجيستر، ، كلية الحقوق والعلوم السياسية–قسم الحقوق، جامعة الحاج لخضر باتنة ،2012–2013، ص107.

-المصالح والمراكز العلمية والتقنية

-هياكل التكوين

-المصلحة المركزية للتحريات الجنائية

-المعهد الوطني لعلم الإجرام

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الآمن العمومية للدرك الوطني وهو قيد الإنشاء[1].

المطلب الثاني: خصائص التحقيق والمحقق في الجريمة المعلوماتية.

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية، لأنها تعد حجر الزاوية الذي سيتم على أساسها بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك قد يعود إلى الطبيعة التقنية لهذه الجرائم، ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإحباط والإعجاب معا[2].

---

[1])_**سعيداني نعيم**، مرجع سابق ، ص107.

[2])_**محمد طارق عبد الرؤوف الحن**، جريمة الاحتيال عبر الأنترنت(الأحكام الموضوعية والأحكام الإجرائية) منشورات الحلبي الحقوقية، طبعة1، بيروت، 2011، ص230 .

الفرع الأول: خصائص التحقيق في الجريمة المعلوماتية:

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

وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير[1].

وذلك أن الفكر البشري المتعلق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا وذلك كنتيجة طبيعية لمواجهة فكر المجرم المعلوماتي.

أولا: منهج وأسلوب التحقيق الابتدائي في الجريمة المعلوماتية.

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في ارتكابها ،ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى[2].

[1])_**خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي،طبعة1، الاسكندرية،2009، ص56.

[2])_**سعيداني نعيم**، مرجع سابق، ص ص106-107.

1/وضع خطة عمل التحقيق:

يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعداته في أعمال التحقيق وذلك على النحو الآتي:

-وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.

-التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح

-عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.

-تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.

-تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة[1].

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية يتم الارتكاز عليها أثناء تنفيذ الخطة، وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب

[1])_**محمد نصر السرحاني**، مهارات التحقيق الجنائي في جرائم الحاسوب والأنترنت، رسالة ماجيستر، جامعة نايف العربية للعلوم الأمنية، الرياض،2004، ص702.

استيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق.

2/تشكيل فريق التحقيق:

إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص وأحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فأنه يُفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة[1].

وإن كان أسلوب علم الفريق يستخدم في التحقيق في الكثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تتطلبه من مهارات فينة وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا.

ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

-المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.

-خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.

-خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.

-خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

[1]) **_سعيداني نعيم**، مرجع سابق، ص111.

-خبراء التصوير والبصمات والرسم التخطيطي[1].

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك.

ثانيا: العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة المعلوماتية:

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[2].

1/الإجراءات التي يجب مراعاتها قبل البدء في التحقيق:

ويمكن أن نسرد الأهم منها كما يأتي:

-تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

-وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

-مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

---

[1])_**عبد الله حسين علي محمود** ، سرقة المعلومات المخزنة في الحاسب الالي، ط4، دار النهضة العربية، القاهرة، 2006، ص613.

[2])_**محمد الأمين البشري** ، المرجع السابق، ص50.

-مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة

يجب فصل التيار الكهربائي عن موقع المعاينة أو جميع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

تصوير الأجهزة المستهدفة (التي وقعت بها أو عليها الجريمة) من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2/الإجراءات التي يجب مراعاتها أثناء التحقيق:

عند البدء في عملية التحقيق الابتدائي لا سيام عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم مراعاة ما يلي :

-عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانات المرئية قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر (DiskComp)

-نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

-أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات المسموحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي انمسحت وضغط على أزرار معينة مثل Shift/Delete في وقت وأحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.

-العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.

-العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها

-حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة[1].

الفرع الثاني: خصائص المحقق:

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية فإن المتخصصين في هذا النوع من الجرائم المستحدثة يختلفون عن أولئك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

1-تعريف المحقق في الجرائم المعلوماتية:

المحقق الجنائي في الجريمة المعلوماتية هو المكلف بالبحث عن الحقيقة في الجريمة المعلوماتية والكشف عن مرتكبها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم للقضاء فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق كل حسب اختصاصه[2].

الخصائص الفنية للمحقق:

يجب أن تتوافر بعض الأمور في المحقق ليقوم بعملة على أحسن وجه مثل:

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

-وصول الأخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنيين الذين يعملون على هذه الأجهزة.

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

---

[1]) **سعيداني نعيم**، مرجع سابق، ص ص 111-113.

[2]) **غرباوي نادية**، مرجع سابق، ص19.

-تشكيل فريق تحقيق فني، وإعطاء كل وأحد منهم مهمة معينة من خلال عملية التفتيش في مسرح الجريمة والبحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول إلى البرامج المخزنة وكيفية الحصول على الأرقام السرية والشفرات التي تمكنه من الدخول إلى الحاسوب.

-وضع خطة عمل مع جميع أعضاء فريق التحقيق والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها[1]

المطلب الثالث: إثبات الجريمة المعلوماتية:

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي وعلى ضوء ذلك فإن البحث في أدلة إثبات في إطار مدى اتفاقها مع الطبيعة التقنية لهذه الجرائم وسائل ارتكابها أصبح غير ذي معنى إذ لم يكن مدعما بتوفيق من قبل التقنية ذاتها، مما أدى إلى ظهور طائفة خاصة من الأدلة الجزائية يمكن الاعتماد عليها في إثبات هذه الجرائم ومن ثم نسبتها إلى فاعلها بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظم المعلوماتية التي تنتج عنها في حالة الاعتداء عليها وتتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية والأدلة الالكترونية حسب ما عبرت عنها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية[2].

فالدليل أثر يولد حقيقة تنبعث من الجريمة المعلوماتية المرتكبة ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر الذي يقع عليه ودليل جريمة القتل قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي استعملت فيها وتطبيق ذلك على الجريمة المعلوماتية فإنه يمكن أن تثبت بأدلة تقنية نتيجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها[3].

---

[1])_**خالد عياد الحلبي**، مرجع سابق، ص ص 183-184.

[2])_ **نايري عائشة**، مرجع سابق، ص44.

[3])_**رشيدة بوبكر**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع المقارن، منشورات الحلبي الحقوقية، طبعة1،مستغانم 2012، ص380.

أولا :تعريف الدليل الرقمي:

عرفته المنظمة العالمية لدليل الحاسوب في قرار لها في اكتوبر 2001 بأنه: المعلومات ذات القيمة المحملة والمخزنة أو المنقولة في صورة رقمية وكانت قد عرفته في مارس 2000 بأنه: المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة[1].

وكذلك عُرف الدليل الالكتروني بأنه الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة وهو كدليل بيانات يمكن إعدادها أو تخزينها بشكل الكتروني وعُرف كذلك بأنه معلومات يقبلها العقل والمنطق ويعتمدها العلم يتم الحصول عليها بإجراءات علمية وقانونية بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة[2].

ويعرف أيضا بأنه الدليل المأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة والصور والأصواتوالإشكال والرسوم وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وفي مجال تعامل جهات التحقيق مع الأدلة الجنائية فإن هذه الأخيرة مقبلة على الانتقال من مرحلة التعامل مع الأدلة المادية الملموسة معروفة المصادر إلى مرحلة التعامل مع الأدلة الرقمية المنتشرة في أماكن افتراضية وهو أمر لا مجال يثير مشكلات مهنية وأخرى قانونية ينبغي تحديدها بوضوح توطئة لوضع الحلول المناسب لعلاجها ذلك أن معطيات التقنية المعلومات أضافت إلى مشكلة الجريمة أنماطا إجرامية على درجة عالية من التعقيد يحتاج إثبات ها إلى أسلحة وأدوات علمية المعلوماتية ثم طبيعته من خلال ما يلي:

---

[1]) **مصطفى محمود موسي**، التحقيق الجنائي في الجرائم الإلكترونية، طبعة1، مطابع الشرطة، القاهرة، 2009، ص213.

[2]) **خالد الحلبي**، إجراءات التحري والتحقيق في الحاسوب والأنترنت، طبعة1، دار الثقافة للنشر والتوزيع، عمان، ص230.

الفرع الأول مفهوم الدليل الرقمي

كما أثارت الثورة المعلوماتية على نوعية الجرائم التي صاحبتها وظهور إنما ط المستحدثة من الجرائم عرفت بالجرائم المعلوماتية فأنها في المقابل ايضا اثرت على إثبات ها فأصبحت الأدلة التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير قادرة على إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية تناسب مع طبيعته بحيث يمكننها فك رموزه وترجمة نبضاته وذلك بأنه إلى كلمات وبيانات محسوسة لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة، وبشكل قانوني يمكن الأخذ به أمام أجهزة تنفيذ وتطبيق القانون [1].

ثانيا خصائص الدليل الرقمي:

تقوم خصائص الدليل الرقم على مدى ارتباطه بالبيئة التي يحيا فيها وهي البيئة الافتراضية والتي انعكست على طبيعة هذا الدليل فأصبح يتصف بعدة خصائص جعلته يتميز على الدليل الجنائي التقليدي.

1-الدليل الرقمي هو دليل علمي:

الدليل الرقمي يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات ذات المبنى العلمي ومن ثم فإنما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة "أن القانون مسعاه العدالة وأما العلم فمسعاه الحقيقة" وإذا كان الدليل العلمي الذي يجب أن لا يخرج عليها، إذ يستبعد تعارضه مع القواعد العلمية السليمة فإن الدليل الرقمي له ذات الطبيعة فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي والا فقد معناه[2].

2-الدليل الرقمي من طبيعة تقنية: إن الطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها فلا تنتج التقنية سكنيا يتم به اكتشاف القاتل أو

[1])_**محمود عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتاب القانونية، مصر/ 2006، ص88.

[2])_**ممدوح عبد الحميد عبد المطلب**، مرجع سابق، ص89.

اعترافا مكتوبا أو مالا في جريمة الرشوة أو بصمة إصبع وإنما تنتجه التقنية هو نبضات رقمية تتشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها ومثل هذا الأمر يجعلنا نقرر انه لا وجود للدليل الرقمي خارج بيئته التقنية وانه لكي يكون هناك دليل رقمي يجب أن يكون مستوحًى أو مستنبطًا من البيئة الرقمية أو التقنية وهي في إطار جرائم المعلوماتية ممثلة في العالم الرقمي أو العالم الافتراضي وهو العالم الكامل في الحاسوب والخوادم والمضيفات والشبكات التي يتم تداول الحركة فيه عبرها.[1]

3-الدليل الرقمي دليل متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداوالها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها

كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات والمنصات والخوادم وقد يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الإلكتروني وقد يكون أيضا مرتبطا بالتشفير وهذا التنوع إنما يعد تعبيرا عن اتساع قاعدة الدليل الرقمي بحيث يمكنه بهذه الصور أن يشمل أنواعا متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لأن تكون دليلا بالإدانة أو البراءة وأما عن كون الدليل الرقمي دليلا متطورا فهي خاصية تكاد تكون تلقائية نظر لارتباطه بالطبيعة التي تتمتع بها حركة الاتصال عبر الانترنت والعالم الافتراضي اللذان لا يزالان في بدايتهما ولم يصلا بعد إلى منتهاهما ولم يكن من السهل احتواؤهما.

[1])_**خالد ممدوح إبراهيم**، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية، ط2008،ص181.

4-الدليل الرقمي صعب التخلص منه: إن القاعدة التي تسري على كافة ما يتعلق بهيكلة التكنولوجيا المعلومات هي أنه كلما حدث اتصال بتكنولوجيا المعلومات في معنى إدخال البيانات إلى ذلك العالم فإنه من الصعب التخلص منها ولو كان ذلك باستخدام أعتى أدوات الإلغاء ومحاولة التخلص من الدليل الرقمي باستخدام خصائص التخلص من الملفات في الحاسوب كخاصية لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة تتوافر برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب.[1]

و يمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية اذ يمكن التخلص بسهولة من الأوراق[2]والأشرطة المسجلة إذا حملت في طياتها دليل جريمة بتمزيقها أو حرقها كما يمكن أيضا التخلص من بصمات الأصابع لمسحها عن موضعها كما يمكن التخلص من الشهود بتهديدهم أو قتلهم كما يحدث في بعض الدول الغربية أو استبعادها أصلا في الإثبات إذا مضى عليها مدة طويلة من الزمن قد لا يكون بعدها الشاهد قادر على التذكر وكل ذلك يجعل عملية التخلص من هذه الأدلة امرا سهلا.

5-الدليل الرقمي ذو طبيعة رقمية ثنائية 01:

إن الآثار التي يتركها مستخدم النظم المعلوماتية والتي تشمل الرسائل المرسلة منه أو التي استقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي وشبكة الاتصالات تكون على الشكل الرقمي الآلي سواء كانت في شكل نصوص أم حروف أم أرقام أم صور أم فيديو تتحول إلى صيغة رقمية حيث ترتكز تكنولوجيا المعلومات الحديثة على تقنية الترقيم التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الإعداد يفهمه الحاسب الآلي قوامه

[1])_**سعيداني نعيم**، مرجع سابق، ص124.

[2])_**سعيداني نعيم**، مرجع نفسه ، ص ص125-126.

العددان صفر وأحد فأي شيء في العالم رقمي يتكون من الصفر الواحد[1]، فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه إنما هي مجموعة من الأرقام التي ترجع إلى أصل وأحد وهو الرقم الثنائي 01 وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة.[2]

إن هذه الخصائص السالف ذكرها أكسبت الدليل الرقمي طابعا متميزا جعلت منه الدليل الأفضل لإثبات الجرائم المعلوماتية لأنه من طبيعة الوسط الذي ارتكبت فيه سواء كانت هذه الجرائم مرتكبة بواسطة نظام المعالجة الآلية أو كانت تشكل اعتداء ومساسا على نظام المعالجة الآلية.

الفرع الأول : أشكال الدليل الرقمي وأنواعه.

أولا: أشكال الدليل الرقمي وأنواعه

ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال نذكر منها على سبيل المثال:

1-الصورة الرقمية: هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقد الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية-والصورة الرقمية تمثل تكنولوجيات بديلة للصورة التقليدية[3].

[1])_**ممدوح عبد الحميد عبد المطلب**، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على الموقع الإلكتروني www.arablawinfo.comص08

[2])_**عمر محمد أبو بكر بن يونس**، مرجع سابق، ص791.

[3])_**سعيداني نعيم**، مرجع سابق، ص127.

2-النصوص المكتوبة: وتشمل الأوراق التحضيرية التي يتم إعدادها بخط اليد كمسودة أو تصور العملية التي يتم برمجتها، وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة[1]

3-التسجيلات الصوتية: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الأنترنت [2]

ثانيا: أنواع الدليل الرقمي:

يأخذ الدليل الإلكتروني نوعين رئيسين: أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعدّ لتكون وسيلة إثبات .

1- السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها، وكذلك السجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤها بواسطة الجهاز [3]

2-أدلة لن تعد لتكون وسيلة إثبات :السجلات التي جزء منها تم حفظه بالإدخال وجزء تم انشاءه بواسطة الجهاز، ومن امثلة ذلك البيانات التي تم ادخالها إلى الأدلة لتتم معالجتها من خلال برنامج خاص. واما النوع الثاني اي الادلة الرقمية التي لا تعد لتكون وسيلة اثبات فهي تلك الادلة التي تنشا دون ارادة الشخص، معنى اي اثر يتركه دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الادلة بالبصمة الرقمية أو الآثار المعلوماتية للرقمية. [4]

وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه و التي يستقبلها و كافة الاتصالات التي تمت من خلال النظام المعلوماتي و شبكة

---

[1])_**محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، ط1، دار الجامعةّ، عمان، 2014، ص117.

[2])_**سعيداني نعيم**، المرجع السابق، ص128.

[3])_**سعيداني نعيم**، مرجع سابق، ص ص128-129.

[4])_**خالد عياد الحلبي**، المرجع السابق، ص ص235،236

الاتصالات ، و الواقع ان هذا النوع من الادلة لم يعد اساسا للحفظ من طرف من صدر عنه غير ان الوسائل التقنية الخاصة تمكن من ضبط هذه الادلة ولو بعد فترة زمنية من نشوئها فالاتصالات التي عبر المنظومة المعلوماتية المرتبطة بشبكة الاتصالات و المراسلات الصادر عن شخص والتي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك.

الفصل الثانـي:

آليات حول البحث والتحري حول الجريمة المعلوماتية

اذا كانت الجهات المكلفة بالبحث و التحري عن الجريمة و المجرمين متعودة عن التعامل مع الجريمة بصورها التقليدية ، و التي يمكن ادراكها بالحواس لما يمكن ان يخلفه مرتكبوها من اثار مادية في مسرح الجريمة من بصمات و أثار أقدام أو بقع و دم أو محررات مزورة فان المشكلات الاجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية الى اخفاء نشاطه الاجرامي عن طريق تلاعبه بالبيانات والذي غالبا ما يتحقق في غفلة من المجني عليه فضلا عن سهولة تدمير الدليل و محوه من مسرح الجريمة مما يعقد امر كشفها و تحديد مرتكبيها و على وضوء ذلك فأن هذه الظاهرة الاجرامية التقنية أثارت العديد من المشكلات في نطاق قانون الاجراءات الجزائية الذي وضعت نصوصه الى تحكم الاجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في اثباتها و التحقيق فيها و جمع الادلة المتعلقة بها مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي.

نظرا للخصوصية التي اكتسبتها الجريمة المعلوماتية أنتجت نوعا خاصا من الأدلة من نفس طبيعتها حيث يصعب اكتشافها وضبطها والتحري عنها بالآليات العامة للتحقيق مما دفع إلى ضرورة تطوير القوانين والعقوبات من أجل استيعاب الجريمة المعلوماتية وضبطها ضمن الجرائم، وقد عمل المشرع الجزائري في هذا المجال على دعم الإجراءات العامة التي تتمثل في التفتيش والخبرة والتسرب بإجراءات وآليات خاصة، وجديرٌ بالذكر أن هذه الآليات الخاصة المتمثلة في المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير.

المبحث الأول: إجراءات الحصول على أدلة الإثبات في الجريمة المعلوماتية :

مما تم ذكره سوف نحاول التطرق إلى الآليات التي تقوم بها جهات التحقيق من أجل التصدي لمواجهة الجرائم المعلوماتية سواء كانت إجراءات تقليدية عامة أو إجراءات مستحدثة خاصة، فكلاهما تهدف إلى الغرض نفسه وهو البحث عن الحقيقة وكشف الغموض عنها وستتم تقسيم الدراسة إلى مطلبين:

المطلب الأول الإجراءات التقليدية

المطلب الثاني: الإجراءات المستحدثة :

المطلب الأول: الإجراءات التقليدية

إن التطور التقني الذي لحق نظم معالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل وهو ما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية ، لذا سأبين مدى اعتماد هذه الإجراءات في مجال الجريمة المعلوماتية للحصول على الدليل وفق الفروع الموالية مثل التفتيش الخبرة والتسرب[1].

الفرع الأول:التفتيش

ان التفتيش عموما هو اجراء من اجراءات التحقيق بهدف الكشف عن الحقيقة تخصص به جهة التحقيق من حيث الاصل و جهة الاستدلال بصفة استثنائية في حالات التلبس وهو على درجة من الاهمية و خطورة لما يستقر عنه من أدلة مادية تساعد في كشف ملابسات الجريمة .

تعريف التفتيش

يُعَرّف التفتيش على أنه البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سندا من القانون.

[1]) **السوقي نور الهدى**، التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي، شعبة الحقوق، تخصص قانون جنائي، كلية الحقوق و العلوم السياسية ، جامعة قاصدي مرباح، ورقلة، 2016-2017، ص29.

كما يعرف على أنه البحث في مستودع سر المتهم عن الأشياء كما تفيد في كشف الحقيقة ونسبتها إليه وهو الاطلاع على محل منحة قانون حماية خاصة باعتباره مستودع سر صاحبة يستوي في ذلك أن يكون محل سكن أو ما هو في حكمه أو أن يكون شخصا.

كما عرفه البعض أيضابأنه إجراء من إجراءات التحقيق، وهو ليس عملا من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين.

ويتضح مما سبق أن إجراء التفتيش من أهم الإجراءات المخولة لضبط الشرطة القضائية حسب نص المادة 05 الفقرة الأولى من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]وكذلك قانون الإجراءات الجزائية حيث يهدف هذا الإجراء إلى ضبط إحراز الأدلة الخاصة بهذه الجريمة بغية تحديد المتهم وتوجيه الاتهام إليه.

ثانيا: شروط التفتيش:

يقتضي التفتيش في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها حيث تعمل هذه الأخيرة على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية وسلطات التحقيق في إزالة الغموض عن الجرائم المعلوماتية وضبط مرتكبيها[2]ومن هنا نجد أن هذه الضوابط تنظم وفق نوعين من الشروط شروط شكلية وأخرى موضوعية:.

الشروط الشكلية : يجب أن يجرى التفتيش بحضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه وكما يجب أن يحضر ضابط الشرطة القضائية المشرف على التفتيش الإذن

[1])_انظر المادة 05 فقرة 1 من قانون رقم 09-04 مؤرخ في 05 غشت 2009،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها- الجريدة الرسمية، العدد 47، الصادر في 16 غشت 2009.

[2])_**رضا هميسي**، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد 05، جوان 2012، ص164.

الصادر من طرف وكيل الجمهورية أو قاضي التحقيق والذي يحتوي على جميع البيانات المتعلقة بالمكان المراد تفتيشه وبعد الانتهاء من عملية التفتيش يتم تحرير محضر يحمل جميع مراحل العملية من بدايتها إلى نهايتها وقد حدد المشرع الوقت المحدد لعملية التفتيش وذلك حسب نص المادة 47 من قانون الإجراءات الجزائية الجزائرية، حيث نصت على أنه:" يجوز للضبطية القضائية القيام بإجراءات التفتيش من الساعة الخامسة صباحا إلى الثامنة مساءً وهناك حالات استثنائية يجوز فيها التفتيش في أي وقت ونجد أن المشرع يقصد بالحالات الاستثنائية الجرائم المحددة على سبيل الحصروالمتمثلة في جرائم المخدرات والجرائم المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآليةللمعطيات (الجرائم المعلوماتية) وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف على أنه يجوز إجراء التفتيش في أي ساعة من ساعات الليل والنهار[1]

الشروط الموضوعية : يقصد بها الضوابط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة له وتتمثل في سبب ومحل التفتيش.

سبب التفتيش: وهو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث ويتمثل في وقوع الجريمة في وقوع جريمة ما جناية أو جنحة أو اتهام شخص أو أشخاص معينين في كشف الحقيقة لدى المتهم أو في مسكنة أو بشخص غيره أو مسكنه.

محل التفتيش: وهو الذي يقع على الأشياء المادية أو اللامادية أي كل ما قد يحتويه مستودع السر وكل ما له صلة بالنظم والبرامج وغيرها من الأجهزة الإلكترونية، ويكون التفتيش إما للأشخاص وإما للمساكن التي تحتوي على تلك الأجهزة أو الشبكات المعلوماتية.[2]

[1])_انظر المادة 47 من الأمر 15-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 40 الصادر في 23 يونيو 2015.

[2])_**رضا هميسي**، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، جامعة الوادي، العدد5، جوان2012، ص160.

بطلان التفتيش : إن مراقبة المحادثات الهاتفية(سلكية ولا سلكية) وتسجيلها هو إجراء من إجراءات التفتيش ألا أنه نظرا لخطورة هذا الاجراء باعتباره يتعرض للمستودع لمستودع سر الفرد ويزيل الحظر على بقاء سريته مقصورة على نفسه وما اراد انتماؤه عليه فيباح لغيره الاطلاع على مكنون سرية فقد حرس الدستور وقانون الإجراءات الجزائية على تأكيد ذلك واشترط لمراقبة المحادثات الهاتفية(سلكية ولا سلكية) صدور أمر قضائي مسبق.

الفرع الثاني:الخبرة

لقد ترتب عن التطور التقني في النظام المعلوماتية إلى تغير كبير في المفاهيم السائدة حول الدليل وقد مثل هذا الدور في الحقيقة إلى تعاظم دور الإثبات العلمي وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية ذلك أن اشتقاق الأدلة الرقمية المطلوبة في إثبات الجرائم المعلوماتية وكشف أنماطهاأمر يضطلع به الخبراء المتخصصون في هذا المجال ولا يمكن التصور أن يرفض القاضي اللجوءإلى ندب خبير في قضايا تقنية المعلوماتية إذ هي قضايا فنية تتطلب خبرة خاصة ويكون حكمه مجانبا للمنطق العلمي ومعيبا إذا لم يستدل إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ هام هو مبدأ التخصص.

أولا: تعريف الخبرة

الخبرة هي أداة لتطبيق العدالة الجنائية في المستقبل فبعد أن كان القاضي يستعين بنظام الأدلة المقبولة ثم تطورت إلى الاقتناع الشخصي ثم إلى الدليل عن طريق الخبرة العلمية [1]

هناك المحللون أي الأشخاص الذين يحللون الخطوات ويقومون بتجميع بيانات نظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن بواسطة الحاسوب والاتصالات وهم المسؤولون عن أعمال

[1])_نور الهدى السوفي، مرجع سابق، ص38.

الصيانة الخاصة بتقنيات الحاسب ومكوناته وأجهزة الاتصال المتعلقة به، وأخيرا مديرو النظم وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

ثانيا: أهمية الخبرة

تبرز أهمية الخبرة في الاستعانة بالخبير في مجال الجرائم المعلوماتية عن غيابها فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه.

فإنه إذا كان للخبرة تلك الأهمية في الجرائم التقليدية فإن أهميتها ازدادتها وأصبحت حتمية في إثبات الجرائم المرتكبة عبر الانترنت فهي وسيلة تساعد في إثبات الجريمة وتهدف إلى كشف بعض الدلائل أو تحديد مدلولها بالمعلومات العلمية.

ونظرا لطبيعة هذه الجرائم فانا إماطة اللثام عنها يحتاج إلى الخبرة في جميع مراحل الدعوى، لذلك لم تكتفِ التشريعات بالنصوص التقليدية التي تنظم الخبرة وعمدت إلى إدراج نصوص قانونية خاصة تنظم الخبرة وقد أبرز المشرع الجزائري ذلك قانون 04/09 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقوله: يمكن للسلطات المكلفة بتفتيش المنظومة الحاسوبية تسخير كل شخص له دراية بعمل المنظومة الحاسوبية محل البحث أو التدابير المتخذة لحماية المعطيات الحاسوبية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.[1]

ثالثا: شروط الخبرة

تقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية والنظرية والممارسة العملية للتخصص العلمي والنظري وكذا متابعة مستمرة للتطورات التي تلحق فرع التخصص غير أن ذلك ليس شرطا لازما في بعض الاحيان، فقد يقتصر الخبير على مجرد

[1]) **صغير يوسف**، الجريمة المرتكبة عبر الأنترينت، مذكرة لنيل شهادة الماجيستر في القانون، تخصص قانون دولي للأعمال، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة 06-03-2013، ص89.

الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة منها مجال الحاسب الآلي حيث يتعين في خبراء الحاسب الآلي المنتدبين للتحقيق أن تتوفر لديهم القدرة الفنية والإمكانات العلمية في المسألة موضوع الخبرة.

ولا يكفي في ذلك حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية ولذلك لا وجود لخبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها أو لديه القدرة على التعامل مع كل أنواع الجريمة المعلوماتية.[1]

تستوجب طبيعة هذه الجرائم توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية بالنسبة لها وهي:

1- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الظرفية الملحقة به وكلمات المرور.

2-طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

3-قدرة الخبير على إتقانمأموريته دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المحصلة من الوسائل الإلكترونية .

4-التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسب أو النظام أو الشبكة .[2]

---

[1])_**عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر 2002، ص138.

[2])_**عبد الفتاح بيومي حجازي**، مرجع سابق، ص98.

يتعين كذلك على الخبير في الجرائم المعلوماتية التنسيق مع المحقق قبل محاكمة الجاني في هذه الجريمة على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضغط أو التحقيق في تلقي البلاغ أو إجراءات الضغط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية على أن يتم في هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بيئة أو قرينة كما يجب على المحقق الجنائي أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة التي قامت عليها الدعوى الجنائية ضد المتهم.

تجدر الإشارة إلى أنه وان كان من المقر أن المحكمة تمتلك سلطة تقديرية بالنسبة لتقدير الخبرة الذي يرد إليها إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها ألا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع ومن ثم فلا تستطيع المحكمة أن تفندها وترد عليها ألا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى.[1]

الفرعالثالث: التسرب

لقد واكب المشرع الجزائري وعلى غرار التشريعات العقابية الأخرى التطور الذي شهدته السياسة العقابية الحديثة في مجال مكافحة الجريمة إذ لم يعد يجابه الجرائم الخطيرة والمستحدثة باستعمال الأساليب التقليدية والقديمة بل عمد وخلال تعديل قانون الإجراءات الجزائية إلى استحداث أساليب وتقنيات جديدة تتماشى والتطور الذي عرفته الجريمة ومن بينها أسلوب التسرب الذي يتيح الفرصة لضابط أو عون الشرطة القضائية بالتوغل داخل الشبكة الإجرامية وهذا قصد الوصول إلى معرفة عناصر الشبكة الإجرامية وتقديمهم للجهات القضائية ومعاقبتهم.

أولا: تعريف التسرب

يعتبر التسرب واحدة من أهم واخطر طرق البحث والتحري وأكثرها تعقيدا حيث يعتمد على المهارات والقدرات الشخصية لضباط وأعوان الشرطة القضائية القائمين بالعملية والذكاء

[1]) **_صغير يوسف**، مرجع سابق، ص92.

وتستخدم فيها مختلف الأساليب من أجل كسب ثقةالمشتبهفيهم وتحديد طبيعة ومدى النشاط الإجرامي حيث يقوم ضابط أو عون الشرطة القضائية باختراق جماعة إجرامية باستعمال هوية مستعارة وإيهامهم بأنه فرد لا يتجزأ من العصابة الإجرامية بنية مراقبة الأشخاص المشتبه فيهم والحصول على المعلومات المتعلقة بمخططات العصابة والكشف عن أنشطتهاالإجرامية والوسائل التي تستعملها في ذلك وغيرها من المعلومات المتعلقة بالجريمة والمجرمين والتصرف في الوقت المناسب شرط أن لا يشكل هذا التصرف تحريضا على ارتكاب الجريمة[1]

ويلاحظ من خلال ما سبق ذكره أن التسرب عملية معقدة تتطلب أن يدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ويربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب اليها، وعلى هذا ذلك فإن التسرب يرتكز على مبدأين:

المبدأ العام: يستند على تقديم صورة على الوسط المراد التسرب فيه، ويستوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات.

المبدأ الخاص: الذي يستند على تعميق التحري عن هذا الوسط ونشاطاته ومميزاته ووسائله وطبيعة الأشخاص المنتمين إليه ليتم بعد ذلك دراسة الوظيفة العملياتية في هذا المجال بتوفير الوسائل البشرية والتقنية اللازمة.

ثانيا: شروط التسرب

من أجل إنجاح عملية التسرب وتسهيل مهام الشخص المتسرب لبلوغ الهدف المرجو من هذا الإجراءباعتباره ممارسة غير مألوفة للضابط أو عون الشرطة القضائية وكذا لكون هذا

[1]) **سليمان أحمد إبراهيم**، القواعد الجنائية للجريمة المنظمة، دار الكتاب الحديث، القاهرة، 2008، ص359.

الإجراء من اخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيه فقد أحاطه المشرع بجملة من الشروط يتعين مراعاتها عندما تقتضي ضرورات التحري والتحقيق اللجوء إليه[1]

1-الشروط الشكلية:

تنحصر الشروط الشكلية لهذا الإجراء في الإذن وما يجب أن يتضمنه فلا يمكن بأي حال من الأحوال أن يباشر ضابط الشرطة القضائية عملية التسرب بمفردة بذلك من قبل الجهات القضائية المختصة وهذا ما نصت عليه المادة 65 مكرر من قانون الإجراءات الجزائية يجوز لوكيل الجمهورية أو الإيقاظ التحقيق بعد إخطار وكيل الجمهورية أي اذنة حسب الحالة بمباشرة عملية المختصة بإصدار أو منح الإذن بالتسرب أن يكون هذا الإذن مكتوبا وإلا كان الإجراء باطلا وهذا ما نصت عليه المادة 65 مكرر 15 بقولها:" يجب أن يكون الإذن المسلمطبقا للمادة 65 مكرر 15 مكتوبا تحت طائلة البطلان" وذلك لان الأصل في العمل الإجرائي الكتابة ومن جهة أخرى فإن الإذن يجب أن يتضمن مجموعة من الشروط يتوقف على تحديدها صحة الإجراء في حد ذاته كذكره هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليتهبالإضافة إلى تحديد المدة المطلوبة في عملية التسرب والتي يجب أن لا تتجاوز أربعةأشهر ويمكن أن تجدد حسب قضايا التحرير والتحقيق ضمن نفس الشروط الشكلية الزمنية، وفي نفس الوقت أجازالقانون للقاضي الذي إذن بهذا الأجراءأن يأمر في أي وقت بوقفه قبل انقضاء المدة المحددة[2]

2- الشروط الموضوعية:

يمكن إيجاز الشروط الموضوعية لعملية التسرب وفق الإحكام الذي نظمها المشرع الجزائري في شرطين أساسيين:

---

[1])_**كوداد عبد الرحمن**، عملية التسرب على ضوء التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص علم الإجرام، جامعة الدكتور الطاهر مولاي سعيدة،2016،2017، ص46.

[2])_**سعيداني نعيم**، مرجع سابق، ص169.

الأول يتمثل في تحديد نوع الجريمة والتي يجب أن لا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 05 في سبعة أنواع وهي جرائم المخدرات الجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموالوالجرائم الإرهابية وجرائم الفساد جرائم متعلقة بالتشريع الخاص بالصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أما الشرط الموضوعي الثاني فهو أن يكون الإذن بالتسرب مسببا فمن خلال التسبيب أن تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابطة الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبهاالإذن.

لذلك فكان لزاما عند إصدارالإذن بالتصرف سواء من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقرير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[1]

المطلب الثاني: الإجراءات الخاصة للتحقيق في الجريمة المعلوماتية:

مع التطور الكبير الذي شهده العالم في ميدان التكنولوجيا الرقمية أصبح مرتكبوالجرائم أكثر حيلة وذكاء باستعمالهم للوسائل التقنية الحديثة في ميادين مختلفة من الجرائم فسهلت وسائل الاتصال الحديثة حرية تنقلاتهم الإجرامية حتى امتدت إلى خارج الحدود الوطنية لتشمل دولا أخرى وتهديد أمنها وسلامتها بحيث أصبح من الصعب تتبع نشاط هاته الشبكات الإجرامية مما استدعى المشرع الجزائرية إلى مكافحة هذا النوع من الجرائم الحديثة في تعديله لقانون الإجراءات الجزائية بحيث ادخل أساليب وطرق جديدة للتحري والبحث والتحقيق في الجرائم وهو ما يسمى بآليات البحث والتحريالخاصة .

ومن هنا سنتطرق إلى هذه الأساليب من خلال فرعين حيث يتضمن الفرع الأولالمراقبة الإلكترونية والفرع الثاني حفظ المعلومات المتعلقة بحركة السير.

[1])_نصت المادة 65 مكرر من قانون الاجراءات الجزائية على أنه يجب أن يكون الإذن بمباشرة عملية التسرب...مسببا وذلك تحت طائلة البطلان".

الفرع الأول: المراقبة الإلكترونية:

منح المشرع الجزائري في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال سنة 2009 العديد من السلطات والصلاحيات للضبطية القضائية تحت اشراف السلطة القضائية في اختيار أسلوب إجراء التحري وبالطريقة التي يراها مناسبة لإتمام العملية بصورة ايجابية ودون المساس بحرمة الحياة الخاصة للحصول على أكبر عدد من المعلومات حول الواقعة محل المتابعة الجزائية لذلك قد يتخذ البحث والتحري عن الجريمة المرتكبة بالوسائل الإلكترونية أسلوب المراقبة الإلكترونية والتي تعتبر أحد ركائز الأساسية التي يستند عليها رجال البحث والتحري لجمع المعلومات حول الجرائم الواقعة على التوقيع الالكتروني[1]

أولا: تعريف المراقبة الإلكترونية.

يقصد بها كل عمل امني له نظام معلومات الكتروني يعتمد على التقنية الإلكترونية حيث يتولى المراقبة عن طريق الأجهزة الإلكترونية وعبر شبكة الانترنت باستخدام البرمجيات الإلكترونية وذلك لتحقيق غرض معين ولكي تحقق المراقبة الإلكترونية أهدافها يجب أن يتوفر أمران: الأول التعاون والتنسيق بين الشخصين المناط به كشف الجريمة والبحث عنها، وبين فريق المراقبة الذي يتولى التأهيل الفني للقائم بها ولفريق المراقبة[2]

ثانيا: الجرائم التي يجوز فيها اللجوء إلى المراقبة الإلكترونية

أجازت المادة 30فقرة ب من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال لسنة 2009 القيام بعمليات المراقبة الإلكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني لذلك فإجراء المراقبة الإلكترونية في جرائم التوقيع الالكتروني يتم اللجوء إليه في حالة احتمال الاعتداء على منظومة معلوماتية متعلقة بالتوقيع الالكتروني بشرط

[1]) **نبيلة هبة هروال**، مرجع سابق، ص197.

[2]) **نبيلة هبة هروال**، مرجع سابق، ص204.

أن يكون هذا الاعتداء يهدد ويمس النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني والتي تخضع للسلطة التقديرية للأمر بالإجراء[1]

ثالثا: صور المراقبة الإلكترونية

المراقبة الإلكترونية من أجل البحث والتحري عبر الانترنت ممكن أن تتخذ صورتين الأولى هي الإرشاد الجنائي عبر الانترنت والصورة الثانية هي المراقبة عبر التقنيات الإلكترونية الحديثة.

1- نظام الإرشاد الجنائي عبر الانترنت يعد نظام الإرشاد الجنائي المتعارف عليه عند البحث في الجرائم المرتكبة في العالم المادي مختلف عما عليه الحال في العالم الافتراضي فلا يتطلب الإرشاد الجنائي في جرائم التوقيع الالكتروني عبر الانترنت إلى الانتقال ومراقبة وتتبع المجرم أو المشتبه فيه من مكان لآخر، إذ يتم الإرشاد الجنائي عبر الانترنت عن طريق الولوج داخل صفحات الانترنت سعيا وراء الكشف عن الجريمة الواقعة على التوقيع الالكتروني عبر الانترنت ومرتكبيها وفق آليات مختلفة والدخول إلى قاعات الدردشة أو حلقات النقاش العامة والتنكر باستخدام أسماء مستعارة وتبادل أطرافالأحاديث المختلفة مع مستخدمي الانترنت وبشكل عام الظهور بمظهر طبيعي كأنه أحد مستخدمي شبكة لأجل جمع المعلومات والتعرف على مستخدمي الشبكات ذات النزعةالإجرامية ومن ثم ليس للمرشد الجنائي عبر الانترنت دفع الغير أو التحريض إلى ارتكاب جريمة عبر الانترنت[2].

ولكي يكون الإرشادالجنائي مشروعا وقانونيا في جرائم التوقيع الالكتروني عبر الانترنت لابد من توافر مجموعة شروط يمكن إجمالها في:

- يجب أن لا يكره الشخص المرشد على عملية الإرشاد

[1])_**محمد كمال شاهين**، مرجع سابق، صفحة 251.

[2])_**خالد عياد الحلبي** ، مرجع سابق، ص220.

– أن يكون الإرشاد مرتبط بمنع وقوع الجريمة أو متصلة بتغطية معلومات مطلوبة من جهة إدارية أو قضائية في غير مجال الجريمة

يجب ألا ينصب بالإرشاد الجنائي على تحريض على الجريمة أو استعمال الغش أو التحايل

– أن يكون الهدف من الإرشاد هو المصلحة العامة ولا يخدم أي مصلحة شخصية.

2–المراقبة الإلكترونية عن طريق التقنيات الإلكترونية الحديثة:

تتم المراقبة الإلكترونية في هذه الصورة عن طريق إرسال برمجيات إلى خوادم مختلفة بقصد التوصل إلى مرتكبي الجرائم المرتكبة بالوسائل الإلكترونية الواقعة على التوقيع الالكتروني ويكون للبرمجيات دور رئيسي في إطار المراقبة أو الإرشاد الجنائي البرمجي ويتعين التفرقة ما إذا كانت المراقبة الإلكترونية بصورتها تتم في الصفحات العامة عبر شبكة الانترنت أو تتم عبر الصفحات والمواقع الخاصة للأفراد وإذا كانت المراقبة الإلكترونية والإرشادالجنائي يتم داخل المواقع والصفحات العامة والمتاحة للكافة فلا يعد عمل المراقب انتهاكا للحق في الخصوصية المعلوماتية للأفراد، اما إذا تم الولوج واختراق المواقع والصفحات الخاصة والتي يتطلب الاطلاع عليها ضرورة الحصول على إذن قضائي بذلك، فهنا تعد المراقبة انتهاكا للحق في الخصوصية المعلوماتية[1].

ويتبين من ذلك أن نظام المراقبة الإلكترونية على درجة كبيرة من الأهميةلاتصالها المباشر بالحق في الخصوصية كما يعد عمل المراقب امرأ لا يمكن إهماله وخاصة إذا كانت الدول تسعى إلى نسج حماية جنائية إجرامية سليمة للمعلومات التي يتم فيها محاصرة الجريمة الإلكترونية من ناحية، وحماية المعلومة من ناحية أخرى بهدف المحافظة على الحق في الخصوصية المعلوماتية للأفراد.

3– أشكال المراقبة الإلكترونية:

[1])_**محمد كمال شاهين**، مرجع سابق، ص ص253–254.

تتلخص إشكال المراقبة الإلكترونية في استخدام وسائل تقنية من خلال ما يسمى بقلم التسجيل أو ما يسمى بالفخ والمتابعة وفي هذه الحالة يتم تسجيل أسماء المراسلين مع متهم معين أو مع بريديه الالكتروني أو ما يقوم بمحادثات ودردشات أو عن طريق استخدام وسائل لتنصت على محتوى الرسالة الإلكترونية أو المحادثة الفورية بوسائل للاعتراض والتصنت، والضبطية تواجه مشكلة تشفير المراسلات الإلكترونية في حالة ارتكاب جريمة من فاعلها عن طريق برامج تشفير تباع بأثمان رخيصة في السوق ما يثير مشكلات بالنسبة للضبطية القضائية بعد ضبط هذه الرسائل هو عدم القدرة على الاطلاع على محتواها لأنها مشفرة[1]

الفرع الثاني : حفظ المعطيات بحركة السير:

لقد أدرك المشرع على الصعيد الوطني والدولي بأنهمن الصعوبة بمكان الوصول إلى الأدلة الرقمية لهذا رأى من الضروري استحداث إجراء يلزم بمقتضاه الإطراف المتدخلة في خدمات الانترنت بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والقيام بحفظ المعطيات المتعلقة بحركة السير وهذا الإجراء أقرتها اتفاقية بودابست لمكافحة جرائم المعلوماتية من خلال أحكام المادتين 12 و17 والتي تقابلها المواد 23 24 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وأكده المشرع الجزائري بموجب المادة 10 من الفصل 04 من القانون رقم 04-09 تحت عنوان التزامات مقدمي الخدمات كما يلي:" في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية...وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أعلاه تحت تصرف السلطات المذكورة.[2]

وعليه سأتناول فيما يلي تحديد مفهوم هذا الإجراء والتطرق إلى التزامات مزودي الخدمات ومسؤولياتهم كما يلي:

[1])_**احسن بوسقيعة**، مرجع سابق، ص124.

[2])_المادة 12 من القانون 09-04.

أولا:تعريفها:

قبل تحديد مفهوم هذا الإجراء يتعين أن أوضح المقصود بمزودي الخدمات الحائزين لهذه المعطيات.

وحسب ما جاء في الفقرة د من المادة 02 من القانون 04-09 فإن مزودي أو مقدمي الخدمات يقصد بهم:

1 - أي كيان عام أو خاص يقدم لمستعمليه خدمات القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات

أي كيان آخر يقوم بمعالجة أو تخزين المعطيات المعلوماتية لفائدة خدمة اتصال مذكورة أو لمستعملها".

قد عرف المشرع الجزائري المعطيات المتعلقة بحركة السير بموجب الفقرة(ه) من المادة 02 من القانون رقم 09-04 بأنها: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه أو وقت وتاريخ وحجم مدة الاتصال ونوع الخدمة[1].

والملاحظ على هذه الفقرة أنها قد تضمنت مصطلحات غريبة نوعا على القانون الجنائي ومن ذلك:

"مصدر الاتصال" ومما لا شك فيه أن هذا الأخير يشير إلى رقم هاتف مثلا أو عنوان بروتوكول الانترنت(IP).

وكذلك مصطلح الوجهة المرسلة إليها ويشير إلى جهاز الاتصال التي تتجه إليه الاتصالات المرسلة.

[1]) **_حبيباتني بثينة**، مرجع سابق ،ص ص307-308

ومصطلح نوع الخدمة يشير إلى نوع الخدمة المستخدمة داخل الشبكة مثل نقل ملف، نشر صور، استخدام البريد الالكتروني[1]

وقد حدد المشرع الجزائري في المادة 11 من القانون رقم 09-04 عدة طوائف من معطيات مرور التي تدخل في نطاق الالتزام بالحفظ من طرف مزود خدمة وحصرها في:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل اليهم الاتصال وكذا عناوين المواقع المطلع عليها.

_المعطيات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

ويعد حفظ حركة سير المعطيات إجراء قانونيا جديدا واداة للتنقيب عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ثانيا:التزامات مزودي الخدمات

بما أن حفظ المعطيات إجراء وقتي فقد جاء المشرع واحتراما للحق في الخصوصية إلى وضع التزام على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها وذلك بعد سنة ابتداء من تاريخ التسجيل وهو ما يستفاد بمفهوم مخالفة مضمون نص المادة 11 من القانون 09-04

[1])_**رشيدة بوبكر**، مرجع سابق ، ص449.

كما يلي: تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة من تاريخ التسجيل..."[1]

ثالثا: مسؤولية مزودي الخدمات عن التقاعس عن حفظ المعطيات

إن الالتزامات المفروضة على مقدمي الخدمات التي كرسها المشرع بموجب المادة 11 من القانون09-04 فضلا عن الالتزامات المفروضة في دفتر الشروط، لان مستعملي هذه الوسائل يتعاملون مع هيئة معينة ولديهم دفتر شروط يتضمن كل الالتزامات الواجب عليهم احترامها وفي حالة عدم احترامها تقوم الإدارة أو الهيئة بفرض عليهم عقوبات كسحب الرخصة إضافة إلى عقوبة إدارية.[2]

كما يتعرض مزود الخدمات عند عدم احترامللالتزامات المنصوص عليها في القانون رقم 09-04 لمتابعته جزائيا بعد تطبيق العقوبات الإدارية لأنه في هذه الحالة يعرقل السير العادل للعدالة وتتراوح العقوبة من ستة أشهر حبسا إلى خمس سنوات إضافة إلى غرامة مالية تتراوح من 50,000 إلى 500,000 دينار جزائري إما الشخص المعنوي فيعاقب بالغرامة وفقا للقواعد المقررة في قانون العقوبات [3]وهو ما أكدته كذلك المادة 394 مكررة 8 من قانون العقوبات[4].

وبناء على ما سبق تناوله يتضح بأن المشرع تبنى إجراءات حديثة مستقلة وقائمة بذاتها من أجل تيسير إجراءات البحث والتحري وجمع الدليل الالكتروني لإظهارالحقيقة.

المبحث الثاني: عقبات البحث والتحري حول الجريمة المعلوماتية:

لقد لاقت إجراءات البحث والتحري عن الجريمة المعلوماتية مشاكل وتحديات كثيرة تختلف في جوانب عديدة عن التحديات والمشاكل التي ترتبط بالجرائم التقليدية وتتمثل أهم الصعوبات التي تعترض الجهات المكلفة بالتحقيق في أن تلك الجرائم ترتكب في نطاق الأنظمة

[1])_**حبيباتني بثينة**، مرجع سابق، ص311.

[2])_**رشيدة بوبكر**، مرجع سابق، ص452.

[3])_**حبيباتني بثينة**، مرجع سابق، ص312.

[4])_المرجع نفسه، ص312.

المعلوماتية وشبكة الانترنت ومحلها هو معلومات وبرامج معالجة آلية عن طريق الحواسيب أو جرائم تتعلق بالأشخاص عبر العالم الافتراضي غير المتناه وغير المحدود،الأمر الذي يمنحها طابعا خاصا ليس فقط في طريقة ارتكابها بل كذلك في الوسيلة التي ترتكب بها وبالرغم من الجهود الكبيرة التي يبذلها المشرعون وسلطات التحقيق والضبطية القضائية سواء كانت دولية أو داخلية إلا إنها تصطدم دائما بعدة عراقيل وصعوبات ومعوقات يمكن تقسيمها إلى معوقات لأسباب تقنية (المطلب الأول) وأخرى بشرية وأخرى قانونية (المطلب الثالث).

المطلبالأول: عقبات تعود لأسباب تقنية

تنقسم هذه العقبات إلى نوعين: الأولى تحول دون اكتشاف الجريمة(فرع الأول) والثانية تؤدي إلى صعوبة إثبات ها(فرع الثاني)

الفرع الأول : عقبات مرتبطة بصعوبة اكتشاف الجريمة.

تتمثل أهم تلك للعقبات فيما يلي:

–عدم وجود آثار مادية للجريمة: الطبيعة الخاصة لهذه الجريمة جعلتها لا تشبه باقي الجرائم في طرق تحريك الدعوى العمومية مثل الشكوى وما إلى ذلك الأمر الذي جعل أمر اكتشافها من قبل السلطات المعنية صعبا نوعا ما وبقاء اغلب تلك الجرائم مجهولا لعدم التبليغ عنها بالإضافة إلى أن مرتكب الجريمة المعلوماتية قد يلجا في غالب الأحيان إلى بذل أقصاحتياطاته لعدم إثارةفعلته مثل الجرائم المعلوماتية التي تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية كجرائم التجسس التي تتم عن طريق برامج التجسس الخاصة، بالإضافة إلى عدم دراية اغلب مستعمليالمعلوماتية لبرامجها ، فلربما يساهمون بجهلهم وبدون قصد في مساعدة مرتكبي تلك الجرائم بطريقة غير مباشرة من خلال تثبيت برامجَ تجسسٍ أو برامج ضارة بالجهاز أو الضغط على روابط مفخخة بالإضافة إلى إننا نتعامل أمام عالم افتراضي مسرحة هو المواقع والأجهزة الإلكترونية التي يمكن فيها الحذف والزيادة والتعديل والنقصان فلسنا أمام وثائق ومستندات ملموسة مثل الجرائم التقليدية،ونسوق هنا قول الأستاذة نهلا عبد القادر المومني التي

قالت بان:" الجريمة المعلوماتية تتميز بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.[1]

-الطبيعة المتعدية للحدود الجغرافية التي تتمتع بها جريمة المعلوماتية: ساهمت شبكة الانترنت في جعل العالم قرية واحدة من خلال تبادل المعلومات وانتقالها في اللحظة والحين ومن خلال التواصل بين مختلف جهات المعمورة إلا أن ذلك رغم طابعه الايجابي فإنه قد تحول إلى جانب سلبي استغله مجرمو المعلوماتية وحولوه إلى ميزة لهم لارتكاب أفعالهمالإجرامية التي تعدت حدود الجغرافية التقليدية للدول، فمثلا يكون المجرم المعلومات في دولة ويخترق حسابا أو موقع مصرف أو بنك دولة ثانية ويقوم بتحويل مبالغ أو عملات إلى دولة ثالثة بالإضافة إلى ما تتمتع به الجريمة المعلوماتية في أن المجرم يبقى قابعا في مكانه دون أن يتحرك لكسر الإقفال أو خلع الأبواب أو ترك البصمات أو تحويل المسروقات ومتحصلات الجريمة بل يكفيه فقط جهاز كمبيوتر حديث وخط انترنت حتى يصول ويجول في مختلف أنحاء العالم مرتكبا لجرائمه.

تعد شبكة الانترنت بطبيعتها عالمية الهوية والانتشار وبناءً على ذلك فإن كل نشاط إجرامي يتم من خلالها يكتسب هذه الصفة بالضرورة وبالنظر للطبيعة الاتصالية لشبكة الانترنت والعلاقات التجارية وغيرها التي تتم بواسطتها يمكن تخيل الكثير من الأسباب التي تساهم بوجود نشاط إجرامي في مجال تبيض الأموالوالاتجار بالمخدرات والترويج للأنشطةالإرهابية المنظمة، ونظرالارتباط أنشطةالاقتصاد الخفي يبعضها البعض خاصة في مجال القمار وتجارة المخدرات فإنه من الممكن أن يطور المجرمون عبر شبكة الانترنت آليات معقدة لتبييض الأموال عبر التحويل الالكتروني من بنك لآخر أو من بلد لآخر يصعب من خلالها تتبع هذه العمليات على الشبكة من الفنية،إضافة إلى تعقيد وضعف تشريعات القانونية في مثل هذه الجرائم الممتدة[2]

[1])_**نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة والتوزيع للنشر، ط1، 2008، الأردن، ص54.

[2])_**صغير يوسف**، مرجع سابق، ص127.

الفرع الثاني:عقبات تتعلق بصعوبة إثبات الجريمة

تبرز أكثر في ما يلي:

-اتخاذ الجنات لتدابير أمنية: يسعى المجرمون الإلكترونيون وتمويهها على إنها أعطالوأخطاء في أنظمة التشغيل أو إزالةاثأر الجريمة عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الحاسوب والبرامج لاسيما من التخزين الالكتروني غير المرئي والبيانات الكثيرة وهي مكتوبة بلغات رقمية لا تفهمها إلا الآلة ما لم تستعاد على شاشة الكمبيوتر، مما قد يُلجئ هؤلاء المجرمين أيضا إلى دس تعليمات خفيه بين تلك المعلومات أو البيانات أو استخدام الرموز أو التشفيرات بالنسبة لها بحيث قد يستحيل على غيرهالاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم غير المشروعة بالإضافة إلى قيام مجرمي الانترنتبإخفاء هوياتهم وانتحال شخصيات أخرى.

-الطبيعة غير المادية للأدلة المستخرجة من الوسائل الالكترونية: لا يكون الدليل الالكتروني مرئيا مثل السلاح الأبيض أو الناري أو الأداة الحادة أو المادة السامة أو الوثائق والمحررات وغيرها وهذا لا يمثل صعوبة في الإثبات إنما يقع الإشكال في الجريمة المعلوماتية كون أدواتها غير مادية وغير ملموسة تتمثل في برامج وروابط وتقع على التجارة الإلكترونية أو العمليات المصرفية أو على أعمال الحكومة الإلكترونية لان الجريمة المعلوماتية يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات.

- صعوبة الوصول إلى الدليل:من خلال قيام مجرمي الانترنت بحماية مواقعهم وأجهزتهم بكلمات سرية أو رموز وشفرات لإعاقةالمحاولات الهادفة إلى الوصول إليها أو الاطلاع عليها أو استنساخها.

بالإضافة إلى أنه حينما يتوجهأفراد الضبطية القضائية من أجل القبض على الجاني وتحرير الأدلة ومنها جهاز الكمبيوتر المستخدم في الاتصال بالشبكة وما يحوي من برامج ومعلومات إذ تثور مشكلة معرفة الرقم السري والذي بدونه لا يعمل جهاز الكمبيوتر وفي هذه

الحالة لا يجوز لأجهزة التفتيش إجبار المتهم على الافشاء بالرقم السري لان ذلك يعد إجراءً غير قانوني.

كذلك قد يتمكن الجاني من تدمير البيانات الموجودة والمخزنة في جهاز الكمبيوتر في ثوان أثناء إجراء التفتيش ففي هذه الحالات تكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب جرائم الانترنت.[1]

-سهولة محو الدليل الرقمي أو تدميره في زمن قصير جدا:يعبر عن ذلك بخاصية تطاير البيانات في الأدلة الرقمية وبحكم أنها بيانات معبر عنها بلغة الآلة والأرقام إلا أنه يمكن التلاعب بها وإخفاؤها بسهولة، حيث يقوم الجاني بمحو وتدمير أدلة الإدانة التي تكون قائمة ضده بسهولة متناهية أي تدميرها في زمن قصير جدا.

-ضخامة حجم المعلومات والبيانات المتعين فحصها:إذاكانت سلطات التحقيق في الجرائم التقليدية أماممسرح جريمة واضحٍ محدد المعالم يمكنهم التحقيق فيه فأنهم في حالة الجريمة المعلوماتية سيكونون أمام عالم افتراضي لا متناه متباعد الإطراف متصل يبعضه البعض من حيث المعلومات والأجهزة وحتى الكم الضخم والرهيب من البيانات والمعطيات الواردة فيه وبالتالي فهؤلاء المحققون لن يستطيعوا بأية حال من الأحوال التحقيق والتثبت في كل تلك البيانات والمعلومات لأنه عمل شاق ومرهق أمام قلة الإمكانات المادية والبشرية المساعدة، الأمر الذي يشكل عائقا أمام كشف الجريمة المعلوماتية والبحث والتحري فيها؛ إذ أن مجرد طباعة كل ما يوجد على الدعامة المغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي قد لا تثبت كلها تقريبا شيئا على الإطلاق، فلربما قام المحققون بتحقيق في جريمة معينة ثم يكتشفون بأنهم في مسار خاطئ يقوم بعدها بإعادة التحقيق من جديد في معطيات ومعلومات أخرى وكل ذلك مرده إلى الكم الهائل من المعطيات والبيانات والمواقع

[1])_**عمرو عيسى الفقي**، الجرائم المعلوماتية(جرائم الحاسب الآلي والأنترنت في مصر والدول العربية) المكتب الجامعي الحديث، طبعة الاولى،2006، مصر، ص93.

وعدم وجود آليات لفرزها بالإضافة إلى إشكالية البعد الجغرافي بين كل مرتكب من الجريمة والضحية[1]

المطلب الثاني: عقبات متعلقة بالجاني والضحية وسلطات الإستدلال:

تنقسم هذه العقبات إلى عقبات متصلة بالمجني عليهم(الفرع01) وعقبات مرتبطة بالجهات التي تتولى التحقيق في الجرائم المعلوماتية(الفرع02).

الفرع الأول: العقبات المتصلة بالمجني عليهم.

تتلخص فيما يلي:

تكتم المجني عليهم وإحجامهم عن الإبلاغ عن الجرائم المعلوماتية:

يمثل تكتم المجني عليهم وإحجامهم في الإبلاغ عن الجرائم المعلوماتية من أكثر الصعوبات التي تكتنف عملية البحث والتحري عن الجريمة المعلوماتية وذلك يعود لعدة عوامل يمكن أن نذكر منها:

خوف الجهات المتضررات من الإبلاغ عن الجريمة خشية كشف نظام حمايتها الضعيف حتى لا تكون عرضة لعمليات إجرامية أخرى وربما كذلك خوفهم من عمليات التفتيش التي تقوم بها جهات التحقيق وما يمثله ذلك من كشف لأسرارهم أو الاطلاع على معلومات وبيانات يتكتمون عن الإفصاح عنها ولا ترغب المؤسسات المتضررة بالكشف عنها هذا بالإضافة إلى خشيتها من تضرر سمعتها في السوق وهو ما يؤدي إلى عزوف الزبائن من التعامل معها في نظام الحماية الخاص بتلك المؤسسات كذلك جهل المجني عليهم من أن تلك الهجمات الإلكترونية هي أعمال إجرامية يعاقب عليها القانون أو عدم ثقتهم في جهات التحقيق.

اهتمام الشركات والمؤسسات بالجانب الترويجي والتسويقي لمنتجاتها وتحقيق الأرباح وإهمالها للجانب الأمني:

[1])_**سليمان بن مهجع العنزي**، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجيستر في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003، ص98.

رغبة من مختلف الشركات في بيع منتجاتها والحصول على أكبر قدر ممكن من الأرباعفإنها تلجا إلى تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها وزيادة المنتجات واقتصارها على تقديم الخدمة وعدم التركيز على الجانب الأمني.

عدم إدراك خطورة الجرائم المعلوماتية من قبل المجني عليهم: كما أسلفنا سابقا فإن جهل الأفراد والمؤسسات بمدى خطورة الجرائم المعلوماتية يجعلهم يتهاونون في الإبلاغ عنها ولا يتخذون احتياطاتهم لتفادي وقوعهم ضحايا تلك الجرائم كتأمين شبكاتهم وأجهزة الحاسوب التي يستعملونها ويتركونها عرضة لاختراق لسرقة البيانات منها حتى دون أن يدركوا ذلك.

الفرع الثاني: عقباتمتعلقة بجهات التحقيق:

تتعلق المعوقات القضائية التي تتولى التحقيق في:

1-نقص خبرة جهات البحث والتحري والتحقيق في الجرائم المعلوماتية:تواجه عملية استخلاص الدليل في جرائم المعلوماتية صعوبات جمة مثل نقص الخبرة لدىرجال لضبط القضائي أو أجهزةالأمن بصفة عامة وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي لهذا فإن عملية البحث والتحقيق في جرائم المعلوماتية هي في غاية الأهمية والصعوبة بالنظر للتكوين العلمي والتدريبي والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي والحكم وذلك لان حداثة جرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلماما كافيا بها، فلا يكفي أن يكون لهم الخلفيةالقانونية أو أركان العمل الشرطي فقط ولكن لابد من الإلمام في مجال الجريمة المرتكبة. بواسطةالإنترنت ومن أجل ذلك فإنه لابد من إيجادأسلوب خاص للتحقيق في تلك الجرائم يجمع بين الخبرة الفنية والكفاءة المهنية ومن الممكن لتحقيق ذلك إتباعالخطواتالتالية:

تبادل المعلومات بين المحقق وخبير الحاسوب وذلك قبل البدء في التحقيق واخذ أقوالالشهود والمشتبهفيهم أو استجواب المتهمين[1]حيث يغطي كل طرف النقص الموجود لدى الطرف الآخر أو يكمل له المهمة التي يريد القيام بها أو من المطلوب منه القيام بها حتى يتفادوا التناقض.

حصر النقاط المطلوب استجلاؤها من قبل الخبير والمحقق قبل في البدء التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

أخذ أقوال الشهود واستجوابالمتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيهالأسئلة التقنية التي لا يدركها المحقق والتي من الممكن أن تكشف الإجابة عنها خيوط الجريمة.

التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسوب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي يتم التحقيق معه.

2-الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية لاسيما وان هذه التقنيات أثبتت جدارتها ونجاحاتها في جميع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق

المطلب الثالث : عقبات مرتبطة بالجانب القضائي

تصطدم مسالة إثبات الجرائم المعلوماتية بالعديد عقبات والمسائل الهامة على الصعيد القضائي تتمثل أساسا في انعدام وجود آليات مرنة للتعاون الدولي في المجال الجنائي لمواجهة جرائم المعلوماتية بحكم أنها جرائم من طبيعة خاصة تتطلب عملية مواجهتها تكاثف الجهود وتنسيقها على المستوى الدولي الفرع ١ وبالخصوص عندما تصطدم أغلبيةإجراءات تحقيق المتبعة بهذه الجرائم بعقبات قانونية على غرار مسالة الاختصاص الفرع 2

[1])_United nation manuel one the prevention and control of computer-related crime, Vienna 1999

الفرعالأول: قصور التعاون الدولي في مجال مكافحة الجرائم المعلوماتية

باعتبارها لا تعترف بالحدود الإقليمية لكل دولة ويمكن ارتكبها عن بعد صارت الجريمة المعلوماتية محل جدل مثار بين عدة دول في النظام القانوني المطبق عليها لهذا فإن التعاون الدولي في مجال مكافحة هذا النوع من الجرائم وإثبات ها يعد مسالة هامة وحاسمة ولكنها في نفس الوقت مسالة معقدة لأسباب عدة نذكر منها:

صعوبة توحيد المفاهيم:لابد أن يؤسس أي تعاون دولي على مفاهيم موحدة غير مختلف فيها وهو أمر لا نجده في حالة جريمة المعلوماتية إذ هي لحد ألان محل اختلاف بين مختلف الأنظمة القانونية بالإضافة إلى أن عالم إجرام المعلومات ينطوي على الكثير من المصطلحات التقنية غير المستقرة بسبب تغير واختلاف مفاهيمها وتجددها المتطور[1]

تنوع واختلافالأنظمةالإجرامية:

التعاون الدولي لا يقتصر على الجانب الموضوعي بل يتعداه إلى التعاون الإجرائي بين مختلف الدول لان التعاون في حد ذاته يتطلب إيجاد وسائل إجرائية وآليات يتم من خلالها وإنه من شأن الاختلاف الموجود بين الأنظمةالإجرائية للدول أن يصعب من مسالة التعامل، كما أن التعاون في المسائل الإجرائية ومن أهم المسائل في مكافحة جرائم المعلوماتية خاصة وان هذه جرائم وبسبب طبيعتها وسرعتها ارتكابها أو سهولة إخفاء الأدلة الناتجة عنها يتطلب ذلك من مختلف الأنظمة القانونية الإجرائية أن تكيف الإجراءات التقليدية المتبعة من طرفها في التحقيق والمحاكمة بما يتوافق مع تلك الطبيعة والسرعة ففي اغلب الأحيان ما تختلف طرق وإجراءات التحري والتحقيق في دول ما عنها في دولة أخرى، وهي إجراءات وان كانت تثبت فعاليتها في دولة ما قد لا تكون مرخص بها أصلا كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية[2]

[1])_**عبد الحليم بن بادة**، اجراءات البحث والتحري عن الجريمة المعلوماتية، (الخصوصية والاشكالات)، مجلة الحقوق والعلوم السياسية، المجلد2، جامعة زيان عاشور، الجلفة،2015،ص93.

[2])_هلالي عبد الله أحمد، جرائم معلوماتية عابرة للحدود، دار النهضة العربية،ط2007،1، مصر، ص66.

الفرع الثاني:إشكالية الاختصاص القضائي

قواعد القانون الجنائي تخضع في تطبيقاتها من حيث المكان لمبدأ مستقر ومعروف هومبدأالإقليمية الذي يعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها ولا تخضع من حيث الأصل لسلطات أي قانون أجنبي وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها في القانون الدولي إلا في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام.

كما هو معلوم فإن الشبكة العنكبوتية لا تستأثر بها دولة بعينها حيث يتسنى لمستخدميها ولوجها من أي موقع في العالم تقريبا من خلال حاسوب يكون متصل بها فهي بطبيعتها لا تحدها حدود ومن ثم تكون من حيث المبدأخارج أي رقابة أو سيطرة من أي جهة وهذا يستتبع عدم كان خضوعها لسلطان قانون جنائي معين فجريمة سب مثلا عبر الرسائل الإلكترونية Email تقع أحيانا في بلد ويتلقاها الضحية في بلد آخر وهنا ينبغي أن يشير إلى أن هذه الرسائل وغيرها من أدواتالاتصال عن بعد بواسطة هذه الشبكة تمر فيه كثير من الأحيان لأكثر من دولة قبل وصولها إلى الاستقبال ناهيك أن بعض الأفعال التي تبثهم من خلال الانترنت تعد أحيانا جريمة في بلد ومباح في غيره من البلدان المرتبطة بهذه الشبكة[1]

لتوضيح اكثر حول قضايا السب والشتم عبر البريد او الرسائل الالكترونية نورد هذه القضية: واقعة المحضر2ح قسم المصنفات الفنية في ديسمبر 2008 (تشهير وسب وقذف) بشان قيام مجهود باختراق البريد الالكتروني في الخاص بالمجني عليها وسرقة محتوياته من صور خاصة بها وبيانات اصدقائها ومراسلات شخصية هامة ونشر ذلك على موقع فيسبوك واضافة عبارات تسيئ لسمعتها واضافة رقم هاتفها المحمول.

[1]) **ين بادة عبد الحليم**، مرجع سابق، ص95-96.

خاتمـــة

سعينا إلى محاولة الإحاطة بجوانب البحث ضمن رؤية إجرائية تتناول مسألة البحث و التحري تتناول مسألة البحث و التحري حول الجريمة المعلوماتية

الأمر الذي رصدناه في الفصل الأول هو الاستدلال و التحقيق في هاته الجريمة أين تناولنا من خلال هذه الدراسة النمط الإجرائي للجريمة المعلوماتية و أبرزت فيه البلاغ و الشكوى في الجرائم المعلوماتية و أيضا الاستجواب و سماع الشهود و هذا ما تطرقت إليه في المبحث الأول في هذا الفصل .

و تناولنا في المبحث الثاني هذه المسائل هو المجري المنطقي للأمور إذ لا يستقيم منطقا و لا عقلا أن يقوم المحققون من رجال الضبطية القضائية أو القضاء بالبحث عن دليل الإثبات الجريمة المعلوماتية .

وفيها بيننا الخصائص التي يتسم بها التحقيق و كذا الصفات التي يجب ان يتميز بها المحقق في هذا النمط من الإجرامي ، ثم فصلت القول فذكرت خصائص الدليل الرقمي كدليل مناسب الإثبات الجريمة المعلوماتية .

لذلك فقد توصلنا في هذا البحث إلى أن طبيعة الخاصة للجريمة المعلوماتية دعى المشرع الى إعادة تقيم بعض القواعد الإجرامية المتاحة في استخلاص الدليل كالتفتيش و جعلها ضائعة الاستعمال في مجال البنية الرقمية هو ما كان فعلا بموجب القانون 09-04 المتعلق بقواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها فضلا عن استحداث نوع من القواعد الإجرائية الأخرى تتلاءم مع طبيعة الرقمية التي يكون عليه الدليل المناسب في إثبات هذا النوع من الجرائم كالمراقبة الالكترونية و حفظ البيانات

حسب مفهوم المادة 44 من قانون الإجراءات الجزائية الفقرة الثانية المدرجة بموجب القانون 06-22 المؤرخ في 20_12_2006 فأنه لا يجوز لشرطة القضائية قي إطار التحري و التحقيق عن الجريمة المعلوماتية الانتقال إلي مساكن الأشخاص الذين يظهرون انه ساهموا في

ارتكاب هذه الجريمة الإجراء التفتيش هناك إلا بإذن مكتوب من الجهة المختصة وجوب استظهار هذا الإذن قبل الدخول إلى المسكن و المشروع في علمية التفتيش ، و عليه فالإذن في هذه المادة يتعلق حصرا في التفتيش لكن المشرع في القانون 09-04 أجاز في إطار التحري و التحقيق في الجريمة المعلوماتية تفتيش محل أخر غير السكن وهو المنظومة المعلوماتية دون ان يشترط الدخول إليها ضرورة الحصول على إذن من الجهة القضائية .

فحصول ضابط الشرطة القضائية على إذن يسمح له بالدخول إلىإمكانالتي تتواجد بها الحواسيب و تفتشيها لاختلاف محل التفتيش أصلا لذلك اقترح المشرع إضافة فقرة أخرى للمادة 05 من القانون 09-04 كمايلي : " **لا يجوز إجراء عمليات التفتيش في الحالات المذكورة أعلاه إلا باذن مكتوب من السلطة القضائية المختصة** "

مما لا شك فيه أن الصعوبات التي تعترض سبيل مكافحة الجريمة المعلوماتية متعددة ، وكلها تنبع من كون هذه الجرائم تختلف جملة و تفصيلا عن الجرائم العادية ، الأمر الذي بات يثير بعض التحديات القانونية و العملية أمامالأجهزة المعنية بمكافحتها، سواء أثناءإجراءات الاستدلال و التحقيق عبر و تقديمه للعدالة أو خلال ملاحقة الجناة و كشف جرائم عبر الحدود

لذلك تثور العديد من المشكلات التي تقف أمام مكافحة الجريمة المعلوماتية منها مايتعلق بالكشف عن الجريمة و الوصول إلى الجناة و بعضها متعلق بإثبات الجريمة المعلوماتية كما قد يبرز للوجود صعوبات متعلقة بالتعاون القضائي الدولي و تحديد قواعد الاختصاص .

قائمة المراجع

قائمة المراجع

أولا: الكتب

1. أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، طبعة الاولى ، دار هومة لنشر و التوزيع ،الجزائر، 2009 .
2. احمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري ، الجزء الأول ، الطبعة الخامسة ، ديوان المطبوعات الجماعية ، الجزائر ، 2003 .
3. خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترانت ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان 2011.
4. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الاولى ، دار الفكر الجامعي 2008.
5. خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية ، الطبعة الثانية ، الدار الجامعية ، الإسكندرية ، 2009 .
6. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الإلية في التشريع الجزائري المقارن ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، مستغانم 2012 .
7. سليمان أحمد أبراهيم ، القواعد الجنائية للجريمة المنظمة ، دار الكتاب الحديث، القاهرة 2008.
8. عبد العال الديري و محمد صادق إسماعيل ، الجرائم الالكترونية ، الطبعة الاولى، المركز القومي للاصدرات القانونية ، القاهرة
9. عبد الفاتح بيرمي حجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الانترانت ، دار الكتب القانونية ، مصر 2002.
10. عمرو عيسي الفقي ، الجرائم المعلوماتية (جرائم الحاسب الالي والانترنت في مصر و الدول العربية) الطبعة الاولى ، المكتب الجامعي الحديث ، مصر 2006.

11. محمد حزيط ، قاضي التحقيق في نظام القضائي الجزائري ، الطلعة الثانية ، دار هومة ، الجزائر ، 2010 .

12. محمد كامل شاهين ، الجوانب الإجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي ، دراسة مقارنة ، دار الجامعة الجديدة ، الإسكندرية ، 2008.

13. مصطفى محمود موسي ، التحقيق الجنائي ، في الجرائم الالكترونية ، الطبعة الأولى ، الأردن ، 2008 .

14. محمود عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبوتر و الانترنت ، دار الكتاب القانونية ، مصر ، 2006.

15. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع، الطبعة الأولى ، الأردن ، 2008.

16. هلالي عبد الله أحمد ، جرائم المعلوماتية عابرة الحدود ، دار النهضة العربية، الطبعة الأولى ، مصر، 2007 .

1-الرسائل و المذكرات الجامعية :

1-الرسائل:

1. حبيباتي بثينة ، الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، أطروحة لنيل شهادة الدكتورا ل م د في القانون العام ، تخصص قانون جنائي و علم الإجرام ، جامعة الجزائر 01 ، 14سبتمبر 2020.

2. ربيعي حسين ، آليات البحث و التحري في الجرائم المعلوماتية ، أطروحة دكتورا، جامعة باتنة 2015-2016

3. سليمان أحمد فضل ، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام الشبكة المعلومات الدولية (الانترنت) ،رسالة دكتورا من كليات الدراسات العليا ، أكاديمية الشرطة ، القاهرة ، 2007.

4.نبيلة هبة هروال ، جرائم الانترنت ، أطروحة لنيل شهادة الدكتورا في العلوم القانونية ، تخصص قانون، جامعة أبي بكر بلقايد ، تلمسان ، 2013-2014

5.سليمان بن مهجع الغنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجستير في علوم الشرطية ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض، 2003.

6.محمد بن نصير السرحاني ،مهارات التحقيق في جرائم الحاسوب و الانترنت، بحث مقدم استكمالا لمتطلبات الحصول على شهادة الماجستير في قسم العلوم الشرطية ، تخصص القيادة الأمنية ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا قسم العلوم الشرطية ، الرياض ، 2004 .

2- المذكرات:

1) مذكرات الماجستير :

1. سعيداني نعيم ، آليات البحث و التحري من الجرائم ، المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، تخصص علوم جنائية ، جامعة لخضر ، باتنة، 2013-2014.
2. يوسف الصغير ، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة ماجستير في القانون ، تخصص قانون دولي للإعمال ، جامعة مولود معمري، تيزي وزو ، كلية الحقوق و العلوم السياسية ، 2013.

2) مذكرات الماستر :

1. السوفي في نور الهدى ، التحقيق في الجريمة المعلوماتية ، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي ، شعبة حقوق تخصص قانون جنائي ، جامعة قاصدي مرباح ، ورقلة ، 2016-2017.

2. بختي فاطمة الزهراء ، إجراءات التحقيق في الجريمة الالكترونية ، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي، جامعة مسيلة ، كلية الحقوق و العلوم السياسية ، 2013-2014.
3. كوداد عبد الرحمان ، عملية التسرب على ضوء التشريع الجزائري ، مذكرة لنيل شهادة الماستر في الحقوق ، تخصص علم الإجرام ، جامعة الطاهر مولاي 2016-2017.
4. نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الاداري ، جامعة أحمد دراية ، أدرار ، 2016_2017
5. غرباوي نادية ، اساليب البحث و التحري في الجرائم المعلوماتية ، مذكرة لنيل شهادة الماستر في القانون الجنائي ، تخصص في القانون الجنائي ، جامعة أكلي محند أولحاج ، البويرة 2016-2017

2-المقالات والمجالات :

1. رضا هميسي ، تفتيش المنظومة المعلوماتية ، في القانون الجزائري، مجلة العلوم القانونية و السياسية ، جامعة الوادي ، العدد 5، جوان 2012.
2. عبد المؤمن بن الصغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت ، في التشريع الجزائري و المقارن ، بحث مقدم إلى أعمال الملتقي الوطني حول الجريمة المعلوماتية بين الوقاية ، والمكافحة ، كلية الحقوق ، جامعة بسكرة، المنعقد بتاريخ 16و 17 نوفمبر 2015.
3. محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي و الانترنت ، المجلة العربية للعلوم الأمنية ،العدد ثلاثون ، أكاديمية نايف العربية للعلوم الامنية 2000.

3-النصوص القانونية :

1. المرسوم رقم 09-04 ، المؤرخ في 16 غشت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، الجريدة الرسمية العدد 47 ، بتاريخ 05 غشت2009 .

2. المرسوم الرئاسي رقم15-261 المؤرخ في 08 أكتوبر 2015 ، يحدد تشكيلة و تنظيم و كيفية سير الهيئة الوطنية للوقاية الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، الجريدة الرسمية ، عدد 53 ، [بتاريخ 08 أكتوبر 2015.

3. أمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021، يتمم الأمر رقم 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8يونيو سنة 1996 و المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية للجمهورية الجزائرية العدد 65 بتاريخ 26 غشت سنة 2021.

4-المواقع الالكترونية:

1. الموقع الرسمي لمركز الشكاوي الخاصة بجرائم الانترنت https://complaint.ic3.gov/default. Aspx تاريخ الدخول 2019\01\03.

2. Htps://www.internet.signalenente.gouv.fr/ portail web/ planets /signaler etape choix type conten input .action. com. Date de consultaion 07/06/2017.

3. Untied nation manuel one the prevention and control of computer.related crime vienna 1999.

فهرس المحتويات