وزارة التعليم العالي والبحث العلمي
Research Ministry of High Education and Scientidic
جامعة محمد البشير الإبراهيمي – برج بوعريريج–
University of Mohamed el Bachir el Ibrahimi –Bba–
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق
تخصص: قانون أعمال
الموسومة بـ:

الأحكـام الإجرائيـــة للجريمـة الإلكترونيـــة فـــي التشريع الجزائـــري

من إعداد الطلبة

- نايلـي محمد أمين
- عراب عمر

تحت إشراف الأستاذة:

سي حمدي عبد المؤمن

لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
زاوي رفيق	أستاذ محاضر – ب–	رئيسا
سي حمدي عبد المؤمن	أستاذ محاضر– ب–	مشرفا
عشاش حمزة	أستاذ مساعد –ب–	ممتحنا

السنة الجامعية: 2022/2021


بسم الله الرحمن الرحيم

شكر و تقدير:

نتقدم بوافـــــــر الشكر و التقديـــر إلى أستاذنا المشرف الدكتور سي حمدي عبد المؤمن على إشرافه على هاته المذكرة وإثرائه لهذا العمل

كمـــــا نشكر اللجنة المحترمة المناقشة لهذه المذكرة.

شكر خاص للأستاذ الدكتور عشاش حمزة الذي لم يبخل علينا بتوجيهاته و نصائحه و لجميع أساتذة كلية الحقوق والعلوم السياسية بجامعة محمد البشير الإبراهيمي ببرج بوعريريج الذين رافقونا طيلة هذا المشوار الدراسي الجامعي.

إهداء

الحمد لله الذي سخر لنا من أسبابه الهداية

و التوفيق ما يسر لنا به إنهاء هذا العمل المتواضع

و شرف لنا أن نهديه

*إلى ...الجزائر التي نحب

* الى الأب الذي علمنا أن الإستقامة هي أقصر طريق للسعادة في الدنيا والآخرة.

* إلى الأم التي إحتضني فكان حضنها دفئا وإشفاقا وحنانا , وربتني فكانت تربيتها نبلا وقيما وأخلاقا.

*إلى زوجتي العزيزة رفيقة الدرب و الحياة

*إلى الإخوة الأعزاء و الأهل و الأحباب.

* إلى كل من علمني حرفا , وإلى جميع الأساتذة الكرام الذين صادفتهم خلال الدراسة من مرحلة الجامعة.

*إلى جميع زملاء العمل عبر الوطن الغالي.

* لكل هؤلاء , نحييهم ونهدي هذا العمل.

نايلي محمد أمين

إهداء

ربي إذا أعطيتني نجاحا فلا تأخذ تواضعي، وإذا أعطيتني تواضعا فلا تأخذ اعتزازي بكرامتي.

أهدي هذا العمل المتواضع

إلى الصدر الدافئ، والقلب العطوف رمز الصبر والتضحية الجوهرة الثمينة "**أمي** " الغالية.

إلى من علمني أن أرسم على الوجوه المستنيرة، وسقاني كؤوس الكفاح، وكان القدوة في النضال،وحسن مثال صاحب الشهامة " **أبي** "الغالي بارك الله في عمره.

إلى تيجان رأسي ومصدر همتي وفخري، إخوتي وأخواتي الأعزاء، إلى الأهل الأحباب لكل من عائلة عراب.

إلى رفيقة دربي و سندي زوجتي حفظها الله.

عراب عمر

إن التطور الهائل الذي شهد كل من مجال تقنية المعلومات و مجال الاتصالات و الاندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على إستخدام الأنظمة المعلوماتية، فبات يطلق على هذا العصر عصر المعلومات.

ونتيجة هذا التطور في عالم المعلوماتية نشأت أنواع جديدة من الجرائم التي ما كانت لتظهر لولا ظهور جهاز الكمبيوتر, هذه الجرائم تنوعت واتخذت مظاهر مختلفة بحيث أصبحت اليوم تطرح إشكالات خطيرة على الصعيدين الإقتصادي والقانوني.

إن ظاهرة الجرائم الإلكترونية، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة – بيانات ومعلومات وبرامج بكافة أنواعها – فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، تطال الإعتداءات على معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت.

ولقد تأثرت جميع الدول بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام، لذلك بات من الضروري مواجهة التحديات التي تواجهها لملائمة أنظمتها مع متطلبات و معطيات العصر التي تمخضت جراء التطور التقني، في هذا السياق المشرع في الجزائر للتدخل لتدارك – و لو نسبيا – الفراغ القانوني في المجال المعلوماتي من خلال تعديل قانون العقوبات لسنة2004، بإضافة قسم سابع مكرر يحمل عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"

والتطور الذي انعكس أثره على قانون العقوبات، قد انعكس أثره أيضا على القانون الإجرائي، حيث وضعت نصوص قانون الإجراءات الجزائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها, فإذا كانت الوسائل التقليدية قد تكفي لإثبات تلك الجرائم، إلا أنها قد تعجز عن إثبات

الجرائم التي ترتكب بالوسائل الإلكترونية خاصة أن مجرمي المعلوماتية من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل إرتكابها لكي لا يقعوا تحت طائلة العقاب، فهم يزيدون بذلك من صعوبة إجراءات التحقيق التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم.

فإذا كان من السهل على جهات التحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة فإثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم، وبالوسائل العلمية التي ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى مرتكبيها، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالإفراد وبالمجتمع. ولا شك في أن كشف ستر هذا النوع من الجرائم يحتاج أيضا إلى طرق إلكترونية تتناسب مع طبيعتها بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة. فتطوير الإثبات الجنائي بتطوير طرقه أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، لكي نمنع ما يمكن أن يقال من أن صعوبه هذا الإثبات قد يؤدي إلى عدم التجريم.

هذا الأمر جعل المشرعين الجنائيين في مختلف الدول يستنفرون لوضع نصوص إجرائية جديدة أكثر ملاءمة لخصوصية الجريمة المعلوماتية. و في هذا الإطار قام المشرع الجزائري بتعزيز القواعد التي تضمنها قانون العقوبات الصادر سنة 2004 من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها. و الذي حاول من خلاله الإحاطة بمختلف الجوانب المتعلقة بمحاربة الجريمة الالكترونية بجمعه بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

أهمية وأهداف هذه الدراسة:

تكمن أهمية دراسة موضوع الأحكام الإجرائية للجريمة الإلكترونية باعتبارها من الجرائم المستحدثة نسبيا، و التي تعرف تطور متسمر بسبب تزايد استخدام تقنية المعلومات التي تعد العصب المحرك لكل أنواع الحياة، الأمر الذي استدعى الى دراستها من الجوانب الموضوعية و كذا الجوانب الإجرائية، كما أن هذا الموضوع يعد من المواضيع المهمة التي تظهر مدى كفاءة الدول في التعامل مع الإجرام الإلكتروني الذي بات محط اهتمام الهيئات و الأجهزة الدولية و الوطنية كونها من الجرائم العابرة للحدود الوطنية.

دوافع إختيار موضوع الدراسة:

ما دفعنا الى إختيار الموضوع هو الرغبة في التعرف على هذا النوع المستحدث من الإجرام الذي انتشر بصورة ملفتة في المجتمع الجزائري مؤخرا، ولأنها ترتبط بالتقنية الحديثة وتعتبر من سلبياتها لابد من أنها تتميز بمجموعة من الخصائص مقارنة مع باقي الجرائم التقليدية، مما يستدعي الوقوف ومعرفة إن كانت هناك إجراءات خاصة في مجال البحث والتحري، ومدى إمكانية تطبيق القوانين التقليدية لمواجهة الجريمة الإلكترونية كذلك دفعنا الفضول لمعرفة بما يحكم به القاضي في مثل هذه الجرائم، إن كان يستعين بالنصوص التقليدية أم أن هناك قوانين خاصة يلجأ إليها.

الإشكالية المطروحة:

لتسليط الضوء على الموضوع تم طرح الإشكالية التالية:

أما بالنسبة للإشكالية التي يطرحها موضوع دراستنا فتتمحور حول الإجابة على الأسئلة التالية :

- **ماهي الآليات الإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري؟ وإلى أي مدى وفق المشرع الجزائري للحد من هاته الجريمة؟**

المنهج المتبع في الدراسة:

للإجابة على إشكالية دراستنا إعتمدنا على المنهج الوصفي والتحليلي. فالمنهج الوصفي يظهر من خلال قيامنا بوصف لظاهرة الجريمة الإلكترونية وكذا تحليل النصوص القانونيةبالإضافة الى المفاهيم الخاصة بالإجراءات المستعملة في استخلاص الدليل والصعوبات التي تواجهها.

صعوبات الدراسة :

واجهتنا بعض الصعوبات، كنقص المراجع المتخصصة في الجانب الإجرائي للجرائم الإلكترونية لا سيما في التشريع الجزائري في حين أن أغلب المراجع و الدراسات و الأبحاث القانونية همت بالجانب الموضوعي للجريمة، وهذا بالإضافة لنقص معالجة هذه القضايا و كذا لندرة الأحكام القضائية في هذا المجال و كذلك الاهتمام بالجانب التقني في مجال المنظومة المعلوماتية بالموازاة مع الجانب القانوني لفهم هذه الظاهرة الإجرامية.

محاور الدراسة :

إتبعنا في تقسيم موضوع الدراسة إلى خطة منهجية ثنائية الفصول، حيث خصصنا الفصل الأول إلى دراسة الأحكام الموضوعية للجريمة الإلكترونية متطرقين في ذلكوفق ثلاثة مباحث إلى مفهومها وأساسها القانوني بالإضافة إلى أركانها.

أما الفصل الثاني و الذي تناولنا فيه إجراءات مكافحة الجريمة الإلكترونية في التشريع الجزائري، حيث تطرقنا كذلك وفق ثلاثة مباحث الى إلى قواعد الاختصاص القضائي في ثم إلى التحقيق فيها و أخيرا الإثبات في هذه الجرائم.، وانهينا الدراسة بخاتمة تضمنت أهم ما توصلنا إليه إضافة للتوصيات المقترحة.

وعليه تكون الخطة كالتالي :

الفصل الأول : الأحكام الموضوعية للجريمة الإلكترونية.

المبحث الأول:مفهوم الجريمة الإلكترونية.

المطلب الاول: تعريف الجريمة الإلكترونية

المطلب الثاني: خصائص الجريمة الإلكترونية

المبحث الثاني: الأساس القانوني للجريمة الإلكترونية

المطلب الأول: على المستوى الدولي

المطلب الثاني:على المستوى الوطني

المبحث الثالث : أركان الجريمة الإلكترونية

المطلب الأول: الركن الشرعي

المطلب الثاني : الركن المادي و المعنوي للجريمة

الفصل الثاني: إجراءات مكافحة الجريمة الالكترونية في التشريع الجزائري

المبحث الأول:قواعد الاختصاص القضائي في الجريمة الإلكترونية.

المطلب الأول: القانون الواجب التطبيق

المطلب الثاني:الاختصاص الاقليمي

المبحث الثاني : التحقيق في الجريمة الإكترونية.

المطلب الأول: الإختصاصات العادية

المطلب الثاني: الإختصاصات المستحدثة

المبحث الثالث : الإثبات في الجريمة الالكترونية.

المطلب الاول : الدليل الالكتروني و حجيته

المطلب الثاني: أدلة الإثبات في الجريمة

خاتمة

الفصل الأول: الأحكام الموضوعية للجريمة الإلكترونية.

تمهيد:

بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات في شتى ميادين الحياة المعاصرة، فإن هذه الثروة التكنولوجية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية و الانحراف عن الإغراض المتوخاة منها، تمثلت في تفشي طائفة من الظواهر الإجرامية المستحدثة ألا وهي ظاهرة الجرائم الإلكترونية. ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية و شكلت أرضا خصبة لكثير من الأنشطة الغير المشروعة المرتبطة بالحسابات الآلية والتي أصبحت توفر للجناة وسيلة هامة لارتكاب العديد من الجرائم الإلكترونية ما كانت لتظهر لولا وجود هذه الحاسبات الآلية و ارتباطها بالتقنية المعلوماتية.[1]

ولما كانت الجريمة الالكترونية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض لأجل ذلك فقد بدى انه وقبل الخوض في المسائل الإجرائية التي تنطبق على الجريمة الالكترونية أن ننوه على الجانب من القواعد الموضوعية لهاته الجريمة. ولأجل إزالة الغموض المحيط بها يتطلب الأمر تحديد مفهوم هذه الظاهرة و خصائصها ورسم الإطار القانوني الواضح لهاته الجريمة و الذي سنتناوله في هذا الفصل بعنوان الأحكام الموضوعية للجريمة الالكترونية. [2]

[1]- لينا محمد الأسدي، مدى فاعلية احكام القانون الجنائي في مكافحة الجريمة المعلوماتية:دراسة مقارنة، دار الحامد للنشر،الطبعة1، الأردن، 2015،ص200

[2] - مشتاق طالب وليد، مفهوم الجريمة المعلوماتية و دور الحاسوب في ارتكابها، مجلة العلوم القانونية و الانسانية ، جامعة ديالي العراق، المجلد الثالث ، العدد1، 2014، ص 443

المبحث الأول: مفهوم الجريمة الإلكترونية.

الجريمة الالكترونية ظاهرة إجرامية مستفحلة حديثا في مجتمعنا و تحديد مفهومها يعد الخطوة الاولى للتعرف على هذه الظاهرة والتطرق الى جوانبها القانونية و في هذا المبحث سوف نتصدى لتعريف الجريمة الالكترونية **(مطلب أول)**، كما سنحاول إعطائها الخصائص **(مطلب ثاني)** التي تتميز بها عن غيرها من الجرائم التقليدية و ذلك في المطالب الآتية:

المطلب الأول : تعريف الجريمة الإلكترونية.

تتكون الجريمة الالكترونية من مقطعين هما الجريمة و الالكترونية ، فيستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب ، أما الجريمة فهي السلوكيات و الأفعال الخارجة عن القانون،[1] فالجرائم الالكترونية ارتبط مفهومها و لا يزال يرتبط بتكنولوجيا الحاسبات و تطوراتها المستخدمة في تشغيل و تخزين و نقل المعلومات في شكل الكتروني ، و كذا بتكنولوجيات ووسائل الاتصال و شبكات الربط لذلك فمن الضروري ان يكون اي تعريف لهذا النمط من الجرائم متسما بالمرونة بما يسمح باستيعابه و تواكبه مع سائر التقنيات المبتكرة الراهنة و المستقبلية في مجال تكنولوجيا التعامل مع المعلومات .

لكن التطور المستمر و اللامتناهي لتكنولوجيا المعلومات و الاتصالات حال دون وضع تعريف فقهي جامع و شامل لمفهوم الجريمة الالكترونية، خشية من حصر نطاقها داخل اطار تجريمي محدد قد يضر بها خاصة في ظل التطور المستمر للتقنية المعلوماتية فما

[1]- مختارية بوزيدي ، **ماهية الجريمة الإلكترونية** ، مداخلة بجامعة مولاي الطاهر–سعيدة، مطوية الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر، 2017، ص9.

يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى تظهر نتيجة استخدام تقنيات جديدة. [1]

وإذا كان التطور المتجدد و المستمر للمعلوماتية يمنع صور التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية فهذا ما يقع على عاتق الفقه بداية بوضع تعريف لهذه الظاهرة الإجرامية و الذي قد يسهم في صياغة المشرع للنصوص القانونية و يساعد القضاء في تفسير هذه النصوص ذو تكييف الواقع.

ولقد ذهب الفقهاء بتعريف الجرائم الالكترونية في مذاهب شتى و وصفو تعريفات مختلفة تتمايز و تتباين تبعا لموضوع العلم المنتمي إليه و تبعا لمعايير التعريف ذاته.

و في سبيل ذلك فان الفقه الجنائي قد بذل معلومات عديدة في تعريف الجريمة الالكترونية و لعل جميع المحاولات التي بذلت من اجل تعريف الجريمة الالكترونية لا تخرج عن احد الاتجاهين أولهما يضيق من مفهومها و الثاني يوسعه.

الفرع الأول: المفهوم المضيق للجريمة الالكترونية.

لقد حصر أنصار هذا الاتجاه مفهوم الجريمة الالكترونية في الحالات التي تتطلب قدرا كبير من المعرفة التقنية في ارتكابها، و ان الجرائم التي تفتقر الى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية ، وذلك على خلاف الجرائم التي يتوفر لها هذه المعرفة فهي فقط التي تكون بحاجة الى نصوص خاصة تتلاءم مع طبيعتها. [2]

[1] -خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009، ص75

[2] - نائلة عادل محمد فريد قورة, **جرائم الحاسب الاقتصادية دراسة نظرية و تطبيقية**، منشورات الحلبي الحقوقية – بيروت– الطبعة الأولى، 2005، ص30.

و من التعريفات التي وضعها هذا الاتجاه ان الجلريمة الالكترونية هي كل غير مشروع يكون العلم بتكنولوجيا الحاسبات الالية بقد كبير لازما لارتكابه من ناحية و لملاحقته و تحقيقه من ناحية اخرى[1]، و في هذا الاتجاه عرفها الفقيه David Thomason (دافيد تومسون) " انها اية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنيات الحاسب .[2]

و حسب هذا التعريف فانه يشترط ان يكون مرتكب الجريمة الالكترونية على درجة كبيرة من العلم بتكنولوجيا الحاسبات ، و هذا المفهوم قد أخذت بها وزارة العدل الأمريكية في تقريرها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للابحاث حينما عرف الجرائم الالكترونية بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من إرتكابها .

و في هذا الاتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الاعتداء ، إذ يرى الأستاذ Mass أن المقصود بالجرائم الالكترونية هي تلك الاعتداءات التي ترتكب بواسطة الكترونية بغرض الربح .و هناك جانب آخر اخذ في تعريفه للجريمة الإلكترونية بمعيار موضوع الجريمة و ذلك كما ذهب اليه الفقيه Rosenblatt على أنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل حاسوب او تغييرها أو حذفها".[3]

والملاحظ على التعريفات المتقدمة انها تضيق على نحو كبير من الجريمة الالكترونية فهي محصورة في الحالات التي تتطلب ان يكون مقترف الجريمة متمتعا بقدر كبير من المعرفة التقنية لارتكابها ولكن قد لا يحتاج الفاعل الى كل هذه المعرفة ، فقد يرتكب

---

[1] - نائلة عادل محمد فريد قورة, المرجع سابق، ص28.

[2] - أمير فرج يوسف، **الجريمة الكترونية والمعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر و الانترنت**، مكتبة الوفاء القانونية الإسكندرية، مصر، الطبعة الأولى، 2011،ص66.

[3]- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، عمان، الطبعة الثانية، 2010،ص48

الفعل الغير مشروع وسط بيئة رقمية و لا يحتاج الفاعل الى قدر كبير من المعرفة فمثلا إتلاف البيانات المخزنة داخل نظام الكمبيوتر لا يتطلب من فاعله قدرا كبيرا من العلم بتكنولوجيا الحاسبات الآلية ، و على الرغم من ذلك فقد جرمته الكثير من التشريعات العقابية.

لذلك فيؤخذ من التعريفات السابقة انها جاءت قاصرة عن الإطاحة بأوجه ظاهرة الإجرام الالكتروني ، فالبعض من فقهاء هذا الاتجاه ركز على موضوع الجريمة و البعض ركز على وسيلة ارتكابها اما البعض الأخر ركز على معيار النتيجة.

الفرع الثاني : الإتجاه الموسع لمفهوم الجريمة الالكترونية.

إزاء الانتقادات الموجهة للاتجاه الأول حاول بعض الفقه تعريف الجريمة الالكترونية على نحو واسع لتفادي القصور الذي شاب في تعريفات الاتجاه المضيق لهاته الجريمة . فعلى العكس من الاتجاه السابق فان أنصار هذا الاتجاه يذهبون الى توسيع من مفهوم الجريمة الالكترونية ، باعتبار ان مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصبغ عليه وصف الجريمة الالكترونية ،و قد تباينت مواقف أنصار هذا الاتجاه في تعريفاتها للجريمة الالكترونية بحسب المعايير التي اعتمد عليها كل فريق في ذلك ، وتتباين مواقف فقهاء هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن ان تمتد اليها هذه الجريمة ، فيذهب فريق الى تعريفها بانها كل سلوك إجرامي يتم بمساعدة الحاسب الآلي ، و فريق اخر يعتبرها انها كل جريمة تتم في محيط الحاسبات الالية و من هذه التعريفات ما جاء به الفقيه(Marwe) الذي يرى ان الجريمة الالكترونية تتمثل في الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الالي.[1]

[1] - محمد أمين الشوابكة ، **جرائم الحاسوب و الأنترنت(الجريمة المعلوماتية)**، دار الثقافة للنشر والتوزيع ، الطبعة الاولى، 2009، ص8

كما تبنى الخبير الأمريكي PARKER تعريفا موسعا للجريمة الالكترونية على انها كل فعل إجرامي متعمد ايا كانت صلته بالمعلوماتية ينشا عنها خسارة تلحق بالمجني عليه او كسب يحققه الفاعل.[1]

وتم تعريفها كذلك أنها " كل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صور كانت." وعرفها البعض أنها "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على أموال المادية أو المعنوية." [2]

وهناك اتجاه فقهي آخر عرفها بالقول " أن الجريمة الالكترونية هي كل سلوك غير مشروع و غير اخلاقي او غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"[3]

ذهب البعض إلى القول أنها كل عمل أو امتناع عن عمل ياتيه الانسان إضرارا بمكونات الحاسب المادية و المعنوية و شبكات الاتصال الخاصة به باعتبارها من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها .

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم هاته الجريمة اذ يصبغ وصف الجريمة الالكترونية على أفعال قد لا تكون كذلك حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة الالكترونية ، و من تم يتضح لنا صعوبة قبول هذا التوجه، فجهاز الحاسب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأسطوانات الممغنطة أو اللواحق على سبيل المثال.

---

[1] - نهلا عبد القادر المومني، المرجع السابق، ص49.

2 – نهلا عبد القادر المومني، نفس المرجع، ص50.

3 – وضع هذا التعريف من طرف مجموعة من خبراء منظمة التعاون الاقتصادي و التنمية في اجتماعها المنعقد في باريس من سنة 1983 ضمن حلقة الاجرام المرتبط بتقنية المعلومات)

ومن ثم لا يمكن إعطاء وصف الجريمة الالكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة.[1]

يمكن الاشارة الى التعريف القانوني و الذي جاء به المشرع الجزائري حيث عبر عنها بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال فإنه يعرفها بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأوي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية ،ولولا هذه النظم المعلوماتية وشبكات الإتصالات ما كان أون نصبغ صفة المعلوماتية على هذه الجرائم.[2]

المطلب الثاني: خصائص الجريمة الإلكترونية .

تتميز الجريمة الالكترونية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية؛ و ذلك نتيجة ارتباطها بتقنية المعلومات و الاجهزة الالكترونية و ما تتمتع به من تقنية عالية ،و قد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات و الحقائق؛ و التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف– بالمجرم الالكتروني – لتميزه أيضا عن المجرم التقليدي . من خلال هذا سوف نحاول فيما يلي التطرق إلى أهم السمات الخاصة بالجريمة الالكترونية سواءا الميزات الذاتية او الموضوعية على حد سواء (الفرع الأول) ثم سنتناول بالدراسة أهم السمات التي تميز المجرم الالكترونية(الفرع الثاني).

[1] - نائلة عادل محمد فريد قورة، المرجع السابق، ص30و31.
[2] - نهلا عبد القادر المومني ، المرجع السابق، ص52

الفرع الأول: السمات الخاصة بالجريمة الإلكترونية.

إن ارتباط الجرائم الالكترونية جهاز الحاسوب و شبكة الانترنت أضفى عليها مجموعة من المميزات التي تميزها عن غيرها من الجرائم التقليدية التي لها اثر كبير على التشريعات العقابية و الإجرائية و من أهم هذه المميزات:

أولا/ وقوع الجريمة في بيئة إلكترونية.

ما يميز الجريمة الالكترونية عن الجريمة التقليدية انها تقع في بيئة الكترونية و ذلك أن:

1- الحاسب عنصر في ارتكاب الجريمة: يعد الحاسب جهاز الكتروني قادر على استخدامه بصوره ايجابية أو سلبية، لذا فقد يستخدم الإنسان هذه الأداة في الغرض الغير الطبيعي المخصص لاستخدامه، فوجود هذه الآلة يشتمل على وجه العموم المكونات الأساسية لأجهزة الحاسب وملحقاتها وكذلك المكونات المعنوية والتي تشمل جميع الكيانات وبرامج التشغيل والتطبيق. فهذه الجريمة ذات طبيعة تقنية والسلوك الإجرامي أيضاً ذا مضمون تقني ، فالحاسب هو دائماً عنصر مهم في الاعتداء مع ما يمكن أن يتعامل معه ضمن مجال معطياته وهذه الخاصية تنفرد بها عن بقية الجرائم، ذلك أن الحاسب العنصر المهم الذي يمكن الشخص من تنفيذ الجريمة ايا كان نوعها فالحاسب وما يرتبط به من تقنيات تلعب أدواراً عديدة في هذه الجرائم, فهو إما أن يكون موضوعاً للجريمة أو هدفاً للجريمة , أو أداة تساعد في تخطيط وتطوير الجريمة, أو قد تكون مثالاً أو نموذجاً للجريمة.[1]

2-وقوع الجريمة اثناء عملية المعالجة الآلية للمعطيات الخاصة بالكمبيوتر: و يمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام او عدم قيام

[1] - مشتاق طالب وليد، **مفهوم الجريمة المعلوماتية و دور الحاسوب في ارتكابها**، مجلة العلوم القانونية والإنسانية، جامعة ديالي العراق، المجلد الثالث، العدد الأول، 2014، ص343.

أركان الجريمة الالكترونية الخاصة بالتعدي على نظام المعالجة للبيانات.[1] فيشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها الكترونيا، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها، أو طباعتـها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية، وعلى الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الإدخال، المعالجة، الإخراج)، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر الى طبيعتها ارتكابها إلا في وقت محدد، ففي مرحلة الإدخال المعلوماتي يمكن إدخال معلومات غير صحيحة، أو عدم إدخال وثائق أساسية، وفي مرحلة المعالجة الآلية للبيانات، فإنه يمكن إجراء أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج الحاسب الآلي، أما في مرحلة المخرجات فقد يقع التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة من المفيد الاشارة أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، ومن الشائع وصف بيانات الحاسوب مثلا كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب، توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر لم يحدد موقفه، لكن من المرجح في الممارسة العملية أن تتضمن تلك البيانات والمعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة، وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية.[2]

[1] - نائلة عادل محمد فريد قورة، المرجع السابق، ص55.

[2] - شوقي يعيش تمام، **الجريمة المعلوماتية (دراسة تأصيلية مقارنة)** سلسلة مطبوعات المخبر بسكرة،الطبعة الأولى،2019، ص23.

ثانيا/ الجريمة الالكترونية متعدية الحدود (عابرة للوطنية):

إنه و بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية او ملموسة تقف امام نقل المعلومات عبر الدول المختلفة ن فالقدرة التي تتمتع بها الحاسبات الالية في نقل و تبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها ألاف الأميال أسفر هذا الأمر إلى نتيجة موعدها أن أماكن متعددة في دول مختلفة قد تتأثر با الجريمة الإلكترونية الواحدة في أن واحد، حيث يمكن ان ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدا.

فالجريمة الالكترونية بهذا الشكل لا تعترف با الحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة ، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف انحاء العالم انعكست على طبيعة الإعمال الإجرامية التي يعمد فيها المجرمون الى استخدام هذه التقنيات في خرقهم للقانون[1]، وهو ما يعني أن مسرح الجريمة الالكترونية لم يعد محليا بل أصبح عالميا،إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد ،وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء ،فقد يوجد الجاني في بلد ما ويستطيع الدخول الى ذاكرة الحاسب الآلي الموجود في بلد اخر، وهو بهذا السلوك قد يضر شخصا أخر موجود في بلد ثالث، [2] أو قيام بإعداد احد البرامج الخبيثة فيه و تظهر ما ثم يتم نسخ هذا البرنامج و يرسل الى دول مختلفة من العالم و تظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية حيث ادلى التوسع الكبير لاجراء التعاملات البنكية عبر شبكات المعلوماتية إلى إعطاء بعد دولي لهذه الجرائم ، ذلك ان ربط وسائل الاتصالات بالحواسيب ضاعف من

[1] - خالد ممدوح إبراهيم، المرجع السابق، ص88.

2 – نائلة عادل محمد فريد قورة، المرجع السابق، ص58.

المعاملات المالية الدولية و التي اصبحت تتم بواسطة وسائل الكترونية ، وبصفة خاصة خلال التحويل الالكتروني للاموال و التبادل الالكتروني للمعلومات.

و مفاد ما سبق ذكره ان الجرائم الالكترونية تتميز بالتباعد الجغرافي بين الفاعل و المجني عليه و من الوجهة التقنية التباعد بين اداة الجريمة و محلها ، و هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة و خارجها ليطال الى دولة اخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الاعتداء.

يمكن القول ان هذه الخاصية الدولية للجريمة الالكترونية اثارت عدة إشكالات قانونية اهمها تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي و محاكمة مرتكب هذه الجريمة ، فهل هي الدولة التي وقع فيها النشاط الاجرامي ، ام التي اضيرت مصالحها نتيجة هذا التلاعب ، بالاضافة الى اشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة الالكترونية.[1]

ثالثا/ صعوبةُ إكتشاف الجريمة الالكترونية و إثباتها.

تقع الجريمة الالكترونية في بيئة افتراضية تقنية لا تترك اية اثار محسوسة ، اذ يغلب عليها انها تحدث في الستر و الخفاء لان الجناة و كونهم يتمتعون بقدرات فنية يعمدون في كثير من الاحيان الى اخفاء نشاطهم الاجرامي ، كما ان الضحية لا يلاحظها رغم وجوده على الشبكة.[2] كما ان الجاني من السهل عليه تدمير الادلة و محوها مما يعقد امر كشف الجريمة ، و اذا قورنت حالات اكتشاف الجريمة الالكترونية على ضوء ما يكتشف

---

[1]- تجدر الاشارة هنا الى قضية R.V thompso و التي تتلخص وقائعها في قيام مبرمج انجليزي يعمل باحد البنوك في دولة الكويت بالتلاعب بنظام الحاسب الالي الخاص بالبنك ليقوم باجراء خصومات من ارصدة العملاء لحسابه الخاص به و بعد رجوع المتهم الى انجلترا قام بالكتابة الى البنك طالبا منه القيام بتحويل الحساب الخاص به الى عدة حسابات بنكية في انجلترا و هو ما قام به البنك. و قدم بعدها للمحاكمة امام القضاء الانجليزي الا انه طعن في الحكم استنادا الى عدم اختصاص القضاء الانجليزي بما ان فعل السحب و الايداع كان بالكويت و ليس بانجلترا . مشار الى هذه القضية لدى نائلة عادل محمد فريد قورة، مرجع سابق، ص 54 .

[2] - خضرة شنتير ، **الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)**، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر،2021، ص14.

في الجريمة التقليدية فان عددها قليل كون المجني عليهم يلعبون دورا اساسيا في اكتشافها، حيث تحرص أكثر الجهات التي تتعرض انظمتها المعلوماتية للانتهاك و تمنى بخسائر فادحة الى عدم الكشف عن ذلك حيث تكتفي فقط باتخاذ اجراءات ادارية داخلية دون ابلاغ السلطات المختصة تجنبا للاضرار بسمعتها و مكانتها.[1]

و يبدو اكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية و مؤسسات الاقراض ، حيث تخشى مجالس ادارتها من ان تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم او اتخاذ الاجراءات القضائية حيالها الى تضاؤل الثقة فيها من جانب المتعاملين معها ، حيث ان الجانب الاكبر من الجرائم الالكترونية لا يتم الكشف عنه و هو مايؤثر سلبا على السياسة التي تمكن من اثباتها و مكافحتها.[2]

يكمن القول ان هاته الجريمة من اصعب الجرائم في الاثبات و يرجع ذلك إلى عدة عوامل منها:

1- أن الجريمة الإلكترونية لا تترك آثار مادية، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية ولا توجد مستندات ورقية. فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الإلكترونية لا تترك شهوداً يمكن استجوابهم ولا أدلة يمكن فحصها.

2-صعوبة الاحتفاظ بدليل الجريمة الإلكترونية، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر.

3- تحتاج الجريمة الإلكترونية لاكتشافها إلى خبرة فنية، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها. كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الإلكتروني، فقد يتسبب المحقق بدون قصد في إتلاف الدليل الإلكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة

[1] - سعيداني نعيم، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير(في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية –قسم الحقوق –جامعة الحاج لخضر باتنة، 2013،ص34.

[2] - نهلا عبد القادر المومني، المرجع السابق، ص 55.

أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي. لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنيين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الإلكترونية.

4/ كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات لما يتميز به الجاني من خداع و مكر و ذهاء و هذا ما يساعد على عدم التعرف على مرتكبيها.[1]

الفرع الثاني: السمات االخاصة بالمجرم الإلكتروني.

من مظاهر الخطورة التي تتجلى بها الجريمة الالكترونية ان مرتكبيها يتسمون بالذكاء و الدراية في التعامل في مجال المعالجة الالية للمعطيات و الالمام بالمهارات و المعارف التقنية ، فقد يتميز المجرم الالكتروني او المعلوماتي عن غيره من المجرمين بصفات و سمات معينة يمكن إستخلاص أهم هذه الصفات :

1-**الذكاء:** للمجرم المعلوماتي ذكاء من نوع معين ودراية بأحدث ما وصلت إليه التقنية الرقمية في اغلب الأوقات, ولديه القدرة على التفكير وفهم العلاقات بين العناصر المكونة لموقف ما والتكييف معه من اجل تحقيق اهدافه وقد اظهرت الإحصائيات التي أجراها العديد من الباحثتين في أوربا وأمريكا ان مستوى الذكاء يرتبط بنوع الجريمة, فارتفاع مستوى الذكاء قد يدفع بعض الناس الأذكياء المجرمين منهم إلى أنواع معينة من الجرائم فالمجرم في هذا المجال يمتلك القدرة على التفكير بطرق جديدة بمعنى يكون مبدعا ، وهذا يتضمن القدرة على معرفة ذاته وإرضائها والقدرة على التعامل مع الأرقام واستخدامها بما يحقق أهدافه الالكترونية الرقمية ، ولديه الإمكانية على رؤية الاشياء مع بعضها االبعض في الفضاء الالكتروني.[2]

---

[1]-حسين فريجة، الجرائم الالكترونية و الأنترنت، 2011، مقال منشور على موقع http://search.mandumah.com/Record/122156 ، اطلع عليه بتاريخ06-06-2022، الساعة23:22 .

[2] - مشتاق طالب وليد، مرجع سبق ذكره، ص350.

2- **المهارة:** تعد المهارة المتطلبة لتنفيذ النشاط الاجرامي ابرز الخصائص المجرم الالكتروني و التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال او عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات او بمجرد التفاعل الاجتماعي مع الاخرين ، و مستوى المهارة التي يكون عليها المجرم الالكتروني هي التي تحدد الأسلوب الذي يرتكب به الجرائم ، بحيث اذا كان الشخص مرتكب الجريمة الالكترونية على قدر ضئيل من مستوى المهارة نجد ان التي قد يرتكبها لا تتعد الاتلاف المعلوماتي او نسخ البيانات و البرامج اما اذا كان المجرم الالكتروني على درجة اعلى في المستوى المهاري فان أسلوب ارتكابه للجرائم يختلف اذ يمكنه عن طريق استخدام الشبكات بالدخول الى أنظمة الحاسب الالي لسرقة الأموال و ارتكاب جرائم التجسس و زرع الفيروسات و غيرها من الجرائم التي تتطلب مهارة عالية .[1]

كما أن المهارة التي تتميزبها المجرم الالكتروني تمكنه من تكوين تصور كامل لجريمته ، اذ يستطيع ان يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها و ذلك قبل تنفيذ جريمته ، حتى لا يتفاجا بامور غير متوقعة من شانها إفشال مخططاته او الكشف عنها ، فعادة ما يلجا المجرم الالكتروني الى التمهيد لارتكاب جريمته بالتعرف على المحيط الذي يدور فيه و كذا ظروف المحيطة بالجريمة المراد تنفيذها و امكانيات نجاحها او فشلها و يساعده في ذلك درجة المهارة التي يتمتع بها.[2]

3- التنظيم و التخطيط : تتميز الجريمة الالكترونية عادة بوجود أكثر من فاعل للنشاط الاجرامي الواحد، اذ ترتكب اغلب الجرائم الالكترونية من عدة اشخاص يحدد لكل شخص منهم دور معين، و يتم العمل بينهم وفق لتخطيط و تنظيم سابق على ارتكاب الجريمة فقد تحتاج جريمة نسخ برامج الحاسب الالي مثلا الى من يقوم بنسخ تلك البرامج و الى من يقوم بعملية بيعها كما انه من الملاحظ ان الاشخاص الذين يقومون بخلق او تعديل

[1] - خالد ممدوح إبراهيم، المرجع السابق، ص135.

[2] - نائلة عادل محمد فريد قورة، المرجع السابق، ص58.

البرامج لاغراض غير مشروعة ليسوا دئما مستفيدين بطريقة مباشرة من النشاط الإجرامي فالجرائم الالكترونية تتطلب عادة شخصين على الاقل احدهما متخصص في الحاسبات الالية يقوم بالجانب الفني من المشروع الاجرامي و شخص اخر من المحيط ذاته او من خا رج المؤسسة المجني عليها لتغطية عملية التلاعب و تحويل المكاسب.[1] و أحيانا اخرى يمكن تجنيد المجرم الالكتروني القادر على اختراق نظم المعلزمات ضمن عصابات الجريمة المنظمة عن طريق شبكة الانترنت و يمكن من خلال هذه الشبكة تبادل افكار و معلومات التطرف و الارهاب كما يمكن الاتفاق معه على ارتكاب احدى الجرائم الاخلاقية او التلاعب في الحسابات او بطاقات الائتمان.[2]

4- المجرم الالكتروني يبرر ارتكاب جريمته : اثبتت بعض الدراسات انه لا يوجد شعور لدى المجرم المعلوماتي بعدم اخلاقية ما يقوم ب هاو بمساسه بمصالح او قيم يحرص المجتمع على حمايتها بل لا يعتبر ان ما يقوم به يدخل في عداد الجرائم خاصة في الحالات التي يقف فيها السلوك عند حد قاهر نظام الحاسوب و تخطي الحماية المفروضة حوله لذلك فان الكثير من العاملين في مجال المعلوماتية لا يجدون اي خطا في استعمال الشفرات السرية الخاصة بالدخول بالى انظمة الحاسبات الالية بطريقة غير مشروعة او في نسخ البرامج بدلا من شرائها او استعمال الحاسبات الالية للمؤسسات التابعين لها لاغراض شخصية و ما ساعد على هذا الشعور هو عدم وجود احتكاك مباشر بين الجاني و المجني عليه فالتباعد في العلاقة الثنائية هذه يسهل مرور الى الفعل الغير مشروع و يساعد على ايجاد نوع من الاقرار الشرعي الذاتي بمشروعية هذا الفعل الا ان الشعور بعدم اخلاقية هذه الافعال الاجرامية المعلوماتية لدى فئة من المجرمين الالكترونيين لات ينفي وجود مجرمين يرتكبون الاجرامي و هم على علم و ادراك بعدم مشروعية و لاإخلاقية هذا الفعل.

---

[1] - نائلة عادل محمد فريد قورة، المرجع السابق، ص61.

[2] - عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي**، منشأة المعارف، مصر،2009،ص105.

من خلال الملامح التي سبق ذكرها عن خصائص المجرم الالكتروني يمكن تصنيف مرتكبي هاته الجرائم الالكترونية إلى مجموعة من الطوائف نذكرها باختصار:

1-فئة صغار مجرمي المعلوماتية: يسميهم البعض صغار نوابغ المعلوماتية (Pranksters) و هي طائفة الاشخاص الذين يرتكبون الجرائم الالكترونية بغرض التسلية و المزاح دون ان تكون لديهم نية احداث الضرر بالمجني عليه.[1]

2- فئة القراصنة او المخترقون: و في هذه الفئة صنفين:

الهاكر(Les Hakers)[2]،و هم المتطفلون الذين يتحدون امن النظم المعلوماتية من خلال الدخول الى انظمة الحسابات الالية و غالبا لا تكون لديهم نية حاقدة او تخريبية.

الكراكر(Les crakers): وهم الأشخاص الذين يقومون بالتسلل الى أنظمة المعالجة الالية للاطلاع على المعلومات المخزنة بغرض احداث ضرر و العبث بها و سرقتها

3- فئة المحترفين: تعد هذه الفئة هي الاخطر بحيث تهدف اعتداءاتهم على الانظمة بالأساس لتحقيق الكسب المادي سواءا لهم او الجهات التي سخرتهم لارتكاب الجرائم التقنية فضلا عن تحقيق أغراض سياسية او التعبير عن موقف فكري).[3]

4- فئة الحاقدين: وهم فئة لا يسعون الى الاشادة بالتفوق العلمي مثل صغار نوابغ المعلوماتية ولا الى تحقيق الربح كفئة المحترفين و انما هدفهم هو الانتقام كثار لتصرف صاحب العمل تعبيرا منهم عن غضبهم.[4]

المبحث الثاني: الأساس القانوني للجريمة الإلكترونية.

أخذت الجريمة الالكترونية منحنى خطير خاصة بعد ما كشفت عنه الدول من إحصائيات نتيجة الاستخدام الواسع للحواسب الالية والتقنيات الرقمية بمختلف أنواعها، الأمر الذي ألزم تدخلا فعالا للمجتمع الدولي بتكثيف الجهود التشريعية من أجل وضع

---

[1] - مشتاق طالب وليد، مرجع سبق ذكره، ص351.

[2] - عرفت اتفاقية الامم المتحدة لمكافحة اساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية رقم 6355 المؤرخة في 2000/04/12 الهاكر بانه المبرمج المتفوق جدا و لكنه يستخدم جل طاقته في اتجاه غير شرعي لمحاولة اختراق انظمة حاسوبية بهدف اثبات قدرته.

[3] - زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري و الدولي**، دار الهدى، الجزائر،2011،ص22.

[4] - عكوم وليد، **التحقيق في جرائم الانترنت**، متاح على الموقع الإلكتروني:www.arabelawinfo.com

الأسس القانونية الدولية الكفيلة لمكافحة هاته الجريمة **(المطلب الاول)**، و قد ساير المشرع الجزائري المجتمع الدولي في ذلك من خلال وضع إستراتجية متكاملة، قام من خلالها بإصدار وتعديل العديد من القوانين بما يتلائم مع التطور الملحوظ في هذا المجال**(المطلب الثاني)**.

المطلب الأول: التكريس القانوني للجريمة على المستوى الدولي.

إن خطورة الجرائم الالكترونية وخاصيتها الدولية نظرا لإمكانها ان تتجاوز حدود الدولة الواحدة وفي طل التطور التكنولوجي، دفع المجتمع الدولي إلى توحيد جهوده بوضع القواعد القانونية لمكافحة تطور الجريمة الالكترونية ، فالتقدم التكنولوجي وجب ان يرافقه التقدم التشريعي ، لذا أبرمت العديد من المعاهدات وعقدت المؤتمرات و الاجتماعات وسنت عدة اتفاقيات، وسنقوم في هذا المطلب بإبراز معظمها خاصة التي انضمت اليها الجزائر أو تأثرت بها قوانيننا الداخلية لحد كبيرو الذي قسمناه كالأتي .

الفرع الأول: إبرام المعاهدات والإتفاقيات.

أولا/معاهدة الويبو: هي المعاهدة الخاصة بالمنظمة العالمية للملكية الفكرية WIPO ،تملك مركز متخصص في تسوية المنازعات المتعلقة بالملكية الفكرية.[1]

و باعتبار ان حق الملكية الفكرية من أكثر الحقوق التي يتم انتهاكها بصفة مستمرة بكافة شبكات الاتصال كالمعلومات وخصوصا على شبكة الأنترنت كان من الضروري إيجاد منظمات تسعى لتوفير الحماية للملكية الفكرية،و كانت اول خطة تجسدت على أرض الواقع تشكيل المنظمة العالمية للملكية الفكرية " WIPO " حيث تعتبر هذه المنظمة منظمة دولية غير حكومية واحدى الوكالات المتخصصة التابعة لمنظمة الأمم المتحدة مقرها جنيف وقد تأسست بموجب اتفاقية ستوكهولم التي أبرمت في 1967 ودخلت حيز التنفيذ عام،1970بلغ عدد الدول الأعضاء في هذه المنظمة 177 دولة في عام 1999، ترتكز نشاطات واختصاصاتها في دعم حماية الملكية الفكرية بفرعيها الملكية الصناعية والملكية الأدبية في جميع أنحاء العالم بفضل تعاون الدول مع بعضها البعض في هذا المجال و تنقسم الى 3 معاهدات :

[1] - زبيحة زيدان، المرجع السابق، ص 17.

1- **معاهدة الويبو بشان حق المؤلف:** تم التوقيع عليها في 20ديسمبر 1990 وتتكون من 18 مادة تقوم على عدة اسس منها الالتزاماتالمتعلقة بالتدابير التكنولوجية.

2- **معاهدة الويبو بشان التسجيل الصوتي** :تم التوقيع عليها هي الاخرى في 20ديسمبر 1990 بها اربع فصول ، الاول متعلق بالاحكام العامة و الثاني بالحقوق المالية و المعنوية لفناني الاداء و الفصل الثالث يتناول حقوق المنتجين كحق إتاحة التسجيلات الصوتية، اما الرابع فيتعلق بالاحكام المشتركة كالحق في مكافأة مقابل الإذاعة والاستثناءات والالتزامات المتعلقة بالتدابير التكنولوجية و كذا التعرض للاجراءات الشكلية.

3- **معاهدة الويبو بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة:** تبدأ الاتفاقية بمقدمة تتناول الطابع القانوني للمعاهدتين الجديدتين ، ثم تتناول جدول الاعمال الرقمي والمعاهدات الجديدة ثم تتعرض الاتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديدتين وأخيرا اعمال المتابعة بعد المؤتمر الديبلوماسي .

إن معاهدة الويبو الخاصة بحماية حقوق المؤلف لها دور هام في حماية البرمجيات حيث نصت المادة 4 منها بتمتع برامج الكمبيوتر بالحماية باعتبارها مصنفات أدبية بالمعنى الوارد في المادة 2 اتفاقية برن، كما تعمل على اقامة التوازن بين مصالح الدول المتقدمة و الدول النامية.[1]

ثانيا/إتفاقية برن: تم التوقيع عليها بسويسرا سنة 1971 وهي حجر الأساس في مجال حماية الدولية لحقوق المؤلف وقعت عليها 120 دولة ، والتي خضعت إلى تعديلات كان آخرها تعديل باريس في 1971/07/24 و 1979/09/28، و قد انضمت إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 341/97 في 1997/09/13. [2]

و بموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي "الكمبيوتر" سواء كانت بلغة المصدر، أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية وفقا لما جاء فيها. كما انها تقوم على مجموعة من المبادئ الأساسية التي تحدد نطاق الحماية الواجبة كأسلوب تطبيقها،

[1] - بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي**، أطروحة دكتوراه تخصص القانون العام، كلية الحقوق و العلوم السياسية – جامعة بن يوسف خدة، الجزائر،2018، ص19و20

[2] - زبيحة زيدان، المرجع السابق، ص 21.

هذه المبادئ لا تتغير مع التعديلات أو البروتكولات التي قد تدخل على الاتفاقية فلابد ان تكون متفقة معها.[1]

-مبدأ المعاملة الوطنية: يقصد بهذا المبدأ أن تتمتع كافة المصنفات الخاضعة لحماية الاتفاقية في اقليم دولية عضو بنفس الحماية التي تتمتع بها المصنفات الوطنية لهذه الأخيرة لدى الدولة الأخرى الطرف في هذه الاتفاقية.

- الحد الأدنى للحماية: يعد هذا المبدأ محاولة من واضعي قواعد الاتفاقية لمواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة وجاء ليقرر تمتع المؤلفين بالحقوق المقدرة في هذه الاتفاقية.

ثالثا/إتفاقية التريبس: إتفاقية أوجه التجارة المتعلقة بالملكية الفكرية بها 73مادة صادقت عليها الجزائر بمقتضى الامر رقم 75/02 المؤرخ في 1975/01/09.[2]

وقد شملت مواد اتفاقية تريبس الخاصة باوجه التجارة المتصلة بحقوق الملكية الفكرية على مكافحة الجريمة الالكترونية بالنص في المادة 1/10على أنه تتمتع برامج الحاسب الآلي أو الكمبيوتر سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971 كما نصت في فقرتها الثانية على حماية البيانات المجمعة أو المواد الاخرى بشروط معينة كشرط الأصالة سواء أكانت مقروءة آليا أو بشكل آخر، وإذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها.[3]

- **رابعا/ إتفاقية بوداباست** : شكلت الاتفاقية الاوربية لمكافحة الجريمة الالكترونية خطوة رائدة لمجابهة هذا الخطر وقد جاءت هذه الاتفاقية لتكتل جهود مجموعة من الخبراء الاوربيين و الغير اوربيين و التي عملت ضمن "خبراء لمكافحة الجريمة في الفضاء السبراني" من الاتفاقيات التي عقدت بشان مكافحة الاجرام الالكتروني ، عقدت من طرف المجلس الاوربي في 08 نوفمبر من سنة 2001 تضمنت هذه الاتفاقية 48 مادة موزعة بنودها على ثلاثة محاور:[4]

---

[1] - بدري فيصل، المرجع السابق، ص16.

[2] - لينا محمد الأسدي، مرجع سبق ذكره، ص 88.

[3]- طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة لنيل شهادة ماجستير تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة الجزائر 1 ، 2011-2012، ص76.

[4] - منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية، 2015، ص115.

– المحور الأول: تناول انسجام بين التشريعات الوطنية التي تجرم الاعمال الغير قانونية في الفضاء السبراني، اي مجموعة الجرائم التي يمكن أن تتعرض لها النظم المعلوماتية

– المحور الثاني: تناول وسائل التحقيق و الملاحقة الجزائية التي تنسجم مع الطبيعة العالمية يمكن أن تتخذ في مواجهة هذا النوع من الجرائم

– المحور الثالث: تناول نظام التعاون بين الدول الأعضاء الموقعة على الإتفاقية

و يمكن الاشارة للمحور الاول ان هذه الاتفاقية قامت على تقسيم صور و انواع الجرائم الالكترونية الى 04 صور نذكرها كالاتي :[1]

–الصورة الاولى : التعريف بمعطيات الكمبيوتر ومزودي الخدمة (المادة 01) و ما يخص أمن المعلومات و تشمل: جريمة الدخول الغير قانوني (المادة 02 من الاتفاقية) – الاعتراض غير قانوني (المادة03) – التدخل في المعطيات(المادة04) – التدخل في نظم الحاسوب(المادة 05) – إساءة استخدام الاجهزة(المادة 6)

اما الصورة الثانية: تضم الجرائم المرتبطة بالكمبيوتر : مثل جريمة التزوير عن طريق الحاسوب(المادة07)– الاحتيال بواسطة الكمبيوتر (المادة 08)

الصورة الثالثة: تشمل الجرائم المرتبطة بالمحتوى وتشمل تلك الجرائم التي تتعلق بالاباحية بالاطفال عن طريق الانترنت(المادة09).

اما الصورة الأخيرة تتعلق بتلك التي من خلالها الاعتداء على الحقوق الفكرية و حقوق المؤلف (المادة 10) .

هذا و قد الزمت هذه الاتفاقية الدول المنظمة اليها إقرار العقوبات الملائمة و التدابير الفعالة لهذه الجرائم سواءا كانت سالبة للحرية للاشخاص الطبيعية او عقوبات مالية للاشخاص المعنوية. [2]

الفرع الثاني : المؤتمرات و تشريعات المنظمات الدولية .

تعد ايضا من المراجع التي تتخذ لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي بشكل عام.

[1] - لينا محمد الأسدي، المرجع السابق، ص88.
[2] -لينا محمد الأسدي، نفس المرجع، ص89.

اولا/ مؤتمرات منظمة الأمم المتحدة : لقد كانت منظمة الأمم المتحدة من الهيئات الدولية السباقة إلى وضع خريطة طريق للتصدي للجريمة الالكترونية، والحث على تعزيز العمل المشترك والتعاون بين الدول الأعضاء من أجل الحد من انتشارها وتعاظم أثارها وذلك من خلال اشرافها على عقد مؤتمرات دولية في هذا المجال ، ويتجلى اهتمام منظمة الأمم المتحدة الجريمة الالكترونية في:

1-المؤتمر السابع للامم المتحدة: الخاص بمنع الجريمة و معاملة المجرمين المنعقد بمدينة ميلانو الايطالية في 1985 والذي أكدت لجنة الخبراء به على ضرورة الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هده الظاهرة. وقد أشارت إلى مسألة الخصوصية واختراقها بالإطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي وضرورة اعتماد ضمانات لحماية سريتها.[1]

2-المؤتمر الثامن للأمم المتحدة : المنعقد بهافانا في عام 1990، وبالفعل عرضت نتائج هذا تقرير المؤتمر السابع وتمت الموافقة عليها ثم أصدرتها منظمة الأمم المتحدة على شكل جملة من التوصيات بخصوص الجريمة الالكترونية، أكدت فيها بأن مواجهة هذا النوع الجديد من الإجرام يتطلب من الدول الأعضاء اعتماد عدة تدابير أهمها:

- ضرورة تحين وتحديث القوانين الموضوعية والإجرائية للجرائم الالكترونية والعمل على تحسين أمن المعلومات والوقاية المتعلقة بالحسابات الآلية وشبكات الانترنت المتصلة بها.
- وضع التدابير الوقائية والأمنية لمنع الجريمة مع مراعاة خصوصية الافراد واحترام حقوق الإنسان.
- توعية الجماهير بخطورة الجريمة الالكترونية و أهمية مكافحتها.

3- القانون النموذجي للامم المتحدة حول الوقاية من الجرائم الالكترونية ومكافحتها : تم اصداره في عام 1994 ، موجه إلى مساعدة حكومات الدول في إحداث نصوص قانونية داخلية خاصة بالإجرام الالكتروني، وكذا تحيين قوانينها الموجودة حتى تواكب تطورات هذا النمط من الاجرام . وقد تضمن هذا القانون على وجه الخصوص تحديد المفاهيم الأساسية للجرائم الالكترونية، والتي قسمها إلى صنفين، الأول يتعلق بالجرائم

[1] - صديق حياة، خصوصية الجريمة المعلوماتية، مذكرة تخرج لنيل إجازة القضاء، المدرسة العليا للقضاء، الجزائر، 2005-2008، ص22.

التي تكون الوسائل الالكترونية محلا لها، أما الصنف الثاني، فيتعلق بالجرائم المرتكبة بواسطة وسائل تكنولوجية الإعلام و الاتصال أو الوسائل الالكترونية بصفة عامة .

ثانيا/ قانون الانسيترال النموذجي بشأن التجارة الالكترونية: اعتمدته لجنة الأمم المتحدة في عام 1996 ، الذي يعتبر مرجعا مهما للدول في مواجهة جرائم الانترنت في مجال التجارة الالكترونية، وقد كان الهدف الرئيسي من وضع هذا القانون هو تعزيز تنسيق وتوحيد القانون التجاري الدولي بغية ازالة أية عقبات لا لزوم لها أمام التجارة الدولية تنتج عن أوجه القصور والاختلاف في القانون المتعلق بالتبادل التجاري، واستمرارا في هذا المسار أصدرت اللجنة ذاتها القانون النموذجي بشأن التوقيعات الالكترونية في عام 2001باعتباره صكا قانونيا جديدا مستمد من قانون الانسيترال النموذجي بشأن التجارة الالكترونية، ومتسقاَ مع أحكامه وبشكل مفصل.

ثالثا/ المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات : المنعقد في ريو دي جانيرو بالبرازيل في 1994 بشان جرائم الكمبيوتر وكانت نتائجه مجموعة من المقررات و التي نصت على الافعال التي تعتبر من قبيل جرائم الكمبيوتر وهي:

جريمة الاحتيال او الغش المرتبط بالكمبيوتر – جريمة التزوير المعلوماتي – جريمة اتلاف بيانات الكمبيوتر –جريمة الدخول الغير مصرح به .[1]

رابعا/ الاتحاد الدولي للاتصالات: الذي يضم أكثر من 192دولة و 700 شركة من القطاع الخاص والمؤسسات الأكاديمية، فانه يوفّر منبرا استراتيجيا للتعاون التشريعي والفني بين أعضائه باعتباره وكالة متخصصة داخل منظمة الأمم المتحدة، إذ سطّر الاتحاد مؤخرا مخططا دوليا لتعزيز الأمن السيبراني العالمي، وناد كل الفاعلين إلى تجسيده والعمل بمقتضاه.

خامسا/ منظمة التعاون و التنمية الاقتصادية (OCD): تعود أولى اهتمامات المنظمة بالجرائم الالكترونية إلى عام ،1980حينما وضعت دليل تشريعي يتضمن مجموعة من قواعد إرشادية لحماية الخصوصية و نقل البيانات عبر وسائل الاتصال الالكترونية وأوصت الدول الأعضاء إدراجها ضمن تشريعاتها الداخلية والالتزام بها، ومن بين هذه القواعد:

[1] - لينا محمد الأسدي، مرجع سابق، ص91.

ـ الحق في الخصوصية مضمون، ولا يجوز الاطلاع على المعلومات الخاصة للأفراد أو إفشائها إلا في إطار القانون بعد علمهم و موافقتهم على ذلك.

ـ لا يجوز استعمال المعلومات الخاصة للافراد لاغراض أخرى غير تلك التي تم الحصول عليها من اجله.[1]

المطلب الثاني: التكريس القانوني للجريمة الالكترونية على مستوى الوطني.

عمل المشرع الجزائري على مسايرة النسق التشريعي الخاص بمكافحة الجرائم المعلوماتية خصوصا و أن الجزائر تعرف مؤخرا وفي السنوات الأخيرة تعميم خدمة الربط بشبكة الانترنت، وهو ما تولد عنه ارتفاع محسوس في معدلات الجريمة المعلوماتية.[2]

ولمسايرة هذا التطور التكنولوجي وتنامي هذا النوع من الجرائم و جعل قوانينا تنسجم مع التشريعات الدولية خاصة بعد انضمام الجزائر الى الاتفاقيات الدولية الخاصة كان لابد للمشرع الجزائري من إيجاد الإطار القانوني المناسب بوضع النصوص الملائمة المختلفة لاستعمالات الإعلام الآلي حيث اعتمد على إستراتيجية مزدوجة لمواكبة الجريمة الالكترونية، بحيث قام من جهة بتعديل العديد من القوانين الوطنية بما فيها التشريعات الجزائية العقوبات و الإجراءات وجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجي الإعلام والاتصال(الفرع الاول). وقام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر انسجاما مع الطبيعة المميزة للجريمة الالكترونية (الفرع الثاني).

الفرع الأول: القوانين العامة .

قام المشرع الجزائري في إطار مواجهة الجريمة الالكترونية على تعديل بعض مواد بالقوانين العامة و التي مست:

---

[1] - براهيمي جمال، **التحقيق الجنائي في الجرائم الالكترونية** ، أطروحة دكتوراه كلية الحقوق و العلوم السياسية، جامعة مولود معمري –تيزي وزو، الجزائر، 2018،ص275–276–277.

[2] - ربيعي حسين، **آليات البحث و التحقيق في الجرائم المعلوماتية**، رسالة دكتوراه كلية الحقوق ، جامعة باتنة ، 2016، ص 114و115

أولا/الدستور الجزائري : لقد كفل دستور الجزائر لسنة 1996وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016حماية حقوق الأساسية والحريات الفردية ،وعلى أن تضمن الدولة عدم إنتهاك حرمة الإنسان ،وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق ،ومن أهم المبادئ الدستورية العامة:

المادة 38:الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

المادة 44: حرية الإبتكار الفكري والفني والعلمي مضمونة للمواطن ،حقوق المؤلف يحميها القانون. ولا 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. [1]

تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة إذ لا يجوز إنتهاك حرمة حياة المواطن الخاصة ، وحرمة شرفه ،كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة و يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي .[2]

كما تتجلى مكافحة التشريعية للجريمة الالكترونية في الدستور الجزائري بالرجوع إلى القانون رقم 16-01 المؤرخ في 2016/03/06 والمتضمن التعديل الدستوري في المادة 46 : على انه" لايجوز انتهاك حرمة حياة المواطن الخاّصة، وحرمة شرفه، ويحميها القانون. سرّية المراسلات الخاصة بكل أشكالها مضمونة3 . وبهذا عمل المشرع عمل حماية حرمة الخاصة للأفراد من كل اعتداء، ومهما كانت الوسيلة المستخدمة ولو كانت إلكترونية. [4]

---

[1] -المرسوم الرئاسي رقم96-438 المؤرخ في 6 ديسمبر1996، المتضمن التعديل الدستوري لسنة 1996.

[2] - بوضياف إسمهان، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف –المسيلة ، العدد الحادي عشر،2018،ص116

[3] - القانون رقم 16- 01 المؤرخ في 6 مارس 2016 الجريدة الرسمية رقم14 مؤرخة في 07 مارس 2016.

4 حوالف عبد الصمد، **الآليات القانونية لتلافي الجريمة المعلوماتية والحد من إنتشارها وفقا للتشريع الجزائري**، مجلة الفكر القانوني و السياسي، كلية الحقوق و العلوم السياسية ، جامعة تلمسان، العدد الرابع، 2018،ص91

ثانيا/ قانون العقوبات : كان أول تشريع خاص بهذا المجال قد صدر بتاريخ 2004/11/10 بموجب القانون 04-15 المعدل و المتمم لقانون العقوبات الجزائري من خلال إقرار واستحداث قسم خاص معنون بقسم جرائم المساس بأنظمة المعالجة الآلية في القسم السابع مكرر من قانون العقوبات من الفصل الثالث في الباب الثاني الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بنص المواد 394مكرر إلى المادة 394مكرر7 [1]،وباستقراء هذه المادة يتضح لنا أن المشرع قسم الجرائم الالكترونية إلى أربع طوائف تتعدد بحسب المصالح المحمية التي نذكرها كالاتي :

-الطائفة الأولى: وتتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

- الطائفة الثانية: الجرائم الالكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص علىها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي.

- الطائفة الثالثة:الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب.

- الطائفة الرابعة:الجرائم الالكترونية للشخص المعنوي والتي تعادل عقوبتها خمس مرات عقوبة الشخص الطبيعي المادة 394مكرر 4من قانون العقوبات.

وفي سنة 2006قام المشرع بإدخال تعديلات جديدة مست القسم السابع مكرر منها، حيث تم تشديد العقوبة على كل الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها،وسعيا منه لتحقيق الردع العام على اثر التزايد الخطير لنسب الجرائم المرتكبة وخطورتها على الأفراد من جهة وعلى الاقتصاد الوطني من جهة أخرى[2].

[1] - القانون 15/04، المؤرخ في 10نوفمبر2004 ، جريدة رسمية عدد71مؤرخة في 10نوفمبر ،2004 المعدل و المتمم للأمر رقم 66-156المؤرخ في 8يونيو1996 المتضمن قانون العقوبات المعدل و المتمم.

[2] - سعيدة بوزنون، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، الجزائر، المجلد 30، العدد3 ،2019، ص52

والملاحظ أن تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة ومتميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطالها وكذا من حيث مبناها وطبيعتها ومحلها، ومن ثم لا يمكن إدراجها تحت أي نوع من الجرائم التقليدية .[1]

ثالثا/ قانون الإجراءات الجزائية: سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها، أو على الأقل الحد من انتشارها، حيث انه بتعديلي ، 09/01 و 14/04وضع قواعد و أحكام خاصة لسلطة المتابعة و الاختصاص و هي : [2]

جواز تمديد الاختصاص المحلي للمحكمة :حيث نصت المادة 329من ق ا ج

توسيع مجال اختصاص النيابة العامة :حيث انه وبموجب المادة 37من ق اج تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى

– العمل بنظام المشروعية في تحريك الدعوى العمومية : حيث سحب نظام الملاءمة من النيابة العامة في مجال متابعة بعض الجرائم

– بالاضافة الى مجموعة إجراءات التحري والتحقيق المتمثلة في : التفتيش، اعتراض المراسلات السلكية واللاسلكية والتقاط الصور وتسجيل الأصوات، التسرب. [3]

الفرع الثاني : القوانين الخاصة.

اولا / القانون المدني الجزائري :ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الإعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124من التقنين المدني الجزائري» كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض «وقد جاء هذا النص عاما وشاملا لأي إعتداء يقع على أوي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة ،وقد أورد هذا النص مبدأ مهما هو حق من وقع إعتداء على حياته الخاصة في

[1] - سعيداني نعيم، المرجع السابق، ص 112.
[2] - طرشي نورة، المرجع السابق، ص138.
[3] -جمال براهيمي، المرجع السابق، ص39.

التعويض عما لحقه من ضرر ،فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض فالفعل الضار هو أساس المسؤولية «وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الإعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الأنترنت ،وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات ،وفي تحديد هوية المعتدى ،وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل إعتداء قابل للإثبات وإن وقع على الشبكة. [1]

ثانيا/القانون الخاص بالوقاية من الجرائم الخاصة المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته[2]: تضمنت المادة الأولى من هذا القانون الهدف منه وهو الوقاية من الجريمة المعلوماتية، ويصبو هذا القانون إلى التمكين من مكافحة الجريمة المعلوماتية عن طريق مجموعة من التدابير متمثلة في تحديد الحالات التي يجوز فيها لسلطات الأمن مراقبة المراسلات الإلكترونية وهي أربع حالات:

-الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب، والجرائم ضد أمن الدولة.

-عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة والدفاع الوطني أو النظام العام

- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية، دون اللجوء إلى المراقبة الإلكترونية.

[1] - اسمهان بوضياف ، المرجع السابق، 361.

[2]-القانون رقم **09-04** مؤرخ في 5 أوت 2004 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد47 ، الصادرة بتاريخ 16 اوت 2009.

-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1]

كما تضمن قانون 09-04 إجراءات جديدة تدعم تلك المنصوص عليها في قانون الاجراءات الجزائية ولاسيما المتعلقة بالجرائم المعلوماتية بخصوص اساليب التحري الخاصة (التفتيش –المعاينة- التسرب – الخبرة- اعتراض المراسلات والتسجيل الصوتي – المراقبة الالكترونية) .

ثالثا/ القانون الخاص بالملكية الأدبية والفنية: بعد انضمام الجزائر الى الاتفاقيات الدولية الخاصة المتعلقة بالملكية الفكرية ذات العلاقة بالتجارة المسماة تريبس و كذا اتفاقية برن للمصنفات الادراية و الفنية حاول المشرع الجزائري مواجهة الجريمة الالكترونية من خلال هذا القانون بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 و المعدل و المتمم بالامر 05/03 المؤرخ في 2003/07/19 [2]حيث تم دمج بموجب هذين الامرين الاخيرين برامج الاعلام الالي ضمن المصنفات الاصلية التي تشملها الحماية القانونية[3]

رابعا/ القانون المتعلق بالبريد و المواصلات السلكية واللاسلكية : وهو القانون رقم 03/2000 المؤرخ في 2000/08/05 حيث سارع هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية في مواجهة الجريمة خاصة اثناء التحويلات المالية بواسطة الحوالات عن الطريق الالكتروني.

[1] - رابح سعاد، مجلة القانون العام الجزائري والمقارن. ضوابط مكافحة الجريمة المعلوماتية ،جامعة جيلالي ليابس بلعباس، المجلد السابع، العدد 1 ، جوان 2021 ، ص 273

[2] - زبيحة زيدان، المرجع السابق، ص 21.

[3] - نص المادة 4 من الامر 10/97:" تعتبر على الخصوص مؤلفات ادبية او فنية محمية ما ياتي: المصنفات الادبية المكتوبة مثل...و قواعد البيانات"

كما أحاط القانون سرية المراسلات بحماية خاصة من اي انتهاك وقرر عقوبات لذلك وهذا ما نص عليه في المادة105 بالفقرة الاخيرة "لا يمكن باي حال من الاحوال انتهاك سرية المراسلات".[1]

خامسا/ قانون التامينات الإجتماعية : القانون رقم 01/08 المؤرخ في 23جانفي 2008 و المتمم للقانون رقم 11/83 المتعلق بالتامينات ، حيث بادر المشرع الجزائري بعد تعميم الشبكة المعلوماتية على مستوى الوطن ، الى ان صفة المؤمن له إجتماعيا تثبت ببطاقة الكترونية و حدد المادة 6 مكرر1 من القانون ان البطاقة الالكترونية تسلم للمؤمن له اجتماعيا مجانا من طرف هيئات الضمان الاجتماعي .[2]

ونظرا لكون البطاقة الالكترونية تحتوي على معلومات خاصة متعلقة بحياة الأفراد فقد أضفى القانون نفسه حماية عليها و اقر كذلك عقوبات على استعمالها بطريقة غير شرعية.[3]

سادسا/ القانون المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي: كما ذكرنا سابقا ان التعديل الدستوري ضمن القانون رقم 16-01 المؤرخ في 2016/03/06 في المادة 46 والذي كرس مبدا حماية الاشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حيث بعد هذا التكريس الدستوري قام المشرع الجزائري بعدها بوضع القانون رقم 07/18 المؤرخ في 10ماي 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي والذي اضاف دفعة تشريعية في مجال مكافحة الجرائم الالكترونية يحتوي على 76 مادة متضمنة مبادئ حماية المعطيات ذات الطابع الشخصي و كذا مهام الهيئة المستجدة المتمثلة في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بالاضافة الى احكام اجرائية و جزائية.[4]

---

[1] -زبيحة زيدان، المرجع سابق، ص78.

[2] - زبيحة زيدان، نفس المرجع، ص78.

[3] -انظر المادة 93 مكرر 3 القانون رقم 01/08 المؤرخ في 23جانفي 2008 و المتمم للقانون رقم 11/83 المتعلق بالتامينات.

[4]- القانون رقم 07/18 المؤرخ في المؤرخ في 10ماي 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي الجريدة الرسمية، عدد34.

المبحث الثالث : أركان الجريمة الالكترونية .

إن أركان الجريمة عموما هي تلك العناصر التي لا وجود للجريمة بدونها، حيث تدور الجريمة معها وجودا وعدما، وتتمثل الأركان العامة للجريمة في الركن الشرعي (**المطلب الأول**) وهو النص الجزائي الذي يحوي النموذج القانوني للفعل أو الامتناع المجرم، ثم العناصر المكونة للركن المادي (**المطلب الثاني**)، وأخيرا الركن المعنوي القائم على العلم والإرادة (**المطلب الثالث**). [1]

غير أن الجريمة الالكترونية تتميز بوجود نظام المعالجة الآلية للمعطيات والذي يعد بمثابة الشرط الأولي الخاص الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام ما يجعلها تختلف عن الجرائم الكلاسيكية و هذا ما سنتطرق إليه في مبحثنا هذا بتبيان أركان الجرائم الالكترونية مع الإشارة إلى خصوصيتها.

المطلب الأول: الركن الشرعي.

هو نص التجريم القانوني الذي يبين الفعل المكون للجريمة و يحدد العقاب الذي يفرضه على مرتكبها.[2] فالركن الشرعي الذي يعزز مبدأ شرعية ، وسنتطرق الى مدى تطبيق المشرع الجزائري لمبدا الشرعية بخصوص الجرائم الالكترونية ونصوص التجريم للفعل .

الفرع الأول: تطبيق مبدأ الشرعية.

إن غالبية التشريعات الجنائية المقارنة تعتد بمبدأ الشرعية الجنائية ، والذي مفاده أن المقصود بالمبدأ هو حصر مصادر التجريم والعقاب في نصوص القانون، بوضع الركن الشرعي للجريمة بتحديد النشاط الذي يعد جريمة جزائية ، وكذلك تحديد العقوبات المقررة لها .[3]

---

[1] – ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية و الاجتماعية ،المجلد الرابع، العدد الثالث، جامعة مولود معمري تيزي وزو، الجزائر، 2019، ص 132.

[2] - عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، 1995، ص68.

[3] - شوقي يعيش تمام، المرجع السابق، ص34.

وتأسيسا على أول مبدأ في قانون العقوبات وهو مبدأ الشرعية الذي يقضي بأن "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"[1]

و تطبيقا للمبدأ يمكن القول ان المشرع الجزائري أشار للجرائم الالكترونية و أعطى لها مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات حيث عرف هذا الاخير بأنه: " كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ،"وهو نفس التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست في 2001.[2]

وقد خصص القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 صور للجرائم الإلكترونية تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر من الفصل الثالث المعنون " الجنايات والجنح ضد الأموال من الباب الثاني المتعلق "بالجنايات والجنح ضد الأفراد وذلك في المواد من 394مكرر الى 394 مكرر08 من قانون العقوبات المعدل والمتمم حيث تطرق الى العديد من صور هاته الجرائم التي سنذكرها لاحقا .

ولجوء المشرع الى تقنين او النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء الى القياس، بمعنى عدم جواز لجوء القاضي الجنائي الى قياس فعل لم يرد نص على تجريمه على فعل ورد نص بتجريمه ، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب تشابه .[3]

للإشارة في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون عقوبات06-23 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا

---

[1]- المادة الاولى من القانون 15/04، المؤرخ في 10نوفمبر 2004 ، جريدة رسمية عدد71مؤرخة في 10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156المؤرخ في 8يونيو 1996 المتضمن قانون العقوبات المعدل و المتمم.

[2] - زيوش عبد القادر، المرجع السابق، ص 132.

[3] - حمزة عشاش، حمزة خضري، المرجع السابق، ص172.

القسم من القانون 15/04. وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل المعلومات حيث بلغ عدد مستخدمي الانترنت ذات التدفق العالي وعبر الهاتف المحمول 11مليون شخص لسنة 2012 .[1]

الفرع الثاني: صور الجرائم الإلكترونية المنصوص عليها في قانون العقوبات الجزائري.[2]

اولا/ الجرائم المنصوص عليها في المادة 394مكرر

- جريمة الدخول عن طريق الغش للأنظمة المعلوماتية.
- جريمة البقاء غير المشروع في الأنظمة المعلوماتية.
- جريمة تغيير أو حذف معطيات المنظومة .
- جريمة تخريب او اتلاف نظام الإشتغال.

ثانيا/ الجرائم المنصوص عليها في المادة 394مكرر1

- جريمة إدخال معطيات في منظومة معلوماتية خلسة.
- جريمة إزالة أو تعديل معطيات في منظومة معلوماتية .

ثالثا/ الجرائم المنصوص عليها في المادة 394مكرر 2:

- جريمة تصميم أو بحث في المعطيات المخزنة او المعالجة آليا
- جريمة إعاقة سير المعلومات بواسطة و منظومة معلوماتية
- جرائم الإحتيال الإلكتروني باستعمال بطاقات الإئتمان و الدفع الإلكتروني .

رابعا/الجرائم المنصوص عليها في المادة 394مكرر3:

- الجرائم الالكترونية المرتكبة إضرارا بمؤسسات الدفاع الوطني

[1] - نعيم سعيداني، المرجع السابق، ص 111و 112.
[2] - زيبحة زيدان، المرجع السابق، ص 46و47.

- الجرائم الالكترونية المرتكبة ضد الهيئات والمؤسسات
- الجرائم الالكترونية الخاضعة للقانون العام.

خامسا/ الجرائم المنصوص عليها في المادة 394مكرر4: الجريمة الالكترونية المرتكبة ضد الشخص المعنوي

سادسا/جريمة الاتفاق الجنائي المنصوص عليها في المادة 394مكرر 5 :قد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394مكرر5 ،بغرض التحضير للجرائم الماسة لأنظمة المعلوماتية، ولم يخضعها لأحكام المادة 176من قانون العقوبات المتعلقة بجمعية الأشرار، بحيث تنص المادة 394مكرر 5 من قانون العقوبات "كل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها قي هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها ".

سابعا/ جريمة الشروع في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات : تبناه المشرع الجزائري في المادة 394مكرر7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي و لا عقاب على الشروع في الجنح إلا بنص.

المطلب الثاني : الركن المادي و المعنوي للجريمة الإلكترونية.

الجريمة الالكترونية كغيرها من الجرائم الكلاسيكية الاخرى تقوم على الأركان العامة للجريمة من ركن مادي وركن معنوي الا انهما يتميزان ببعض الاختلافات عن اركان هاته الاخيرة وهذا ما سنتناوله في هذا المطلب :

الفرع الأول: الركن المادي للجريمة الإلكترونية.

الركن المادي للجريمة هو المظهر الخارجي لها وكيانها المادي الظاهر، وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، فالقاعدة انه "لا جريمة دون ركن مادي" أو " إلا أن الركن المادي للجريمة الالكترونية يختلف نوعا ما عن الجرائم التقليدية كون انه يقوم على عدة صور من الاعتداءات .[1]

[1] - حمزة عشاش، حمزة خضري، المرجع السابق، ص174.

وقد تطرقنا من قبل إلى صور الجرائم الالكترونية أو الاعتداء الواقع على النظم المعلوماتية المنصوص عليها بقانون العقوبات الجزائري و التي يختلف سلوكها الإجرامي من جريمة الى اخرى ، عليه سنوضح الأفعال الإجرامية المنصوص عليها على سبيل الحصر والتي نوردها كما يلي:

أولا/ في جرائم الدخول والبقاء غير المرخص بهما في النظام : لقد نصت المادة 394 مكرر من قانون العقوبات الجزائري على تجريم سلوكي الدخول والبقاء غير المرخص بهما للنظم المعلوماتية.

الدخول: هو الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام . ويتحقق الدخول غير المصرح به متى كان مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه .

البقاء : يقصد به استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السيطرة عليه، بمعني أخر هو بقاء شخص داخل نظام المعالجة ملك الغير بعد الدخول إليه خطأ أو صدفة، رغم علمه بأن بقاءه فيه غير مرخص.

ثانيا/ في جرائم الاعتداء على المعطيات الداخلية للنظام: لقد جرم المشرع الجزائري أي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الآلية من خلال المادة 394 مكرر 1 من قانون العقوبات ، وحدد في ذات المادة صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر . [1]

الإدخال : يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام و التي تمت معالجتها آليا.

المحو: يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

التعديل: يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات أخرى. ولا يشترط اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني إحداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة.

[1] - عبد القادر عميمر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري(دراسة مقارنة)**، أطروحة لنيل شهادة الدكتوراه تخصص قانون جنائي، جامعة يوسف بن خدة الجزائر، 2019-2020، ص111و112.

ثالثا/ في جرائم الاعتداء على المعطيات الخارجية للنظام: يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقيق نتيجة معينة تمثل في المعالجة الآلية للمعطيات، وقد نص عليها المشرع الجزائري في المادة 394مكرر2 من قانون العقوبات حيث ان كل من يقوم عمدا أو عن طريق الغش بـ: [1]

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيـات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

الحيازة : هي سيطرة واقعية وإرادية للحائز على المنقول تخوله مكنة الانتفاع به أو تعديل كيانه أو تحطيمه أو نقل فهي سيطرة إدارية للشخص على الشيء والحيازة قد تستند إلى سبب صحيح قانونا كما يمكن أن تكون غير مشروعة ولكن في جريمة التعامل في المعطيات غير مشروعة تكون دائما غير مستندة لسبب غير شرعي ذلك أنها متحصله من إحدى جرام المعطيات .

الإفشاء : يفترض تقديم معطيات غير مشروعة لأشخاص آخرين ولا يشترط أن يكون هذا الشخص ملتزما بكتمان هذه المعطيات، بمقتضى وظيفة أو عقد ما وإنما هو شخص تحصل على هذه المعطيات بطريقة غير مشروعة.

النشر : من قبيله قيام المخترقين (الهاكرز) باختراق مواقع معينة وحصولهم على كلمات العبور فيها والقيام بنشرها على الجميع نكاية بأصحابها وتحديا لهم . ولم تحدد المادة إدا كان النشر بمقابل أم لا ولا كيفية ووسيلة النشر فقد يكون عن طريق شبكة الإنترنت أو الأقراص المضغوطة أو كانت طريق الكتابة .

[1] - حوالف حليمة، مهاجي فاطمة الزهراء، **معالم الجريمة المعلوماتية في القانون الجزائري**، مجلة البحوث القانونية و السياسية ،جامعة ابو بكر بلقايدتلمسان، الجزائر، المجلد 3 العدد 16،فيفري 2021، ص 148.

الإستعمال: يعتبر أخطر الأفعال كأن تستعمل شركة ما معطيات أو معلومات عن شركة منافسة لها تم الحصول عليها بطريقة غير مشروعة، ويشمل التجريم كل أنواع الاستعمال مما كان الغرض.

التصميم: تتمثل في إخراج المعطيات إلى الوجود أي القيام بخلق وإيجاد معطيات صالحة لإرتكاب الجريمة وهذا العمل يقوم به المختصون كالمبرمجين و مصممي البرامج. ومثال هذه الجريمة تصميم برنامج يحمل فيروسا أو ما يعرف بالبرامج الخبيئة أو تصميم برنامج اختراق.

البحث: ويقصد به البحث في كيفية تصميم هذه المعطيات أي إجراء أبحاث فيما يتعلق إيجاد هذا النوع من المعطيات.

التجميع: هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة دخول غير مصرح به أو جريمة تلاعب ويفترض أن يكون الفاعل احتفظ بمجموعة من المعطيات التي تشكل خطرا وذلك من الممكن استعمالها في ارتكاب تلك الجرائم .

التوفير : ويقصد به توفير معطيات تمكن أن ترتكب بها جريمة دخول أو بقاء والمراد بذلك هو تقديم المعطيات وإتاحتها لمن يريدها أي جعلها في متناول الغير ووضعها تحت تصرفه.

والفرق بين التجميع والتوفير هو أن الحيازة في التجميع لا تتعدى الحائز بينما في التوفير فإن الحيازة تتعدى الشخص و أشخاص آخرين وتتسع بذلك وتزيد الخطورة بزيادة عدد الأشخاص

الاتجار: الاتجار بالمعطيات هو تقديمها للغير بمقابل ولا يهم إن كان المقابل نقديا أو عينيا أو قد يمثل قي خدمات أو غير ذلك. ويفهم من ذلك أن التوفير الذي نص عليه المشرع يكون بدون مقابل عكس الاتجار الذي يكون بمقابل[1].

رابعا/ في جرائم الاعتداء على سير نظام المعالجة الآلية : يمكن استخلاص ذلك من خلال النصوص التي استحدثها بخصوص تجريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات هذه الأنظمة سواء كانت معطيات داخلية أم خارجية و تتخذ الأفعال الماسة بسير النظام عدة صور نذكر منها:

[1] - صديق حياة، المرجع السابق، ص 55.

التعطيل: يمكن أن يصيب التعطيل الأجهزة المادية للنظام كتحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي إلى عرقلة سير النظام.

الإفساد :هو جعل نظام غير صالح للاستعمال بإحداث خلل في نظام سيره وفقدان توازن في أداء وظائفه، كان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ومثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فانه يحول دون تحقيقه لوظائفه بشكل صحيح.

تجدر الإشارة إلى أن المشرع الجزائري جرّم كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة، و جعل العقوبة لهما تساوي العقوبات المقررة للجريمة ذاتها. وقد تشمل هذه العقوبات المذكورة في القسم السابع مكرر من قانون العقوبات.[1]

من خلال وصف الأفعال الإجرامية للجريمة الالكترونية نقول ان عناصر الركن المادي تختلف من جريمة الى اخرى حسب نوع الجريمة، فهناك جريمة شكلية لا يتكون ركنها المادي إلا من عنصر السلوك فقط كفعل الدخول الغير المشروع لمنظومة الكترونية بينما هناك جريمة تحتاج الى نتيجة إجرامية لتكون جريمة كاملة كجريمة تعطيل اجهزة مادية للنظام فركنها المادي يتكون من السلوك الإجرامي و النتيجة و كذا العلاقة السببية.

الفرع الثاني: الركن المعنوي للجريمة الإلكترونية .

الركن المعنوي هو الجانب الشخصي أو النفسي للجريمة فلا تقوم الجريمة بمجرد الواقعة المادية التي تخضع لنص التجريم بل لابد أن تصدر عن إرادة فاعلها وترتبط بها ارتباطا معنويا فهو الرابطة المعنوية أو الصلة النفسية التي تربط بين ماديات الجريمة و نفسية فاعلها حتى يقال بان الفعل هو نتيجة لارادة الفاعل و بالتالي قيام هذه الرابطة التي تعطي للواقعة وصفها القانوني و توصف بالجريمة.[2]

[1] -أ نظر المادة 394 مكرر7من القانون 15/04 المتضمن قانون العقوبات.

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

فيتخذ في اغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بان القانون يجرمه ، ونفس الأمر ينطبق على الجريمة الالكترونية التي يقوم ركنها المعنوي على توافر الإرادة الجرمية لدى الفاعل، وهذا ما يظهر من خلال استعمال المشرع الجزائي لعبارة " الغش" و" العمد" في المواد 394 مكرر و394 مكرر 394 مكرر وكذا عبارة "الإعداد لجريمة " في المادة 394مكرر 5 من قانون العقوبات، وهذا ما يدل على أن الجريمة الالكترونية جريمة عمدية ولا يفترض فيها عنصر الخطأ.

ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة الى أخرى فجريمة الدخول الغير مصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا يتمثل في علم الجاني بعناصر الركن المادي للجريمة ، اي العلم بان الولوج الى داخل النظام بشكل غير مصرح يعد جريمة باعتبار حماية المشرع لمحل الحق وهو الحاسب الالي لما يتضمنه من برامج ومعلومات.

وفي جريمة الاحتيال الإلكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط و القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع لو أو للغير أو تجريد شخص اخر من ممتلكاته على نحو غير مشروع.[1]

[1] -حمزة عشاش، حمزة خضري، المرجع السابق، ص 175.

الفصل الثاني: إجراءات مكافحة الجريمة الإلكترونية في التشريع الجزائري.

تمهيد:

من خصائص الجريمة الإلكترونية أنها لا تعرف حدود إقليمية للدولة بل تتعداها إلى دول أخرى خاصة في ظل تطورها المستمر و ظهور شبكة الانترنت و نظرا لما لها من خصوصية في التحقيق كل هذا أدى بروز تحديات جديدة للمنظومة القانونية الإجرائية على المستوى الدولي و المحلي خاصة بعد أن أصبحت هذه المنظومات يعتمد عليها الجناة في ارتكاب الجرائم المستحدثة التي تختلف عن الجرائم الكلاسيكية في الطريقة و المنهج و ألقت بضلالها على العالم بأسره ، فكانت الأضرار و الخسائر التي انجرت عليها فادحة على المستوى الدولي و المحلي الأمر الذي أدى إلى الإسراع لمحاولة التصدي لهذه الظاهرة فتظافرت الجهود من اجل إيجاد سبل مكافحة الجريمة.[1]

فعلى الصعيد الوطني أثناء قيام المشرع الجزائري بوضع نصوص خاصة لتجريم الأفعال التي تمثل الاعتداءات على الأنظمة المعلوماتية بعد تعديل قانون العقوبات سنة 2004 ، قام بالموازاة إلى تطوير السياسة التشريعية الخاصة بإجراءات مواجهة هذا النوع من الجرائم و تطوير وسائل التحقيق التقليدية فقام بوضع الأحكام الإجرائية التي تتماشى مع طبيعة الجريمة الالكترونية و خصوصيتها ، حيث قام بإعادة تكييف تلك الوسائل مثل التفتيش و المعاينة حتى تتلاءم و مقتضيات التحقيق في مثل تلك الجرائم الغير تقليدية إذ قام بتعديل قانون الإجراءات الجزائية 04-14 ، كما قام باستحداث وسائل إجرائية أخرى مستحدثة حيث أصدر المشرع الجزائري قانون خاص بالجرائم الالكترونية رقم وهو القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها. في هذا الصدد وبعد أن تناولنا الجريمة الالكترونية من حيث جانبها الموضوعي وإطارها القانوني و ما يميزها عن الجرائم التقليدية ، سوف نتطرق في هذا الفصل إلى الجانب الإجرائي و دراسة خصوصية

[1] - محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الأنترنت(دراسة مقارنة)، مركز الدراسات العربية للنشر، مصر،2017، ص103.

مكافحة هذا النوع من الجرائم، فبعد أن عرفنا أنها جريمة عابرة لحدود إقليم الدولة وجب التعرف على قواعد الاختصاص الإقليمي و كذا القضائي و تحديد القانون الواجب التطبيق **(المبحث الأول)** ، كما سيتعين علينا معرفة طرق و إجراءات التحقيق في ظل تعديل قانون الإجراءات الجزائية و استحداث قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها **(المبحث الثاني)** بالإضافة مشروعية الأدلة الغير مادية المتحصلة من تلك الجرائم أو ما يسمى بالدليل الالكتروني ومدى الاعتداد بها كوسيلة من وسائل الاثبات **(المبحث الثالث)**.

المبحث الأول: قواعد الإختصاص القضائي للجريمة الإلكترونية.

قواعد الاختصاص القضائي هي مباشرة سلطة المتابعة والتحقيق والحكم في الجريمة وفقا للقواعد التي رسمها القانون والحدود التي تبناها المشرع لهذه السلطات أثناء ممارسة مهامها .[1]

وتعد الجرائم المعلوماتية من أكثر الجرائم التي تطرح مسألة تحديد قواعد الإختصاص القضائي، ذلك أن السلوك أو النشاط الإجرامي فيها لا يعترف بالحدود، إذ أن الطبيعة التقنية العالية لنظم المعلوماتية المرتبطة بشبكات الإتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة، الأمر الذي قد ينجم عنه تنازع في الإختصاص بين هذه الدول. ومن ثم تتعدد القوانين التي يمكن أن تحكم هذه الجرائم بتعدد الدول المرتبطة بالجرم.[2] من هذا المنطلق سنتطرق إلى تحديد القانون الواجب التطبيق (المطلب الأول) والذي يترتب عليه تحديد المحكمة المختصة (المطلب الثاني) كالاتي:

المطلب الأول : تحديد القانون الواجب التطبيق في الجريمة الإكترونية .

نصت المادة 22 من القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت على أنه : " تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها كما تختص المحاكم فيها بنظر الدعوى المترتبة عن تلك الجرائم وعلى الدول العربية عقد اتفاقات لتبني المعيار الأول في حالة تنازع

[1] - عراب مريم، الاختصاص القضائي في الجرائم المعلوماتية ، حوليات الحقوق، كلية الحقوق والعلوم السياسية جامعة محمد بن أحمد وهران، الجزائر، العدد3، 2015، ص262

[2] - نعيم سعيداني، المرجع السابق، ص95.

الاختصاص بين الدول، كما يسرى التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات". كما تنص المادة 03 من قانون العقوبات الجزائري" تسري أحكام قانون العقوبات الجزائري داخل إقليم الجمهورية على أي شخص ارتكب جريمة في نظر القانون الجزائري سواء كان مواطنا جزائريا أو أجنبيا".[1]

من خلال نص المادتين السابقتين نميز بيفن حالتين لبيان القانون الواجب التطبيق، الحالة الأولى هي ارتكاب الجرائم داخل الاقليم الوطني(الفرع الأول) ، وارتكابها خارج الاقليم الوطني في الحالة الثانية(الفرع الثاني)

الفرع الأول: القانون الواجب التطبيق داخل إقليم الدولة .

يعد القانون الجنائي الجزائري مظهر من مظاهر السيادة الدولة فلا يسري الا في حدود إقليمها و هو ما يعبر عنه بمبدأ الإقليمية القوانين الجنائية حيث تخضع الجرائم المرتكبة على اقليم الدولة لقانونها الوطني فحسب فلا يطبق قانون عقوبات أجنبي على جريمة ارتكبت في الإقليم الوطني ، و بالمقابل لا مجال لان يمتد قانون الجنائي الوطني الى خارج اقليم الدولة حيث يصطدم بسيادة غيرها من الدول التي تمنع بدورها تطبيق القوانين الاجنبية في اقليمها ويعتر اهم مبدأ في تطبيق القانون اضافة الى مبدأ الشخصية و مبدأ العينية .[2]

فإذا وقعت الجريمة على إقليم الدولة تكون لها ولاية القضاء الأصلية ، لكن تحديد مكان الجريمة ليس سهلا دائما فقد يقوم أحد المخترقين باستعمال جهاز كمبيوتر محمول مجهز بخدمة الإنترنت باختراق وتخريب نظام أحد البنوك في دولة أخرى أو عدة دول في آن واحد . فما هو الحل بالنسبة لارتكاب أحد الأعمال المكونة للجريمة في دولة ما و إتمامها في إقليم دولة أخرى؟

وقد أجاب المشرع الجزائري في هذه النقطة بموجب المادة 586 من قانون الإجراءات الجزائية على أنه "تعتبر مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر". كذلك نصت المادة 585 من قانون

[1] - فيصل بدري، المرجع السابق، ص 197.
[2] - عبد الله سليمان، المرجع السابق، ص 101

الإجراءات الجزائية على أنه يطبق قانون العقوبات الجزائري على كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة في الخارج.

غير أن تطبيق هذا الحكم يتوقف على توفر شرطين هما :

- أن يكون الفعل معاقبا عليه في الجزائر وفي القطر الذي ارتكب فيه
- أن تكون الواقعة الموصوفة بأنها جناية أو جنحة قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية.[1]

الفرع الثاني : القانون الواجب التطبيق خارج إقليم الدولة.

الأصل أن لا يطبق قانون العقوبات الجزائري على الجرائم المرتكبة خارج إقليم الجمهورية وذلك لانعدام أي إخلال بالنظام العام إعمالا لقاعدة إقليمية القوانين الجزائية.

غير أن المشرع الجزائري حاد عن القاعدة معملا مبدأ شخصية النص الجزائي ومقتضاه أن يطبق النص الجزائي على كل من يحمل جنسية الدولة ولو ارتكب جريمة خارج إقليمها أو عندما يكون هناك مساس بالمصالح الأساسية للدولة.

أولا/ الجنايات والجنح المرتكبة من قبل الجزائريين:

حسب المادتين 582 و 583 من قانون الإجراءات الجزائية فإن القانون الجزائري يطبق على الجناية أو الجنحة التي ارتكبها جزائري خارج إقليم الجمهورية لكن ذلك مشروط بـ:

- أن تكون الواقعة المرتكبة هي جناية أو جنحة في التشريع الوطني وفي تشريع القطر الذي ارتكبت فيه.
- أن يكون المتهم جزائريا وقت ارتكاب الجريمة.
- أن يعود المتهم للجزائر.
- أن لا يكون المتهم قد حكم عليه نهائيا في الخارج فلا يجوز محاكمة الشخص مرتين على واقعة واحدة.

ثانيا/ **الجنايات و الجنح الماسة بالمصالح الأساسية للدولة:**

تنص المادة 588 من قانون الإجراءات الجزائية على أن قانون العقوبات يطبق على كل جناية أو جنحة يرتكبها أجنبي أو جزائري خارج إقليم الجمهورية ضمن أمن الدولة الجزائرية أو تزييف النقود أو أوراق تجوز متابعته ومحاكمته وفقا لأحكام القانون

[1] - حياة صدوق، المرجع السابق، ص 55.

الجزائري, وهذا تكريسا لمبدأ عينية الجريمة ويبرر الأخذ به وجوب الدفاع عن السيادة إذ قلما تجد الجرائم الماسة بالمصالح الأساسية للدولة اهتماما في الخارج.[1]

يمكن القول أن إختلاف التشريعات والنظم القانونية في مكافحة الجرائم الالكترونية ، ينجم عنها تنازع في الإختصاص القضائي الدولي، فيؤدي تارة إلى تنازع إيجابي في الإختصاص القضائي بين محاكم أكثر من دولة لملاحقة نفس النشاط، وتارة أخرى يؤدي إلى تنازع سلبي في الإختصاص القضائي بأن تمتنع أي دولة من الدول المعنية بملاحقة نشاط الجاني . حيث تعد مسألة تنازع الإختصاص القضائي من أكبر التحديات التي تواجهها عملية التحقيق في هذا النوع من الجرائم لما تتميز به من طابعها المتخطي لحدود الدولة الواحدة، وإ تسامها بالطابع الدولي، بالإضافة إلى تجرد السلوك الإجرامي فيها من الطابع المادي لإرتباطه بالعالم الإفتراضي أو الرقمي.[2]

المطلب الثاني: الإختصاص المحلي.

كما يسمى أيضا الاختصاص الإقليمي باعتبار أن القضاء الوطني هو المختص بالنظر في الدعوى الجنائية دون منازع ، ويقوم هذا الاختصاص على تحديد دائرة اختصاص مكاني وجغرافي بمنطقة معينة من إقليم الدولة .[3]

الفرع الأول: القواعد العامة للاختصاص.

ينعقد الاختصاص المحلي للمحاكم بناءا على ثلاثة معايير طبقا لنص المادتين 37و 40من قانون الإجراءات الجزائية إذ تنصان على تحديد الاختصاص المحلي لوكيل الجمهورية و قاضي التحقيق حيث يتحدد الاختصاص المحلي طبقا لقانون الإجراءات الجزائية كالتالي :

- مكان وقوع الجريمة
- محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها.

[1] - حياة صدوق، المرجع السابق، ص56.

[2] - الطيبي البركة، **الحماية الجنائية لنظام المعالجة الآلية للمعطيات** (دراسة مقارنة) أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021، ص313.

[3] - فيصل بدري، المرجع السابق، ص 200.

- بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص ولو كان القبض قد حصل لسبب آخر.[1]

وبالنسبة للأحداث فإن المحكمة المختصة إقليميا طبقا للمادة 3/41 من قانون الإجراءات الجزائية هي:(المحكمة التي ارتكبت الجريمة في دائرتها أو التي بها محل إقامة الحدث أو والديه أو وصيه أو محكمة المكان الذي عثر فيه على الحدث أو أودع به بصفة مؤقتة أو نهائية.

اما فيما يخص ضباط الشرطة القضائية فانه يمارسون إختصاصهم المحلي في الدائرة التي يباشرون فيها مهامهم ، وفي حالات الإستعجال لهم مباشرة مهامهم في كافة إختصاص المجلس القضائي الملحقين به أو كافة الإقليم الوطن بناء على أمر من القاضي المختص وبعد إطلاع وكيل الجمهورية التابعين له.[2] وتحديد مكان وقوع الجريمة يختلف باختلاف طبيعة الجريمة:

أ- في الجريمة الوقتية : التي ترتكب دفعة واحدة وفي برهة من الزمن يعد مكان الجريمة هو المكان الذي وقع فيه تنفيذ الفعل.وإذا كانت تتكون من عدة أفعال وقعت في أكثر من مكان كان جميع قضاة التحقيق الذين وقعت في دائرتهم أفعال التنفيذ مختصين بنظر الدعوى من حيث المكان.

ب-في الجريمة المستمرة: والتي يستغرق ارتكابها مدة من الزمن يعتبر مكان ارتكاب الجريمة كل مكان تقوم فيه حالة الاستمرار ما لم ينص القانون على خلاف ذلك.

ج- في الجرائم المتتابعة أو المتكررة: يعتبر مكان الجريمة كل مكان يقع فيه أحد الأفعال المكونة لها ولا يبدأ سريان مدة التقادم بالنسبة لها إلا من اليوم التالي لآخر فعل من أفعال التنفيذ.

أما محل الإقامة فالعبرة بالمحل الذي كان يقيم به المتهم وقت اتخاذ إجراءات المتابعة هذه بغض النظر عن التغيرات التي تحدث به.[3]

---

[1] - فيصل بدري، المرجع السابق، ص 201.

[2] - أنظر المادة 16 مكرر 1 من القانون06-22 المتضمن قانون الاجراءات الجزائية

[3] - حياة صدوق ، المرجع السابق، ص58.

الفرع الثاني: تمديد الاختصاص في الجرائم الإلكترونية.

إن المشرع الجزائري في مسالة تحديد الاختصاص في الجرائم الالكترونية فانه سارع إلى بسط الإختصاص القضائي وتوسيعه ويتجلى ذلك في:

اولا/ التعديل الصادر في 2004/11/10 بموجب القانون 14/04 : فقد أجاز في جملة من الجرائم ومنها الجرائم الماسة بانظمة المعالجة الالية للمعطيات تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى وهذا حسب نص المادتين 2/37 و 2/40 من قانون الإجراءات الجزائية، سواء فيما يتعلق باختصاص وكيل الجمهورية أو قاضي التحقيق.[1]

ثانيا/ المرسوم التنفيذي رقم 348/06 : والمؤرخ في 05اكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم الاخرى ووكلاء الجمهورية وقضاة التحقيق، يتضمن هذا المرسوم تنظيم ما يعرف بالأقطاب القضائية والذي يتضمن استحداث جهات قضائية متخصصة للفصل في نوعية خاصة من الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (انظر المادة الاولى من المرسوم) يهدف هذا المرسوم إلى تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى) وحددت المواد 2، 3 ، 4 ، 5 هذه الأقطاب وهي :

– محكمة سيدي أمحمد بالجزائر العاصمة تشمل جميع محاكم المجالس القضائية: الجزائر، البليدة ، الشلف، الجلفة، بومرداس، البويرة، الاغواط، المدية، تيبازة، تيزي وزو، المسيلة، عين الدفلى

– محكمة قسنطينة يمتد اختصاصها الى محاكم المجالس التالية: قسنطينة، بجاية، جيجل،عنابة،الطارف،سوق اهراس،، ام بواقي، بسكرة، سطيف،قالمة،الوادي،ميلة، باتنة، تبسة،سكيكدة، برج بوعريريج، خنشلة

– محكمة ورقلة يمتد اختصاصها الى محاكم المجالس الاتية: ورقلة،الزي، أدرار ،تندوف،تمنغرست، غرداية

[1] - حياة صدوق ، المرجع السابق، ص58.

– محكمة وهران يمتد إختصاصها الى محاكم الكجالس الاتية: وهران، تيارت، مستغانم، تيسمسيلت، غيليزان، بشار، سعيدة، معسكر،النعامة،تلمسان،سيدي بلعباس،البيض، عين تموشنت .

يمكن الاشارة انه في حالة وقوع إشكاليات قد يثيرها تطبيق هذا المرسوم فإن رئيس المجلس القضائي الذي يقع في دائرة اختصاص المحكمة التي تم تمديد اختصاصها يفصل بموجب أمر لا يكون قابلا للطعن.[1]

ثالثا/ في القانون 09-04 : والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها فقد تدخل المشرع الجزائري في تمديد الاختصاص خارج الإقليم الجزائري بالنسبة للجرائم الإلكترونية ، إذ نص في المادة 15من القانون 09-04 على :" أنه وفضلا عن الإختصاص المنصوص عليه في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال المرتكبة خارج الإقليم الوطن عندما يكون مرتكبها أجانب وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطن أو المصالح الإستراتيجية للإقتصاد الوطن[2].

المبحث الثاني : التحقيق في الجريمة الإكترونية.

في ظل تطور وسائل ارتكاب الجريمة الالكترونية ، أدرك المشرع الجزائري بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية ، اين قام بتعديل بعض المواد في قانون الإجراءات الجزائية وكذا إصدار قوانين خاصة و جديدة في مجال الإجراءات [3] ، فإلى جانب إجراءات التحقيق التقليدية قام المشرع الجزائري ايضا باستحداث إجراءات أخرى من اجل استخلاص الدليل او حتى الوقاية من هذا النوع من الجرائم .و هذا ما سنتعرض اليه في هذا المبحث بالتطرق الى اجراءات

[1] - زيدان زبيحة، المرجع السابق، ص 111-112.

[2] - خليفي محمد، **إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية** ، مجلة الميزان، المركز الجامعي النعامة، الجزائر،العدد الأول، 2016 ، ص258

[3] - إسمهان بوضياف ، المرجع السابق، ص 364.

التحقيق من أجل استخلاص الدليل وفق مطلبين الإجراءات العادية او التقليدية و كذا الاجراءات المستحدثة .

المطلب الأول: الإجراءات العادية الخاصة بالتحقيق في الجرائم الإلكترونية.

إن طبيعة الجرائم المعلوماتية بعناصرها ووسائل إرتكابها قد تدفع المشرع الجزائي إلى ان يعيد النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون[1]، وللوصول الى الدليل وجب ضرورة ملاءمة و التكيف مع إجراءات التحقيق والبحث التقليدية من معاينة و تفتيش و ضبط للأدلة لكي تتناسب مع الطبيعة الخاصة للإجرام المعلوماتي.

الفرع الأول: الإنتقال و المعاينة الإلكترونية.

أولا/ مفهوم المعاينة:هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

وتعتبر المعاينة إجراءا من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها . كما يمكن للمحكمة أن تقوم بإجراءات معاينة إذا رأت ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة .[2]

والمعاينة إجراء جوازي في الجنح والمخالفات و وجوبي في الجنايات وذلك حسب المادة 42 من قانون الإجراءات الجزائية بقولها: " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ... وأن يضبط كل ما يمكن أن يؤدي لإظهار الحقيقة.[3]

ثانيا/ كيفية إجراء المعاينة التقنية لمسرح الجريمة الإلكترونية: عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة ، لأن هذا الأخير حجز الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة الالكترونية على أنه مسرحان هما:

---

[1] - نعيم سعيداني، المرجع السابق، ص101.

[2] - عبد الله أوهيبية، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة، طبعة 2003،الجزائر ،ص89

[3] - حياة صديق، المرجع الصابق، ص60

1-المسرح تقليدي : يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة أثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية

2-المسرح افتراضي : يقع داخل البيئة الالكترونية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت في ذاكرة الأقراص الصلبة(الموجودة بداخله)

ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه الجريمة[1] وذلك بإتباع عدة قواعد فنية قبل الانتقال المسرح الجريمة الإلكترونية والمتمثل في:

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

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

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

-تامين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج

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

-تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حده ، وذلك حتى لا تتداخل الاختصاصات.

-إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

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

[1] - مراد مشوش،الجريمة المعلوماتية في ظل قانون العقوبات و قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، مجلة القانون ، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، المجلد9، العدد الاول، 2020، ص122

الفرع الثاني: التفتيش الإلكتروني و ضبط الأدلة .

أولا /التفتيش:

يعد التفتيش اجراء من اجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن [1]و التفتيش الالكتروني كذلك هو اجراء تقوم به سلطة مختصة من أجل الدخول الى إلى نظام المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين و مخرجات و البحث من خلالها عن الافعال الغير مشروعة[2]. من هذا المنطلق سنحاول التطرق الى خصوصية ضوابط التفتيش الالكتروني سواءا الشكلية او الموضوعية والاستثناءات الواردة :

1-بالنسبة إلى الضوابط الموضوعية: تتمثل في السبب و المحل و السلطة المختصة بالتفتيش

أ- السبب: سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث، ويتمثل في وقوع جريمة ما جناية أو جنحة وهو ما ينطبق كذلك على الجرائم الالكترونية .

ب-المحل: يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره في الجريمة التقليدية فإن التفتيش ينصب على شخص المتهم أو غير المتهم، وكذلك على مسكن المتهم وما في حكمه وملحقاته، أو على مسكن غير المتهم وما في حكمه وملحقاته لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به اي قد يقع على المكونات المادية لنظام و تتكون من الحواسيب و الأجهزة الملحقة بها من كابلات و طابعات, أو يقع على المكونات المعنوية أو المنطقية لنظام المعلوماتي التي

[1] - نعيم سعيداني، المرجع السابق، ص 143.

[2] - بن بادة عبد الحليم ، **اجراءات البحث والتحري عن الجريمة المعلوماتية** ، مجلة العلوم القانونية ، جامعة زيان عاشور الجلفة، الجزائر، المجلد الثاني، العدد23 ،2015، ص78

تشمل البرامج و التطبيقات و الشبكات المتصلة بالحاسب الآلي كجرائم الدخول الغير مشروع لنظم الغير .[1]

ج-السلطة المختصة في التفتيش : حتى يكون التفتيش المعلوماتي صحيحا و منتجا لآثاره, يجب أن يصدر إذن من سلطة التحقيق المختصة بتفتيش مسكن المتهم و الولوج لجهاز حاسوبه الآلي و البحث عن أدلة ارتكاب الجريمة المعلوماتية التي تتطلب جرأة و مهارة فنية معينة في المحقق حتى يتمكن من المحافظة على الأدلة من الإتلاف أو الشطب أو التعديل .ويمكنه الاستعانة بخبراء فنيين بإذن من السلطات المختصة.

وقد نص المشرع الجزائري في المادة 05 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام بتفتيش المنظومة المعلوماتية في إطار قانون الإجراءات الجزائية، وهي :

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة من الدولة
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحري والتحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة من الأبحاث الجارية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

[1] - ليندا بن طالب، **التفتيش في الجريمة الالكترونية**، مجلة العلوم القانونية و السياسية، جامعة مولود معمري تيزي وزو، الجزائر، عدد16 جوان2017 ، ص491

[2] - وردة شرف الدين ، بلجراف سامية، الجوانب **الموضوعية و الإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة المنار للبحوث والدراسات القانونية و السياسية،جامعة محمد خيضر بسكرة، الجزائر، العدد الثالث، ديسمبر2017، ص50.

2-بالنسبة للضوابط الشكلية:

أ-الإذن بالتفتيش: يشترط المشرع الجزائري لصحة التفتيش ان يكون هناك اذن كتابي يتم فيه وصف الجرم و تحديد المكان إذ نصت المادة44 "..... يجب أن يتعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها وذلك تحت طائلة البطلان."وفي نطاق تفتيش الأنظمة المعلوماتية فمن المعلوم أن التخزين هو البيئة التي تتصفا الحوسبة أو الرقمية، فالبيئة الرقمية هذه الصفة تعد مجالا ضخما يمكنه تخزين مليارات المعلومات والملفات، من أجل هذا فإن صياغة الإذن بالتفتيش الخاص بالبيئة الرقمية وحتى تنفيذه يشكلان تحديات كبيرة .[1]

ب- محضر التفتيش : باعتبار أن التفتيش في الجرائم المعلوماتية من أعمال التحقيق، لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة، والقانون لما يتطلب شكلا خاصا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكونا مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية.[2]

ج- حضور المتهم عملية التفتيش: يجب حضور المتهم عملية التفتيش إذا حصل في مسكنه فإذا تعذر عليه الحضور وجب على ضابط الشرطة القضائية أن يكلفه بالحضور بتعيين ممثل عنه و إذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة شاهدين من غير الخاضعين لسلطته. إلا أن المشرع في المادة 7/45 من قانون الإجراءات الجزائية بموجب قانون 22/06 أعفت ضابط الشرطة القضائية إذا كانت الجريمة متعلقة بالمعالجة الآلية للمعطيات من هذا الإلتزام وبذلك يكون حضور المتهم عملية التفتيش غير إلزامي.

[1] - نعيم سعيداني، المرجع السابق، ص152.

[2] – ليندا بن طالب، المرجع السابق، ص494.

د- ميقات التفتيش: تنص المادة 47 من قانون الإجراءات الجزائية على:(أنه لا يجوز البدء في تفتيش المساكن و معاينتها قبل الساعة الخامسة صباحا و لا بعد الثامنة مساءا إلا إذا طلب صاحب المنزل ذلك ...). غير أن المادة 47 نفسها أوردت استثناءا خاصا بمجموعة من الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون 22/06 المعدل لقانون العقوبات, فإن التفتيش يكون في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص.[1]

ثانيا/ ضبط الأدلة:

بالنسبة إلى الضبط في مجال الجرائم الإلكترونية فيتصل بضبط المكونات المادية لأنظمة الحاسوب، ضبط المكونات المعنوية والبرمجيات، وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب وما يتصل بضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش والتي يتم الحصول عليها أثناءه. وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم:

-ضبط جهاز الكومبيوتر وملحقاته": ذلك أن ضبطه أمر مهم جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية وانها مرتبطة بالمكان والشخص الحائز على الجهاز ولأجهزة الكومبيوتر

-ضبط المعدات المستعملة في شبكة الأنترنات وأهمها المودم Modem وهي الوسيلة التي تمكن أجهزة الكومبيوتر من الإتصال ببعضها البعض عبر خطوط الهاتف.

-وسائط التخزين المتحركة كالأقراص المدمجة، أقراص الليزر والأقراص المرنة

-ضبط البرمجيات Softwareفإذا كان الدليل الرقمي ينشأ بإستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

-ضبط البريد الإلكتروني والذي يحتوي على برامج متخصصة لكتابة وإرسال وإستعراض وتخزين الرسائل الإلكترونية بـ: boitte Email .[2]

[1] - حياة صدوق، المرجع السابق، ص63.
[2] - نعيم سعيداني، المرجع السابق، ص 162-163.

المطلب الثاني: الإجراءات المستحدثة الخاصة بالتحقيق في الجرائم الإلكترونية.

عقب قصور إجراءات التقليدية لمكافحة الجريمة الالكترونية قام المشرع الجزائري باستحداث إجراءات أخرى أكثر فعالية تحمل معها طرقا مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى دليل الإثبات فيها بسرعة و سهولة وهي التسرب و المراقبة الإلكترونية

الفرع الأول: التسرب

أولا/ مفهومه : هو الإجراء المستحدث الذي نصت عليه المواد من 65 مكرر 11 إلى مكرر 18 من قانون الإجراءات الجزائية يعرف التسرب على أنه اجراء يقوم به ضابط الشرطة القضائية أو أحد أعوانه تحت مسؤوليته بتنسيق العملية لمراقبة الأشخاص المشتبه فيهم بإيهامهم أنه فاعل معهم أو شريك لهم وهو اجراء مستحدث جاء به المشرع الجزائري إذا اقتضت ضرورة التحري والتحقيق اللجوء له في الجرائم السبعة المحددة على سبيل الحصر من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

ثانيا/ الهدف من عملية التسرب: هو جمع أكبر قدر ممكن من المعطيات والبيانات الخاصة التي تشير إلى كافة الأعمال الإجرامية وكذلك تمكين المصالح الأمنية من معرفة الإمكانيات المادية والبشرية المستعملة وكذلك أساليب العمل ووسائل الاتصال و التنقل المستغلة من أجل ارتكاب الأفعال المشبوهة.

ثالثا/ ضوابط التسرب في الجرائم الالكترونية :

– الحصول على إذن مسبب مكتوب و مسبق من طرف القاضي (وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية).

–يجب أن يتضمن الإذن الجريمة التي تبرر اللجوء للتسرب وهوية ضابط الشرطة المنسق للعملية و تحديد المدة التي يجب أن لا تتجاوز 04 أشهر قابلة للتجديد.

[1] - رجاء أومدور، المرجع السابق، ص 177.

– أن تكون الجريمة محل البحث ضمن الجرائم المذكورة على سبيل الحصر في و التي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

رابعا/ مدة التسرب: حددها المشرع بـ 04 أشهر قابلة للتجديد بإذن كتابي حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية و الزمنية ، غير أن العون المتسرب يمكنه مواصلة النشاط المذكور للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه ، دون أن يكون مسؤولا جزائيا على أن لا يتجاوز ذلك أربعة أشهر ، وفي هذه الحالة يجب إخطار القاضي الذي أصدر الرخصة.[2]

خامسا/ طرق التسرب في الجرائم الإلكترونية: يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الإفتراضي وذلك بإختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو إشتراكه في محادثات غرف الدردشة أو حلقات الإتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للإستفادة منهم حول كيفية إقتحام الهاكر للموقع[3].

الفرع الثاني: المراقبة الإلكترونية.

نتيجة القصور في مواجهة الجرائم المعلوماتية من الناحية الموضوعية في قانون العقوبات ومن الناحية الاجرائية في قانون الاجراءات الجزائية جاء المشرع الجزائري بموجب القانون 09-04 المؤرخ في 5أوت 2009 بإجراء جديد يتمثل في وجوب وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها آنيا.[4]

أولا/ مفهوم المراقبة الإلكترونية: : عرف المشرع الجزائري الاتصالات الإلكترونية بموجب المادة 02 من القانون 04/09 بأنها أي تراسل او ارسال او استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

1 - أنظر المادة المادة 65 مكرر 05 من القانون 04-14 المتضمن قانون الإجراءات الجزائية.
2 - حياة صديق، المرجع السابق، ص66.
3 - نعيم سعيداني، المرجع السابق، ص177.
4 - رجاء أومدور، المرجع السابق، ص167.

اعتبر الفقه إجراء المراقبة الإلكترونية على أنه مراقبة شبكة الإتصالات و هو العمل الذي يقوم به المراقب بإستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[1].

كيفية و شروط المراقبة الإلكترونية للإتصالات :نص القانون 09-04 المؤرخ في 2009/08/05 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها في المادة 3 منه على ما يلي: " مع مراعاة الاحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام او لمستلزمات التحريات او التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الاجراءات الجزائية و في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام باجراءت التفتيش و الحجز داخل منظومة معلوماتية" .

ومن الواضح ان مراقبة الاتصالات حددها القانون على سبيل الاستثناء و في خالات محددة حصريا في المادة04 من القانون المشار اليه :

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب او التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني

ج- لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية

د- في إطار تنفيذ طلبات المساعدة القضائية للدولة المتبادلة .[2]

المبحث الثالث: الإثبات في الجريمة الالكترونية.

تهدف إجراءات التحري و التحقيق أساسا للحصول على أدلة تثبت وقوع الجريمة وتثبت إدانة او براءة المتهمين بارتكابها غير أن أدلة الاثبات في الجرائم العادية تختلف

[1] - نعيم سعيداني، المرجع السابق، ص178.
[2] - زيدان زيبخة، المرجع السابق، ص128-129.

عليها في الجرائم الالكترونية ، حيث أن هذه الأخيرة ذات طابع علمي رقمي و تقني و سنتطرق في هذا المبحث الى الدليل التقني .[1]

المطلب الأول: الدليل الإلكتروني.

الفرع الأول : مفهوم الدليل الالكتروني.

عرف بأنه الدليل الذي يجد له أساسا في العالم الإفتراضي و يقود إلى الجريمة، وعرف أيضا بأنه: المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام ب ارمج و تطبيقات و تكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم و ذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون.[2]

الفرع الثاني: خصائص الدليل الالكتروني.

أولا/ الدليل التقني دليل علمي مستوحى من البيئة الرقمية :فهذا الدليل لا يأخذ أشكال مادية ملموسة كأدوات الجرائم مثلا في الجرائم العادية بل نجده في هيئة إلكترونية غير ملموسة لا يمكن ادراكه بالحواس ، بل يجب إدراكه باستعمال أجهزة علمية و تكنولوجية ، كالحاسب الآلي و معداته والإستعانة بنظم برامجية معلوماتية.

ثانيا/ السعة التخزينية العالية : فالأقراص المضغوطة كبطاقات الذاكرة يمكنها تخزين كم هائل من المعطيات والمعلومات، وآلة تصوير رقمية يمكنها تخزين الاف الصور و الفديوهات.

ثالثا/ سهولة مسح الدليل والتلاعب به : حيث يمكن للجاني أو الجناة التلاعب بالدليل من خلال تعديله او نقله إلى مستندات أخرى أو حتى محوها .

رابعا/ الدليل التقني قابل للنسخ : حيث يمكن نسخ الدليل المتحصل عليه في أقراصٍ كأشرطة أو ديسكات أو غيرها من التقنيات.

---

[1] - فيصل بدري، المرجع السابق، ص224.

[2] - عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2018، ص193.

خامسا/ الدليل الالكتروني يرصد معلومات عن الجاني : حيث يمكن للتسجيل أن يرصد تحركات الشخص وأصواته وأفعاله مما يسهل عملية تحليلها و استخلاص عادات و سلوكيات الشخص.[1]

المطلب الثاني: أدلة الإثبات في الجريمة الإلكترونية.

الفرع الأول: الشهادة.

أولا/ مفهومها: الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وإسنادها للمتهم أو براءته منها ، لذلك فإن الشهادة في مجال الإجراءات الجنائية أهمية بالغة و ذلك لأن الجريمة على غير مشروع يجتهد الجاني عند ارتكابه في التكتم عليه وإخفائه عن أعين الناس. حيث تنص المادة 88 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق أن يسمع كل شخص يرى فائدة من سماع شهادته سواء كان شاهد نفي أو إثبات بعد استدعائه بكتاب عادي أو موصى عليه أو بالطريق أو بواسطة أحد أعوان القوة العمومية.

ثانيا/ **فئات الشهود في الجريمة المعلوماتية.**

يعرف الشاهد في الجريمة المعلوماتية بأنه ذلك الشخص الفني صاحب الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات أساسية وجوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية للمعطيات أو البيانات .

ويطلق عليه باسم الشاهد المعلوماتي : (Témoin Informatique) نسبة للجريمة المعلوماتية وذلك تمييزا له عن الشاهد التقليدي ومن فئاته: [2]

*مشغلو الكمبيوتر: Opérateur d'ordinateur هو الشخص المسؤول عن تشغيل الجهاز والمعدات والملحقات والأدوات المتصلة به و يجب أن تكون لديه خبرة كبيرة في استخدام جهاز الحاسب ومكوناته ومعلومات عن قواعد كتابة البرامج ونقل البيانات من الوثائق إلى وسيط التخزين حتى تتم معالجتها بواسطة الكمبيوتر.

*خبراء البرمجة : Programmeur : هم الأشخاص المتخصصون في كتابة أوامر البرامج الخاصة بجهاز الكمبيوتر و يقسمون إلى:

[1] - فيصل بدري، المرجع السابق، ص226-227.
[2] - حياة صديق، المرجع السابق، ص68.

مخططي برامج التطبيقات Programmeur D'Application

مخططي برامج النظم Programmeur Système

*المحللون : Analystes : هو الشخص الذي يحلل و يجمع البيانات النظام ودراسة هذه البيانات و تتبعها داخل النظام عن طريق ما يسمى مخطط تدفق البيانات واستنتاج الأماكن التي تحتاج إلى تزويد بخدمات الحاسب الآلي.

*مهندسو الصيانة : هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الكمبيوتر بمكوناته وشبكة الاتصال المتعلقة به

الفرع الثاني: الخبرة و مقدمو الخدمات.

أولا/ الخبرة

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية ، ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات وكذلك إعداد البرمجيات و تشغيل الحاسب الآلي وعلومه و أن نجاح الاستدلالات و أعمل التحقيق في هذه الجرائم يكون مرتهنا بكفاءة و تخصص هؤلاء الخبراء.[1]

ورغم ما أنيط به الخبير من مهام حيث أجاز له القانون تلقي أي تصريح مفيد من الغير و سماع المتهم ، يبقى الخبير مجرد مساعد للقاضي تنحصر مهمته في إنارة القاضي بخصوص مسائل فنية ولا يجوز له بأي حال من الأحوال أن يحل محل القاضي أو ينوب عنه. إن الخبرة في الجريمة المعلوماتية تطرح إشكالا مضمونه تحديد مهام الخبير وهذا يقتضي تأهيل القضاة سواء قضاة التحقيق أو الحكم.

من بين المسائل التي يتعين تضمينها في مهمة الخبير المعلوماتي :

1 – تركيب الكمبيوتر و نوعه و نظام تشغيله و الأنظمة الفرعية رتب يستخدمها.

2 – المكان المحتمل لأدلة الإثبات ضمن النظام وشكلها ونمطها.

3 – كيفية عزل النظام المعلوماتي عند الحاجة.

4 – إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون تلف.

5 – إمكانية نقل أدلة الإثبات لأوعية مادية كالأوراق على أن تكون مطابقة كما هو مسجل في الحاسب الآلي أو النظام أو الشبكة.

[1] - عبد الحليم بن بادة، المرجع السابق، ص 67.

ثانيا/ مقدمو الخدمات:

مفهوم مقدمو الخدمات : يطلق على مقدم خدمة الإنترنت عدة تسميات مثل متعهد الوصول، متعهد الخدمة أو مقدم الخدمة، كما سماه المشرع الجزائري في القانون رقم 09-04 الخاص بقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال الفقرة الرابعة من المادة الثانية 2 والمادة 11 من نفس القانون.

وهو كل شخص طبيعي أو معنوي يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات سواء قام بمعالجة أو تخزين المعلومات بذاته أو قام بها من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

دور مقدمي الخدمات في الإثبات: لمقدمي الخدمات دور مهم فيكشف الجرائم والوصول لمرتكبيها، فقد فرضت عليهم مختلف التشريعات التزامات يتعين عليهم القيام بها، كتقديم المساعدة للسلطات المكلفة بالتحريات القضائية سواء كانت داخلية أو خارجية من أجل جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها ووضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المحددة في القانون والاتفاقيات الدولية، وكذا التدخل الفوري والسريع من أجل سحب المحتويات غير المشروعة بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين أو جعل الدخول إليها غير ممكن، ووضع الترتيبات التقنية الضرورية التي تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها.[1]

[1] - خضرة شنتير، المرجع السابق ، ص143.

الخاتمـــــــــــــــــــــــة:

في ختام دراستنا لموضوع الجريمة الإلكترونية نقول أن التطور السريع للوسائل التكنولوجية الحديثة، والتحول إلى العالم الرقمي خلق مجموعة من أخطر الجرائم التي يشهدها العالم اليوم، ألا وهي الجرائم الإلكترونية التي باتت تهدد المجتمعات ، الأمر الذي دفع أغلب الدول من بينها الجزائر إلى رفع التحدي لمكافحة هاته الجريمة من الناحية الموضوعية و الإجرائية بتخصيص قوانين واستحداث آليات للحد منها، وإستوجب من المشرع الجزائري ملاءمة النصوص القانونية لهذه التطورات الحديثة والأخذ في الحسبان خصوصية التحقيق لضمان فاعليته بغرض الوصول الى الحقيقة، وقد توصلنا الى مجموعة من النتائج والتوصيات التي نوردها على النحو الآتي:

النتائج المتوصل إليها:

أول ما يمكن استنتاجه خلال دراستنا في الفصل الأول الخاص بالأحكام الموضوعية:

– عدم وجود تعريف موحد للجريمة الإلكترونية، فبالنظر الى المشرع الجزائري نجد انه اخذ كذلك بالتعريف الضيق بادراجها ضمن قانون العقوبات تحت اسم الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات , ثم وسع من نطاقها لتشمل كل جريمة ترتكب عبر المنظومة المعلوماتية في القانون الخاص بالوقاية من جرائم تكنولوجيا الاتصال و الإعلام ,و رغم ذلك فإن المعالجة التشريعية تتسم بالجمود .

– كذلك نجد المشرع الجزائر نص على الجرائم الإلكترونية في صور على سبيل الحصر حيث أنه أغفل النص على تجريم بعض الجرائم الإلكترونية الحساسة و التي انتشرت بشكل خطير في كل المجتمعات وحتى في المجتمع الجزائري و هي جرائم الاستغلال الجنسي للأطفال وتحريضهم على الدعارة و المخدرات عن طريق الشبكات . فالتجريم الوارد بنص المادة 342 من قانون العقوبات الجزائري و ما يليها، لا يعد في

نظرنا كافيا لتطويق هذا النوع الخطير.ويعود سبب ذلك الى الطبيعة المتسارعة والتطور الكبير الذي تشهده هذه الجريمة وعدم قدرة التشريع على مجاراتها.

- أن تميز الجرائم المعلوماتية بخاصية اللاحدودية،و تعديها الى حدود الدول الأخرى أوقع الدول بما فيها الجزائر في صعوبات التعاون الدولي في إجراءات التحقيق في هذه الجرائم ، وكذا صعوبات من ناحية تنازع الإختصاص و القانون الواجب التطبيق.

- أنه من الناحية الإجرائية، نظرا لطبيعة الجريمة الإلكترونية الخاصة تظهر صعوبة مهام رجال التحقيق على جميع المستويات في أداء دورها للكشف عن الجريمة و البحث عن أدلتها، فحتى و إن كان هناك تطور ملحوظ في تطبيق الأساليب الإجرائية التقليدية كالمعاينة و التفتيش و الضبط بوضع بعض الخصوصيات و الشروط عليها، لتتلاءم و طبيعة الجريمة الإلكترونية ، تبقى العديد من الصعوبات للكشف عن هذه الجريمة و المتمثلة في قلة الآثار المادية التي تتركها وسهولة محو الدليل من طرف مرتكبي هذه الجرائم بين فترة ارتكابها و فترة اكتشافها مما يصعب عملية الكشف عنها.

- المشرع الجزائري من ناحية الأحكام الإجرائية رغم محاولاته لمسايرة الجريمة الإلكترونية بإضفائه للصبغة الخاصة باساليب التحري من خلال تعديل الخاص بقانون الاجراءات الجزائية**06-22** و ووضع إجراءات جديدة مكافحة للجريمة كذلك بالقانون 09-04 الخاص القواعد الخاصة للوقاية من بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الا أنه يبقى متأخرا و شبه عاجز عن مسايرة مكافحة التطور الهائل للجريمة الإلكترونية و أساليب إرتكابها .

التوصيات:

- العمل على إيجاد تعريف شامل وجامع للجريمة الإلكترونية لكي يتسنى للمشرع وضع نصوص عقابية تتلاءم مع طبيعة هاته الجريمة .

– إعطاء الفرص لأصحاب الكفاءات للاستفادة من مهارتهم وخبراتهم، والاستعانة بها في مجال مكافحة الجريمة المعلوماتية أثناء مثلا طلب إجراء الخبرة او المساعدة التقنية وفق الإطار القانوني.

– أهم خطوة لنجاح المكافحة الإجرائية لابد من القيام بالعديد من الدورات التكوينية les cours de formation في مجال تكنولوجيات المعلومات و الاتصالات داخل أو خارج الوطن سواءا بالنسبة لمؤسسات التحقيق (ممارسو الضبطية القضائية، المؤسسات غير قضائية) أو السلطات القضائية المختصة في هذا المجال من أجل الرفع من الكفاءة.

– ضرورة دعم و تعزيز التعاون الدولي القضائي و الاتفاقي لمتصدي لهذا النمط المتجدد و المعقد من الإجرام المعلوماتي العابر للحدود, خاصة أمام عجز المجهودات الفردية للدول وقصور الآلة التشريعية على إحتوائها و مكافحتها.

قائمة المصادر والمراجع

أولا/ المصادر

المواثيق الدولية:

1- الإتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) ، مجلس أوروبا، مجموعة المعاهدات الأوروبية ، بودابست- المجر، رقم 185، صادرة بتاريخ :23-11-2001 .

النصوص التشريعية:

القوانين:

1- القانون رقم **04 – 14**، المؤرخ في 10نوفمبر 2004، المعدل والمتمم للأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 71بتاريخ 10نوفمبر 2004.

2- القانون رقم **15/04**، المؤرخ في 10نوفمبر2004 ، جريدة رسمية عدد71، مؤرخة في 10نوفمبر 2004 ،المعدل و المتمم للأمر رقم 66-156المؤرخ في8 يونيو1996، المتضمن قانون العقوبات المعدل و المتمم.

3- القانون رقم 06-**22** ،المؤرخ في 20ديسمبر 2006المعدل والمتمم للأمر رقم 66-155المؤرخ في 08 يونيو 1996يتضمن قانون الإجراءات الجزائية.

4-القانون رقم **01/08** ، مؤرخ في 23جانفي 2008 ، و المتمم للقانون رقم 11/83 المتعلق بالتامينات.

5- القانون رقم **09-04** مؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد47 ، الصادرة بتاريخ 16 اوت 2009.

6-القانون رقم **07/18** المؤرخ في المؤرخ في 10ماي 2018 ، المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي الجريدة الرسمية عدد34.

الأوامـــــر:

1- الأمر رقم **66-155**، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 71، بتاريخ 10نوفمبر ،2004.

2- الأمر رقم **05/03** ، مؤرخ في 19يوليو 2003 ، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد44.

المراسيـــــم:

1- المرسوم الرئاسي **رقم96-438**، المؤرخ في 6ديسمبر1996، المتضمن التعديل الدستوري سنة 1996.

2- المرسوم التنفيذي رقم 06-348 ، المؤرخ في5 اكتوبر2006، المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ، الجريدة الرسمية عدد 63.

3- **ثانيا/المراجـــــع:**

الكتـــــــب:

1- أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، دار هومة، الجزائر، الطبعة الثانية،2007.

2- أمير فرج يوسف، **الجريمة الكترونية والمعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر و الانترنت**، مكتبة الوفاء القانونية الإسكندرية، مصر، الطبعة الأولى، 2011.

3- خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي الإسكندرية ، الطبعة الأولى، 2009.

4- رشيدة بوكر، **جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، منشورات الحلبي الحقوقية ، الطبعة الأولى،2012.

5- زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري و الدولي**، دار الهدى، الجزائر،2011.

6- شوقي يعيش تمام، **الجريمة المعلوماتية (دراسة تأصيلية مقارنة)** ، سلسلة مطبوعات المخبر بسكرة، الجزائر، الطبعة الأولى،2019 .

7- عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي**، منشأة المعارف، مصر،2009.

8- عبد الله أوهيبية، **شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق**، دار هومة، الطبعة 2003.

9- عبد الله سليمان، **شرح قانون العقوبات الجزائري القسم العام الجزء الأول**، ديوان المطبوعات الجامعية، الجزائر، 1995.

10- عفيفي كامل عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**،دراسة مقارنة ، منشورات الحلبي، الطبعة الثانية،2007.

11- لينا محمد الأسدي، **مدى فاعلية احكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)**، دار الحامد للنشر،الطبعة الأولى، الأردن، 2015.

12- محمد أمين الشوابكة ، **جرائم الحاسوب و الأنترنت**، دار الثقافة للنشر والتوزيع ، الطبعة الاولى، 2009.

13- محمد ممدوح بدير، **مكافحة الجريمة المعلوماتية عبر شبكات الأنترنت(دراسة مقارنة)**،مركز الدراسات العربية للنشر، مصر،2017

14- منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية للنشر، لبنان، 2015.

15- نائلة عادل محمد فريد قورة, **جرائم الحاسب الاقتصادية دراسة نظرية و تطبيقية**، منشورات الحلبي الحقوقية –بيروت– الطبعة الأولى، 2005.

16- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، عمان ،الطبعة الثانية، 2010.

الرسائل العلمية والأطروحات:

أولا/ أطروحات الدكتوراه:

2- بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي**، أطروحة دكتوراه في القانون العام، كلية الحقوق و العلوم السياسية، جامعة بن يوسف خدة، الجزائر ،2018

3- جمال براهيمي، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر ،2018.

4- خضرة شنتير، **الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)**، أطروحة دكتوراه في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021.

5- ربيعي حسين، **آليات البحث و التحقيق في الجرائم المعلوماتية**، رسالة دكتوراه كلية الحقوق جامعة باتنة ، 2016

1-الطيبي البركة، **الحماية الجنائية لنظام المعالجة الآلية للمعطيات** (دراسة مقارنة) أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2021.

6- عبد القادر عميمر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري(دراسة مقارنة)**، أطروحة لنيل شهادة الدكتوراه تخصص قانون جنائي، جامعة يوسف بن خدة الجزائر، 2019-2020.

7- عفاف خذيري، **الحماية الجنائية للمعطيات الرقمية**، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2018.

ثانيا/ مذكرات الماجستير:

1- صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة تخرج لنيل شهادة ماجستير،تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية جامعة مولود معمري –تيزي وزو، 2013.

3- طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة لنيل شهادة ماجستير تخصص قانون جنائي،

كلية الحقوق و العلوم السياسية، جامعة الجزائر1 ، 2012/2011.

4- حياة صديق ، **خصوصية الجريمة المعلوماتية**، مذكرة تخرج لنيل إجازة القضاء، المدرسة العليا للقضاء، الجزائر، 2005-2008.

5- نعيم سعيداني ، **آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير(في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر باتنة، 2013 .

المجلات والمقالات:

1- آمنة امحمدي بوزينة، **خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري**، مجلة ببليوفيليا لدراسة المكتبات والمعلومات، جامعة العربي التبسي، تبسة، الجزائر، 2020.

2- بن بادة عبد الحليم ، اجراءات البحث والتحري عن الجريمة المعلوماتية ، مجلة العلوم القانونية ، جامعة زيان عاشور الجلفة، الجزائر، المجلد الثاني ، العدد23 ،2015.

3- بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف –المسيلة ، العدد الحادي عشر،2018 .

4- حمزة عشاش، حمزة خضري، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية و السياسية، جامعة عمار ثليجي، الأغواط الجزائر، المجلد6 العدد الثاني ، 2020.

5- حوالف عبد الصمد، **الآليات القانونية لتلافي الجريمة المعلوماتية والحد من إنتشارها وفقا للتشريع الجزائري**، مجلة الفكر القانوني و السياسي، كلية الحقوق و العلوم السياسية ، جامعة تلمسان، العدد الرابع، 2018.

6- خليفي محمد، **إشكالية الاختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية** ، مجلة الميزان، المركز الجامعي النعامة، الجزائر،العدد الأول، 2016.

7- رابح سعاد، ضوابط مكافحة الجريمة المعلوماتية ، مجلة القانون العام الجزائري والمقارن، جامعة جيلالي ليابس بلعباس، الجزائر، المجلد السابع، العدد 1 ، جوان 2021 .

8- رضا هميسي، **تفتيش المنظومة المعلوماتية في القانون الجزائري**، مجلة العلوم القانونية والسياسية، العدد الخامس ،جوان 2012.

9- سعيدة بوزنون، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، الجزائر، المجلد 30، العدد3 ،2019.

10- عراب مريم، **الاختصاص القضائي في الجرائم المعلوماتية** ، حوليات الحقوق، كلية الحقوق والعلوم السياسية جامعة محمد بن أحمد وهران، الجزائر، العدد3، 2015.

11- عطاء الله فشار ، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مقال مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المنعقد بأكادمية الدراسات العليا ، ليبيا ،2009.

12- ليندا بن طالب، **التفتيش في الجريمة الالكترونية**، مجلة العلوم القانونية و السياسية، جامعة مولود معمري تيزي وزو، الجزائر، عدد16، جوان2017.

13- مختارية بوزيدي، **ماهية الجريمة الإلكترونية**، مداخلة بجامعة مولاي الطاهر-سعيدة مطوية الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري الجزائر،2017.

14- مراد مشوش،**الجريمة المعلوماتية في ظل قانون العقوبات و قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال**، مجلة القانون ، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، المجلد9، العدد الاول، 2020.

15- مشتاق طالب وليد، **مفهوم الجريمة المعلوماتية و دور الحاسوب في ارتكابها**، مجلة العلوم القانونية و الانسانية ، جامعة ديالي العراق، المجلد الثالث ، العدد الأول، **2014**

16- وردة شرف الدين ، بلجراف سامية، **الجوانب الموضوعية و الإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة المنار للبحوث والدراسات القانونية و السياسية،جامعة محمد خيضر بسكرة، الجزائر، العدد الثالث، ديسمبر 2017

17- ونوغي نبيل، زيوش عبد الرؤوف، **الجريمة المعلوماتية في التشريع الجزائري**، مجلة العلوم القانونية و الاجتماعية، المجلد الرابع، العدد الثالث، جامعة مولود معمري تيزي وزو، الجزائر، 2019.

المواقع الإلكترونية:

1- حسين فريجة، الجرائم الالكترونية و الأنترنت بحث منشور على موقع **http://search.mandumah.com/Record/122156**

2-عكوم وليد، **التحقيق في جرائم الانترنت**، على الموقع الإلكتروني: **www.arabelawinfo.com**

3- الجرائم الالكترونية – بحث منشور على الفيس بوك- صفحة **Legal Consulting**