جامعة البشير الابراهيمي – برج بوعريريج –

كلية الحقوق والعلوم السياسية

قسم الحقوق

دور رجال الضبطية القضائية في مكافحة الجريمة الالكترونية

مذكرة تخرج لنيل شهادة ماستر

تخصص: قانون إعلام آلي وأنترنت

إعداد الطالبين **تحت إشراف الأستاذ**

– وشن لبنى **الدكتور/ خنتاش عبد الحق**

– نباش مراد

لجنة المناقشة:

السنة الجامعية: 2022/2021

بسم الله الرحمن الرحيم

(يرفع الله الذين آمنوا منكم والذين أوتوا العلم

درجات)

صدق الله العظيم

سورة الإسراء الآية 85

إهـــداء

إلى الوالدين الكريمين رزقهما الله الصحة والعافية

إلى زوجي الغالي الذي دائما إلى جانبي

إلى إخوتي وأخواتي

وإلى قرة عيني أبنائي رتيل، زهراء ، أنس، محمد

وإلى زميلاتي وزملائي المحامين وزملائي بالدراسة حفظكم الله جميعا ورعاكم

وشن لبنى

شكر وعرفان

نحمد الله عز وجل الذي وفقنا لإتمام هذا العمل وسخر لنا كل الأسباب لذلك، وبهذا نتقدم بخالص الشكر للأستاذ الفاضل ** خنتاش عبد الحق** الذي كان عونا وسهل العمل لإنجاح هذه المذكرة

كما نتقدم بجزيل الشكر إلى أساتذة وموظفين وعمال كلية الحقوق والعلوم السياسية وكل من كان عونا وأمدنا علما

مـــــــقـــــدمـــــــــة

مقدمة :

إن التطور العلمي للبشرية باكتشافاتها في مجال الاتصالات والمعلوماتية وشبكة الانترنت الت جعلت العالم قرية صغيرة متصل ببعضه البعض، ونشات معه التجارة الالكترونية والتي توسع نشاطها عالميا وزادت قيمة المبادلات النقدية الالكترونية فيها ونشأت عملة نقدية الكترونية.

كما تم تبادل على الشبكة المعلوماتية النتاج الفكري للإنسانية من كتب علمية وأدبية وموسيقى وافلام وكذلك النتاج الصناعي من اختراعات وعلامات تجارية، وكذلك أصبحت الحكومات تدار الكترونيا بربط الوزارات والإدارات بشبكة الإنترانت وتم خلق ما يسمى بالحكومة الالكترونية.

مع إيجابيات هذا التطور الا ان له سلبيات ومنها تعرض هذه الشبكة والمعاملات التجارية والمصرفية ومن نتاج فكري وصناعي ومعلومات أمنية لإجرام جديد يختلف عن الاجرام التقليدي من عدة نواحي سواء من حيث نوعية المجرم وكفاءته التقنية أو نوع الجريمة من جريمة مادية الى جريمة رقمية تقترف بواسطة جهاز الحاسوب وعبر شبكة الانترنت لإحداث آثار مختلفة سواء قرصنة الكترونية بسرقة مال الغير أو سرقة بيانات اشخاص او مؤسسات او دول ، بينما يرجع البعض الآخر البداية الحقيقية لظاهرة الجرائم الإلكترونية إلى عام 1985م حينما بدأ معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية رصد حالات ما مسي في ذلك الحين بإساءة استخدام الحاسوب بصورة منظمة، فهذا النوع من الاجرام لا يعترف بالحدود فهو عابر للحدود ويرتكب

في عالم مجرد وفي زمن قصير وآثاره سريعة الزوال بمحوها من المجرم ويمس بحرية الاشخاص ويضرب ثقة الانسان في التعاملات التجارية عبر الانترنت مم يؤكد على أهمية دراسة الجريمة المعلوماتية من حيث أسباب ظهورها وكذا شخصية المجرم وسبب نزوعه لهذا النوع من الجريمة ومن ثم دراسة أساليب مكافحتها الوقاية منها والأجهزة المتكفلة بذلك سواء المشرعون القانونيون أو القضاء أو رجال الضبطية القضائية.

فكان على التشريع أن يتلاءم مع هذا التطور في الإجرام من تقليدي الى تقني والكتروني وهذا بتدعيم قانون العقوبات بسن قوانين تتماشى مع الجريمة الالكترونية، ومنها منع الدخول غير الشرعي للمواقع الالكترونية بقصد القرصنة أو السرقة بكل صفاتها أو لتخريب المواقع بنشر فيروسات مم يعود بالخسارة المادية أو المعنوية لملاكها.

كما كان على القضاء أن يتطور تقنيا وماديا للتلاؤم مع النوع الجديد من الجريمة وذلك بتكوين قضاة في مجال الإعلام الآلي والانترنت وتخفيف وسرعة المواجهة للجريمة الالكترونية والتي تتصف بذلك بعكس الجرائم التقليدية والتي تستغرق زمنا لتنفيذها.

وبالضرورة كان لرجال الضبطية القضائية أن يتطوروا من حيث تكوينهم التقني وتجهيزهم بأجهزة متطورة وحبذا لو كان من بينهم عناصر ذكية وذات كفاءة لمواجهة القراصنة الالكترونيين وعادة ما توظف الدولة عناصر تائبة من فئة المجرمين في الاعلام الآلي.

أما سبب اختيارنا لهذا الموضوع فهذا لكونه موضوع العصر في مايخص الإجرام السيبراني الى جانب آثاره الوخيمة على المجتمع المحلي او الدولي، فهو إجرام إلكتروني

خفي من مجرم خبير بالتقنية تمس المعطيات الآلية على مستوى شبكة الانترنت وأما اختيارنا لرجال الضبطية القضائية فهذا مرده الى قلة التطرق لهذا الجهاز المهم في الكشف عن الجريمة المعلوماتية ومكافحتها باعتباره جيش الدفاع الأول عن المنظومة المعلوماتية والذراع المختصة في مواجهة المجرم السيبراني.

وقد يرجع كذلك الى عدم تطور دولنا في المعلوماتية باعتبار الغرب المتقدم في هذا المجال، إلا أن الجريمة الإلكترونية بدأت في الانتشار في مجتمعنا فأصبح من الضروري التجهز لمكافحتها برجال ضبطية اكفاء واذكياء متمكنون من تقنيات الاعلام الآلي ومجهزون بأجهزة متطورة للتصدي للإجرام السيبراني.

أما المشاكل التي واجهتنا في البحث فهي قلة الدراسات والأبحاث حول دور الضبطية القضائية في مكافحة الجريمة الالكترونية.

الإشكاليات المطروحة في مذكرتنا فهي من هم رجال الضبطية القضائية المعنيون بمواجهة الجريمة المعلوماتية ثم الاشكال الثاني المطروح فهو هل المنظومة القانونية تعطي دورا كبيرا لرجال الضبطية القضائية لمواجهة الإجرام الإلكتروني وأخيرا ما مدى اعتماد القضاء على رجال الضبطية القضائية في مكافحة الجريمة.

ففي الفصل الأول سنتطرق في المبحث الأول لماهية الجريمة الالكترونية بتعريفها فقها وقانونا ومن ثم ذكر خصائصها فأركانها من مادي ومعنوي وشرعي، ثم في مطلب ثاني نتطرق لأنواع الجرائم الالكترونية، وفي المبحث الثاني سنعرج على محترفي الجرائم

الإلكترونية من حيث أشخاص الجريمة الإلكترونية والصفات التي يتميزون بها، ثم سنذكر أسباب الجريمة الالكترونية وآثارها.

وفي الفصل الثاني نتطرق في المبحث الأول إلى الضبطية القضائية بين المتابعة وأساليب مكافحة الجريمة الالكترونية وفي المبحث الثاني نتطرق إلى آليات محاربة الجريمة الإلكترونية، ثم نختم بتوصيات.

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

في وقتنا الحاضر تخلى الانسان بفعل ما وفرته له تقنية المعلوماتية في مجال التعامل مع المعلومة ،سواء من حيث نقلها أو تخزينها أو استرجاعها بل حتى استعمالها للتنبؤ بما قد يحدث مستقبلا، وذلك من خلال انتشار الحواسيب على أعلى نطاق وظهور تقنيات حديثة لتبادل المعلومات والاتصال في شكل وشبكة الانترنت، كل ذلك خلق جانبا مشرقا تمثل في تحسين شبكة المعلومات الدولية (The Web). وتيسير عمل الدول والحكومات والمؤسسات في مجال التعامل فيما بينها، أو مع المجتمعات التي تحكمها وتتعامل معها.

كما ساهمت هذه التقنية في تطور نمط حياة الانسان الذي أصبح يعتمد بشكل شبه كامل على الحواسيب وشبكات الاتصال وتبادل المعلومات لأجل قضاء حوائجه دون عناء التنقل من مكان لآخر سعيا وراء المعلومة أو المرفق، غير أنه وبالموازاة مع ذلك ظهر جانب مظلم لهذه التقنية تمثل في سوء مزياها لأجل الاعتداء على مصالح الغير المتمثلة في جملة المعلومات ذات الطابع المتاح أو السري المتداولة عبر النظم المعلوماتية من خلال الحواسيب والشبكات، وذلك من قبل فئة اصطلح عليها وصف مجرمي المعلوماتية (1).

(1)غازي عبد الرحمان هيان الرشيد،الحماية القانونية من جرائم المعلوماتية الحاسب والانترنت، أطروحة لنيل درجة دكتوراه في القانون، الجامعة الاسلامية في لبنان ، كلية الحقوق،2004، ص 92.

المبحث الأول

ماهية الجريمة الإلكترونية

من أجل التعرف على ماهية الجريمة الالكترونية لابد من التطرق للتعريفين الفقهي والقانوني لها ومن ثم التطرق لخصائصها ودوافعها فهي جريمة معاصرة وحديثة قد اجتهد الفقهاء والقانونيون في تعريفها واستخلاص خصائصها، فمن جهة نجدها تختلف عن الجريمة التقليدية من حيث الوسيلة فالجريمة الالكترونية وسيلتها الوسائط الالكترونية وشبكة المعلوماتية والانترنت عكس وسائل الجرائم التقليدية، وثانيا موضوع الجريمة الالكترونية يمس ميادين لا تتعلق بالجريمة التقليدية، وأخيرا فان مكافحة الجريمة الالكترونية تستوجب الماما بالتقنيات الحديثة.

وتعد الجرائم الالكترونية جريمة معاصرة وحديثة بحداثة وسائلها من حاسوب أو شبكة معلوماتية، وكذا ارتباطها بعالم التجارة الالكترونية والمصارف الالكترونية وكذلك مجالات الجوسسة الاقتصادية والتجارية.

المطلب الأول

تعريف وخصائص الجريمة الالكترونية

إن البحث البحث في إيجاد التعريف المناسب للجريمة الالكترونية تكتنفه الكثير من الصعوبات، ويرجع السبب في ذلك الى عدم توصل الفقهاء الى وضع مفهوم شامل يحدد ماهية الجرائم الالكترونية ويحصر نطاقها، ليس هذا فحسب بل إن تعدد مسمياتها عقد من محاولة فهم هذه الظاهرة الحديثة نسبيا واختيار التعريف المناسب لها، فقد تنوعت التغيرات على الجريمة الالكترونية(1)، مما أدى الى الاختلاف وتعدد التسميات التي تطلق على هذا النوع من الإجرام، ونظرا لحداثته والذي ولد نتيجة التطور العلمي والتكنلوجي الهائل والمتسارع الذي شهدته البشرية(2).

معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري ةالتشريع المقارن، مذكرة نيل شهادة ماجستير، كلية الحقوق، جامعة العقيد الحاج لخضر باتنة، 2012/2011 ص05.

(2) لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، (دراسة مقارنة)،دار الحامد للنشر والتوزيع،الطبعة الأولى،عمان الأردن 2015،ص20.

الفرع الأول

تعريف الجريمة الإلكترونية

إن الظهور الحديث لهذه الجريمة جعل من تعريفها في تطور وفيه اختلاف كبير بين الفقهاء وعلماء التقنية، فهناك اختلاف بين الجانب التقني والقانوني في مفهومها كما ظهر اختلاف ثاني بين الوسيلة المستعملة فيها وبين موضوعها أو محلها.

أولا: المدلول الفقهي.

فالاختلاف الأول بين الفقهاء كان بين معناها التقني والذي يتجه الى تعريفها على أنها كل عمل غير مشروع تستخدم فيه أجهزة الاعلام الالي من حاسب او هاتف ذكي.

ثانيا: المدلول القانوني.

أما الاتجاه القانوني لتعريف الجريمة المعلوماتية فيذهب لتعريف قانوني لمفردات مهمة فيها من حاسب آلي أو معلوماتية أو البيانات أو التجارة الالكترونية.

الاتجاه الثاني في التفرقة بين الوسيلة والموضوع فيرى ألفقيه الألماني تاديمان أن الجرائم المعلوماتية هي (كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي)(1)

(1)/K Tiedemen fraude et aetesd affairs commise al aidedordinateurElenorigue rev Drypen .crim 1989.

أما من حيث موضوع الجريمة فقد عرفها خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية بأنها **"كل سلوك غير مشروع ومناف للأخلاق او غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"**وذلك إذا اتجه قصد الجاني الى تخريب البيانات او قرصنة برامج أو تحريفها. بينما ذهب اغلب الفقهاء الى تعريف شامل للجريمة الالكترونية كالآتي:

كل نشاط إيجابي او سلبي من شانه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي أو بنظام المعلومات العالمي الأنترانت، أو الإبقاء عليه عند تحققه . أو التأثير عليه بتعطيله أو اضعاف قدراته على أداء وظائفه بالنسخ أو التعديل بالإضافة او الحذف الكلي او الجزئي او بالمناقلة للخصائص الأساسية للبرامج او بمجرد النسخ أو الوصول الى البرامج ،او المعلومات المخزنة او الوصول اليها اثناء نقلها او ارسالها او الاتصال بها من غير وجه حق بأي وسيلة كانت. **(1)**

حيث أن التعريف جاء شاملا لحد ما بوصفه الجريمة الالكترونية على أنها فعل أو عمل إيجابي أو سلبي بدون وجه حق أي غير مشروع باتصاله بواسطة جهاز حاسب كوسيلة للجريمة بشبكة المعلوماتية الأنترنت وهي المجال المعنوي حيث يتم تبادل البيانات والمعلومات كموضوع أو محل للجريمة، عن طريق نسخ أو حذف أو مناقلة

([1]) محمد حماد الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية، بحث منشور في مجلة الشريعة والقانون، العدد27، جمادى الثانية 1427 هـ – يوليو 2006، ص427.

للبيانات و لخصائص برامج بقرصنتها أوبنسخها للوصول لمعلومات مخزنة ذات قيمة.

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة رقم 02من القانون 09-04 على أنها: "**جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية(1)**، بمعنى كل الجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعلومات أو عن طريق منظومة معلوماتية، كما نصت عليها المواد 394 و394 مكرر 7من قانون العقوبات الجزائري.

الفرع الثاني

خصائص الجريمة الإلكترونية:

إن الجريمة المعلوماتية تختلف من الخصائص عن الجريمة التقليدية كالسرقة او القتل، فهي جريمة حديثة تتسم بخصائص خاصة بها.

1/ تتميز الجريمة المعلوماتية باستعمال المجرم للحاسب الالي كوسيلة لارتكاب الجريمة عبر شبكه المعلوماتية. بينما الجرم الذي يمس الحاسب الآلي كجهاز مادي سوآءا بسرقته أو تحطيمه فهذه جريمة تقليدية (تحطيم ملك الغير).

(1)-المادة 2/أ من القانون رقم 04/09 المؤرخ في 5 أوت 2009 .

2/ **انها جريمة عابرة للحدود** فالمجرم قد يقترف الجريمة المعلوماتية في بلد ما بينما يكون ضحية جرمه في بلد آخر، كأن يقرصن ارصدة في بلد أجنبي انطلاقا من بلده. مما يسبب اشكالا حول القانون الواجب التطبيق لإقليمية الجريمة. وهذا ما يسمى بعولمة الجريمة.

3/ **انها جريمة لا يتم التبليغ عنها** في الغالب من الشركات التي تكون ضحية لها خشية فقدان ثقة العملاء والشركاء في مصداقيتها ومستوى الأمان في معاملاتها.

4/لا توجد احصائيات دقيقة لعدد الجرائم المعلوماتية المرتكبة سنويا، وذلك بسبب عدم(1)

تعاون المجني عليهم مع الأجهزة الأمنية، حيث أنه لا يقوم بالتبليغ عن الجريمة في حقه.

5/ كما تتميز الجريمة المعلوماتية **بصعوبة كشف آثارها** أو اثباتها فهي تتم في عالم رقمي مجرد بواسطة رموز لا يترك أثرا مثل الجريمة التقليدية سوآءا بصمات أو أثر للحمض النووي او غيره، مم يصعب عمل الأجهزة المكلفة بمكافحتها وتتطلب إمكانيات تقنية متطورة لتتبع آثارها.

6/ الجريمة المعلوماتية تتطلب في المجرم الالمام بتقنيات الحاسب الآلي ويتميز بالذكاء الخارق والعبقرية في هذا المجال، فلا يمكن ان ترتكب من جاهل بالتقنية.

هذا وان الالمام بالتقنية للحاسب الآلي غالبا ما تتيح للجاني طرقا ليعيق عمل الشرطة أو السلطة المنوطة بالتحري للوصول للدليل، مثل إضافة كلمات سر أو دس تعليمات خفية

(1)– د مجيد ناصر الفتال ، أمن المعلومات ،دار اليازوري للنشر والتوزيع عمان الأردن بدون سنة النشر ص 20

بينها لتصبح كالرمز او بتشفير البيانات. مما يستوجب بالتالي ضرورة الاستعانة بالخبرة الفنية عالية المستوى(1).

7/ ان الجريمة المعلوماتية لا تتميز بالعنف لا يحتاج الجاني لاستعمال القوة الجسدية لأنها تتعلق باستعمال الخبرة الفنية والذكاء عكس الجريمة التقليدية.

(1) المستشار صالح بن علي، الجريمة المعلوماتية ومخاطرها، مجلة ارؤيا، 2003 العدد45 ص 04.

المطلب الثاني

أركان الجريمة الالكترونية وأنواعها

تنهض الجريمة على ركنين هما الركن المادي والركن المعنوي فلابد للجريمة المعلوماتية إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها ، ولابد أيضا من ركن معنوي يعبر عن إرادة المجرم المعلوماتي. وهناك الركن الشرعي فلا جريمة ولا عقوبة إلا بنص.

االفرع الأول

أركان الجريمة الإلكترونية

تقوم جرائم الدخول غير المشروع والبقاء، على مبدأ عدم إحداث أي تأثير سلبي على الأنظمة المعلوماتية، ويقوم بهذا النوع من الأنشطة ما يطلق عليهم المخترقون ذوي القبعات البيضاء، مستغلين الثغرات الأمنية لتلك النظم ومخترقين اجراءات الأمن المعلوماتي وذلك بهدف الوصول إلى معلومات محاطة بالخصوصية والسرية، وقد يتعدى ذلك إلى إتلاف ألمعلومات(1).

---

(1) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت،دار الثقافة، الأردن، 2011ص 90

أولا: الركـن المـــادي.

ويمثـل كيان الجريمـة وهو عبارة عـن فعـل الفاعـل بصـورة يمكن إثباتهـا كجريمـة وبـه يتحقـق الاعتـداء علـى المصلحـة المـراد حمايتهـا وعـن طريق هـذا الفعل تقع الأعمـال التنفيذيـة للجريمة فهو يمثل النشاط الذي يصدر عن الجانـي ليتدخـل مـن أجـل

هـذا الفعل النظام ويقوم بعقابه (2) ويتكون من عنصرين:

المحل الاجرامي: معطيات نظام المعالجة الالية.

السلوك الاجرامي: ادخال، إزالة، تعديل معطيات.

إن السلوك الاجرامي في الجريمة الالكترونية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها للحاسب، وصعوبة المشكلة أن السلوك الاجرامي قد يتحقق بمجرد الضغط على زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير او السرقة عن طريق التسلل الى نظام ارصدة العملاء في البنوك أو إساءة

استعمال بطاقات الائتمان والسلوك الإجرامي في الجريمة المعلوماتية يتطلب ود بيئة رقمية وجهاز حاسب آلي متصل بالشبكة المعلوماتية الويب، وفي الحقيقة يصعب

---

(2).بوضياف اسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر،العدد الحادي عشر،جامعة محمد بوضياف المسيلة، 2018 ص 353.

الفصل بين العمل التحضيري والبدأ في النشاط الاجرامي في جرائم الكمبيوتروالانترنت حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية إلا أنه في مجال تكنلوجيا المعلوما، الأمر يختلف بعض الشيء، فشراء برامج الاختراق ومعدات لفك الشفرات وكلمات المرور وحيازة صور دعارة للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

ثانيا: الركن المعنوي

ويعبر عن إرادة المجرم الالكتروني **(القصد الجنائي)** فلابد أن يرتكب الفعل المَجّرم من شخص حر بإرادة فعلية بطواعية ورغبة وعن إدراك وذو أهلية وخال من عيوب الإرادة. فالعلم يعني علم الجاني بالصفة الاسمية او الشخصية للبيانات وان يعلم

إن من طبيعة الحاسوب الالكتروني اجراء المعالجة الالكترونية لهذه البيانات دون ترخيص من اللجنة المختصة بذلك اما الارادة فهي أن تتجه ارادة الجاني إلى اجراء المعالجة الالكترونية لهذه البيانات بأية صورة كانت أي بالمخالفة لاتخاذ الاجراءات الاولية لإجراء المعالجة الالكترونية للبيانات وهنا تطرح إشكالية المجرمين القصر فعقابهم يكون حسب نوع الجريمة(1).

(1) لينا محمد الاسدي، معوقات مكافحة الجريمة الالكترونية، رسالة ماجستير،جامعة عمان الأردن، 1434 هـ ص 83

فالركن المعنوي هو الحالة النفسية للمجرم، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني او النفسي له باعتباره المحور الأساسي للقانون الجنائي ذلك انه في اطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع اقرارحق الدولة في العقاب الذي يبنى عل هذه المقومات.

ثالثا: الركن القانوني (الركن الشرعي)

وهو الركن الذي يضع النص لتجريم هذا الفعل المقصود من المجرم فالقاعدة القانونية تنص على أنه (لا جريمة ولاعقوبة إلا بنص) ولقد تم التجريم في نظام مكافحة الجرائم المعلوماتية وتم وصف الجريمة وصفاً دقيقاً سنتعرف عليها في أنواع الجرائم المعلوماتية وفي الجزائر نص على ذلك القانون 04/09 وقانون العقوبات في المواد 394 و349 مكرر 7 (2).

(2) أنظر القانون 04/09 وقانون العقوبات في المواد 394 و349 مكرر 7.

الفرع الثاني

أنواع الجريمة الإلكترونية

إن للجريمة المعلوماتية عدة أنواع ولها بالمقابل دوافع تختلف عن الجريمة التقليدية وتترك آثار مدمرة في المجتمع والاقتصاد والأمن القومي .

تتنوع الجريمة المعلوماتية حسب محلها أي ما تمسه بالضرر فمنها ما يمس المال ومنهاما يمس الأشخاص ومنها ما يمس المعالجة الآلية للمعلومات ....

أولا: جرائم الأموال.

وتختص بجرائم التحويل المصرفي للأموال بطريقة غير مشروعة وغسيل الأموال، والتجارة الالكترونية وهي:

1-جريمة التجارة الالكترونية.

فالتجارة الإلكترونية هي نظام يتيح عبر شبكة الإنترنت حركات بيع وشراء وتأجير السلع والخدمات والمعلومات .ويمكن تشبيه التجارة الإلكترونية بسوق الكتروني يتقابل فيه البائعون والموردون والمستهلكون وتقدم فيه المنتجات والخدمات يصوره رقمية أو افتراضية ويتم دفع ثمنها بالنقود الإلكترونية. (1)

---

(1)-عبد الله الدغمش ، الجرائم المراكبة عبر مواقع التواصل الاجتماعي،العدد39 ، ص 16،

وقد تنامت التجارة الالكترونية لتصبح تدار بمئات المليارات، مما زاد الاجرام حولها ويمس كثيرا المستهلكين بسبب تعاملاتهم بالبطاقات الإلكترونية والتي تتعرض للقرصنة بتحويل الأموال بطريقة غير مشروعة. كما أن المستهلك قد يتم تضليله عبر إعلانات مضللة.

2/جريمة التحويل المصرفي للأموال

إن نظام التحويل المالي الالكتروني بين المصارف والبنوك جد مهم وخطير لما له أهمية في التجارة الالكترونية حيث يتم عبره دفع المال المقابل للخدمات أو السلع التي يتبادلها التجار بينهم أو مع المستهلكين. ويعتبر نظام SWIFTمن أهمها في العمل البنكي للتحويلات المصرفية بين الدائن والمدين لتسوية المعاملات التي تتم بينهم.ـ

ومن صور التعدي على نظام التحويل الإلكتروني للأموال ما أشار إليه التقريرالصادرعن إدارة العدالة الأمريكية لعام 1982بعنوان جرائم الحاسب الآلي والتحويل الإلكتروني للأموال ويتم التلاعب في نظام التحويل الإلكتروني للأموال بأي وسيلة من وسائل الاحتيال المعلوماتي، حيث يتم التلاعب عند إدخال البيانات أو في برامج الكمبيوتر أو في المكونات المادية له أو أثناء عملية نقل البيانات إلكترونيا(1).

(1)–عبد الله الدغمش ، المرجع السابق، ص 16

3-جريمة غسل الأموال الكترونيا

وهي جريمة تتعلق بتحويل أموال مصدرها غير مشروع مثل المخدرات أو الإرهاب أو تجارة التهريب من مصرف الى آخر الكترونيا وتنتشر كثيرا في دول أمريكا الجنوبية.

وقد شرع المشرع الجزائري قانونا خاصا بجرائم الفساد عدد من بينها جريمة غسيل الأموال.وهي من الجرائم المعاصرة وتقوم بها منظمات إجرامية، ويقصد بغسيل الأموال توظيفها داخل الدولة أو خارجها في أعمال مشروعة وذلك لطمس الأصل غير المشروع لهذه الأموال (1)

وتستعمل الشبكة المعلوماتية كأرضية للغسيل بسبب سرعتها وسهولة التحويل باستعمال البطاقات الالكترونية.

4- الجريمة الواقعة على بطاقات الائتمان:

ان من أهم منتجات التجارة الالكترونية والمصارف هي البطاقات الائتمانية وهي وسيلة الكترونية توزعها المصارف على زبائنها بضمان رصيد بنكي حيث يستعملها لشراء سلع أو الاستفادة من خدمات.

---

(1)- مجلة المعلوماتية. العدد362 أكتوبر 2011ص.4

أصبحت البطاقة محلا للاستهداف الاجرامي من المجرمين المعلوماتيين بسرقة البيانات الخاصة بها وصناعة نماذج منها للقيام بسحب أموال أو شراء سلع بطريقة غير مشروعة من الإعتداءات التي تقع على البطاقة الإئتمانية باعتبارها محل للحقوق مالية سرقة البطاقة عن طريق حاملها بصورة مباشرة، فالسارق سواء إستعمل البطاقة أو لم يستعملها، فهو يعد ارتكب لجريمة السرقة لمجرد توافر أركان هذه الجريمة (1).

ثانيا: جرائم الاعتداء على الأشخاص

إن حياة الانسان وحرمتها من اهم حقوق الانسان التي نص عليها ديننا الحنيف وكذلك المواثيق الدولية خاصة منظمة حقوق الانسان. فالجرائم الالكترونية تعدت المساس بالمال الى المساس بحرمة الانسان وحريته الشخصية واسرته وكل ما يتعلق بحياته الشخصية.

وهي جرائم ذات قيمة معنوية وأدبية غير مادية أي تمس الجانب المعنوي للإنسان، ومنها القذف والسب وسرقة البيانات الشخصية والتهديد والابتزاز والتجسس وانتهاك حرمة البيوت، هنا سنتحدث عن بعض الأنواع الجرائم التي تقع على الأشخاص عبر الانترنت.

ويذ كر أن الحامل الشرعي لبطاقة الإئتمان ممغنطة يفقد صفته كحامل شرعي لهذه البطاقة منذ إبلاغ بسرقتها أو فقدها، وبالتالي المعارضة فيها لدى البنك المصدر لها .

(1) عبد الكريم الردايدة. ، جرائم بطاقات الائـتمـان لدراسـة تطبيقيـة ميدانية، الطبعـة الأولى، الأردن، دار حامد، 2013 ص .32

ولذلك فهو يعد من الغير بالنسبة لها في حالة إساءة استعمالها ومن ناحية أخرى فإن التاجر قد يرتكب غشا بقبول البطاقة المسروقة أو المفقودة في الوفاء، وذلك بالتواطؤ مع الجاني، حيث يقوم التاجر بعمل فواتير وهمية لاتقابلها مشتريات حقيقية مستخدما في ذلك الطباعة اليدوية(1).

1-جرائم القذف والسب

وهي جرائم شائعة على شبكة الأنترنت. حيث توجد مواقع متخصصة تعمل على

إبراز سلبيات الشخص المستهدف وافشاء اسراره، والتي غالبا ما يتم الحصول عليها بطرق غير مشروعة بعد الدخول على جهازه عن طريق تلفيق الاخبار (2).

وهذه الجرائم تستهدف النيل من كرامة المجني عليه او فضحه وفضح اسراره على شبكة الانترنت اما بغرض الانتقام منه او للابتزاز. او قد ترتكب هذه الجريمة بواسطة شبكة المعلوماتية العالمية من خلال اسناد مادة كتابية او صوتية او فيديو، تسيا الى أحد الأشخاص ومن شئنها ان تنال من شرفه (3).

(1)-عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية ، الكتاب الثاني الحماية الجنائية لنظام التجارة الالكترونية، الطبعة الأولى، الاسكندرية، دار الفكر الجامعي، 2002 ص 336

(2)-د مدحت رمضان ، جرائم الاعتداء على الأشخاص والانترنت ،دار النهضة العربية –القاهرة-2000 ، ص 87

(3)-محمد حماد الهيتي مرجع سابق ص 167.

ويقوم في الغالب الجاني بإخفاء هويته عن طريق برامج حاسوبية تخفي العنوان البريدي لها او ما يسمى ب IP وهذا تهربا من العقاب او الخجل من التصرفات اللائقة التي يقومون بها.

وهنا نخلص الى نتيجة مفادها ان جرائم القذف السب تمارس من خلال الاستغلال السيء للأنترنت وارتكاب هذه الجريمة عبر شبكة الويب العالمية، الا اننا نقف عند نقطة مفادها التساؤل عن الاختصاص القضائي بين بلدان قد تجيز حرية التعبير عن الراي، كما ان هذه الأفعال قد لا تعد من قبيل اعمال الذم والقدح والتحقير، وفي دول أخرى تعد.

في حين تسعى بلدان أخرى الى تطبيق قوانينها المحلية على كل ما يمكن ان يمس كرامة واعتبار الافراد، وبالتالي ضرورة التشريعات التي تنظم هذه المسائل وبنصوص خاصة، فيما لو ارتكبت عبر الانترنت ومواجهة العلانية بطريق الانترنت بما يتماشى مع مبدا الشرعية الجنائية(1).

2-جرائم غير جنسية

تستهدف الأشخاص بعدة أوجه منها القتل بالكمبيوتر –التسبب بالقتل –الإهمال المرتبط بالحاسب الآلي–التحريض على الانتحار –التحريض القصدي للقتل عبر الانترنت –

1- د لينا محمد الاسدي مرجع سابق ص 56.

التحرش والمضايقة عبر وسائل الاتصال المؤتمنة–الملاحقة عبر الوسائل التقنية أنشطة اختلاس النظر والاطلاع على البيانات الشخصية.

3–الجرائم الجنسية

ومنها تحريض القاصرين على أفعال جنسية غير مشروعة –افساد القاصرين عبر الانترنت اغواء القاصرين لارتكاب أفعال جنسية غير شرعية–نشر وتسهيل المواد الجنسية عبر الانترنت بوجه غير مشروع ترويج الدعارة بصورة قصرية للإغواء او نشر المواد الفاحشة.

"لقد سعى المجتمع الدولي إلى التدخل لمواجهة الانتهاكات التي تقع على الأطفال نتيجة لظهور الإباحية والخلاعة على الانترنت عبر المواقع الإباحية وغرف الدردشة والبريد الالكتروني، والتي غالبا ما تعرض الأفلام الإباحية والصور الخليعة والتي منها ما يتعلق بالأطفال(1)

وقد تولى قانون العقوبات حماية حرمة الأشخاص عبر المواد 394 و394 مكرر7،"هذا وتدخل ضمن الحياة الخاصة ضرورة توفير الحماية الجنائية للبيانات الشخصية ضد الاعتداءات اتي تقع عليها.

---

(1)–د عبد الفتاح بيومي حجازي ، الاحداث والإنترانت – دار الكتب القانونية –سنة 2002 مصر ص 8.

4 جرائم الاعتداء على حرمة الحياة الخاصة

إن شبكة الأنترنت يتصل بها الملايين من الاشخاص مما جعلهم الاسر والأشخاص متعرضين للتلصص والتجسس عليهم من المتطفلين السيبرانيين واستعمالها للتربح المادي.

الوسائط الالكترونية. فغالبا ما يلجأ الافراد الى الاحتفاظ بهذه البيانات في ذاكرة الحاسوب، بالإضافة الى معلومات يهمه الاحتفاظ بها **(1)**

5-جرائم الماسة بالملكية الفردية

وهي جرائم معلوماتية تمس الإنتاج الفكري والادبي بالقرصنة والسرقة المعلوماتية لها وتتعدى الى الملكية الصناعية بما تتضمنه من اختراعات او رسوم هندسية او اسم تجاري او غيرها حماية ضمنها قانون الوقاية من الجرائم الالكترونية 04/09."فالاعتداء على الحقوق الملكية الفكرية لبرامج الحاسوب هو اعتداء على الحقوق المالية وعلى الحقوق الأدبية ايضا، وتتميز عن الأنواع الأخرى بان محلها هو البرامج فقط (2).

6-جرائم التصنت والتقاط الرسائل الالكترونية

ان المراسلات الالكترونية تختلف عن غيرها من المراسلات التقليدية سواء عن طريق البريد او غيره من عدة أوجه منها:

---

(1)-د احمد عبد الجواد حجازي –الحياة الخاصة ومسؤولية الصحفي ، دار الفكر العربي – القاهرة 2001 ص9.

(2)-د علاء حميد الجبوري ،احكام المعالجة لحساب الأوراق المالية ،أطروحة دكتوراه مقدمة الى كلية الحقوق – جامعة النهرين 2003 ص 45

إن المراسلات غير الالكترونية يمكن تحديد المسؤول عن ارسالها في الغالب بينما العكس بالنسبة للإلكترونية حيث يصعب تحديد من أرسلها ومن المسؤول عنها لأنها تتم عبر عالم رقمي مجرد غير ملموس واقعا، لا بصمات فيه ولا توقيع ولا ادلة تثبت من ارسله(1).

-ان جريمة التنصت تتم غالبا على الاتصالات بين الافراد او بين الدول (التجسس) مثالها برنامج التجسس الإسرائيلي بيغاسوس والذي طال الاتصالات الهاتفية وكذلك المواقع على شبكة الويب والصفحات، بهدف التجسس عليها.

وضمن هذه الجريمة التقاط الرسائل الالكترونية. التي يتم ارسالها من البريد الالكتروني بين الأشخاص على شبكة الويب العالمية وعند توافر العلم والإرادة فان الجريمة تتحقق.

7- جـــرائـــم أخـــرى

أ-جرائم التهديد

وهي التي يتم من خلالها ارسال بعض الصور او الكتابات الى الشخص المراد تهديده او ابتزازاه بغية حمله على القيام بفعل معين او منعه من القيام به (2) .ولقد نصت العديد من التشريعات على هذه الجريمة . الا ان المشرع الجزائري ترك مجال لجريمة التهديد عبر الانترنت الى مفهوم عام وغير محدد باعتبارها جريمة تمس الأشخاص.

---

(1)-د لينا محمد الاسدي مرجع سابق ص 44 . (2)-د لينا محمد الاسدي مرجع سابق ص 45

ب-انتحال الشخصية

وهي جريمة الالفية كما اسماها بعض المختصين في امن المعلومات ، وذلك نظرا لسعة انتشارها وكثرة ارتكابها خاصة في الأوساط التجارية . ان هذه الجريمة غالبا ما تكون بصورة استخدام هوية شخصية أخرى بطريقة غير شرعية و الهدف من ذلك هو الاستفادة من هوية الضحية و إخفاء هوية شخص المجرم لتسهيل ارتكابه جرائم أخرى ،مع الملاحظة ان ارتكاب هذه الجريمة عبر شبكة الانترنت امرا سهلا ، خاصة بالنسبة للأشخاص المتمرسين ن او من يرتكب هذه الأفعال مرات عديدة .(1)

هذا ولقد بدأت العديد من الشركات و المؤسسات التجارية و في اطار المعلومات الحساسة عن طريق شبكة الانترنت ، الاعتماد على وسائل متينة للتأكد من هوية الزبون كما في القنية المستخدمة (التوقيع الالكتروني) والتي تجعل من الصعب ارتكابها.

ج-المضـــايقة

غالبا ما يحصل ذلك عن طريق البريد الالكتروني او وسائل الحوارات الآنية المختلفة على الشبكة ، وقد تمثل هذه الجريمة بإرسال رسائل تخويف او تهديد او مضايقة

هذا و تتفق جرائم الملاحقة على شبكة الانترنت مع مثيلاتها خارج الشبكة، وذلك في حالة الأشخاص الذين يرغبون في التحكم في الضحية. (2)

---

(1)- لينا الاسدي مرجع سابق ص46 . (2)- لينا الاسدي نفس المرجع ص 47

المبحث الثاني

محترفو الجرائم الالكترونية أسبابها وآثارها

حيث يسمى هذا النوع من المجرمين ب(Cracker ‘s) وهم من الطائفة العمرية المتجاوزة الخامسة العشرون سنة ، حيث يتمتعون بمهارات عالية في المعلوماتية والذكاء الاصطناعي وجرائمهم اخطرمن جرائم الهواة. واغلبهم يعملون في شركات للمعلوماتية حيث يكونون متصلين دائما في الشبكة المعلوماتية والحاسب الالي وظهرت منهم منظمات المجموعات تقوم بالهجوم على مواقع لأنترنت الخاصة منها اوالحكومية (1).

المطلب الأول

اشخاص الجريمة الإلكترونية

إن الجرائم المعلوماتية كغيرها من الجرائم تحتاج الى طرفين جاني ومجني عليه إلا إن اطراف الجريمة الالكترونية يختلفون نوعا ما عن اطراف باقي الجرائم وعليه فجوهر البحث بهذا الصدد ينص على مصدر وجود الافعال وتوجيهها ومما لاشك فيه ان الشخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية ولكن هل يعد كذلك

---

(1)غانم مرضي الشمري، الجرائم المعلوماتيةالدار العلمية الدولية،2000، عمان الأردن ص 44.

ايضا حين ترتبط شبكة المعلومات عموما بين حواسيب متعددة يبدو ان الامر يختلف بعض الشيء فالمؤسسات العامة والبنوك وغيرها التي تحمل صفة الشخص المعنوي معرضة لاعتداءات عن طريق هذه الشبكة من المعلومات فعلى الرغم من وسائل الحماية المتعددة الا انه تثبت عدم ويمكن تحديد اشخاص الجريمة المعلوماتية بالاتي فعاليتها امام قرصنة شبكة المعلومات.

الفرع الأول

المجـرم الالكتـروني

في الجريمة المعلوماتية لا نكون بصدد مجرم عادي بل امام مجرم ذي مهارات تقنية وذي علم بالتكنيك المستخدم في نظام الحاسبات الالية فشخصية المجرم المعلوماتي سواء اكان طبيعيا او معنويا والية ارتكاب الجريمة تجعل منه شخصا يتسم بسمات خاصة تضاف الى الصفات الاخرى التي يجب ان تتوافر في المجرم ولعل اهم ما يتميز به الشخص المذكور انه يتوافر لديه خبره بالمسائل المعلوماتية ومعرفة كافية بالية عمل الحاسب الالي وتشغيله باعتبار ان الاجرام المعلوماتي ينشا من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية او البيانات بيد انه ذلك لا يعني امكانية تصور العنف الموجه ضد الجهاز نفسه اي ان لنظام المعلوماتي فقد يكون محل الجريمة اتلاف الحاسب الالي ذاته او وحدة المعالجة المركزية مايمكن الاعتداء عليه قد

يكون بهيكلية الحاسبات لا بمعلوماتها المتنقلة عبر شبكة المعلومات(1) .

ولايمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام او الردع الخاص مالم نضع في الاعتبار شخصية المجرم حتى يمكن اعادة تأهيله اجتماعيا لكي يندمج بالمجتمع مرة اخرى ليغدو مواطنا ، فالإجرام المعلوماتي يعد صالحا على اعتبار أن اصلاح المجرم هو نقطة الارتكاز للنظام العقابي الحديث اجرام الاذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف على الرغم من تصور الاجرام العنيف الموجه ضد النظام

المعلوماتي الذي يتجسد كما بينا بإتلاف الحاسب الالي .والاجرام المعلوماتي بوصفه ظاهرة اجتماعية قد اسفر عن عوامل مستحدثة في اذهان مرتكبيه اذ يلجا العديد من مرتكبي هذه الجرائم إلى ارتكابها بدافع اللهو او لمجرد اظهار تفوقهم على الآلة او على البرامج المخصصة لأمن النظم المعلوماتية دون الحصول على منفعة مالية بل الاكتفاء بالتفاخر بأنفسهم وان يظهروا لضحاياهم ضعف انظمتهم مما يبدوا انعدام أي خطر اجتماعي للإجرام المعلوماتي وليس السبب في ذلك عدم وجود نوايا اثمة ولكن للسلوك

غير الواعي الذي يمكن أن يتسبب في اضرار جسيمة حتى وان لم يكشف عن أي عداء للمجتمع(2) .

---

(1) David Jhonsons Electronic Pravicy Sttodart Canada 1997 page66

(2) محمد سامي الشوا،ثورة المعلومات وانعكاساتهاعلى قانون العقوبات دارالنهضةالعربيةالقاهرة–1994 ص173

وعليه فان مرتكبي الجرائم المعلوماتية ليسوا على درجة من الخطورة او الكفاءة وعلى هذا الاساس يمكن تصنيفهم حسب امكانياتهم ومقاصدهم من ارتكاب الجريمة إلى صنفين **الأول:** مجرمين مستخدمين وهم من تتوافر لديهم خبرة لابأس بها في مجال عمل الحاسب الالي ومكوناته ووظائفه الاساسية ومعرفة بعض البرامج التي يجري العمل بها كالبرامج المحاسبية ولما كان هؤلاء يمارسون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسة هواية اللهو وهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي إلى افعالهم غير المشروعة بالنسبة إلى نشاط معين لذا فان هذه الفئة من المجرمين تعد اقل خطورة مقارنة بغيرها.

ولكن مع ملاحظة ازدياد الاعداد المستخدمة لتكنلوجيا(الانترنيت) وما سيتبعه بلا شك من ازدياد نسبة الجرائم في هذا المجال، فليس من المستبعد احتمال انزلاق هذه وخصوصا اذا ما تم احتضانهم من قبل الفئة من مجرد هواة صغار للأفعال غير المشروعة إلى محترفين للإجرام منظمات اجرامية لتحقيق اغراض خطرة تؤثر بصورة او بأخرى على معطيات التطور العلمي(1) .

---

(1)-سعد الحاج بكري- شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة- العربية للدراسات الامنية والتدريب- س6 -ع11) - 92- 1990- الرياض.

الفـــرع الثـــاني

مجرميـــن مبرمجيـــن

نظرا إلى المستوى المهارى الذي يتمتع به المجرمون من دخول واقتحام للأنظمة الحاسوبية بكل سهولة واقتدار رغم احتياطات الامن المتعددة، ورغم قلة العناصر الخبيرة على اكتشافها مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، إذ

غالبا ماتكون جرائم التحويل والنسخ والاضافة للمعلومات، علاوة على أنه باستطاعة هذه الفئة استخدام الامكانيات والاساليب على البرامج وتفسير محتواها من هذه الفئة ضخمة المعلوماتية ليس في ارتكاب الجريمة فقط بل حتى في التهرب من محاولة كشف امرهم بالعمل على اعاقة ملاحقتهم، من خلال تضييع الادلة الموجودة المؤدية إلى ادانتهم. (1)

من هذا يتضح أن مرتكب الفعل الجرمي المعلوماتي قد يكون فاعلا اصليا او شريكا في ارتكابه للجريمة فصفة الفاعل الاصلي في الجريمة المعلوماتية غالبا ما تكون من احد العاملين او المستخدمين في منشاة تدار بالنظام المعلوماتي بصرف النظر عن المستفيد من وراء ارتكاب مثل هذه الافعال ولما كان هذا النوع من الاجرام يستلزم الدقة والتنفيذ للعمليات غير المشروعة فانه يستلزم كذلك مشاركة او مساعدة اشخاص اخرين

---

(1) د محمد سامي الشوا مرجع سابق ص 46.

سواء اكانوا فنيين ام مجرد وسطاء وقد يكون هذا الاشتراك سلبيا يتمثل بالامتناع بيد انه في الغالب الاعم يتمثل بالمساعدة الفنية والمادية وخصوصا عندما تستلزم اليات الابتكار

لمخادعة الحاسب الالي الاستعانة بمجموعة من الوسطاء او الشركاء والمؤتمنين على اسرار اسطوانات الحاسبات الالية اذ يؤدون الدورالرئيسي في نجاح العملية غيرالمشروعة.

الفرع الثالث

المجني عليه في الجريمة المعلوماتية

فكما يمكن أن يرتكب جرائم المعلوماتية شخص طبيعي او معنوي فان المجني عليه في تلك الجرائم قد يكون كذلك ايضا مع انه الغالبية العظمى من هذه الجرائم تقع على شخص معنوي يتمثل بمؤسسات وقطاعات مالية وشركات الا أن المعلومات المجردة تعد في الوقت الحاضر من اهم المصالح المستهدفة بعد الاموال وخصوصا اذا ضخمة كانت هذه المعلومات ذات اهمية بالغة وكان هدف المجرم المعلوماتي هو الحصول على مقابل وعوض عن طريق او بيعها لغير اصحابها الشرعيين وسواء اكانت المعلومات مخزنة بذاكرة المقايضة غير المشروعة لهذه المعلومات وتصنف المعلومات إلى معلومات المالية والمعلومات التجارية والمعلومات الشخصية.(1)

1/د محمد سامي الشوا مرجع سابق ص61.

المطلب الأول

آثارالجريمة الالكترونية

للجريمة الإلكترونية أسباب تدفع بالمجرم الالكتروني يقوم بها، التي تترك آثارا يبقى يعاني منها كل مستخدم للجاز الالكتروني.

الفرع الأول

آثار الجريمة المعلوماتية

شهد العالم في الفترة الأخيرة ارتفاعا ملحوظا في مؤشر عدد الجرائم الالكترونية صاحبه تطور نوعي في المستوى احرفي للجناة الذين ارتكبوا تلك الجرائم التي لا تعرف حدود معينة لبلد معين ، ومع هذه الطبيعة العالمية هذه الجرائم التي تؤثر على الاقتصاد العالمي فإن ذلك التأثير الناجم عنها يفوق بكثير الآثار الاقتصادية التي تنجم عن الجرائم التقليدية.(1)

وأشارت دراسة جديدة نشرت في 9 يونيو 2014 إلى أن جرائم الإنترنت تكلف الاقتصاد العالمي نحو 445 مليار دولار كل عام، وأن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة حقوق التأليف كما ذكر التقرير الصادر الملكية الفكرية تتسبب

---

(1)– د محمد سامي الشوا مرجع سابق ص 46.

في تأثريات للجرمية الإلكترونية على مستوى الفرد الذي قد يتعرض لها والتي تؤثر خسارة الأفراد لحوالي 160 مليار دولار، كما ان الجرائم الالكترونية لها تؤثر كبير على الاقتصاد العالمي حيث تمس سائر الشركات العالمية بأضرار جسيمة جراء القرصنة وسرقة الاسرار المالية و الصناعية لما يمس بروح الابتكار و الابداع ويزيد من فقره وتخلف الاقتصادات النامية.على الجانبً منها فيما يلي :املادي لديه ربما نوجز بعضا سرقة الهوية الشخصية-سرقة بطاقة الائتمان الخاصة به- الابتزاز والتهديد- عمليات احتيال- تحويل أو نقل حسابه المصرفي- نقل ملكية الأسهم- زيادة الفواتير بتحويل فواتير المجرم للضحية (2).

الفرع الثالث

أسباب الجريمة الالكترونية

ان الاجرام عامة له عدة أسباب وظروف تتهيأ لنشأته ووقوعه فهذه لأسباب تختلف كما تختلف سمات مرتكبي جرائم المعلوماتية. فظهور الجريمة المعلوماتية مرده أساسا من التطور العلمي الحاصل في مجال الاتصالات الالكترونية، حب الظهور في الإعلام، البطالة والظروف الاقتصادية الصعبة، وأسبابها سهولة نسخها، توفر البيانات في كل مكان، طول عمر الأجهزة(2).

---

(1)-د محمد سامي الشوا مرجع سابق ص61.

(2)-د.عبد السلام المايل، الجريمة الالكترونية في الفضاء الالكتروني، كلية الاقتصاد والتجارة ص 249.

الفصل_الثاني:

الضبطية القضائية بين المتابعة وأساليب مكافحة الجريمة الالكترونية:

تهدف هذه الدراسة إلى تسليط الضوء على الضبطية القضائية وأعمالها أثناء التحريات الأولية وخلال مرحلة التحقيق القضائي المأمورين بتنفيذها من طرف قاضي التحقيق والآثار المترتبة على سير الدعوى الجزائية حين مخالفتها للأحكام والشروط الموضوعية من قبل المشرع الجزائري، ونظر إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الضبطية القضائية لتواكب التطور الحاصل في مجال الجريمة الإلكترونية (المعلوماتية)، لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الانتربول واليوربول والأنريبول.أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني.لضمان الحماية الجنائية للمعاملات الالكترونية ومع هذا فيبقى السؤال مطروح حول مدى فعلية وفعالية هذه القوانين في مواجهة الجرائم الإلكترونية ،من هم الضبطية القضائية المخول لهم إجراء التحري والتحقيق فيها؟

نتناول في المبحث الأول هيئات ووحدات متخصصة في البحث والتحري في الجرائم الإلكترونية واختصاصاتها.وذلك من خلال تقسيم المطلب الأول إلى ثلاثة فروع وهي:
ف1: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ف2: الوحدات التابعة لسلك الأمن الوطني ووحدات تابعة للقيادة العامة للدرك الوطني.
ف3: الهيئات القضائية الخاصة للبت في الجرائم الإلكترونية. وصولا إلى دراسة الحماية الإجرائية للنظام المعلوماتي وذلك في المطلب الثاني.وفي المبحث الثاني نتناول آليات رجال الضبطية القضائية في محاربة الجريمةالالكترونية.

المبحث الأول :هيئات ووحدات متخصصة في البحث والتحري في الجرائم الإلكترونية :

وضع المشرع الجزائري كغيره من التشريعات بعض القواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الآلي خاصة في مرحلة جمع الاستدلالات حيث أن أجهزة الشرطة تقوم بدور فعال ورئيسي حال وقوع الجريمة لمعاينة مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة(1).

وقد ساهم المشرعون من القانونيين وكذا الأساتذة الجامعيون من الفقهاء القانونيي الدور الكبير عبرالمؤسسات التشريعية في سن القوانين المتعلقة بذلك.

(1)– ابتسام بخوش ،مذكرة تكميلية ماستر في القانون –تخصص قانون جنائي للأعمال،اجراءات المتابعة الجزائية في الجريمة المعلوماتية جامعة العربي بن مهيدي أم البواقي.2015 2016 ص2.

المطلب الأول:

الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الإلكترونية

الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الالكتروني(3).

الفرع الأول: الهيئة الوطنية والهيئة القضائيةالجزائية:

رغبة من المشرع الجزائري في مواجهة الأنماط الجديدة للجرائم أراد أن يستحدث بموجب القانون هيئتين.

(3) المرسوم الرئاسي رقم 15- 261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئةالوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية في 205/10/08 ، عدد 53

أولا: الهيئة الوطنية للوقاية من الجائم المتصلة بتكنولوجيات الاعلام والإتصال: وقد استحدثها المشرع الجزائري بموجب قانون رقم 09 -04 المؤرخ في 05 أوت 2009المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها 2 وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08

أكتوبر 2015، ومن مهامها تفعيل التعاون القضائي والأمني الدولي وغدارة وتنسيق العمليات الوقائية والمساعدةالتقنية للجهات القضائية والأمنية مع إمكانية تكاليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أوالمصالح الإستراتيجية للاقتصاد الوطني(1).

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء. تظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين.

(1)فضيلة عاقلي، الجريمة الإلكترونية واجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017 ،طرابلس

وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى

تحت سلطة القاضي المختص .للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 100 جريمة إلكترونية منها 30 %على مواقع التواصل الاجتماعي هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخصا متورطا في قضايا إرهاب الكتروني تمت إحالتهم على القضاء .

هذا وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن160جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق،سوريا وليبيا كما تمكنت من فك شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجميده عبر مواقع الأنترنت ومنصات التواصل الاجتماعي خاصة الفيسبوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منتديات إرهابية غلى جانب اتصالات محلية ودولية 1.

(1) لمعرفة مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المستقبلية.

أنظرwww. legifrance..gouv . .fr/affich texte.de

أ_ مهام الهيئة : من خلال اسمها فإنَّ للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها:

1/الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : إنَّ إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات ومن أهم هذه الجرائم :التجسس على الاتصالات والرسائل الالكترونية التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية..إلخ.

2/ مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :بحسب نص المادة14 من القانون 04 / 09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14فقرة ب من القانون09/04،وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا، فإن لها مهام أدرجها المرسوم رقم 405/2000المؤرخ في15ماي2000 المتضمن إنشاء هذه الهيئة تتمثل في 6:

–تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في إرتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

–القيام بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت

أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون.

– تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية(المديريات العامة المختلفة)فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.

– التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة(المادة 4 فقرة 2 من القانون 04 / 09 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.

– من أجل القيام بمهامها فلها تركيز، تحليل، إستقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) ، وكذلك كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها.

– يجب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما

تسمح به القوانين –وخاصة منها ما يتعلق بالسر المهني –بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والاتصال.(1)

3/ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وتحديد مكان تواجده في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات(الهيئات)لمماثلة لها على مستوى الدول، بدون المساس بتطبيق الإتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم1 أما فيما بخص مجال تطبيق الوقاية من هذه الجرائم ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالإتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيان بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية[2].

(1) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007 ،ص233 – 232

(2) برابح يمينة، "تطبيقات الأمن المعلوماتي"، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي 7 و8 فبراير 2017، ص 9.

وإنشاء هذه الهيئة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك في المجال الجزائي من أجل تحسين حماية حقوق وحريات المواطنين وتشديد العقوبات على أي تقصير في هذا المجال[1].

(1)إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته التي سبق ونص عليها القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أنظر: مرسوم رئاسي رقم 261-15 المؤرخ في 24من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم الجزائرية

السنة	2005	2006	2007	2008	2009	2010	المجموع
عدد الجرائم	01	01	03	06	12	12	35
عددالأشخاص المتابعين	00	01	03	13	51	20	88

ولكن تثبت التقارير الإحصائية، أن هذا الرقم هو أقل بأضعاف من حجم الاعتداءات الفعلية التي أثبتت تقارير أنها تكون بين200إلى250اعتداء يوميا بمختلف الأشكال التي وإن وضع المشرع نظام حماية نظام المعالجة الآلية للمعطيات،إلا أنه لم تعالج نصوصه الأفعال المقترفة بشكل مفصل،والتي تتطور بشكل مذهل في الثانية الواحدة وكأنها مسابقة عالمية بين المخترقين والقراصنة حول من يبتكر أكثر جريمة انترنت تطورا وسرعة، وحتى الدول الكبرى لم تتمكن من وضع آليات ووسائل فعالة للحد من الإجرام المعلوماتي أثبتت التقارير الصادرة عن مكتب التحقيقات الفدرالي (FBI)أن جرائم الكمبيوتر تكلف الاقتصاد الأمريكي67.2دولار سنويا، وحوالي 64بالمئة من الشركات الأمريكية؛ تعرضت لخسائر مالية بسبب حوادث اختراق أنظمة الكمبيوتر خلال العام الماضي.

ب –المعهد الوطني للأدلة الجنائية على الإجرام :يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الألي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات 1.

(1) فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجرائم الإلكترونية ، طرابلس، بتاريخ 25 – 24 مارس ص 133.

ثانيا: الهيئات القضائية الجزائية المتخصصة:

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04 -14 المؤرخ في :1نوفمبر 2004. (1)

وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب دعم حقوق الإنسان وتسهيل حق اللجوء إلى القضاء وإعادة دراسة ثلاث نقاط أساسية(2):

-الإعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة، ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا

(1) القانون -04/ 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم - 66 155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية، عدد 71 ،بتاريخ ن 10 وفمبر 2004 .

(2) بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016 ،ص . 52

النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت في أعمال المنظمات الإجرامية واستعمالها السنوات الأخيرة تزايد في العلميات الإرهابية وتزايد القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04 -14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف(1).

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه

(1) سعيدة يوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر، 2019. ، ص .54

المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3- 4- 5 المعدلة للمواد 3-4 -5 من المرسوم السابق وجاء التقسيم كالتالي:

محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزوو، الجلفة، المدية، المسيلة، وبومرداس،البويرة، وعين الدفلى .

محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تيسة، جيجل، سطيف، سكيكدة، عنابة، ثالمة، برج بوعريريج، الطارف، خنشلة، سوقأهراس، وميلة .

محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، وغرداية .

محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسنمسلت، النعامة، عين تيموشنت، وغليزان .

بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنوبا، شرقا، وغربا، وذلك لدى أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيها الجريمة الإلكترونية.(1)

للإستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها، ونظرا لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها :

مؤتمر روما سنة 1958 ،مؤتمر نيس سنة1972 ،مؤتمر ريو دي جانيرو لسنة 1978 ،وقد أكدت هذه المؤتمرات أن التخصص في مجال القضاء له أهمية كبيرة ودور فعّال في رفع مستوى العمل القضائي، ولنظام التخصص جانبين هما: تخصص القضاة، وتخصيص جهات القضاء.

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 14 / 04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية(ق.إ.ج)على أنَّه يجوز تمديد دائرة الإختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال

(1) سعيدة بوزنون، المرجع السابق، ص .55

والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، كما نصت المادة 40 مكرر من ق إ ج على أنَّه » تُطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع إختصاصها المحلي طبقا للمواد 40 ، 37 ، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه«. وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنَّه جعل المشرع الجزائري لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية (1) ، فيتجنب إنشاء هيئات قضائية جديدة لكنّه يوسع من دائرة الإختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها إختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن إختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أنَّ التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية. هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسوم التنفيذي رقم348 / 06 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد

(1) أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04 / 09 ، مذكرة لنيل شهادة الماجستير،تخصص قانون جنائي ، جامعة قاصدي مرباح " كلية الحقوق "، ورقلة ، – 2012 2013،ص49-50

الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق(جريدة رسمية رقم(63 :) في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، 1 والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم ريع الخاص بالصرف، ولأنَّ الجريمة المنظمة تشمل جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتش متنوعة تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وتُرتكب من طرف عدة أفراد

يتصرفون بطريقة منظمة، تعدُّ الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكبعن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الإختصاص القضائي في إطار الإهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة(2).

الفرع الثاني: جهازي الأمن الوطني والدرك الوطني :

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء

---

(1) أحمد مسعود مريم –المرجع السابق–ص50

(2) أحمد مسعود مريم المرجع السابق ص 51

على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام (1).

أولا: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الالكترونية والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات(2).

على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم وهي

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة .
- المخبر الجهوي للشرطة العلمية بوهران .

---

(1) محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات،العدد الثاني، ديسمبر 2017 ،المركز الجامعي إليزي، الجزائر، ص .35 -34

(2) يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016 ،ص .20

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني **سنة** 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن(1).

ثانيا: الوحدات التابعة للقيادة العامة للدرك الوطني :

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

- المصالح والمراكز العلمية والتقنية . - هياكل التكوين .

- المصلحة المركزية للتحريات الجنائية .

- المعهد الوطني لعلم الإجرام .

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، والمقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل

(1) سعيدة بوزنون، المرجع السابق ص 53

استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء(1).

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية حيث يوجد بهذا المركز قسم الإعلام الآلي والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية(2).

(1)يوسف جفال، المرجع السابق، ص .21

(2)سعيدة بوزنون، المرجع السابق، ص .54 -53

المطلب الثاني: اختصاص الضبطية القضائية في مجال حماية النظام المعلوماتي:

أن القاعدة الإجرائية ليست غاية في ذاتها، وإنما هي وسيلة لغاية تتمثل في حسن تطبيق القانون الجنائي الموضوعي، فبينما تجرى بالدعوى العمومية محاكمة القاضي للمتهم، فإنه بتطبيق القواعد الإجرائية التي خالفتها الدعوى تجرى محاكمة القانون للقاضي، وبالتالي فإن للإجراءات الجنائية خطورة لا تقل بحال القواعد المقررة في قانون العقوبات، لأنها تمس مباشرة بحريات المواطنين واستقرارهم.1 وعليه كان لابد من التطرق إلى الجوانب الإجرائية بخصوص الجريمة الإلكترونية، ومدى توافر الحماية الإجرائية للنظام.

الفرع الأول :اختصاص الضبطية القضائية

إن أعضاء الضبطية القضائية وهم يمارسون صلاحياتهم في إجراء التحريات اللازمة بشأن الجريمة لمعرفة مرتكبيها مقيدين في ذلك بنطاق إقليمي محدد يسمى بالاختصاص المحلي وبنوع معين من الجرائم ويسمى الاختصاص النوعي(2).

أولا: الاختصاص المحلي

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة ولذلك يتعين ان يكون مكان وقوع الجريمة أو محل إقامة المتهم أو محل القبض عليه.

1–طارق إبراهيم الدسوقي عطية،الأمن المعلوماتي،النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية،2009،ص342–343

2– ابتسام بخو ،مذكرة تكميلية ماستر في القانون –تخصص قانون جنائي للأعمال،اجراءات المتابعة الجزائية في الجريمة المعلوماتية جامعة العربي بن مهيدي أم البواقي.2015 2016 ص2

امتداد الاخصاص المحلي: يجيز القانون تمديد الاختصاص المحلي لضابط الشرطة القضائية في حالة الاستعجال أو بناءا على طلب السلطة القضائية وهو ما نصت عليه المادة 16ف 2 ق إ ج (دائرة المجلس) وكذا تحديد الاختصاص المحلي لضابط الشرطة

القضائية في الجرائم ال6 الخطيرة إلى كافة التراب الوطني أنظر المادة 16ق إ ج.

ثانيا:الاختصاص النوعي

يقصد به اختصاص عضو الضبطية القضائية بنوع معين من الجرائم دون غيرها من الجرائم،وقد ميز المشروع بين الاختصاص العام لبعض فئات أعضاء الضبطية القضائية أي الاختصاص بالبحث والتحري بشأن جميع الجرائم دون تحديد نوع معين من الجرائم دون الأنواع الأخرى من الجرائم وهي الئات المنصوص عليها في المادة 15 ق إ ج ،فلهم الاختصاص العام بالبحث والتحري في جميع الجرائم ،أما الفئات الأخرى من الضباط المحددين في الفقرة 7 من المادة 15 والمواد 21 و27 و28 ق إ ج فإنهم ذوو اختصاص خاص وليس عام يتحدد بنطاق جرائم معينة.

الفرع الثاني: التحقيق في الجريمة الالكترونية:

يعرف التحقيق بأنه إجراء يتخذ بعد وقوع الجريمة، لما له من أهمية في التأكد من وقوع الجريمة، وإسنادها إلى مرتكبيها بأدلة الإثبات بأنواعها، وبالتالي تتجلى الحقيقة التي تهدف إلى إدانة المتهم من عدمه.وتمر الدعوى الجنائية بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بدورها بمرحلتين، مرحلة التحقيق الأولي(الضبطية القضائية) ومرحلة التحقيق الإبتدائي(قاضي التحقيق)، وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا للقانون الإجراءات الجزائية، فإذا كان التحقيق يعتمد على ذكاء المحقق وقوة ملاحظته، فإن التحقيق في البيئة الإلكترونية يستوجب كفاءة بالإضافة إلى ذلك تطوير

لأساليبه، وتكليف جهات مختصة لممارسته من أجل مواكبة الجريمة وتطورها وهذا ما سيتم بيانه في الفروع الموالية .1

خصائص التحقيق والمحقق:للتحقيق الإلكتروني مميزات خاصة عن التحقيق الجنائي التقليدي وكذا المحقق الإلكتروني، لمسايرة متطلبات الجريمة الإلكترونية بما فيها العالم الافتراضي الذي نرتكب فيه.

أولا:خصائص التحقيق الإلكتروني:

01- منهج أو أسلوب التحقيق الإبتدائي-:وضع خطة عمل التحقيق:

وذلك وفق المعلومات المتوفرة لدى المحقق، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك بوضع خطة مناسبة، ولا تبتدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية ، وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة، ثم التخطيط الفني للتحقيق من أجل الوصول إلى أفضل الطرق للتعامل مع هذه الجريمة بالتفصيل والوضوح، وبعدها 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 التي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبراء 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.ويجب أن ترتكز

1-نايري عائشة، مذكرة لنيل شهادة الماستر في القانون الإداري ،قسم الحقوق ،جامعة أحمد داية – أدرار – 2016- 2017 .ص40.

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 إيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الظروف المحيطة بالواقعة، إذ أن هذه الظروف قد تشمل عوامل مهمة يجب مراعتها عند وضع خطة العمل ومنها:مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة–مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها–مدى الاختراق الأمني الذي تسبب فيه الجاني،ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش، وذلك بتحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.(1)

تشكيل فريق التحقيق:

يجب أن يتشكل الفريق من فنيين وأخصائيين ذوي الخبرة في مجال الحاسوب والانترنت ما يكفي لمكافحة هذا النشاط الإجرامي وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين في مجال المعلوماتية، والمعرفة باللغات الأجنبية 2 ، ولهم مهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهم الإستعانة بخبراء ليتمكنوا من فك التعقيدات التي تفرضها ملابسات كل جريمة، ويتكون الفريق من المحقق الرئيسي، ويكون ممن لهم خبرة في التحقيق الجنائي، خبراء الحاسوب وشبكات الأنثرنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم، خبراء ضبط وتحرير الأدلة الرقمية والعارفين بأمور تفتيش الحاسوب، خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية، خبراء التصوير والبصمات والرسم التخطيطي.

1- نايري عائشة، مذكرة الماستر المرجع السابق، ص42.

2-كوثر فرام، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب،المعهد العالي للقضاء،2007-2009 ، ص.88

إجراءات التحقيق:

- **إجراءات سابقة على بدء التحقيق الإبتدائي:**_تحديد نوع نظام المعالجة الآلية للمعطيات، أي هل الحاسوب معزول أم متصل بشبكة معلومات.

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

- إذا وقعت الجريمة على شبكة، فإنه يجب حصر طرفيات الإتصال بها أو منها، لمعرفة الطريقة التي تمت بها عملية الإختراق من عدمه، وهل هناك حواسب آلية خارج هذه المشكلة ولها إمكانية الإتصال بها أم لا؟

الفصل الثاني دور رجال الضبطية القضائية في مكافحة الجريمة الإلكترونية

-مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة الإلكترونية – مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

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

-فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق.

-التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، لأنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق(الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة والتخطيط).

-إبعاد الموظفين عن أجهزة الحاسب الآلي بعد حصول المتهم على كلمة كذا الشفرات في حالة وجودها.

تصوير الأجهزة المستهدفة–التي وقعت بها أو عليها الجريمة من الأمام والخلف لإثبات أنها كانت تعمل(1).

–**إجراءات أثناء التحقيق الإبتدائي–:**عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها، والتأكد فنيا من دقة النسخ عن طريق الأمر–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 الممسوحة ويمكن استعادتها من سلة المهملات، وكذا معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب –العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في اختلاس معلوماتي–العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها–حفظ المعدات والأجهزة التي تضبط بطريقة فنية سليمة(1).

ثانيا:خصائص المحقق الإلكتروني: تتمثل في الخصائص الفنية للمحقق الالكتروني وتأهيل وتدريب المحقق الإلكتروني.

(1) نايري عائشة، مذكرة الماستر المرجع السابق ، ص من43

الخصائص الفنية للمحقق الإلكتروني:

معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت، لأن افتقار ضابط الشرطة القضائية إلى التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل–إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك، ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة لأي مؤثرات خارجية، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها–معرفة آلية عمل تشكيلات الحاسوب والانترنت –معرفة المحقق بالأنظمة المختلفة ، لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة– معرفة معطيات الحاسوب لمعرفة صيغ الملفات وما تحتويه–معرفة وإدراك أساليب ارتكاب الجريمة الالكترونية وتقنيات الأمن المعلوماتي.

تأهيل وتدريب المحقق الإلكتروني

لابد من وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب إلى العاملين بأجهزة الضبطية القضائية.ويرى الفقه الجنائي أنه في حالة التدريب على التحقيق يتعين مراعاة شخص المتدرب، ومنهج الدورة التدريبية، وصفة وأسلوب التدريب، كما يجب أن يشمل منهج التدريب تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، والمتعلقة بالكشف عنها و كيفية اتباعها ومعاينتها وفحصها فنيا(2).

(2) نايري عائشة، مذكرة الماستر نفس المرجع ، ص45.

ومن العقبات التي تعيق عمل الأجهزة حتى على فرض أنه تم إعدادها الإعداد المناسب، ضخامة حجم البيانات محل الفحص، ما يتعذر على المحقق الكفئ الوصول إلى الدليل المناسب(1).

1- موسى مسعود أرحومة ، الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطن ورقة مقدمة من المؤتمر المغاربي الأول حول المعلوماتية والقانون، الذي تنظمه أكادمية الداسات العليا ، طرابلس خلال الفترة 2009/10/29/28 ، ص 05

المبحث الثاني:آليات محاربة الجريمة الالكترونية أو إجراءات التحقيق والمتابعة في الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم الحديثة النشأة، ولذلك فإن القواعد العامة لمكافحة استحدث قواعد وآليات جديدة خاصة فقط بالجريمة الإلكترونية نظرا لخصوصيتها من الناحية الإجرامية خاصة في مجال التحقيق، فيجب على المحقق في حالة وقوعها أي لابد أن يستظهر أركانها الثلاث، الشرعي، والمادي والمعنوي للجريمة محل التحقيق.

أ /**إظهار الركن المادي:** يتطلب النشاط أو السلوك الإجرامي في جرائم الأنترنت وجود بنية رقمية واتصال بالانترنت، وأيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته.

ب/ **إظهار الركن المعنوي للجريمة الإلكترونية:** يتمثل في الحالة النفسية التي يكون عليها الجاني التي دفعت به لإرتكاب الجريمة والعلاقة التي تربط بين الشخص الجاني والفعل المرتكب أو المكون للجريمة ويتمثل أساسا في العلم و الإدارة المعروف باسم القصد الجاني العام .

ج/ علانية التحقيق من الضمانات اللازمة للعدالة الجنائية علاقة التحقيق في الإجراءات الجنائية وهي تختلف عن التحقيق الإبتدائي عنها في مرحلة المحكمة(1).

---

(1) خالد ممدوح إبراهيم، فن التحقيق الجاني في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2008 ،ص 59 .

المطلب الأول:

القواعد الإجرائية التقليدية لمكافحة الجريمة_المعلوماتية

إن أهمية جهاز الشرطة القضائية في الكشف عن الجريمة الإلكترونية والتعرف على المجرم الإلكتروني، تبعه استعداد المشرع الجزائري لأساليب التحري الخاصة المستعملة بما تناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن يتكيف دورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر،

وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الإلكترونية كشكل من أشكال الجريمة المنظمة (1).

ما تجدر الإشارة إليه أن هذه الإجراءات م يتم تنظيمها إلا في بعض الجرائم المعنية من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية التي استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية، القانون رقم 06 -22 والتي تتمثل في التقاط التالية :

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية ولا سلكية .

---

(1) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة 2، دار الفكر الجامعي، مصر، 2011، ص .76

– وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص يتواجدون في أماكن عمومية أو خاصة أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص .

– جواز التسرب أو الاختراق للكشف عن الجريمة الإلكترونية حسب المادة 65 مكرر 12 من القانون 06–22 المتضمن قانون الإجراءات الجزائية.

– ولأنه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطه المشرع الجزائري بجملة من الضوابط أبعادها، الإذن القضائي والتسرب من قاضي التحقيق أو وكيل الجمهورية، المادة 65 مكرر 11 ،وأيضا احترام المدة القانونية للتسرب **(1)**.

الفرع الأول: جمع الاستدلالات في الجريمة الإلكترونية:

المحقق أو المحتوى هو الشخص المكلف بإبراء التحري بواسطة الحاسب الإلكتروني عن المتحري عنه، سواء كان شخصا أو مكانا أو شيئا حسب طبعته، على المتحري أن يكون لديه استعداد وقدرة على إجراء مهامه وأن يميز من الحقائق والأقوال والآراء والاستنتاجات، أي الاستعداد لقدرات خاصة تساهم في قيام المتحري بمهامه بشكل سليم، من أهم السيمات التي يجب أن تتوفر في المحقق يمكننا أن نذكر، دقة الملاحظة في تتبع للمهتمين والشهود أثناء التعامل معهم، سرعة الأداء، كتمان السر حتى لا يضر بمصالح الغير الترتيب والدقة والتأني وبذل العناية، الصبر، قوة الذاكرة (2).

(1) نبيلة هبة هروال، المرجع السابق ص 76. _ (2)مروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، 2011 ،ص .81

المتحري المهني هو مأمور الضبط القضائي المسؤول عن تلقي البلاغ وسماع الشهود وسؤال المتهمين، والمهارة الرئيسية التي يجب على المتحري تنميتها بالتدريب هي ترتكز في مهارات الإتصال التي أصبحت اليوم أساس أي تعامل أمني سواء على المستوى الشخصي أو العملي تنقسم هذه المهارة إلى 3 أقسام هي: الحديث إلى الغير، الإنصات، كتابة المحاضر.

وبما أن الحديث إلى الغير في مجال التحري يكون في حدود توجيه الأسئلة والإستفسارات، فيجب أن تكون مقنعة مليئة بالثقة، في حين أن كتابة المحاضر يجب أن تتميز بالوضوح والتسلسل المنطقي والإقناع لتصل إلى العدالة، كما أن الإنصات وحسن الإستعمال يساعد المتحري في اتخاذ القرارات المحبة(1).

أولا: تلقي البلاغات في الجريمة الإلكترونية

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوي التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند وردها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص المكاني أو النوعي بها، حالة في حين أن الواجب إتخاذ الإجراءات المقرة بشأنها، تم إخطار جهة الاختصاص والمحضر إليها.

1-مروك نصر الدين، المرجع السابق، ص 81

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى بإجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية مثلا تتضمن التبليغ عنى وجود موقع منشور فيه صور الإستغلال الجنسي للأطفال .

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ، يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ وقت تلقي البلاغ، المعلومات الخاصة، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة (1).

ثانيا: الشكوى في الجريمة الإلكترونية

قد يترتب على الجريمة ضرر خاص قد يصيب أحد الأفراد ماديا أو معنويا، فينشأ له حق تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في قانون الإجراءات الجزائية أنه يحق لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص وقد عرفت الشكوى بأنها

(1)خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائمالحاسوب والانترنت، دارالثقافة، الأردن، 2011،ص .79

البلاغ أو الإخطار الذي يقدمه المجني عليه أو ووكيله الخاص إلى السلطات المختصة طلبا تحريك الدعوى العمومية بشأن جريمة معينة .

ولقد خصصت العديد من المراكز لمعالجة هذه الشكاوي من بينها مركز نلقي الشكاوي عن جرائم الإحتيال عبر الأنترنت المؤسسة في فيرجينيا الغربية بالولايات المحتدة الأمريكية من طرف مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء من أجل مكافحة ظاهرة الإحتيال عبر الانترنت **(1)**.

الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية

أولا الاستجواب

وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وإ ن لم يقدر يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق بذلك(2)

ثانيا: سماع الشهود في الجريمة الإلكترونية .

سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن

(1) خالد عباد الحلبي، المرجع السابق، ص 79

(2) خالد عياد الحلبي، المرجع السابق، ص .80

الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية.

المطلب الثاني التحقيق في الجريمة الإلكترونية

عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما، فإنه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها إلا أنه تجدر الإشارة إلى أن مسرح الجريمة الإلكتروني بالإضافة إلى المسرح المادي يوجد مسرح إلكتروني متمثل في البيئة الإلكترونية التي يجد فيها المحقق صعوبة استخلاص الدليل منها، مما يدفعه بالاستعانة بالخبراء الفنيين في هذا المجال، في معاينة مسرح الجريمة أو القيام بالعمليات التفتيش والضبط وفحص آثار الجريمة، لا تشكل خللا فنيا أو قانونيا، كما هو الحال في التحقيق مع الشهود والمتهمين، إذ أن أخذ أقوال الشهود واستجواب المتهمين يعتمد على خبرات المحققين، ويعتبر الاستجواب مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق،ومطالبته له بإدلاء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة الكشف عن الحقيقة واستظهارها بالطرق القانونية (1).

تتولى سلطة مختصة إجراء الاستجواب، إذ يجب على جهات التحقيق أن تكون مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن استيعاب واقعة التحقيق، إن طريقة توجيه

---

(1) محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2010 ،ص 102.

الأسئلة وترتيب أولوياتها واستنتاج الحقائق من الطريقة التي يتحدث بها المتهم وقراءة لغة الجسد لديه، أمور مهنية لا يوفيها حقها إلا المحققون الذين اكتسبوا الخبرة والمعرفة العلمية.

يمكن القول بصفة عامة أنه لا يوجد حتى الآن خبير معلوماتي لديه المعرفة المتعمقة في سائر أنواع الحسابات وشبكاتها، كما لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم،ولهذا يتمتع مأمور الضبط القضائي وكذلك المتحري بحرية كاملة حتى يتمكن من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها هو أنها مناسبة، ولذلك لأي منهما أن يندب الخبير يأنس فيه الكفاءة الفنية اللازمة لحل هذه المسألة (1).

الفرع الأول التفتيش وحجز المعطيات المعلوماتية

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه مأمور الضبط القضائي بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية؛ بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة[2]، وهو ما سنبرزه فيما يلي:

---

(1) محمد حزيط، نفس المرجع، ص 102.

(2) طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009، ص 441.

أولا :تفتيش نظم المعلوماتية

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

الحالة الأولى :في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية :إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن، ففي ألمانيا يرى الفقه [1]، أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر تطبيقا لمقتضيات القسم 103 من قانون الإجراءات الجزائية

---

(1)طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012، ص 115.

الألماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان الذي يتم فيه التفتيش.

إذن لتفتيش الحاسوبات الآلية ذات نهاية طرفية في دولة أجنبية، نصت بعض التشريعات على طريقة ثانية كإجراء للتحقيق في الجريمة المعلوماتية وهذه الطريقة هي: التنصت والمراقبة الالكترونية لشبكات الحاسوب ويقصد بهذه الطريقة –التنصت– مراقبة المحادثات التلفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثته في الكشف عن الجريمة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور(1).

(1) طرشي نورة ، نفس المرجع، ص 115.

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات، وقد اتفقت بعض التشريعات، كالتشريع الجنائي الكندي في المادة 487 التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت صراحة على إمكانية تفتيش مكونات الحاسوبات المادية للكشف عن الجريمة المعلوماتية باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها[1].

1-تفتيش نظم الحاسوب المنطقية أو المعنوية :يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات(2)وهو يشتمل على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي كالبرامج ونظم التشغيل وقواعد البيانات ... الخ، لقد ثار الخلاف في التشريع المقارن في مسألة ضبط وتفتيش المكونات المعنوية أو المنطقية للحاسوب، فتعددت الآراء في هذا الشأن؛

---

(1) طارق إبراهيم الدسوقي عطية، المرجع السابق، ص385.

(2) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007، ص65.

فذهب رأي إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يجب أن يمتد ليشمل البيانات الالكترونية، كالقانون الإجرائي اليوناني في نص المادة 251 التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، تفسيرا لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة آليا أو الكترونيا، بما فيها ضبط البيانات المخزنة في حاملات البيانات المادية، أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل للمحاكمة الجنائية، على أساس إنها كيانات يمكن قياسها بما انها نبضات أو ذبذبات الكترونية قابلة لان تسجل وتخزن على وسائط معينة يمكن قياسها[1].

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك."

1- هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية القاهرة، 2000، ص 52

هناك بعض الحالات الخاصة يفرض التساؤل عن كيفيات التعامل معها قانونيا في إجراءات ضبط المعلوماتية، والتي سنرى كيف تصدت لها القوانين المقارنة، بالحل كالتالي:

- **مدى جواز الاطلاع على المحتويات المعلوماتية:**

يطرح في مجال التفتيش والضبط المعلوماتي في الجريمة المعلوماتية إشكال جواز أو عدم جواز اطلاع مأمور الضبط القضائي على المحتويات المعلوماتية، فجرى العمل في ألمانيا على أن سلطة الاطلاع على مطبوعات الحاسوب وحاملات البيانات تقتصر على المدعى العام فقط، ولا يكون لضباط الشرطة الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى البيانات المخزونة دون إذن من الشخص الذي له الحق في نقل هذه البيانات، لكن كل ما يمكنهم هو مجرد فحص حاملات البيانات دون استخدام أي مساعدات فنية تطبيقا لما جاء في القسم 110 من قانون الإجراءات الألماني [1].

- **حق المتهم في الصمت:**

يقصد بالحق في الصمت أن للشخص المتهم في جريمة ما مطلق الحرية في الكلام أو عدمه أو عدم الإجابة على الأسئلة الموجهة إليه من قبل مأمور الضبط القضائي أو الموظف القائم بالتحقيق معه، لأنه غير ملزم بالكلام كما يجب أن يراعى أن رفضه

---

(1)طرشي نورة، المرجع السابق، ص 120

الإجابة وصمته، لا يجوز أن يؤخذان كقرينة ضده، وذلك تطبيقا للقاعدة الإجرائيةالعامة التي مفادها: "عدم إجبار الشخص على الكلام أمام أي جهة أو سلطة كحق من حقوق الإنسان"، والتي أوصى بها كل من المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة 1953، والمؤتمر الدولي الذي نظمته اللجنة الدولية لرجال القانون في أثينا في جوان لعام 1955، كما حرصت معظم التشريعات الجنائية على النص صراحة على هذا الحق كالقانون الفرنسي في المادة 114 قانون إجراءات جزائية التي تلزم قاضي التحقيق أن ينبه المتهم عند حضوره أمامه لأول مرة إلى أنه حر في عدم الإدلاء بأي إقرار، ويثبت ذلك التنبيه في محضر التحقيق، ومثلما فعل المشرع الجزائري في المادة 100 من قانون الإجراءات الجزائية.

أما بالنسبة للشاهد المعلوماتي، نعلم أن الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شهده أو سمعه أو أدركه بحواسه عن هذه الواقعة، كما يقصد بسماع الشهود السماح لغير أطراف الدعوى الجنائية بالإدلاء بما لديهم من معلومات أمام سلطات التحقيق، والشاهد المعلوماتي قد يكون شاهدا عاديا أو خبيرا في الدعوى القائمة، بالنسبة للشاهد العادي فهو ذلك الشخص الذي يقدم إلى القاضي معلومات حصل عليها بالملاحظة الحسية، أما الخبير فهو ذلك الشخص المختص الذي يقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية وأصول فنية[1].

1- سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى ، 1998، ص 187

مدى جواز إجبار المتهم والشاهد المعلوماتي على الإدلاء ببيانات

بالنسبة للمتهم المعلوماتي جرى العمل في الفقه والقانون في فرنسا حسب نص المادة 27 من ق اج ج الفرنسي التي نصت على أنه من غير الممكن إجراء تفتيش المساكن وضبط الأشياء التي يمكن أن تكون متعلقة بالجريمة إلا بموافقة صريحة للشخص المراد تفتيش منزله أو أشيائه كما بينت الفقرة الثانية من نفس المادة، بأن الموافقة يجب أن تكون صريحة لا ضمنية، وفي حالة رفض الموافقة الصريحة فإن ذلك يعني رفض ذوي الشأن، ولذلك تعد الإجراءات باطلة وعلى هذا لا يجوز قانونا إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر خاصة بالدخول إلى هذه المعلومات أو إجباره على تقديم الأمر اللازم لوقف فيروس، تطبيقا لمبدأ عدم جواز إلزام الشخص بتقديم دليل ضد نفسه سواء عن طريق الشهادة أو غيرها من عناصر الإثبات، إلا أن ذلك لا يمنع من إجباره على تسليم الشفرة الخاصة بالحاسوب الآلي المخزنة فيه البيانات محل الجريمة[1].

والشاهد المعلوماتي بنوعيه المذكورين سابقا يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، كما أنه يلتزم في بعض الدول الأوروبية بإجراء ما يسمى بإنعاش الذاكرة، بفحص الأماكن والمستندات التي توجد تحت سيطرته وذلك في كل من

1- جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001، ص 106

السويد وفنلندا والنرويج، أما في انجلترا فالقانون الانجليزي الصادر عام 1984 يعطي المحققين الحق في إلزام الغير بتمكين سلطات التحقيق الدخول إلى المعلومات المخزنة في الحاسوب الآلي أو الاطلاع عليها أو قراءتها، كما تسمح بعض التشريعات المقارنة في مجال التحقيق المعلوماتي الاستفادة من الشهود كخبراء أو كمساعدين للقضاء من تلقاء أنفسهم ودون حاجة لاستدعائهم[1].

2-القواعد الشكلية لتفتيش نظم المعلوماتية

تتلخص هذه القواعد كما يلي:

أ -**إجراء التفتيش بحضور أشخاص معينين بالقانون** :من بين هذه الأشخاص: المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية-القائم بالتفتيش-، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".

---

(1) محمد زكي أبو عامر، الاجراءات الجنائية، دار الجامعة الجديدة ، ط 8، 2008، ص 68

ب **إعداد محضر خاص بالتفتيش** :ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ج **إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده** :لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي[1].

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خدمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة.

1- طرشي نورة، المرجع السابق، ص 126.

- إبعاد المتهم عن مكان النظام إن كان قريبا منه.
- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.
- الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.
- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها(1). وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من ق إ ج ج(2).

---

(1) عفيفي كامل عفيفي، المرجع السابق، ص 65.

(2) طرشي نورة ، المرجع السابق ، ص 126.

ثانيا :حجز المعطيات المعلوماتية

أكدت المادة 6 من القانون رقم 04/09، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه في أحكام المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[1].

1- المادة 07 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

ويمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[1].

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[2].

وفي إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون رقم 04/09 تحت تصرف السلطات المذكورة، وذلك لتمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[3].

1- المادة 08 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

2- المادة 09 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

3- المادة 10 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من القانون رقم 04/09، على مقدمي الخدمات إلتزامات خاصة، هي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلي الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجود[1].

الفرع الثاني: المعانية وندب الخبراء في الجريمة الإلكترونية

أولا: المعاينة

المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تسلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يري المحقق أن لها صلة بالجريمة، والأصل أن إجراء المعاينة متروك لتقدير المحقق، لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية ملتبس بها، يجب على

(1)طرشي نورة ، المرجع السابق ، ص 134.

القائمين بالمعاينة تأمين الأجهزة والمعدات التي يتم الإستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة وا خطاره مسبقا حتى يستعد من ناحية الفنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية(1).

ثانيا: ندب الخبراء

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها(2).

ثانيا ندب الخبير: هو كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء أو على مستوى المحاكم أم لا، وهو كل شخص له دراية بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستشير فيها خبراء كما هو الحال في تقرير الصفة التشريعية ف ي جرائم القتل أو تحليل المادة المطعومة في جريمة تسمم، أو فحص لخطوط الكتابة المدعي بتزويرها، ولما كان قاضي التحقيق هو المختص

(1)عبد الفتاح بومي حجازي، مكافة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، بدون سنة، ص. 237

بالتحقيق، قد يتعرض في عمله لمسائل فنية يصعب عليه كرجل قانون البت فيها، حينئذ يجوز له ندب أهل الخبرة، حتى يخرج التحقيق في صورة موضوعية صادقة.

المطلب الثاني:

القواعد الإجرائية المستحدثة لمكافحة الجريمة الالكترونية

تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في الكشف أو في التحري عن الجرائم عموما، وفي سبيل كشفها عن هذه الجرائم، أعطاها القانون سلطة التحري عن الجرائم، كما منحهم قانون الوقاية من الفساد ومكافحته وكذا قانون الإجراءات الجزائية الجديد أساليب جديدة للتحري، أسماها "أساليب التحري الخاصة"، كما أضافت التأكيد على اعتبار جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم التي قرر المشرع صراحة وبنص صريح إمكانية إتباع إجراءات التحري الخاصة في الكشف عنها ومكافحتها، نص المادة 04 من القانون 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني."

أول خطوة في الكشف عن جرائم الإعلام الآلي على مستوى الضبطية القضائية هي مرحلة التحري، حيث يقصد بالتحري في مجال الضبط القضائي، البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها[1]، لذلك فإن رجال الضبطية القضائية إذا أخطروا بجريمة من الجرائم، فإنهم يقومون بالإجراءات الأولية وهذه الإجراءات مرتبطة بالبحث والتحري والذي يعد كمرحلة تمهيدية للدعوى، هذه الإجراءات في حد ذاتها ضرورية، فكلما قرب الزمن بين الإجراء والجريمة كانت الأدلة واضحةً أكثر وأسلم ولم يشبها أي تغيير أو تحريف ومن تم كانت أدعى للثقة[2]، وفي سبيل مكافحة جرائم الفساد، نص المشرع على مجموعة من أساليب التحري تضاف إلى تلك الأساليب التقليدية، وأطلق على هذه الأساليب عبارة "أساليب التحري الخاصة"، ويتمثل الهدف من هذه الأساليب في الكشف عن هذه الجرائم واستئصال الفساد وردع المفسدين.

لقد أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية ، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية و تحفظية ، و التي من شانها ان تتفادى وقوع الجريمة

---

(1) محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية ، دراسة مقارنة ، منشأة المعارف ، الإسكندرية ، مصر، بدون سنة نشر ، ص 289.

(2) محدة محمد، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، عين مليلة، الجزائر، ص 105.

الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها. و هو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها (الفرع01) والتسرب (الفرع 02).

الفرع الأول :مراقبة الاتصالات الإلكترونية وتجميعها:

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري ، ألا وهو الدستور، وهذا في إطار القواعد العامة التي تعنى بالحماية القانونية للحياة الخاصة للأفراد ، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة ."...كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة2016 ، حاول المشرع مواكبة التطور الذي يشهده العالم

في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه:" لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم[1].

إذ أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بالحماية البيانات هو مسألة وقت فقط، خاصة في ظل النشاط التشريعي الذي الجزائر في العشرية الأخيرة، وأن وزارة البريد وتكنولوجيات الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حول حماية البيانات الشخصية على الأنترنيت والذي يفترض أن يصدر قريبا.

علما أن الجزائري هو الوحيد بين الدساتير العربية الذي تطرق لحرمة البيانات الخاصة من المعالجة الإلكترونية، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط[2].

---

(1)القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016.

(2) لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017، ص .6

وبهذا يكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

كما بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر، وهذه الحالات هي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم

تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الأنترنيت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز

المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما، لكن بعد ماذا؟.

بغرض تأطير هذه العملية الحساسة وتخفيف تأثيراتها السلبية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

1 –حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية :

هي الحالات التي أوضحتها المادة الرابعة من القانون 04/09 على سبيل الحصر":

أ– للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة– .

ب– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني – أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون – اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة[1].

بإستقراء الحالات هذه، نجد أن المشرع ق لص من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة "ج " والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

2 –**وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء** تضيف المادة 2/4 من القانون 04/09، بأنه:"لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة ."كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها [2].

1- **لوكال مريم ، المرجع السابق ، ص 09.**

2- نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية، على أنه: " يتضمن الإذن كل العناصر التي تسمح على التعرف على الاتصالات ويسلم مكتوبا ويكون صالحا لمدة أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، يسلم الإذن لوضع الترتيبات بغير رضا أو علم الأشخاص الذين لهم حق على تلك الأماكن."

كما تنص المادة 41 من المرسوم الرئاسي رقم 15/261المؤرخ في 08 أكتوبر 2015 ، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها' على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسر المهني)المادتين 27و28 المرسوم الرئاسي . (15/261)

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانة حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق وإلزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد مجرما، وهذا ما يسمى ضمانات المحاكمة العادلة.

3- تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها:

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

---

(1)الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر 2015.

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في: اعتراض المراسلات الإلكترونية [1]،تسجيل الأصوات، التقاط الصور[2]، تفتيش المنظومات المعلوماتية وحجزها)المادة 5 و7 من القانون 04/09، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟

أجابت المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

1-تعرف المادة 2 /والاتصالات الإلكترونية على أنها": أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

[2]- المادة 65مكرر 5 من القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015

4- سن عقوبات لجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية:

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني.

لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك[1].

الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات و التقاط الصور

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج و التوزيع، التخزين، الاستقبال و العرض، التي تتم عن طريق قنوات

1- المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية 2015.

او وسائل الاتصال السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدلة عنها.(1)

ولقد أشار المشرع الجزائري إلى ظروف و كيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو :" اذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في ...الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن:

-باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكي .

- وضع الترتيبات التقنية، دون موافقة المعنيين، من اجل التقاط و تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ."

فموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق و الاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الالكترونية، اللجوء الى إجراء اعتراض المراسلات السلكية اللاسلكية و تسجيل المحادثات و الأصوات

1- براهيمي جمـــــال، مكافحة الجرائم الالكترونية في التشريع الجزائري أستاذ مساعد "أ "كلية الحقوق والعلوم السياسية، جامعة مولو د معمري، تيـزي وزو.

و التقاط الصور، و الاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف عن ملابسات الجريمة و إثباتها دون (1)أن يتقيدوا بقواعد التفتيش و الضبط المألوفة .

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال و التحري و تصون الحقوق و الحريات العامة و الحياة الخاصة للأفراد و التي يمكن ان تتلخص فيما يلي:

1 - **ترخيص السلطة القضائية و مراقبتها** :بمعنى لا يمكن لضابط الشرطة القضائية القيام بإجراء اعتراض المراسلات إلا بعد الحصول على إذن مكتوب و مسبب من طرف وكيل الجمهورية او قاضي التحقيق في حالة فتح تحقيق قضائي، يحدد فيه نوع - 1 انظر هذه القواعد في المادتين 45 و 47 من قانون الإجراءات الجزائية رقم 06-22 مرجع سابق .الجرائم الالكترونية 141المجلة النقدية الجريمة التي اقتضت ضرورة

التحري أو التحقيق القضائي و طبيعة المراسلة و الاتصال محل الاعتراض أو التنصت، على إن يتم هذا الإجراء تحت الإشراف المباشر للسلطة المصدرة للاذن.

---

1 –لوجاني نور الدين " أساليب البحث و التحري الخاصة و إجراءاتها وفقا لقانون رقم 06-22 المؤرخ في 20-12-2006 "مداخلة في يوم دراسي حول " علاقة النيابة العامة بالشرطة القضائية-احترام حقوق الإنسان و مكافحة الجريمة" وزارة الداخلية، المديرية العامة للأمن الوطني، المنعقد باليزي،. يوم 12/12/2007 ، الجزائر الجرائم الالكترونية المجلة النقدية 140ص 08

2-ضرورة الاعتراض لإظهار الحقيقة : ويعتبر السند الشرعي المبرر للاعتراض، ذلك لما يمكن أن يحمله هذا الإجراء من اعتداء جسيم على حرمة الحياة الخاصة و سرية الاتصالات، فيباح استثناءا و في حدود ضيقة اعتبارا 1للفائدة المنتظرة منه، و المتعلقة بكشف اللثام عن الجريمة و ضبط الجناة 1 .

3مراعاة الجرائم التي يجوز فيها الاعتراض: أي أن ينصب الاعتراض على إحدى الجرائم التي سمحت فيها المادة 65 مكرر 5 من قانون الإجراءات الجزائية الاستعانة بهذا الإجراء، و حددتها على سبيل الحصر في مقدمتها جرائم الاعتدا على نظم المعالجة الالية

– 4 . **مراعاة مدة الإجراء :** حددتها الفقرة 2 من المادة 65 مكرر7 ب أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية و الزمنية، حسب تقدير نفس السلطة مصدرة الإذن لمقتضيات التحقيق2.

– 5 .**مراعاة السر المهني أثناء الاعتراض:** اي عند القيام باعتراض المراسلات تلتزم سلطات التحقيق بعدم المساس بالسر المهني المتعلق بالتفتيش المنصوص عليه في المادة 45 من قانون الإجراءات الجزائية ، خاصة إذا تعلق الأمر بأماكن يشغلها أشخاص ملزمون بكتمان السر المهني ، مثل مكتب المحامي، مكتب المحضر القضائي، أو تعلق

1– انظر : لوجاني نور الدين، مرجع سابق، ص10

2– تنص الفقرة 2 من المادة 65 مكرر7 من قانون الإجراءات الجزائية رقم 06–22 على:" يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد ...."

الأمر بأشخاص يحملون اسرار مهنية مثل القضاة، الأطباء، نواب البرلمان، فبرغم ان تلك الأماكن وهؤلاء الأشخاص غير مستثنين من إجراء الاعتراض إلا انه يقتضي الأمر وجوب اتخاذ التدابير اللازمة 1لضمان احترام السر المهني الذي يخصها 1.

6–تحرير محضر حول عملية الاعتراض: اي يجب على سلطات التحقيق المختصة تحرير محضرا عن تفصيل كل عملية اعتراض و تسجيل المكالمات و المراسلات و عن عملية الالتقاط و التسجيل الصوتي او السمعي البصري، كما يذكر بالمحضر تاريخ بداية هذه العمليات و نهايتها2.

1- محمد ابو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، طبعة ثانية، دار النهضة العربية، القاهرة، 2008،ص 192- .

2-انظر المادة 65 مكرر 9 من قانون الإجراءات الجزائية رقم 06-22.

الفرع الثالث: التسرب

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون الإجراءات الجزائية رقم 06 -22 على انه :" قيام ضابط او عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف."

من خلال هذا التعريف يمكن تصور عملية التسرب في نطاق جرائم الاعتداء ،مرجع سابق .الجرائم الالكترونية 143المجلة النقدية على أنظمة المعالجة الآلية في ولوج

ضابط او عون الشرطة القضائية الى العالم الافتراضي (الانترنت) و اشتراكه مثلا في محادثات غرف الدردشة او حلقات النقاش و الاتصال المباشر في كيفية قيام احدهم باختراق شبكات او بث الفيروسات، منتحلا في ذلك هوية مستعارة أو باستخدام أسماء و صفات هيئات وهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منه إلى الكشف والإطاحة بالمجرمين.(1)

ولقد سمحت المادة 65 مكرر 14 من قانون الإجراءات الجزائية لضابط أو العون المتسرب من اجل إنجاح العملية، استعمال الوسائل المادية كالأموال أو المنتجات او الوثائق المتحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، كما يجوز له

---

(1) رشيدة بوكر، مرجع سابق، ص 434. .

تسخير وضع تحت تصرف مرتكبي هذه الجرائم كل الوسائل المادية المتاحة لتنفيذ الجريمة كوسائل النقل او التخزين أو الإيواء أو الحفظ أو الاتصال، وكذا الوسائل القانونية كتوفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة التعريف الوطنية او بطاقة رمادية او جواز السفر و لو استدعى الأمر تزويرها ، دون أن يكون الضابط أو العون المتسرب مسئولا جزائيا عن هذه الأعمال .

اعتبارا أن التسرب إجراء غير مألوف عند سلطات الضبط القضائي، و انه من اخطر إجراءات التحقيق انتهاكا لحرمة الخاصة للمتهم، كان لزاما على المشرع إحاطته بجملة

من الضمانات و الضوابط التي يتعين مراعاتها عندما تقتضي ضرور ات التحري او التحقيق في إحدى الجرائم المذكورة اللجوء إليه، و التي يمكن تلخيصها فيما يلي:

1 – صدور إذن قضائي بالتسرب : نصت على هذا الشرط المادة 65مكرر 11 ومفاده انه لا يجوز لضابط الشرطة القضائية اللجوء إلى التسرب إلا بناءا على إذن مكتوب (1) ، صادر من وكيل الجمهو رية المختص او قاضي التحقيق بعد إخطار وكيل الجمهورية، على أن يذكر فيه اسم الضابط المشرف على العملية و هويته الكاملة، و تاريخ بداية التسرب.

1–تجدر الإشارة إلى أن الكتابة شرط جوهري لصحة الإذن بالتسرب وهو ما نصت عليه المادة 65 مكرر 15 بأنه " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 أعلاه مكتوبا... تحت طائلة البطلان"

2/احترام المدة المقررة للتسرب: حددت الفقرة الثالثة من المادة 65مكرر 15 من قانون الإجراءات الجزائية مدة التسرب بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري و التحقيق بنفس الشروط ، و يجوز للقاضي الذي رخص بإجراء التسرب أن يأمر في أي وقت بوقفه قبل انقضاء المدة القانونية. و في هذه الحالة و تحسبا للظروف الأمنية للضابط المتسرب أجازت المادة 65 مكرر 17من نفس القانون لهذا الأخير مواصلة نشاطه لمدة لا تتجاوز أربعة أشهر دون ان يكون مسئولا جزائيا على ذلك، بشرط ان يخطر السلطة مصدرة لإذن في اقرب اجل(1).

3-**تسبيب عملية التسرب :** يعتبر التسبيب شرط جوهري لمشروعية عملية التسرب، لذلك اشترط القانون عند إصدار الإذن بالتسرب من السلطات المختصة ذكـر السبب أو الدافع الحقيقي الجاد الذي يبرر اللجوء إلى هذ الإجراء تحت طائلة البطلان.

4-محل التسرب: بمعنى أن عملية التسرب يجب أن تنصب على إحدى الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5، وهي: جرائم المحذرات، الجريمة المنظمة، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف .و فيما عدى ذلك يعتبر التسرب إجراء باطلا.

---

(1) انظر الفقرة الثالثة من المادة 65 مكرر 15 و نص المادة 65 مكرر 17 قانون الإجراءات الجزائية، مرجع سابق.

لجدير بالذكر في الأخير هو أن المشرع الجزائري سمح لسلطات الضبطية القضائية إذا اقتضت ضرورة التحري و التحقيق ممارسة عملية اعتراض المراسلات و تسجيلها و التقاط الأصوات و التسرب و كذا باقي إجراءات التحقيق التي تدخل في اختصاصاتها، عبر كافة الإقليم الوطني إذا تعلق الأمر ببحث و معاينة جرائم الماسة بالمعالجة الآلية للمعطيات. و هذا الإجراء المتمثل في تمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني هو من ضمن التدابير غير المألوفة في السابق و التي

استحدثها المشرع في المادة 16 الفقرة 7 و 8 و المادة 16 مكرر من قانون الإجراءات الجزائية رقم 06-22 من اجل تحقيق المواجهة الفعالة لظاهرة الإجرام الالكتروني .(1)

---

(1)انظر نص المادة 65 مكرر 15 من قانون الإجراءات الجزائية، نفس المرجع.

الخـــــــــاتمـــــــة

في الأخير نخلص، إلى أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيمانا بأهمية الوقوف

أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختم هذا البحث ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت النقاط الآتية:

1-عقد دورات مكثفة للعاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوبات، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

2- تعديل بعض التشريعات الحالية بما يتلائم مع طبيعة جرائم الإنترنت والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح، وخاصة وأن في مجال الملكية الفكرية فالتشريع الوحيد الذي تقع برامج المعالجة الآلية للمعطيات تحت حمايته هو قانون حقوق المؤلف وحتى في إطار هذا القانون لا تتعدى الحماية شكل البرنامج فقط، لهذا السبب تبرز أهمية البحث عن إطار أكبر وأوسع لبرامج الكمبيوتر

يتعدى النصوص التقليدية لجريمة التقليد المنصوص عليها في قانون حقوق المؤلف والحقوق المجاورة.

3-إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية والدولية على السواء، مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، باعتبار أن جرائم الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية،

والاهتمام بالتعاون الدولي في مجال المكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

4- نظرا لطبيعة الجريمة المعلوماتية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة والبحث عن أدلتها فحتى؛ وإن نجحت الدّول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعاينة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط عليها، لتتلائم وطبيعة الجريمة المعلوماتية، تبقى بعض الصعوبات دائما للكشف عن هذه الجريمة والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها وفترة اكتشافها، مما يصعب عملية الكشف عنها.

5- مساعدة شركات التقنية والإنترنت العربية في اتخاذ إجراءات أمنية مناسبة، سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.

6

6-التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الإنترنت لا تحدها حدود وطنية، أو قومية.

7–سرعة تماشي عملية التشريع مع المعطيات الواقعية، والإسراع في إصدار القوانين التنظيمية، من خلال محاولة وضع مدونة قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.

8–كما تظهر ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى.

9–وأخيرا في رأينا، أن أحسن حماية هي الحماية الوقائية بحيث من الأفضل نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية) عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، عدم نشر معلومات شخصية، عدم إعطاء كلمة السر.الخ.)

قائمـــــــة المراجـــــع

أ- الكتب:

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

2- د مجيد ناصر الفتال ، أمن المعلومات ،دار اليازوري للنشر والتوزيع عمان الأردن بدون سنة النشر

3--المستشار صالح بن علي. الجريمة المعلوماتية مخاطرها مجلة رؤية 2003 العدد 45

4--د.بوضياف اسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، العدد الحادي عشر ،جامعة محمد بوضياف المسيلة، 2018

5-د لينا محمد الاسدي ،امعوقات مكافحة الجريمة الالكترونية رسالة ماجستير 1434 هـ

6-عبد الله الدغمش ، المشكلات العملية والقانونية ،رسالة ماجستير ،جامعة الشرق الأوسط 2014.

7- مجلة المعلوماتية. العدد362 أكتوبر 2011

8-عبد الكريم الردايدة. ، جرائم بطاقات الائـتمـان لدراسـة تطبيقيـة ميدانية ، الطبعـة الأولى، الأردن، دار حامد، 2013

9-عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية ، الكتاب الثاني الحماية الجنائية لنظام التجارة الالكترونية، الطبعة الأولى، الاسكندرية، دار الفكر الجامعي، 2002

10-د مدحت رمضان ، جرائم الاعتداء على الأشخاص والانترنت ،دار النهضة العربية –القاهرة-2000 ، 11- محمد حماد الهيتي مرجع سابق.

12–د عبد الفتاح بيومي حجازي ، الاحداث والإنترانت – دار الكتب القانونية –سنة 2002 مصر

13–د احمد عبد الجواد حجازي –الحياة الخاصة ومسؤولية الصحفي ، دار الفكر العربي – القاهرة 2001.

14 / –د أحمد حسام طه تمام، الجرائم الناشئة عن إساءة استخدام الحاسب الآلي، ط 1، دار النهضة العربية– القاهرة 2000،

15–د. محمد سامي الشوا– ثورة المعلومات وانعكاساتها ا على قانون العقوبات– دار النهضة العربية– القاهرة– 1994

16–سعد الحاج بكري– شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة– ا لة العربية للدراسات الامنية والتدريب– س6 –ع11) – 92– 1990– الرياض.

17–فضيلة عاقلي، الجريمة الإلكترونية واجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017 ، طرابلس.

18–عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت ، دار الكتب القانونية ، مصر، 2007.

19–بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016

20–سعيدة يوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر، 2019.

21–طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009،

22–خالد ممدوح إبراهيم، فن التحقيق الجاني في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2008

23-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة 2 ،دار الفكر الجامعي، مصر، 2011

24-مروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، 2011

25-خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011

26- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2010

27- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الطبعة الثانية،

28- هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة،2000.

29- سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى، 1998

30-جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001.

31-محمد زكي أبو عامر، الإجراءات الجنائية، ط 8، دار الجامعة الجديدة، مصر، 2008.

32-محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر.

33-محدة محمد، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، عين مليلة، الجزائر

34- محمد ابو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، طبعة ثانية، دار النهضة العربية، القاهرة، 2008

35- ابتسام بخو ،مذكرة تكميلية ماستر في القانون –تخصص قانون جنائي للأعمال،اجراءات المتابعة الجزائية في الجريمة المعلوماتية جامعة العربي بن مهيدي أم البواقي.2015 2016

36-ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2015 -2016 ،

ب-المذكرات والرسائل

1- د علاء حميد الجبوري ،احكام المعالجة لحساب الأوراق المالية ،أطروحة دكتوراه مقدمة الى كلية الحقوق – جامعة النهرين 2003

2- الدكتور نبيل صالح حمد العريب، أستاذ مساعد بكلية الاقتصاد والإدارة – جامعة القصيم دراسة بعنوان "اقتصاديات الجرائم المعلوماتية

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

4- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات،العدد الثاني، ديسمبر 2017 ،المركز الجامعي إليزي، الجزائر

5-نايري عائشة، مذكرة لنيل شهادة الماستر في القانون الإداري ،قسم الحقوق ،جامعة أحمد داية – أدرار – 2016- 2017 .

6-فرام، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب،المعهد العالي للقضاء،2007-2009

7-طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر1، 2011-2012.

8- ضريفي نادية، سلطات القاضي الجاني في تقدير الدليل الإلكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04 ،العدد ، 02 219

9-غازي عبد الرحمان هيان الرشيد،الحماية القانونية من جرائم المعلوماتية الحاسب والانترنت، أطروحة لنيل درجة دكتوراه في القانون، الجامعة الاسلامية في لبنان ، كلية الحقوق،2004

ج- الندوات والمؤتمرات:

1-برابح يمينة، تطبيقات الأمن المعلوماتي، بالملتقى الوطني الموسوم بـ :الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017.

2-موسى مسعود أرحومة الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطن ورقة مقدمة من المؤتمر المغاربي الأول حول المعلوماتية والقانون، الذي تنظمه أكادمية الداسات العليا ، طرابلس خلال الفترة 10/29/28/

3-لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017.

4-برا هيمي جمـــــال، مكافحة الجرائم الالكترونية في التشريع الجزائري ، محاضرة ، أستاذ مساعد "أ "كلية الحقوق والعلوم السياسية، جامعة مولـو د معمري، تيـزي وزو.

5- لوجاني نور الدين " أساليب البحث و التحري الخاصة و إجراءاتها وفقا لقانون رقم 06-22 المؤرخ في 20-12-2006 "مداخلة في يوم دراسي حول " علاقة النيابة العامة بالشرطة القضائية-احترام حقوق الإنسان و مكافحة الجريمة" وزارة الداخلية، المديرية العامة للأمن الوطني، المنعقد باليزي،. يوم 12/12/2007 ، الجزائر الجرائم الالكترونية المجلة النقدية 140

د- القوانين والمراسيم:

1-مرسوم رئاسي رقم 261-15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر 2015.

2-القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

3-القانون رقم 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد (71) لسنة 2004.

4-القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016.

5-المادة 65 مكرر 7 من قانون الإجراءات الجزائية الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

6-الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر 2015.

7- المادة 65مكرر 5 من القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015

8- المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966

9-الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية 2015

الفهـــرس

المطلب الأول: تعريف وخصائص الجريمة الالكترونية

الفرع الأول: تعريف الجريمة الالكترونية

الفرع الثاني: خصائص الجريمة الالكترونية

المطلب الثاني: أركان الجريمة الالكترونية وأنواعها

الفرع الأول: أركان الجريمة الالكترونية

أولا: الركن المادي ثانيا:الركن المعنوي ثالثا: الركن الشرعي

الفرع الثاني: أنواع الجريمة الالكترونية

أولا: جرائم الأموال ثانيا:جرائم الاعتداء على الأشخاص

المبحث ألثاني: محترفوا الجرائم الاكترونية أسبابها وآثارها

المطلب الأول: أشخاص الجريمة الالكترونية

الفرع الأول:المجرم الإلكتروني

الفرع الثاني:مجرمين مبرمجين

الفرع الثالث: المجني عليه في الجريمة الإلكترونية

المطلب الثاني:أسباب الجريمة الإلكترونية وآثارها

الفرع الأول:أسباب الريمة الالكترونية

الفرع الثاني:آثار الجريمة الالكترونية

الفصل الثاني:الضبطية القضائية بين المتابعة وأساليب مكافحة الجريمة الالكترونية

المبحث الأول:هيئات ووحدات متخصصة في البحث والتحري في الجرائم الالكترونية

المطلب الأول:اليئات الفنية المتخصصة في البحث والتحري في الجرائم الالكترونية

الفرع الأول:الهيئة الوطنية والهيئة القضائية

أولا:الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

ثانيا:الهيئات القضائية الجزائية المتخصصة

الفرع الثاني:جهازي الأمن الوطني والدرك الوطني

أولا:الوحدات التابعة لسلك الأمن الوطني

ثانيا:الوحدات التابعة للقيادة العامة للدرك الوطني

المطلب الثاني:صلاحيات الضبطية في مجال حماية النظام الالكتروني

الفرع الأول:اختصاص الضبطية القضائية

أولا:الاختصاص المحلي ثانيا:الاختصاص النوعي

الفرع الثاني:التحقيق في الجريمة الالكترونية

أولا:خصائص التحقيق الالكتروني

ثانيا:الخصائص الفنية للمحقق الالكتروني

المبحث الثاني:آليات محاربة الجريمة الالكترونية

المطلب الأول:القواعد الإجرائية التقليدية لمكافحة الجريمة الالكترونية

الفرع الأول: جمع الاستدلالات في الجريمة الإلكترونية

أولا:تلقي البلاغات في الجريمة الالكترونية

ثانيا:الشكوى في الجريمة الالكترونية