جامعة ابن خلدون– تيارت
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر
في الحقوق
التخصص: القانون الجنائي والعلوم الجنائية
بعنوان:

خصوصية الجريمة الإلكترونية

إعداد الطالبة:
* بن لعربي أسماء

إشراف الأستاذ الدكتور:
* بوشي يوسف

لجنة المناقشة		
أ/د. هروال هبة نبيلة	أستاذ التعليم العالي	رئيسا
أ/د. بوشي يوسف	أستاذ التعليم العالي	مشرفاومقررا
د. سيهوب سليم	أستاذ محاضر (أ)	عضوا مناقشا
د. قاصدي فايزة	أستاذ محاضر (أ)	عضوا مدعوا

السّنة الجامعيّة

1441 ـ 1442هـ /2020- 2021م

بسم الله الرحمن الرحيم

كلمة شكر

﴿وَأَمَّا بِنِعْمَةِ رَبِّكَ فَحَدِّثْ﴾

الحمد والشكر لله تعالى الذي ألهمني وأعانني على إتمام بحثي هذا، والذي آمل أن أكون قد حققت الغاية المرجوة منه

أتقدم بالشكر والتقدير إلى الأستاذ الدكتور *بوشي يوسف* الذي تفضل بالإشراف على هذه المذكرة وتقديم النصح والإرشاد طوال فترة إعداد المذكرة فله مني فائق الاحترام والتقدير

كما أتقدم بالشكر إلى كل أعضاء اللجنة المحترمة الذين قبلوا مناقشة هذا البحث

وأخص بالذكر الأستاذة *هروال نبيلة هبة* التي لطالما استفدنا من نصائحها حفظها الله وأطال في عمرها

وأتقدم بالشكر إلى جميع أساتذة كلية الحقوق وجميع من ساعدني من قريب أو بعيد في إعداد هذه المذكرة

إهداء

أهدي عملي هذا و جهدي المتواضع:

إلى من علمني معنى الحياة و الحياء و الحب و التضحية و العطاء، إلى من تكتحل عيناه برؤية ما جنيت "أبي العزيز" حفظه الله وأطال في عمره وأمده بالصحة والعافية

إلى من أضاءت لنا درب الحياة بنور الأخلاق والتربية الفضيلة فعلمتنا أن العلم تواضع و العبادة إيمان و نجاح إلى منبع الحنان "أمي الغالية" أطال الله في عمرها

إلى من أشد بهم أزري إخوتي: عبد الحق وإيمان

إلى أخي "محمد" والذي لا يفوتني أن أشكره على كل ما قام به من مجهودات من أجلي خلال مساري الدراسي

إلى صديقاتي العزيزات

و إلى كل من ساعدني من قريب أو من بعيد في إعداد هذه المذكرة

أسماء

قائمة المختصرات

المختصر	المعنى
ق ع	قانون العقوبات
ق م	القانون المدني
ق إ ج	قانون الإجراءات الجزائية
ج ر ج ج	الجريدة الرسمية للجمهورية الجزائرية
ص	صفحة
ط	طبعة
د ط	دون طبعة
د ت	دون تاريخ
د د ن	دون دار نشر
مج	مجلد
ج	جزء
د د ن	دون دار نشر
ف	فقرة
ع	عدد
P	Page

مقدمة

مقدمة:

شهدت الإنسانية في العقدين الرابع والخامس من القرن الماضي عن ابتكار أعظم ما قدمته البشرية، لما حدث من تطورات كبيرة في مجال تكنولوجيا الإعلام والاتصال، فالعالم اليوم يعيش أزهى عصوره العلمية والتكنولوجية بسبب هذا الابتكار الذي يتمثل في الحاسوب، مما نتج عنه ثورة معلوماتية بالغة الأهمية أحدثت تغيرا في المجتمع، حيث ساهمت في تطوره، وذلك نتيجة لتدخلها في مختلف نواحي الحياة، حيث أصبحت مصدرا أساسيا للأشخاص والمؤسسات باعتمادهم عليها في كافة شؤونهم نظرا لامتيازها بالسرعة والدقة في معالجة المعلومات وتخزينها في ظرف قصير.

حيث انه في هذه الفترة عرف المجتمع الدولي في مجال تكنولوجيا الإعلام والاتصال تطورا مذهلا في مجال شبكات الاتصال، حيث أصبحت هذه الشبكات من أهم الوسائل التي تتم بها المعاملات على المستوى الدولي، مما أضحى من الصعوبة الاستغناء عنها، ومن أهم الشبكات الاتصالية التي يتعامل بها الأفراد والمؤسسات والدول في الحياة اليومية على حد سواء هي شبكة الانترنت.

في الآونة الأخيرة شملت استعمالات الانترنت مختلف نشاطات الإنسان التجارية والاقتصادية، بالإضافة إلى مجالات التعليم والترفيه، برزت أيضا في مجال الاتصالات وتبادل الأفكار والمعلومات، بشكل يجعلها لا تعترف بالحدود الجغرافية ولا سياسية.

الأمر لذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى استعمال المنظمات المعلوماتية على نحو غير مشروع، من أجل ارتكاب أعمالهم الإجرامية المختلفة، والتخلص من المسؤولية الجزائية.

ومع هذا التطور المتزايد لأنظمة المعلومات ظهر شكل جديد للإجرام وهو ما يسمى بمصطلح "الجرائم الالكترونية"، أو بمفهوم آخر "الجرائم المعلوماتية".

فالنشاط الإجرامي لم يعد مقتصرا على الوسائل التقليدية المعروفة فقط، بل صار يعتمد بالإضافة إلى ذلك على وسائل أكثر حداثة، وذلك بالاستعانة بنظم المعلومات والاتصالات.

وهذا ما يجسد الجانب المظلم الذي يواجهه المشرع الجنائي خاصة في إثبات هذا النوع من الجرائم.

الأمر الذي أدى إلى تدخل المجتمع الدولي من أجل وضع حد لانتشاره، فكان لابد من وضع قوانين ملائمة جديدة أو تعديل القوانين سارية المفعول بما يتلاءم مع هذه الظاهرة، بالإضافة إلى تحدد شروط استعمال هذه الوسائل في نختلف المعاملات من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في إطار الاتفاقيات الدولية.

والجزائر باعتبارها واحدة من الدول التي تعرضت لهذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا فهي أيضا معنية بالتصدي لهذه الظاهرة، فكان لابد من إيجاد حلول مناسبة لسد الفراغ القانونين انطلاقا من تجريم وعقاب مرتكبي الجريمة الإلكترونية، وذلك بتحديد مجموعة من الأحكام لقيام هذه الجرائم وتحديد العقاب المقرر لها، بالإضافة غلى وضع مجموعة من الإجراءات، منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المستحدثة عن طريق تعديل قانون الإجراءات الجزائية باستحداث وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة كالجريمة الإلكترونية. ومنها إجراءات تطبق فقط على الجريمة الإلكترونية تم النص عليها في قانون مستقل يتضمن القواعد الخاصة للوقاية من جرائم المساس بتكنولوجيا الإعلام والاتصال ومكافحتها 09-04.

تكمن أهمية البحث أساسا في كون الجرائم الإلكترونية حديثة النشأة، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيات الإعلام والاتصال، حيث تستخدم في جميع مجالات الحياة سواء من طرف الأفراد أو المؤسسات مما يحتم إيجاد طرق وتدابير جديدة ونافعة لمكافحتها.

بالإضافة إلى كون الجرائم الإلكترونية جرائم جديدة، فبالتالي لتا يمكن تطبيق نفس الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات التي لم تنل حظها من البحث والتحقيق والمحاكمة على المستوى الجزائي، حيث لا يمكن تطبيق القواعد الإجرائية التقليدية عليها، بالإضافة إلى الصعوبات والمعوقات التي يواجهها رجال العدالة في إجراءات الضبط والتحري، والصعوبة البالغة في جمع الأدلة بناء على ما هو متوفر في الجريمة الإلكترونية.

وتأسيسا على ذلك حاولنا من خلال هذه المذكرة مناقشة المفاهيم القانونية المتعلقة بالجريمة الإلكترونية، وربطها بالمفاهيم القانونية المتعلقة بإجراءات تحصيل واستقصاء الدليل في إثبات الجريمة، ووضع التصورات المتعلقة بالجوانب الإجرائية في إطار التعامل مع الجريمة الإلكترونية في ظل النصوص القانونية الحالية ف التشريع الجزائري.

على الرغم من الصعوبات التي واجهناها في إعداد هذه المذكرة منها قلة المراجع التي يمكن الاعتماد عليها خاصة في الجانب الإجرائي، لاسيما هذا الموضوع الذي يتم بالحداثة، ونظرا لصعوبة الموضوع وتشعبه.

ومن أسباب اختيارنا لموضوع الجريمة الإلكتروني ة يرجع في حقيقة الأمر إلى العديد من الأسباب منها أسباب ذاتية وأخرى موضوعية.

فالأسباب الذاتية تكمن في اهتمامنا بمجال الجرائم المستحدثة ولا سيما الجريمة الإلكترونية لأنها باتت ترتكب بكثرة في الوقت الراهن، بالإضافة إلى أن هناك الكثير من الدراسات التي عنيت بهذه الجرائم ترتكز على الجانب الموضوعي فقط، فوجدنا ندرة في المؤلفات التي تتعرض

للجانب الإجرائي، لهذا حاولنا من خلال هذه المذكرة إثراء النقاش القانوني والمكتبة الجزائية بمراجع في هذا الموضوع من الناحية الموضوعية والإجرائية.

أما الأسباب الموضوعية تكمن في كون الجرائم الإلكترونية موضوع حديث يمس الواقع المعاش، كما أنها تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية وحكومة إلكترونية وهذا ما يساعد على انتشار هذا النوع من الجرائم، نظرا لحداثة الموضوع فلابد من الوقوف للجانب الموضوعي لتجريم الأفعال أو الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، والقواعد الإجرائية الحديثة التي جاء بها تعديل قانون الإجراءات الجزائية وكذا القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وعليه سنحاول من خلال هذه الدراسة أن نبين أبرز النقاط المهمة المتعلقة بهذه الجريمة الحديثة وذلك من خلال طرح الإشكال التالي:

فيما تتمثل خصوصية الجريمة الإلكترونية من الناحية الموضوعية والإجرائية؟

ومنة هنا نطرح عدة تساؤلات فرعية تتمثل:

-ما المقصود بالجريمة الإلكترونية؟

-ماهي السمات والخصائص التي تميز الجريمة الإلكترونية عن الجريمة التقليدية؟

-هل النصوص التقليدية قادرة على الإيفاء بالغرض لمواجهة هذه الجرائم الفنية المعقدة؟

-فيما تتمثل إجراءات متابعة الجريمة الإلكترونية طبقا للتشريع الجزائري؟

-هل تخضع الجريمة الإلكترونية للقواعد الإجرائية العامة أو قرر لها المشرع أحكاما خاصة؟

-إلى أي مدى تقيد المشرع الجزائري بالإجراءات العادية في الجرائم الإلكترونية؟

واعتمدنا في دراستانا هذه على المنهج التحليلي، الوصفي كونه الأنسب لمثل هذه الدراسات، من خلال وصف هذه الظاهرة وبيان المفاهيم القانونية الخاصة بها، بالإضافة إلى تحليل

مختلف المواد القانونية التي تتضمن الجريمة الإلكترونية، وكذا إجراءات المتابعة فيها واختلافها عن النصوص الإجرائية التقليدية.

لقد تطرقت عدة دراسات سابقة إلى الجرائم الإلكترونية من الناحية الموضوعية فقط، مع وجود بعض الدراسات التي تطرقت لها من الناحية الإجرائية، لكن ليس بالتفصيل، الأمر الذي جعلها قاصرة، ومن بين هذه الدراسات التي تم الاعتماد عليها في بحثنا هذا هي:

-كتاب مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، للدكتور عبد الفتاح بيومي حجازي، مصر، لسنة 2007، حيث تناول موضوع إجراءات التحقيق في الجريمة الإلكترونية تفصيلا وتحليلا، حيث تطرق لمختلف المشكلات المتعلقة بالدليل الإلكتروني والمتعلقة بسلطات الاستدلال والتحقيق.

-وكتاب الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، للأستاذة هراول هبة نبيلة، الإسكندرية، لسنة 2007، تناولت هي الأخرى هذا الموضوع بشكل موسع، حيث تطرقت إلى ماهية جرائم الانترنت وأنواعها، بالإضافة إلى إجراءات متابعة هذه الجرائم في مرحلة جمع الاستدلالات باعتمادها على دراسة مقارنة.

بينما تطرقنا نحن في هذه المذكرة إلى إجراءات متابعة الجريمة الإلكترونية في جميع مراحل الدعوى العمومية بداية بمرحلة جمع الاستدلالات، مرورا بالتحقيق، وصولا إلى إجراءات المحاكمة في هذه الجريمة، بالإضافة إلى الجانب الموضوعي للجريمة الإلكترونية.

ومن أجل معالجة الإشكالية الرئيسية والإشكاليات الفرعية التي تم طرحها، وجب تقسيم الدراسة وفقا لخطة منهجية تتمثل في مايلي:

تطرقنا في الباب الأول إلى الإطار الموضوعي للجريمة الإلكترونية قسمناه إلى فصلين هما:

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية.

الفصل الثاني: أركان الجريمة الإلكترونية.

أما الباب الثاني تطرقنا فيه إلى الإطار الإجرائي للجريمة الإلكترونية قسمناه إلى فصلين هما:

الفصل الأول: إجراءات البحث والتحري في الجريمة الإلكترونية.

الفصل الثاني: إجراءات التحقيق والمحاكمة في الجريمة الإلكترونية في كب مبحث مطلبين.

لنختم جهدنا هذا بخاتمة لهذا الموضوع.

الباب الأول

الإطار الموضوعي للجريمة الإلكترونية

الباب الأول: الإطار الموضوعي للجريمة الإلكترونية

منذ قديم الأزل والجريمة جزء لا يتجزأ من سلوك الإنسان في المجتمع، حيث ندرة الموارد وحاجة هذا الأخير وأطماعه التي ليس لها حدود تجعل من تضارب المصالح والتناحر عليها سمة يتميز بها كل مجتمع، بصرف النظر عن درجة ثقافته وتقدمه الاقتصادي والعلمي، وعلى الرغم من الجهود الحثيثة التي تبذلها كل دولة لمقاومة الظاهرة الإجرامية إلا أن الإحصائيات تشير دوما إلى زيادة نسبة الإجرام في الغالبة العظمى من دول العالم، وخصوصا خلال القرن الأخير، الذي شهد ثورة معلوماتية من نمط مميز، وما أفرزته تلك الأخيرة من جرائم مستحدثة لم يسبق أن عرفها العالم.[1]

وبدورنا في هذا الموضوع سنحاول في هذا الباب التطرق إلى الجانب الموضوعي للجريمة المرتكبة عبر الانترنت، من خلال التعرف على ماهية الجريمة الإلكترونية (**الفصل الأول**)، ثم تبيان أركان هذه الجريمة (**الفصل الثاني**).

[1] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، ط 1، دار الفكر الجامعي، الإسكندرية، 2007، ص 20.

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

تعتبر الجريمة المرتكبة عبر الانترنت من الآثار السلبية التي خلّفتها التقنية العالية، حيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها.[1]

فإن محاولة تعريف وضبط المقصود بجرائم الحاسب الآلي بعد استعراض النماذج الموضوعية لتعريفها، والتي تتسم بتنوعها وتعدد تسمياتها جريمة الحاسب Computer Crime وإساءة استخدام الحاسب Computer Abuse، والجريمة المرتبطة بالحاسب Computer Related Crime، وجريمة المعالجة الآلية للبيانات Automatic Data Processing ، والجريمة المعلوماتية Informatic crime، كل هذه التسميات تكشف عن اختلاف في مفهوم هذه الجرائم لدى واضعيها، الأمر الذي يزيد الوضع تعقيدا.[2]

وضع المشرع في مختلف أنحاء المعمورة في موضع المتفرج رغم المحاولات التي جاء بها، فإذا كانت الجرائم التقليدية قد نالت جانبا من الاعتناء، وذلك بتحديد مختلف المفاهيم والتعاريف الخاصة بها، إضافة إلى طرق مكافحتها فإن الجريمة المرتكبة عبر الانترنت مازالت قيد البحث من طرف الفقهاء والقانونيين.[3]

وفي هذا الفصل سنحاول تحديد الإطار المفاهيمي لهذه الجرائم، من خلال تناول هذا الموضوع بمبحثين، يخصص الأول لتحديد مفهوم الجريمة الإلكترونية (**المبحث الأول**)، ويخصص الثاني للتعرف على خصائص هاته الجريمة وأنواعها (**المبحث الثاني**).

---

[1] – صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 07.

[2] – محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، د.ط، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 11.

[3] – عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، سعيدة، العدد الثاني، 2014، ص 69.

المبحث الأول: مفهوم الجريمة الإلكترونية

عرّفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة، يقرر له القانون عقوبة أو تدبيرا احترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم.[1]

ومن ثمة سوف نتناول الاتجاهات المختلفة في تعريف الجريمة الإلكترونية (**المطلب الأول**)، وسنتطرق إلى التطور التاريخي لهذه الجريمة وإحصائيات حولها (**المطلب الثاني**).

المطلب الأول: تعريف الجريمة الإلكترونية

لقد تعددت واختلفت التعاريف بشأن الجريمة الإلكترونية باعتبارها ظاهرة جديدة مازالت قيد البحث والدراسة من طرف القانونيين والعديد من الفقهاء، وبالمثل لا يوجد تعريف محدد ومتفق عليه لهذا النوع المستحدث من الجرائم.[2]

ولقد خصصنا هذا المطلب لتحديد المقصود من هاته الجرائم، وذلك من خلال تقسيمه إلى فرعين، نتناول تعريف الجريمة الإلكترونية من الناحية القانونية (**الفرع الأول**)، وبعد ذلك نتطرق إلى تعريفها من الناحية الفقهية (**الفرع الثاني**).

الفرع الأول: التعريف القانوني للجريمة الإلكترونية

منذ عشر سنوات مضت لم يكن المشرع (سواء في البلدان العربية أو الغربية) يعبأ وعلى نحو جدي بانعكاسات استخدام شبكة الانترنت وغيرها من التطبيقات التقنية الحديثة، سواء أكانت تلك الانعكاسات إيجابية (إبرام وتنفيذ وتسهيل المعاملات المدنية والتجارية عن طريق

[1] – محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، د.س.ن، ص32.

[2] – بالطي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر،2015، ص ص 15-16.

عقود تسمى بالعقود الإلكترونية وعن طريق التجارة الإلكترونية...، تسهيل وتنفيذ مهام سلطات الدولة عن طريق ما يسمى بالحكومة الإلكترونية...) أو سلبية (ارتكاب الجرائم المستحدثة وبالضبط جرائم الانترنت).

ونظرا لتفوق الجانب السلبي لهذه الانعكاسات على الجانب الإيجابي أصبح من الضروري وضع قوانين عقابية تحكم وتواجه إجرام الانترنت، والإشكال المطروح هنا هو هل تناول المشرع في هذه القوانين العقابية بتعريف جرائم الانترنت؟.[1]

الأصل كما هو متعارف عليه في القانون أن المشرع لا يعرّف الجريمة لأن ذلك ليس من اختصاصه بل من اختصاص الفقه والقضاء في بعض الأحيان، غير أنه وللضرورة الملحة يجد نفسه مضطرا إلى ذلك إما لتحديد أركان الجريمة العامة أ, الخاصة، أو تحديد السلوك الإجرامي المستحدث للجريمة،[2] والشأن ذاته بالنسبة لجرائم الانترنت، فالمشرع لم يعرفها تاركا ذلك للفقه والقضاء كما سبق ذكره، [3] إلا أن بعضهم من جهة أخرى اتجهوا إلى وضع تعاريف للجريمة الإلكترونية لكن تحت مسميات أخرى متقاربة أو مشتقة من الإجرام الإلكتروني، ولاسيما الجريمة المعلوماتية.

ولهذا نجد المادة الأولى من القانون المصري النموذجي الموحد في شأن مكافحة سواء استخدام تكنولوجيا المعلومات والاتصالات قد عرفت الجريمة الإلكترونية بأنها: "كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني، ويقصد في تطبيق أحكام هذا القانون بالكلمات والعبارات الآتية، المعاني المبينة قرين كل منها 1-الوسيط الإلكتروني...". وهكذا نجد أن المشرّع قد عرّف

[1] – هروال هبة نبيلة، جرائم الانترنت "دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2014/2013، ص ص 14-15."

[2] – عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، د.ط، دار الكتب القانونية، مصر، 2007، ص 18.

[3] – هروال هبة نبيلة، جرائم الانترنت "دراسة مقارنة"، المرجع السابق، ص15.

الجريمة المعلوماتية، وعرّف كذلك المفردات أو المصطلحات ذات العلاقة بالجريمة المعلوماتية من ذلك الوسيط الإلكتروني، والشفرة والبطاقة وتعطل النظام والبيانات وكلمة السر وغيرها.[1]

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف الجريمة الإلكترونية بأنها: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[2]

أما المشرع السعودي فقد عرّف الجريمة المعلوماتية بأنها: "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[3]

وعرّف القانون الإماراتي الجريمة الإلكترونية من خلال قانون مكافحة جرائم تقنية المعلومات في المادة الثانية منه على النحو التالي: "كل فعل عمدي بقصد اختراق موقع مؤمن نتج عن ذلك إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات حكومية كانت أو شخصية"[4]

وأيضا نجد المشرع الجزائري عرّف الجرائم الإلكترونية تحت مسمى الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المادة 02/ الفقرة01 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها كما يلي: "يقصد في مفهوم هذا القانون بـ: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة

[1] – عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، المرجع السابق، ص18.

[2] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، د.ط، 2011، ص 30.

[3] – المادة 08/01 من نظام مكافحة الجرائم المعلوماتية السعودي.

[4] – المادة 02 من قانون مكافحة جرائم تقنية المعلومات الإماراتي، 2006.

الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم اتصالات إلكترونية"[1]

تجدر الإشارة إلى أن المشرع الجزائري لم يعرف جرائم الانترنت في القانون 04-15 المؤرخ في 2004/11/10 المعدل والمتمم لقانون العقوبات، بل عدد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تعتبر جزء من ظاهرة إجرامية حديثة وخطيرة تسمى الجريمة المعلوماتية.

واكتفى بالعقاب عليها في الكتاب الثالث المعنون بالجنايات والجنح وعقوبتها في الفصل الثالث المعنون بالجنايات والجنح ضد الأموال في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلي للمعطيات في المواد 394 مكرر غلى غاية المادة 394 مكرر7.[2]

الفرع الثاني: التعريف الفقهي للجريمة الإلكترونية

يمكن القول أنه من الصعوبة الاتفاق على تعريف موحد جامع مانع لهذه الجريمة، وذلك راجع إلى التطور المتلاحق الذي تمر به، وتنوع واختلاف وسائل ارتكابها وظهور أشكال جديدة مستحدثة، إضافة إلى اختلاف الزاوية التي ينظر من خلالها من يحاول تعريفها.[3]

ولصعوبة إيجاد هذا التعريف أدى بالبعض إلى القول بأن هذه الجريمة مستعصية على التعريف ويستدلون على ذلك بالمحاولات العديدة التي بذلت لتعريفها والتي استخدمت العديد من الكلمات من أجل ذلك، لكن دون التوصل إلى تعريف موحد لها. [4] ويرى البعض الآخر، [5] أنه يجب وضع تعريف لهذه الظاهرة، بحيث يكون شاملا للعناصر الجوهرية التي تسهل تحديدها بغية

---

[1] – المادة 1/2 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت 2009، ج ر ج ج، العدد47.

[2] – هروال هبة نبيلة، جرائم الانترنت "دراسة مقارنة"، المرجع السابق، ص18.

[3] – محمود أحمد عبابنة، المرجع السابق، ص 14.

[4] – عفيفي كامل عفيفي ، جرائم الكمبيوتر (دراسة مقارنة)، د.ط، منشورات الحلبي الحقوقية، الإسكندرية، دت، ص31.

[5] – المرجع نفسه، ص 31. وينظر كذلك: زبيحة زيدان، الجريمة المعلوماتية ف التشريع الجزائري والدولي، د.ط، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص 43.

التعرف عليها فهناك من عرّفها بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[1]

وكذلك قد عرّفها جانب آخر من الفقه بأنها: "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية –مذنبة– ومحله معطيات الحاسب الآلي"[2]

وهناك من يعرّفها بأنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والانترنت في أعمال وأنشطة إجرامية عادة ما ترتكب بهدف تحقيق عوائد مالية ضخمة جراء أعمال غير شرعية يعاد ضخها في الاقتصاد الدولي عبر شبكة الانترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الانترنت أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة.[3]

وهناك من عرّفها بأنها: "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية"، ويوسع البعض في مفهوم هذه الجريمة حيث يعرفها الخبير الأمريكي Parker بأنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل"[4]

ومن التعريفات المضافة للجرائم المعلوماتية، ما جاء به الفقيه Marwe

حيث يرى أن الجريمة المعلوماتية تتمثل في: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[5]، وهناك من عرّفها بأنها: "كل نشاط إجرامي يؤدي فيه نظام الكمبيوتر دورا

---

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 18.

[2] – المرجع نفسه، ص 22.

[3] – عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (دراسة مقارنة)، د.ط، منشورات الحلبي الحقوقية، د.س.ن، ص 15.

[4] – نقلا عن: عفيفي كامل، المرجع السابق، ص 32.

[5] – نقلا عن: محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، ط3، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 08.

لإتمامه على أن يكون هذا الدور مؤثر في ارتكاب الجريمة، ولا يختلف الأمر سواء كان الكمبيوتر أداة لإتمام الفعل الإجرامي أم كان محلا لها"[1]

المطلب الثاني: التطور التاريخي للجرائم الإلكترونية وإحصائيات حولها

لقد أحدث التحول الحضاري والتقدم الذي اجتاح عالمنا في العصر الحديث تغيرا ملموسا في نوعية الجرائم والمجرمين، فبعد أن كانت الغلبة للجرائم القائمة على العنف أو القسوة أصبحت الغلبة للجرائم القائمة على المقدرة الذهنية والذكاء، بحيث استغل المجرمون هذا التقدم في تطوير المخترعات العلمية الحديثة لخدمة أهدافهم الإجرامية.[2]

حيث تعتبر الانترنت إحدى وأهم نتائج هذا التقدم العلمي إذ حوّل العالم بأكمله إلى قرية صغيرة يتبادل الناس أخبارهم فيها انطلاقا من أماكنهم دون الحاجة إلى مبارحتها، وفي المقابل أصبح يهدد المصالح نتيجة سوء استغلالها.

وهذا ما تبينه الإحصائيات والدراسات التي أجريت حولها. [3] وبدورنا في هذا المطلب سنحاول التطرق إلى التطور التاريخي لهاته الجرائم (**الفرع الأول**)، وإرفاقه بإحصائيات حول هاته الأخيرة (**الفرع الثاني**).

الفرع الأول: التطور التاريخي للجرائم الإلكترونية

ظهرت جرائم الانترنت لأول مرة في نهاية الثمانينات من خلال إطلاق فايروس عرف باسم (دودة مورس) عبر الانترنت في تشرين الثاني عام 1988 حيث تمكن طالب يبلغ من العمر 23 سنة يدعى " Rober Morris" من إطلاق ونشر هذا الفايروس الإلكتروني (Morris Worms) أدى إلى إصابة 06 آلاف جهاز يرتبط معها حوالي 60.000 نظام عبر الانترنت

[1] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، د.ط، دار الفكر الجامعي، الإسكندرية، 2019، ص ص 74-75.

[2] – هراول هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، المرجع السابق، ص28.

[3] – ينظر إلى الملاحق.

من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار، وقد حكم على موريس بالسجن لمدة 03 سنوات و10 آلاف دولار غرامة.[1]

وقد مرت الجرائم الإلكترونية بثلاث مراحل في تطورها التاريخي تبعا لتطور التقنية واستخداماتها، بداية من شيوع استخدام الحواسيب في الستينات والسبعينات، اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر. وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة. ومع تزايد استخدام الحواسيب الشخصية في السبعينيات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من القضايا الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة، حيث طغى على السطح في الثمانينات مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج، حيث شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام، حيث شهدت التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات.[2]

[1] – أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، د.ط، دار المطبوعات الجامعية، الإسكندرية، 2008، ص 99.

[2] – علاء رضوان، الجريمة المعلوماتية من النشأة في الستينات إلى "القرصنة" في القرن 21، 16 نوفمبر 2018، بحث منشور على الانترنت، نقلا عن الموقع الإلكتروني: www.soutalomma.com، اطلع عليه بتاريخ: 22أفريل 2021 على الساعة 14:00.

الفرع الثاني: الإحصائيات التي أجريت حول الجرائم الإلكترونية

يؤدي الاستخدام المتزايد للتقنيات الرقمية في قطاع الأعمال دورا حيويا في نمو الأعمال التجارية، غير أن هذا الاستخدام له مخاطر أيضا تستهدف الجرائم الإلكترونية الضحايا من الأفراد وحتى الشركات الكبيرة، وذلك عبر طرق مختلفة مثل التصيد الاحتيالي والتثبيت غير المشروع للبرامج الضارة، الأمر الذي يؤدي إلى خسارة الدخل، والإضرار بالسمعة وتكبد خسائر مالية وتشفير البيانات بالفيروسات التي لا يمكن معالجتها إلا عن طريق دفع مبالغ مالية لقراصنة الانترنت، وعلى الرغم من أن غالبية المجرمين يمتلكون قدرات تقنية بسيطة جدا، إلا أن الهجمات الرقمية تشهد تزايدا في استخدام الأدوات المتطورة المتاحة في السوق الإجرامي الإفتراضي على الانترنت، مع تطوير بعض الجماعات الإجرامية لأنشطتها، فإن الجرائم الإلكترونية تتطور أيضا وتنمو بسرعة.[1]

بالرغم من أن هذه الأخيرة حديثة ومتميزة، إلا أنها تمكنت في وقت قياسي قصير جدا من غزو واجتياح العالم بأكمله، وهذا ما تثبته الإحصائيات التي أجريت حولها.[2]

-الإحصائيات:

تتنوع العمليات الإلكترونية بتنوع المجالات التي تستخدم شبكة الأنترنت، فنجد أمثلة لها في الأعمال المصرفية، الإدارة الإلكترونية، التجارة الإلكترونية، لذلك فإن بتصور تنوع الجرائم التي تقع على هذه العمليات الإلكترونية المستخدمة في ارتكابها، حيث تقتضي عمليات البحث الجنائي والتحقيق في المعلوماتية الاستعانة بخبرات عديدة ومتنوعة، ومن أهم هؤلاء الخبراء في مجال مساعدة المحققين على ضبط الجريمة في الجزائر هو المعهد الوطني للأدلة الجنائية وعلم الإجرام "بالجزائر العاصمة" حيث عالجت دائرة الإلكترونيك والإعلام الآلي التابعة للمعهد ببوشاوي 325

[1] – ينظر الموقع الإلكتروني: www.business.algeria.hsbc.com

[2] – هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، المرجع السابق، ص 31.

طلب تحليل وخبرة سنة 2014، في حين تم معالجة 268 طلب سنة 2013 أي بزيادة قدرها 57 بنسبة تطور بلغت 21.26% وقد جاءت هذه القضايا كالآتي:[1]

- 11قضية تتعلق بانتهاك الآداب.
- 04قضايا تتعلق بتكوين جمعية أشرار.
- 03 قضايا تتعلق بالاعتداء على الأمن والنظام المعلوماتي العمومي.
- 04 قضايا تتعلق بالتشهير.
- 04قضايا تتعلق بالتهريب.
- 03قضايا تتعلق بالقرصنة المعلوماتية.
- 34قضية تتعلق بمعلومات قضائية.
- 02 قضيتان تتعلقان بتبييض الأموال.
- 01 قضية تتعلق بالرشوة.

حيث تقوم دائرة الإعلام والإلكترونيك بمهمة معالجة تحليل وتقديم للعدالة كل دليل رقمي وتماثلي كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

كما سجل مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني ببئر مراد رايس في معالجة 102 قضية سنة 2014 مقابل 46 قضية سنة 2013 أي بزيادة قدرها 56 قضية بنسبة تطور 21% حيث بلغت نسبة حل القضايا 95% ومن بينها:[2]

-13 قضية تتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما تمكنت من جهة أخرى الفرق المتخصصة في مكافحة الجرائم للأمن الوطني سنة 2014 بناء على شكاوى من معالجة

[1] – إحصائيات من المعهد الوطني للأدلة الجنائية وعلم الإجرام.

[2] - بيان صحفي لإدارة الإعلام والعلاقات العامة بالمديرية العامة للأمن الوطني بتاريخ 18جانفي 2015.

211 قضية تتعلق بجرائم الأنترنت قدم من خلالها الدليل المادي عن تورط 205 مشتبه فيه منهم 28 امرأة، ومن بين هذه القضايا قضايا تتعلق بالجريمة الإلكترونية.

-75 قضية ماسة بأنظمة المعالجة الآلية للمعطيات.

-03 قضايا متعلقة بالنصب والاحتيال عن طريق الأنترنت.

-06 قضايا متعلقة بالإهانة والسب عن طريق الانترنت.

-02 قضايا متعلقة باستعمال الغير للبطاقات الإلكترونية.

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية

إن الارتباط الحاصل بين الجريمة الإلكترونية وتقنية المعلومات، باعتبار هذا النوع من الجرائم إفرازا لتقنية المعلومات، جعلها تكتسب طابعا قانونيا خاصا ميزها عن غيرها من الجرائم التقليدية، ونتيجة للطبيعة المستحدثة للأفعال الإجرامية التي ترتكب من خلالها أصبحت تكتسب خصوصية غير عادية إذا ما قارنها بالجرائم التقليدية.[1]

وهذا ما سنحاول ترجمته من خلال إبراز أهم الخصائص التي تمتاز بها (**المطلب الأول**)، وكيف صنفها فقهاء القانون الجنائي وقانون العقوبات (**المطلب الثاني**).

المطلب الأول: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بطبيعة خاصة تميزها عن الجريمة التقليدية، ولذا اتصفت بعدة سمات وحقائق سواء تعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي، أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي.[2]

---

[1] – أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مج 19، عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم، مجلة جامعة الأزهر، غزة، 2017، ص 07.

[2] – يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ضبي، 2002، ص 07.

وسوف نبين هذه الخصائص التي ميزت الجريمة المرتكبة عبر الانترنت عن غيرها، بداية بأنها جريمة عابرة للحدود الدولية وصعبة الاكتشاف والإثبات (**الفرع الأول**)، وبأنها جريمة خفية ومستترة (**الفرع الثاني**)، وخصوصية الجاني المرتكب لهذه الجريمة (**الفرع الثالث**)، على النحو التالي:

الفرع الأول: جرائم عابرة للحدود الدولية وصعبة الاكتشاف والإثبات

من أهم الخصائص التي تتميز بها الجريمة الإلكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بتقنية المعلومات والانترنت (**أولا**)، وأنها صعبة الاكتشاف والإثبات (**ثانيا**).

أولا: الجرائم الإلكترونية عابرة للحدود الدولية

تتسم الجريمة الإلكترونية غالبا بالطابع الدولي، ذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط 'online'، يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة الإلكترونية لا تعترف بالحدود بين الدول والقارات، لذلك فهي جريمة عابرة للقارات، فهي تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل: جرائم التعدي على قواعد البيانات، وتزوير وإتلاف المستندات الإلكترونية، والاحتيال المعلوماتي، وسرقة بطاقات الائتمان، والقرصنة، وغسيل الأموال.[1]

وتثير خاصية عالمية الحدود للجريمة الإلكترونية عدة آثار قانونية أهمها القانون الواجب التطبيق عليها، والقضاء المختص بها، فهل هو قانون الدولة التي وقع فيها النشاط الإجرامي، أم الدولة التي يقيم فيها الجاني، أو الدولة التي أضرّ بمصالحها هذا التلاعب، لذا بات من الضروري

[1] – خالد ممدوح إبراهيم، المرجع السابق، ص 77.

إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.[1]

وتجدر الإشارة أن المشرع الجزائري قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات،[2] والذي استحدث بموجبه أحكام خاصة بالجرائم الماسة بالأنظمة المعلوماتية من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، إضافة إلى القانون رقم 09-04،[3] السابق الذكر المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛ إذ تضمن بعض القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال هذه الجرائم كما أنشأت هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته، وسنّ أحكام خاصة بالتعاون والمساعدة القضائية الدولية.

ثانيا: الجرائم الإلكترونية صعبة الاكتشاف والإثبات

من أهم خصائص الجريمة الإلكترونية أنها صعبة الاكتشاف والإثبات لأسباب ترجع إلى الجاني أو إلى المجني عليه، وإلى وسيلة تنفيذها، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الانترنت، أضف إلى أن الجاني (المجرم المعلوماتي) كما اسلفنا الذكر مجرم محترف ذكي مثقف لا يترك أثارا جانبية خارجية للجريمة مما يصعب إثباتها، كما أن المجني عليهم وهم غالبا

[1] – نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، 24-25 مارس 2017، طرابلس، ص 07.

[2] – الأمر رقم 66-156 المتضمن قانون العقوبات المؤرخ في 18 صفر 1326هـ الموافق لـ 06 يونيو 1966 المعدل بالقانون رقم 04-15 المتضمن تعديل قانون العقوبات المؤرخ في 10 نوفمبر 2004، ج رج ج،

[3] – القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد علّق المشرع الجزائري على التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على شرط احترام الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل، ومن ثمة نستخلص أنه لا غنى عن الاتفاقيات الدولية في مجال مكافحة هذه الجريمة.

مؤسسات عامة أو خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية.[1]

فإذا كانت الجريمة التقليدية تمتاز بكونها تترك خلفها آثارا خاصة مرئية كالجثث أو الدماء المسفوكة، فإن ذلك غير متوافر في إطار الجريمة الإلكترونية كونها ترتكز على تغيير أو تعديل أو مسح البيانات كليا أو جزئيا، بالدخول إلى السجلات المخزنة في ذاكرة الحاسب الآلي، الأمر الذي يجعل إمكانية اكتشافها في غاية الصعوبة، وبالتالي الصعوبة في توقيع الجزاء على مرتكبها.[2]

وهذا النوع من الجرائم لا يترك أثرا خارجيا ومرئيا نتيجة ارتكابها في الخفاء، وبشكل لا يلحظه المجني عليه، أو لا يدري حتى بوقوعها، أضف إلى الإمعان في حجم السلوك المكون لها وإخفائها بحكم الخبرة والمعرفة التي يمتاز بها مرتكبي هذه الجرائم. [3] الأمر الذي يجعل عملية إثباتها بالطرق التقليدية في الإثبات أمرا مستحيلا.

الفرع الثاني: خفاء الجريمة وسرعة التطور في ارتكابها

تتسم الجرائم الناشئة عنها استخدام الانترنت بأنها خفية ومستترة في أغلبها؛ لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة؛ لأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرعة المكالمات وغيرها من الجرائم.[4]

وجرائم الانترنت في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها وإمعان الجاني في حجم السلوك المكون لها، وإخفاءه بطريق التلاعب غير المرئي في النبضات أو

[1] – غنية بالطي، المرجع السابق، ص ص 28-32.

[2] – شمس الدين ابراهيم أحمد، وسائل الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوادني والمصري "دراسة مقارنة"، ط1، دار النهضة العربية، القاهرة، 2005، ص 104.

[3] – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسيوط، 1994، ص 16.

[4] – محمد عبيد الكعبي، المرجع السابق، ص 32.

الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمرا ليس في الكثير من الأحوال إثباته بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها، يستفيد المجرمون في مختلف المواقع من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم، ويظهر لنا ذلك جليا في مختلف المواقع الإلكترونية ومنتديات القراصنة (الهاكرز) التي تضمن لهم الاتصال فيما بينهم من أجل تبادل المعارف والخبرات في مجال القرصنة، وذلك من أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن.[1]

تجدر الإشارة في هذا الصدد أن الجريمة المرتكبة عبر الانترنت أسرع تطورا من التشريعات، وذلك راجع إلى التطور التكنولوجي الهائل والمتسارع، والذي تجسده شبكة الانترنت بالإضافة إلى مختلف المؤتمرات التي يعقدها القراصنة، والتي تسمح لهم بابتكار وسائل وطرق في غاية التعقيد لم تعرفها التشريعات من قبل، وذلك من أجل ارتكابهم لجرائمهم.[2]

الفرع الثالث: خاصية الجاني في الجريمة الإلكترونية

مرتكب هذه الجرائم غالبا ما يكون شخصا يمتاز بالذكاء والدهاء، وذو مهارة تقنية عالية ودراية بأنظمة الحاسوب، وهذا عكس الحال في الجريمة التقليدية التي غالبا ما يكون الجاني فيها شخصا عاديا بسيطا، ويكون مرتكب هذه الجرائم في أغلب الحالات متكيفا اجتماعيا وقادرا ماديا، هدفه من ارتكاب هذه الجرائم الحصول على الربح أو النفع المادي، وهو عكس الواقع في حالة الجرائم التقليدية التي يكون فيها الجاني شخصا غير متكيف اجتماعيا، وباعثه في ارتكاب الجرم النفع المادي السريع.[3]

[1] – عبد المومن بن الصغير، المرجع السابق، ص ص 73-74.

[2] – المرجع نفسه، ص 74.

[3] – نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص ص 77-78.

ولا يقتصر ارتكابه لهذه الجرائم لحسابه الخاص، بل قد يكون ذلك لحساب أحد الأشخاص المعنوية، كشركة عامة أو خاصة تعمل في ميدان المعلوماتية، أو حتى في مجال آخر.[1]

يوجد عدة أنواع من المجرمين المعلوماتيين، فهناك:

01-طائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون إحداث أي ضرر ويسمونهم "Pranskers".

02- طائفة الأشخاص الذين يستهدفون الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بهدف الفضول أو اكتساب الخبرة، أو لمجرد القدرة على اختراق هذه الأنظمة ويسمون "Hackers".

03-طائفة الأشخاص الذين يستهدفون إلحاق خسائر بالمجني عليهم، دون أن يكون بغرض الحصول على مكاسب مالية ضمن هذه الأهداف، ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية وموزيعيها، ويسمون "Malicieuse Hackers".

04- طائفة الأشخاص الذين يهدفون إلى إلحاق الأذى بالمجني عليهم، ويكون الباعث إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية ويسمون بـ " Personnel Problème Solvers".

05- طائفة الأشخاص الذين يهدفون إلى تحقيق ربح مادي بطريق غير مشروع ويسمون بـ "Green criminels".[2]

[1] - محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، ط1، الهيئة المصرية للكتاب، القاهرة، 2003، ص 56.

[2] - عبد العال الديبي، الجريمة المعلوماتية "تعريفها-أسبابها وخصائصها":
www.acconline.com/article.detail.aspr?id;7509 ، نقلا عن: نميدلي رحيمة، المرجع السابق، ص ص 07-08.

المطلب الثاني: أنواع الجريمة الإلكترونية

اختلف الفقه والقانون في تصنيف الجرائم الإلكترونية باختلاف الزاوية التي ينظر منها إلى الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي.

وعليه سنقوم في هذا المطلب بتقسيم الجرائم الإلكترونية وفقا لما أقره فقهاء القانون الجنائي (**الفرع الأول**)، ثم تقسيمها وفقا لقانون العقوبات الجزائري (**الفرع الثاني**).

الفرع الأول: التقسيم الفقهي للجرائم الإلكترونية

اختلف الفقه الجنائي في تقسيم الجريمة الإلكترونية، حيث قد يكون النظام المعلوماتي هو نفسه موضوع أو محل هذه الجريمة (**أولا**)، وقد يكون من ناحية أخرى أداة أو وسيلة ارتكاب الجريمة (**ثانيا**).

أولا: الجرائم الواقعة بواسطة النظام المعلوماتي

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، ويهدف الجاني من ورائها إلى تحقيق ربح مادي بطريقة غير مشروعة، يستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة.[1] وتنقسم هذه الجرائم بدورها إلى:

01-الجرائم الإلكترونية جرائم واقعة على الأشخاص

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي، إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص، وعليه ظهرت عدة أنواع خاصة من الجرائم الإلكترونية الواقعة على الأشخاص، كجريمة التهديد والمضايقة والملاحقة،

[1] – سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، 2010، ص 33.

خاصة عن طريق البريد الإلكتروني بإرسال رسالة خاصة للترويع والتهديد، أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنت: كالفايسبوك، والفايبر، والوتساب.[1]

أيضا جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم عن طريق وسائل التواصل الاجتماعي، أو الكتابة أو عن طريق المطبوعات أو المبادلات الإلكترونية، صفحات الويب، غرف المحادثة. وقد يتم السب أو القذف عبر البريد الإلكتروني للمقذوف أو المسبوب فيتم إرسال رسالة إلى الشخص وحده، وقد ترسل إلى عدة أشخاص فيعظم بذلك الجرم، ويشتد الأذى على من وقع عليه القذف أو السب لانتشاره بين الناس.[2]

كما تعتبر من أهم الجرائم الإلكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين أو الأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنت، بأشكال متعددة انطلاقا من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت.[3]

يضاف إلى الجرائم الإلكترونية الواقعة على الأشخاص جرائم انتحال الشخصية والتغرير والاستدراج وغيرها من الجرائم.

02-الجرائم الإلكترونية جرائم واقعة على الأموال

صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل: البيع والشراء مما انجرّ عليه تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر

[1] – يوسف الصغير، المرجع السابق، ص 50.

[2] – عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات والانترنت)، د.ط، دار الوراق للنشر والتوزيع، بيروت، 2006، ص 213.

[3] – كريستا سكولمان، جرائم الانترنت "طبيعتها وخصائصها"، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و 20 يونيو 2006، ص 102. نقلا عن: نميدلي رحيمة، المرجع السابق، ص09.

الانترنت انتهز بعض المجرمين من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقة، والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة.[1]

فلم تقتصر أساليب إساءة استخدام الثروة المعلوماتية على الاعتداء على الأشخاص فقط، بل تعدتها لتطال الذمة المالية للغير، لاسيما فيما يخص إساءة استخدام تقنية الانترنت التي أتاحت -نظرا لما تتمتع به من خصائص فريدة من نوعها- الفرصة لمجرمي المعلوماتية وهيأت لهم المناخ المناسب في تسهيل ارتكاب شتى أنواع الجرائم المالية وذلك بكل ارتياح وطمأنينة بجلوس الشخص وراء حاسوبه المرتبط بالانترنت وبارتكاب ما شاء له من الجرائم التي كانت في السابق تصعب عليه، وذلك بمجرد النقر بأقل مجهود ممكن ومن دون خسائر مالية على لوحة مفاتيح الحاسوب المربوط بالانترنت، وعلى هذا ظهرت صور مستحدثة من هذا النوع من الجرائم محلها الأموال ووسيلة ارتكابها الانترنت.[2]

وجرائم الاعتداء على الأموال عبر الانترنت هي:

-جرائم السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني غير المشروع للأموال.

- جرائم غسيل الأموال والمخدرات.

- جرائم الاعتداء على الملكية الفكرية.

- جرائم السرقة والنصب.

- جرائم الاعتداء على التجارة الإلكترونية.

[1] - صغير يوسف، المرجع السابق، ص44.

[2] - هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، المرجع السابق، ص176.

03-الجرائم الإلكترونية جرائم واقعة على أمن الدولة

استغلت الكثير من الجماعات المتطرفة الطبيعة الإتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا منحنى آخر في استعمال الانترنت، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الأخطر من ذلك أتاح الانترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة فيما يتعلق بالدول التي يكون بينها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت، حيث تعطي الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.[1]

ومن أبرز وأشهر هذه الجرائم التي تقع على أمن الدولة عبر الانترنت هي جريمتي الإرهاب والتجسس.

ثانيا: الجرائم لواقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي، هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي، أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي،[2] وتنقسم هذه الجرائم بدورها إلى:

01-الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطونات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو

[1] – صغير يوسف، المرجع السابق، ص 54.

[2] – سوير سفيان، المرجع السابق، ص 39.

العبث بمفاتيح التشغيل، مما يترتب عنها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى إلى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية وقدرت الخسائر بـ 05 ملايين فرنك فرنسي.[1]

02-الجرائم الواقعة على البرامج الإلكترونية

وتنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، حيث يقوم الجاني في هذه الصورة بتحديد البرامج أولا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية، ومن أمثلتها قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات، وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم zzwick. وكذلك تضم هذه الجرائم الجرائم الواقعة على برامج التشغيل وهي تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام، وتقوم الجريمة في هذه الصورة عن طريق تزويد البرامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي، ومثالها: تصميم برنامج وهمي من خلاله تنفذ الجريمة.[2]

03-الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

عرّف القانون الفرنسي الخاص بالاتصالات السمعية والبصرية الصادر في 29 جويلية 1982 المعلومة بأنها: " Sons d'images de documents, de données ou de message de toute nature"، كما عرّفها الفقيه الفرنسي " Catala" على أنها: "رسالة معبر عنها في الشكل بجعلها قابلة للنقل أو الإبلاغ للغير"[3]

[1] - Lucas (A) : droit de Informatique, paris, PUF, 1987, p 519-521.

[2] - سوير سفيان، المرجع السابق، ص ص 41-42.

[3] - غنية بالطي، المرجع السابق، ص ص 58-59.

وتعد المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة أو عن طريق إتلافها أو استبدالها أو محوها، وهذا ما يسمى بجريمة الغش أو التزوير المعلوماتي ومثالها ما قام به شخص يدعى Vladimir Loriblitt بالكيان الصهيوني باستخدام طريقة تدعى bluff، وهو موظف بوزارة المالية، حيث قام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها.[1]

الفرع الثاني: التقسيم القانوني للجرائم الإلكترونية

تعددت الجرائم الإلكترونية بتعدد وسائلها وأنماطها في مختلف التشريعات. ففي الجزائر وضع المشرع الجزائري قسم في قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.[2]

حيث نصت عليها المواد: 394مكرر، 394مكرر1،394مكرر2، 394مكرر3، 394مكرر4، 394مكرر5، 394مكرر6، 394مكرر7.

باستقرائنا لهذه المواد يتضح أن المشرع الجزائري قد قسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أو الجرائم الإلكترونية إلى:

01-جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير، وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات طبقا للمادة 394 مكرر من قانون العقوبات، يعاقب الجاني بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000دج إلى 200.000دج وتضاعف العقوبة إذا

[1] - محمد سامي الشوا، المرجع السابق، ص 34.

[2] - أنظر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ج ر ج ج، العدد44.

ترتب على الفعل الإجرامي حذف أو تغيير المعطيات، كما يعاقب الجاني بالحبس من 06 أشهر إلى سنتين وغرامة من 50.000دج إلى 300.000دج في حالة تخريب النظام المعلوماتي.[1]

02-الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذلك التصميم أو البحث أو التجميع أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق نظام معلوماتي، وهذا ما نصت عليه المادة 394 مكرر2 وعقوبتها الحبس من شهرين إلى 03 سنوات وبغرامة من 1000.000دج إلى 10.000.000دح.[2]

03-الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب وعقوبتها تضاعف العقوبات المنصوص عليها في هذا القسم من قانون العقوبات لخطورتها وهذا ما نصت عليه المادة 394 مكرر3.

04-الجرائم الإلكترونية التي يرتكبها الشخص المعنوي، وعقوبتها تعادل خمس مرات الجرائم المرتكبة من طرف الشخص الطبيعي طبقا للمادة 394 مكرر4 من قانون العقوبات الجزائري.[3]

كما عاقب المشرع الجزائري على الشروع في الجريمة الإلكترونية كما هو الحال في الجريمة العادية بنفس العقوبة للجريمة الكاملة مع تكييفها جنحة وفقا لقانون العقوبات الجزائري. [4] ونص أيضا على الاشتراك في الجريمة الإلكترونية بنفس العقوبة المقررة للشريك في الجريمة العادية طبقا لقانون العقوبات الجزائري. ونص أيضا على جريمة الاتفاق الجنائي الإلكتروني بغرض الإعداد لجريمة

[1] – المادة 394 مكرر من القانون 04-15.

[2] – المادة 394 مكرر2 من القانون 04-15.

[3] – المواد 394 مكرر3 و 394مكرر 4 من القانون 04-15.

[4] – المادة 394 مكرر7 من القانون 04-15.

أو أكثر من الجرائم المنصوص عليها في هذا القسم يعاقب بالعقوبات المقررة للجريمة ذاتها طبقا للمادة 394 مكرر 5 من القانون 04-15 المعدل والمتمم لقانون العقوبات.[1]

الفصل الثاني: أركان الجريمة الإلكترونية

لا تقوم الجريمة إلا بتوافر الركنين المادي والمعنوي ، فلا بد أن تتبلور ماديا وتتخذ شكلا معينا وهو الركن المادي، أو المظهر الخارجي لنشاط الجاني، إلا أنه لا يكفي وحده لإسناد المسؤولية إلى شخص معين بل يجب أن تتوفر لديه النية الجرمية التي تشكل الركن المعنوي للجريمة، الذي قد يأخذ أيضا صورة الخطأ- وبالإضافة إلى هذين الركنين لابد من نص قانوني يجرم الفعل إذ لا جريمة بغير قانون[2]، وقد انقسم الفقه الجنائي إلى مذاهب شتى في تحديد الجريمة فهناك من يرى [3] أن لها ركنين، هما الركن المادي والمعنوي فقط، أما الركن الشرعي فيعتبرونه شرطا أساسيا للتجريم وهو من يخلق الجريمة، فليس من الصواب أن يقال أن الخالق عنصر فيما يخلقه[4].

وعلى الخلاف من ذلك، هناك من يرى أن القانون ركن من أركان الجريمة، وهو ركن ضروري لها، إذ لا جريمة بدون نص قانوني[5].

تتخذ الجريمة الإلكترونية من الفضاء الافتراضي مسرحا لها، يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع والمجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف

---

[1] - المادة 394 مكرر5 من القانون 04-15.

[2] -أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباع والنشر والتوزيع، ط17، الجزائر، 2018، ص 63.

[3] -سليمان عبد المنعم، القسم العام من قانون العقوبات، دار الجامعة الجديدة، د.ط، الإسكندرية، 2002، ص 135-136؛ وعلي عبد القادر القهوجي، شرح قانون العقوبات- القسم العام، الكتاب الأول، دار المطبوعات الجامعية، القاهرة، 1997، ص 41-42.

[4] -محمودمحمود مصطفى، شرح قانون العقوبات-القسم العام، دار النهضة العربية، د.ط، القاهرة، مصر،1983، ص38.

[5] -أحسن بوسقيعة، المرجع السابق، ص 64، فتوح عبد الله الشاذلي، قانون العقوبات- القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية، 1998، ص 66.

نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة [1]، وبالتالي نعمد إلى تبيان النموذج القانوني (الشرعي) والمادي للجريمة الإلكترونية (**المبحث الأول**)، ثم الركن المعنوي فيها (**المبحث الثاني**).

المبحث الأول: النموذج القانوني والمادي للجريمة الإلكترونية

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان، هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل غير المشروع وإعطاءه صفة الجريمة بتحديد الركن المادي فيه، الذي يتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غاية ما ويحدد له القانون العقاب اللازم[2].

فلا تختلف الجريمة الإلكترونية عن أي جريمة أخرى، إذ أنها تتطلب ضرورة تواجد الشرط المبدئي في كل جريمة أي النص الشرعي المجرم أو الصفة غير المشروعة [3] (**المطلب الأول**)، بالإضافة إلى الركن المادي والمتمثل في السلوكيات المادية المجرمة (**المطلب الثاني**).

المطلب الأول: النموذج القانوني للجريمة الإلكترونية (الركن الشرعي)

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل[4]، ويتجسد هذا النص من خلال مبدأ شهير هو مبدأ 'لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون'؛ أي ما يعرف بمبدأ شرعية الجرائم والعقوبات.

---

[1]-صغير يوسف، المرجع السابق، ص 59.

[2]-أحسن بوسقيعة، المرجع السابق، ص 64.

[3]-علي عبد القادر القهوجي، المرجع السابق، ص 43.

[4]- عبد المحسن بدوي محمد أحمد، استراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيري، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الخرطوم، 2005، ص 5.

فمبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني، ومتى انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هذه الجرائم[1]. غير أن السؤال المطروح هو ما محل الجريمة الإلكترونية مبدأ شرعية الجرائم العقوبات؟

تناولت التشريعات الجرائم التقليدية التي تقع على الأموال الأشخاص وغيرها بالتجريم، إلا أنه ومع تزايد ظاهرة قرصنة برامج الحاسوب، وتعدد العمليات الإلكترونية غير المشروعة ووقوف المشرع عاجزا أمام هذه الظاهرة الخطيرة، أدى به إلى التدخل ليتناول ما يستجد من هذا الشكل الجديد للإجرام تطبيقا لمبدأ الشرعية[2]، وفيما يلي نماذج عن بعض التشريعات على المستوى الدولي (**الفرع الأول**) وعلى المستوى الوطني (**الفرع الثاني**).

الفرع الأول: على المستوى الدولي

تعتبر الجريمة الواقعة من نتاج التطور التكنولوجي أنها من المستحدثات التي عجزت مواد القوانين العقابية التقليدية مواجهتها، لذلك سعت معظم دول العالم ولاسيما تلك المتقدمة قانونيا إلى سن التشريعات والقوانين لمواجهة هذه الجرائم[3].

تعتبر الولايات المتحدة الأمريكية من بين الدول السباقة التي جسدت تشريع مستقل بشأن جرائم الكمبيوتر بصفة عامة وجرائم الإنترنت بصفة خاصة. كما تتميز الولايات المتحدة

[1]-يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورشة عمل في تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، المنعقدة بمسقط، سلطنة عمان، 2-4 أفريل 2006، ص 43، 55.

[2]-بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2014/2013، ص 30-31.

[3]-محمد عبيد الكعبي، المرجع السابق، ص 58.

الأمريكية بوجود أكبر قدر من التشريعيات التي تغطي مسائل جرائم الكمبيوتر والانترنت والاتصالات[1].

وضعت الولايات المتحدة الأمريكية قانونا خاصا بحماية الحاسوب وشبكات الحوسبة وذلك عام 1976، وفي عام 1985 حدد معهد العدالة القومي فيها خمسة أنواع رئيسية لهذا النوع من الجرائم وهي:

1-جرائم الحاسوب الداخلية.

2-جرائم الاستخدام غير المشروع عن بعد، شبكة المعلومات المحوسبة.

3-جرائم التلاعب بالحاسوب، أي التلاعب غير المخول وغير المشروع في الشبكات المحوسبة.

4-دعم التلاعبات الإجرامية للنظم والشبكات المحوسبة، وإسنادها من قبل الآخرين.

5-سرقة البرامج الجاهزة والمكونات المادية[2].

قام كذلك المشرع الفرنسي بسن تشر يع خاص فيما يخص الإجرام المعلوماتي وذلك في أغسطس 1986، حيث تقدم النائب 'جاك جودفران' باقتراح قانون تم اعتماده من البرلمان الفرنسي وصدر في 05 يناير 1988 برقم 19 تحت عنوان "الجرائم في المواد المعلوماتية "، وتم إدماجه في الفصل الثاني من قانون العقوبات وخصصت له المواد من 2/432 إلى 9/462[3].

والجدير بالذكر أن الفصل المخصص لهذه الجرائم ألحق بالباب المخصص بالجنايات والجنح ضد الأشخاص؛ أي بعد الفصل الثاني من الجرائم المخصصة بالجنايات والجنح ضد الملكية، وقد ركزت اللجنة التشريعية على الهدف الذي توخاه اقتراح 'جودفران' حماية النظام المعلومات ضد أي

[1]-يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، المرجع السابق، ص3، 55.

[2]-عبد المومن بن صغير، المرجع السابق، ص85.

[3]-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، ط2، الإسكندرية، 2006، ص 126.

اعتداء خارجي، فقررت أن الهدف من النصوص الجديدة تجريم وردع الدخول غير المشروع على برامج المعلوماتية[1].

أيضا هناك الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية 'بودابست' 22 نوفمبر 2001، تناولت كل ما يتعلق بالجريمة الإلكترونية، سواء ما يقع ضد الشبكات أو الجرائم التقليدية التي تستخدم في ارتكابها شبكات المعلوماتية، فقد جاء في الفصل الأول منها تعريف لبعض المصطلحات المتعلقة بالحاسوب والانترنت، أما الفصل الثاني فتناول الإجراءات الواجب اتخاذها على المستوى المحلي، وقد وردت بعض من صور الجريمة الإلكترونية وذلك من خلال المواد من 02 إلى 10، والفصل الثالث احتوى المواد من 23 إلى 31 التي أوجبت التعاون الدولي لمكافحة الجريمة والقبض على المجرمين، وقد أوردت بعض صور هذا التعاون[2].

أما على المستوى الجهود العربية فقد اعتمد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد قانونا نموذجيا بموجب القرار 229 لسنة 1996 حيث تناول الجريمة الإلكترونية في الفصل التاسع منه بعنوان "الاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية "، حيث جاء في المادة 461 من هذا الفصل صور للجريمة الإلكترونية وعقوبة التحريض على هذه الجريمة في الفقرة الأولى والثانية، والفقرات الثالثة والرابعة من نفس المادة والمواد 462 و463، أما المادة 465 فقد عاقبت على الاشتراك في الأفعال التي تشكل الجريمة الإلكترونية بذات عقوبة الفاعل الأصلي[3].

---

[1]- أحمد خليفة الملط، المرجع السابق، ص 126.

[2]-خالد عياد الحلبي، المرجع السابق، ص 256.نون الجزائي العربي الموحد، جامعة الدول العربية، الجزء ال ثني، رقم 229، د12، بتاريخ 19 نوفمبر 1996.

[3]-مذكرة توضيحية للقانون الجزائي العربي الموحد، جامعة الدول العربية، الجزء الثاني، رقم 229، د12، بتاريخ 19 نوفمبر 1996.

غير أن الملاحظ على المستوى الدولي وجود فجوة رقمية رهيبة بين الدول، فبالنسبة للدول التي تعاني من التخلف في المجال المعلوماتي، لم تسن بعد قوانين تجرم بها الأفعال غير المشروعة عبر الانترنت، واكتفاءها بتطبيق قواعد قانون العقوبات الخاصة بها، غير أن هذه القوانين أثبتت قصورها في هذا المجال، الأمر الذي يستوجب منها التوسع في تفسير هذه النصوص لتطبيقها على الجرائم الإلكترونية[1].

الفرع الثاني: على المستوى الوطني

تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، ورغبة منه في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى. قام من خلال ذلك إلى إصدار قوانين عامة (أولا) وقوانين خاصة (ثانيا) لمواجهة الجريمة الإلكترونية.

أولا: القوانين العامة المنظمة للجريمة الإلكترونية

نظم المشرع الجزائري الجريمة الإلكترونية بقوانين عامة هادفا بذلك إلى ردع هذا النوع المستحدث من الجرائم، وذلك عن طريق الدستور الجزائري (أ)، وقانون العقوبات (ب)، وقانون الإجراءات الجزائية (ج).

[1]-صغير يوسف، المرجع السابق، ص 63.

أ-الدستور الجزائري

كفل الدستور الجزائري[1] حماية الحقوق الأساسية والحريات الفردية والسهر على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى تحذر كل مساس بهذه الحقوق.

ومن بين المبادئ الدستورية نجد بحسب المواد التالية:

المادة 35 التي تنص على ما يلي: «**تضمن الدولة الحقوق الأساسية والحريات** »[2]. وبالتالي المشرع الجزائري سعى لحماية الحقوق من جميع الانتهاكات.

بينما نصت المادتين 74 و75 على أن حرية الإبداع الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون، لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون، تعمل الدولة على ترقية البحث العلمي وتنميته خدمة للتنمية المستدامة

[1]-دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996 المصادق عليه في استفتاء 28 نوفمبر 1996، الجريدة الرسمية، عدد76 الصادر في 08 ديسمبر معدل والمتمم بـ:
-قانون رقم 02-03 مؤرخ في 10 أفريل 2002، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 25 الصادر في 14 أفريل 2002.
- قانون رقم 08-19مؤرخ في 15 نوفمبر 2008، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 63 الصادر في 16 نوفمبر 2008.
- قانون رقم 16-01 مؤرخ في 06 مارس 2016، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 214 الصادر في 07 مارس 2016.
- قانون رقم 20-251مؤرخ في 15 سبتمبر 2020، يتضمن استدعاء الهيئة الانتخابية للاستفتاء المتعلق بمشروع تعديل الدستور، الجريدة الرسمية، العدد 54، الصادر في 16 سبتمبر 2020.

[2]-المادة 35 من القانون رقم 20-251، المتضمن الدستور الجزائري.

للأمة، ولا يجوز انتهاك حرمة حياة المواطن الخاصة؛ وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

يفهم من سياق المادتين، أن المشرع سعى لحماية حق المؤلف من جهة فلا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، وحماية الحياة الخاصة من كل أشكال الاعتداءات.

ب–قانون العقوبات الجزائري

انطلاقا من مبدأ الشرعية وفقا للأحكام المادة الأولى [1] من قانون العقوبات الجزائري سالفة الذكر جرم القانون رقم 04-15 بعض صور الجريمة الإلكترونية، ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات " من الفصل الثالث المعنون بـ "الجنايات والجنح ضد الأموال " من الباب الثاني المتعلق بـ "الجنايات والجنح ضد الأفراد" وذلك في المواد من 394 مكرر إلى 394 مكرر 07 من قانون العقوبات المعدل والمتمم[2].

ج–قانون الإجراءات الجزائية

لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بالجريمة الإلكترونية، محاولة منه القضاء عليها، أو على الأقل الحد من انتشارها. حيث وع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون الإجراءات الجزائية[3].

---

[1]–المادة الأولى من قانون العقوبات الجزائري: «**لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون**»

[2]–لمزيد من التفاصيل ينظر: ص30 من هذه المذكرة.

[3]–أمر رقم 66-156، المؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 47، الصادر في 09 جوان 1966، المعدل والمتمم لا سيما بالقانون رقم 19-10 المؤرخ في 11 ديسمبر 2019، الجريدة الرسمية، العدد 78.

متابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة والضبط...إلخ، كما قام باستحداث أساليب أخرى خاصة كاعتراض المراسلات، المراقبة الإلكترونية، التسرب، تسجيل الأصوات، والتقاط الصور والتي سنتطرق لها بالتفصيل في الباب الثاني من هذه المذكرة[1].

ثانيا: القوانين الخاصة المنظمة للجريمة الإلكترونية

كما أقر القانون الجزائري الحماية القانونية لنظم المعلومات في قوانين خاصة لمواكبة هذا النوع المستحدث من الجرائم. من هذه القوانين القانون رقم 03-2000 المتضمن قانون البريد والمواصلات السلكية واللاسلكية [2](أ)، وقانون التأمينات الاجتماعية رقم 08-01[3](ب)، والقانون 09-04 المتضمن القواعد الخاصة لوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها (ج) سالف الذكر.

أ-قانون البريد والمواصلات السلكية واللاسلكية

سعى قانون البريد والاتصالات لمواجهة هذه الظاهرة الإجرامية، من خلال المواد التي تضمنها لهذا الغرض، كما نص القانون سالف الذكر إلى استخدام حوالات دفع عادية أو إلكترونية أو برقية.

بينما نصت المادة 23 منه على ما يلي: « **يجوز إنشاء و/أو استغلال شبكات المواصلات السلكية واللاسلكية مهما كان نوع الخدمات المقدمة، وفق الشروط المحددة في هذا القانون وفي النصوص التنظيمية المتخذة لتطبيقه.**

[1]-لمزيد من التفاصيل ينظر: الباب الثاني من هذه المذكرة.

[2]-قانون رقم 2000-03 المؤرخ في 05 جمادى الأولى عام 1421 الموافق لـ 05 أغسطس سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية، العدد48.

[3]-قانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11، المؤرخ في 21 رمضان عام 1403 الموافق لـ2 يونيو 1983 المتعلق بالتأمينات الاجتماعية.

لا تشمل أحكام هذه المادة منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي»[1].

بحسب هذه المادة يجوز كأصل عام إنشاء استخدام شبكات الاتصال السلكية واللاسلكية، باختلاف نوع الخدمة المقدمة، لكن وفقا للرو ابط المحددة قانونا، باستثناء منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي.

كما نصت المادة 93 الفقرة الأخيرة على ما يلي: «**لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات**»[2]؛ بمعنى أنه يجب احترام سرية المراسلات.

ب–قانون التأمينات الاجتماعية

تطرق القانون رقم 08-01 إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية، التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كافة التراب الوطني.

حدد هذا القانون الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية وفقا لنص المادة 93 مكرر2 من قانون التأمينات الاجتماعية، حيث نصت على ما يلي: «**دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين إلى 5 سنوات وبغرامة من 100.000دج إلى 200.000دج، كل من يسلم أو**

[1]–المادة 23 من القانون 2000-03.

[2]–المادة 93 الفقرة الأخيرة من القانون 2000-03.

يتسلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو مفتاح إلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة»[1].

طبقا لنص المادة، نجد أن المشرع الجزائري يعاقب كل من يستخدم البطاقة الإلكترونية، أو المفتاح الإلكتروني لهيكل العلاج أو لمهني الصحة، أغراض غير شرعية، كما قام أيضا المشرع وفقا لهذا القانون بتجريم مجموعة الأفعال غير المشروعة، من القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية التي تتضمنها البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني سواء لهيكل العلاج أو لمهني الصحة.

ج–قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

نص القانون 09–04 على مراقبة الاتصالات الإلكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية؛ حيث نصت المادة 4 منه[2] على الحالات التي يسمح فيها للسلطات الأمنية باللجوء للمراقبة الإلكترونية وهي: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

حالة توفر معلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني و مؤسسات الدولة أو الاقتصاد الوطني.

في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، واشترط المشرع إجراء عمليات المراقبة بإذن مكتوب من السلطة القضائية المختصة[3].

[1]–المادة 93 مكرر 2 من القانون 08–01.

[2]–المادة 4 من القانون 09–04 .

[3]–زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، د.ط، الجزائر، 2011، ص 129.

كما نص كذلك هذا القانون على قواعد إجرائية تساهم بدورها في كشف الجريمة ومعالمها، من تفتيش وحجز للمعطيات المعلوماتية وحفظ المعلومات المتعلقة بحركة السير[1].

يسمح هذا القانون للسلطات التي تباشر التفتيش في منظومة معلوماتية، بنسخ المعطيات محل البحث، وكذل المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في وفقا للقواعد المقررة في قانون الإجراءات الجزائية[2].

يعتبر القانون 09-04 خطوة أولى للجزائر في مجال مواجهة الجريمة الإلكترونية من ناحية، وسدا للفراغ التشريعي الذي كان يعتري القانون الجزائري من ناحية أخرى. لكن هذا لا يكفي لردع الجرائم الإلكترونية بمختلف أنواعها[3].

ولجوء المشرع إلى تقنين أو النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس؛ بمعنى عدم جواز لجوء القاضي الجنائي إلى قياس فعل لم يرد النص على تجريمه على فعل ورد نص بتجريمه؛ فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين[4].

المطلب الثاني: النموذج المادي للجريمة الإلكترونية (الركن المادي)

يعتبر الركن المادي في الجريمة التقليدية الفعل أو السلوك المجرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته، كما يجب أن يرتبط السلوك الإجرامي والنتيجة الضارة

[1]-المادة 3 من القانون 09-04.

[2]-المادة 5 من نفس القانون.

[3]-زبيحة زيدان، المرجع السابق، ص 131.

[4]-أحمد خليفة الملط، المرجع السابق، ص 10.

بعلاقة سببية، بمعنى حتى يعاقب المجرم على سلوكه الإجرامي لابد أن يتطابق هذا الفعل المجرم مع النموذج الإجرامي المنصوص عليه في قانون العقوبات[1].

أما الركن المادي في الجريمة الإلكترونية يتطلب قيام السلوك الإجرامي والنتيجة والعلاقة السببية. علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقيق نتيجتها، مثلا (إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل)[2].

ويتخذ الركن المادي للجريمة الإلكترونية عدة صور بحسب الجريمة، وهو ما سنقوم بتبيانه بداية بالسلوك الإجرامي (الفرع الأول)، النتيجة (الفرع الثاني)، ثم العلاقة السببية (الفرع الثالث).

الفرع الأول: السلوك الإجرامي

يعتبر السلوك المادي عبر الانترنت محلا لجملة من التساؤلات لا سيما فيما يتعلق ببداياته أو الشروع في ارتكاب الجريمة، وهو يختلف عما هو الحال في العالم المادي، ذلك لأن ارتكاب الجريمة عبر الإنترنت تحتاج بالضرورة إلى منطق تقني، أي أنها تتم عبر الإنترنت أو باستخدام المعالجة الآلية للبيانات، كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والإنترنت[3].

ويتخذ السلوك الإجرامي في الجرائم الإلكترونية صورتين:

[1]-بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2018/2017، ص 27.

[2]-مرابط حياة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، مستغانم، 2019/2018، ص 13

[3]-هروال هبة نبيلة، الجوانب الإجرائية لجرائم الإنترنت، المرجع السابق، ص 46-47.

أ-الصورة الأولى تتمثل في السلوك الإيجابي والذي يتطلب مجهود بدني يتمثل في الإقدام على فعل ينهى القانون عن ارتكابه[1]. و مثال ذلك كل الأفعال التي يرتكبها الجاني، كفعل الدخول أو البقاء عن طريق الغش في كل جزء من نظام المعالجة الآلية للمعطيات، نص المشرع الفرنسي على فعل الدخول أو البقاء في المادة 1/323-1 من قانون العقوبات الفرنسي والتي تنص على الآلي: "فعل الدخول أو البقاء –بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنتين وبغرامة مقدارها 60.000أورو"[2].

كما قام المشرع السعودي في المادة الثالثة من نظام مكافحة الجرائم الإلكترونية بالنص على بعض الأفعال التي تعتبر السلوك الإجرامي المكون للركن المادي لهذه الجريمة، نذكر البعض منها:

1-التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح، أو التقاطه أو اعتراضه.

2-الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.

3-الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله، أو تغير عنوانه[3].

[1]-أحسن بوسقيعة، المرجع السابق، ص 116.

[2]-L'article 323/1-1 du code pénale français , www.Legifrance.gouv.Fr.

[3]-المادة03 من نظام مكافحة الجرائم المعلوماتية السعودي.

قد يكون النشاط الإجرامي في الجرائم الإلكترونية وقتيا؛ أي يبدأ وينتهي بمجرد تمامه، مثل السرقة المعلوماتية أو الاعتداء على معطيات الحاسب الآلي بإتلافها، وقد يكون مستمر مثل إنشاء مواقع لتحريض القصر على الفسق أو الانتحار[1].

أما الصورة الثانية وهي السلوك السلبي؛ وهو الامتناع أو إحجام شخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به وعليه فلا يجوز للموظف أن يمتنع على أداء مهام وظيفته[2].

أما الامتناع في الجرائم الإلكترونية يكون مثل امتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها، أو عدم الإبلاغ عن الجريمة للحفاظ على حقوق الغير وخصوصياتهم[3].

وبالتالي فالسلوك الإجرامي في الجريمة الإلكترونية يتم عن طريق الجهاز الإلكتروني أيا كان نوعه أو شكله متصلا بشبكة الانترنت، وبدون هذه الوسيلة لا يمكن مباشرة السلوك الإجرامي.

الفرع الثاني: النتيجة الإجرامية

يقصد بالنتيجة الإجرامية، الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، فالسلوك قد أحدث تغييرا حسيا ملموسا في الواقع الخارجي، ومفهوم النتيجة كعنصر في

---

[1]-كلعبة الحوت الأزرق **blue whale** أو تحدي الحوت الأزرق؛ وهي لعبة على شبكة الإنترنت، حيث قام فيليب بودكين بابتكار هذه اللعبة وكان هدفه منها تنظيف المجتمع من خلال دفع الناس إلى الانتحار الذي اعتبر أنه ليس له قيمة، تتكون اللعبة من تحديات لمدة 50 يوم وفي التحدي النهائي يطلب من اللاعب الانتحار، بدأت هذه اللعبة بالانتشار الواسع في روسيا ونجم عنها العديد من الضحايا وخلق موجة من الذعر في روسيا، لتنتشر بعد ذلك في مختلف مناطق العالم، تعتمد هذه اللعبة على غسل لدماغ المراهقين الضعفاء، وأمرهم بالقيام بأعمال معينة مثل مشاهدة أفلام الرعب والاستيقاظ في ساعات متأخرة من الليل وإيذاء النفس بعد أن يتم استنفاذ قواهم في النهاية يتم أمرهم بالانتحار، أنظر الموقع الإلكتروني: www.albawaba.com.

[2]-عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية، الجزائر، 1995، ص 148.

[3]-بوشعرة أمينة، موساوي سهام، المرجع السابق، ص 31.

الركن المادي لجريمة يقوم على أساس ما يعتد به المشرع ويترتب عليه نتائج، بغض النظر عما يحدثه السلوك الإجرامي من نتائج أخرى[1].

وتعتبر الجريمة الإلكترونية كغيرها من الجرائم التي يفترض فيها وجود النتيجة الإجرامية كأساس لقيام الركن المادي لهذ ا النوع المستحدث من الجرائم، حيث تعتبر من العناصر المكونة للركن المادي والذي يعد من أهم أركان الجريمة، والذي بدونه لا تقوم الجريمة[2].

بصدد دراستنا للنتيجة الجرمية كأحد عناصر الركن المادي، فإننا نسلط الضوء فقط على ذكر النتيجة الإجرامية للجريمة الإلكترونية بصفة عامة دون الحديث بالتفصيل عن النتيجة الإجرامية لكل جريمة إلكترونية، وبالتالي تثير النتيجة الإجرامية في هذا النوع من الجرائم مشاكل عديدة من أهمها: تحديد هل الجريمة الإلكترونية هي جريمة مرتكبة سلوكا ونتيجة في العالم الافتراضي أم أن هناك امتداد للنتيجة ليتحقق منتهاها في العالم المادي؟[3].

الفرع الثالث: العلاقة السببية

تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وهمة الرابطة السببية ترجع إلى أن اسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحدد العلاقة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت الجريمة غير عمدية فإن نفي العلاقة السببية يؤدي إلى انتفاء المسؤول كلية عنها؛ ذلك أنه لا شروع في الجرائم غير العمدية[4].

---

[1]-عبد الله سليمان، المرجع السابق، ص 149.

[2]-بوشعرة أمينة، موساوي سهام، المرجع السابق، ص 33.

[3]-هروال هبة نبيلة، الجوانب الإجرامية لجرائم الانترنت، المرجع السابق، ص 47.

[4]-أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية الحقوق بجامعة بنها، 2009، ص82.

تعد العلاقة السببية عنصر مهم من عناصر الركن المادي للجريمة؛ حيث تعتبر حلقة وصل بين السلوك الإجرامي والنتيجة الإجرامية، ذلك بإثبات أن هذا السلوك هو سبب في حدوث النتيجة الضارة.

أما في نطاق الجرائم الإلكترونية، تعتبر العلاقة السببية أساسية ليتم هذا النوع المستجد من الجرائم، والمبدأ العام الذي يحكم العلاقة السببية أن الإنسان لا يسأل إلا على النتائج التي يكون لنشاطه دخلا في إحداثها، فاستحقاق العقاب في القانون هو رهن قيام الرابطة السببية بين نشاط الجاني وبين الواقعة الإجرامية، وبالتالي ينبغي لمسألته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية[1].

ففي جريمة انتهاك الحق في الخصوصية عبر شبكة الانترنت يجب أن يكون هناك دخول غير مصرح به، واستخدام الحاسوب والقيام باختراق الخدمات المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع ما، وتكون العلاقة السببية قائمة بمجرد ثبوت الضرر الناتج عن السلوك غير المشروع[2].

المبحث الثاني: الركن المعنوي للجريمة الإلكترونية

يتخذ الركن المعنوي في أغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه [3]. ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكاب جريمته، حيث لا تقوم الجريمة قانونا بدونه، فلا بد من توفر الإرادة الآثمة لدى الجاني عند إقدامه على السلوك الإجرامي، كما يجب أن تكون الأفعال إرادية وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال متجه نحو مخالفة القواعد القانونية،

[1]-بوشعرة أمينة، موساوي سهام، المرجع السابق، ص 35-36.

[2]-المرجع نفسه، ص 36.

[3]- أحسن بوسقيعة، المرجع السابق، ص 145.

ليترتب على مخالفتها ا لجزاء الجنائي المناسب، فمن التصور غالبا أن لا تقع الجريمة الإلكترونية إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اخترق الشبكة، والأصل في الجرائم هو العمدية إلا ما استثني بنص[1].

يتخذ الركن المعنوي في هذا النوع المستجد من الجرائم صورة القصد الجنائي العام بعنصريه العلم والإرادة، إذ يجب أن تتجه إرادة الجاني إلى فعل الاعتداء، كما يجب أن يعلم بأن نشاطه الإجرامي يؤدي إلى ارتكاب سلوك يعاقب عليه القانون.

ولقد ثار جدل فقهي حوى مدى ضرورة توافر القصد الجنائي الخاص في بعض الجرائم الإلكترونية فهناك من يرى [2] ضرورة توافر هذا القصد، في حين يرى البعض الآخر [3] أن القصد الجنائي العام كاف لوحده لقيام الركن المعنوي للجريمة الإلكترونية، وبالتالي لا يتطلب وجود القصد الجنائي الخاص لاكتمال الركن المعنوي، ويختلف الركن المعنوي باختلاف نشاط غير المشروع المقترف من طرف المجرم المعلوماتي. لذلك نقوم بعرض القصد الجنائي العام (المطلب الأول)، والقصد الجنائي الخاص (المطلب الثاني).

المطلب الأول: القصد الجنائي العام

يهدف الجاني عند ارتكابه للواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، بتحقيقه قد تتم الجريمة ويتوفر لها القصد الجنائي العام[4].

---

[1]-بالطي غنية، المرجع السابق، ص 48.

[2]-أحمد خليفة الملط، المرجع السابق، ص121. خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، د.ط، الإسكندرية، 2007، ص 212-213. هروال هبة نبيلة، الجوانب الإجرامية لجرائم الانترنت، المرجع السابق، ص 50.

[3]-الشوابكة محمد أمين أحمد، مرجع سابق، ص 221، معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلومات في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماستر في العلوم الجنائية، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2015، ص24.

[4]-عبد الله سليمان، المرجع السابق، ص 261.

بمعنى أن للقصد الجنائي العام صورتين العلم والإرادة؛ أي أن يتكون من إرادة الفاعل التي تهدف إلى تحقيق عمل يجرمه القانون مع علمه بكل عناصره التي يحددها القانون من ويختلف القصد الجنائي العام باختلاف السلوك المؤدي لارتكاب الجريمة، فهناك بعض من الجرائم المعلوماتية بحكم طبيعتها لا يشترط لقيامها وجود قصد خاص، كجريمة الدخول الغير المصرح بها إلى نظام المعالجة الآلية للمعطيات، تتطلب قصدا جنائيا عاما يتمثل في العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار أن المشرع الجزائري سعى لحماية محل الحق وهو جهاز الحاسب الآلي بما يتضمنه من معلومات وبرامج[1].

كما اشترط المشرع توافر القصد الجنائي العام في جريمة إتلاف المعلومات، حيث يكفي علم الجاني بأنه يقوم بأعمال من شأنها أن تؤدي إلى تغيير الحالة التي كانت عليها المعلومات أو المعطيات بمحوها أو إتلافها وأن تتجه إرادته إلى تحقيق ذلك[2].

وبالتالي نجد معظم الجرائم المعلوماتية اشترط فيها المشرع القصد الجنائي العام، حيث اكتفى بالضرورة إلى توافر القصد الجنائي العام لوحده لقيام الركن المعنوي لهذا النوع من الجرائم المتحدثة على غرار التشريعات الأخرى التي دعت إلى توافر القصد الجنائي الخاص إلى جانب القصد الجنائي العام في بعض الجرائم الإلكترونية وهو ما نقوم بتبيانه في المطلب الثاني.

المطلب الثاني: القصد الجنائي الخاص

إن أغلب الجرائم ترتكب بصورة قصدية، وبالتالي يعد القصد الجنائي من بين أكثر عناصر الركن المعنوي تصورا.

لقد اختلفت بعض التشريعات حول مدى ضرورة توافر القصد الجنائي الخاص في البعض من جرائم المعلوماتية، فنجد أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي

[1]-معتوق عبد اللطيف، المرجع السابق، ص 24.

[2]-الشوابكة محمد أمين أحمد، المرجع السابق، ص 221.

ترتكب باستخدام الانترنت من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما أم خاص ا. فنجده لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد عبر البريد الإلكتروني[1].

أما القضاء الفرنسي، فعلى غرار مثيله الأمريكي، نجد أن منطق سوء النية يكتسح النصوص التي تطبق بشأن جرائم الانترنت مثلما هو مقرر في المادة 15 و 226 من قانون العقوبات الفرنسي، حيث يشترط سوء النية في منطق القصد الخاص حين وجود عدوان على البريد الإلكتروني[2].

حيث يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى، فجريمة الاحتيال الإلكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الحاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع[3].

كما يرى جانب من الفقه أن جريمة التعامل في معلومات غير مشروعة تشترط قصد جنائي عام بالإضافة إلى قصد جنائي خاص سواء في صورة الجريمة الأولى وهي التعامل في معلومات صالحة لارتكاب الجريمة أو في صورتها الثانية المتمثلة في التعامل في معلومات متحصلة من جريمة[4].

نجد أن المشرع الجزائري لم يشترط قصد جنائي خاص في الصورة الثانية من جريمة التعامل في معلومات غير مشروعة، وذات الوضع بالنسبة للمشرع الفرنسي.

---

[1]-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، د.ط، القاهرة، 2004، ص 294.

[2]-المرجع نفسه، ص 294.

[3]-أحمد خليفة الملط، المرجع السابق، ص 121.

[4]-خليفة محمد، المرجع السابق، ص 212-213.

وبالتالي المشرع الجزائري لم يشترط توافر القصد الجنائي الخاص في هذه الجريمة بصورتيها، وبالنسبة إلى الجرائم الأخرى المتعلقة بالاعتداء على أنظمة المعالجة الآلية للمعطيات بل اكتفى بالضرورة توافر القصد الجنائي العام لقيام الركن المعنوي لهذا النوع المستحدث من الجرائم[1].

[1]- خليفة محمد، المرجع السابق، ص 213، 215.

خلاصة الباب:

بعد أن تناولنا في هذا الباب خصوصية الجريمة الإلكترونية من الناحية الموضوعية. تبين لنا أن هذا النوع من الجرائم يعد من أكثر الجرائم خطورة. حيث اتسمت بطبيعة خاصة، وجدنا صعوبة في وضع تعريف عام جامع وموحد لها، فقد اختلفت المفاهيم حولها باختلاف الزاوية التي ينظر منها إليها. أين بينا مختلف التعاريف الفقهية والقانونية للجريمة الإلكترونية، وانتهينا إلى كونها كل اعتداء على النظام المعلوماتي أو يتم باستخدام النظام المعلوماتي حيث أن له دور رئيسي في السلوك المجرم، وهي بهذا المفهوم تتميز بعدة خصائص تميزها عن باقي الجرائم الأخرى، إذ من أهم هذه السمات طبيعتها المتعدية للحدود، وأنها جرائم خفية ومستترة، وطابعها التقني الذي يعقد من مسألة اكتشافها وإثباتها الشيء الذي يميز مرتكبيها ويجعل دوافع ارتكابهم للجرائم الإلكترونية بمختلف أنواعها تختلف عن المجرمين العاديين.

كما تطرقنا أيضا إلى أنواع الجريمة الإلكترونية المتمثلة في التقسيم الفقهي والتقسيم القانوني لهذه الجرائم. إضافة إلى تحديد أركان الجريمة الإلكترونية فهي تقوم بقيامها وتزول بزوال أحدها كأي جريمة أخرى، المتمثلة في الركن الشرعي والركن المادي والركن المعنوي.

وبالنسبة للمشرع الجزائري نجده اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. وما يعاب عليه أنه اهتم بها بالنص على بعض الجرائم الإلكترونية وليس كلها، وأهمل المجرم الإلكتروني، إذ لم يتعرض له في أي نص قانوني بالإشارة إلى تعريفه أو سماته، سواء في قانون العقوبات أو القانون 09-04، كما أن التطرق للجريمة الإلكترونية من الناحية الموضوعية والتعرف عليها بعمق يفيدنا في إيجاد الحلول لمواجهتها.

الباب الثاني

الإطار الإجرائي للجريمة الإلكترونية

تخضع المادة الجزائية بشقيها الموضوعي والإجرائي لمبدأ الشرعية، الذي يعمل على حصر سلطة التجريم والعقاب في يد المشرع، ويعمل على إقرار التوازن بين الحقوق والحريات وضمان المصلحة العامة. واعتبرت هذه القاعدة من القواعد الراسخة والمنصوص عليها قانونيا ودستوريا؛ إلا أن ظهور الجريمة الإلكترونية قد احدث ثورة في فلسفة التجريم والعقاب والإجراءات الجزائية، فقد أثارت الجريمة الإلكترونية بعض الصعوبات والتحديات للأجهزة المعنية بالقيام بالإجراءات الجزائية وفقا لما هو منصوص عليه في القانون[1].

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

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

حاولنا في هذا الباب دراسة الجانب الإجرائي للجريمة الإلكترونية، ومن ثمة سوف نتطرق إلى إجراءات البحث والتحري في الجريمة الإلكترونية (**الفصل الأول**)، بينما نتناول إجراءات التحقيق والمحاكمة في الجريمة الإلكترونية (**الفصل الثاني**)

[1]-أحمد أسامة حسنية، المرجع السابق، ص 22.

الفصل الأول: إجراءات البحث والتحري في الجريمة الإلكتروني

لم تكتف التشريعات الحديثة بحماية معطيات الحاسب الآلي بصفة عامة من خلال تجريم صور الاعتداء عليها؛ أي حماية موضوعية، وإنما نظرا لخطورة الإجرام الإلكتروني في حد ذاته لكون محل الجريمة مجموعة معطيات هي عبارة في الحقيقة عن ذبذبات إلكترونية يسهل على الجاني القيام بعمل إجرامي عليها دون ترك آثار، ودون أن يستغرق هذا العمل وقتا طويلا، وهو ما جعلها صعبة الاكتشاف والإثبات، مما أدى إلى ظهور مشكلات إجرائية في هذا النطاق؛ حيث أن ضابط الشرطة القضائية أو القاضي نفسه في حيرة أمام هذه الجرائم نظرا لقصور التشريع الإجرائي خاصة وأن هذه الجرائم حديثة ولا يمكن تطبيق النصوص التقليدية عليها وعدم القدرة الكافية والفنية لرجال القانون لاستيعابها.

لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية، ومنها لا يطبق إلا على الجريمة الإلكترونية خاصة في مرحلة جمع الاستدلالات.

ومن خلال طرح التساؤل الذي مفاده فيما تتمثل إجراءات البحث والتحري في الجريمة الإلكترونية؟

يمكن من هذا المنطلق تقسيم هذا الفصل إلى مبحثين: الإجراءات العامة لمتابعة الجريمة الإلكترونية (**المبحث الأول**)، و الإجراءات الخاصة وقواعد الاختصاص (**المبحث الثاني**)

المبحث الأول: الإجراءات العامة لمتابعة الجريمة الإلكترونية

تنقسم الإجراءات العامة لمتابعة الجريمة الإلكترونية إلى إجراءات مادية تتمثل في المعاينة التقنية والتفتيش (**المطلب الأول**)، وأخرى إجراءات شخصية تتمثل في الخبرة وشهادة شاهد إلكتروني والتسرب (**المطلب الثاني**).

المطلب الأول: الإجراءات المادية

وتتمثل الإجراءات المادية كما ذكرنا سابقا في المعاينة التقنية من جهة (**الفرع الأول**)، والتفتيش في البيئة الإلكترونية من جهة أخرى (**الفرع الثاني**).

الفرع الأول: المعاينة التقنية

المعاينة التقنية هي المكان الذي ارتكبت فيه الجريمة، والوعاء الأساسي الذي يحتوي على أخطر الأدلة الجنائية التي يخلفها الجاني وراءه عقب ارتكابه للجريمة، وفي لحظة يكون فيها اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تتيح المراجعة الدقيقة لأعماله وإزالة الآثار التي يخلفها في مكان الحادث، فالمجرم مهما كانت دقته سوف يترك وراءه ما قد يشير إلى شخصيته [1]، لذلك كان من الواجب على ضباط الشرطة القضائية الانتقال إلى ذلك المكان لمعاينة وإثبات الآثار المادية للجريمة والمحافظة عليها.

ويقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد. وهي المرحلة الأولى للاستدلال حول ملابسات أية جريمة، ونظرا لاختلاف الجريمة المعلوماتية كثيرا عن الجرائم التقليدية نظرا لكون مسرحها الإجرامي قد يتعدى حدود الدولة، فإن المعاينة التقنية تتم بإتباع مجموعة من الإجراءات الخاصة[2] سنوردها فيما بعد.

وتظهر أهمية المعاينة أنها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بكل ما يحتويه هذا الموقع من تفصيلات سواء تعلقت هذه التفصيلات بمكانه أو وصفه من الداخل أو

[1]-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 212.
[2]-أمير فرج يوسف، المرجع السابق، ص 219-220.

الآثار الموجودة به، والتي تنقلها بالجريمة، وكل ما يمكن جهات الشرطة والقضاء من وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها[1].

وحتى تحقق المعاينة ثمارها وتفي بأغراضها المشهودة، نجد بعض التشريعات الجزائية الإجرائية قررت عقابا جنائيا لكل من يحدث تعديل أو تغيير في مكان وقوع الجريمة[2].قبل قيام سلطة التحقيق أو الاستدلالات بإجراء المعاينة الأولى أيا كان مرتكبها[3].

وقد نصت المادة 42 من قانون الإجراءات الجزائية الجزائري على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو جهاز مخول لجهاز الضبطية القضائية سواء في الحالات العادية أو في حالات التلبس [4]. ويترتب على أي تغيير أو تعديل يطرأ على مكان وقوع الجريمة الجزاءات المنصوص عليها في المادة 43 من قانون الإجراءات الجزائية الجزائري[5].

وحتى يكون التفتيش في بيئة إلكترونية لابد أن يتم على مستويين يتمثل الأول في تفتيش المكونات المادية للحاسب الآلي التي تمثل مسرح الجريمة التقليدي، أما الثاني فيتمثل في تفتيش المكونات المعنوية للحاسوب التي تمثل مسرح الجريمة الافتراضي[6].

---

[1]–نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 216.

[2]–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، د.ط، مصر، 2007، ص 180.

[3]–الأصل العام المعاينة يمارسها ضباط الشرطة القضائية تحت سلطة القضاة بمعاينة مسرح الجريمة وضبط الأدلة وكل ما يتعلق بالجريمة والجناة، كما يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، طبقا للمادة 79 ق.إ.ج.ج، سالف الذكر.

[4]–المادة 42 من قانون الإجراءات الجزائية الجزائري.

[5]–المادة 43 من قانون الإجراءات الجزائية الجزائري.

[6]–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص182.

أولا: مدى صلاحية مسرح الجريمة الإلكترونية للمعاينة

إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي، فإن الجريمة المعلوماتية تتم فيها المعاينة على مستوين:

أ-المسرح التقليدي (الجرائم الواقعة على المكونات المادية)

يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية، ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس[1].

وليس هناك صعوبة لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية، والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، مع إخطار النيابة العامة بذلك[2].

في هذه الحالة تتميز المعاينة بالسهولة، باعتبار أنها تتم على عناصر ملموسة كانت محلا للجريمة أو تخلفت عنها.

ب-المسرح الافتراضي (الجرائم الواقعة على المكونات الغير مادية أو بواسطتها)

يقع داخل البيئة الإلكترونية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله.

[1]-المادة 3/42 من قانون الإجراءات الجزائية الجزائري.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص182.

وفي مقدمة هذه الجرائم تأتي الواقعة على برامج الحاسب الآلي أو بياناته، أو تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الإنترنت، ومنها كذلك جرائم التزوير المعلوماتي والتخريب الذي يتم بواسطة الفيروس المعلوماتي[1].

وللمعاينة في جرائم الانترنت والحاسوب أشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على أن هناك طرقا عامة تتوافق مع طبيعة الاتصال بالإنترنت أو الوسيلة التي تستخدم مثلا: وسيلة تصوير شاشة الحاسوب impression de captures d'écran والتي تكون بواسطة آلة تصوير تقليدية أو عن طريق استخدام برمجة حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة frozen وغيرها[2].

ثانيا: إجراءات المعاينة التقنية

لابد على ضابط الشرطة القضائية إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية، تتمثل هذه الإجراءات في[3]:

1-ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها.

2-وجود خريطة توضح الموقع الذي سيتم معاينته، وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

3-تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة.

4-إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

[1]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 183.

[2]-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 218.

[3]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، د.ط، الإسكندرية، 2006، ص 84، 86.

5-إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها.

6-أن تتم هذه المعاينة وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

7-تحديد عناوين IP وعناوين البريد الإلكتروني[1] المستعملة في ارتكاب الجريمة.

8-الاستعانة بالخبراء في المسائل العلمية والتقنية التي تحتاج إلى خبرة خاصة كخبرة الطبيب الشرعي.

9-استخدام برامج التتبع؛ التي تسمح لهم بالتعرف على الأشخاص المشتبه فيهم وتحديد أماكن تواجدهم.

10-استخدام تقنيات التخفي عن طريق نظام البروكسي proxy[2].

الفرع الثاني: التفتيش المعلوماتي

يعتبر التفتيش[3] إجراء من إجراءات البحث والتحقيق ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها، وإن لإجراء التفتيش أهمية بالغة وخطورة معتبرة على الحياة الخاصة، لهذا نص عليه المشرع الجزائري بمقتضى قواعد دستورية [4]، حيث تضمن الدولة عدم انتهاك حرمة مسكن، فلا تفتيش إلا بمقتضى القانون. وفي إطار احترامه فلا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة. هذا بالإضافة إلى نصوص قانون الإجراءات الجزائية وأيضا القانون 09-04 سالف الذكر.

---

[1]-**IP**: هو وسيلة للتواصل بين الأشخاص، حيث يرسل شخص ما رسالة إلى شخص آخر عن طريق خط تلفوني.

[2]-**Proxy**: هو باختصار نوع من أنواع firewall حيث أنه ينظم الحركة بين الشبكة المحلية كشبكة الجامعة وبين شبكة الانترنت حتى يمكن الاتصال بالمواقع الممنوعة.

[3]-التفتيش: وهو إجراء من إجراءات البحث عن الأدلة لإثبات وقوع جريمة ما في مكان ما. وقد حددت ضوابطه في قانون الإجراءات الجزائية الجزائري من المواد 44 إلى 47 منه.

[4]-المادة 40 من دستور 1996 الجزائري.

غير أنه في الجريمة الإلكترونية يثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب والانترنت. لكن من المعروف أن نظم المعالجة الآلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال بعدية[1].

أولا: محل التفتيش

محل التفتيش في جرائم الحاسب الآلي يعتبر النافذة التي تطل بها الانترنت على العالم، والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي وغيرها.

وتجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون قائما بذاته، وإنما يشمله مكان أو عقار أو يكون بصحبة مالكه أو حائزه، لذا يجب على ضابط الشرطة القضائية عند استصداره لإذن التفتيش أن يحدد محل ذلك الإجراء تحديدا دقيقا، وكذلك الغرض منه وإلا كان باطلا.

إن إجراء التفتيش في الجريمة الإلكترونية يحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش العادية (التقليدية) لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات أجهزة الإعلام الآلي وأماكن إخفاء المعلومات فيها، لأنه يسهل إتلافها كليا او جزئيا، كما يصعب تحديد مكان الدليل[2].

وبالتالي يقع التفتيش في إطار الجرائم الإلكترونية على تفتيش مكونات الحاسب الآلي (المادية والمعنوية) وتفتيش الشبكات المعلوماتية المتصلة بالحاسوب (التفتيش عن بعد).

ثانيا: ضوابط التفتيش

من الشروط والضمانات التي يجب توافرها لإجراء التفتيش، نجد شروط شكلية وشروط موضوعية. نبرزها فيما يلي:

[1]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 378.

[2]-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 234.

أ-الشروط الشكلية للتفتيش

حددت المادة 44 منق.إ.ج.ج لاسيما بعد التعديل الذي حصل بموجب القانون 06-22 في 20 سبتمبر 2006 وهي[1]:

- ✓ وجود إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق.
- ✓ الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.
- ✓ أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها، وعنوان الأماكن المقصودة بالتفتيش.
- ✓ حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.
- ✓ في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين عنده.
- ✓ الميقات الزمني لإجراء التفتيش في الجرائم الإلكترونية: وهو الفترة التي يجوز فيها التفتيش، نصت عليها المادة 47 من قانون الإجراءات الجزائية الجزائري على أنه: "من الساعة الخامسة صباحا إلى السعة الثامنة مساءا، أما إذا طلب صاحب المنزل ذلك وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا، وهناك حالات استثنائية كحالة الطوارئ وغيرها يجوز التفتيش في كل ساعة من ساعات الليل والنهار".
- ✓ محضر التفتيش في الجرائم الإلكترونية: يتم تحرير محضر لكي يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة ولم يتطلب القانون شكل خاص للمحضر وبالتالي لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما"[2].

ب-الشروط الموضوعية للتفتيش

ويقصد بها الشروط اللازمة حتى يكون التفتيش صحيحا، وتتمثل في:

[1]-زبيحة زيدان، المرجع السابق، ص 20-21.

[2]-عائشة بن قارة مصطفى، المرجع السابق، ص 103-104.

1-سبب التفتيش: حتى يكون التفتيش صحيحا، لابد أن تكون هناك جريمة معلوماتية[1]، وهو ما أكدته المادة 5 من القانون 09-.04

2-الغاية من التفتيش: لابد أن يكون التفتيش بقصد ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة طبقا لنص المادة 44 من ق.إ.ج.ج، وإلا كان باطلا إذا كان يجرى لغاية أخرى[2].

3-محل التفتيش: وهو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الانترنت، فقد يكون محل الحاسب الآلي، مكانن أو عقار ما، أو يكون بصحبة مالكه أو حائزه، أو المكونات المادية والمعنوية للحاسب الآلي[3].

4-إذن التفتيش: طبقا للتشريع الجزائري فإن إذن التفتيش لابد أن يكون مكتوبا من طرف إما وكيل الجمهورية أو قاضي التحقيق المختص[4].

المطلب الثاني: الإجراءات الشخصية

وهي إجراءات تتعلق بالشخص في حد ذاته وتتمثل في الخبرة (الفرع الأول)، وشهادة شاهد إلكتروني (الفرع الثاني)، والتسرب (الفرع الثالث)، وهو ما سنتناوله بالتفصيل.

الفرع الأول: الخبرة

الخبرة هي إجراء يستهدف استخدام قدرات الشخص الفنية أو العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرينة يفيد معرفة الحقيقة بشأن وقوع جريمة ونسبتها إلى المتهم، ولهذا فإن للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة؛ حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية في مجال الشبكات، ونظرا لأن الجريمة

[1]-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص 229.
[2]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 358.
[3]-خالد عياد الحلبي، المرجع السابق، ص 168.
[4]-المادة 45 من قانون الإجراءات الجزائية الجزائري.

الإلكترونية لها خصوصيتها؛ فإن الخبير المعلوماتي لابد أن تتوافر لديه القدرة الفنية والإمكانيات العلمية والفنية في مسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية[1].

أولا: مهام الخبير

- ✓ تركيب الحاسب الآلي ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها.
- ✓ بيئة الحاسوب أو الشبكة من حيث طبيعتها وتركيزها أو توزيعها، نمط ووسائل الاتصال[2].
- ✓ المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.
- ✓ الآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة الإلكترونية.
- ✓ كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها[3].

ثانيا: ضوابط الخبرة

تخضع الخبرة لمجموعة من الضوابط القانونية (أ) والفنية(**ب**).

أ-الضوابط القانونية

وتنحصر في تلك الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء، وواجبات والتزامات الخبير (حلف اليمين، خضوعه للرقابة القضائية)[4].

- ✓ القيام بمهامه بنفسه واستجابته لطلبات الخصوم
- ✓ إيداعه التقارير خلال المدة المحددة[5]

[1]-صغير يوسف، المرجع السابق، ص 88-89.

[2]-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 138.

[3]-صغير يوسف، المرجع السابق، ص 90.

[4]-المواد: 143، 144، 145، 148، 153 من قانون الإجراءات الجزائية الجزائري.

[5]-المادة 5 الفقرة الأخيرة من القانون 09-04.

ب–الضوابط الفنية

تشمل خطوات اشتقاق الدليل الإلكتروني، والتي تتمثل في خطوات ما قبل التشغيل والفحص، وخطوات التشغيل، وتحديد مدن الترابط بين الدليل المادي، والإلكتروني ومرحلة تدوين النتائج[1]، وتتمثل هذه الضوابط في:

- ✓ القدرة على أداء المهام دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصل عليها من الوسائل الإلكترونية.
- ✓ الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر ورموز التشفير.
- ✓ بالإضافة إلى إلمام الخبير بنظم الحاسب الآلي بمكوناته المادية والبرامجية[2].

الفرع الثاني: شهادة الشاهد الإلكتروني (الشهادة في الجريمة الإلكترونية)

الشهادة هي ما يدلي به الشخص شفاهة أو كتابة سواء من تلقاء نفسه أو بدافع من غيره لما رآه أو سمعه أو أدركه بحواسه. والشهادة كإجراء من إجراءات التحري هي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد [3]. أما الشاهد في الجريمة الإلكترونية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي يكون لديه معلومات جوهرية لازمة للدخول في نظام المعالجة الآلية للبيانات، فلذ الك نجد أن الشاهد المعلوماتي ينحصر في عدة

[1]–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص140.

[2]–سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص 170.

[3]–فيروز عوض الكريم صالح ميرغني، إجراءات التحري والضبط في الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الدراسات العليا والبحث العلمي، جامعة شندي، السودان، 2017/2016، ص 112.

طوائف تتمثل في: مشغلة الحاسب الآلي، خبراء البرامج، المحللون، مهندسو الصيانة والاتصالات، مدير النظم. لذلك يطلق عليه اسم الشاهد المعلوماتي تمييزا عن الشاهد التقليدي[1].

الفرع الثالث: التسرب

إن التسرب هو تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط لمعرفة أو استعلام عن نشاط جرمي، ومعرفة أدق التفاصيل فيه وخصوصياته، أما من الناحية القانونية فالمشرع الجزائري حدد مقصود هذا الإجراء بموجب المادة 65 مكرر 12 على أنه: "قيام ضابط الشرطة القضائية أو عون تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة أشخاص مشتبه فيهم في ارتكاب جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك"[2].

ويلاحظ مما سبق ذكره أن التسرب عملية معقدة، تتطلب أن يتدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم، ويربط معهم علاقة من أجل تحقيق الهدف النهائي من العملية، وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية[3].

أولا: شروط التسرب

يعتبر هذا الإجراء من أخطر الإجراءات لكونه يقتضي انتهاك لحرمة الحياة الخاصة للمشتبه فيه[4]. فقد أحاطه المشرع بجملة من الشروط، تتمثل في:

أ-الشروط الشكلية

- ✓ أن يكون صادر بإذن قضائي إما من وكيل الجمهورية أو قاضي التحقيق المختص.

[1]-مرابط حياة، مرجع سابق، ص 42-43.

[2]-المادة 65 مكرر 12 من ق.إ.ج.ج.

[3]-سعيداني نعيم، المرجع السابق، ص 169.

[4]-باعتبار أن حرمة الحياة الخاصة حق مكفول دستوريا، وكذا في الاتفاقيات التي صادقت عليها الجزائر ولذلك حدد القانون ضوابط لإجراء عملية التسرب.

- ✓ أن يكون الإذن مكتوبا وإلا وقع تحت طائلة البطلان[1].
- ✓ ذكر اسم الضابط الذي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة القضائية باعتباره مساعدا له[2].
- ✓ المدة المطلوبة لعملية التسرب 4 أشهر محددة قانونا قابلة للتجديد ويمكن توقيفها حتى انتهاء المدة المحددة[3].

ب–الشروط الموضوعية

- ✓ تسبيب الإذن بالتسرب خاصة إذا اثبت أن الاعتداء على الوسائط الفعلة العادية غير كاف للتوصل إلى الحقيقة، ومن ثمة لابد من وكيل الجمهورية أو قاضي التحقيق أن يقدم تبريرا أو الأساس الذي تم اعتماده من أجل السماح بالقيام بعملية التسرب.
- ✓ أن نوع الجريمة هي من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[4].

ثانيا: التسرب الرقمي

يمكن تصور التسرب في نطاق الجرائم المعلوماتية في دخول ضابط شرطة قضائية أو عون شرطة قضائية إلى العالم الافتراضي (شبكة الانترنت) وذلك بتسجيله على مواقع معينة كمواقع التواصل الاجتماعي أو اشتراكه في محادثات عبر غرف الدردشة أو حلقات الاتصال المباشر لرفع ومعاينة الجرائم، أو ربط الاتصال مع المشتبه فيهم، والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أو صفات مستعارة ووهمية سعيا منه للتعرف عليهم وتحديد أماكنهم[5].

[1]–المادة 65 مكرر 15 من ق.إ.ج.ج.
[2]–المادة 65 مكرر 16 من ق.إ.ج.ج.
[3]–المادة 65 مكرر 15 فقرة3 من ق.إ.ج.ج.
[4]–المادة 65 مكرر 5 من ق.إ.ج.ج.
[5]–سعيداني نعيم، مرجع سابق، ص 177.

المبحث الثاني: الإجراءات الخاصة لمتابعة الجريمة الإلكترونية

إن سرعة ارتكاب الجريمة المعلوماتية وسهولة محو آثارها من الجاني جعلها من أصعب الجرائم للاكتشاف ولهذا استحدثت التشريعات الحديثة، ومنها التشريع الجزائري إجراءات خاصة من أجل ضبطها وتسهيل اكتشافها قبل تفاقم خطرها، ويمكن تقسيم هذه الإجراءات إلى مراقبة الاتصالات الإلكترونية (**المطلب الأول**) وحفظ المعطيات المتعلقة بحركة السير (**المطلب الثاني**).

المطلب الأول: مراقبة الاتصالات الإلكترونية

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستعان بها في البحث والتحري عن الجرائم سواء تلك التقليدية أو المستحدثة كجرائم الانترنت وهي ما يعرف بالمراقبة الإلكترونية.[1]

وقد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.[2]

من خلال هذا يتضح أن أساليب التحري الخاصة هي إجراءات خطيرة تمس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.[3]

ومن أجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 الذي طرأ عليه وفق القانون 06-22 الذي حصر وجوبية اللجوء إلى مثل هذا الإجراء على الجرائم الستة الخطيرة ومن بينها الجريمة المعلوماتية الذي أعطاها اسم "جريمة المساس بأنظمة المعالجة الآلية للمعطيات" وتتمثل هذه الأساليب في:

- اعتراض المراسلات.

---

[1] - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، المرجع السابق، ص197.

[2] – اختلف المشرع الجزائري في إعطاء مصطلح واحد للمراقبة الإلكترونية فأحيانا يقر بمصطلح المراقبة الإلكترونية كما قررها في القانون 09-04، وأحيانا أخرى بمصطلح أساليب التحري الخاصة إلا أنها نفس الإجراءات تختلف فقط في التسمية والقانون الذي قررها.

[3] – المادة 34 من دستور 1996.

- التقاط الصور.

- تسجيل الأصوات.

وهو ما سنتطرق إليه بالتفصيل في بحثنا هذا:

01-اعتراض المراسلات

يقصد بالمراسلات [1] جميع الخطابات والرسائل والطرود والبرقيات، وقد حصر المشرع الجزائري مفهوم المراسلات في تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية فقط، طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري، [2] ويكون بذلك قد استبعد المراسلات المكتوبة العادية والخطابات الخطية التي تتم عن طريق البريد العادي أو الإلكتروني.

02-تسجيل الأصوات

يقصد به مراقبة الأحاديث وتسجيلها وكل الاتصالات التي تتم عن طريق سلكي أو لاسلكي، أي أن عمليات المراقبة تشمل كل أدوات الاتصال سواء سلكية أو لاسلكية، وتتمثل في وضع تقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص.[3]

03-التقاط الصور

هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.[4]

---

[1] - المادة 39 من دستور 1996.

[2] - يقصد بالمراسلات الإلكترونية هي الخدمة التي تسمح بانتقال الرسائل المرسلة عبر نظام الرسائل الإلكترونية عن طريق شبكة إلكترونية.

[3] - المادة 65 مكرر5 و 65 مكرر 10 من قانون الإجراءات الجزائية، تعديل 2006.

[4] - المادة 65 مكرر5/ف5 من قانون الإجراءات الجزائية، تعديل 2006.

وتتم هذه الإجراءات بالسرية التامة، لأنها إجراءات تمس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا، غير أن المشروع كفلها بضمانات وضوابط أساسية سيتم التطرق إليها فيما بعد.

الفرع الأول: تعريف مراقبة الاتصالات الإلكترونية

ويقصد بها العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجميع بيانات ومعلومات عن المشتبه فيه سواء كان شخص أو مكان أو شيئا حسب طبيعته وبالتالي فمن خلال هذا التعريف يتضح لنا أن المراقبة الإلكترونية هي وسيلة حديثة تخص فقط الجريمة الإلكترونية دون غيرها، وأيضا هي من وسائل جمع البيانات والمعلومات عن المشتبه فيه.[1]

وقد عرفت المادة 03 من القانون 09-04 مراقبة الاتصالات الإلكترونية حيث تشمل الاتصالات السلكية واللاسلكية والخلوية كالفاكس والبريد الإلكتروني ومواقع الدردشة حتى المنتديات وساحات الرأي والنقاش التي تسمح بنقل الأفكار والمعلومات،[2] وهذا ليس إجراء جديد على المشرع الجزائري، فقد تعرض له خلال تعديل قانون الإجراءات الجزائية وذلك بإضافة الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان اعتراض [3] المراسلات[4] وتسجيل الأصوات والتقاط الصور.

الفرع الثاني: حالات اللجوء إلى المراقبة

لقد نص المشرع الجزائري من خلال المادة 04 من القانون 09-04 على الحالات التي بتوافرها يمكن اللجوء إلى المراقبة الإلكترونية المنصوص عليها في المادة 03 المذكورة أعلاه وتتمثل هذه الحالات في:[5]

[1] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الكمبيوتر والأنترنت، المرجع السابق، ص204.

[2] – المادة 03 من القانون 09-04.

[3] – الاعتراض هو الحصول على محتوى الاتصال السلكي أو الشفوي أو الإلكتروني.

[4] – المراسلات هي انتقال الرسائل المرسلة.

[5] – المادة 04 من القانون 09-04.

-الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

- في حالة توافر معلومات عن اتصال اعتداء على المنظومة على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تخدم الأبحاث دون اللجوء إلى مراقبة الاتصالات الإلكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

الفرع الثالث: ضوابط المراقبة الإلكترونية

حتى يكون إجراء مراقبة الاتصالات الإلكترونية صحيحا لابد أن يخضع إلى مجموعة من الإجراءات التي تحكمه وهو ما كان منصوص عليه في قانون الإجراءات الجزائية المعنون باعتراض المراسلات والتقاط الصور وتسجيل الأصوات (**أولا**)، وأخرى منصوص عليها في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (**ثانيا**).

أولا: الضوابط المنصوص عليها في قانون الإجراءات الجزائية

وهي تلك الضوابط المنصوص عليها في المادة 65 مكرر1 وما بعدها من تعديل قانون الإجراءات الجزائية الجزائري لسنة 2006، وفي حالة عدم احترامها يترتب بطلان الإجراء، وتتمثل هذه الضوابط في:

-صدور إذن من السلطة المختصة (قاضي التحقيق أو وكيل الجمهورية) لأن هذا الإجراء كما رأينا سابقا فيه مساس بحرمة الحياة الخاصة للأشخاص وإلا كان هذا الإجراء باطلا.[1]

[1] - المادة 65 مكرر5 من تعديل قانون الإجراءات الجزائية لسنة 2006.

– لابد أن يتضمن كل العناصر التي تسمح للضابط بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكينة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.[1]

–لابد أن يكون نوع الجريمة إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.[2]

–مدة الإجراء هي 04 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية.[3]

– لابد من تحرير محضر بالمعطيات التي تمت عليها العملية وأن يتضمن ذلك المحضر ساعة بداية ونهاية تلك العملية وتاريخها.[4]

ثانيا: الضوابط المنصوص عليها في القانون 09–04

نصت المادة 04 من القانون السابق ذكره على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، حيث نص المشرع الجزائري على جميع الحالات التي يجوز اللجوء إليها إلى القواعد الخاصة لقانون الإجراءات الجزائية إلى الحالة "أ" وهي حالة ما إذا كان الأمر يتعلق بأفعال موصوفة بجرائم الإرهاب والتخريب أو الماسة بأمن الدولة وتتمثل هذه الشروط في:

–الإذن: لابد من صدور إذن مكتوب من السلطة القضائية المختصة.[5]

– صدور الإذن من النائب العام لدى مجلس قضاء الجزائر العاصمة.[6]

[1] – المادة 65 مكرر7/ف1 من تعديل قانون الإجراءات الجزائية لسنة 2006.

[2] – المادة 65 مكرر5/ف1 من تعديل قانون الإجراءات الجزائية لسنة 2006.

[3] – المادة 65 مكرر7/ف2 من تعديل قانون الإجراءات الجزائية لسنة 2006.

[4] – المادة 65 مكرر9 من تعديل قانون الإجراءات الجزائية لسنة 2006.

[5] – المادة 04/ف2 من القانون 09–04.

[6] – المادة 04/ف2 من القانون 09–04.

– يباشر عملية المراقبة ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها في المادة 13 من القانون 09-04 سالف الذكر.

– تكون مدة الإذن 06 أشهر قابلة للتجديد.[1]

المطلب الثاني: حفظ المعطيات المتعلقة بحركة السير

قررت التشريعات الحديثة ومنها المشرع الجزائري إلزام مقدمي الخدمات حفظ المعطيات المتعلقة بحركة السير ضمانا للوصول إلى آثار الجريمة مهما كانت.

الفرع الأول: تعريف المعطيات المتعلقة بحركة السير

قبل التعرف على المعطيات المتعلقة بحركة السير لابد من التعرف على المقصود بمقدمي الخدمات.

فيقصد بمقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.[2]

ويقصد بالمعطيات المتعلقة بحركة السير؛ "تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتهجها تلك الأخيرة باعتبارها جزء من حلقة الاتصال توضع مصدر الاتصال، والوجهة المرسلة إليها والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة"[3]

[1] – المادة 13 من القانون 09-04.

[2] – المادة 02/ف 'د' من القانون 09-04.

[3] – المادة 02/ ف 'هـ' من القانون 09-04.

الفرع الثاني: المعطيات الواجب حفظها

لقد حدد المشرع الجزائري المعطيات التي يجب على مقدمي الخدمات حفظها،[1] فيما يلي:

-المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وكذا عناوين المواقع.

- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال وتكون مدة الحفظ لا تتجاوز سنة، وإلا تعرض مقدمي الخدمة للعقوبات المقررة في المادة 11 من القانون 09-04.

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

الفصل الثاني: إجراءات التحقيق والمحاكمة في الجريمة الإلكترونية.

تعتبر الجريمة الإلكترونية كأي جريمة من الجرائم المنصوص عليها في قانون العقوبات والقوانين الأخرى، فلذلك تتسم بالدعوى العمومية، وهذه الدعوى تتم بمراحل والتي هي عمل دراستنا، بداية بمرحلة جمع الاستدلالات كما درسنا سابقا، وصولا غلى مرحلتي التحقيق والمحاكمة.

تعد البيئة الرقمية مسرحا لارتكاب الجريمة الإلكترونية والتي تستدعي كافة الإجراءات من أجل الوصول إلى الدليل الذي لا يخلو من أي جريمة، مهما كانت طبيعتها المادية أو التقنية، كما هو الحال بالنسبة لهذا النوع المستحدث من الجرائم، الذي يقوم على الدليل الرقمي.

التحقيق في الجريمة الإلكترونية يعتبر المرحلة الثانية بعد مرحلة جمع الاستدلالات، فهو مرحلة من اختصاص قاضي التحقيق الذي يتعين بمقتضى قرار من وزارة العدل، وصولا إلى مرحلة المحاكمة وهي آخر مرحلة من مراحل الدعوى العمومية والتي تؤدي إلى انقضائها.

[1] - المادة 11 من القانون 09-04.

نقتصر في هذا الفصل على دراسة إجراءات التحقيق (المبحث الأول)، والمحاكمة في الجريمة الإلكترونية (المبحث الثاني).

المبحث الأول: إجراءات التحقيق في الجريمة الإلكترونية.

التحقيق الجنائي يحكون في جميع الجرائم التقليدية والمستحدثة، وباعتبار أن الجرائم الإلكترونية حديثة المنشأ تخضع لشخص المشتبه فيه للتحقيق من طرف السلطات المختصة.

إن عملية التحقيق الجنائي تمر بمرحلتين، المرحلة الأولى تسمى التحقيق الأولي والمرحلة الثانية تسمى التحقيق الابتدائي، المرحلة الأولى هي مرحلة جمع الاستدلالات يباشرها أعضاء الضبط القضائي، وذلك حسب المادة 12/ف3 من قانون الإجراءات الجزائية الجزائري والتي تنص بأنه: "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي"، [1] والمرحلة الثانية تدخل في اختصاص قاضي التحقيق وهذا حسب المادة 38 من نفس القانون حيث تنص على أنه: "يناط لقاضي التحقيق إجراءات البحث والتحري ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق وإلا كان ذلك الحكم باطلا".[2]

سنبين في هذا المبحث اختصاص قاضي التحقيق وكيفية اتصاله بملف الدعوى (المطلب الأول)، وسلطات قاضي التحقيق واستئناف أوامره (المطلب الثاني).

المطلب الأول: اختصاص قاضي التحقيق وكيفية اتصاله بملف الدعوى.

سنتناول في هذا المطلب اختصاص قاضي التحقيق (الفرع الأول)، وكيفية اتصاله بملف الدعوى (الفرع الثاني).

---

[1] –المادة 12 من قانون الإجراءات الجزائية الجزائري.

[2] المادة 38 من قانون الإجراءات الجزائية الجزائري.

الفرع الأول: اختصاص قاضي التحقيق.

سنتطرق إلى قواعد الاختصاص الشخصي (أولا)، ثم النعي (ثانيا)، وأخيرا المحلي (ثالثا)، لقاضي التحقيق.

أولا: الاختصاص الشخصي لقاضي التحقيق.

الأصل أن قاضي التحقيق يحقق مع جميع الأشخاص دون تمييز، إلا أن المشرع الجزائري استثنى بعض الفئات كالأحداث، العسكريين، ضباط الشرطة القضائية، قضاة الحكم والتحقيق ومساعدي وكيل الجمهورية، قضاة المجالس القضائية ورؤساء المحاكم ووكلاء الجمهورية، قضاة المحكمة العليا، ورؤساء المجالس القضائية والنواب العامون وأعضاء الحكومة والولاة.[1]

ويختص كذلك في التحقيق في جميع جرائم القانون العام سواء كانت جنائية أو جنحة أو مخالفة، التي من خلالها تقدم النيابة العامة طلب افتتاحي أو الجنايات أو الجنح التي من خلالها يقدم الطرف المدني ادعاءا مدنيا، وهذا ما جاء في المادة 67 من قانون الإجراءات الجزائية الجزائري.[2]

ثانيا: الاختصاص النوعي لقاضي التحقيق.

يختص قاضي التحقيق بالتحقيق في جميع الجرائم ويكون ذلك وجوبي في الجنايات وجوازي في الجنح إذا كان هناك نص، واختياري في المخالفات طبقا لنص المادة 66 من قانون الإجراءات الجزائية الجزائري التي تنص على مايلي: «التحقيق الابتدائي وجوبي في مواد الجنايات، أما في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة، كما يجوز إجراؤه في مواد المخالفات إذا طلبه وكيل الجمهورية»[3]

[1]-عبد الرحمن خلفي، المرجع السابق، ص 226، 228.

[2]-المادة 67 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة 66 من قانون الإجراءات الجزائية الجزائري.

إن قاضي التحقيق يختص في المحاكم الجهوية في الجرائم التي اختصها المشرع بالنظر في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب، وجرائم الصرف طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006.[1]

ثالثا: الاختصاص المحلي لقاضي التحقيق.

تنص المادة 40 من قانون الإجراءات الجزائية الجزائري "يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر..."، [2] يمتد اختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 40/ف2 من قانون الإجراءات الجزائية الجزائري.

الفرع الثاني: كيفية اتصال قاضي التحقيق بملف الدعوى.

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب افتتاحي لإجراء التحقيق، وإنما عن طريق شكوى جزائية مقدمة من طرف المضرور وهذا ما أكدته المادة 38/ف3 من قانون الإجراءات الجزائية الجزائري حيث نصت على: «...يختص بالتحقيق في الحادث بناءا على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و73»[3]

[1]-المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المتعلق بتحديد الاختصاص الإقليمي لبعض المحاكم والوكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية، العدد63.

[2]-المادة 40 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة 38/ف3 من قانون الإجراءات الجزائية الجزائري.

سنتناول في هذا العنصر كيفية اتصال قاضي التحقيق بالدعوى العمومية، وهذا يكون إما عن طريق وكيل الجمهورية بموجب طلب افتتاحي لإجراء التحقيق (أولا)، وإما عن طريق شكوى مصحوبة بإدعاء مدني من طرف المتضرر من الجريمة (ثانيا).

أولا: الطلب الافتتاحي لإجراء التحقيق.

يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن له أن يطلب فتح تحقيق، ما لم ينص القانون على وجوب التحقيق في بعض الجنح؛ ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا ظهرت وقائع جديدة طبقا للمادة 67/ف3 من قانون الإجراءات الجزائية الجزائري حيث نصت على انه: "لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها".[1]

وبتقييد قاضي التحقيق بالوقائع دون الأشخاص طبقا للمادة 67/ف3و4 من قانون الإجراءات الجزائية الجزائري حيث تنص على مايلي: "...ولقاضي التحقيق سلطة اتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه.

فإذا وصلت علم قاض التحقيق وقائع لم يشر إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع".[2]

ثانيا: الشكوى المصحوبة بإدعاء مدني.

تنص المادة 72 من قانون الإجراءات الجزائية الجزائري "يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص".[3]

[1]-المادة 67/ف3 من قانون الإجراءات الجزائية الجزائري.

[2]-المادة 67/ف3و 4 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة72 من قانون الإجراءات الجزائية الجزائري.

إن إحدى طرق تحريك الدعوى من طرف الأفراد، هي في نفس الوقت إحدى طرق اتصال قاضي التحقيق بملف الدعوى، ويلجأ المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصها للوقت، وحرصا منه على أن يكون الإشراف على الملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية القضائية التي عادة يكون لها تأثير على مجرى التحقيق، كما أن يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها، إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء استعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية الكاذبة إذا ما خسر دعواه، ولهذا عليه أن يتأكد من أن اتهامه كان مبنيا على دليل قوي في الدعوى.[1]

المطلب الثاني: سلطات قاضي التحقيق واستئناف أوامره.

خصصنا هذا المطلب لدراسة سلطات قاضي التحقيق (الفرع الأول)، بالإضافة إلى الجهات التي تستأنف أوامره (الفرع الثاني).

الفرع الأول: سلطات قاضي التحقيق وحدود الدعوى الجنائية أمامه.

القيام باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، وبالتحري عن أدلة الاتهام وأدلة النفي طبقا للمدة 68/ف1 من قانون الإجراءات الجزائية الجزائري.[2]

يجوز لقاضي التحقيق أن يأمر بإجراء فحص طبي، كما له أن يعهد إلى الطبيب بإجراء فحص نفساني أو يأمر باتخاذ أي إجراء يراه مفيدا طبقا للمادة 68/ف8 من قانون الإجراءات الجزائية الجزائري.[3]

[1]-عبد الرحمن خلفي، المرجع السابق، ص 231، 233.

[2]-المادة 68/ف1 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة 68/ف8 من قانون الإجراءات الجزائية الجزائري.

ينسق القاضي المكلف بالتحقيق سير إجراءات التحقيق وله وحده الصفة في مسائل الرقابة القضائية والحبس المؤقت اتخاذ أوامر التصرف في القضية طبقا لنص المادة 70/ف3 من قانون الإجراءات الجزائية الجزائري.[1]

يستطيع القاضي سماع كل من يشير إليهم في الشكوى باعتبارهم شهودا طبقا لنص المادة 73/ف5 من قانون الإجراءات الجزائية الجزائري.[2]

استدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية طبقا لنص المادة 88/ف1 من قانون الإجراءات الجزائية الجزائري.[3]

يجوز لقاضي استدعاء مترجم طبقا لنص المادة 91 من قانون الإجراءات الجزائية الجزائري،[4] إصدار أمر بإحضار المتهم أو بإيداعه السجن أو بإلقاء القبض عليه حسب نص المادة 109 من قانون الإجراءات الجزائية الجزائري.[5]

تفتيش المتهم، وتفتيش المسكن غير مسكن المتهم، ومراقبة المحادثات السلكية واللاسلكية، وضبط الخطابات والرسائل والجرائد والطرود والمطبوعات والبرقيات لدى مكاتب البريد والبرق حسب نص المادة 91 و94 و95 من قانون الإجراءات الجزائية المصري.[6]

وأيضا هناك سمات خاصة يتميز بها قاضي التحقيق بالنسبة للجريمة الإلكترونية لكونها تختلف عن الجريمة التقليدية، فلذلك لا يمكن أن يحقق فيها أي قاضي تحقيق، وإنما لابد أن يكون لها صفات خاصة؛ كان يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، وان يميل إلى

[1]–المادة 70/ف3 من قانون الإجراءات الجزائية الجزائري.

[2]–المادة 73/ف5 من قانون الإجراءات الجزائية الجزائري.

[3]–المادة 88/ف1 من قانون الإجراءات الجزائية الجزائري.

[4]–المادة 91 من قانون الإجراءات الجزائية الجزائري.

[5]–المادة 109 من قانون الإجراءات الجزائية الجزائري.

[6]–المواد 91 و94 و95 من قانون الإجراءات الجزائية المصري رقم 189 لسنة 2020، المؤرخ في 5 سبتمبر 2020 المعدل والمتمم للقانون رقم 150 لسنة 1950.

تصميم البرامج أكثر من تشغيلها وأن يستطيع تحليل وتصميم البرامج أو لأنظمة التشغيل بسرعة وان يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة، وكل هذه الأمور لا تتوافر إلا لمن كان لديه إمكانيات عقلية تزيد على متوسط العام المألوف.[1]

الفرع الثاني: استئناف أو أمر قاضي التحقيق.

الجهات التي تستأنف أوامر قاضي التحقيق هي النيابة العامة (أولا)، المتهم (ثانيا)، أو المدعي المدني (ثالثا).

أولا: النيابة العامة.

لوكيل الجمهورية أو أحد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري "لوكيل الجمهورية الحق في أن يستأنف أمام غرفة الاتهام جميع أوامر قاضي التحقيق.

ويكون هذا الاستئناف بتقرير أمانة ضبط المحكمة، ويجب أن يرفع في ثلاثة أيام من تاريخ صدور الأمر...".[2]

يجوز للنائب العام الطعن في أوامر القاضي التحقيق في ظرف 20 يوم على أن لا يكون لهذا الطعن أثر موقف في حالة استئناف أمر الإفراج، ويفرج على المتهم رغم استئناف النائب، طبقا للمادة 171 من قانون الإجراءات الجزائية الجزائري "يحق الاستئناف أيضا للنائب العام في جميع الأحوال أن يبلغ استئنافهم للخصوص خلال العشرين يوما التالية لصدور أمر قاضي التحقيق ولا يوقف هذا الميعاد ولا رفع الاستئناف تنفيذا الأمر بالإفراج".[3]

[1]-عبد الرحمن خلفي، المرجع السابق، ص 231.

[2]-المادة 170 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة 171 من قانون الإجراءات الجزائية الجزائري.

ثانيا: استئناف المتهم.

إن المتهم لا يجوز له استئناف جميع أوامر قاضي التحقيق، ويرفع الاستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة (3) أيام من تبليغ الأمر إلى المتهم طبقا للمادة 172 من قانون الإجراءات الجزائية الجزائري.[1]

ثالثا: استئناف المدعي العام.

كما أجاز المشرع الجزائري للمدعي المدني الحق في استئناف أوامر قاضي التحقيق التي لهالا علاقة بالعقوبة المدنية، وبمفهوم المخالفة لا يجوز له استئناف الأوامر المتملقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية، ويرع الاستئناف خلال ثلاثة (3) أيام من تاريخ تبليغ الأمر المراد استئنافه إلى المدعي المدني وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا لنص المادة 173 من قانون الإجراءات الجزائية الجزائري.[2]

المبحث الثاني: إجراءات المحاكمة في الجريمة الإلكترونية.

تطرقنا في العناصر السابقة إلى كل من أعمال الضبطية وسلطاتهم الاستثنائية في البحث والتحري عن الجريمة المعلوماتية والإجراءات العامة والخاصة لضبطها واكتشافها، وكذا سلطات قاضي التحقيق في مجال الجريمة الإلكترونية حيث من المؤكد أن القضية (الجريمة الإلكترونية) لا يمكن بأي حال من الأحوال أن تبقى حبيسة أو رهينة التحقيق والتحريات، إذ لابد لها أن تدخل في مرحلة جديدة لتصل إلى أروقة المحاكم التي تختص بمحاكمة أو متابعة مرتكبي الجريمة الإلكترونية، وبالتالي وجود جاز قضائي من أجل محاكمة هؤلاء المجرمين يختص بالفصل في نوع معين من الجرائم وذلك نظرا لخطورتها، وهو ما سنتناوله في هذا المبحث، بداية باختصاص المحكمة وتشكيلتها (**المطلب الأول**)، وصولا إلى الإجراءات والقواعد العامة للمحاكمة (**المطلب الثاني**).

[1]–المادة 172 من قانون الإجراءات الجزائية الجزائري.

[2]–المادة 173 من قانون الإجراءات الجزائية الجزائري.

المطلب الأول: اختصاص المحكمة وتشكيلتها.

أما الطبيعة الخاصة التي تمتاز بها الجريمة الإلكترونية والخصوصيات المتعددة التي تحيط بها – ولعل أهمها اعتبارها جريمة عابرة للحدود–، جعلها تستعصي على القواعد التي تحكم مسألة الاختصاص المكاني، التي تخضع لها الجرائم التقليدية، فطابعها الافتراضي يجعلها لا تتلاءم مع معيار محل وقوع الجرم الذي يتم اعتماده لتمديد المحكمة المختصة.[1]

بالإضافة إلى الاختصاص النوعي الذي يتحدد تبعا لنوع الجريمة التي ينظر فيها، وهذا ما سنتناوله في (الفرع الأول)، ثم التطرق إلى تشكيلة المحكمة (الفرع الثاني).

الفرع الأول: اختصاص المحكمة.

تم النص في قانون الإجراءات الجزئية المعدل في المواد 37، 40؟، 329 منه على توسيع الاختصاص المحلي لكل من وكيل الجمهورية وقاضي التحقيق وكذا المحكمة إلى دائرة اختصاص المحاكم الأخرى تحدد عن طريق التنظيم وذلك بخصوص، جرائم مذكورة على سبيل الحصر، ومن بينها الجريمة الإلكترونية (أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات) موضوع بحثنا هذا، حيث تم إنشاء محاكم أو أقطاب جزائية متخصصة ذات اختصاص إقليمي ومحلي موسع وهو ما سنعرضه من خلال الاختصاص المحلي (أولا) والاختصاص النوعي (ثانيا).

أولا: الاختصاص الإقليمي (المحلي) في الجريمة الإلكترونية.

تتميز الأقطاب الجزائية المتخصصة بأنها ذات اختصا محلي موسع طبقا القانون الإجراءات الجزائية،[2] فقد تم تمديد الاختصاص المحل لوكيل الجمهورية وقضاة التحقيق.

[1]–أحمد أسامة حسنية، المرجع السابق، ص 296.

[2]–أنظر المواد 37، 40، 329 من قانون الإجراءات الجزائية الجزائري.

وبصدور المرسوم التنفيذي رقم 06-348[1] والذي تم بموجب تحديد وتعيين المحاكم ذات الاختصاص الإقليمي الموسع وكذا الجهات القضائية لهذه المحاكم، حيث تم تحديد هذه المحاكم كما يلي:

1-القطب الجزائي بالجزائر (سيدي محمد) ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، شلف، الأغواط، البلدية، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس؛ [2] أي عشر مجالس قضائية.

2-القطب الجزائي بقسنطينة يمتد اختصاصه المحلي ليشمل المجالس القضائية التالية: قسنطية، أم البواقي، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، وبرج بوعريريج؛ [3] أي 12 مجلس قضائي.

3-القطب الجزائي بوهران ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية: وهران، بشار، تلمسان، سعيدة، سيدي بلعباس، مستغانم، معسكر، غليزان؛[4] أي تسع مجالس قضائية.

4-القطب الجزائي بورقلة، ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية: ورقلة، أدرار، تمنراست، إيليزي، غرداية؛[5] أي خمس مجالس قضائية.

ويتضح مما سبق أن الاختصاص الإقليمي الموسع للقطب الجزائي المتخصص يشمل جميع مراحل الدعوى العمومية ابتداء من جمع الاستدلالات إلى المحاكمة.

وفي نطاق الجرائم الإلكترونية، فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس، وتتحقق النتيجة بتدمير المعلومات في مكان آخر، فإن

[1]-المرسوم التنفيذي رقم 06-348.
[2]-المادة 02 من المرسوم التنفيذي 06-348.
[3]-المادة 03 من المرسوم التنفيذي 06-348.
[4]-المادة 05 من المرسوم التنفيذي 06-348.
[5]-المادة 04 من المرسوم التنفيذي 06-348.

الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، وتعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الانترنت جريمة مستمرة، حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها.[1]

ومتى كانت الجريمة الإلكترونية، أيا كان نوعها، فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم المعلوماتية أو المتصلة بتكنولوجيا الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني، أو إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.[2]

ثانيا: الاختصاص النوعي في الجريمة الإلكترونية.

يتحدد الاختصاص النوعي للمحكمة بالفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في افصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من ق.إ.ج.ج، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 من ق.إ.ج.ج.[3]

ولأن الطبيعة التقنية المعقدة للجرائم الإلكترونية تفرض على رجال القضاء تكوين يمكنهم من متابعة هذه الجرائم، فقد خصصها المشرع مع بعض أنواع الجرائم المتعلقة بالتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة، إذا جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى وهذا ما نصت عليه المواد 37 و40، والمادة 329 من قانون الإجراءات الجزائية الجزائري إثر التعديل

[1]-عبد الرحمن خلفي، المرجع السابق، ص 319.

[2]-المادة 05 من القانون 09-04.

[3]-المادة 328 من قانون الإجراءات الجزائية الجزائري.

الذي جاء به القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من: الجزائر العاصمة، قسنطينة، وهران، ورقلة.[1]

الفرع الثاني: تشكيلة المحكمة.

تختلف المحكمة الجزائية بحسب قسم ونوع كل جريمة، فقسم الجنح على مستوى المحكمة يتشكل من قاضي فرد ويساعده كاتب ضبط وبحضور وكيل الجمهورية أو أحد مساعديه.[2]

أما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فيها ثلاثية، أي تتشكل من رئيس الغرفة ومستشارين اثنين بالإضافة إلى كاتب الضبط وبحضور النائب العام لوحده أو أحد مساعديه.[3]

أما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة أو من يمثلها.[4]

المطلب الثاني: الإجراءات والقواعد العامة للمحاكمة.

سنتناول في هذا العنصر إجراءات المحاكمة (الفرع الأول)، بالإضافة إلى القواعد العامة للمحاكمة (الفرع الثاني).

[1]-المواد 37، 40، 329، من القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004.

[2]-المادة 30 من قانون الإجراءات الجزائية الجزائري.

[3]-المادة 30 من قانون الإجراءات الجزائية الجزائري.

[4]-المادة 258 من قانون الإجراءات الجزائية الجزائري.

الفرع الأول: إجراءات المحاكمة.

تستهل المحكمة جلستها بالإعلان أولا على افتتاحها بالقول: "باسم الشعب الجزائري الجلسة المفتوحة"، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها.[1]

وإذا كانت الدعوى غير مهيأة للحكم، أمرت المحكمة بتأجيلها إلى أقرب جلسة، وفي هذه الحالة طبقا لأحكام المادة 339 مكرر6 المستحدثة بموجب الأمر 15-02 المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية الجزائري،[2] تتخذ المحكمة إحدى الإجراءات التالية:

1-ترك المتهم حرا.

2-إخضاع المتهم لتدبير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر1 من قانون الإجراءات الجزائية الجزائري.

3-وضع المتهم في الحبس المؤقت.

مع الإشارة إلى أنه لا يجوز الاستئناف في الأوامر التي تصدرها المحكمة وفقا لهذه المادة.

إذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت بموجب إجراء المثول الفوري، فإنه يساق بواسطة القوة العمومية لحضور الجلسة، ويخطره رئيس الجلسة بأن له الحق في اختيار محام للدفاع عنه، فإن طلب ذلك أمهله القاضي مهلة لا تقل عن ثلاثة (03)

[1]-عبد الرحمن خلفي، المرجع السابق، ص 321.

[2]-المادة 339 مكرر6، المستحدثة بموجب الأمر 05-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر 66-155 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 40.

أيام لتحضيره دفاعه طبقا للمادة 339 مكرر 5 من الأمر 15-02 المعدل والمتمم لقانون الإجراءات الجزائية.[1]

ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم مناقشتها من طرف القاضي، وبعدها يقوم القاضي بسماع الشهود.

وبعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية، لتقوم النيابة العامة بعد ذلك بالمرافعة وتقديم التماساتها في الشق الجزائي فقط، وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم التماساتها، ويكون بعدها للنيابة العامة والمدعي الحق في الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه، ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق منطق بالحكم.[2]

الفرع الثاني: القواعد العامة للمحاكمة.

تنفيذ المحاكمة بمجموعة من المبادئ تنطبق على المحكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية، سنحاول شرحها بداية بعلانية الجلسة (أولا)، شفوية المرافعات (ثانيا)، حضور أطراف الخصومة (ثالثا)، ثم تدوين التحقيق النهائي (رابعا).

أولا: علانية الجلسة.

جل التشريعات تقر بمبدأ علانية الجلسة، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة، ومنه الاطمئنان والشعور بالعدالة وهذا عكس التحقيق الأولي الذي يقوم به ضباط الشرطة القضائية، وكذا التحقيق الابتدائي الذي تقوم به جهات التحقيق، فكلاهما يتم في سرية، إلا أن العلانية ليست في جميع الجلسات، بل للقاضي السلطة التقديرية لإخراج القصر من

[1]-المادة 339 مكرر5 من الأمر 15-02.

[2]-المادة 304 من قانون الإجراءات الجزائية الجزائري.

الجلسة، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على النظام العام والآداب العامة، إلا أن الحكم يجب أن يصدر في جلسة علنية، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري.[1]

ثانيا: شفوية المرافعات.

لأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة، حتى يتمكن الجميع من الدفاع عن نفسه، ولا يتم الاكتفاء بالتحقيقات الأولية والابتدائية التي سبقت المحاكمة.[2]

وبعبارة أخرى يجب أن تكون المرافعات لمحمل الوقائع علنا وشفاهية، فيقرر قانون الإجراءات الجزائية أن تكون المرافعات شفوية أمام القاضي الجزائي، فالأصل في المرافعات أن تتم شفاهة، فيقدم الخصوم طلباتهم فتناقش شفاهة وعلنا عملا بالأحكام الواردة في المواد 233، 287، 288، 289، 304، 333، 353 من قانون الإجراءات الجزائية الجزائري ، فتنص مثلا المادة 304 من قانون الإجراءات الجزائية الجزائري: "متى انتهى التحقيق بالجلسة سمعت أقوال المدعي المدني أو محاميه"، "وتبدي النيابة طلباتها"، "ويعرض المحامي والمتهم أوجه الدفاع ويسمح للمدعي المدني والنيابة العامة بالرد، ولكن الكلمة الأخيرة للمتهم ومحاميه دائما".[3]

ثالثا: حضور أطراف الخصومة.

لا يجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم، أما بالنسبة للنيابة فهي جزء من التشكيلة.[4]

[1]-المادة 285 من قانون الإجراءات الجزائية الجزائري.

[2]-عبد الرحمن خلفي، المرجع السابق، ص 323-324.

[3]-المواد 233، 287، 288، 289، 304، 333، 353 من قانون الإجراءات الجزائية الجزائري.

[4]-عبد الرحمن خلفي، المرجع السابق، ص 324.

ويقرر القانون لأطراف القضية حق الحضور، تمكينا لهم من إبداء أوجه دفاعهم أمام الجهة القضائية المختصة، كرسته مجموعة من النصوص في قانون الإجراءات الجزائية، ومنها المواد 287، 288، 289، 290، 294، 296، 343، 344، 345، 347، 348، 349، 351، 353، 355، 407.[1]

رابعا: تدوين التحقيق النهائي.

لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دوره يتجسد في تدوين كل ما يدور بالجلسة.[2]

حيث يقوم كاتب الضبط بالهيئة الجزائية أو أمين الضبط وجوبا بتحضير محضر الجلسة، يدون فيه جميع الإجراءات التي تتم فيها، ويوقع عليه طبقا لأحكام المواد 257، 314، 340، 380، 429 من قانون الإجراءات الجزائية الجزائري، لتتاح للقاضي الجزائي أو هيئة القضاء الجزائي التفرغ كليا لإدارة الجلسة وجمع المعلومات والسماع للمرافعات التي من شأنها أن تتيح له أو لهم تكوين اقتناعهم وإصدار الأحكام على ضوء ما اقتنعوا به.[3]

وفي الأخير نستنتج أن الجريمة الإلكترونية لم يخصص لها إجراءات محاكمة خاصة بها وإنما تخضع لنفس إجراءات الجريمة التقليدية.

[1]-لمزيد من التفاصيل ينظر المواد: 287، 288، 289، 290، 294، 296، 343، 344، 345، 347، 348، 349، 351، 353، 355، 407 من قانون الإجراءات الجزائية الجزائري.

[2]-عبد الرحمان خلفي، المرجع السابق، ص 325.

[3]-لمزيد من التفاصيل ينظر المواد: 257، 314، 340، 380، 429 من قانون الإجراءات الجزائية الجزائري.

خلاصة الباب:

وفي الأخير وبعدما تناولنا في هذا الباب الإطار الإجرائي للجريمة الإلكترونية، حيث بينا الإجراءات العامة التي تخضع لها الجريمة الإلكترونية والتي تشترك فيها مع الجريمة التقليدية نوعا ما في مرحلة جمع الاستدلالات، حيث قسمناها إلى إجراءات مادية تقتصر فقط على المعاينة التقنية والتفتيش المعلوماتي الذي يخضع تارة إلى أحكام قانون الإجراءات الجزائية (المكونات المادية)، وتارة أخرى قانون 09-04 (المكونات المعنوية)، وأخرى شخصية تتمثل في الخبرة، وشهادة شاهد إلكتروني، والتسرب وهو من أساليب التحري الخاصة، التي جاء بها تعديل قانون الإجراءات الجزائية، والذي قرر هذا الأخير إلا على الجرائم الخطيرة.

وإجراءات خاصة لا تطبق إلا على الجرائم الموصوفة بالخطيرة، والتي من بينها الجرائم الإلكترونية، وتتمثل في مراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير والتي جاء بها القانون 09-04، وهذا كله أثناء مرحلة البحث والتحري في الجريمة الإلكترونية.

أما أثناء التحقيق الابتدائي أو القضائي فقد عرفت الجريمة الإلكترونية في هذا المجال خصوصية خاصة من حيث اختصاصات قاضي التحقيق سواء كان الاختصاص المحلي (لكونها جريمة عابرة للحدود الدولية)، أو الاختصاص النوعي، وأيضا كيفية اتصاله بملف الدعوى، بالإضافة إلى تحديد سلطات قاضي التحقيق والسمات التي يتميز بها في مجال الجريمة الإلكترونية وكذا استئناف أوامره.

ونظرا للخصوصيات التي تتميز بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتطورها السريع والمستمر، جعل من الدول ومنها الجزائر إلى وضع آلية قانونية جديدة للحد من خطورة هذه الجريمة على المجتمع ككل من خلال تمديد الاختصاص المحلي لبعض المحاكم لقضاة التحقيق، ووكيل الجمهورية من خلال آلية قضائية جديدة تعرف بالقطب الجزائي المتخصص، من خلال

عرض وجيز لاختصاص هذه الأقطاب الجزائية سواء كان اختصاص نوعي أي تخص في نوع معين من الجرائم محددة على سبيل الحصر ومنة بينها الجريمة الإلكترونية طبقا لنص المادة 37 من قانون الإجراءات الجزائية الجزائري، وكذا توسيع اختصاصها المحلي ليشمل بعض المجالس القضائية، وحددها في أربعة أقطاب فقط طبقا للمرسوم التنفيذي رقم 06-348، بالإضافة إلى تبيان تشكيلة المحكمة وعرض الإجراءات والقواعد العامة للمحاكمة.

خاتمة

خاتمة:

حاولنا من خلال دراساتنا لهذا الموضوع الإلمام بالجوانب القانونية للجريمة الإلكترونية في شقيها الموضوعي والإجرائي، حيث ميزنا بينها وبين الجريمة التقليدية، مستندين في ذلك على تعديل قانون العقوبات بموجب القانون 14-15 والقانون 09-04 المتعلق بالوقاية من الجرائم لمتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى قانون الإجراءات الجزائية.

ولاشك أن هذه القوانين كانت لها أهمية كبرية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري، كما أن هذا التعديل يعد قفزة في مجال التشريع، كونه واكب التشريعات المقارنة بتجسيده معظم أحكام الاتفاقية الدولية للإجرام المعلوماتي.

مما سبق يمكن القول أن الجريمة الإلكترونية هي وليدة الثروة المعلوماتية والتكنولوجية، حيث لم تسلم منها كل دول العالم المتطورة كانت أو النامية على حد سواء، مما جعل الجريمة الإلكترونية متميزة عن الجريمة التقليدية من حيث تسميتها وتعريفها وخصائصها وكذا الأركان التي تقوم عليها وصولا إلى الإجراءات المتابعة فيها.

ومما سبق ذكره استخلصنا من البحث مجموعة من النتائج يمكن إجمالها فيايلي:

*/عدم وجود تعريف جامع مانع للجريمة الإلكترونية، حيث اختلفت التعريفات بين المفهوم الواسع والمفهوم الضيق.

*/عدم وجود مصطلح موحد للجريمة الإلكترونية، فهناك من يسميها الجريمة المعلوماتية أو السيبرانية، أو جريمة الياقات البيضاء، أو جريمة الانترنت...إلخ، حتى المشرع الجزائري نجده لم يستقر على تسمية واحدة، حيث سماها طبقا للقانون 04-15 بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال طبقا للقانون 09-04، ورغم هذه الاختلافات إلا أنها كلها تصب في معنى واحد.

*/الجرائم الإلكترونية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق، ويتصف المجرم المعلومات فيها بالذكاء والسرعة والدقة والتخصص في مجال تكنولوجيا المعلومات.

*/رغم كل الاختلافات بينها وبين الجريمة التقليدية إلا أنها تتوافق معها في مدى توفر القصد الجنائي العام.

*/رغم اجتهاد وتدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام الإلكتروني، إلا أنه لم يستطع التصدي لهذه الجريمة.

*/ لم يخصص المشرع الجزائري قانون خاص قائم بذاته للتحكم في هذه الجريمة وحسن سيرها.

*/تتميز الجرائم الإلكترونية كغيرها من الجرائم التقليدية بالخطورة لكونها تمس الإنسان والمؤسسات وتتعداها حتى لتكون خطر على أمن الدولة، نظرا لطبيعتها المتعدية للحدود لارتباطها بشكة الانترنت، كما تتميز بكونها تعتمد على التقنيات الحديثة، وصعوبة اكتشافها وإثباتها.

*/الشاهد في الجريمة الإلكترونية شخص فني، صاحب خبرة وتخصص في مجال التقنية الحديثة وعلوم الحاسوب، كمشغلو الحاسب الآلي وخبراء البرمجة.

*/عجز قواعد الإجراءات الجزائية والنصوص العقابية التقليدية وقصورها عن مواجهة الجرائم الإلكترونية والمجرم الإلكتروني.

*/إن التفتيش كإجراء تحقيقي تعتريه صعوبات كثيرة عملية وقانونية، نتيجة تعدد أماكن ارتكاب الفعل الجرمي والطابع الغير مرئي للأدلة الإلكترونية.

وفي ضوء النتائج التي أظهرتها الدراسة نستخلص بعض التوصيات والاقتراحات تتمثل في:

*/ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل فيه كل السلوكات المجرمة.

*/لابد من تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم الإلكترونية، أو إصدار قانون خاص بالجرائم الإلكترونية وكطرق مكافحتها.

*/ضرورة تخصيص شرطة جنائية خاصة بجرائم الانترنت، مع تكوين لجان خبراء لهذا الشأن.

*/تعزيز التعاون الدولي والمساعدة الوطنية والدولية في مجال مكافحة الجرائم الإلكترونية.

*/ضرورة تسجيل أسماء الأشخاص الذين يستخدمون الشبكة في مقاهي الانترنت، والمدة التي استغرقوها.

*/ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع المستحدث من الجرائم، بالتعاون مع التقنيين وأصحاب الخبرة.

*/وضع إجراءات خاصة للتحقيق والمحاكمة في الجريمة الإلكترونية تختلف عن الجريمة التقليدية.

*/توعية المجتمع، وخلق له ثقافة اجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبها لعقوبات جزائية.

*/إعادة النظر في مدى تطبيق القوانين من عدمه.

*/الأخذ بالتجارب السابقة بالنسبة للدول المتطورة، والتي ساهمت بشكل كبير في محاربة الجريمة الإلكترونية كالولايات المتحدة الأمريكية وكندا.

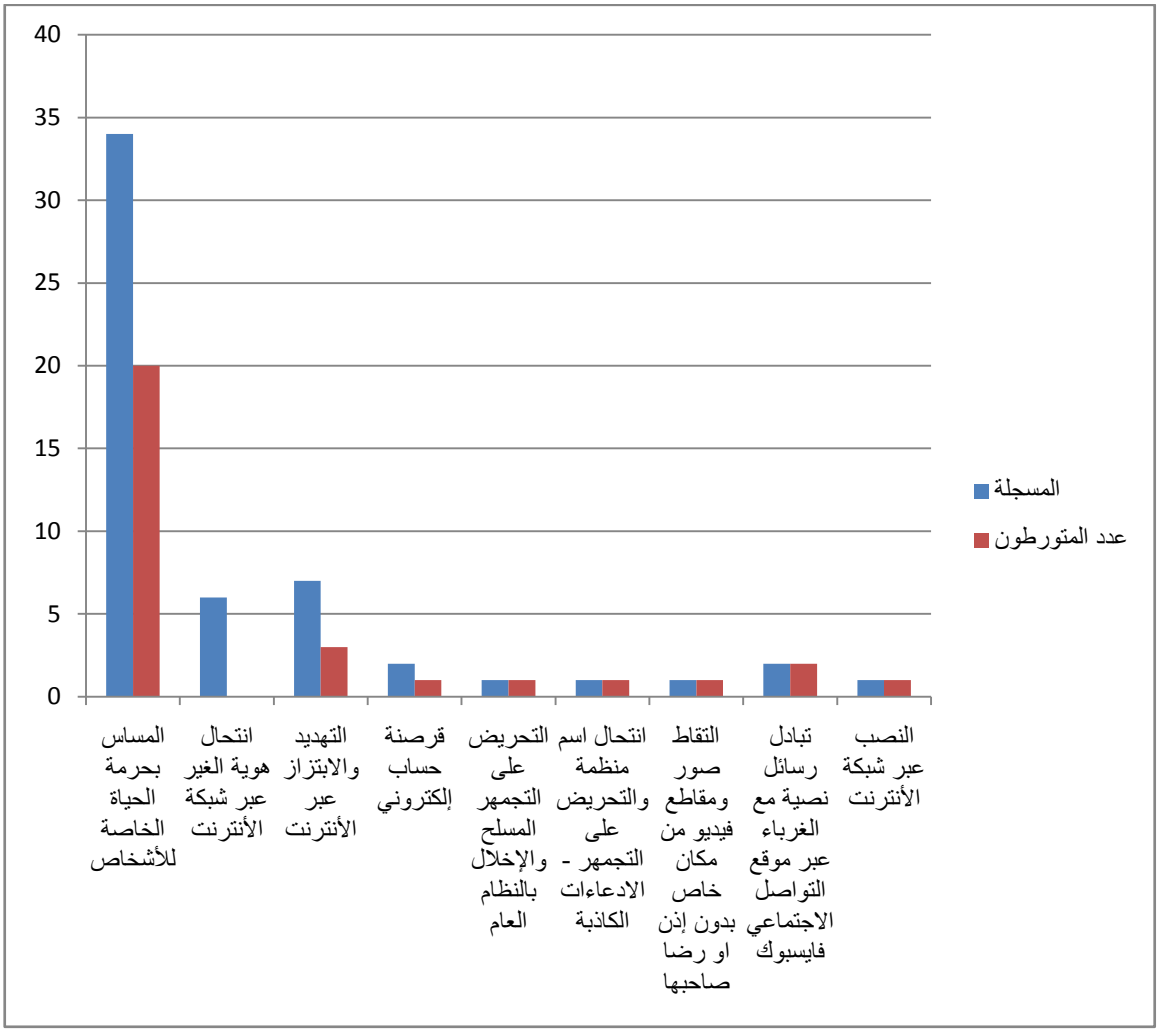
الملاحق

الملحق رقم 01: القضايا المسجلة خلال سنة 2017

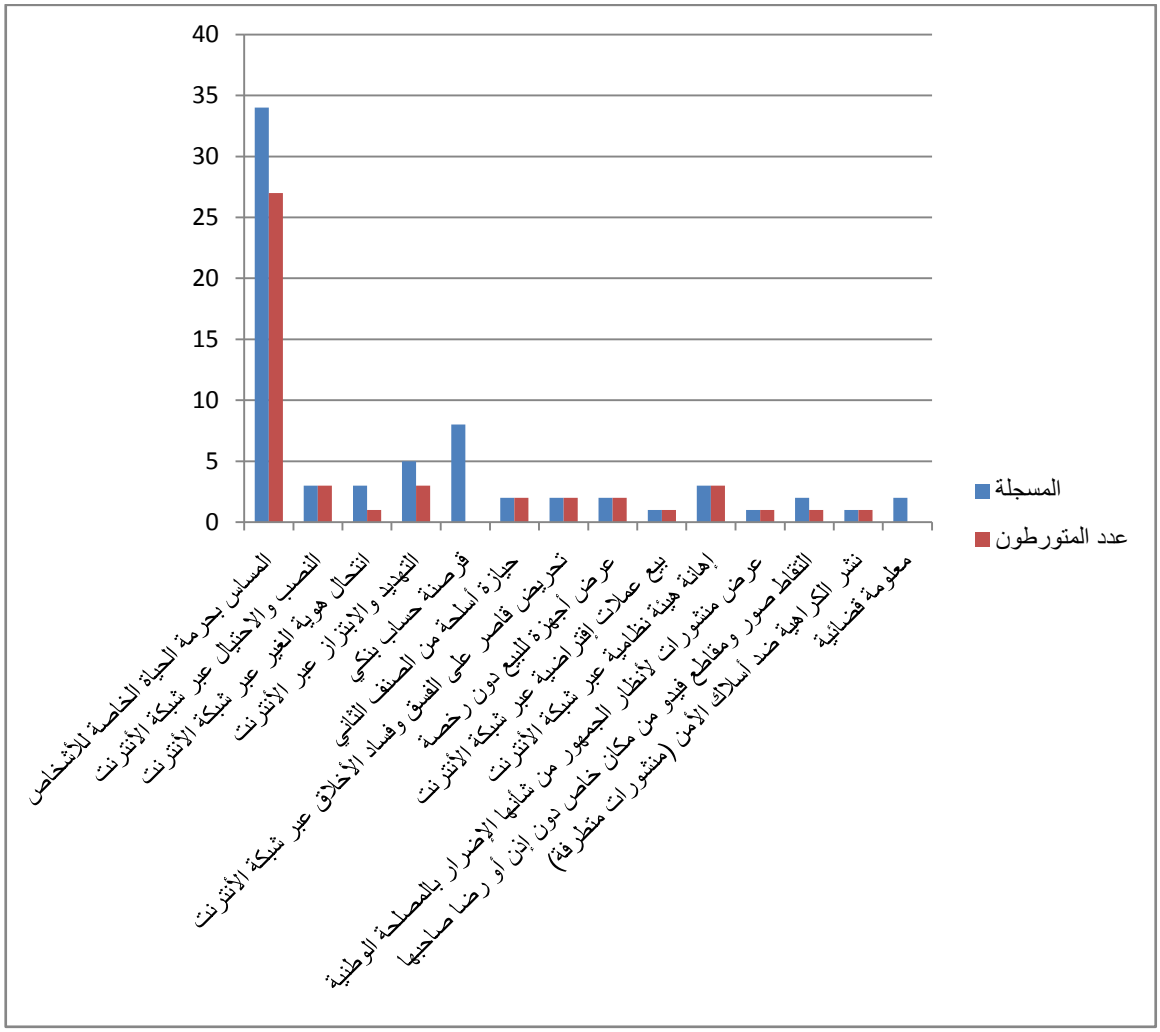
طبيعة الجريمة	المسجلة	عدد المتورطون
المساس بحرمة الحياة الخاصة للأشخاص	34	20
انتحال هوية الغير عبر شبكة الأنترنت	6	
التهديد والابتزاز عبر الأنترنت	7	3
قرصنة حساب إلكتروني	2	1
التحريض على التجمهر المسلح والإخلال بالنظام العام	1	1
انتحال اسم منظمة والتحريض على التجمهر –الادعاءات الكاذبة	1	1
التقاط صور ومقاطع فيديو من مكان خاص بدون إذن او رضا صاحبها	1	1
تبادل رسائل نصية مع الغرباء عبر موقع التواصل الاجتماعي فايسبوك	2	2
النصب عبر شبكة الأنترنت	1	1

من خلال الإحصائيات المذكورة في الجدول أعلاه يتبين لنا أن الجرائم الإلكترونية في سنة 2017 كانت قليلة نوعا ما فقد بلغت على المستوى المحلي –ولاية تيارت– حوالي 55 قضية مسجلة عند مصالح الشرطة القضائية وأغلبها جرائم المساس بحرمة الحياة الخاصة للأشخاص فقد بلغت أكثر من 80 % وهذا ما يوضحه التمثيل البياني أدناه –الملحق رقم 02–.

الملحق رقم 02: القضايا المسجلة خلال سنة 2017



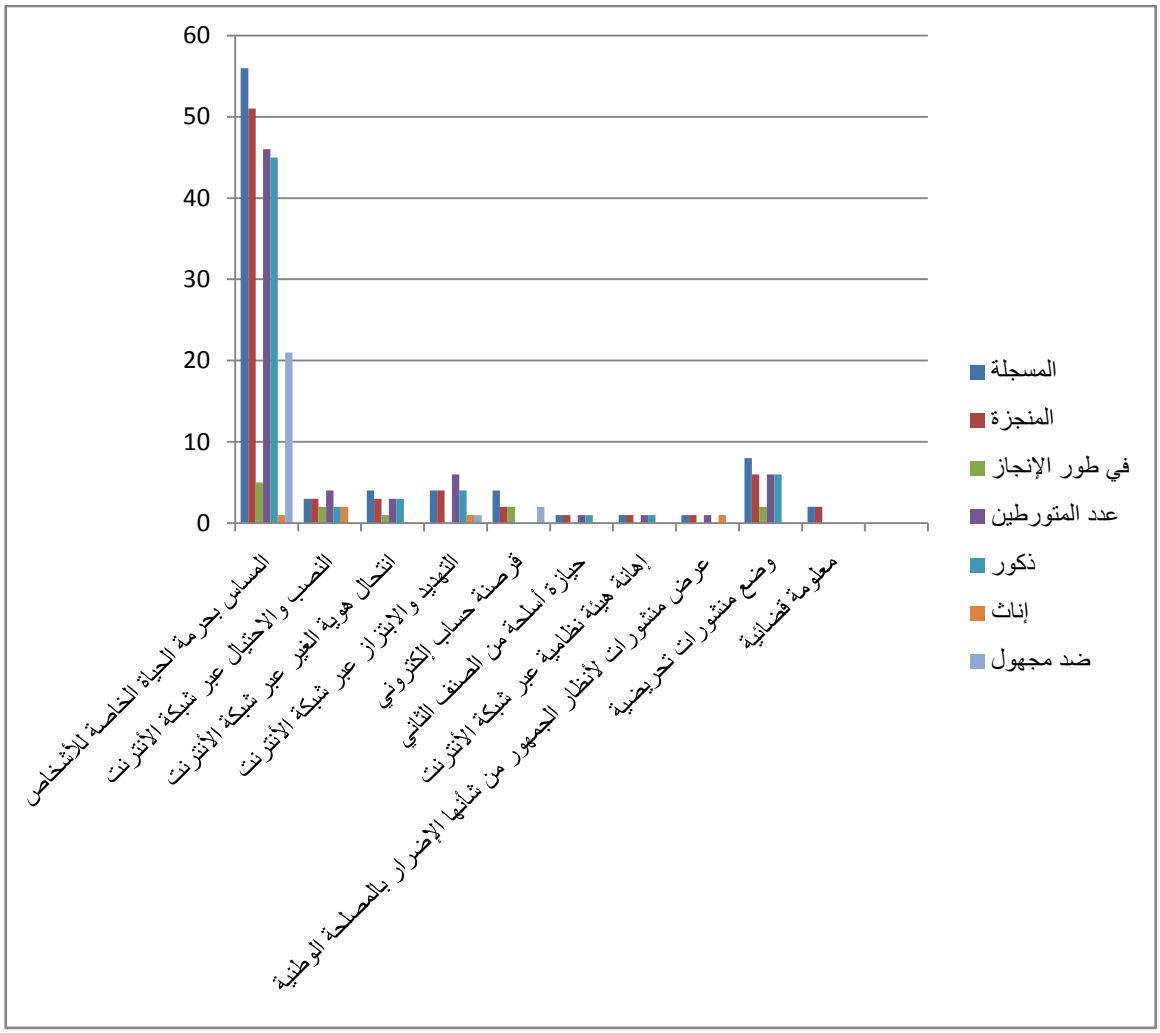
الملحق رقم 03: القضايا المسجلة خلال سنة 2018



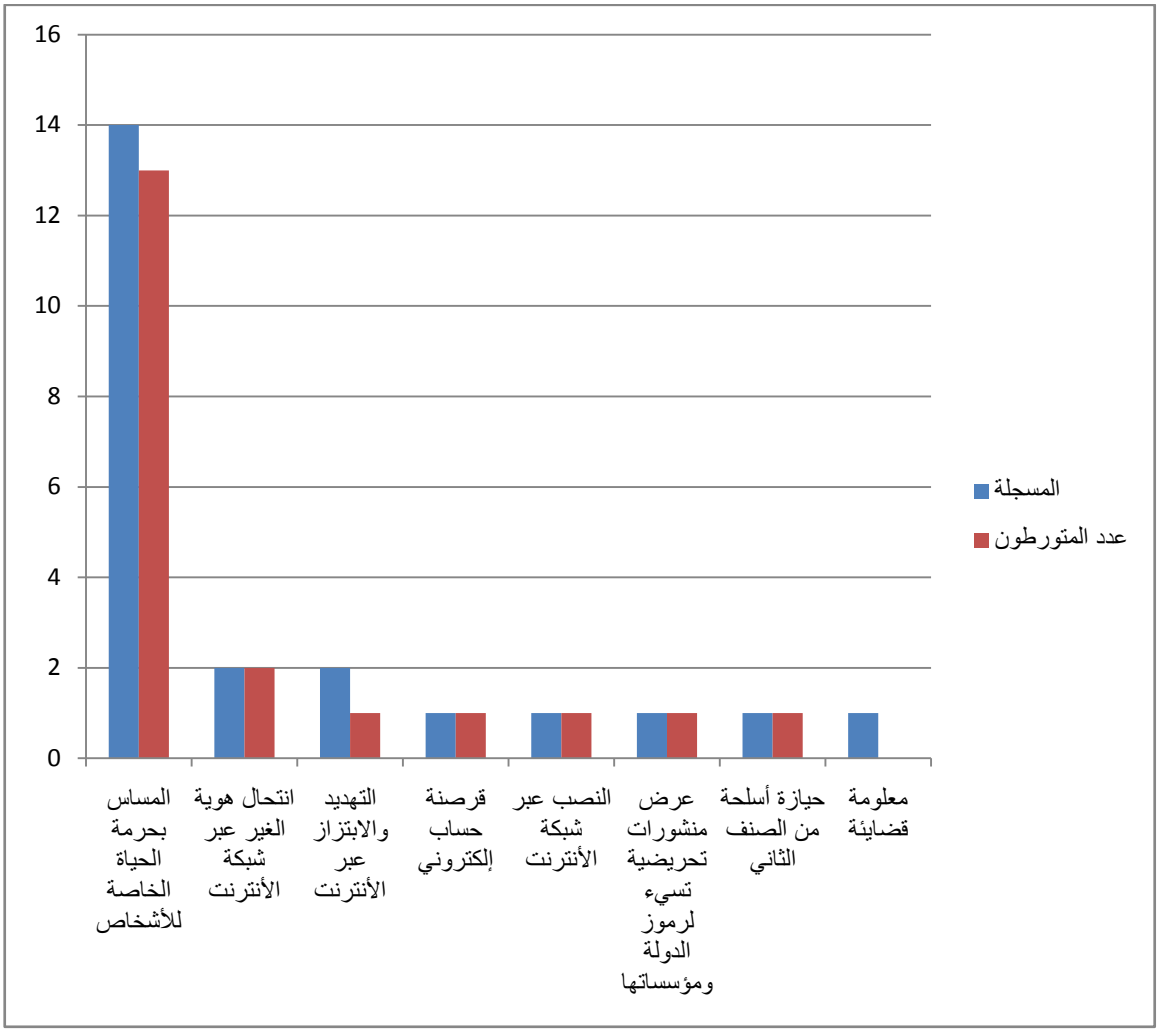
الملحق رقم 04: القضايا المسجلة خلال سنة 2019

طبيعة الجريمة	المسجلة	المنجزة	في طور الإنجاز	عدد المتورطين	ذكور	إناث	ضد مجهول
المساس بحرمة الحياة الخاصة للأشخاص	56	51	5	46	45	1	21
النصب والاحتيال عبر شبكة الأنترنت	3	3		4	2	2	
انتحال هوية الغير عبر شبكة الأنترنت	4	3	1	3	3		
التهديد والابتزاز عبر شبكة الأنترنت	4	4		5	4	1	1
قرصنة حساب إلكتروني	4	2	2				2
حيازة أسلحة من الصنف الثاني	1	1		1	1		
إهانة هيئة نظامية عبر شبكة الأنترنت	1	1		1	1		
عرض منشورات لأنظار الجمهور من شأنها الإضرار بالمصلحة الوطنية	1	1		1		1	
وضع منشورات تحريضية	8	6	2	6	6		
معلومة قضائية	2	2					
المجموع	84	74	10	67	62	5	24

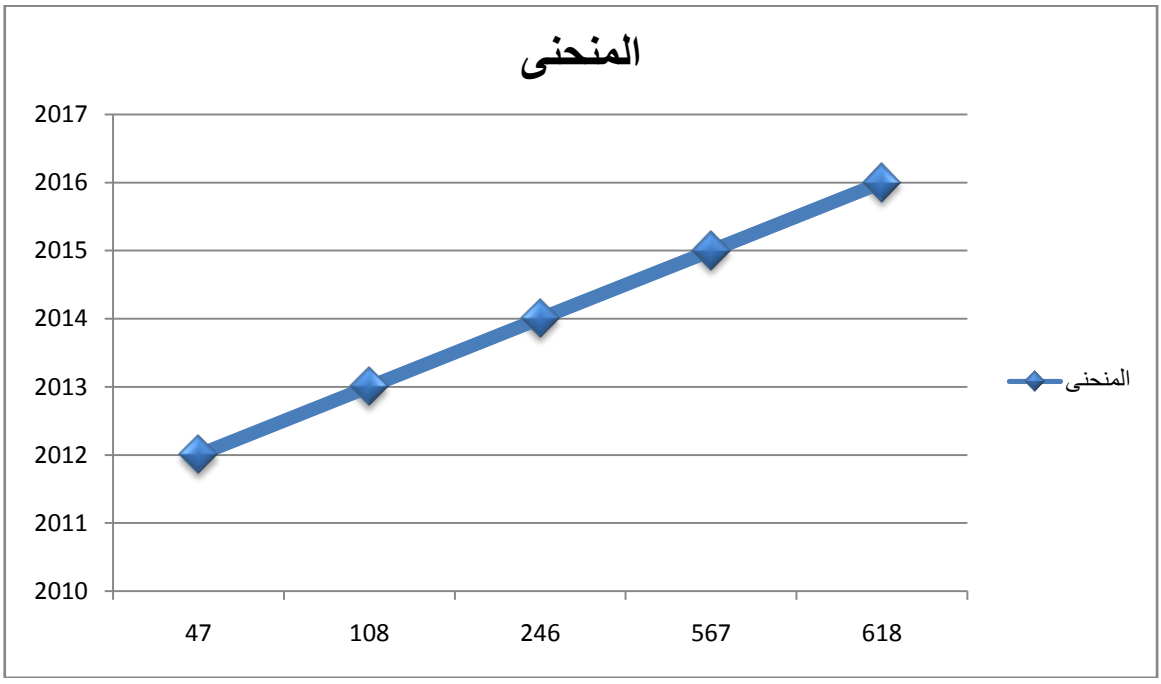
الملحق رقم 05: القضايا المسجلة خلال سنة 2019.



الملحق رقم 06: القضايا المسجلة خلال فترة 2019/01/01 إلى غاية 2019/05/31



الملحق رقم 07: إحصائيات الجريمة الإلكترونية على المستوى الوطني خلال فترة (2012– 2016)



قائمة المراجع

قائمة المراجع

أولا: النصوص التشريعية والتنظيمية.

01-النصوص التشريعية:

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996 المصادق عليه في استفتاء 28 نوفمبر 1996، ج ر ج ج، عدد 76 الصادر في 08 ديسمبر.

2-الأمر رقم 66-156، المؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 47، الصادر في 09 جوان 1966، المعدل والمتمم لا سيما بالقانون رقم 19-10 المؤرخ في 11 ديسمبر 2019، الجريدة الرسمية، العدد .78

3-الأمر 05-02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر 66-155 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد .40

4-القانون الجزائي العربي الموحد، جامعة الدول العربية، الجزء الثاني، رقم 229، د12، بتاريخ 19 نوفمبر 1996.

5-قانون رقم 02-03 مؤرخ في 10 أفريل 2002، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 25 الصادر في 14 أفريل .2002

6-القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ج ر ج ج، العدد44.

7-قانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11، المؤرخ في 21 رمضان عام 1403 الموافق لـ2 يونيو 1983 المتعلق بالتأمينات الاجتماعية.

8-قانون رقم 08-19مؤرخ في 15 نوفمبر 2008، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 63 الصادر في16 نوفمبر .2008

9-القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت 2009، ج ر ج ج، العدد47.

10-قانون رقم 16-01 مؤرخ في 06 مارس 2016، يتضمن تعديلا للدستور، الجريدة الرسمية، العدد 214 الصادر في 07 مارس .2016

11-قانون رقم 20-03 المؤرخ في 05 جمادى الأولى عام 1421 الموافق لـ 05 أغسطس سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية، العدد48.

12-قانون رقم 20-251مؤرخ في 15 سبتمبر 2020، يتضمن استدعاء الهيئة الانتخابية للاستفتاء المتعلق بمشروع تعديل الدستور، الجريدة الرسمية، العدد 54، الصادر في 16 سبتمبر 2020.

13-قانون الإجراءات الجزائية المصري رقم 189 لسنة 2020، المؤرخ في 5 سبتمبر 2020 المعدل والمتمم للقانون رقم 150 لسنة 1950.

14-قانون مكافحة جرائم تقنية المعلومات الإماراتي، 2006.

15-نظام مكافحة الجرائم المعلوماتية السعودي.

02-النصوص التنظيمية:

16-المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المتعلق بتحديد الاختصاص الإقليمي لبعض المحاكم والوكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية، العدد63.

ثانيا: الكتب.

17-أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع، ط 17، الجزائر، 2018.

18-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، ط2، الإسكندرية، 2006.

19-أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة، طبعة خاصة لطلاب التعليم المفتوح بكلية الحقوق بجامعة بنها، 2009.

20-أمير قرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، د.ط، دار المطبوعات الجامعية، الإسكندرية، 2008.

21-بالطي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015.

22-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، د.ط، 2011.

23-خالد ممدوح إبراهيم، الجرائم المعلوماتية، د.ط، دار الفكر الجامعي، الإسكندرية، 2019.

24-خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، د.ط، الإسكندرية، .2007

25-زبيحة زيدان، الجريمة المعلوماتية ف التشريع الجزائري والدولي، د.ط، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

26-سليمان عبد المنعم، القسم العام من قانون العقوبات، دار الجامعة الجديدة، د.ط، الإسكندرية، 2002.

27-شمس الدين ابراهيم أحمد، وسائل الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوادني والمصري "دراسة مقارنة"، ط1، دار النهضة العربية، القاهرة، 2005.

28-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، د.ط، الإسكندرية، 2006.

29-عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات والانترنت)، د.ط، دار الوراق للنشر والتوزيع، بيروت، 2006.

30-عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، د.ط، دار الكتب القانونية، مصر، 2007.

31-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، د.ط، مصر، 2007.

32-عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية، الجزائر، 1995.

33-عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (دراسة مقارنة)، د.ط، منشورات الحلبي الحقوقية، د.س.ن.

34-عفيفي كامل عفيفي ، جرائم الكمبيوتر (دراسة مقارنة)، د.ط، منشورات الحلبي الحقوقية، الإسكندرية، دت.

35-علي عبد القادر القهوجي، شرح قانون العقوبات- القسم العام، الكتاب الأول، دار المطبوعات الجامعية، القاهرة، 1997.

36-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، د.ط، القاهرة، 2004.

37-فتوح عبد الله الشاذلي، قانون العقوبات- القسم العام، الكتاب الأول، دار المطبوعات الجامعية، الإسكندرية، 1998.

38-محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، ط 3، دار الثقافة للنشر والتوزيع، عمان، 2004.

39-محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، ط 1، الهيئة المصرية للكتاب، القاهرة، 2003.

40-محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، د.س.ن.

41-محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، د.ط، دار الثقافة للنشر والتوزيع، عمان، 2005.

42-محمود محمود مصطفى، شرح قانون العقوبات-القسم العام، دار النهضة العربية، د.ط، القاهرة، مصر، 1983.

43-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

44-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010.

45-هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، ط 1، مكتبة الآلات الحديثة، أسيوط، 1994.

ثالثا: الأطروحات والرسائل الجامعية.

46-فيروز عوض الكريم صالح ميرغني، إجراءات التحري والضبط في الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الدراسات العليا والبحث العلمي، جامعة شندي، السودان، 2017/2016.

47-هروال هبة نبيلة، جرائم الانترنت "دراسة مقارنة"، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2014/2013.

48-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012.

49-سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، 2010.

50-صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

51-بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2014/2013.

52-بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2018/2017.

53-مرابط حياة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخ صص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، مستغانم، 2019/2018.

54-معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلومات في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماستر في العلوم الجنائية، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2015.

رابعا: المقالات والندوات العلمية.

55-أحمد أسامة حسنية، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مج 19، عدد خاص بمؤتمر كلية الحقوق الخامس المحكّم، مجلة جامعة الأزهر، غزة، 2017.

56-عبد المحسن بدوي محمد أحمد، استراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيري، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، جامعة نايف العربية للعلوم الأمنية، الخرطوم، 2005.

57-عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، سعيدة، العدد الثاني، 2014.

58-كريستا سكولمان، جرائم الانترنت "طبيعتها وخصائصها"، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و 20 يونيو 2006.

59-نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017.

60-يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ضبي، 2002.

61-يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورشة عمل في تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، المنعقدة بمسقط، سلطنة عمان،2-4 أفريل 2006.

خامسا: المراجع باللغة الأجنبية.

62-Lucas (A) : droit de Informatique, paris, PUF, 1987.

63-L'article 323/1-1 du code pénale français , www.Legifrance.gouv.Fr.

سادسا: المواقع الإلكترونية.

64-www.soutalomma.com

65- www.business.algeria.hsbc.com

66-www.acconline.com/article.detail.aspr?id;7509

67-www.albawaba.com.

فهرس الموضوعات

فهرس الموضوعات

كلمة شكر .....

الإهداء.....

قائمة المختصرات .....

مقدمة ..... أ

الباب الأول: الإطار الموضوعي للجريمة الإلكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية..... 09

المبحث الأول: مفهوم الجريمة الإلكترونية 10

المطلب الأول: تعريف الجريمة الإلكترونية 10

الفرع الأول: التعريف القانوني للجريمة الإلكترونية..... 10

الفرع الثاني: التعريف الفقهي للجريمة الإلكترونية..... 13

المطلب الثاني: التطور التاريخي للجرائم الإلكترونية وإحصائيات حولها..... 15

الفرع الأول: التطور التاريخي للجرائم الإلكترونية..... 15

الفرع الثاني: الإحصائيات التي أجريت حول الجرائم الإلكترونية..... 17

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية 19

المطلب الأول: خصائص الجريمة الإلكترونية..... 19

الفرع الأول: جرائم عابرة للحدود الدولية وصعبة الاكتشاف والإثبات..... 20

الفرع الثاني: خفاء الجريمة وسرعة التطور في ارتكابها 22
الفرع الثالث: خاصية الجاني في الجريمة الإلكترونية..... 23
المطلب الثاني: أنواع الجريمة الإلكترونية..... 25
الفرع الأول: التقسيم الفقهي للجرائم الإلكترونية 25
الفرع الثاني: التقسيم القانوني للجرائم الإلكترونية 30
الفصل الثاني: أركان الجريمة الإلكترونية..... 32
المبحث الأول: النموذج القانوني والمادي للجريمة الإلكترونية 33
المطلب الأول: النموذج القانوني للجريمة الإلكترونية (الركن الشرعي) 33
الفرع الأول: على المستوى الدولي 34
الفرع الثاني: على المستوى الوطني 37
المطلب الثاني: النموذج المادي للجريمة الإلكترونية (الركن المادي) 43
الفرع الأول: السلوك الإجرامي 44
الفرع الثاني: النتيجة الإجرامية..... 46
الفرع الثالث: العلاقة السببية 47
المبحث الثاني: الركن المعنوي للجريمة الإلكترونية 48
المطلب الأول: القصد الجنائي العام..... 49
المطلب الثاني: القصد الجنائي الخاص 50

خلاصة الباب 53

الباب الثاني الإطار الإجرائي للجريمة الإلكترونية

الفصل الأول: إجراءات البحث والتحري في الجريمة الإلكتروني 56

المبحث الأول: الإجراءات العامة لمتابعة الجريمة الإلكترونية..... 56

المطلب الأول: الإجراءات المادية..... 57

الفرع الأول: المعاينة التقنية 57

الفرع الثاني: التفتيش المعلوماتي..... 61

المطلب الثاني: الإجراءات الشخصية..... 64

الفرع الأول: الخبرة..... 64

الفرع الثاني: شهادة الشاهد الإلكتروني (الشهادة في الجريمة الإلكترونية) 66

الفرع الثالث: التسرب 67

المبحث الثاني: الإجراءات الخاصة لمتابعة الجريمة الإلكترونية..... 69

المطلب الأول: مراقبة الاتصالات الإلكترونية..... 69

الفرع الأول: تعريف مراقبة الاتصالات الإلكترونية 71

الفرع الثاني: حالات اللجوء إلى المراقبة..... 71

الفرع الثالث: ضوابط المراقبة الإلكترونية 72

المطلب الثاني: حفظ المعطيات المتعلقة بحركة السير 74

الفرع الأول: تعريف المعطيات المتعلقة بحركة السير..... 74

الفرع الثاني: المعطيات الواجب حفظها..... 75

الفصل الثاني: إجراءات التحقيق والمحاكمة في الجريمة الإلكترونية 75

المبحث الأول: إجراءات التحقيق في الجريمة الإلكترونية..... 76

المطلب الأول: اختصاص قاضي التحقيق وكيفية اتصاله بملف الدعوى 76

الفرع الأول: اختصاص قاضي التحقيق..... 77

الفرع الثاني: كيفية اتصال قاضي التحقيق بملف الدعوى 78

المطلب الثاني: سلطات قاضي التحقيق واستئناف أوامره..... 80

الفرع الأول: سلطات قاضي التحقيق وحدود الدعوى الجنائية أمامه 80

الفرع الثاني: استئناف أو أمر قاضي التحقيق 82

المبحث الثاني: إجراءات المحاكمة في الجريمة الإلكترونية..... 83

المطلب الأول: اختصاص المحكمة وتشكيلتها..... 84

الفرع الأول: اختصاص المحكمة 84

الفرع الثاني: تشكيلة المحكمة..... 87

المطلب الثاني: الإجراءات والقواعد العامة للمحاكمة..... 87

الفرع الأول: إجراءات المحاكمة 88

الفرع الثاني: القواعد العامة للمحاكمة 89

خلاصة الباب..... 92

خاتمة..... 95

الملاحق..... 99

قائمة المراجع..... 107

فهرس الموضوعات..... 115

ملخص:

تعرضنا في هذه المذكرة إلى خصوصية الجريمة الإلكترونية من الناحية الموضوعية والإجرائية بنوع من التفصيل من خلال بابين أساسيين: فقد تناولنا في الباب الأول الإطار الموضوعي للجريمة الإلكترونية، وذلك بالتطرق إلى مفهومها، وكذا تطورها التاريخي وإحصائيات حولها، ثم بيان خصائصها التي جعلتها تنفرد عن نظيرتها التقليدية، سواء تعلقت هذه الخصائص بالجريمة في حد ذاتها، أو بالمجرم الإلكتروني، هذه الطبيعة المتميزة للجريمة الإلكترونية جعلت المشرع الجزائري يدرك مدى خطورة هذه الجريمة على المجتمع، مما يوجب التصدي لها، كما تطرقنا أيضا إلى التقسيمات الفقهية والقانونية للجريمة الإلكترونية، بالإضافة إلى تحديد الأركان التي تقوم عليها.

حيث تناولنا في الباب الثاني الإطار الإجرائي للجريمة الإلكترونية، وذلك بالتطرق إلى خصوصية الجريمة الإلكترونية في مرحلة جمع الاستدلالات والتحقيق، حيث تختلف الإجراءات عن الجريمة التقليدية من حيث طبيعتها ومن حيث المعاينة والتحقيق وغيرها من الإجراءات، وتتميز أيضا الجريمة الإلكترونية بخصوصية خاصة على مستوى التحقيق من حيث اختصاص قاضي التحقيق وكيفية اتصاله بملف الدعوى، بالإضافة إلى تحديد سلطاته والسمات التي يتميز بها في هذا المجال وكذا استئناف أوامره.

حيث يستلزم التحقيق في حد ذاته إلى التفتيش واعتراض المراسلات وكذا حفظ المعطيات لمتعلقة بحركة السير، وكلها إجراءات مستخدمة جاء بها تعديل قانون الإجراءات الجزائية الجزائري لسنة 2006ن وكذا القانون 09-04، مما استوجب على المشرع الجزائري ضرورة تكييف الواقعة طبقا لمنظومته التشريعية والقانونية خاصة الإجرائية من خلال منح بعض الصلاحيات والسلطات الواسعة بتمديد الاختصاص المحلي والإقليمي لوكلاء الجمهورية وقضاة التحقيق من أجل كشف خيوط وملابسات القضية، وتقديم الفاعلين الحقيقيين للعدالة أمام الأقطاب الجزائية المختصة طبقا للمرسوم التنفيذي رقم 06-348.

الكلمات المفتاحية: الإلكتروني-المجرم المعلوماتي- جمع الاستدلالات- المعلومات- التحقيق

Résumé:

Dans cette note, nous avons abordé en détail la spécificité de la cybercriminalité, à la fois objectivement et procéduralement, à travers deux sections principales : Dans le premier chapitre, nous avons abordé le cadre objectif de la cybercriminalité, en abordant son concept, ainsi que son évolution historique et les statistiques à son sujet, puis en clarifiant ses caractéristiques qui la rendaient unique par rapport à son homologue traditionnel, que ces caractéristiques soient liées à la crime en lui-même, ou au cybercriminel, cette nature distincte de la cybercriminalité fait Le législateur algérien est conscient de l'étendue de la gravité de ce crime sur la société, qui nécessite d'y remédier. Là où, dans le deuxième chapitre, nous avons traité du cadre procédural de la délinquance électronique, en abordant la confidentialité de la délinquance électronique au stade de la collecte des inférences et de l'enquête, où les procédures diffèrent de la délinquance traditionnelle en termes de nature et en termes d'inspection, d'enquête et autres procédures, et la criminalité électronique se caractérise également par une spécificité particulière au niveau de l'enquête en termes de compétence du juge d'instruction et de la manière dont il se rapporte au dossier de l'affaire, en plus de définir ses pouvoirs et les caractéristiques qui le distinguent dans ce domaine, ainsi que de faire appel de ses ordonnances. Lorsque l'enquête en elle-même comporte le contrôle et l'interception de correspondances, ainsi que la conservation des données relatives au trafic, autant de procédures utilisées par la modification du code de procédure pénale algérien de 2006, ainsi que la loi 09-04, qui a obligé le législateur algérien à adapter l'incident selon son système législatif et juridique, notamment procédural de En accordant des pouvoirs et pouvoirs étendus pour étendre la compétence locale et régionale des agents républicains et des juges d'instruction afin de démêler les pistes et les circonstances de l'affaire l'affaire, et de traduire en justice les véritables auteurs devant les pôles pénaux compétents conformément au décret exécutif n° 06-348.

Mots-clés : électronique - information criminelle - collecte d'inférences - information - enquête