وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجريمة الالكترونية في التشريع الجزائري

مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق

تخصص قانون جنائي

إعداد الطلبة:

- عديلــة مــراد
- عبدلي ردوان

إشراف الدكتور:

مهـدي رضـا

السنة الجامعية: 2021/2020

كلمة شكر و عرفان

بسم الله الرحمن الرحيم

((ربي أوزعني أن اشكر نعمتك التي أنعمت علي و على والدي وان اعمل صالحا ترضاه و أدخلني برحمتك في عبادك الصالحين)) سورة النمل الاية 19.

أول شكري لله سبحانه وتعالى على ما أسبغه علي من نعم فله الحمد والشكر في كل وقت وفي كل حين.

يسـرني أن أتقـدم بجزيل الشكـر و العـرفان الى اللجنة الموقرة التي قبلت مناقشة هذا البحث المتواضع.

كما أتقـدم بالشكـر الجزيـل الى الذي شجعني و وقف وراء هذا العمل المتواضع بمجـهوداته و نصائحه القيمة و توجيهاته التي أنارت طريقي و قومت مساري ، الى رمز العلم و العمل و الالتزام الى من أرى فيه مستقبل الدارسين و المتعلمين من الطلبة .

أستـاذي المشرف الدكتـور

مهـدي رضـا

مـراد

إهـــــداء

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

اهـــــدي ثمــرة جهـــــدي

إلى والدي الكريمين حفظهما الله و رعاهما وأطـال في عمرهما و متعهما بالصحـــــة و العافيـــــــة

إلى رفيقة دربي وسندي زوجتي حفظها الله بحفظه التام وعينه التي لاتنام وابعد عنها كل مكـــــروه.

إلى من اشد بهم أزري إخوتي جميعا ذكورا و إناثا

إلى كل أساتذتي في كلية الحقوق و العلوم السياسية بجامعة محمد بوضياف المسيلة

إلى كل من ساعدني من قريب أو بعيد في انجاز هذا العمل المتواضع

إلى جميع الزملاء و الأصدقاء.

مراد

مقدمة

يعكـــــس القانون الجنـائي مدى التقدم والتغير الحضـاري للدول و المجتمعات في جميع نواحيه المختلفة السيـاسية والاقتصـادية و الاجتمـاعية والروحية والخلقية فقواعده تعتبر مرآة صادقة لحياة المجتمع التي تطبق فيه ومنه يمكن معرفة مدى مدنية الدولة وانه بقدر ما تكون تلك القواعد والنصـوص متطورة بقدر ما تحقق الغايات والأهداف المنشـودة التي وجدت لأجلها ، وقد رافق التطور الكبـير الذي شهده العالم في مختلف الميـادين تطور الظاهرة الإجرامـية في العصر الحـديث تطورا ملحوظا ومذهـلا سواء في شخصية مرتكبـيها أو أسلوب ارتكابها مع استخـدام آخر ما توصلت إليه العلـوم التقنية والتكنـولوجية وإذا كانت التكنـولوجيا هي الجانب التطبيـقي للعلم فهي بمـثـابة الوسيـط بين البحث العلـمي والصنـاعة ما يؤكد أن جميع المخترعات إنما هي نتـائج التكنـولوجيا ، وقد تميز القرن العشرين باختراعات هائلة على المستوى التقني لعل من أهمها ظهور **الحاسوب الالكتـــروني** و وجود ما يعرف **بالأنترنت.**

لقد غزت هاتين الوسيلتين جميع مجالات الحياة نظرا لما تتسم به من الدقة والسرعة وأصبحتا في متناول الجميع ، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم ونوع جديد من المجرمين وهو ما يجسد الانعكاس السلبي لهذه الثورة العلمية ، وانه على الرغم من الايجابيات التي وفرها النظام المعلوماتي عن طريق التقنية – **الحاسوب الالكتروني و الانترنت**– في شتى الميادين إلا انه لا يخلو من بعض المخاطر لان المعلومة باعتبارها علم للمعالجة الآلية للمعطيات أصبحت تثير عدة مشكلات من الناحية القانونيـــة إذ قد يساير استخدامها لارتكـــاب الجرائم عن بعـــد وفي هذا الصدد تقول " **روى جودسون** " خبيرة بالمركز الوطني الأمريكي للمعلومات ((**لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة**)) أو قد تكون محلا للاعتداء حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الالكترونية أو المعلوماتية ، فهذه التقنية تسمح بنقل المعلومة صوتا وصورة عبر الانترنيت وفي أي مكان من العالم مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم ، وهذا يعتبر خطر يهدد المجتمع والعالم ككل .

حيث استغل البعض المخترعات العلمية وما تقدمه من وسائل ، متقدمة في ارتكاب العديد من الجرائم الالكترونية الحديثة مستغلين الإمكانيات الهائلة لهذه المستحدثات ، واستحدثت صور أخرى من إجرام يرتبط بهذه التقنيات ويصير محلا لتلك الجرائم أو وسيلة لارتكابها ، وتطور العالم التكنولوجي بصورة أدت إلى ميلاد ظاهرة إجرامية حديثة تسمى بالإجرام الالكتروني ، وأدى ذلك إلى ظهور سطو على البنوك بمساعدة هذه الوسائل المستحدثة وفقا لتنظيم حكم متنامي ، وذلك ما يسمى بالجريمة المنظمة التي ولدت في أحضان الثورة العلمية في مجال المعلومات والاتصالات في وجه الخصوص في مجالات تجارة المخدرات ، التجارة بالسلاح ، مجال الإرهاب والدعارة المنظمة باستخدام الانترنت كذلك سهلت و ساعدت على ارتكاب الجرائم التقليدية كالنصب وخيانة الأمانة وتزوير المحررات والاعتداء على الحياة الخاصة للناس وعلى البيانات الشخصية ، وظهرت جرائم ملازمة لهذه المستحدثات منها الغش الالكتروني بالتلاعب في مدخلات البرامج ، النسخ غير المشروع للبرامج والعديد من الجرائم المتعلقة بالتجارة الالكترونية كإتلاف جميع المدونات في الحاسب الآلي ، بث صور أفلام جنسية عبر مختلف الأجهزة .

إن خطورة هذه الظاهرة الإجرامية المستحدثة تثير العديد من الأسئلة ذلك أن هذه الجرائم يسهل ارتكابها على هذه الأجهزة و تنفيذها يستغرق دقائق معدودة بل أحيانا ترتكب في بضع ثواني وان محو هذه الجريمة وإتلاف أدلة إثباتها غالبا ما يلجا إليه الجاني عقب ارتكابه الجريمة ، فضلا عن مرتكبي هذه الجرائم بالذات يلجأون إلى تخزين بياناتهم المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استعمال شفرات ورموز سرية لإخفائها عن الأجهزة المكلفة بمتابعة والتحقيق ومكافحة هذه الجرائم مما يثير مشكلات كبيرة في جمع الأدلة الجنائية واثبات هذه الجرائم– الأمر الذي أدى إلى وجود تشريعات في مختلف دول العالم تهدف إلى التماشي مع جميع الظروف المتغيرة والسريعة نظرا لطبيعة هذه الجرائم الالكترونية وفي مكافحة والتصدي لهذه الجرائم مع لإنشاء معاهد متخصصة لهدف تطوير الآليات المكلفة بالتصدي لهذه الجرائم .

الجزائر كغيرها من الدول التي استقطبت هذه التكنــولوجيا واستهلكت منتجاتها فقد حملت إليها الجــانبين : الايجابي المتمثل في تسهيل وتبسيط الحياة الاجتماعية والسلبي المتمثل في الضرر الناتج عن سوء استعمــالها عندها كان لابد من إيجاد إطار قانــوني مناسب لسد الفــراغ الإجرائي لذلك تم وضع مجموعة من الإجــراءات والتي تعد قاسما مشتركا بين الجرائم التقليدية والجرائم الالكترونية عن طريق تعــديل قانون الإجــراءات الجزائية لتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجــرائم المستحدثة ومنها الجــريمة الالكتــرونية ومنها الإجــراءات التي تطبق على الجريمة الالكترونية فقط .

لقد أحدثت الجريمة الالكترونية انقلابا هاما في النظريات التقليدية بما فيها نظرية الإثبات الجنائي و تحديد ما إذا كانت النصوص الجنائية التقليدية تواجه الأفعال الغير مشروعة التي ترتكب عبر شبكة الانترنيت و نظرا للخصوصية التي تتميز بها الجريمة الالكترونية في أنها لا تترك أي اثر خارجي أين يصعب إثباتها أدى ذلك إلى عدم تناسب النصــوص المنظمة لطرق الإثبات التقليدية مع طبيعة الجريمة الالكترونية و تطورها بسبب سرعة إخفاءها وطمس معالمها في زمن قياسي ومن اي مكان في العالم وهو ما اتفق عليه البــاحثين والفقهاء في مجال المعلوماتية – مما استلزم على المشرعين تبني أنــواع جديدة من الأدلة تسمى بالأدلة الرقمية مع حرصهم على توفــير الغطاء التشريعي لها .

لقد تبــاينت التشريعات واختلفت رؤى الفقــهــاء في دراسة هذه الظــاهرة المستحدثة – الجريمة الالكترونية – فهناك من اعتبرها ظاهرة إجرامية حديثة النشأة اكتنفها الكثير من الغموض أدى إلى القول أنها جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها غير أن تطبيقها على هذا النوع من الأنماط المستحدثة من الجرائم أسفر عن الكثير من المشكلات القانونية منها من أيد تطبيق النصوص التقليدية عليها ، ومنها من اعتبر هذه الأفعال سلوكا مباحا لم يرد بشأنه نص يجرمه التزاما بمبدأ الشرعية الجنائية والذي يقضي بان لا جريمة ولا عقوبة إلا بنص.

والمشرع الجزائري كغيره من التشريعات المقارنة تصدى لمثل هذه الظواهر ومعاقبة مرتكبيها انطلاقـــا من مبـــدأ الشرعية وفقا لأحكـــام المادة الأولى من قانون العقوبـــات الجزائري التي تنص على: " لا جريمة ولا عقوبة أو تدابير امن بغير قانون ".

وانه من اجل مسايرة التشريع للتطورات التكنولوجية وعدم استغلال وتـــيرة النمو المتسارع الذي تشهده الدول العربية منها الجزائر في استخدام النظم المعلوماتية فضلا عن العولمة والتبعية التكنولوجية نظم المشرع الجزائري الجريمة الالكترونية و وضع الآليات المختصة بالمتابعة للحد منها و التي تهدف إلى تطوير التنظيم القضائي الرامي إلى مكافحتها وردع مرتكبيها لحماية الاقتصاد الوطني على وجه الخصوص .

تتجلى أهمية هذا البحث في كون هذا النوع المستجد من الإجرام مرتبط بالتقنية الحديثة المتمثلة في الحاسب الآلي وشبكة الانترنيت كما سبق ذكره والتي هي في تطور دائم مما يفرض على المشرعين لمختلف الدول مواكبة هذه الظاهرة مع إيجاد الحلول التشريعية لمكافحتها وعدم الاكتفاء بالنصوص التقليدية التي أضحت عاجزة سواء من الناحية الموضوعية باعتبار ان الجريمة الالكترونية تمس حقوقا غير مادية) المعلومات، البيانات ، التجارة الالكترونية....(أو من الناحية الإجرائية وما تثيره من صعوبات وتتمحور حول إثبات الجريمة أو القانون الواجب التطبيق أو المحكمة المختصة في نظر هذه الجريمة وكذا حتمية التعاون الدولي في هذا المجال.

من خـــــلال ما سبـــق تبيانه من أهمية لموضوع الجريمة الالكترونية ارتأيت طرح الإشكالية التاليـــة و هي :

فمـــا ماهيـــة الجريمة الالكـــترونية ؟ و كيف عالجها المشرع الجـــزائري؟

وتتفرع عن هذه الإشكالية العامة الإشكاليات الفرعية التالية:

مـــا مفهوم الجريمة الالكـــترونية في التشريع الجزائري؟ و ما أركانها و صورها؟ وماهي طبيعتها القانونية ؟ و فيما تتمثل إجراءات متابعتها في التشريع الجزائري ؟ وما هي الآليات المختصة في مكافحتها؟ وفيما تكمن المعوقات والصعوبات التي تعترض مكافحة الجريمة الالكترونية واثر ذلك على التشريع الجزائي الجزائري؟

انـــه للإجابـــة عن الإشكاليـــة العامة و الإشكاليات المتفرعـــة قمت بتقسيم بحثي هذا الى فصلين اين تطرقت في الفصل الاول الى ماهية الجريمة الالكترونية وتناولت فيه مبحثين، المبحث الاول تعرضت فيه لمفهوم الجريمة الالكترونية بصفة عامة ويتضمن ثلاث مطالب (تعريف الجريمة الالكترونية ، خصائص و أسباب الجريمة الالكترونية ، التطور التاريخي للجريمة الالكترونية) و المبحث الثاني تعرضت فيه الى مفهوم الجريمة الالكترونية في التشريع الجزائري و يتضمن ثلاث مطالب (تعريف المشرع الجزائري للجريمة الالكترونية ، الطبيعة القانونية للجريمة الالكترونية ، أركان و صور الجريمة الالكترونية في التشريع الجزائري).

كما تطرقت في الفصل الثاني الى الجريمة الالكترونية بين المعالجة و المعوقات ، و تناولت فيه ايضا مبحثين اثنين، خصصت المبحث الاول الى معالجة الجريمة الالكترونية في التشريع الجزائري و يتضمن ثلاث مطالب (تجريم الأعمال الالكترونية ، إجراءات المتابعة للجريمة الالكترونية في التشريع الجزائري ، الآليات المختصة في متابعة ومكافحة الجريمة الالكترونية) و أفردت المبحث الثاني الى تبيان معوقات مكافحة الجريمة الالكترونية و انعكاسها على التشريع الجزائي الجزائري و يتضمن ثلاث مطالب (المعوقات المتعلقة باكتشاف و إثبات الجريمة الالكترونية ، المعوقات المتعلقة بالجانب القضائي ، المعوقات المتعلقة بالمحكمة المختصة و القانون الواجب التطبيق) و في الاخير ختمت بحثي بخاتمة.

الفصل الأول

ماهية الجريمة الالكترونية

المبحـــــث الأول: مفهـــــوم الجريمـــــة الالكترونيـــــــــة

لأول مرة ظهرت الجريمة الالكترونية في الدول التي عرفت تطورا لا مثيل له في المجالين التكنولوجي و المعلوماتي ، ثم انتقلت إلى الدول الأخرى المستهلة للتكنولوجيا حيث أصبحت هاجس دق بشأنه ناقوس الخطر وأصبحت محل اهتمام المشرعين ، لهذا سنتطرق في هذا المبحث إلى دراسة الجريمة الالكترونية و ذلك من خـــــلال تحديد مفهومها و خصائصها و أسبـــابها و دوافـــع ارتكـــابها ثم تطورها التاريخي.

المطلب الأول: تعريف الجريمة الالكترونية

تقتضي دراسة الجريمة الالكترونية التطرق إلى تعريفها وقبل ذلك لابد من تحديد المصطلحات و المفاهيم الدالة على هذه الظاهرة الإجرامية المستحدثة و من ثمة بيان مختلف التعريفات للجريمة الالكترونية في التشريعات المقارنـــة فقـــها و قانـــونا .

حيث ينقسم هذا المطلب الى فرعين نتطرق بالدراسة في الفرع الأول إلى تعريف المصطلحات والمفاهيم المتعلقة بالجريمة الالكترونية ونتطرق في الفرع الثاني إلى تعريف الجريمة الالكترونية.

الفرع الأول: تعريف المصطلحات و المفاهيم المتعلقة بالجريمة الالكترونية

ترتبـــط الجريمـــة الالكترونيـــة بعـــدة مصطلحات ومفاهيـــم أهمهـــا ما يـــلي:

أولا/ الحاسب الالكتروني أو بما يسمى بالحاسب الآلي:

هو عبارة عن جهاز الكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة ولمعالجة وإدارة المعلومات بطريقة ما ، وذلك بتنفيذ ثلاث عمليات أساسية وهي :

- استعمال البيانات المدخلة (الحصول على حقائق مجردة) .
- معالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات).
- إظهار المعلومات المخرجة (الحصول على النتائج). [1]

[1] نهلة عبد القادر المومني، الجرائم المعلوماتية، ماجيستير في القانون الجنائي المعلوماتي،دار الثقافة للنشر والتوزيع 1429 هـ- 2008 م، الطبعة الاولى ، الاصدار الاول ،2008 – ص 20.

ومن التعريفات التي أعطيت للحاسب الآلي انه مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات المدخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة.

كما يعرف أيضا بأنه مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة، وهو آلـــة حاسبة الكترونية ذات سرعة عالميـــة و دقة كبيرة يمكنها قبـــول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة. [1]

كما عرفه آخرون بأنه جهاز الكتروني يعمل طبقا لتعليمات محددة سلفا ويمكنه استقبال البيانات وتخزينها والقيام بمعالجتها بدون تدخل الإنسان ثم استخراج النتائج المطلوبة. [2]

– كما عرفه البعض بان آلة أو نظام أو جهاز يستخدم في معالجة البيانات آليا للوصول إلى معلومات مقيدة لشخص أو أشخاص معنيين يهدفون إلى اتخاذ القرار الذي يساعدهم للوصول إلى هدف معـــين. [3]

و لعل من انسب التعريفات التي عرضت بيان الحاسب الآلي ما جاء في الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، حيث عرفت تلك الموسوعة الحاسب الآلـي بأنه " جهاز الكتروني يستطيع ترجمة أوامر مكتوبة، بتسلسل منطقي، لتنفيذ عمليات إدخال بيانات Data input، أو إخراج معلومات Information out put، وإجراء عمليات حسابية أو منطقية، و هو يقوم بالكتابة على أجهزة الإخراج Out put derices أو التخزين، و البيانات يتم إدخالها بواسطة مشغل الحاسب Operateur عن طريق وحدات الإدخال مثل لوحة المفاتيح Keyboard، او استرجاعها من خلال وحدة المعالجة المركزية Central processingunit ، التي تقوم بإجراء العمليات الحسابية Arithmatic Operations وكذلك

[1] خالد ممدوح ابراهيم ،امن الجريمة الالكترونية،دار الجامعة، الاسكندرية، عنوان84 شارع زكرياء غنيم الابراهيمية الاسكندرية ،2008 – ص20.

[2] محمد عبد الله ابو بكر سلامة، موسوعة جرائم المعلومات، جرائم الكمبيوتر و الانترنت، منشاة المعارف الاسكندرية، 2006 – ص 26 ، 27.

[3] محمد عبد الله ابو بكر سلامة،موسوعة جرائم المعلومات، جرائم الكمبيوتر و الانترنت – المرجع السابق.

العمليات المنطقية Logic Operations وبعد معالجة البيانات تم كتابتها على أجهزة الإخراج Out put devices مثل الطابعات Printers او وسائل التخزين المختلفة Stocage units[1]

ثانيـــــا/ المعلومـــــــــــــات: وتأخذ عدة معاني مختلفة نذكر منها:

المعلومات هي المعنى الذي يستخلص من البيانات عن طريق العرض او الاتفاق او الخبرة او المعرفة وقد اقترح الأستاذ كتالان Catalan تعريف المعلومات بأنها رسالة ما يعبر عنها في شكل يجعلها قابلة للنقل او الإبـــلاغ للغـــير. [2]

و لقد عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الأمريكية لسنة 1999 بالفقرة العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات وبرامج الكمبيوتر الموضوعية على الأقراص المرنة وقواعد البيانات وما شابه ذلك .

وفي فرنسا و وفقا للقانون رقم 82 – 652 الصادر في: 26 يوليو 1982، تعرف المعلومات بأنها صوت او صورة او مستندا او معطيات او خطابات ايا كانت طبيعتها.

و من القوانين العربية التي عرفت المعلومات القانون الأردني للمعاملات الالكترونية رقم 85 لسنة 2001 حيث المادة الثانية من هذا القانون تعرفها بأنها: البيانات او النصوص او الصور او الأشكال او الأصوات او الرموز او برامج الحاسوب او قواعد المعلومات التي انشات وأرسلت واستلمت او خزنت بوسائل الكترونية.[3]

ثالثـــــا/ المجـــــرم المعلومـــــــــاتي:

هو شخص يتمتع بالمهارة والمعرفة والذكاء وعند ارتكابه للجريمة يبررها بمبررات مختلفة لأنه يخاف من كشف جريمته ومن الدوافع التي تدفع المجرم المعلوماتي لارتكاب جريمته الرغبة في التعلم وقهر النظام المعلوماتي واثبات الذات والرغبة في الانتقام والمتعة والتحدي وهناك

[1] محمد عبد الله ابو بكر سلامة – نفس المرجع

[2] سامي علي حامد عباد ، الجريمة المعلوماتية و اجرام الانترنت ، ماجيستر في القانون ، دار الفكر الجامعي 30 شارع سوتر ، الاسكندرية 2008 – ص24 .

[3] نهلة عبد القادر المومني، الجرائم المعلوماتية – المرجع السابق – ص77 – 80.

دوافع مادية مثل الربح كما ان هناك دوافع أخرى كالتنافس السياسي والاقتصادي و التسابق العسكري بين الدول. [1]

وفي الفقه الجنائي هناك من لخص سمات المجرم المعلوماتي في الأتي: [2]

•المجـــرم المعلوماتي مجرم متخصص ، فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر ، أي أنهم متخصصون في هذا النوع من الجرائم .

•المجـــرم المعلومـــاتي مجرم عـــائد إلى الإجـــرام رغبة منه إلى سد الثغـــرات التي أدت إلى التعرف عليـه .

•المجـــرم المعلوماتي مجرم محترف فالشخص العادي لا يسهل عليه ارتكاب جرائم عن طريق الحاسب الالكتروني ، فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال وذلك لأجل التغلب على العقبات التي أوجدها المتخصصون لحماية الأنظمة المعلوماتية.

كما انه يمكن تصنيف مجرمي المعلوماتيـة الى طائفتين :

الأولى: و هم صغار نوابـــــــــغ المعلوماتيـــــة .

الثانية: و هم محترفو الجرائم المعلوماتيـــة . [3]

رابعـــــا/ شبكـــــة الانـــــترنـــت:

الانترنت او الشبكة العالمية للمعلومات كما يطلق عليها المتخصصون في علوم الحاسبات الآلية هي في ابسط تعريف لها (شبكة مشاركة معلوماتية لوكالات حكومية ، ومعاهد تعليمية ، وهيئات خاصة في أكثر من 200 دولة عن طريق أجهزة الحاسب الآلـــي الموصلة بالانترنت) .[4] والانترنت INTERNET اختصار للكلمة الانجليزية التالية:

(International Net Work) وهي منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها بعضا بطريقة لا مركزية ويدخل في تركيب هذه الشبكة ملايين

---

[1] خالد ممدوح ابراهيم ،امن الجريمة الالكترونية– المرجع السابق – ص26 .

[2] عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، مصر، سنة النشر 2007 ص 80 .

[3] عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر و الانترنت– المرجع السابق – ص 80 .

[4] محمد عبد الله ابو بكر سلامة، المرجع السابق – ص 28 .

الحواسيب الموزعة في مختلف دول العالم ، بالإضافة الى أجهزة الاتصالات والتحكم التي تعمل جميعها لتوفير وتوصيل الخدمات المختلفة للمستفيدين ، و هذا يعني اتساع إمكانية ارتكاب الجرائم وصعوبة إثباتها لهذا تسمى الشبكة الدولية .[1]

ومن أهم الاستخدامات لشبكة الانترنت نذكر منها المتعلقة بالموضوع وهي :

البريد الالكتروني – شبكة العنكبوت العالمية – استرجاع المعلومات التجارة الالكترونية – الخدمات المالية والمصرفية – البنوك الالكترونية – التعليم – الصحافة – الحكومة الالكترونية.....الخ .

الفرع الثـــاني: تعريف الجريمة الالكترونية

أدت الحداثة التي تتميز بها الجريمة الالكترونية واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح موحد للدلالة عليها ، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية ، وذلك خشية حصرها في مجال ضيق ، وترتيبها على ذلك اختلف مصطلحات الجريمة الالكترونية فما لمقصود بهذه المصطلحات؟ وما هو المصطلح المناسب لهذه الجريمة وعليه سنحاول تعريف مصطلح الجريمة الالكترونية من الجانب اللغوي والاصطلاحي :

أولا/ التعريف اللغوي للجريمة الالكترونية:

لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم او التسمية الدقيقة لهذا المصطلح ، اي الجريمة الالكترونية لوجود مجموعة من المفاهيم المتقاربة والمنشقة من الإجرام الالكتروني والغش المعلوماتي ، والانحراف الذي يقع بواسطة الجانب الآلـــي او جرائم الانترنت ، حيث تطرح إشكالية التشابه والاختلاف مصطلحي الجريمة الالكترونية والجريمة المعلوماتية ، فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية او العكـــــس؟[2]

[1] علي حسن الطوالبة، **الجرائم الالكترونية**، مؤسسة فخراوي للدراسات و النشر، مملكة البحرين، الطبعة الاولى 2008م– ص 30– 31 .

[2] محمد علي العريان ، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الاسكندرية، 2004 – ص 43 .

حيث ترى الدكتورة غنية باطلي في هذا الشأن ان استعمال مصطلح الجريمة الالكترونية من شانه ان يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي او جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالإفراد والجماعة ، مما جعل المشرع يعزز الحماية الجنائية ، فلا يستطيع المجرم ان يتحايل ويحقق مآربه عن طريق استغلال التقديم العلمي وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص.[1]

ان مصطلح الجريمة الالكترونية يعد أوسع من الجريمة المعلوماتية التي يقصد بها الجرائم المرتكبة على الكمبيوتر وجرائم الانترنت فالجريمة الالكترونية هي جريمة محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر او اي وسيلة الكترونية أخرى ، وهذا ما أكدته اتفاقية بودابست او الاتفاقية المتعلقة بالجريمة الالكترونية ، التي صادق عليها المجلس الأوروبي في بودابست المجر في: 23 نوفمبر 2001.[2]

و يقصد بالمعلوماتية المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي Informatique وتعني تكنولوجيا التجميع ، ومعالجة وإرسال المعلومات بواسطة الكمبيوتر وقد استعمل مصطلح Traitematique automatise de donnes ويعني المعالجة الآلية للبيانات ومصطلح Télématique ، أي اتصالات وهي تعادل مصطلح Telematic في اللغة الانجليزية وان كان ليس لها أصل في لقاموس الانجليزي مستمد من اللغة الفرنسية.[3]

ثانيا/ التعريف الاصطلاحي للجريمة الالكترونية:

عرفت الجريمة بصفة عامة على أنها " كل فعل غير مشروع صادر عن إرادة آثمة يقررها القانون عقوبة او تدبير احترازي" بينما تعتمد الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة

[1] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية للنشر و التوزيع، الجزائر، 2015 ص 12 – 13 .

[2] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، المرجع السابق – ص24 .

[3] خالد ممدوح ابراهيم ،امن الجريمة الالكترونية– المرجع السابق – ص43 .

الانترنت على المعلومة بشكل رئيسي و هذا الذي أدى إلى إطـــلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم .[1]

وقد اختلفت التعريفات الفقهية والقانونية خاصة بهاته الجريمة نظرا لاختلاف الوسائل والنظم القانونية المتعلقة بها ، كما يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة ، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي او الجريمة المعلوماتية .

حيث انقسم تعريف هذه الظاهرة الإجرامية إلى عدة اتجاهات تقوم على أسس مختلفة وتتمثل هذه التعريفات فيما يلي:

1- على أساس وسيلة ارتكاب الجريمة:

يعتمد هذا التعـريف على وسيلة ارتكاب الجريمة ، فلطالما كان الحاسوب الالكتـروني او إحدى الوسائل التقنية من وسـائل ارتكابها حتى تعتبر من جـرائم الانترنت ويعرفها الفقيه (تايدمان) Tiedman بأنهـا كل أشكـــال السلوك الغـــير المشروع (او الضار بالمجتمع) الذي يرتكب باستخدام الحاسوب .[2]

كما عرفها – توم فور سيتر– مؤلف كتاب قصة تقنية المعلومات – الجرائم الالكترونية ، تعريفا مطابقا للتعريف السابـق ، بقولـــه " أنها فعـــل إجـــرامي والتي تتـــم باستخـــدام الحـاسوب كأداة رئيســيـــــة ".[3]

وهنـاك من عرفهـــــا بأنهـــا " أي عمـــــل غير قـــانوني يستخـــــدم فيه الحـــاسب كـــــأداة أو موضـــوع للجـــريمة ".[4]

بينما يعرفها بعض الفقـــــه أنها نشـــــاط إجرامي تستخدم فيه التقنيـــــة الالكتـــرونية – الحاسب الآلـــي وشبكـــــة الانترنـــــت – بطـــريقة مبـاشرة أو غير مبـــاشرة كوسيلة لتنفيذ الفعل الإجـــرامي المستهـــــدف .[1]

---

[1] غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، المرجع السابق – ص5 .

[2] علي حسن الطوالبة، الجرائم الالكترونية، المرجع السابق – ص 47 .

[3] علي حسن الطوالبة، المرجع نفسه – ص48.

[4] نفـــــس المرجـــــع – ص48 .

و ترتيبا على هذه التعاريف ، تعرف الجريمة الالكترونية على أنها الفعل غير المشروع المرتكب بواسطة الحاسب الالكتروني أو الانترنت أو أي وسيلة الكترونية وقد لقي هذا التعريف عدة انتقادات أهمها اتسامه بالعمومية والاتساع لأنه يدخل كل سلوك ضار بالمجتمع يستخدم فيه الجانب الآلـــي في قائمة الجرائم الالكترونية .

2- على أساس موضوع الجريمة:

و يعتمد أصحاب هذا الاتجاه في تعريفهم للجريمة الالكترونية على أساس موضوع الجريمة او محل الجريمة ، فيجب ان يتم الاعتداء على الحاسوب او نظامه اي على المعالجة الآلية للبيانات بالتعديل او النقل او النسخ غير المشروع لها يعد جريمة الكترونية وعليه فقد عرفت الجريمة الالكترونية وفقا لهذا الاتجاه بأنها: " الجريمة المرتكبة عبر الانترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة واساءت استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر ".[2]

كما عرفها الفقيه روزنبلات (Rosenblatt) بأنها: " نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسوب او التي تحول عن طريقه ". [3]

وعرفت الدكتورة هدى قشقوش الجريمة الالكترونية بأنها: " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات او نقل هذه البيانات ، والجرائم الالكترونية مجموعة الجرائم التي تتصل بالمعلوماتية ".[4]

و نستنتج من هذه التعاريف أنها اعتمدت على محل موضوع الجريمة دون الوسيلة المرتكبة بها ، و هذا ما يشكل أهم انقاد موجه لها ذلك ان ما يميز الجريمة الالكترونية أنها تتم في وسط افتراضي و تمس بمعطيات الحاسب الآلـي او الالكتروني او كل تقنية الكترونية .

---

[1] يوسف الصغير، الجرائم المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجيستر، كلية الحقوق جامعة مولود معمري، تيزي وزو الجزائر– ص 9 .

[2] يوسف الصغير، الجرائم المرتكبة عبر الانترنت، المرجع السابق

[3] علي حسن الطوالبة، الجرائم الالكترونية، المرجع السابق – ص 48 .

[4] علي حسن الطوالبة، المرجع نفسه

3- على أساس توفر المعرفة بتقنية المعلومات او بما يسمى الجانب الشخصي للجريمة الالكترونية:

يعتمد أصحاب هذا الاتجاه على ضرورة إلمام الفاعل بتقنية المعلومات واستخدام الحاسوب لإمكانية اعتبارها من الجرائم الالكترونية ، حيث عرفها الأستاذ ديفيد تومبسون David Thompson بأنها: " اية جريمة يكون متطلبا لاقترانها ان تتوافر لدى فاعلها معرفة بتقنية الحاسوب ".[1]

ويعرفها الفقيه ستين سكيو ليبرغ Stein Schioberg بأنها: "اي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا ، كما عرفت بأنها: الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب بعمل غير قانوني".[2]

ويستخلص من هذه التعاريف أنها ارتكزت في مجملها في تعريف الجريمة الالكترونية على معيار شخصي بحت يتمثل في مدى معرفة الجاني بتقنية المعلومات وإتقانها وهو أمرا يعاب عليه ذلك انه حصر وربط شخصية الجاني او الفاعل في تعريفه للجريمة الالكترونية وهذا غير كاف فيمكن لأي شخص عادي حتى و لو لم يكن مؤهلا بتقنيات الحاسب الالكتروني ارتكاب جريمة الغش المعلوماتي او السرقة المعلوماتية.

4- على أساس الجمـــع بين عدة معايـــــير:

نظرا لعدم نجاعة التعاريف السابقة للجريمة الالكترونية ، فقد اعتمد أصحاب هذا الاتجاه إلى الجمع بين عدة معايير مختلفة وعرفوا الجريمة عبر الانترنت بأنها الجريمة التي يستخدم فيها الحاسب الآلـــي كوسيلة او أداة لارتكابها او الجريمة التي يكون الحاسب نفسه ضحيتها .[3]

[1] علي حسن الطوالبة، الجرائم الالكترونية، نفس المرجع – ص49 .

[2] نفس المرجع، نفس الصفحة.

[3] يوسف الصغير، الجرائم المرتكبة عبر الانترنت، المرجع السابق – ص11 .

و قد عرفتها منظمة التعاون الاقتصادي والتنمية ((OCDE)) في أوروبا بأنها: " كل فعل او امتناع من شانه الاعتداء على الأموال المادية او المعنوية ، يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية ".[1]

و يعرف الفقيه الفرنسي ماس Mass الجرائم الالكترونية بأنها: " الاعتداءات القانونية التي يمكن ان ترتكب بواسطة المعلوماتية بغرض تحقيق الربح ".

و يعاب على هذا الاتجاه انه جمع بين عدة تعاريف لتعريف الجريمة الالكترونية (جرائم الانترنت والكمبيوتر)، و مع هذا فان هذا التعريف يعد الناجح والراجح من الناحية العملية نظـــرا لتنوع الجرائم و تطـــــورها .

وفي تقديري أن جميع التعاريف السابقة للجريمة الالكترونية تعرضت للانتقاد وذلك راجع إلى قصورها واخذ أصحابها و النظر إليها من زاوية واحدة او معطى وحيد او النظر إليها من عدة زوايا ولكنها مختلفة وغير شاملة ولا يتوافر فيها التكوين القانوني السليم لتعريف الجريمة من حيث توافر أركانها مجتمعة ، وهذا أمرا مهم عن وضع تعريف جامع مانع للجريمة او الجرائم الالكترونية .

وهناك من الفقهاء من وضعوا تعريفا للجريمة الالكترونية في مجالين مجال واسع ومجال ضيق .

5- على أساس الاتســـــاع والتضييـــق:

أ/- **التعريف الواسع للجريمة الالكترونية:** حيث عرفها أصحابها وفق هذا الجانب بأنها: " كل فعل او امتناع عمدي ينشأ عن الاستخـدام غير المشروع للتقنية المعلومــاتية بهدف الاعتداء على الأمــوال او الأشيــاء المعنوية ". ويرى الخبــير الأمــريكي Parker مفهومها واسعا للجريمة المعلــوماتية والمتمثل في كل فعل إجرامي معتمد ايا كانت صلته بالمعلــوماتية ، وينشأ عنه خسارة تلحق بالمجني عليه ، او كسب يحققه الفــاعل ، كما يعرف الأستــاذ

[1] نهلة عبد القادر المومني، الجرائم المعلوماتية – المرجع السابق – ص49 .

Hestanc Vivant الجـريمة الالكتــرونية بأنها: " مجمــوعة من الأفعال المرتبطة بالمعلــوماتية التي يمكن أن تكون جديرة بالعقاب ".[1]

جرائم الكمبيوتر مصطلح اشمل من المصطلح السابق ويعتد فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء كان أداة للجريمة او كان هدف الجريمة ويدخل من ضمنها الاعتداء على الشبكات المحلية الخاصة بالهيئات والمنشأة الخاصة و العامة.[2]

الجريمة الالكترونية هي ببساطة استخدام التقنية الرقمية لإخافـــة الآخرين .

ب/- التعريف الضيق للجريمة الالكترونية: تعرف وفق هذا الجــانب على أنها: " كـل فعل غير مشــروع يكون العلم بتكنولوجيات الحــاسبات الآلية بقدر كبير لازمــا لارتكابه من نــاحية ، ولملاحقته وتحقيقه من نــاحية أخرى ".

يرى الأستاذ ماس Mass أن المقصود بالجريمة الالكترونية هو: " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح ".[3]

أما بالنسبة للفقه المصري فهي تنشأ عن الاستخدام غير المشروع للتقنية المعلوماتية و يهدف الى الاعتداء على الأموال أو الأشياء المعنوية.[4]

و هناك فريق آخر يرى أن الجريمة الالكترونية هي: " عمل او امتناع يأتيه إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به والتي يحميها قانون العقوبات ويفرض له عقابا ". وقد عرفها محمد علي العريان بأنها: " كل فعل ايجابي او سلبي عمدي يهدف الى الاعتداء على تقنية المعلومات ايا كان غرض الجاني ".[5]

و يعتبر الاقتراح المقدم من طرف مجلس الشيوخ الفرنسي بشأن نظام المعالجة الآلية عند تبنيه للقانون 88-19 المتعلق بالغش المعلوماتي المعدل والمتمم المؤرخ في: 1988/01/05

---

[1] أمــير فــرج يوســف، الجرائم المعلوماتية على شبكــة الانترنت، دار المطبوعات الجامعية ، امام كلية الحقوق، ت 4126869، الاسكندرية 2009 – ص 106 – 107 .

[2] نهلــة عبد القادر المومني ، المرجع السابق – ص48.

[3] نشناش مونية ، مداخلة حول الركن المفترض في الجريمة الالكترونية ، جامعة بسكرة 2015 / 2016 – ص 2 ، 3

[4] محمد علي العريان ، الجرائم المعلوماتية، مرجع سابق – ص45 .

[5] نشناش مونية ، المرجع السابق – ص2 -3 .

والذي تم إدماجه في قانون العقوبات الفرنسي يعتبر أهم تعريف الاعتماد عليه لتحديد مفهوم المعالجة الآلية للمعطيات ، بحيث اقترح هذا المجلس التعريف التالي: نظام المعالجة يتكون كل منه من ذاكرة ، برامج ، معطيات ، أجهزة إدخال وإخراج ، أجهزة ربط ، يربط بينها مجموعة من العلاقات تتحقق عن طريق نتيجة معينة وهي معالجة المعطيات ، مع ضرورة أن يكون هذا المجموع المركب محميا بأجهزة أمان.[1]

وانه على الرغم من شيوع هذا التعريف في أوساط الفقه إلا أن الجمعية الوطنية الفرنسية لم تحتفظ به عند الصياغة النهائية لنص القانون 19/88 و يعزى ذلك لأسباب منهجية بحث لا علاقة لها بمضمون هذا التعريف انه اشترط على نظام المعالجة الآلية للمعطيات أن تتوافر على شرطين لا قائمة له ولا حماية قانونية بدونهما وهما:

ضرورة وجود علاقات تربط بين العناصر الداخلية في تكوين النظام وتواجدهما نحو تحقيق هدف واحد محدد هو المعالجة الآلية للمعطيات هذا مع الملاحظة أن العناصر الأدبية والمعنوية التي يتكون منها المركب ، والتي ذكرت في تعريف مجلس الشيوخ إنما وردت على سبيل المثال و هذا يفتح المجال أمام إضافة عنـــاصر جديدة أو حذف بعضها حسب ما يقرره التطور التقني في هـــذا المجال مستقبـــلا.

ضرورة توافر النظام على أجهزة أمـــان تحقق له حماية فنية كشرط للتمتع بالحمـاية الجنـائية .[2]

ثالثـــــا/ التعريف القانوني للجريمة الالكترونية:

لقد تجنبت أغلبية التشريعات العالمية من الخوض في مسالة وضع تعريف تشريعي او قانوني للجريمة الالكترونية او بما يسمى عن بعض التشريعات من نظام المعالجة الآلية للمعطيات و اوكلو تلك المهمة إلى الفقه والقضاء ، إلا أن بعضهم اتجه الى وضع تعاريف

[1] علي عدنان الفيـــل ، الاجـــرام الالكتروني ، دراســـة مقارنة ، منشورات زين الحقوقية ، الطبعة الاولى 2011 –ص 123 – 313 ((قانون امارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات التجارية الالكترونية صادر بتاريخ:12 /02 /2002)) .

[2] نشناش مونية ، مداخلة حول الركن المفترض في الجريمة الالكترونية، المرجع السابق – ص3 .

لنظام المعلومات وليس لنظام المعالجة الآلية للمعطيات ومن بين التشريعات التي عرفت النظام المعلوماتي نذكر منها:

1- قانون اليونسترال النموذجي بشأن التجارة الالكترونية لسنة 1996:

حيث عرف هذا القانون من خلال نص المادة 02 الفقرة 6،ويعرف نظام المعلومات على انه"النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو تخزينها لتجهيزها على أي وجه آخر.[1]

2- قانون المعاملات الالكترونية الأردني رقم 28 لسنة 2001:

حيث عرف هذا القانون من خلال المادة 02 الفقرة 10 أيضا نظام معالجة المعلومات على انه " النظام الالكتروني لإنشاء رسائل المعلومات او إرسالها او تخزينها على أي وجه أخر".[2]

3-قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم 02 لسنة 2002:

حيث عرف هذا القانون هو الأخر من خلال نص المادة 02 الفقرة 06 نظام المعلومات الالكتروني على انه " نظام الكتروني لإنشاء او استخراج او إرسال او استلام او تخزين او عرض او معالجة المعلومات او الرسائل الالكترونية ".[3]

ما يلاحظ على التعريفات المشار إليها أعلاه أنها في مجملها تنطبق على نظام المعالجة الآلية للمعطيات أكثر منها على نظام المعلومات ككل ، وأنها انصبت في مجرى واحد معتمد في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها او ينجزها هذا النظام ، والتي تمثل طرق المعالجة المعلوماتية وتعتبر " المعالجة الآلية " مجرد وظيفة من تلك الوظائف على الرغم من ان فكرة المعالجة الآلية أوسع من فكرة المعالجة المعلوماتية ، ضف

[1] علي عدنان الفيل ، الاجرام الالكتروني، المرجع السابق، ص 123 – 313 ((قانون رقم 85 لسنة 2001 ، الجريدة الرسمي للمملكة الاردنية الهاشمية رقم:4524 الصادر بتاريخ: 2001/12/31 – ص 6010)).

[2] علي عدنان الفيل ، نفس المرجع ، ص 123 – 313 ((قانون امارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات التجارية الالكترونية صادر بتاريخ:12 /02 /2002)).

[3] نشناش مونية ، المرجع السابق – ص3.

إلى ذلك خلوها من الإشارة الى الشرطين اللذين أشار إليهما مجلس الشيوخ الفرنسي الى ضرورة توافرها في النظام .[1]

4-المشرع السعودي: عرف المشرع السعودي نظـــام مكافحـــة جرائم المعلوماتيـــة بأنه: " مجموع

برامج وأدوات معدة لمعالجة البيانات وإدارتها ، وتشمل الحاسبات الآلية ". وينطبق على تعريف المشرع السعودي ما تقدم من انتقادات بسان تعريف التشريعات الثلاثة أعلاه لكن ما يحسب له هو اشتراطه اشتمال النظام على حاسبات آلية ، اذ توجد في هذه الأخيرة على اختلاف أنواعها وان صح التعبير غرقه المعالجة الآلية للمعطيات ، يتميز الحاسب الآلـي بقدرته الهائلة على معالجة أحجام ضخمة من البيانات والمعطيات و بسرعة عالمية جدا ودقة متناهية دون تعب أو ملل .[2]

المطلب الثاني/ خصائص و أسباب الجريمة الالكترونية:

من خصوصية الجريمة الالكترونية ان بعض حالات ارتكابها يعتمد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة منها المعالجة الالكترونية للبيانات ، و مجال المعاينة الالكترونية للنصوص ، و الكلمات الالكترونية .

في المجال الأول: يتدخل الجاني من خلال ارتكاب الجريمة الالكترونية في مجال المعالجة الالكترونية للبيانات ، سواء من حيث تجميعها او تجهيزها حتى يمكن إدخالها الى جهاز الحاسب الآلي ، و ذلك بغرض الحصول على المعلومات.

أما في المجال الثاني: يتدخل الجاني في مجال المعالجة الالكترونية للنصوص و الكلمات، و هي طريقة اوتوماتيكية تمكن مستخدم الحاسب الالي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الادوات الموجودة تحت يده، و بفضل إمكانيات الحاسب الآلي نتاج إمكانية التصحيح و

[1] عمر محمد ابو بكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية 2004 – ص 6 .

[2] نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر ، الجرائم الالكترونية ، طرابلس 24 – 25 مارس 2017 – ص 6 .

التعديل و المحو و التخزين و الاسترجاع و الطباعة ، و هي بذلك علاقة وثيقة بارتكاب الجريمة.[1]

و بالرغم من خصوصية التي تتميز بها هاته الجريمة الا ان الدافع و القصد يشكلان اهم الركائز التي تحرك لارتكاب افعال الاعتداء المختلفة تحت مفهوم الجريمة الالكترونية وهذا ما سنحاول توضيحه من خلال التطرق الى خصائص الجريمة الالكترونية في الفرع الاول و أسباب و دوافع ارتكابها ضمن الفرع الثاني.

الفرع الأول: خصائص الجريمة الالكترونية:

تتمـــيز الجريمة الالكترونية بطبيعة خاصة يميزها عن الجريمة التقليدية و لذا أخذت هذه الخاصية بهذا النوع من الجرائم عدة سمات وحقائق سواء تعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي .[2]

وبناءا عليه سنتطرق بالبحث في خصائص الجريمة الالكترونية كما يلي:

أولا/الجريمة الالكترونية جريمة عالميـــة الحـــــدود:

إن من أهم الخصائص التي تميز الجريمة الالكترونية انها جريمة عابرة وتتخطى الحدود الجغرافية للدول وذلك لاتصالها بعالم الانترنت وتقنية المعلومات ، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد ، وسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها .

حيث أدت هذه الخاصية الى انعكاسها على طبيعة الأعمال الإجرامية التي يعد فيها المجرمون الى استخدام هذه التقنيات في خرقهم للقانون وهو ما يعني ان مسح الجريمة الالكترونية لم يعد محليا بل أصبح عـالميا. فهي قد تتجـاوز الجدود الجغـرافية باعتبـار أن تنفيذهـا يتم عبر الشبكة المعلومـاتية، وهو ما يشير في كثير من الأحيان الى تحديات قانونية إدارية فنية بل وسياسية ، بشأن مواجهتها لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية ،

[1] محمد علي العريان،المرجع السابق، ص 37 .

[2] ادهم باسم نمر بغدادي ، وسائل البحث والتحري عن الجرائم الالكترونية ، اطروحة بدرجة ماجيستر في القانون العام بكلية الدراسات العليا ، جامعة النجاح الوطنية ، نابلس، فلسطين 2018 – ص 11 .

القيام بإعداد احد البرامج في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دولة مختلفة من العالم.[1]

ومن أهم القضايا التي أكدت هذه الخاصية قضية عرفت باسم مرض نقص المناعة المكتسبة ايدز ، وتتخلص وقائعها عام 1989، حيث قام احد الأشخاص وهو جوزيف بين النسخ احد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الايدز لكن في الحقيقة يحتوي هذا البرنامج على فيروس يؤدي الى تعطيل جهاز الحاسب الآلـــي عن العمل فيقوم الفاعل او الجاني بطلب مبلغ مالي للحصول على عنوان الكتروني مضاد للفيروس ، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرسال البرنامج على أراضيها ، و بالفعـــل تمت محاكمته أمام القضـــاء الانجلـــيزي إلا أن إجـــراءات محاكمتـــه لم تستمر بسبب حالته العقلية.[2]

و تشير خاصية عالمية الحدود للجريمة الالكترونية عدة أثار قانونية أهمها القانون الواجب التطبيق عليها والقضاء المختص بها ، فهل هو قانون الدولة التي وقع فيها النشاط الاجرامي ، أم الدولة التي يقيم فيها الجاني أو الدولة التي أضرت بمصالحها هذا التلاعب .

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إجرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم

و لقد قام المشرع الجزائري بموجب القانون 04/09 المؤرخ في: 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

[1] نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة اعمال المؤتمر الدولي الرابع عشر ، الجرائم الالكترونية ، طرابلس – 24 – 25 مارس 2017 – ص7 .

[2] انظر القانون 09 – 04 المؤرخ في:2009/08/05 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها – الجريدة الرسمية رقم: 47 الصادرة في:16 /2009/08.

ومكافحتها بسن أحكام خاصة بالتعاون والمساعدة القضائية والدولية المتبادلة عن طريق المواد 16-17- 18 من هذا القانون .[1]

ثانيـــا/الجريمة الالكترونية سريعـــــة التنفيـــــــذ:

ان تنفيذ الجريمة الالكترونية لا يتطلب الوقت الكثير فبضغطة واحدة على لوحة المفاتيح يمكن ان تنتقل ملايين الدولارات من مكان الى آخر وهذا يعني انها لا تتطلب الإعداد قبل التنفيذ او استخدام معدات وبرامج معينة ، بالإضافة الى ذلك فان الجريمة الالكترونية في اغلبها ما عدى جريمة سرقة معدات الحاسب لا تتطلب وجود الفاعل في مكان الجريمة سواء من خلال الدخول للشبكة العنكبوتية او اعتراض عملية تحويل مالية او سرقة معلومات هامة او تخريب .....الخ.[2]

ثالثـــا/صعوبـــــة إثبـــات الجريمة الالكترونية:

حيث ان الجرائم الالكترونية تتصف بالخفاء اي عدم وجود اثار مادية يمكن متابعتها ، وهي خطيرة وصعبة الإثبات او هي صعبة في تحديد موقعها، او مكان التعامل معها بسبب اتساع نطاقها المكاني، وضخامة البيانات ترجع صعوبة الجريمة الالكترونية الى عدة أمور منها:

- لانها جريمة لا تترك اي آثار جانبية لها بعد ارتكابها، فهي جريمة تقع في بنية الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية الغير مرئية ولا توجد مستندات ورقية.
- صعوبة الاحتفاظ الفني بآثارها ان وجدت ، باعتبارها جريمة لا تترك أثرا ، فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات ، ولذا فان معظم هذه الجرائم تم اكتشافها بالصدفة او المصادفة وبعد وقت طويل من ارتكابها ، فالجريمة الالكترونية من الجرائم المستحدثة التي لا تترك شهودا يمكن استجوابهم ولا أدلة مادية يمكن فحصها من هنا تأتي صعوبة الكشف عن هذه الجريمة .

[1] داود وسيلة ، الجريمة الالكترونية على ضوء قانون العقوبات الجزائري ، كلية الحقوق و العلوم السياسية جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2018 - 2019 –ص 21 – 22 .

[2] خالد ممدوح ابراهيم ،امن الجريمة الالكترونية– مرجع سابق – ص45 – 46.

– تحتاج الى خبرة فنية ويصعب على المحقق التقليدي التعامل معها حيث تتطلب جرائم الكمبيوتر والانترنت المهام الخاص بتقنيات الحاسبات الآلية ونظام المعلوماتية سواء لارتكابها او التحقيق فيها او متابعتهم قضائيا .[1]

– قلة الإبلاغ عن الجريمة الالكترونية ذلك ان المجني عليه يحجم عن طلب مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها حتى في حالة الإبلاغ، فان المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين في الحالة التي يكون فيها المجني عليه عادة بنكا او مؤسسة مالية (شخصا معنوي) لمهمة المحافظة على سمعته وثقة عملائه، أكثر من اهتمامه بالكشف عن الجريمة ومرتكبيها لذلك يفضل المجني عليه تقديم ترضية سريعة لعميله، وينهي الأمر داخليا كما ان للمجني عليه دور مثير لريبه ، قد يشارك بطريقة غير مباشرة غير مباشرة في ارتكاب السلوك الإجرامي، ذلك في حالة التي يكون فيها مثلا المجني عليه امرأة ثم التحرش بها وابتزازها عبر مواقع التواصل الاجتماعي فيسبوك فتضطر الضحية للرضوخ لطلبات الجاني خشية من تشويه سمعتها .[2]

لكن هناك حالات ضئيلة أين تم فيها الإبلاغ عن الجريمة الالكترونية نسبة الى شخصية المجني التي تلعب دور مهم في عملية الإبلاغ .و لذا كان من الأحسن إيجاد صيغة عمل مشتركة بين مختلف أجهزة القضاء والأمن وحتى الخبراء والتنسيق بينهم عن طريق عقد دورات تدريبية بغرض تحقيق التعاون بين هذه الجهات والوصول إلى طرق وحلول قانونية كفيلة بمعالجة الجرائم الالكترونية.

[1] داود وسيلة ، الجريمة الالكترونية على ضوء قانون العقوبات الجزائري – ص 23 .

[2] نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة ، – اعمال المؤتمر الرابع عشر ، الجرائم الالكترونية ، طرابلس – 24 – 25 مارس 2017 – ص7 – 8 .

رابعـــا/مرتكبـــو الجريمة الالكترونية ذوو صفـــات خاصة:

يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا الى السلوك الإجرامي النمطي بعدة خصائص عددها الأستاذ Parker فيما يلي:

أ/ المجرم المعلوماتي مجرم متخصص ومحترف في تنفيذ جريمته الالكترونية حيث ان ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر .

ب/ خلافا على المجرم العادي، فالمجرم المعلوماتي لا يلجا الى العنف في تنفيذ جرائمه ، فهو مجرم ذكي يتمتع بالمهارة او المعرفة وبدرجة عالمية من الثقافة .

ج/ يوجد عدة أنواع من المجرمين المعلوماتيين فهناك:

1-طائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون إحداث اي ضرر ويسمونهم Pransker .

2-طائفة الأشخـــاص الذين يستهدفون الدخول الى أنظمة الحاسبات الآلية الغير المصرح لهم بهدف الفضول او اكتساب الخبرة او لمجرد القدرة على اختراق هذه الأنظمة ويسمون Hackers.

3-طائفة الأشخاص الذين يستهدفون إلحاق خسائر بالمجني عليهم ، دون ان يكون الحصول علو مكاسب مالية ضمن هذه الأهداف، ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية و موزعيها ويسمون Malicieuses Hackers .

4- طائفة الأشخاص الذين يهدفون إلى إلحاق الأذى بالمجني عليهم ، ويكون الباحث إيجاد حلول لمشاكل مادية تواجد الجاني لا يستطيع حلها بالطرق العادية ويسمون Personnel problème Solvers

5- طائفة الأشخاص الذين يهدفون الى تحقيق ربح مادي بطريق غير مشروع ويسمون Carier Criminels.[1]

[1] لعقال فريال ، الجريمة المعلوماتية في ظل التشريع الجزائري ، مذكرة لنيل شهادة الماستر في القانون العام ، تخصص القانون و العلوم الجنائية ، جامعة اكلي محند الحاج ، البويرة ، السنة الجامعية 2014 – 2015 – ص 22

6-طـــائفة الأشخاص المشكلة للجهات الإرهابية او المتطرفة يهدفون الى نشر أفكارهم ومعتقداتهم باللجوء الى استخدام النشاط الإجرامي بالعنف ضد الأشخاص والممتلكات من اجل لفت الأنظار الى ما يدعون إليه ويسمون Exterme Advocates.

7- طـــائفة الأشخاص تحت مسمى The Criminally Negligent والتي تضم واحدة من أهم المشكلات التي تتصل بإســـاءة استخدام الحـــاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحـاسبات الآلية وفي اغلب الأحيـان نتائج خطيرة قد تصـل الى حد إزهاق الروح.[1]

و تلخص الباحثة إسراء جبريل رشاد مرعي في كتابها الجرائم الالكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها " خصائص الجريمة الالكترونية فيما يلي:

1- تتسم بسهولة الوقوع في فخها،حيث أن غياب الرقابة الأمنية تساهم في انتشارها وتسهيل ذلك.

2- الضرر الناجم عن عن الجرائم الالكترونية غير قابل للقياس إذ أنها تلحق إضرار جسيمة .

3- صعوبة الكشف عن مرتكبها الا بأساليب أمنية وتقنية عالمية .

4- سلوك خارج عن المألوف وغير أخلاقي مجتمعيا .

5- ذات عنف وجهد اقل من الجرائم التقليدية .

6- جريمة غير مقيدة بزمان ومكان اذ تمتاز بالتباعد الجغرافي وعدم تقيدها بالتوقيت الزمني .

7-سهولة إخفاء آثار الجريمة والأدلة التي تدل عن الجاني نظرا للترميز والتشفير الذي يحدث على الرموز المخزنة على وسائط التخزين الممغنطة .

الفرع الثاني: أسباب و دوافع الجريمة الالكترونية

مما لا شك فيه فان فئات مرتكبي الجريمة تختلف عن الأفعال الإجرامية التقليدية لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب و العوامل التي تدفع في ارتكاب الفعل غير المشروع فضلا عن ذلك تتمتع جرائم الكمبيوتر و المعلوماتية بعدد من الخصائص التي تختلف

[1] لعقال فريال ، الجريمة المعلوماتية في ظل التشريع الجزائري، المرجع السابق – ص 22 .

تماما عن الخصائص التي تتمتع بها الجرائم التقليدية ، كما أن الجاني الالكتروني (أو المجرم الالكتروني) يختلف أيضا عن المجـــرم العـــــادي.[1]

ولا بد من التأكيد على أن الجريمة مهما اختلفت وتنوعت تسميتها في الأخير ستتشكل من عناصر رئيسية لتشجيع المجرم على ارتكابهـــا وهي:

1- دافـــع معين لارتكاب العمل.
2- هـــــدف الضحيـــــة.
3- الفرصـــــة المواتيـــــة.
4- غياب عيون الأمـــن.[2]

بالإضافة إلى جملة من الدوافع الشخصية والخارجية التي تقف في غالب الأحيان وراء الجريمة الالكترونية والتي سنتناولها بالشرح في ما سياتي.

أولا/ الدوافـــــع الشخصيـــــة:

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميلوا مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة انه إزاء ظهور أي تقنية مستحدثة فان مرتكبو هذه الجرائم لديهم شغف الآلة يحاولون إيجاد وغالبا ما يجدون الوسيلة إلى تحطيمها بل التفوق عليها ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة، وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الجريمة المعلوماتية، وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي هو سر كل نظام قد ينتابه إحساس بالإهمال أو النقص داخل، المنشأة التي يعمل بها وقد يندفع تحت تأثير الرغبة

[1] مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، انظر الرابط hrdoegypt.org/wp-content/uploads/2014/12 تقرير الجريمة الالكترونية، تاريخ الزيارة 2021/04/18 على الساعة 14:52سا.

[2] احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، 2005، ص 126 وما بعدها.

القوية من اجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيته أمام العامة.[1]

بالإضافة إلى دوافع أخرى نذكر منها على سبيل المثـــال:

1- حـــــب التعلـــــم:

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع إلى ارتكاب مثل هذه الجرائم لان المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب ألا تبقى المعلومات حكرا على أي احد: أن للجميع الحق في التعرف والاستفادة من هذه المعلومات.

2- المنفعـــــة الماديـــــة:

قد تكون محاولات الكسب السريع وجني الأرباح الطائلة دون تعب ولا رأس مال من الأسباب التي تدفع الى اختراق أنظمة الكترونية كالتي تستخدمها المصارف عن طريق الدخول الى الحسابات المصرفية والتلاعب فيها او الاستخدام غير المشروع لبطاقات الائتمان.[2]

3- التسليـــــة واللهـــــو:

عدد غير قليـل من مختـرقـي الأنظمة يتخذون من عملهم هـذا وسيلة للمرح والتسلية وتقضية اكبر وقت ممكن في أنظمة وحـواسيب الآخرين ويكون هـذا الاختـراق غـالبا سلميا ودون أن يحدث تـأثيـر يـذكر.

ثانيـــا/ الدوافـــع الخارجيـــة:

إن تأثير الإنسان من بعض المواقف يجعله في حالة استسلام تام لكثير من المؤثرات والدوافع الخارجية التي تدفعه إلى ارتكاب بعض الجرائم الالكترونية، وذلك نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، و مع توافر هذه المؤثرات، فان الأمر حتما سيؤدي إلى ارتكابه للجريمة الكترونية، أما بدافع الانتقام او جنون العظمة او بدافع التعاون والتواطؤ على الأضرار والتهديد.

---

[1] مركز هردو لدعم التعبير الرقمي، مرجع سابق، ص 10.

[2] موقع جزا يرس، جرائم الالكترونية تهدد امن الجزائريين، نشر في أخبار اليوم يوم 2018/04/10 من الرابط –https //www.djazairess.com/akhbarelyoum/240271 تاريخ الزيارة 2021/04/18 بتوقيت الساعة 15 سا11د.

1- دافع الانتقام وإلحاق الضرر برب العمل.

قد يكون الانتقام مؤثر في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشات بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشأة، ولقد لوحظ ان العاملين في قطاع التقنية او المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من منشأة او رب العمل.[1]

2- دافـــــع عقائـــــــدي:

تتمثل في تلك القوى الداخلية المحركة لأشخاص حيث يبرر الكثير محاولاتهم لاختراق أجهزة الغير بحجة أنهم على مذاهب او طوائف دينية معادية لمذاهبهم او بحجة تكفيرهم وفضح أسرارهم.

3- دافع عنصري:

والذي يكون وراء هذا النوع من الجرائم الالكترونية ويأتي عن طريق تميز بين عرق وأخر وقبيلة وأخرى فتجد مرتكبيها يسعون بكل الطرق إلى افتعال المشاكل وعمل أعمال تخريبية من شانها جر المشاكل عن طريق نشر شائعات وأكاذيب.

4- دافع سياسي وإيديولوجي:

وهو الدافع الذي يلعب فيه الإرهاب الدور المركزي والأساسي وذلك من خلال لجوئه إلى الانترنت كوسيلة رئيسية لبث أفكاره العصرية المتمثلة في استخدام المتفجرات أصبحت الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمر البنية المعلوماتية وتغلق مواقع حيوية وتشل أنظمة القيادة والاتصالات او حتى قطع شبكات الاتصال بين الوحدات والقيادات

[1] خالد دوادي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، 2018، ص 40.

المركزية او تعطيل أنظمة الدفاع الجوية والبرية والبحرية او شل محطات إمداد الطاقة والماء أو اختراق النظام المصرفي مما يضر بأعمال البنوك والأسواق المالية العالمية.[1]

و في الأخـــير نجد أن الإرهـــاب الالكتروني مهما تعددت أسبابـــه وأنواعه فهي نفسها عموما أسباب ظاهرة الإرهاب حيث تتداخل الدوافـــع الشخصية مع الدوافع الفكرية والسياسية والاقتصادية والاجتماعية.

المطلب الثالث: التطور التاريخي للجريمة الالكترونية:

لقد ظهرت جرائم الانترنت في حقل جرائم التقنية في نهاية الثمانينات، ولكن ذلك من خلال عدوان الفيروس و بالأخص جريمة "دودة موريس" المؤرخة واقعتها في نوفمبر 1988.

و لقد أطلق مصطلح جرائم الانترنت في مؤتمر انعقد في استراليا في الفترة 16-1988/02/17. وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الانترنت. إذ نجد البعض يستخدم مصطلح "الإجرام المعلوماتي" ومنهم من يستخدم مصطلح "الغش المعلوماتي" في حين يجب استخدام المصطلح الدقيق و المتماشي مع طبيعة تلك الجرائم وهو "الجريمة الالكترونية" ذلك لان الإجرام المعلوماتي وان كان يقصد به التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني أن الاعتداء على المعلومة يتحقق دائما باستخدام الكمبيوتر، وخصوصا باستخدام الانترنت، وعليه فالجريمة الالكترونية قد تكون اشمل من جرائم الانترنت وذات الشأن بالنسبة للغش المعلوماتي و كذا "جرائم التكنولوجيا المتقدمة".[2]

لقد لاحظ مؤتمر القانون و الانترنت المنعقد في لشبونة / البرتغال في: 2001/01/26 انه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة، واعتماد مصطلح Cyber Crime

[1] جميل عبد الباقي الصغير، مدى كفاية نصوص العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الانترنت، الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، أبو ظبي من 15 إلى 2008/11/19.

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي 30 شارع سوتير، الإسكندرية، 2013، ص 31.

دون غيره للتعبير عن الجرائم الالكترونية، مع الأخذ بعين الاعتبار التمييز بين تلك الجرائم التي يمكن ارتكابها عبر الانترنت.[1]

لقد مرت الجرائم الالكترونية بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ولهذا مرت بثلاث مراحـــــل وهي:

الفرع الاول: مرحلـــــــة استخدام الحواسيب من الستينات إلى التسعينات من القرن الماضي:

من شيوع استخدام الحواسيب من الستينات إلى التسعينات من القرن الماضي، اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر. وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أو ظاهرة إجرامية مستحدثة، وان الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات، ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجر سلوكيات مرفوضة.

يشير (دون باركر) إلى أول حالة موثقة لجريمة ارتكبت بواسطة الحاسوب ترجع الى عام 1958 م، و شهد ذلك العام العديد من الجرائم التي رصدها معهد (ستانفورد) الدولي للابحاث في امريكا ، و صنفها الى اربع جرائم : العبث او التخريب الموجه الى الحاسوب، سرقة المعلومات او الممتلكات ، الاحتيال او الغش المالي، الاستخدام غير المصرح به لخدمات الحاسوب.[2]

ووصفت مرحلة الستينات بانها مرحلة طرح البيانات الاولية لاجرام تقنية المعلومات، وظهرت تستهدف المعطيات من خلال انظمة الاتصالات البعدية (او عن بعد) ، و جرى التعبير عن انشطة اختراق شبكات الحواسيب باصطلاح هاكنك Hacking ، و لكنها بقيت محدودة .

الفرع الثاني: مرحلـــــة استخدام الحواسيب ما بعد الثمانينات:

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص 158.

[2] علي حسن الطوالبة، الجرائم الالكترونية، مرجع سابق – ص 92 .

في الثمانينيات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت وارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد أنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج.

شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظام، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني. ولكن هؤلاء المغامرون أصبحوا أداة إجرام. وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على ارتكاب أفعال تستهدف الاستيلاء على المال، أو التجسس أو الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية.

كما شهدت الثمانينات ، تبلور ركائز السياسة التشريعية في مجال الجرائم الالكترونية من حيث الموائمة بين الحق في المعلومات بما يتطلبه من كفالة انسياب و تدفق المعلومات ، أما الأنماط الجرمية المستحدثة ضمن إطار الجرائم الالكترونية مثل جرائم الاستخدام غير المصرح به لخدمات الحاسوب ، وجرائم غش الحاسوب ، و جرائم التلاعب بالمنافذ البنكية بواسطة البطاقات الممغنطة ، و الفيروسات كما شهدت هذه المرحلة سن قوانين لحماية استخدام الحاسوب و تجريم الأفعال او بعضها ، و تزايد النشاط المؤسساتي ، كهيئة الامم المتحدة ، و منظمة التنمية الاقتصادية ، و المجلس الأوروبي، و المنظمة العالمية للملكية الفكرية ، و الجمعية المصرية للقانون الجنائي، ومركز الدراسات الأمنية في الرياض.[1]

الفرع الثـــالث: مرحلة شيوع استخدام الحواسيب ما بعد التسعينات:

شهدت التسعينيات تناميا هائلا في حقل الجرائم الالكترونية و تغيير في نطاقها و مفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات، ظهرت أنماط تقوم على فكرة تعطيل نظام تقني و تمنعه من القيام بعمله المعتاد و أكثر ما مورست ضد الانترنت التسويقية الهامـــة التي يتسبب انقطاعها عن الخدمـــة ساعات في خسائر مالية بالملايـــــين، ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت. وظهرت الرسائل

[1] علي حسن الطوالبة، المرجع نفسه – ص95 – 96.

المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير قانونية أو غير مشروعة.[1]

المبحث الثـــاني : مفهـــوم الجريمة الالكتـــرونية في التشـريع الجـــزائري .

الجزائر كغيرها من الدول التي استقطبت التكنــولوجيا واستهلكت منتجاتها فقد حملت إليها الجـــانبين الايجابي المتمثل في تسهيل وتبسيط الحياة الاجتماعية والسلبي المتمثل في الضرر الناتج عن سوء استعمـــالها عندها كان لابد من إيجاد إطار قانـــوني مناسب لسد الفـــراغ الإجرائي لذلك تم وضع مجموعة من الإجـــراءات والتي تعد قاسما مشتركا بين الجرائم التقليدية والجرائم الالكترونية عن طريق تعـــديل قانون الإجـــراءات الجزائية لتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجـــرائم المستحدثة او ما يصطلح على تسميته بالجرائم الالكترونية ، ومجالها هو جهاز الكمبيوتر المستخدم لاختراق شبكة الانترنيت . لذلك يمكن القول إن كل تطور ايجابي لا يخلو من سلبيات ، والآثار السلبية للانترنيت كبيرة وخطيرة ذلك هو الأمر الذي القي رجال القانون مسؤوليته تاريخية وإنسانية تجاه هذا الخطر الدائم . إذ لا يخفى على احد بان الجرائم الالكترونية لم تعد مقتصرة على القرصنة لسرقة المعلومات والسطو على أرقام بطاقات الائتمان لاستخدامها والاستغلال الجنسي للأطفال والإخلال بالآداب العامة ناهيك عن جرائم التجسس الإرهاب شملت مختلف المجالات .[2]

المطلب الأول : تعـــريف المشرع الجـــزائري للجـــريمة الالكـــترونية .

سنتطرق في هذه المطلب إلى تعريف الجـــريمة الالكتـــرونية في التشـــريع الجزائري تعريفا فقـــهيا ، أكاديمـــيا وقـــانونيا .

الفرع الأول : التعريف الفقهي .

[1] عبد الفتاح مراد، دور الكمبيوتر في مجال ارتكاب الجريمة الالكترونية، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية.

[2] زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى ، عين مليلة ، الجزائر ،د ط ،2001 ، ص42

إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلا في الجرائم التقليدية ، فلهذا ظهر اختلاف في تعريفها . من بين التعاريف نجد تعريفا يعرفها بأنها " الجريمة التي تتام باستخدام جهاز الكمبيوتر من خلال الاتصال ".

وهناك من يعرفها على أنها ، " كل عمل أو امتناع عن عمل يقوم به شخص إضرار بمكونات الحاسوب المادية والمعنوية ، وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانونا العقوبات لحمايتها ".

أو أنها استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف الثابت .أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع .

ومن خلال هذه التعـــاريف تبنى الفقه الجـــزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلـــي أو شبكاته، إذ عرف الجريمة الالكترونية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب . وتتمثل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئـــــة الكترونيـــــة.[1]

الفرع الثـــــــاني: التعريف الأكـــــاديمـــــي.

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

– عندما تكون المعلومـــاتية موضوعا للاعتداء (عندما تقع الجريمة على المكونـــات المادية للأجهزة والمعدات المعلوماتية) .

– عندما تكـــون المعلومـــاتية أداة و وسيلة لاعتـــداء (عندما يستخدم الجـــاني جهاز معلومـــاتي لتنفيـــذ معلوماته) .[2]

[1] زبيخة زيدان ، مرجع سابق ، ص43،44 .

[2] المقدم عز الدين عز الدين ، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية ، بسكرة ، 2015/11/16 .

الفرع الثـــالث: التعريف القـــانوني.

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، ويمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي لابد من تحقيقه حتى يمكن البحث في توافر أركان الجريمة من جرائم الاعتداء على هذا النظام . فان ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث .

والمشرع الجزائري على غرار الكثير من التشريعات لم يعرف نظام المعالجة الالية للمعطيات ، و أوكل بذلك المهمة لكل من الفقه و القضاء ، و لمزيد من التفاصيل نتطرق الى تعريف الجريمة الالكترونية من خـــــــلال القانونـــــين 15/04 و 04/09 على التوالي:

اولا/ تعريف الجريمة الالكترونية في التشريع الجزائري في القانون 15/04 :

جـــــرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية، وهي شكل من أشكال الإجرام الجديدة التي لم تشهدها البشرية من قبل . وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04- 15 ، المؤرخ في العاشر من نوفمبر 2004 المتمم للأمر رقم (66- 156) المتضمن قانون العقوبات ، والذي افرد السابع مكرر منه تحت عنوان ، " المساس بأنظمة المعالجة الآلية للمعطيات "، والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 397 مكرر 07 .[1]

بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر 1 إلى المادة 394 مكرر 2 نجد انه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات. حيث حددها في المادة 394 مكرر 1 بالاتي:[2]

- الدخول والبقاء بالغـــش في كـــل أو جـــزء من المنظومة للمعالجة الآليـــة للمعطيات أو محاولـــة ذلك.

[1] عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق ، جامعة الإسكندرية ، 2006 ، ص27 .

[2] نعيمة دوادي، الجريمة الالكترونية (خصائصها ومجالات استخدامها، واهم سبل مكافحتها) ، جامعة علي لونيسي ، البليدة الجزائر مقال منشور بمجلة معهد اللغات المجلد 2 العدد 1 / 2020 تاريخ النشر:2020/08/20 ص 47 .

– حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر 1 فقد أشارت على ما يلي:

- إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

- 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 استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.(القانون رقم 04-15 المؤرخ في:10 نوفمبر، يعدل ويتمم الأمر 66-156 المؤرخ في: 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004).

اولا/ تعريف الجريمة الالكترونية في التشريع الجزائري في القانون 04/09 :

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات، حيث انه عرف من خلال نص المادة 02 من القانون رقم 09- 04 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .[1]

مسميا إياه " المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مرتبطة ، يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين .

[1] قانون رقم 09- 04 ، المؤرخ في 14 شعبان 1430هـ ، 2009 ، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح ر ع 47 ، صادر بتاريخ 2009/08/16 ، ص5 .

حددت المادة (02) منه الجريمة الالكترونية بقولها: "يقصد في مفهوم هذا القانون بما يأتي:

- **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:**

جـرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قــانون العقوبات وأي جريمة أخــرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصــالات الالكترونية.

- **منظــومة معلومـــاتية:**

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة. يقوم واحد منا أو أكثر بمعالجة آلية للمعطيات تنفيذ لبرنامج معين.

- **معطيات معلوماتية:**

أي عملية عرض للوقـائع أو المعلومات أو المفــاهيم في شكل جــاهز للمعالجة داخـل منظومة معلومــاتية. بمــا في ذلك البرامج المنــاسبة التــي من شأنها جعل منظــومة معلومـــاتية تؤدي وظيفتها. (القــانون 09-04 المؤرخ في 05 أغسطس 2009).

وفقا للمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها ، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات . أما فيما يخص الشرط الثاني لمجلس الشيوخ الفرنسي والمتعلق بضرورة توافر النظام على حماية فنية فيبدو أن النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية النظام المعالجة الآلية للمعطيات الجنائية .[1]

المطلب الثاني: الطبيعة القانونية للجريمة الالكترونية .

من خلال ما تقدم من تعريفات للجريمة الالكترونية في التشريع الجزائري نستنتج موقف المشرع من هذه الجريمة، وهذا الموقف متمثل في أن التقدم التكنولوجي ولانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام، مما دفع الكثير من الدول إلى النص

[1] نشناش مونية ، مرجع سابق ، ص4 .

لمعاقبة هذا النوع من الجرائم، وتسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال وكان ذلك بموجب القانون رقم 04- 15 المؤرخ في 2004/11/10 المتمم والمعدل لأمر 66- 156، المتضمن لقانون العقـــوبات والذي اقر له القسم السابع مكرر منه تحت عنوان، "المساس بأنظمة المعـــالجة الآلية للمعطيـــات" فقد أثار المشرع الجـــزائري استخدامه للمصطلح للدلالة على كلمة المعلـــومات والنظام الذي يحتوي عليها ويخرج بذلك من نطـــاق تجريم تلك الجـــرائم التي يكون النظـام المعلوماتي وسيلة ارتكابها وحصرها فقط في صورة الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها.[1]

وقدر المشرع من خلال هذا التعديل ان جوهر المعلوماتية هي المعطيات التي تدخل الى الحاسوب فتحولها الى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من عدة زوايا ، و بصدور القانون رقم 04/09 السابق الذكر عبر المشرع الجزائري على الجريمة المعلوماتية بتسمية " الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال" .

و ما يلاحظ في هذا الشأن أن المشرع الجزائري لم يستقر على تسمية واحدة ، حيث اعتمد على تسميات مختلفة بين قانون العقوبات و القوانين المكملة في المجال الجنائي فسماها جريمة المساس بأنظمة المعالجة الالية للمعطيات في القانون 15/04 ، في حين اعطاها تسمية الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال في القانون 04/09 و رغم هذا الاختلاف فان هاتين التسميتين و غيرها من التسميات الاخرى تصب في هدف واحد وهو مجابهة الجريمة الالكترونية.[2]

فمن حيث التكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة اذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة ، و تطبيق النصوص التقليدية على الجرائم

[1] سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية ، جامعة الحاج لخضر ، باتنة 2013/2012 ، ص41 .

[2] حمزة عشاش، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، جامعة محمد بوضياف المسيلة، مقال منشور بمجلة الدراسات القانونية و السياسية ، المجلد 06 العدد 02 جوان 2020 تاريخ النشر:05 /06 /2020 ص 172 .

المعلوماتية يثير العديد من المشاكل و التي في مقدمتها صعوبة إيجاد دليل مادي يدين مرتكب الجريمة .

أما عن محل الجريمة المعلوماتية فيتميز عن محل الجريمة التقليدية ، فمحل الجريمة الاولى هو المال المعلوماتي تمييزا لماليته المغايرة للمال التقليدي في الجريمة الثانية بكل مكوناته ، فالجريمة المعلوماتية تشمل كل من أفعال السرقة او التغيير او حذف المعلومات مثل النشاط الجرمي الذي يستهدف اختراق بريد الكتروني و العبث بمحتوياته ، و الذي يحمل في طياته انتهاك الخصوصية و حقوق الملكية الفكرية و أنماط جرمية أخرى.[1]

المطلب الثالث: أركان الجريمة الالكترونية في التشريع الجزائري.

من المتعارف عليه من الناحية القانونية ان الجريمة في القانون هي جريمة الارتكاب المتعمد لفعل ضار من الناحية الاجتماعية او فعل خطير محظور يعاقب عليه القانون ، بينما الجرائم المعلوماتية مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات او أجهزة الكترونية او شبكة الانترنت او تبث عبرها محتوياتها ، بينما الجريمة الالكترونية هي ذلك النوع من الجرائم ، التي تتطلب الإلمام الخاص بتقنيات الحاسب الالي و نظم المعلومات لارتكابها او التحقيق فيها و مقاضاة فاعليها ، وهي اي عمل غير قانوني يستخدم فيه الحاسب كأداة او موضوع الجريمة

و سبق و ان تطرقنا في بداية بحثنا إلى مفهوم الجريمة الالكترونية في التشريعات المقارنة والتشريع الجزائري، و عن الطبيعة القانونية للجريمة الالكترونية وأسمائها، كما تم التطرق إلى خصائص الجريمة الالكترونية ودوافع ارتكابها .

نتناول في هذا المبحث أركان الجريمة الالكترونية الأساسية والمتمثلة في الركن الشرعي المتمثل في النصوص القانونية والركن المادي المتمثل في السلوكيات المادية المجرمة والركن المعنوي المتمثل في القصد الجنائي للجريمة الالكترونية .

الفرع الأول: الركن الشرعي للجريمة الالكترونية

[1] حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، المرجع السابق، ص 173 .

تتحقق الجريمة بالفعل الصادر عن الإنسان فيتخذ صورة مادية معينة . وهذه الأفعال تختلف باختلاف نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتحديد فئة من الأفعال الضارة او الخطرة على سلامة أفراد المجتمع فينهي عنها بموجب نص قانوني يجرم هذه الأفعال ويحدد عقوبة من يأتي على ارتكابها.[1]

القاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية النص الجنائي(الا ماكان اصلح للمتهم " استثناء") يقتضي ذلك لمعاقبة شخص لا بد ان تكون الجريمة قد حددت اركانها بموجب قانون مطبق وقت ارتكابها ولا يجوز معاقبة شخص على فعل كان مباحا وقت ارتكابه ثم صدر قانون يجرمه ، و هـذا ما نصت عليه المـادة الأولى من قانون العقوبات، "لا جريمـة ولا عقوبـة او تدابـير امـن بغـير قانـون".[2]

و يمـيز هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره ضيقا . بالإضافة إلى منع اللجوء إلى القيـاس بمعنى عدم لجوء القـاضي الجنائي إلى قياس فعل لم يـرد نص جريمته على فعل ورد نص تجريمه فيقر القـاضي الجنـائي الأول عقوبة الثـاني للتشابه بين الفعـلين.

إن ظهـور شبكة الانترنـيت أدى إلى تطور ظـاهرة الإجرام بشكل خطيـر في تفشي الجريمة الالكتـرونية وازداد هذا الوضع خطـورة خاصة حين اصـدر المجلس الأوروبي سنة 1989 ، توصية لتشجيـع دول الأعضـاء على تبني نصـوص عقـابية خاصة بجريمة المسـاس بأنظمة المعـالجة الآلية للمعطيـات . وقد اختلفت في اختيار التقنية التشريعية المناسبة ، فمنها من قام بإدماج النصوص العقابية المتعلقة بالإجرام المعلوماتي في قانون العقوبات التقليدي ، ومنها من قام بوضع قانون جنائي مستقل للمعلوماتية يدخل في القانون الجنائي التقني .

تستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بشان الجريمة المعلومـاتية ، فقد بذلت هيئة الأمم المتحدة جهودا كبيـرة إضافة جهود المجلس

[1] أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط18 ، 2019 ، ص64 .

[2] أحسن بوسقيعة ، قانون العقوبات في ضوء الممارسة القضائية ، برتي للنشر ، طبعة جديدة 2015 اص 01 .

الأوروبي لإقناع الدول بوضع تشريعـات للتصدي ومواجهة ومكـافحة الجرائم الالكتـرونية وتعزيز التعـاون الدولي في هـذا المجـال .

وكمثال على تلك التوصية رقم 9 (89) R المتعلقة بالجرائم المرتبطة بالحاسوب الآلـي التي أصدرها المجلس الأوروبي والاتفاقية التي تخص الإجرام المعلـوماتي او السبراني الموقعة في نوفمبر سنة 2001 ببودبست ، ودخلت حيز التنفيذ في جويلية سنة 2004 وصادق عليها بعض أعضاء المجلس الأوروبي بالإضـافة إلى كندا والولايات المتحدة واليـابان وجنوب إفريقيا ، حيث جعل منها وثيقة دولية ملزمة بالنسبة للدول الأطـراف فيها.[1]

واجه المشرع عدة عراقيل عند تنظيمه لمجال الحماية الجنائية من مخاطر الجرائم . أم إخلال بمبدأ الشرعية ؟ والوقوع في التفاسير المخلة بمبادئ القانون الجنائي ؟

وللإجابة عن هذا الإشكال ، ظهر اختلاف المشرعين بين ضرورة وضع نصوص جديدة خاصة بالجرائم الالكترونية وبين تكييف النصوص القديمة مع هذه الجرائم الحديثة وبالخصوص من يقول لا فائدة من تطبيق تشريع خاص بجرائم عادية ترتكب بوسائل و تقنيات متطورة ، البعض الأخر يرى في ذلك إخلالا بالبنيان القانوني حيث أن المشرع يتطلب في الجرائم التقليدية سلوكا محددا وتتحقق مع الركن المادي للجريمة وتختلف عن السلوكيات المطلوبـة في الجرائم الالكترونيـة .

وهنـاك من يقول أن الجـرائم المعلومـاتية ما هي إلا جرائم عادية ترتكب بواسطة الحاسب الآلـي ، فالمطلـوب من المشرع توقيع العقاب على ارتكاب هذه الجرائم بنصوص تقليدية ، وعلى المشرع فقط الإلمـام بمصطلحـات تقنية حتى لا يتم المسـاس بجريمة تبادل المعارف والحفـاظ على الحق في احتـرام الحيـاة الخـاصة .

مما يطرح إشكاليتين أساسيتين هما : إشكالية الموقع وإشكالية المصطلحات .

أولا: إشكـالية المـوقع

[1] معتوق عبد اللطيف ،الاطـار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقـارن، مذكرة لنيل شهادة الماجستير في العلوم القانونيـة ،جامعـة العقيـد الحـاج لخضر ، باتنـة ، السنـة الجامعية 2011 – 2012 ، ص 25 .

أين يمكن إدماج النصـوص القانونية الجديدة في قـانون العقوبـات التقليدية ؟ أم هو قـانون خاص هناك من يقول بإمكانية إدمـاجها في جرائم الأموال باعتبار انه يمكن إضفـاء صفة المال على الكيـانات المادية والمعنوية كالحـاسوب ، والبعض الأخر يفضل إدمـاجها في إطار الجزء الخـاص بالجـرائم ضـد الملكية باعتبـار الكيان المادي للحـاسوب عناصر مـادية قـابلة للتملك كما أن الكيـان المعنوي يدخل في إطار الملكية الفكـرية . وهنـاك من يرى إضـافة جزء خـاص بالجـرائم الالكتـرونية مستقل عن الأجـزاء التقليدية باعتبـار أن هذه الجـرائم تتعلق بقيمة اقتصـادية جديـدة لهـا طـابع خـاص .

هناك اتجاه ثالث يرى إلحاق كل جريمة معلوماتية بما يقابلها في قانون العقوبات التقليدي **مثلا:** وضع جريمة التزوير المعلوماتي في باب المحررات ، الاعتداء على المعطيات يلحق بالإتلاف ....الخ .

ثـانيا: إشكـالية المصطلحـات

نظـرا لما تتميز به الجريمة الالكترونية من طابع تقني ، فإنها تطرح مشكل المصطلحات التقنية نظرا لغموض مفهومها باعتباره مصطلح غريب عن لغـة القانون .

بالنسبة للإشكـالية التي تطرح الركن الشرعي للجريمة الالكترونية، يختلف موقف التشريعات في تحديد تعريف المصطلحات التقنية في الدول الأنجـلوسكسونية التي تعتمد على طريقة إعطاء تعريفـات في صلب القـانون، أما الطريقة الفرنسية توكل مهمة تحـديد المعاني والمصطلحات التقنية للقضـاء، وهي الطريقة المفضلة نظرا لسرعة تطور تقنيـات الإعلام الآلـي وإمكانية القانون الجنـائي مواكبة هـذا التطور .

بدأت المحاولة في فرنسا سنة 1985، حين تقدم وزير العدل بمشروع قانون العقوبات الجديد الذي أضيف إلى كتاب القانون الثالث منه، بابا رابعا بعنوان "جرائم المعلوماتية" مكونا من ثماني مواد 307/01 إلـى 307/08 والتي كـانت تجرم التقاط البرامج والمعطيـات أو عنصر أخر من النظام المعلومـاتي وبدون موافقة من لهم الحق عليه، وتخريب أو تعيب كل أو جزء من نظـام المعالجة الآلية لمعطيـات، وكـذلك عرقلة لأدائه كوظيفة والحصـول أو

السماح [1] بالحصول على فائدة غير مشروعة عن طريق الاستخدام غير المشروع لنظام المعالجة الآلية للمعطيات، ولكن هذا المشروع ظل حبيس الأدراج ولم يرى النور .

وفي 05 أوت 1986، تقدم إلى الجمعية الوطنية الفرنسية النائب Jacque Codfrain مع بعض النواب من أعضاء حزب تجمع من اجل الجمهورية باقتراح مشروع قانون في الغش المعلوماتي، وكان هذا المقترح مجرد تعديل وتطويع بعض الجرائم التقليدية مثل السرقة والنصب وخيانة الأمانة والإخفاء والتخريب والإتلاف والتزوير واستعمال المحررات المزورة .

ولكن عند نظر البرلمان الفرنسي لهذا المقترح، دارت حوله مناقشات طويلة ومعمقة، وأدخلت عليه تعديلات جوهرية و تم إقراره في شكل جديد يختلف عن شكله الأول الذي قدم به، حيث اقترب من الاقتراح الذي سبق الإشارة إليه في مشروع قانون العقوبات لسنة 1985 وكان ذلك في 1987/12/22 وأصبح قانونا منذ 1988/01/05 بشان الغـــش المعلـــوماتي .

وادمج هذا الباب على المواد من 2/462 الى 9/462 ويحرم الدخول او البقاء غير المشروع في نظام المعالجة الآلية للمعطيات او جزء منه ، وشدد عقوبة تلك الجريمة في حالة محو او تعديل المعطيات الموجودة فيه او طرق معالجتها او نقلها، سواء تم ذلك بطريقة مباشرة او غير مباشرة، ويجرم كل من عرقل او افسد عمدا او بدون مراعاة لحقوق الغير أداء النظام لوظيفته، كما يجرم تزوير المستندات آليا أيا كان شكلها، وكذلك استعمال تلك المستندات . ويجرم أخيرا الشروع في ارتكاب الجرائم السابقة وكذلك الاتفاق الجنائي على ارتكابها .[2]

إن المشروع الفرنسي فقد فصل بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات وبين جريمتي تزوير المستندات المعالجة أليا واستعمالها، ويلاحظ على نصوص السابقة كذلك تجريم كل الاعتداءات على نظام المعالجة أليا واستعمالها .

ففي الكتاب الثالث من هذا القانون، "الجنايات والجنح ضد الأموال" وفي القسم الثاني من هذا الكتـاب وفي الاعتداءات الأخرى على الأمـوال، يعالج الباب الأول منه الإخفـاء والجرائم

[1] على عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلـي ، دار الجامعية للطباعة والنشر ، بيروت ، د ط ، 1999 ، ص24 .

[2] علي عبد القادر القهوجي ، مرجع سابق ، ص 24، 35 .

الأخرى المشابهة أو القريبة منه، ويخصص الباب الثاني للإتلاف والتخريب والتغييب . أما الباب الثالث، فقد كرسه المشرع للاعتـداءات على الأنظمة المعالجة الآلية للمعطيــات .

أما جريمتا تزوير المستنــدات المعالجة آليا واستعمالها فقد اختفيا من الباب الثالث المذكور لان المشرع رأى أن المصلحة المحمية فيهما الثقة العامة، وليس نظام المعـالجة الآلية للمعطيات، وإضافة إلى جريمة التزوير العــادية بعد تطوع نصوصها بما يتلاءم وتلك المستنــدات حيث نصت المادة 1/441 قانون العقــوبات الفرنسي الجديد في باب التزوير على تجـريم كل تغيير للحقيقة مكتوب أو محرر أو أي دعـاية أخرى تحتوي على الأفكار . أما بالنسبة للمشرع الجـزائري فقد أورد قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيــات، وهو القسم السابع مكرر بمحتوى المـادة 394 مكرر إلى 394 مكرر 7 بمقتضى القـانون 04- 15 المؤرخ في 2004/11/10، ولم يكتفي المشرع الجزائري بذلك، بل فرض حماية جنـائية للحياة الخاصة للأفراد من خلال قانـون 23/06، المؤرخ في 2006/12/20، والذي مس المادة 303، وإقــراره بالمادة 303 مكرر 03، وهذا تصـديا للاستخدام السيئ لوســائل التكنولوجيا الحــديثة.[1]

الفرع الثاني: الركـــن المـــادي للجريمة الالكترونية

يعتبر الركن المادي للجريمة هو المظهر الخارجي لها و كيانها المادي الظاهر ، و هو الماديات المحسوسة في العالم الخــارجي كما حددتها نصوص التجريم ، فالقاعـــدة انه " لا جريمة دون ركن مادي " او " لا جريمة فعـــل" [2] الا ان الركن المادي للجريمة المعلوماتية يختلف نوعا ما عن الجرائم التقليدية كون انه يقوم على صور في فعل الاعتداء .

إن الركن المادي للجريمة الالكترونية يقوم على صورتين أساسيتين، الصورة الأولى و المتمثلة في الاعتداء على نظام المعالجة الآلية، وهذه الأخيرة تحتوي على نوعين من الاعتداء.

النوع الأول: وهو الدخـــول و البقـــاء غير المشروع في نظام المعالجة الآلية للمعطيات او الشروع في ذلك وتنطوي تحت هذا النوع ثلاثة أفعال، فعل الدخول و البقاء، فعل العرقلة أو

[1] على عبد القادر القهوجي ، مرجع سابق ، ص 35 .

[2] عبد الرحمان خلفي ، محاضرات في القانون الجنائي العام، دار الهدى للنشر ة الطباعة و التوزيع، الجزائر، ص 101

التأخير . أما **النوع الثاني:** متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال، وهي فعل الإدخـــال، المحـــو، التعديـــل . أما الصورة الثانية فهي متمثلة في الاعتداء على منتجات الإعلام الآلي، و تحتوي هذه الصورة على أفعـــال التزوير المعلوماتي . ومن خلال ما تقدم سندرس هذا الفرع على هذا المنـــــــوال.

أولا: الاعتداءات على أنظمة تشغيل المعطيات

سنتطرق أولا إلى دراسة الدخول و البقاء غير المشروع في نظام المعالجة الآلية، ثم نتطرق ثانيا إلى الاعتداء العمدي على نظام المعالجة الآلية.

1/الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

نصت المادة 394 مكرر من قانون العقوبات الجزائري على انه، " يعاقب بالحبس من ثلاث (3) أشهر إلى سنة واحدة، وبغرامة مالية من 50.000دج إلى 10.000دج لكل من يدخل أو يبقى عن طريق الغش في جزء أو كل المنظومة المعالجة الآلية للمعطيات، أو يحاول ذلك".

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة بالحبس من ستة (6) أشهر إلى سنتين (2) و الغرامة من 50.000دج إلى 300.000 دج. [1]

نصت المادة 1/323 من قانون العقوبات الفرنسي على انه، " فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، أو جزء منه، يعاقب بالحبس لمدة سنة كاملة، وغرامة مالية تقدر بـ 100.000 فرنك فرنسي . فإذا نتج عن الدخول في النظام تغير أو حذف فان العقوبة تتضاعف لتصير عقوبة بالسجن لمدة سنتين وغرامة مالية تقدر بـ 200.000 فرنك فرنسي .[2]

ونستخلص من النصين وجود صورتين لفعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، الصورة الأولى تتمثل في الصورة البسيطة، وهي مجرد الدخول أو

[1] أحسن بوسقيعة ، قانون العقوبات في ضوء الممارسة القضائية ، مرجع سابق، ص 212 – 213

[2] المـــــادة 1/323 قانون رقم 97– 1159، المؤرخ في 1997/12/19 المتضمن قانون العقـــــوبات الفرنسي

البقاء غير المشرع في النظام، أما الصورة الثانية فهي صورة متشددة تتحقق بتوفر الظروف التالية:

أ/ حذف أو تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروعين.

ب/ تخريب نظام تشغيل المنظومة بعد الدخول أو البقاء غير المشروعين.[1]

1/الصورة البسيطة:

يتمثل النشاط الإجرامي في هذه الصورة في الأفعال التالية:

أ/ فعـــــل الدخـــــول: يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبها، لان هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين، أو يسمح ولكن مقابل نفقات.[2]

أما بالنسبة للتشريعات المختلفة فقد تباين موقفها تجاه تحديد محل الركن المادي في جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات وبذلك يمكن أن نميز ثلاث صور المحل لهذه الجريمة وهي: الصورة الأولى والمتمثلة في ذاتها، والثانية تتمثل في أنظمة المعالجة الآلية للمعطيات التي لا ترتبط فيما بينها من خلال شبكة الاتصال، والثالثة هي شبكة المعلومات. فهذا التباين والاختلاف حول محل الركن المادي لهذه الجريمة أورد ثلاثة اتجاهات وهي:

الاتجـاه المـوسع: يجمع بين الصور الثلاث ويتخذها جميعا كمحل الجريمة وهي المعلومات الواسعة للمعالجة الآلية وشبكات المعلومات. وتبني هذا الاتجاه المشرع الفرنسي واقتدى به. نفس الأمر بالنسبة للمشرع الجزائري.

الاتـــجاه الثـــاني: استبعد شبكات المعلـــومات من نطاق التجريم، ويتبنى هذا الاتجـاه المشرع الانجليـــزي.

الاتـــجاه الثـــالث: جرم فعل الدخول عبر شبكات المعلومات وهذا التشريع ســـويسري.[3]

---

[1] نـــائلة فريد عادل محمد قورة، جـرائم الحاسب الآلـي الاقتصادية، منشـورات الحلبي الحقوقية، ط1، 2005، ص 223.

[2] نائلة فريد عادل محمد قورة، نفس المرجع، ص 323.

[3] نائلة فريد عادل محمد قورة، نفس المرجع، ص 322،323.

إن جريمة الدخول غير المصرحة إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة، ويكفي الوصول إلى المعلومات المخزنة بداخل النظام . فبمجرد الوصول إليها تقوم الجريمة.[1]

يرتكب فعل الدخول بأية طريقة أو وسيلة كانت لان المشرع الجزائري لم يحددها.[2]

ويستوي أن يتم الدخول بطريق مباشر يستطيع الجاني الوصول للمعلومات المخزنة لدى أنظمة المعالجة الآليـــة باستخدام الشاشة النظام والاطلاع بالقراءة على ما هو مكتوب عليه باستخدام آلة الطابعة المرفقة بجهاز الحاسب الآلـــي استخراج البرامج الموجودة داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالالتقاط المعلوماتي بعد التقاط المعلومات المتواجدة في الحاسب الآلي والنهاية الطرفية والتقاط الإشعاعات الكهرومغناطيسية المنبعثة من الجهاز المعلوماتي. [3]

ب/ البقـــــــــــــــاء:

معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام،ويتحقق هذا البقاء غير المشروع عند دخول شخص في نظام بتصريح ولكن تجاوز الفترة المدة المسموح له البقاء بها، أو يكون ذلك عن طريق الخطأ أو السهو في نظام آخر ولم ينسحب على فوره ولا قطع وجوده، أو يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة آليا للمعطيات.

يجتمع فعل البقاء مع فعل الدخـول غير المشـروع إلى نظام المعـالجة الآلية للمعطيـات مثل إلا يكون للجـاني حق الدخـول ويدخل عن طريق الغش ويبقى عند ذلك، حيث نصت المـادة 394 مكرر من قانون العقوبـات الجزائري على فعل البقاء غير المشـروع، على غرار القانون الفرنسي في المـادة 1/323

[1] نائلة فريد عادل محمد قورة، نفس المرجع، ص 324.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط2، 2007، ص 100.

[3] نائلة فريد عادل محمد قورة، مرجع سابق، ص 324،327.

من قـــانون العقوبات الفرنسي يصعب تطبيق النص في قـراءته الأولى لأنه ينص فقـط على الدخـــول غير مرفق إدراج الجزء الخـاص بالبقاء غير المشـــروع وصيـاغة النص أصبح يمكن تطبيـقه.[1]

جرمت محكمة الاستئناف في بـــاريس في حكمها في 1994/04/05 البقـاء الغير مشروع سواء تم عن طريق الخطأ أو بطريقة مشـروعة داخل نظـام المعالجة الآلية للمعطيـات، إلا انه اكتسب بعد ذلك صفة عدم المشـــروعية نظرا لاختلاف الطبيعة القـــانونية بين فعل الدخول غير المصرح به والبقاء غير المشروع وكذا يمكن وضعها في نص قانوني واحد حيث يعد فعل الدخول غير المصرح به والبقاء غير مشروع، لذا يمكن البقاء بعد جريمة سلبية ومستمرة.[2]

2/الصـــــورة المشـــــــددة:

نصت المادة 394 مكرر فقرة 2 و 3 من قانون العقوبات الجزائري على ظروف تشديد عقوبة فعل الدخول و البقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل للمعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائف نتيجـــة التخريـــب.

إن ظرف تشديد ظرف مادي تربط بينه و بين الجريمة العمدية الأساسية علاقة سببية لكي نقول أن الشرط متوفر ، و في المادة 394 مكرر من الفقرة الأخيرة شدد المشرع عقوبة محو وتعديل المعطيات كل واحد على حدى وتخريب نظام اشتغال المنظومة من جهة أخرى، وعقوبة هذه الأخيرة اشد لان عقوبة المحو أو التغيير هي ضعف عقوبة الدخول والبقاء غير المشروعين. أما بالنسبة للمشرع الفرنسي فجمع بين طرفين في فقرة واحدة في المادة 1/323 من قانون العقوبات الفرنسي.[3]

ثانيـــا: الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات .

[1] أمال قارة، مرجع سابق، ص 110.

[2] نائلة فريد عادل محمد قورة، مرجع سابق، ص 348 .

[3] أمال قارة، مرجع سابق، ص 113 .

نصت على هذه الصورة المادتان 5 و 8 من الاتفاقية الدولية للإجرام المعلوماتي، والمادة 2/323 من قانون العقوبات الفرنسي، والتي نصت على انه، "بمجرد إعاقة أو إفساد اشتغال نظام المعالجة الآلية للمعطيات". أما بالنسبة للمشرع الجزائري لم يرد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة داخل النظام. وهذا راجع إلى تفسير أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام و وظائفه واختلف الفقه في الرأي حول ما إذا كان الاعتداء وسيلة أم غاية ؟

فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فان الفعل يشكل جريمة اعتداء عمدي على المعطيات، ومع عدم وجود نص خاص بالاعتداءات العمدية على نظام المعالجة الآلية للمعطيات، فان الاعتداء على سير النظام النـــاجمة عن الدخول المشروع للنظام تفلت من العقــاب، وتتمثل السلوكيــات الإجرامية في هذه الاعتداءات في فعل عرقلة أو تعطـيل وإفساد لنظـــام معالجة آلية للمعطيـــات عن أداء نشـاطه العــادي و المنتظم منه القيام به.[1]

1/ التعطيـــــــــل (العرقلة):

إن المشرع لم يشترط الوسيلة التي يتم بها فعل التعطـيل قد تكون وسيلة مادية أو معنــوية سواء اقترنت الوسيلة المــادية بعنف أم كسر الأجهزة المــادية للنظام أو تحطيم الاسطوانة، وتكــون معنوية إذا وقعت على الكيـانـات المنطقية للنظام مثل البرامج والمعطيــات بإتباع التقنيات التــالية:

كإدخال برنامج فيــروسي، استخــدام قنابـــل منطقية تجعـل النظام يتباطأ في أداءه للوظــائف إلى غيرها من التقنيـــات.

2 / الإفســـــــــــاد:

يقصد بفعل الإفساد وهو كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.[2]

ثالثا: الاعتداءات العمدية على نظام المعالجة الآلية المعطيات.

---

[1] أمال قارة، مرجع سابق، ص 113.

[2] على عبد القادر القهوجي، مرجع سابق، ص 7،49.

نصت على الاعتداءات العمدية على المعطيات المواد 3،4،8 من الاتفاقية الدولية للإجرام المعلوماتي. كذلك المادة 323 من قانون العقوبات الفرنسي بنصها، "كل من ادخل بطرق الغش المعطيات بنظام المعالجة الآلية للمعطيات أو محا أو عدل" ونصت على الاعتداءات تلك المعطيات بعقوبة الحبس تصل إلى 03 سنوات وبغرامة مالية تقدر بـ 300 ألف فرنك فرنسي.[1]

بالإضافة إلى ذلك، نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري على الاعتداءات العمدية بنصها، "يعاقب بالحبس مدة شهرين (2) إلى ثلاثة سنوات (3) وبغرامة مالية تقدر بـ 100.000.0دج إلى 500.000.0دج كل من يقوم عمدا او عن طريق الغش بما يلي:

- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة او إفشاء أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.[2]

الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة.

تتجسد هذه الاعتداءات العمدية على المعطيات في ثلاث أفعال: الإدخال والمحو والتعديل ، ولتوافر الركن المادي في هذه الجريمة لابد من توافر الأفعال الثلاثة ولا يشترط اجتماع هذه الأفعال، ويكفي أن يصدر من الجاني إحدى هذه الأفعال لتوافر الركن المادي.

1/ الإدخـــال: يقصد بفعل الإدخال هو إضافة معطيات جديدة على الدعـاية الخـاصة سواء كانت خـالية، أم كان يوجد عليها معطيــات من قبل، ونكون أمام فعل الإدخــال في حـالة الاستخدام التعسفي لبطاقـات السحب والائتمان سواء من صـــاحبها الشرعي او عن غيره كحـــالة السرقة او التـــزوير.[3]

---

[1] المادة 323 من قانون العقوبات الفرنسي، رقم 97ـــــــ1195، المرجع السابق

[2] مولود ديدان، قانون العقوبات، المرجع السابق، ص 121.

[3] أمال قارة، مرجع سابق، ص 120، 121.

2/ المحـــــــــــو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة داخل النظام، وتحطيم تلك الدعامة او نقل او تخزين جزء من المعطيات في ذاكرة مختلفة.

3/ فعل التعـــديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى يتحقق ذلك عن طريق برامج تتلاعب في المعطيات سواء بالمحو الكلي او الجزئي، وهي برامج الفيروسات وهي مختلفة الأنواع والإشكال.[1]

الصورة الثانية: المســـــاس العمـــدي بالمعطيـــات خـــارج النظـــام.

نص المشرع الجزائري على صورتين للمساس بالمعطيات خارج النظام، الصورة الأولى وتتعلق بحماية المعطيات من استعمالها في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، والثانية تتعلق بحماية المعطيات المتحصل عليها من هذه الاعتداءات، وذلك في نص المادة 394 مكرر 2 من قانون العقوبات المشار إليه سابقا.[2]

و يتضح من خلال النص ان هناك فرق بين الصورتين المنصوص عليهما في المادة 394 مكرر 2 من قانون العقوبات حيث ان الصورة الأولى تكون فيها المعطيات وسيلة للارتكاب هذه الاعتداءات، فالحماية التشريعية هنا تخصها قبل ارتكاب الاعتداءات أما صورة الثانية فتكون المعطيات هي المحصلة او نتيجة لارتكاب الاعتداءات الماسة بالأنظمة والحماية التشريعية في هذه الصورة تهدف الى الوقاية من ارتكاب جريمة أخرى، تتمثل في حيازة او إفشاء أو نشر او استعمال هذه المعطيات المتحصل عليها من إحدى هذه الاعتداءات لأي غرض كان. [3]

رابعا: الاعتداءات على منتجات الإعـلام الآلـي- التزوير المعلوماتي.

إن الاعتداءات على منتجات الإعـلام الآلـي هي الفعل الثاني لتحقق الركن المـادي من الجريمة الالكترونية، فيعد هذا الفعـل من اخطر صور الغش المعلومـاتي نظرا لما يتمتع به الحـاسب الآلـي من خطـورة.

---

[1] لمعيني محمد، محاضرات ألقيت على طلبة ثانية ماستر، جنائي، 2016/2015.

[2] نائلة فريد عادل محمد قورة، مرجع سابق، ص 366.

[3] نـائلة فريد عـادل محمد قورة، مرجع سـابق، ص 367.

و تجـــــدر الإشارة إلى ان المشرع الجزائري اقتدى بالمشرع الفرنسي الذي اخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير لكن هناك فرق بين نصوص قانون العقوبات الجزائري وقانون العقوبات الفرنسي حيث ان نصوص العقوبات الجزائري الخاصة بالتزوير الذي يرد على محرر لذلك لا يمكن الاقتـــــداء بالمشرع الفرنسي الذي يجعل موضوع التزوير عامة ماديـــــة ولهذا الاختلاف لابد من تعديـــــل نصوص الـــــتزوير التقليدية او إدراج نـــــص خـــــاص بالتزويـــــر المعلومـــــاتي في قانون العقوبات الجزائري.[1]

3- 1/ مفهوم منتجات الإعلام الآلي:

قبل التطرق الى مفهوم المنتجات، لابد من توضيح معنى المستند المعالج أليا والمستند المعلوماتي، فالمستند المعالج أليا في الاصطلاح القانوني هو الدعاية المادية التي تم تحويل المعطيات المسجلة عليه لغة الآلة.

أما بالنسبة للمستند المعلوماتي، تعتبر مستندات معلوماتية وهي أوراق معدة لتسيطر المعلومات على الأقراص الممغنطة التي لم يسجل عليها أي شيء بعد.

2/ مدى خضوع منتجات الإعلام الآلي لنصوص التزوير:

هل يمكن تطبيق نصوص التزوير في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتجات الإعـــــلام الآلي؟ و للإجـــــابة على هذا الإشكال لابد من التطرق إلى ما يلي:

- مدى انطباق وصف المحرر على منتجات الإعلام الآلي:

ان مفهوم المحرر في النصوص التقليدية يختلف عن مفهومه في مجال المعالجة الآلية للبيانات لأنه يشترط ان يكون شكلا كتابيا وان يكون منسوبا لشخص معين وان يحدث المحرر آثار قانونية، فلذلك لا يمكن إسقاط معنى المحرر التقليدي على المحرر في مجال المعالجة وذلك لعدم توفر شرط الكتابة، فجريمة التزوير عنصر قيامها الكتابة فأي تغيير في الوعاء المعلوماتي لا يعتبر تزوير لاستيفاء هذا الشرط.[2]

[1] أمـــال قارة، مرجع ســـابق، ص 133، 134.

[2] أمال قارة، مرجع سابق، ص 133- 137 .

ومن بين التشريعات الحديثة التي واجهت القصور في النصوص التقليدية التي استحلت نصوص تجريمية جديدة او تعديلات على نصوص تقليدية من اجل المعاقبة على جريمة التزوير الواقعة على المستندات المعلوماتية هو التشريع الفرنسي الذي استحدث نصا خاصا بالتزوير المعلوماتي، وهو المادة 21462 من قانون العقوبات وذلك بموجب تعديل سنة 1988 غير أنه بموجب تعديل 1994 تراجع المشرع الفرنسي عن موقفه والغى النص الخاص بالتزوير المعلوماتي وأخضعه لنصوص التزوير التقليدية.

أما من بين التشريعات التقليدية نجد التشريع الجزائري، حيث أدرج النصوص الخاص بتزوير المحررات في المادة من 214 الى 229 من قانون العقوبات التي تشترط المحرر لتطبيق جريمة التزوير.

- مدى خضوع منتجـــات الإعلام الآلي للنشـــاط الإجـرامي لجريمة التزويـر:

تقوم جريمة التزوير على فعل تغيير الحقيقة القانونية السببية وليست الحقيقية الواقعة المطلقة بمعنى استبدالها بما يخالفها وإذا انتفى هذا التغيير، انتفى التزوير معه، ويقع فعل التغيير الحقيقة من خلال طرق التزوير المادية والمعنوية.

ونستخلص من كل هذا إلى ان المشرع الجزائري رغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديثة.[1]

الفرع الثالث: الركن المعنوي للجريمة الالكترونية

الركن المعنوي للجريمة الالكترونية يختلف باختلاف أشكالها، وعليه ارتأينا التعرض للركن المعنوي لكل جريمة على حدة.

أولا: جريمـــة الدخـــول والبقـــاء غير المشروع داخل نظام المعـالجة الآلية للمعطيـــات.

[1] أمال قارة، مرجع سابق، ص 139، 140.

ان جريمة الدخول غير المشروع هي جريمة عمدية تتطلب قصدا جنائيا وذلك بنص المادة 394 مكرر من قانون العقوبات الجزائري التي عبرت عن المقصد الجنائي بنصها، "كل من يدخل او يبقى عن طريق الغش". وتعني هذه العبارة ان الفاعل له كامل العلن بان الدخول والبقاء غير مشروع، كما تطرق له المشرع الفرنسي في نص المادة 323/01 بعبارة Frauduleusement ".

ولتوفير القصد الجنائي لابد أن يكون الجاني محيطا علما بكافة عناصر الجريمة وله علم بان الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات برامج، وباعتبار محل الحق الذي يحميه المشرع.[1]

بمعنى أخر انه اتجاه إرادة الجاني اتجهت إلى فعل الدخول او فعل البقاء، وان الجاني يعلم بان ليس له الحق في الدخول الى النظام والبقاء فيه، ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله او بقـــاءه داخل النظام مسموح به أي مشروع، وان كـــان الجاني يجهل بوجود حظر الدخول او البقـــاء.[2]

فإذا اعتقد الفاعل بناءا على أسباب معقولة بأنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلـــي دون ان يتجه علمه إلى انه يقوم بالدخول او البقاء في نظام المعالجة الآلية للمعطيات، فان قصد الدخول او البقاء لا يتوفر فيه.[3]

أما بالنسبة لنية الغش تبدو من خلال الغش الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام. بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام، وفي الحقيقة ان الدخول والبقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، وإنما يظهر من خلال الولوج دون وجه حق إلى النظام، وان الدخول للنظام غير مرخص به.[4]

ثانيا: جريمة الاعتداءات على سير نظام المعالجة الآلية للمعطيات.

---

[1] نائلة فريد عادل محمد قورة، مرجع سابق، ص 366.

[2] أمال قارة، مرجع سابق، ص 124.

[3] نائلة فريد عادل محمد قورة، مرجع سابق، ص 366.

[4] أمال قارة، مرجع سابق، ص 124.

إن جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لان أفعال العرقلة والتعطيل من الأفعال العمدية و هذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يعتبر ظرف مشددا لجريمة الدخول والبقاء غير المشروع للنظام، وعليه فالقصد الجنائي المفترض ينتج من طبيعة الأفعال المجرمة.

ثالثا: الاعتداءات العمدية على المعطيات.

إن جريمة الاعتداء العمدي على المعطيات هي جريمة عمدية يتخذ فيها القصد الجنائي بعنصرية العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بان نشاطه الإجرامي يترتب عليه التلاعب بالمعطيات، ويعلم أيضا انه ليس له الحق في القيام بذلك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.[1]

ويشترط لتوافر الركن المعنوي بالإضافة الى القصد الجنائي العام نية الغش، هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو تعديل مع العلم بذلك واتجاه الارادة اليه، وان كان الضرر قد يتحقق في الواقع نتيجة للنشاط الاجرامي الا انه ليس عنصرا في الجريمة.

رابعا: استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية.

ان هذا الاستخدام يكون عمديا وذلك باستخدام متمثل في التصميم او البحث او التجميع او التوفير او النشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية، ويكون هذا الاستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام اضافة القصد الجنائي الخاص والمتمثل في النية.[2]

وفي ظل عصر السرعة والثورة المعلوماتية لا يستطيع احد أن ينكر أهمية الانترنت لأنها احد أهم دعائم تكنولوجيا الاتصال والمعلومات، و لكن هناك على الجانب الآخر أثار سلبية من أهمها ظهور نوع جديد من الجرائم الالكترونية،ونتيجة لهذا فقد كانت هناك التشريعات المقارنة

[1] نفس المرجع، ص 125، 126.

[2] أمـــال قارة، مرجع سابق، ص 126.

التي عرفت الجريمة الالكترونية وبينت كيفية التصدي الى هذا الشبح، وكذلك المشرع الجزائري الذي عرفها كذلك وبين سماتها ونطاقها وطبيعتها، وهذه الجريمة كأي جريمة أخرى لها أركان تقوم بقيامها وتزول بزوالها وفي هذا الفصل تناولنا مفهوم الجريمة الالكترونية في التشريعات المقارنة كما تطرقنا كذلك الى الجريمة الالكترونية في التشريع الجزائري وكذا تناولنا أركانها المتعارف عليها والمتمثل في الركن الشرعي والركن المادي والركن المعنوي و إضافة الى ذلك تحدثنا عن الركن المفترض لهذه الجريمة.

وفي نهاية هذا الفصل، يتضح لنا أن الجريمة الالكترونية هي جريمة وليدة التطور العلمي والتكنـولوجي الذي وصلت إليه المجتمعـات، فبرغم من الايجابيـات التي تطغى على هذا التقدم إلا أن الجانب السلبي له والذي يستعمل في أغراض سلبية يعرف انتشـار كبيرا خاصة في أوساط الجيل الصـاعد، فلمرتكبي هـذا النوع من الجرائم أو ما يعرفون بالمجرمين المعلومـاتيين لهم قدرة كبيرة على تكيف بالمجتمعـات الأخرى وكذا يتميزون بالذكـاء والفطنة وهي اكبر مقومات ارتكـاب هـذا النـوع من الجـرائم.

كما أن صعوبة التي تحيط بالجريمة الالكترونية من حيث سرعة اكتشافها وكذا صعوبة إثباتها شكل اكبر عوائق التي توجهنا في مكافحة هذا النوع من الجرائم.

الفصل الثاني

الجريمة الالكترونية بين المعالجة و المعوقات

عرفـــت الجزائر تطورات و تغيرات في العديد من المجالات الحياتية على غرار دول العالم نتيجة لما أفرزته ثورة المعلومات ، حيث صارت تكنولوجيا الإعلام و الاتصال تفرض نفسها على عادات وسلوكيات الأفراد ، مما حتم على المشرع الجزائري القيام بإعادة النظر في المنظومة التشريعية لمواجهة الأنماط الجديدة من الإجرام، و على الرغم من أن المشرع الجزائري قد استحدث نصوصا تهيأ لما سترفضه البيئة الالكترونية من تحديات تتعلق أساس بمدى قدرة السلطات على مسايرة هذه التطورات المتلاحقة، إلا ان طرحه لهذه النصوص جاء بصفة غير منتظمة و غير متوازنة، فقد اصدر القانون رقم 04-15 الخاص بجرائم المساس بأنظمة المعالجة الآلية للمعطيات في 10 نوفمبر 2004 [1] لينتظر حتى سنة 2009 ليصدر القانون رقم 09-04 الذي نص على القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها [2]، على الرغم من تناول هذا القانون الأخير لشرح مصطلحات وردت في القانون السابق استدراكا لذلك، كما انه اصدر القانون رقم 10-05 المتعلق بالإثبات بالكتابة الالكترونية [3] المعدل للقانون المدني في المادتين 323 مكرر 1 والمادة 327 الصادر بتاريخ 20 جوان 2005 الا انه لم ينظم التجارة الالكترونية على غرار المشرع التونسي كما انه لم يضع أحكامها توضح كيفية إثبـــــات هوية الموقع الكترونيا مما يحتم على المشرع الجزائري تدارك هذا الفراغ التشريعي.

و لو أن المشرع الجزائري قد استدرك جوانبـــا من التشريع في مجال الجريمة الالكترونية و اغفل أخرى، إلا أن هذا لا يمنعنا من القول ان التشريع الجزائري قد خطى خطوات عملاقة لمواكبة التشريعات الدولية بهذا الصدد.

---

[1] القانون رقم 04-15 المؤرخ في: 10نوفمبر 2004 المعدل والمتمم للامر 156/66 المتضمن الجرائم المساس بأنظمة المعالجة الآلية للمعطيات ،ج،ر عدد 71، ص 11-12.

[2] القانون رقم 09-04 مؤرخ في:5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، ج،ر عدد 47، ص 5.

[3] المواد 44-46 من القانون رقم 05-10 مؤرخ في: 20 جوان 2005 المعدل والمتمم لامر 75-58 المؤرخ في:26 سبتمبر 1997 المتضمن القانون المدني ،ج،ر عدد 44، ص17.

سنحاول في هذا الفصل تناول أهم ما جاء به المشرع الجزائري من قواعد إجرائية وموضوعية لغرض التصدي للجريمة الالكترونية،و الى الصعوبات التي تعترض سبل مكافحتها ، حيث نتناول في المبحث الأول معالجة الجريمة الالكترونية في التشريع الجزائري ، حيث نستعرض أهم ما نص عليه القانون المتعلق بالمساس بنظام المعالجة الآلية للمعطيات وكذا القانون المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال تحت ما يسمى بتجريم الأعمال الالكترونية ثم نتناول قواعد الاختصاص و الإجراءات الخاصة بمتابعة الجريمة الالكترونية و الآليات المختصة في مكافحتها ، على أن نتطرق في المبحث الثاني الى الصعوبات التي تعترض سبل مكافحة الجريمة الالكترونية لا سيما تلك المتعلقة باكتشافها و إثباتها او تلك المتعلقة بالاختصاص و القانون الواجب التطبيق مع تبيين أهم الصعوبات التي تواجه المحققين خلال مراحل البحث عن الأدلة الجنائية في هذا النوع من الجرائم.

المبحث الاول: معالجة الجريمة الالكترونية في التشريع الجزائري

إن التطور المذهل و المتسارع و المتلاحق لتكنولوجيا المعلومات و شبكات المعلومات أدى الى ظهور نمط جديد و هو الجريمة الالكترونية بفضل توفر الوسائل التقنية ، حيث ساهمت شبكات الاتصال المتعددة في عولمة الجريمة الالكترونية و تنوعت الأنشطة الإجرامية فيها ، مما حتم تنوعا في ملاحقتها و متابعتها ابتداء من تجريمها و بيان إجراءات ملاحقتها وكذا الأجهزة المختصة في الوقاية منها على المستوى الإقليمي و الدولي.

المطلب الاول : تجريم الأعمال الالكترونية

إن معظم التشريعات جرمت الأعمال الالكترونية و لكنها تباينت و اختلفت اختلافا كبيرا و ذلك راجع أساسا الى اختلاف المستوى الرقمي و التكنولوجي للدول المتقدمة و المشرع الجزائري كغيره من التشريعات في العالم تدخل عن طريق سن نصوص واليات قانونية عملية لاحتواء الظاهرة و التصدي لها تماشيا مع متطلبات المنظومة الدولية و التزاماتها المنبثقة عن مصادقتها على عديد الاتفاقيات المتعلقة بالجريمة الالكترونية.

الفرع الاول: تجريم الأعمال الالكترونية في التشريع الجزائي الجزائري

أولا/ في قانون العقوبات الجزائري.

لقد تطرق المشرع الجزائري الى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثرها بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم يشهدها العالم في قبل مما دفع المشرع الجزائري الى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 2004/11/10 المتمم لامر رقم 66-156 والمتضمن قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات ". و يتضمن هذا القسم ثمانية مواد من المادة 394 مكرر الى 394 مكرر 7 [1]، و نصت هذه المواد على ما يـــــــلي:

نصت المادة 394 مكرر على جريمة الدخول والبقاء عن طريق الغش في كل او جزء من منظومة المعالجة الآلية للمعطيـــات محاولة ذلك بنصها، يعاقب بالسجن من ثـلاثة أشهر الى سنة وغرامة مـــالية تقدر بـ : 50.000دج الى 100.000دج لكل من يدخل او يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات او يحاول ذلك.

تضاعف العقوبة اذا ترتب على ذلك حذف او تغيير معطيات المنظومة، واذا ترتب على الافعال المذكورة اعلاه تخريب نظام الاشتغال تكون العقوبة الحبس لمدة ستة اشهر الى سنتين وبغرامة مالية تقدر بـ : 50.000دج الى 150.000دج.

نصت المادة 394 مكرر 1 على إدخال أو إزالة او تعديل في نظام المعالجة الآلية بنصها، " يعاقب بالسجن لمدة ستة اشهر الى ثلاث سنوات وبغرامة مالية تقدر بـ 200.000دج الى 500.000دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية او ازال او عدل المعطيات التي يحتويها النظام".

نصت المادة 394 مكرر 2 على أن يعاقب بالسجن من شهرين الى ثلاث سنوات وبغرامة من 100.000.00دج الى 500.000.00دج لكل من يقوم عمدا او عن طريق الغش بما ياتي:

[1] ماشوش مراد، مكافحة الجرائم في التشريع الجزائري، مذكرو مقدمة لنيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، سنة 2014/2013، ص 71.

1- تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم.[1]

2- حيازة أو إفشاء أو نشر أو استعمال لاي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

نصت المادة 394 مكرر 3 على انه، "تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني او الهيئـــات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبـــات اشـــــــد".

نصت المادة 394 مكرر 4 على انه، "يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي".

نصت المادة 394 مكرر 5 على فعل اشتراك في جريمة او اكثر من الجرائم المنصوص عليها في هذا القسم، فان لم يعاقب بنفس العقوبة المقررة للجريمة في حد ذاتها وذلك بنصها، " كل من شارك في مجموعة او اتفاق بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل او عدة افعال مادية، يعاقب بالعقوبات المقررة لجريمة ذاتها.

نصت المادة 394 مكرر 6 على انه، "مع الاحتفاظ بحقوق الغير بحسن نية بحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

نصت المادة 394 مكرر 7 على انه، "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".[2]

---

[1] مولود ديدان، قانون العقوبات، مرجع سابق، ص 120، 121.

[2] مولود ديدان، قانون العقوبات، مرجع سابق، ص 120،121.

في عـــــام 2006 ادخل المشرع الجزائري تعديل أخر على قانون العقوبات بموجب قانون رقم 06-23 المؤرخ في:2006/12/20، حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبات المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون 04-15، وربما يرجع سبب هذا التعديل الى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الاولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار والمستويات التعليمية نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل المعلومات حيث بلـــــغ عدد مستخـــدمي الانترنت ذات التدفـــق العالي وعـــبر الهاتف المحمـــول 11 مليون شخص سنة 2012.[1]

نجد المشرع الجزائري اخذ نفس منوال المشرع الفرنسي، الفرق نجد ان المشرع الجزائري لم يتطرق الى جريمة استعمال المستندات المعلوماتية المـــزورة بخلاف المشرع الفرنسي الذي نص على هذه الجريمة في المادة 6/462 من قانون العقوبات الفرنسي.

ثانيـــا/ في قانون الإجراءات الجزائية.

إن الإجراءات الالكترونية تمت متابعتها بنفس الإجراءات التي تبعت بها الجريمة التقليدية كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة التي يتم التطرق اليها في مرحلة الاستدلالات.

الفرع الثاني: القوانين التي نصت على الجريمة الالكترونية في الجزائر.

1/ الدستور الجزائري.

نصت المادة 38 منه على القانون يحمي حقوق المؤلف ولا يجوز حجز اي مطبوع او تسجيل او أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي.

نصت المادة 39 منه على انه لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه ويحميها القانون، "سرية المراسلات والاتصالات الخاصة بشكل مضمون".[2]

[1] ماشوش مراد، مرجع سابق، ص 72.

[2] مولود ديدان، الدستور، التعديل نوفمبر 2008، دار بلقيس الجزائر، ص 16.

2/ القوانـــــــــــــــين.

قانون رقم 2000-03 المؤرخ في: 2000/08/05 والذي يحدد القواعد العامة بالبريد والمواصلات السلكية واللاسلكية.

تسارع هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهل بمكان اجراء التحويلات المالية عن الطريق الالكتروني، ذلك ما نصت عليه المادة 87 من هذا القانون بالقول، "يمكن ان ترسل الاموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد او البرقية او عبر الطريق الالكتروني.[1]

نصت المادة 2/84 منه بقولها،"تطبق احكام المادة 89 من هذا القانون عن طريق استعمال حوالات دفع عادية او الكترونية او برقية".[2]

رتبت المادة 127 منه جزاء كل من تسول له نفسه وبحكم مهنته ان يفتح او يحول او يخرب البريد او ينتهك حرية المراسلات بنصها، "كل موظف او عون من اعوان الدولة او مستخدم او مندوب عن مصلحة البريد يقوم باختلاس او اتلاف رسائل مسلمة الى البريد او يسهل فضها او اختلاسها او اتلافها يعاقب بالسجن من ثلاث اشهر الى خمس سنوات وبغرامة مالية تقدر بـ 30.000دج الى 500.000دج، ويعاقب بالعقوبة نفسها كل مستخدم او مندوب في مصلحة البرق او يختلس او يتلف برقية او يذيع محتواها، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف والخدمات العمومية من خمس الى عشر سنوات.[3]

قانون رقم 01/08 المؤرخ في 2008/01/23 والمتعلق بالتامينات.

المادة 6 مكرر 1 نصت على ان البطاقة الالكترونية تسلم للمؤمن له اجتماعيا مجانا من طرف هيئات الضمان الاجتماعي وهي صالحة في كل التراب الوطني وتقدم لكل مقدم علاج او

---

[1] المادة 87: قانون رقم 2000-03 المؤرخ في: 2000/08/05، والذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية والمواصلات.

[2] المـــــادة 2/84، نفس المرجع.

[3] المـــــادة 127: قانون رقم 2000-03 المؤرخ في: 2000/08/05، والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات، السلكية واللاسلكية.

مقدم خدمات مرتبطة بالعلاج، وهذا الاخير يزود الكترونيا يسمى "المفتاح الالكتروني ليهكل الصحة" حسب نص المادة 65 مكرر.[1]

نصت المادة 93 مكرر 2 منه على معاقبة كل من يسلم البطاقة الالكترونية بغرض استعمالها بطريقة غير مشروعة وجاءت كما يلي: "دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالسجن من سنتين الى خمس سنوات وبغرامة من 100.000دج الى 200.000دج.

كل من يسلم او يستلم بهدف الاستعمال غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا او المفتاح الالكتروني لهيكل العلاج او المفتاح لمهن الصحة.[2]

نصت المادة 93 مكرر 3 على انه من يقوم عن طريق الغش بتعديل او حذف كلي او جزئي للمعطيات التقنية او الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا او في المفتاح الالكتروني ليهكل العلاج او مهن الصحة وهي نفس العقوبة التي تطبق كذلك على كل من قام بالوصول او استعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا او في المفتاح الالكتروني ليهكل او مهن الصحة.[3]

قانون 09-04 المؤرخ في: 2009/09/05 للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

نصت المادة 2 منه على مفهوم كل من: الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، منظومة المعلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المعلقة بحركة السير، الاتصالات الالكترونية.

نصت المادة 4 منه على مراقبة الاتصالات الالكترونية في الحالات التي تسمح باللجوء الى المراقبة الالكترونية.

نصت المادة 5 منه على القواعد الإجرائية لتفتيش المنظومة المعلوماتية.

---

[1] زوبيخة زيدان، مرجع سابق، ص 77، 78.

[2] المادة 93 مكرر 2، قانون رقم 08-01 المؤرخ في: 2008/01/23، المتمم لقانون رقم 83-01 المتعلق بالتامينات.

[3] المادة 93 مكرر 3، قانون رقم 01/08 المؤرخ في: 2008/01/23، المتمم لقانون رقم 83-01 المتعلق بالتأمينات.

المادة 7 نصت على الحجز عن طريق منع الوصول الى معطيات.
المادة 8 نصت على المعطيات المحجوزة ذات المحتوى الاجرامي.
المادة 9 نصت على حدود استعمال المعطيات المتحصل عليها.
المادة 10 نصت على التزامات مقدمي الخدمات ومساعدة السلطات.
المادة 11 نصت على حفظ المعلومات المتعلقة بحركة السير.
المادة 12 نصت على الالتزامات الخاصة بمقدمي خدمة الانترنت.
المادة 13 و 14 نصت على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.[1]

المطلب الثاني: قواعد الاختصاص و الإجراءات الخاصة بمتابعة الجريمة الالكترونية

تعد متابعة الجريمة الالكترونية من أهم التحديات التي تواجه رجال الضبطية القضائية بالنظر إلى طبيعتها الخاصة من حيث أنها تتعلق بمحل غير مادي بالإضافة إلى صعوبة دور الشرطة ومختلف الأجهزة الأمنية في مراقبتها ومنع حدوثها وكذا التحري عن مرتكبيها.

و لان متابعة الجريمة الالكترونية تفرض على المحقق أن يتمتع بمهارات تخص التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود، والاهم من ذلك هو معرفة المحقق لأساسيات عمل الحاسب الآلي و مبادئ عمل شبكة الانترنت، فان دراسة كل هذه الجوانب يمكننا من إيجاد الحلول المناسبة لتجاوز المعيقات التي تقف في وجه رجال الشرطة أثناء مراحل جمع الأدلة واثبات الجريمة الالكترونية.[2]

سنتطرق في هذا المطلب لأهم القواعد الإجرائية التي جاء بها المشرع الجزائري لمواجهة هذه الأنماط المستجدة من الجرائم، حيث نتناول في الفرع الأول قواعد الاختصاص النوعي والمحلي أما في الفرع الثاني فسوف نتطرق فيه لبعض الإجراءات الخاصة بمتابعة الجريمة

[1] قانون 09-04، مرجع سابق.

[2] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية ، جامعة باتنة، السنة الجامعية 2011 – 2012 ، ص 104 .

الالكترونية على أن نتناول مراحل إثباتها والصعوبات التي تعترض مراحل البحث عن الأدلة في المطلب الثالث.

الفرع الاول: قواعد الاختصاص النوعـــي والمحلـــي في الجريمة الالكترونية حسب القـانون الجزائري.

إدراكا من المشرع الجزائري لخصوصية الجريمة الالكترونية وطبيعتها المعقدة، ولغرض التحكم أكثر في معالجة الأنواع المستحدثة من الإجرام، ورغبة منه في ضمان فعالية وسرعة الفصل في القضايا ذات الطبيعة الخاصة مثل الجريمة المنظمة العابرة للحدود الوطنية، وجريمة الإرهاب وتبييض الأموال والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والجرائم المتعلقة بالتشريع الخاص بالصرف، والتي تتطلب تخصصا وتكوينا خاصا لمختلف الجهات القضائية من نيابة وقضاة تحقيق وقضاة حكم لمتابعة هذه الجرائم، فقد تم إنشاء جهات قضائية موسعة الاختصاص او ما يعرف بالأقطاب القضائية المتخصصة.[1]

دورا كبيرا في جمع الأدلة في الجريمة الالكترونية فهاته الجرائم غالبا ما ترتكب من قبل شخص أجنبي وفي إقليم أجنبي مما يؤكد حتمية التعاون الدولي حتى تتسنى متابعة هذه الجرائم بفعالية اكبر .

سنتناول فيما يلي أحكام الاختصاص النوعي و المحلي التي جاء بها القانون رقم 04-14 ونوضح كيف يمتد اختصاص وكيل الجمهورية و قاضي التحقيق الى دائرة اختصاص محاكم أخرى .

أولا/الاختصاص النوعي في الجريمة الالكترونية.

يتحدد الاختصاص النوعي للمحكمة للفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي تنظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح

[1] معتوق عبد اللطيف، المرجع السابق ، ص 104 .

والمخالفات فيما عدا الاستثناءات المنصوص عليه في قوانين خاصة حسب المادة 328 من قانون الإجراءات الجزائية الجزائري.

ولان الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء ان يخضعوا لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع الجزائري مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخدرات و الجريمة المنظمة عبر الحدود الوطنية وجرائم تبيض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذ جعل الاختصاص ينعقد الى دائرة اختصاص محاكم أخرى وهذا ما نصت عليه المواد 37 ، 40، و المادة 329 من قانون الإجراءات الجزائية الجزائري اثر التعديل الذي جاء به القانون رقم 04-14 المؤرخ في: 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة، قسنطينة، وهران و ورقلة.[1]

ثانيــا/الاختصاص المحلي في الجريمة الالكترونية

من المتعارف عليه ان الاختصاص المحلي يتحدد طبقا لضوابط ثلاث هي مكان وقوع الجريمة او مكان إقامة المتهم او مكان ضبطه حسب نص المادة 37 من قانون الإجراءات الجزائية الجزائري والتي عدلت بموجب القانون رقم 04-14.

كما نصت أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في: 5 أكتوبر 2006 على تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق الى دائرة اختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة و محكمة وهران. [2]

[1] القانون رقم 04-14 المؤرخ في: 10 نوفمبر 2004 المعدل والمتمم للامر 155/66 المتضمن قانون الإجراءات الجزائية، ج،ر، عدد 71، ص 4.

[2] المرسوم التنفيذي رقم 06-348 المؤرخ في: 5 اكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، ج،ر عدد 63، ص 29.

و في نطاق الجرائم الالكترونية او المعلوماتية فان السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان أخر، فان الاختصاص ينعقد لمكان السلوك او مكان تحقق النتيجة، و تعد الجريمة الالكترونية اذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها.[1]

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

الفرع الثاني:قواعد المتابعة الخاصة بالجريمة الالكترونية حسب القانون الجزائري.

كان لتطور الأساليب ارتكاب الجريمة الالكترونية و أخذها منحى تصاعديا بين الجرائم المرتكبة في الجزائر ان فرض على المشرع الجزائري الاعتماد على قواعد إجرائية خاصة في سبيل مكافحة الجريمة الالكترونية او المعلوماتية، وهو ما جاء به القانون رقم 06-22 المؤرخ في: 20 ديسمبر 2006 المعدل والمتمم للامر رقم 66-155 المؤرخ في: 8 يونيو 1966 والمتضمن لقانون الإجراءات الجزائية [3]، حيث نص على إجراءات خاصة تهدف الى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب، التي نتطرق لها تبعا لما يلي .

اولا/اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

[1] جميل عبد الباقي الصغير، المرجع السابق، ص 63.

[2] قانون رقم 09-04 مؤرخ في 5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، جر عدد 47، المادة 15.

[3] القانون رقم 06-22، مرجع سابق ذكره، المادة 65 مكرر 5 الى 65 مكرر 18.

أتاح المشرع الجزائري حسب نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري لضابط الشرطة القضائية القيام ببعض الأعمال اذا ما دعت الى ذلك مقتضيات البحث والتحري و التحقيق الابتدائي في الجرائم المتلبس بها وكذا جرائم المخدرات او الجريمة المنظمة عبر الحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات او جرائم تبييض الأموال او الجرائم الموصوفة بأفعال الإرهاب او التخريب او الجرائم المتعلقة بالتشريع الخاص بالصرف او جرائم الفساد، حيث أجاز لوكيل الجمهورية ان يأمر ضابط الشرطة القضائية باعتراض المراسلات التي تجري عن طريق وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات التقنية اللازمة لالتقاط الصور وتسجيل المكالمات السرية وبدون موافقة المعني وذلك في الأماكن العامة والخاصة، كما يسمح الاذن المسلم من قبل وكيل الجمهورية بالدخول الى المحلات السكنية او غيرها ولو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية، ويكون تنفيذ هذه العمليات تحت إشراف ورقابة وكيل الجمهورية في مرحلة البحث والتحري، اما في مرحلة التحقيق الابتدائي فتكون تحت إشراف قاضي التحقيق الذي أمر بها.

ثانيـــا/التســـــــرب:

المقصود بالتسرب حسب نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري هو قيام ضابط او عون الشرطة القضائية بمراقبة الأشخاص المشتبه في أنهم ارتكبوا الجريمة بإيهامهم انه مساهم معهم او شريك بحيث يستعمل الضابط او العون هوية مستعارة وذلك إذا ما اقتضى البحث والتحري في واحدة من الجرائم التالية:

جرائم المخدرات او الجريمة المنظمة عبر الحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات او جرائم تبييض الأموال او الجرائم الموصوفة بأفعال الإرهاب او التخريب او الجرائم المتعلقة بالتشريع الخاص بالصرف او جرائم الفساد.

وقد نظم المشرع الجزائري أحكام التسرب في الفصل الخامس من قانون الإجراءات الجزائية من المادة 65 مكرر 11 الى المادة 65 مكرر 18 حيث بين فيها كيفية القيام بعملية التسرب وكذا شروط الإذن بالقيام بهذا الإجراء و كذلك الأحكام الجزائية لمن تسبب في كشف هوية الضابط او العون المتسرب حيث نص على عقوبة الحبس من سنتين الى خمس سنوات

وغرامة من 50.000دج الى 200.000دج وتشدد العقوبة في حالة ما أدى الكشف عن هوية الضابط المتسرب الى أضرار بالضابط المتسرب او احد أقاربه المباشرين ، ويتم الاستماع الى الضابط المتسرب بوصفه شاهد عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب.

الفرع الثالث: إجراءات متابعة الجريمة الالكترونية في التشريع الجزائري.

إن الجريمة الالكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قوانين العقوبات والقوانين الأخرى، فلذلك تتسع الجريمة الالكترونية بدعوى عمومية وهذه الدعوة تتم بمراحل وهي عمل دراستنا، مرحلة جمع الاستدلالات ومرحلة التحقيق ومرحلة المحاكمة.

الفرع الرابع: إجراءات المتابعة في مرحلة التحقيق التمهيدي أمام الضبطية القضائية.

إن المرحلة من اختصاص ضباط الشرطة القضائية وهم نوعان، النوع الأول هم الذين يتمتعون باختصاص عام و يختصون بإجراءات الاستدلال بشان الجرائم المنصوص عليها في قانون العقوبات، أما النوع الثاني فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر هؤلاء المشار اليهم في المادة 21 من قانون الاجراءات الجزائية وسلطتهم كذلك محددة لا تمتد الى مرحلة التفتيش ودخول المنازل والمعامل والمباني والأماكن المحاطة بأسوار الا بحضور احد ضباط الشرطة القضائية، و من بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي وتعد محاضرهم ذات حجية وقوة اثبات كما استقر عليه القضاء الوطني. وما يهمنا في هذه الدراسة هو دور الضبطية القضائية ومجال اختصاصها فيما يتعلق بالجريمة الالكترونية.[1]

اولا/ الإجراءات التقليدية لجمع الدليـــــل:

سنتطرق إلى إجرائيين وهما الإجراءات المادية والإجراءات الشخصية.

1/الإجـراءات الماديـة: وتتمثل في إجراءات الانتقال و معاينة مسرح الجريمة الالكترونية والتفتيش والضبـــــط.

[1] زبيخة زيدان، مرجع سابق، ص 116،117.

ا/ الانتقال و معاينة مسرح الجريمة الالكترونية:

تعرف المعاينة عند فقهاء القانون الجنائي بأنها " رؤية بالعين لمكان او شخص او شيء لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة".[1]

و تعرف كذلك بأنها " إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة".[2]

و يتطلب هذا الإجراء انتقال ضابط الشرطة القضائية الى مكان ارتكاب الجريمة وذلك لإثبات حالة مكان ارتكاب الجريمة وحالة الأشياء الموجودة التي قد تساعد في كشف الحقيقة وذلك قبل ان تمحي أثار ارتكاب الجريمة.

و تعتبر المعاينة إجراء من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها او تندب ضباط الشرطة القضائية للقيام بها، كما يمكن للمحكمة ان تقوم بإجراءات معاينة اذا رات ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها او بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة.[3]

و قد نصت المادة 42 من قانون الإجراءات الجزائية الجزائري على وجوبيه انتقال ضابط الشرطة القضائية فورا الى مكان وقوع الجريمة للقيام بالمعاينات، وجاء في نص المادة انه " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل الى مكان الجناية و يتخذ جميع التحريات اللازمة، كما نصت المادة نفسها على ضرورة ضبطه لكل ما يمكن أن يؤدي الى إظهار الحقيقة".[4]

كما نصت المادة 64 الفقرة 3 جواز قيام ضابط الشرطة القضائية القيام بمعاينة في اي وقت وأي مكان إذا تعلق الأمر بواحدة من الجرائم المذكورة في المادة 47 ومنها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

4- ب/ التفتيـــــــــــــــش:

---

[1] محمد زكي أبو عامر، الإجراءات الجنائية، دار منشاة المعارف، الإسكندرية، الطبعة الثانية،(د،ت)، ص 222.

[2] إبراهيم حامد طنطاوي، سلطات مأمور الضبط القضائي، مطبعة دار التأليف، القاهرة، 1991، ص 288.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص 84.

[4] الأمر رقم 66-156 الصادر بتاريخ في: 8 يونيو 1966 المتضمن لقانون الإجراءات الجزائية الجزائري،ج ر عدد 48، المادة 42، ص 622.

ان التفتيش المنصب على منظومة معلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والوضعية وموضوع التفتيش على الرغم من ان المشرع الجزائري اعتبر التفتيش إجراء من إجراءات التحقيق وإحاطته بقواعد صارمة الا انه لم يورد تعريفا خاصا ودقيقا وقد اهتم الدستور الجزائري بعدم المساس بحرية الأشخاص وكرامتهم وأكد ذلك في المادة 40 منه بالقول: "فلا تفتيش الا بمقتضى القانون في إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

ج/ الضبـــــــــــــــط:

إن الضبط في قانون الإجراءات الجزائية هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها.[1]

ان الضبط في الجريمة الالكترونية يختلف هن ضبط الجرائم الاخرى ومن حيث المحل لان الجريمة الالكترونية يرد الضبط على أشياء ذات طبيعة مادية كالورق والكمبيوتر وملحقاته كالأقراص الصلبة والمرنة وأقراص الليزر والبطاقات الممغنطة.

2/ الإجـــراءات الشخصيـــــة:

سنتطرق في هذه المجموعة التي تتسم بالطابع الشخصي لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل وتتمثل هذه الإجراءات في: عملية التسريب، الشهادة، الخبرة التقنية واستجواب المتهم.

ا/ التســـــــــرب:

جاءت المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري تعرف التسرب بأنه يقصد به مراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة باتهامهم وتواطئهم مع شريك في الجريمة.

يسمح لضباط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وان ارتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان ان تشكل هذه الأفعال تحريض على ارتكاب الجرائم.[1]

[1] عائشة بن قارة مصطفى، مرجع سابق، ص 201، 114.

ب/ الشهادة في الجريمة الالكترونية:

يطلق على صاحب الشهادة باسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب والذي يكون لديه معلومات جوهرية لازمة للدخول للنظام، فلذلك نجد ان الشاهد المعلوماتي ينحصر في عدة طوائف تتمثل في: مشغل الحاسب الآلي، خبراء البرمجة، مهندسو الصيانة والاتصالات، مديرو النظم.[2]

ج/ الخـــــبرة في الجريمة الالكترونية:

لابد ان يكون الخبير صاحب مقدرة وإمكانيات علمية وفنية في مسالة موضوع الخبرة ويستطيع القيام بدوره للقيام بهذا الأخير عليه ان يبين المكان المحتمل لأدلة الإثبات وشكلها و هيئتها والآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية وكيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة والأجهزة او تدميرها.

ت/ استجواب المتهم في الجريمة الالكترونية:

أحالت التشريعات استجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث من الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الاستعانة بمحام أثناء الاستجواب وتمكينه من الاطلاع على الملف والاتصال به.[3]

ثانيـــا/ الاجراءات الحديثة لجمع الدليل الالكتروني.

1/ الاجراءات المتعلقة بالبيانات الساكنة.

ا/ التحفظ على البيانات المخزنة:

في المادة 16 من اتفاقية بودابست نصت على ضرورة كل طرف السماح للسلطات المختصة أن تأمر او تفرض بطريقة اخرى مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالأمور المخزنة بواسطة نظام معلوماتي،

[1] زبيخة زيدان، مرجع سابق، ص 169

[2] بوكثير خالد، مرجع سابق، ص 23،26.

[3] بوكثير خالد، مرجع سابق، ص 22-27.

وذلك ما تكون هناك أسباب تدعو للاعتقاد بان هذه البيانات على وجه الخصوص معرفة للفقد والتغيير، وذلك من خلال مدة 90 يوم كحد أقصى وهذه المدة قابلة للتمديد.

ب/ مـــــــزود الخدمـــــة:

مزود الخدمة هو من يقدم خدمة الى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.[1]

ج/ التحفظ المعجل على البيانات المخزنة:

يقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته او تحت سيطرته، وفي انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش او الأمر بتقديم بيانات معلوماتي.[2]

2/ الإجراءات المتعلقة بالبيانات المتحركة (اعتراض الاتصالات الالكترونية).

نتيجة للتطور التكنولوجي الذي أدى الى إفراز أجهزة المراقبة ذات التقنية الى مراقبة الأحداث التي تمس الإنسان في خصوصيته وما يتفرغ عنه من سرية الأحاديث الخاصة و هو لصر صلة الإنسان، فلذلك أقرت معظم التشريعات على توفير قدر كبير من الحماية الجنائية على سرية الاتصالات الخاصة بالأفراد، حيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية دون اذن بذلك، "بموجب القانون رقم 06-23 المؤرخ في: 2006/12/20 المعدل لقانون العقوبات الجزائري، حيث تنص المادة 303 مكرر من قانون العقوبات على انه، "يعاقب بالحبس من ستة أشهر الى ثلاث سنوات و بغـــرامة من 50.000دج الى 300.000دج لكـــل من تعمـــــد المســـــاس بحرمة حياة خاصة باي تقنية كانت.[3]

[1] عائشة بن قارة مصطفى، مرجع سابق، ص 154.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص 155،159.

[3] نفس المرجع، ص 162،168.

الفرع الخامس: إجراءات المتابعة في مرحلة التحقيق القضائي.

تعتبر هذه المرحلة هي المرحلة الثانية بعد مرحلة جمع الاستدلالات وسنخص في هذا الفرع على دراسة هذه المرحلة كما يلي:

اولا/ تعيـــين قـاضي التحقيـــق:

في الجزائر يتعين قاضي التحقيق بمقتضى قرار من وزارة العدل، ثم عدل المشرع عن ذلك بموجب القانون 01-08 المؤرخ في: 2001/06/26 وأصبح التعيين بموجب مرسوم رئاسي، وفقا لنص المادة 39 من قانون الاجراءات الجزائية، الا انه حتى هذا الاخير تم الغائه بموجب قانون رقم 06-22 المؤرخ في: 2006/12/20 ليرجع من جديد للتعيين بموجب قرار وزاري من وزارة العدل بعد استشارة المجلس الأعلى للقضاء من بين قضاة الجمهورية، و هذا رجوعا الى نص المادة 50 من القانون الاساسي للقضاة، وتكون مدة التعيين ثلاث سنوات و تنتهي مهام قاضي التحقيق بنفس الأشكال التي يتعين فيه، اي بقرار من وزارة العدل.[1]

ثانيـا/ السمات التي تميز قاضي التحقيق فيما يخص الجرائم الالكترونية:

ان الجريمة الالكترونية تختلف عن الجريمة التقليدية فلذلك لا يمكن ان يحقق فيها اي قاضي تحقيق، وإنما لابد ان يكون له صفات خاصة، هذه الصفات هي كان يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة وان يميل الى تصميم البرامج أكثر من تشغيلها و يجب معرفة الجديد عن هذه البرامج وان يستطيع تصميم و تحليل البرامج او أنظمة التشغيل بسرعة وان يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة وكل هذه الأمور لا تتوافر الا لمن كان لديه إمكانيات عقلية تزيد من متوسط العام المألوف.[2]

ثالثـــا/ استئناف أوامر قاضي التحقيق: الجهات التي تستأنف أوامر قاضي التحقيق هي:

1/ النيابـــة العامـــة: لوكيل الجمهورية او احد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري،

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 223، 224.

[2] مصطفى محمد موسى، مرجع سابق، ص 265.

"لوكيل الجمهورية الحق في أن يستأنف أمام غرفة الاتهام جميع أوامر قاضي التحقيق و يكون هذا الاستئناف تقرير لدى المحكمة ويجب ان يرفع في ثلاثة ايام من تاريخ صدور القرار".[1]

2/ **استئنـــــاف المتهـــم:** ان المتهم لا يجوز له استئناف جميع أوامر قاضي التحقيق و يرفع الاستئناف بعريضة يودع لدى قلم كتاب المحكمة في ظرف ثلاثة أيام من تبليغ الأمر الى المتهم طبقا للمادة 168 من قانون الاجراءات الجزائية.

3/ استئناف المدعى المدني: كما أجاز المشرع الجزائري للمدعى المدني الحق في استئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية، وبمفهوم المخالفة لا يجوز له استئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية.

الفرع السادس: إجراءات المتابعة في مرحلة المحاكمة.

اولا/ اختصاص المحكمة:

1/ الاختصاص المحلي في الجريمة الالكترونية:

طبقا لنص المادة 37 من قانون الإجراءات بتحديد الاختصاص المحلي للجريمة في ثلاث ضوابط منها مكان إقامة المتهم ومكان الضبط.[2]

كما نصت أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في: 2006/10/05 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق الى دائرة اختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة و كذا محكمة قسنطينة ومحكمة ورقلة وقسم محكمة وهران.[3]

و في نطاق الجرائم الالكترونية فان السلوك الاجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث فيروس وتتحقق النتيجة بتدمير المعلومات في مكان آخر، فان الاختصاص ينعقد اما في مكان السلوك او مكان تحقق النتيجة، وتعد الجريمة الالكترونية اذا

[1] عبد الرحمان خلفي، مرجع سابق، ص231، 233.

[2] مولود ديدان، قانون الإجراءات الجزائية، مرجع سابق، ص 79.

[3] نفس المرجع، ص 17.

تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر انها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها.[1]

2/ الاختصاص النوعي في الجريمة الالكترونية:

يتحدد الاختصاص النوعي لمحكمة الفصل في قضية معروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية او تخريبية المحالة اليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري، كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب نص المادة 328 من قانون الإجراءات الجزائية.[2]

ثانيـــا/ تشكيلـــــة المحكمـــة:

تختلف تشكيلة المحكمة الجزائية بحسب قسم ونوع قسم الجنح الخاصة بالجرائم الالكترونية.

على مستوى المحكمة يتشكل من فرد ويساعده كاتب ضبط بحضور وكيل الجمهورية ومساعديه.

اما الغرفة الجزائية على مستوى المجلس القضائي فالتشكيلة فيها ثلاثية، اي تشكل من رئيس الغرفة ومستشارين اثنين بالإضافة الى كاتب ضبط وبحضور النائب العام او احد مساعديه.

اما محكمة الجنايات فتتشكل من رئيس المحكمة ومستشارين ومحلفين وكاتب الضبط والنيابة العامة او من يمثلها.

ثالثا/ القواعد العامة للمحكمة:

[1] المرسوم التنفيذي رقم 06-348 المؤرخ في: 2006/10، المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر عدد 63، ص 29.

[2] القانون رقم 04-14، مرجع سابق، ص 4.

تنفيذ المحكمة بمجموعة من المبادئ تنطبق على المحكمة الجزائية لقسم الجنح على مستوى المحكمة او الغرفة الجزائية سنحاول شرحها على توضيح الاتي بيانه.

1/ علانيـــــة الجلســـــة:

جل التشريعات تقر بمبدأ علانية الجلسة، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الاطمئنان والشعور بالعدالة وهذا على التحقيق الأول الذي يقوم به ضباط الشرطة القضائية وكذا التحقيق الابتدائي الذي تقوم به جهات التحقيق، فكلاهما يتم في سرية، الا ان العلانية ليست في جميع الجلسات بل للقاضي سلطة تقديرية في إخراج القصر من الجلسة، كما يمكن ان تكون الجلسة سرية اذا كان في علانيتها خطر على النظام العام والآداب العاملة، الا ان هذا الحكم يجب ان يصدر في جلسة علنية و يحكم هذا المبدأ نص المادة 258 من قانون الإجراءات الجزائية الجزائري.

2/ شفويـــة المرافعـــات:

فأطراف الخصومة القضائية لهم الحق في المناقشة لكل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولا يتم الاكتفاء بالتحقيقات الأولية والابتدائية التي سبقت المحاكمة.

3/ تدويـــن التحقيـــق النهـــائي: لا يمكن للمحكـــمة ان تنعقد في حـــالة غياب أمين الضبط لان دوره يتجسـد في تدوين كل مـا يـدور في الجلسة.[1] ويحرر بذلك صحيفة الجلسة التي يسجل فيها جميع الأقوال و التصريحات التي دارت بالجلسة.

وفي الأخير نستنتج ان الجريمة الالكترونية لم يخص لها المشرع إجراءات متابعة خاصة لها وإنما تخضع لنفس إجراءات الجريمة التقليدية.

المطلب الثالث: الآليات المختصة في متابعة و مكافحة الجريمة الالكترونية

نظرا لتفاقم ظاهرة الإجرام الالكتروني من يوم لأخر و بالنظر الى الطبيعة الخاصة التي تتميز بها هاته الجرائم ، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة الالكترونية او المعلوماتية ، لهذا عمدت معظم الدول الى استحداث

[1] عبد الرحمن خلفي، مرجع سابق، ص 323، 324.

وحدات خاصة لمكافحة هذا النوع من الجرائم ، كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث و التحري في العالم الافتراضي على غرار هيئة الانتربول و اليوروبول و الافريبول.[1]

ان الجريمة الالكترونية أصبحت اشد خطورة على المجتمع والفرد خاصة، و للحفاظ عليها وضعت اغلب التشريعات سواء الجزائري او الأجنبي وسائل لمتابعة هذه الجرائم.

الفرع الأول: الآليات المختصة في متابعة الجريمة الالكترونية في التشريع الجزائري.

في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة الى وحدات قضائية و أخرى تابعة لسلك الأمن و الدرك الوطني ، سنتطرق الى ثلاث أجهزة لمتابعة الجريمة الالكترونية والمتمثلة في ما يلي:

أولا/ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام الاتصالات الالكترونية.

وأنشئت الهيئة في الجزائر بموجب المادة 13 من القانون رقم 09-04 المؤرخ في: 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[2] و تحديدا بنص المادة 13 ، لكنه ترك أمر تحديد تشكيلة الهيئة و تنظيمها و كيفيات سيرها للتنظيم الصادر بموجب المرسوم الرئاسي 15/ 261 [3]

تعد الهيئة سلطة إدارية مستقلة لدى وزير العدل ، تعمل تحت إشراف و مراقبة لجنة مديرة يترأسها وزير العدل ، و تضم أساسا أعضاء من الحكومة معنيين بالموضوع ، و مسؤولي

[1] سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مقال منشور في مجلة العلوم الانسانية ، جامعة الإخوة منتوري قسنطينة 1 الجزائر 2019 ، عدد 52 ديسمبر 2019 ، ص 52 .

[2] سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد، ص 11.

[3] المرسوم الرئاسي 15- 261 المؤرخ في: 08 اكتوبر 2015 ،ج ر عدد 53 المحددة لتشكيلة و تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.

مصالح الامن ، و قاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء و تضم الهيئة قضاة وضباط و أعوان من الشرطة القضائية التابعين لمصالح الاستعلام العسكرية و الدرك و الأمن الوطنيين ، وفقا لقانون الإجراءات الجزائية تكلف بتجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من اجل استعمالها في الإجراءات القضائية و ضمان المراقبة و الوقاية للاتصالات الالكترونية قصد الكشف عن الجـــرائم المنصوص عليها في قانون العقوبـــات او الجرائم الأخـــرى ، تحت سلطة القاضي المختـــص.[1]

ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

هناك الحالات التي تسمح بمراقبة الاتصالات الالكترونية لأغراض وقائية كالوقاية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بإذن النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد و الوقاية من الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة او الدفاع الوطني او المصالح الإستراتيجية كالاقتصاد الوطني بإذن السلطة القضائية المتخصصة.

للإشارة تمكنت الجزائر ممثلة أساسا في اجهزتها الامنية التابعة للدرك الوطني و الامن الوطني و بالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الاعلام و الاتصال من معالجة اكثر من 1000 جريمة الكترونية منها 30 بالمائة على مواقع التواصل الاجتماعي ، هذا و قد سجلت مديرية الشرطة القضائية بالمديرية العامة للامن الوطني خلال السداسي الاول من عام 2016 وجود 11 قضية متعلقة بالارهاب الالكتروني اغلبها خاصة بتهديدات ارهابية باسم تنظيم داعش الارهابي لتسفر جهود البحث و التحري و التنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا ارهاب الكتروني تمت احالتهم على القضاء. [2]

[1] سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري ، ص 53 .

[2] سعيدة بوزنون، المرجع السابق .

هذا و قد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق و سوريا و ليبيا كما تمكنت من فك شفرات الرسائل المتبادلة و ما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت و منصات التواصل الاجتماعي خاصة الفيسبوك و التويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة و تلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية الى جانب اتصالات محلية و دولية.

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة:

والمتمثلة في الأقطاب القضائية المتخصصة.

1/ إنشائهـــــا:

نشأت بموجب القانون 04-14 المؤرخ في: 2004/11/10 المعدل لقانون الإجراءات الجزائية.[1] تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37-329-40 من قانون الإجراءات الجزائية. [2]اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في: 2006/01/05.

إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى لو كان مرتكبها أجنبيا اذا كانت تستهدف مؤسسات الدولة او الدفاع الوطني حسب المـــــادة 15 من القانون رقم 04.

2/ توسيع صلاحية الضبطية القضائية:

عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني حسب المـــــادة 16 من قانون الإجراءات الجزائية.

كما يمكن تفتيش المحلات السكنية وغير السكنية في اي ساعة من ساعات الليل والنهار باذن من وكيل الجمهورية حسب المـــــادة 47 من قانون الإجراءات الجزائية.

3/ أساليب التحري الخاصة:

[1] سالم عبد الرزاق، مرجع سابق، ص 14.

[2] مولود ديدان، قانون الإجراءات الجزائية، مرجع سابق، ص 18.

اعتراض المراسلات الالكترونية حسب المادة 65 مكرر 5 من قانون الإجراءات الجزائية المدرجة بموجب القانون 06-22 المؤرخ في: 2006/12/20.

الفرع الثالث: المعهد الوطني للأدلة الجنائية وعلم الجرائم:

يتكون المعهد الوطني للأدلة الجنائية وعلم الجرائم من إحدى عشرة دائرة متخصصة في مجالات مختلفة تضمن انجاز الخبرة، التكوين والتعليم، تقديم المساعدات التقنية، البحوث، الدراسات والتحاليل في علم الجريمة.

دائرة الإعلام الآلي والتكنولوجي مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي وتماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

أفراد الدائرة يسهرون على تامين اليقظة التكنولوجية من اجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لانجاز المهام المنوطة بها، تنقسم الدائرة الى ثلاث مخابر ذلك حسب نوع المعلومات (سمعيـــة، بصريـــة وإعـــــلام الي).

كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي: مخـــبر الإعلام الالي، مخبر الفيديو، مخبر الصوت.[1]

1/ مخـــبر الإعـــــلام الآلي:

من مهامـــــه: تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفـــــلاش). بالإضافة الى تحديد التزوير الرقمي للبطاقة البنكية.

من تجهيزاتـــــه: محطـــة ترميم و تصليح الأجهزة والحوامل المعطلة.

الشبكات الإعلامية (خبرات الاعلام الالي والتجهيزات البيانية).

محطة ثابتة ومحمولة لإجراء خبرات الإعلام الالي.

جهاز اقتناء معلومات الهواتف و الحاسوب.

[1] هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الاجرام، جامعة بسكرة، كلية الحقوق، 2016، ص 3.

والقاعات التي تحتوي عليها: تتمثل في 7 قاعات (مكتب توجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، فصيلة اقتناء المعطيات، قاعة موزع وقاعات تخزين).

1- 2/ مخـــــبر الفيديـــــو:

يختص مخبر الفيديو بمقارنة الأوجه وشرعية الصور والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد و تحسين نوعية الصورة بمختلف التقنيات.

من تجهيزاتـــه: جهاز الفيديو بوكس وحوامل الفيديو الرقمية والممغنطة وحبكات إعلامية،(كونتك ستوديو، ماكس ثلاثي الأبعاد) وموزع لحفظ شرائح الفيديو.

أما بالنسبة للقاعـــات يحتـــوي مخـــبر الفيديـــو على 4 قاعـــــات (قاعتان للتحليل، قاعة التخزين و قاعة موزع).

3/ مخـــــبر الصـــــــوت:

من مهامه: تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

من أجهزتـــه: جهاز الازدواجية و السماع وحبكات إعلامية (معالجة وتحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة وأجهزة التصليح والتعبير)، اما بالنسبة للقاعات فانه يحتوي على مخبر الصوت وخمس قاعات إضافية.[1]

الفرع الرابع: المديريـــة العامـــة للأمـــن الوطـــني:

1/ جوانب التصدي للجرائم الالكترونية: تصدت هذه المديرية للجريمة الالكترونية من مختلف الجوانب منها:

الجانـب القانـــــوني: و المتمثل في النصوص القانونية كقانون 06/22 المؤرخ في: 2006/12/10 و القانون 03/05 و القانون المدني 09/04 المؤرخ في: 2009/08/05 و قانون العقوبات الخاص بالمواد من 394 مكرر الى 394 مكرر 7 .[1]

[1] سالم عبد الرزاق، مرجع سابق، ص 4-7.

الجانـــب التنظيـــــمي:

و يتمثل في التكوين المتواصل و التخصص و تدعيم مخابر الشرطة العلمية و تدعيم المصالـــح الولائيـــة للشرطة القضائية و تدعيم هيكلـــة مصالـــح الشرطة القضائية للتصدي للجريمة .

الجانـــب التوعـــــوي:

لم تغفل المديرية العامة للأمن الوطني الجانب الوقائي التوعوي و يظهر ذلك من خلال برمجة المديرية العامة لخطوات استباقية للتصدي للجريمة الالكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية و كذا المشاركة في الملتقيات و الندوات الوطنية و جميع التظاهرات التى من شانها توعية المواطن حول خطورة الجرائم الالكترونية .

الجانـــب الـــــدولي:

في إطار مكافحة الجريمة الالكترونية و نظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم. لم تغفل المديرية العامة للأمن الوطني استغلال عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية الانتربـــــول INTERPOL هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي و تسهل الإجراءات القضائية المتعلقة بتسليم المجرمين . و كذا مباشرة الانابات القضائية الدولية و نشر أوامر القبض للمبحوث عنهم دوليـــــــا.

2/ العمل الميداني للتصدي للجريمة الالكترونية:

عالجت المديرية العامة للأمن الوطني على المستوى الوطني مجموعة من القضايا المتعلقة بالجانب الالكتروني[2] اين بلغ عدد القضايا المعالجة خلال سنة 2015 – 409 قضية تورط فيها 347 شخص

[1] حملاوي عبد الرحمان . مداخلة بعنوان "دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية " . جامعة محمد خيضر. بسكرة. كلية الحقوق. 2016 .ص 2 .

[2] حملاوي عبد الرحمان .نفس المرجع. ص 6 – 7 .

كما سجلت مصالح المديرية العامة للأمن الوطني المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خلال الـ 08 أشهر الأولى من السنة الجارية 567 قضية تتعلق بجرائم الانترنت تورط فيها 543 شخصا.

حيث كما تمكنت الفرق المختصة في مكافحة الجرائم الالكترونية للأمن الوطني و من خلال معالجة كافة المعطيات التقنية والأدلة المادية المرتبطة بالقضايا السالفة الذكر من معالجة 385 جريمة الكترونية من أصل 567 قضية مسجلة ومحل متابعة لفك خيوطها و هذا وفق ما توضحه المعطيات.

الواردة في الجدول التالي:

نــوع الجريمـة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الانترنت	430	289	365	%68
جرائم الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	%55
جرائم الاحتيال عبر الانترنت	25	17	32	%68
جرائم التحريض و التطرف عبر الانترنت	14	14	31	%100
الجرائم المخلة بالحياء	12	08	22	%67
جرائم بيع السلع المحظورة عبر الانترنت	06	05	15	%84
جرائم مختلفة (نسخ البرامج دون حق – القرصنة)	23	21	39	%92
المجمـــــوع	**567**	**385**	**543**	**%68**

المصدر: إحصائيات مصالح المديرية العامة للأمن الوطني المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منشورة على الرابط:

https://www.algeriepolice.dz – تاريخ الزيارة: 2021/04/28 الساعة: 10:00.

المبحـــث الثـــــاني: معوقات مكافحة الجريمة الالكترونية و انعكاسها على التشريع الجزائي الجزائري.

أدى التطور الكبير والانتشار الواسع و المتسارع للتقنية العالية والمتمثلة في الأنظمة المعلوماتية، الى ظهور جملة من الجرائم تعددت صورها وإشكالها أطلق عليها الجرائم الالكترونية.

فلم تعد الجريمة ترتكب بشكلها التقليدي بل تعدته الى استعمال شبكة المعلومات إما كوسيلة لارتكاب العديد من الجرائم بعيد عن أعين الجهات الأمنية، أو أن تكون هي بيئة الجريمة، خاصة مع انتشار استعمال شبكة الويب العالمية (الانترنت)، والتي صنعت عالما افتراضيا لا يعترف بالحدود الجغرافية، فانتقلت الجريمة من صورتها المادية التقليدية إلى أخرى

معنوية عابرة للدول والقارات، مما فرض على المجتمع الدولي البحث عن وسائل لمكافحة هذه الطائفة من الجرائم وذلك بإيجاد نظام عقابي لمرتكب جرائم المعلوماتية.

وعلى الرغم من ان مواجهة هذه الطائفة من الجرائم تتم بعدة اتجاهات، سواء بسن الدول لتشريعات جديدة او تعديل تشريعات القائمة، إلا ان محاولات التصدي لها اصطدمت بعدة صعوبات، كما ان محو آثارها وإتلاف أدلتها عملية سهلة، وكشف هوية مرتكبها ليس بالأمر الهين، حيث يمكن للجاني تخزين البيانات المتعلقة بنشاطه الإجرامي في دولة أخرى، او في مكان بعيد عن مكان ارتكاب الجريمة، ومع تمكنه من ترميز المعطيات الأمر الذي جعل إخفائها عن أجهزة العدالة أمرا بسيطا.

مما لا شك فيه أن الصعوبات التي تعترض سبل مكافحة الجريمة الالكترونية متعددة، وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئـــة الافتراضية لتعقب المجرمـــين و تقديمهم للعدالة، أو خـــلال ملاحقة الجناة وكشف جرائمهم عبر الحدود.

لذلك تثور العديد من المشكلات والتي تقف عائقا أمام مكافحة الجريمة الالكترونية، منها ما يتعلق بإثبات الجريمة نفسها، كما قد يبرز للوجود صعوبات متعلقة بالتعاون القضائي الدولي وتحديد قواعد الاختصاص.

و لما كانت هذه الجرائم من طبيعة خاصة، فان خطرها او آثارها لم تعد محصورة في النطاق الإقليمي لدولة معينة، الأمر الذي بات يثير بعض التحديات أمام السلطات القضائية الدولية.

وعلى هذه الأفكار، يمكننا طرح التساؤل التالي: فيما تتمثل الصعوبات التي تعترض سبل مكافحة الجريمة الالكترونية ؟ وبعبارة أخرى: ما هي أهم المشكلات القانونية والفنية التي تواجه مكافحة الجريمة الالكترونية ؟

وعليه سنتناول في هذا المبحث المعوقات المتعلقة باكتشاف واثبات الجريمة الالكترونية من خلال المطلب الأول، و في المطلب الثاني نتعرض الى المعوقات المتعلقة بالجانب

القضائي للجريمة الالكترونية لا سيما منها تلك المتعلقة بالمحكمة المختصة و القانون الواجب التطبيق.

المطلب الاول: المعوقات المتعلقة باكتشاف و إثبات الجريمة الالكترونية

تحيط الجريمة الالكترونية جملة من الصعوبات التي تقف أمام الكشف عنها والوصول الى الجاني، نظرا للوسيلة المستعملة في ارتكابها وطبيعة المحل المتعدي عليه والمتمثل في معلومات معالجة آليا هذا من جهة، ومن جهة اخرى فانه يصعب اثبات هذا النوع المستحدث من الإجرام وإسناد الجرم لفاعله لكون هذا الاخير يتميز بالذكاء والخبرات الفنية والعقلية، فيسعى الى محو وإخفاء الدليل بشتى الطرق مما يجعل عملية إثباتها تعترضها العديد من العراقيل.

الفرع الأول: معوقات اكتشاف الجريمة الالكترونية.

ان مرد صعوبات اكتشاف الجريمة راجع لعدة اعتبارات منها ما هو متعلق بالإحجام عن ابلاغ السلطات المختصة، وكذلك نقص خبرة سلطات الاستدلال، ومنها ما هو راجع الى فقدان الآثار التقليدية للجريمة، وكذلك فرض الجناة لتدابير الحماية.

أولا/ إحجام الجهات المتضررة عن إبـــــلاغ السلطات المختصة:

إن عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد احدى معوقات اكتشاف الجريمة، اذ تحرص الجهات المجني عليها والتي غالبا ما تكون مصرفا، او مؤسسة مالية، او شركة، او مشروعا صناعيا ضخما، على الإحجام عن الابلاغ عن الجريمة بسبب الحفاظ على سمعة المؤسسات ومصداقيتها وثقة عملائها وعدم رغبتها في الظهور بمظهر مشين امام الاخرين، لان تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا او قلة خبرتها او عدم وعيها الامني، ولم تتخذ الاحتياطات الامنية اللازمة لحماية معلوماتها [1]، الامر الذي يجعلهم يفضلون الترضية المالية لعملائهم حتى لا يفقدوهم، ولا تتاثر سمعتهم المالية بدلا

[1] خالد ممدوح ابراهيم، فن التحقيق في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ص 68.

من البحث على الجناة، فهذه المؤسسات لا تكتفي في اطار ذلك بالاحجام عن الابلاغ، و انما الى جانب ذلك تلجا الى الترضية الودية فيما بينها، وبين الجناة[1].

كما يكون الاحجام عن الابلاغ عن هذا النوع من الجرائم من اجل اخفاء أساليب ارتكابها للحيلولة دون تقليد الاخرين للجناة ومحاكاتهم في جرائمهم، كما قد يتوخى بعض المجني عليهم من وراء العزوف عن الابلاغ عدم اتاحة الفرصة للأجهزة الامنية من الاطلاع على معلومات لم يجر الابلاغ عنها، وربما يظهر ذلك بصورة اكبر في نطاق الجرائم التي تستهدف شركات التامين البنوك او البنوك رغبة في توقي الخسائر التي يتوقع تحققها نتيجة هذا الابلاغ بسبب نقص ثقة العملاء في هذه المؤسسات.[2]

ثانيا/ نقص خبرة سلطات الاستدلال:

المعلوم أن متطلبات العـدالة الجنـائية تفرض على الأجهزة المسؤولة عن تتبع الجـرائم و ضبطها و التحقيق فيها ان تتحمل مسؤوليتها نحو اكتشـاف المجرمين وضبطهم ومحـاكمتهم، ومثل هـذا الأمر بمقتضى توفير الإمكانات التقنية اللازمة في عملية الكشف والاستدلال عن الجرائم، لا سيما بعد ان تطورت أساليب ارتكاب الجرائم وظهور أنماط مستحدثة من الجرائم ما كانت التشريعات لتعرفها من قبل، الا بعد ان ظهرت رسائل متطورة تمكن المجرمين ارتكاب جرائمهم بأساليب وطرق غير معهودة لرجال السلطة العامة[3].

وعليه فان توفير الإمكانيات التقنية في الاستدلال والتحقيق عن هذه الجرائم سيكون اكثر حاجة فيها من غيرها من الجرائم، اذ ان القصور في توفير هذه الإمكانيات من شانه ان يؤدي الى صعوبة في اكتشاف او قلة الوسائل والإمكانيات لدى تلك الجهات ان توفر الكادر الفني، لذلك في هذا المجال للاستعانة به في التحقيق، وضرورة الاستعانة بالنخبة المتخصصة في

[1] محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، اهمم صورها، والصعوبات التي توجهها، ط1، دار المناهج، الاردن، 2005، ص 218.

[2] موسى مسعود ارحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الاول حول المعلوماتية والقانون، اكاديمية الدراسات العليا، طرابلس، 28-2009/10/29، ص 6.

[3] محمد حماد مرهج الهيتي، المرجع السابق، ص 215.

انظمة المعالجة الالية لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها، وتولي شرح هذه الأدلة و إبعادها أمام المحاكم[1].

فهناك جملة من الصعوبات تواجه عمل المحققين، وخاصة منهم غير المتخصصين او غير ذوي الخبرة والدراية، والذين انحصرت معلوماتهم في جرائم قانون العقوبات التقليدية من قتل وسرقة، فمثل هؤلاء لن يكونوا قادرين على التعامل معها، كونها ترتكب بطريقة تقنية، حيث لا تتوفر لهم الدراية الفنية بهذا المجال، ولا التدريب والتقنية المطلوبين لكيفية التعامل من أنظمة المعالجة الآلية [2]، الأمر الذي جعل بعض الدول تخصص وحدات وفرقا متخصصة، بل لابد من إتباع إستراتيجية تدريبية وتكوين متعمق في ميدان تكنولوجيات الاعلام والاتصال[3].

كما ان بعض هذه المعوقات ترجع الى شخصية المحقق، مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت، بالإضافة الى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية[4].

وفي الجزائر فانه بالإضافة الى مصالح الضبطية القضائية فانه بموجب المرسوم الرئاسي رقم 183/04 المؤرخ في: 2004/06/26 تم احداث المعهد الوطني للادلة الجنائية وعلم الاجرام تحت وصاية القيادة العامة للدرك الوطني، ويحتوي هذا المعهد على قسم الإعلام الالي يختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية، والى جانب ذلك يوجد مركز الوقاية من جرائم الإعلام الالي والجرائم المعلوماتية تابع ايضا لقيادة الدرك الوطني، اما على مستوى المديرية العامة للامن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة

---

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الالي والانترنت، دار الكتب القانونية، القاهرة، 2002، ص 37.

[2] محمد حماد مرهج الهيتي، المرجع السابق، ص 215.

[3] فرنسا مثلا قامت بانشاء عدة وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة هذا الاجرام المستحدث بجميع صوره ومن ذلك المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات والاتصالات، بالاضافة الى قسم الانترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصار (STRTD)، والقسم الالكتروني التابع لمعهد البحوث الجزائية التابع للدرك الوطني المعروف اختصارا بـ (IRCGN) وكذا وحدات اقسام الاستعلامات والتحقيقات القضائية المعروف اختصارا بـ (BDRIJ) .

[4] Myriam QUEMENER et joel FERRY, cybercriminalité défi mondial, édition,2009,p214

القضائية ومن الفروع التقنية التي تتضمنها هذه المخابر، خلية الاعلام الالي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية، وحتى تكتمل قدرات تلك الاجهزة في هذا المجال فقد تم انشاء الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته.[1]

ثالثا/ فقدان الآثـــــار التقليديـــــة للجريمة:

إذا كان من السهل على جهات التحري والتحقيق ان تتحرى على الجرائم التقليدية عن طريق المشاهدة او التتبع او سماع الشهود فانه يصعب عليها ذلك في الجرائم المعلوماتية، إذ أن الجريمة تظل مجهولة ما لم يبلغ عنها للجهات المعنية بالاستدلالات والتحقيق الجنائي، وفي هذا الصدد تجدر الإشارة ان أهم الجرائم لا تصل الى علم السلطات المعينة بطريقة اعتدائية كباقي جرائم قانون العقوبات، لكونها جرائم غير تقليدية لا تصل الى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، لكونها جرائم غير تقليدية لا تخلف اثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة [2]، ومشاهدة الجروح التي على المجني عليه، وعلامات التسمم التي ظهرت على المجني عليه نتيجة استخدام المواد السامة في جريمة القتل وكذلك التزوير والتزييف حيث يمكن مشاهدة النقود المزورة والمزيفة، وهذا كله يعود الى طبيعة الجريمة المرتكبة، والوسيلة التي تستخدم في ارتكابها، اما الجريمة المعلوماتية فان الامر جدا مختلف، فمن حيث الوسيلة التي ترتكب بها مثل هذه الجرائم فانها يتم ارتكابها عن طريق نقل المعلومات على شكل نبضات الكترونية غير مرئية تنساب عبر اجزاء الحاسب بالاشاعات، وغالبا ما يتم هذا عن طريق وحدات طرفية بعيدة، ربما تكون هذه الوحدات لا سلكية الاتصال مما يصعب ضبطها، بل ان هذه الجرائم يمكن ارتكابها عن طريق الهاتف اذ

[1] خالد ممدوح ابراهيم، المرجع السابق، ص 69، لينا محمد الاسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط1، دار الحامد، الاردن، 2015، ص 246.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 41.

يمكن عن طريقه اصدار تعليماته للحاسب الالي، ومن مسافات بعيدة قد تتعدى نطاق اقليم الدولة، مما يزيد من صعوبة اكتشافها[1].

وكما يرجع السبب في افتقاد الاثار التقليدية للجريمة المعلوماتية الى ما لاحظه جانب من الفقه من ان هناك بعض العمليات التي يجري ادخال بياناتها مباشرة في جهاز الحاسب الالي دون ان يتوقف ذلك على وجود وثائق او مستندات يتم النقل منها[2].

رابعـــا/ فـــرض الجنـــاة لتدابـــير أمنيـــــــة:

ان المتورطون في الجرائم المعلوماتية لديهم قدر كبير من الذكاء والتفوق يجعلهم يباشرون إجرامهم بدقة متناهية خشية افتضاح أمرهم وضبطهم، اذ غالبا ما يضرب المجرم المعلوماتي سياجا امنيا على أفعاله غير المشروعة قبل ارتكابه لها، لكي لا يقعوا تحت طائلة العقاب، كما يزيد ذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه وذلك بالعمل على ترميز او تشفير البيانات المخزنة الكترونيا او المنقولة عبر شبكات الاتصال، بالإضافة الى دس بعض التعليمات الخفية بين الأدلة لتصبح كالرمز، بحيث يستحيل على غيره الاطلاع عليها وفهم مقصودها ويتعذر على سلطات البحث والتحقيق الوصول الى كشف أفعالهم غير المشروعة[3].

الفرع الثاني: معوقات إثبـــات الجريمة الالكترونية.

سبق وان تناولنا بعض الصعاب التي تحيط بالجريمة الالكترونية، وكان لابد لنا في هذا المقام من التطرق الى باقي الصعوبات المتعلقة باثبات الجريمة، من غياب الدليل المرئي وسهولة إخفاء الدليل وقصور إجراءات الحصول عليه، بالإضافة الى تعقد الشبكة العنكبوتية وتشابكها وضخامة كم البيانات المتعين فحصها.

---

[1] محمد حماد مرهج الهيتي، المرجع السابق، ص 214.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 83.

[3] علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي**، ص20، مقال منشور على شبكة الانترنت: https://www.mohamah.net/law/تاريخ الدخول الى الموقع: 2021/05/05 على الساعة: 10:46.

كل هذا كان من المعوقات التي تدخل في إطار إثبات الجريمة الالكترونية، ولذلك كان لزاما علينا التطرق لمختلف هذه الصعوبات، وذلك من خلال الاتي:

أولا/ غيـــــاب الدليـــــل المـــــــرئي:

ان هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات المكتوبة، بل على نبضات الكترونية غير مرئية لا يمكن قراءتها الا بواسطة الحاسب، فالدليل في الجريمة التقليدية مرئي على العكس من الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة.[1]

وكما هو معلوم ان اغلب البيانات والمعلومات التي يتم تداولها من حاسب الى آخر تكون في هيئة رموز ونبضات وعادة تكون مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها او فهمها الا بواسطة الحاسب الآلـــي[2].

لعل خفاء وعدم ظهوره في الجريمة المعلوماتية يجد سنده في ان هذه الجريمة قائمة على معلومة يتم سرقتها او الاحتيال عن طريقها او تزويرها، وبمعنى اخر ان هذه المعلومة هي الوسيلة لاقتران الجريمة والتي تخلف اثر ماديا فيما بعد، لهذا يجد الفقه الجنائي صعوبة في التسليم بكونها موضوعا للسرقة او اعتبارها من قبيل المال الذي يمكن سرقته، ذلك ان المعلومات ليست من الأشياء لانها ليست من المنقولات، كما لا ترد عليها الحيازة ولا تنتقل بالاختلاس[3].

---

[1] ميسون خلف حمد الحمداني، **مشروعية الادلة الالكترونية في الاثبات الجنائي**، مجلة كلية الحقوق، المجلد 18، العدد 2، كانون الثاني، جامعة النهرين، 2016، ص215، مقال منشور على شبكة الانترنت:
https://iasj.net/iasj/search?query=au تاريخ الدخول الى الموقع: 2021/05/05 الساعة: 11:00 .

[2] عبد الرحمن محمد بحر، **معوقات التحقيق في جرائم الانترنت** (دراسة مسحية على ضباط الشرطة في دولة البحرين)، رسالة مقدمة الى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجيستر في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، 1999، ص27.

[3] ميسون خلف حمد الحمداني، المرجع السابق، ص2016.

ولا يوجد شك في أن إثبات الجرائم التي تترك أثار ملحوظة يكون سهلا ميسورا، على العكس في اثبات الجرائم التي تقع على الامور المعنوية، لان اثباتها يكون في منتهى الصعوبة، لكونها لا تترك ورائها اي اثر قد يدل او يكشف عنها.

ثانيـــــا/ سهولـــة إخفـــاء الدليـــل:

من الصعوبات التي يمكن أن تعيق إثبات الجريمة المعلوماتية سهولة إخفاء الجناة لأدلة الإدانة او محوها او تدميرها، اذ يستخدمون في ذلك التلاعب غير المرئي في النبضات والذبذبات الالكترونية التي يتم تسجيل البيانات عن طريقها.

ومما يزيد من إمكانية وسهولة إخفاء هذا الدليل المتحصل من الوسائل الالكترونية، انه يمكن محوه في زمن قصير جدا قد لا يستغرق أكثر من دقائق، وربما بعض أجزاء الدقيقة، بحيث لاتتجاوز تلك الفترة عدد من الثواني، وبشكل لا يمكن للسلطات اكتشاف الجريمة التي ارتكبها، إذا ما علمت هذه السلطات وقوع الجريمة، وبالتالي عدم استطاعة السلطات إقامة الدليل ضد الجاني[1].

ومن الوقائع العملية التي تؤيد ذلك ما قامت به عصابة محترفة في اختراق أنظمة الحاسب الآلي، وذلك من خلال تصميمها جهاز يمحو جميع أثار أي خطوات وتعاملات سابقة استخدمته في اختراق نظم لحاسبات خاصة بشركات معينة، وفي جميع أنحاء العالم، وكذلك ما قام به احد الجناة بإدخال تعديل على الحاسب، حيث ضمنه، وفي نطاق التعليمات الأمنية لحماية ما فيه من معلومات مخزنة، برنامج مهمته محو هذه المعلومات بشكل تلقائي، اذا ما تم اختراق المعلومات من قبل شخص غير مرخص له[2].

ثالثـــــا/ ضخامـــة البيانـــات المتعين فحصها:

يشكل الكم الهائل للبيانات والمعلومات والتي هي بحاجة الى فحص ودراسة لاستخلاص دليل الجريمة منها، احد مصادر الصعوبات التي تعيق عملية الإثبات في الجرائم المعلوماتية، حيث ان طباعة كل ما هو موجود في الدعامات الممغنطة قد يتطلب مئات الآلاف من

[1] لينا محمد الاسدي، المرجع السابق، ص269.

[2] محمد حماد مرهج الهيتي، المرجع السابق، ص 213.

الصفحات، وفي نفس الوقت قد لا تقدم هذه الأخير اي فائدة للتحقيق، ولذلك على السلطات القائمة بالضبط والتحقيق ان لا تتمتع بالخبرة الفنية في مجال الحاسب الالي فحسب، وانما لابد ان تمتلك هذه السلطات ايضا القدرة على فحص الكم الهائل من المعلومات والبيانات المخزنة على أنظمة المعالجة الآلية[1].

ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة احد السبيلين:

اما حجز البيانات الالكترونية بقدر يفوق قدرة البشرية على مراجعتها او التغاضي عن هذه البيانات كلها على امل الحصول على اعتراف بالجريمة من المتهم[2].

لذلك وفي ظل تواضع القدرات التي يتمتع بها رجال الضبط والتحقيق،كان لزاما لهذه الجهات ان تستعين بالخبراء التي تقوم على التمييز بين ما هو مفيد للتحقيق وبين ما هو خارج عن إطار التحقيق وما من شانه تعطيل سير العدالة، حيث ان الاستعانة بالخبراء خاصة في هذا الإطار قد يضع المحقق في دائرة مغلقة من المعلومات وكم هائل من البيانات، قد لا يستطيع الخروج منها، خاصة ان لم يكن مسلحا بالتقنية والقدرة والخبرة المعلوماتية[3].

فتواجد البيانات والمعلومات في الجريمة المعلوماتية يعد عائقا أمام جهات التحقيق والتي تسعى للوصول الى دليل الإثبات في هذا النوع من الجرائم ونسبتها الى الفاعل، فكلما كانت هناك بيانات ومعلومات أكثر في جهار الحاسب الآلي كلما ازداد الأمر تعقيدا للوصول الى الدليل.

رابعـــا/ لا محدوديـــة شبكـــة الانـــترنت:

من الصعوبات التي تواجه سير الإثبات في الجرائم الالكترونية، هو ان شبكة الانترنت ليس لها حدود دولية، فهي لا تعترف بتلك الحدود القائمة بين الدول، كما انها ليست مملوكة لاحد، و بالتالي فليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، فالانترنت ظاهرة

[1] لينا محمد الاسدي، المرجع السابق، ص 273.

[2] عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الالي**، ط2، دار النهضة العربية، القاهرة، 2002، ص 359.

[3] ميسون خلف حمد الحمداني، المرجع السابق، ص 227.

دولية تنعدم مركزيتها وتتساوى أمامها الدول الكبيرة والصغيرة دون المساس بسيادة الدول، ما يخلق صعوبة كبيرة امام الجهات التي تقوم بتعقب دليل الاثبات عبر هذه الشبكة[1].

فنظرا لانتشار الشبكات على مستوى العالم فانه يستحيل الحصول على دليل في حالة توزيع مسرح الجريمة بين اكثر من دولة، بسبب تعقيد الاجراءات ووجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول على دليل رقمي، كما ان سرعة مرور البيانات الرقمية عبر الشبكات في اقل من ثانية له تاثير عكسي على دليل الإدانة او البراءة[2].

المطلب الثاني: المعوقات المتعلقة بالجانب القضائي

يتزايد عدد الجرائم المعلوماتية ذات البعد الدولي، ولا سيما لان وجود مرتكبي هذه الجرائم في مكان وجود الضحية لم يعد لازما في كثير من الأحيان بالنظر الى أنهم يرتكبون جرائمهم من خلال شبكة الانترنت عبر الوطنية، لهذا أصبح من الضروري ان تتعاون السلطات القضائية دوليا وان تساعد الدولة صاحبة الاختصاص القضائي.

وعلى الرغم من كون التعاون الدولي الفعال له أهمية بارزة في مجال مكافحة الجريمة المعلوماتية، وذلك بعد ان أصبحت الأخيرة تتخطى حدود الدول، إلا أن الملاحظ في الواقع قصور هذا التعاون مقارنة بتطور هذا النوع المستحدث من الإجرام .

فالتعاون الدولي قد يكون صعبا بسبب الاختلافات القائمة في التشريعات والممارسات بين الدول وكذلك بسبب العدد المحدود نسبيا من المعاهدات والاتفاقات المتاحة للدول بشان التعاون الدولي[3].

ومن جانب اخر فانه يتزامن مع ظهور الجرائم المعلوماتية العديد من المشكلات الخاصة بتحديد القانون الواجب التطبيق والقضاء المختص بنظر تلك الجرائم.

---

[1] لينا محمد الاسدي، المرجع السابق، ص 273.

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة**، المؤتمر العربي الاول لعلوم الادلة الجنائية والطبي الشرعي، جامعة نايف العربية للعلوم الامنية، 12-2007/11/14، ص 32.

[3] فريق الخبراء المعني بالجريمة السيبرانية وتدابير التصدي لها، فينا 21/17/يناير/2001، ص 16.

وعليه سنتعرض في هذا المطلب الى المعوقات المتعلقة بالتعاون الدولي من خلال الفرع الأول، والمعوقات المتعلقة بالقانون الواجب التطبيق والاختصاص القضائي من خلال الفرع الثاني.

الفرع الأول: المعوقـــات المتعلقة بالتعـــاون الدولي.

على الرغم من كون التعاون بين أعضاء المجتمع الدولي يتقدم وبشكل مشجع بشان مكافحة الجرائم، الا انه لم يصل الى درجة تسمح بإيجاد نظام جنائي فعال يوازي التقدم التكنولوجي الذي شهده العالم، حيث ان الوسائل والتدابير المتخذة في هذا المجال وعلى الرغم من جديتها إلا أنها لا ترتقي الى مستوى التحدي التي تقرضه الجريمة العابرة لحدود الدولة.

وان كان التعاون الدولي في مجال مكافحة الجرائم المعلوماتية يعد مطلبا تسعى الى تحقيقه اغلب الدول، الا انه ثمة صعوبات ومعوقات تقف دون تحقيقه سنتعرض اليها فيما يلي:

أولا/ عدم وجود نموذج موحد للنشاط الإجرامي:

فمن بين الصعوبات التي تقف أمام التعاون الدولي بشان مكافحة الجريمة الالكترونية هو غموض المفاهيم القانونية او اختلافها، والسبب في ذلك هو عدم الاتفاق على مفهوم موحد للجريمة الالكترونية او المعلوماتية، حيث ان الاختلاف في تعريف الفعل المجرم يعد سببا في فضل الجهود الدولية في مكافحة هذا النوع من الإجرام المستحدث.

وعلى الرغم من إصدار العديد من الدول التشريعات التي تكافح الجريمة المعلوماتية، الا انه لا يمكن اعتبارها جامعة مانعة والدليل على ذلك ان المؤسسات المحلية في فرنسا والولايات المتحدة الأمريكية وكندا، تطالب في كل عام بإضافة صور وأشكال جديدة من السلوك المعلوماتي والتي لم ينص عليها في التشريعات العقابية المعمول بها في هذا المجال، وبهذا يتبين عدم وجود اتفاق عام مشترك بين الدول حول صور الجريمة الالكترونية.

فما يكون مباحا في احد الأنظمة قد يكون مجرما وغير مباح في نظام آخر، ويرجع السبب في ذلك الى طبيعة النظام القانوني السائد في الدولة و الى اختلاف العادات والتقاليد والأديان والثقافات من دولة الى اخرى بل من مجتمع الى اخر وبالتالي اختلاف السياسة

التشريعية، ولعل هذا الاختلاف قد أتاح الفرصة لمرتكبي الجرائم المعلوماتية على تنظيم أنفسهم وارتكاب الجرائم بشكل عابر للحدود الجغرافية[1].

ثانيـــــا/ تنوع واختـــــلاف النظم القانونية الإجرائيـــــة:

إن اختلاف النظم الإجرائية التي يتم إتباعها في البحث والتحري والتحقيق في الجرائم الالكترونية او المعلوماتية يعد احد المعوقات التي تقف أمام التعاون الدولي، والسبب راجع لكون الإجراءات التي تثبت فائدتها وفعاليتها في دولة ما قد تكون غير ذي فائدة في دولة أخرى،و قد لا يسمح للجهات المختصة بالتحقيق بإجرائها أصلا، كما هو الحال بالنسبة للتنصت، والمراقبة الالكترونية، والتسليم المراقب، وغيرها من الإجراءات الشبيهة.

فإذا ارتكبت الجريمة المعلوماتية بين أكثر من دولة، فان الدولة الأولى ستصاب بالإحباط لعدم قدرة السلطات المختصة القيام بالإجراءات اللازمة في الدولة الثانية، كما قد تمنع السلطة القضائية في الدولة الثانية قبول الدليل الذي يساعد في إثبات الجريمة لأنها ترى بان الطريقة التي تم الحصول عليه من خلالها غير مشروعة[2].

ثالثـــا/ التجريـــــم المـــــــزدوج:

ان اختلاف النظم القانونية والتشريعات العقابية لها دور بارز في مجال وضع العوائق امام تحقيق التعاون الدولي في مجال الجرائم المعلوماتية، حيث ان اشتراط تجريم ذات الفعل في التشريعات الوطنية هو من اهم الشروط، خاصة في نطاق تسليم المجرمين والذي تشترطه اغلب التشريعات الوطنية و الصكوك الدولية المعنية بتسليم المجرمين[3].

الا انه من جانب آخر، نجد أن معظم الدول لم تصدر التشريعات التي تعالج أو تضع الآلية المناسبة لمحاربة الجريمة الالكترونية، وهنا كان من الصعوبة أن يتم تحديد ما اذا كانت النصوص التقليدية لدى الدولة المطلوبة منها التسليم، يمكن ان تطبق على الجرائم الالكترونية

[1] لينا محمد الاسدي، المرجع السابق، ص253.

[2] براء منذر كمال عبد اللطيف، ناظر احمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.

[3] لينا محمد الاسدي، المرجع السابق، ص 256.

أم لا، وهذا بالطبع الذي يعوق الاتفاقيات الدولية في مجال تسليم المجرمين، وهذا الأمر الأخير ينعكس بشكل سلبي على إجراءات جمع الأدلة وملاحقة ومحاكمة الجناة في الجرائم المعلوماتية.[1]

رابعـــا/ الصعوبات الخاصة بالمساعدات القضائية:

من صور التعاون الدولي في المجال القضائي، هو طلب المساعدات القضائية الدولية، ومنها على سبيل المثال الإنابة القضائية والتي تعتبر من أهم صور التعاون الدولي في المجال الجنائي، إلا أنها عادة ما تتم بين الدول بالطرق الدبلوماسية ما يجعلها تتسم بالبطء في إجراءاتها بالإضافة الى تعقيدها.

ان من الصعوبات الكبيرة التي تواجه المساعدات القضائية الدولية هي التباطؤ في الرد، إذ أن الدولة التي تتلقى طلب المساعدة عادة ما تكون متباطئة في الرد على هذا المطلب، والسبب يعود في ذلك، اما الى نقص عدد الموظفين المربين او صعوبات لغوية او الاختلاف في كيفية الإجراءات بين الدوليتين [2] .

خامســـا/ عـــدم وجـــود قنـــوات اتصـــال:

ان أهم الأهداف المرجوة من التعـاون الدولي في مجال الجريمة والمجـرمين، الحصـول على المعلـومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزامـا أن يكون هناك نظـام اتصال يسمح للجهـات القـائمة على التحقيـق بالاتصـال بجهات أجنبية لجمع أدلة معينة أو معلـومات مهمة، فعدم وجـود مثل هذا النظـام يعني عدم القـدرة على جمع الأدلة والمعلـومات العملية التي غـالبا ما تكون مفيدة في التصدي لجرائـم معينة ولمجرمين معينين، وبالتـالـي تنعدم الفـائدة منه[3].

الفرع الثاني: المعوقـــات المتعلقة بالمحكمة المختصة والقانون الواجب التطبيق.

[1] جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998، ص 91.

[2] حسين بن سعيد بن يوسف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، ص 55، مقال منشور على شبكة الانترنت: http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=12005, 80014، تاريخ الدخول الى الموقع: 2021/05/05 على الساعة: 10:20 .

[3] حسين بن سعيد بن يوسف الغافري، المرجع نفسه، ص53.

إن صعوبة تحديد الاختصاص القضائي للمحكمة التي تنظر في القضية المتعلقة بالجريمة الالكترونية وعلى الخصوص المتعلق منها بالإنترنت، يعد إحدى أهم المشكلات التي تعرقل عملية مكافحة الجريمة الالكترونية او المعلوماتية، حيث ان هذا النوع من الجرائم هو الأكثر إثارة لموضوع الاختصاص على المستوى الوطني و الدولي نتيجة الترابط في شبكة الانترنت.

و ليس هذا فحسب، و إنما تبرز صعوبة أخرى تكمن في إشكالية تحديد القانون الواجب التطبيق، وذلك نظرا لعدم وجود قانون جنائي موحد يحكم الجريمة الالكترونية، اذ ان هناك العديد من القوانين المحددة للجرائم والمتعددة بتعدد الدول والتي تختلف باختلاف الأنظمة القانونية السائدة في تلك الدول.

أولا/ إشكاليـــة القضاء المختص بنظر الجرائم الالكترونية.

لقد ثـــار خلاف بين الفقه حول تحديد المحكمة المختصة في نظر هذه الجرائم، فذهب الجانب الأول منه الى أن الاختصاص ينعقد في هذه الجرائم الى محاكم الدولة التي تم فيها تحميل البيانات، كون عملية جمع الأدلة والبيانات تكون سهلة لكونها دولة المصدر، كما ان بنك معلومات محل التحميل يكون أكـــثر ثباتا.

وقد وجهت العديد من الانتقادات لأصحاب هذا الجانب يتمثل أهمها في أن بعض الأفعال قد لا يكون معاقب عليها في دولة التحميل و بالتالي يكون فعلا مباحا ولا يعاقب عليه القانون، لذلك ظهر جانب آخر من الفقه يتجه لإعطاء الاختصاص لمكان وقوع النتيجة الإجرامية لتعدد دول التحميل مما يعقد الاختصاص لأكثر من دولة مما يؤدي لضياع المسؤولية خصوصا اذا كانت دولة التحميل لا تعاقب على مثل هذه الأفعال، ولكن كان على هذا الرأي مآخذ أيضا ، حيث لم تضع في الحسبان مصلحة المتهم بان تطبق عليه قوانين الدولة التي يحمل جنسيتها مما يزيد من تكلفة المحاكمات في هذه الجرائم، وزيادة مدة واجل المحاكمة[1].

[1] أسامة احمد مناعسة، جلال محمد صايل فاضل الهواوشة، جرائم الحاسب الالي والانترنت، ط1، دار وائل للنشر، 2001، ص 211، 210.

كل هذه المبررات استدعت نشأت اتجـاه ثالث يرى بانعقاد الاختصـاص القضائي لمكان المعتـدي عليه فهو المكـان الذي تحققت فيه النتيجة الإجــرامية ومرتبط بشخص المعتــدي عليـه[1].

وقد حسم المشرع الجزائري موضوع الاختصاص القضائي بان منح القضاء الجزائري صلاحية نظر الجرائم المعلوماتية المرتكبة في الجزائر وعلى إقليمها، اذ ينعقد الاختصاص إما لمكان ارتكاب الجريمة او محل إقامة المتهم، او مكان القبض عليه.

و ينعقد الاختصاص وفقا لمعيار من المعايير المشار إليها بحسب السبق للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها، فإذا نظرت القضية محكمة محل ارتكاب الجريمة فإنها بالتالي تكون هي المختصة دون غيرها، ويكون من حقها تمديد اختصاصها بشان اتخاذ اي إجراء من إجراءات المحاكمة وهو ما نصت عليه المادة 47 والمادة 80 والمادة 329 من قانون الإجراءات الجزائية.

ثانيـــا/ إشكاليـــة تحديد القانون الواجب التطبيق:

إن الجرائم الالكترونية لا ترتبط بحدود إقليمية لدولة ما، بل على العكس من ذلك، فهي جريمة عابرة للحدود، بالإضافة الى اختلاف التشريعات والنظم القانونية من دولة الى أخرى في مواجهة تلك الجرائم، لهذا وجدت العديد من المبادئ التي تحدد القانون الواجب التطبيق.

وعليه سنبحث على معيار يتلاءم وطبيعة الجريمة الالكترونية.

1/ مبـدأ إقليميـــة النـــص الجنـــــائي:

إن القاعدة العامة المطبقة في اغلب الدول هي مبدأ الإقليمية، بمعنى ان القانون الجنائي يطبق على كافة الجرائم التي ترتكب في إقليمها أو جزء من إقليمها بغض النظر عن جنسية فاعلها او مرتكبها.

[1] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، 2014، ص 374.

وتأخذ بهذا المبدأ اغلب التشريعات على غرار المشرع الجزائري من خلال نص المادة 3 من قانون العقوبات والتي نصت على أن: " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية ".

وتطبيقا لهذا المبدأ، فان الجرائم المعلوماتية العابرة للحدود تخضع في كثير من الأحيان لأكثر من قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر، فان كلا البلدين يكون قانونه واجب التطبيق على الواقعة، بمعنى انه يتم تطبيق قانون كل دولة تحقق في نطاقها احد عناصر الركن المادي للجريمة.

كما قد يثير إشكالية ازدواجية الاختصاص حيث يختص بها القانون الأجنبي في نفس الوقت الذي تدخل في اختصاص القانون الوطني، وذلك قد يؤدي الى الإحاطة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة[1].

كما يترتب على تطبيق هذا المبدأ عدم اهتمام الدولة الا بالجرائم التي تقع على اقليمها، فلا يمتد الى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدولة، كما ان هذا المبدأ لا يتفق مع جرائم الانترنت نظرا للبعد العالمي لشبكة الانترنت وانتقال المعلومات من خلالها الشيء الذي يخلق إشكالا كبيرا في القانون الواجب التطبيق خاصة في ظل اختلاف تشريعات هذه الدول، وعدم وجود اتفاقات فيما بينها.

وعليه يبدوا أن مبدأ الإقليمية غير ملائما للجريمة الالكترونية، وهذا بالنظر لطبيعتها الغير مادية وكذلك صعوبة اكتشافها وتحديد زمان ومكان وقوعها بدقة.

2/ مبـــــدأ شخصيـــة النـــص الجنـــائي:

يأخذ هذا المبدأ وجه ايجابي ووجه سلبي، فالوجه الايجابي يعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها، أما الوجه السلبي فيعني تطبيق القانون الجنائي على جريمة يكون فيها المجني عليه ينتمي الى جنسية الدولة ولو كان الجاني أجنبيا وارتكبت الجريمة خارج إقليم الدولة.

[1] موسى مسعود ارحومة، المرجع السابق، ص18.

وقد اخذ المشرع بمبدأ الشخصية في شقه الايجابي وذلك من خلال نص المادتين 582-583 من قانون الإجراءات الجزائية، و لا يعترف بمبدأ الشخصية في الوجه السلبي.

غير أن هذا المبدأ وردت عليه قيود بصفة عامة وبالتالي فان الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج، بل لابد من علم النيابة العامة بها.

و الملاحـــظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف على جنسيته، و هذه المعلومات تعد صعبة وعسيرة في الجرائم المعلوماتية أين يستعمل الأسماء المستعارة و التشفير بالإضافة الى اللغة الصعبة والمعقدة في كشفها والتعامل معها.

ومن مخاطر تطبيق القانون الجنائي الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت أنها تؤدي الى المساس بمبدأ عدم جواز محاكمة الشخص عن نفس الفعل الواحد مرتين[1].

3/ مبـــــــدأ العينيـــــــة:

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بغض النظر عن جنسية مرتكبها، ويرجع هذا المبدأ الى المساس بسيادة الدولة.

وقد نص القانون الجزائري على هذا المبدأ من خلال نص المادة 566 من قانون الإجراءات الجزائية، كما نص القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على هذا المبدأ وذلك من خلال المادة 15 حيث ورد النص كالتالي: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية او الدفاع الوطني او المصالح الإستراتيجية لاقتصاد الوطني".

[1] بثينة حبيباتي ، معوقات مكافحة الجريمة الالكترونية، مقال منشور بمجلة العلوم الإنسانية، كلية الحقوق جامعة الجزائر 1 ،عدد 50، ديسمبر 2018، مجلد أ، ص،ص 85-97، ص 93.

وعلى هذا الأساس يطبق هذا المبدأ على الجرائم المعلوماتية إذا كانت تمس مؤسسات الدولة الجزائرية او الدفاع الوطني او المصالح الإستراتيجية للاقتصاد الوطني.

غـــير أن هذا المبدأ في الواقع يصادف العديد من المشكلات التي تعيق التنفيذ، ومنها مشكلة تعارض تطبيق القانون الجنائي وفقا لمبدأ الإقليمية في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسالة تنازع الاختصاص والقانون الواجب التطبيق بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية و الدول الأخرى التي تعـــد الجريمة من الجرائم التي ينـــاط بقضائها نظـــرها وفـــقا لمبـــدأ العينيـــة، و بالتالي فقد يحـــاكم الشخص على فعله مرتين.[1]

[1] بثينة حبيباتني ، معوقات مكافحة الجريمة الالكترونية،المرجع السابق، ص93 .

خاتمـــــة

يتجلى لنا من خلال دراستنا هذه أن الجريمة الالكترونية هي من أكثر الجرائم التي عرفها العالم الحديث خطورة فهي آفة أنتجتها الثورة التكنولوجية و المعلوماتية، حيث لم تسلم منها كل دول العالم سواء كانت متطورة أو ضعيفة، وذلك نظرا لما تتسم به من اختلاف عن الجرائم المعروفة في العالم التقليدي و يكمن تمايزها عن الجريمة الكلاسيكية بدءا بتسميتها و تعريفها وصولا إلى الأركان التي تقوم علـيها.

حيث اتسمت الجريمة الالكترونية بطبيعة خاصة وجدت صعوبة في وضع تعريف عام جامع و موحد لها ، فقد اختلفت المفاهيم حولها باختلاف الزاوية التي ينظر إليها ، فمنهم من عرفها على أنها أساس وسيلة لارتكاب الجريمة ، ومنهم من عرفها على أساس محل أو موضوع الجريمة ، و البعض الآخر على أساس شخصية الجاني ، و الأخر جمع بين هذه التعاريف، كما أن طبيعتها الخاصة تجلت في خصائصها المتميزة ، و المتمثلة في أنها جريمة عابرة للحدود باعتبارها ترتكب بواسطة الحاسوب الآلي او في مجالاته، كما تميزت بسرعة تنفيذها و التطور المتسارع في ارتكابها ، و مما أعطاها خصوصية أكثر الخصائص التي يتميز بها المجرم المعلوماتي و أشكاله ، حيث لا يلجا الى العنف كما هو الحال في المجرم التقليدي ، بل يتميز بالذكاء و المهارة و السلطة و المعرفة.

ومما سبق ذكره استخلصنا من هذه الدراسة مجموعة من النتائج يمكن إجمالها فيما يلي:

– عدم وجود مصطلح موحد للدلالة على الجريمة الالكترونية ، فهناك من يطلق عليها ظاهرة الغش المعلوماتي الاختلاس المعلوماتي، وهناك من يسميها الجريمة المعلوماتية أو السبرانية، وعلة هاته الاختلافات هو خشية حصر هذه الجريمة في مجال ضيق وكلها تصب في معنى واحد.

– عدم وجود إجماع فقهي بخصوص تعريف الجريمة الالكترونية، حيث تباينت التعريفات بين المفهوم الواسع والمفهوم الضيق.

– يلاحظ أن المشرع الجزائري لم يستقر على تسمية واحدة، حيث سمى الجريمة الالكترونية تارة المساس بأنظمة المعالجة الآلية للمعطيات للتعبير عنها وذلك في القانون 04-15، في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تارة أخرى في القانون 09-04،

ورغم هذا الاختلاف فان هاتين التسميتين تصبان في هدف واحد هو مكافحة الجريمة الالكترونية.

– تميز الجريمة الالكترونية بعدة خصائص تميزها عن الجريمة التقليدية، مع خصوصية أركان الجريمة الالكترونية مقارنة الأركان التقليدية للجرائم العادية.

انه و في ظل هذه الخصائص المميزة للجريمة الالكترونية ، وقفت القوانين و النظم القانونية عاجزة عن مكافحتها نظرا للعـــــدد الهائل من هذه الجرائم المتطورة بتطور تقنية المعلومات ، حيث أصبـــح مبـــــدا " لا جريمة و لا عقوبة الا بنص " لا يتسع لمكافحة هذا النوع من الجرائم ، بل يجب التوسع في تفسيره لإيجاد التكييف القانوني السليم للجرائم الالكترونية المستحدثة.

و ترتيبا على ذلك ، لجأت القوانين المقارنة الى تبني فكرة المساعدة القضائية والتعاون التشريعي والقضائي في مجال مكافحة هذه الجرائم ، حيث تم إبرام العديد من الاتفاقيات الثنائية والدولية من اجل إيجاد القانون الواجب التطبيق و القضاء المختص بها.

كما تم عقد الكثير من المؤتمرات والندوات في إطار مؤتمر الأمم المتحدة أو الاتحاد الأوروبي أو الإفريقي للتصدي لهذه الجرائم ذات البعـــــد العالمي.

مما سبق نخلص إلى أن المشرع الجزائري خطى خطوة هامة في مجال مكافحة الجريمة الالكترونية والحد من انتشارها، وذلك من خلال استحداث العديد من الآليات العقابية بداية بتعديل قانون العقوبات سنة 2004 ومن ثم استحداث القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي وضع من خلاله المشرع آليات عقابية تخص كلا من الأشخاص الطبيعية والأشخاص المعنوية، الا ان ما يسجل في المقابل ان هذه النصوص القانونية مازالت تعاني العديد من مواضع النقص والقصور التي فرضتها الجريمة الالكترونية في حد ذاتها والتي تتميز بالتطور الدائم والمستمر الأمر الذي يفرض صعوبة القدرة على تغطية كافة جوانبها بنصوص وإجراءات قانونية ردعية دون الحرص على تزويدها بأرضية وقاية مسبقة.

و رغم اهتمام المشرع الجزائري بالجرائم الالكترونية و بالعقوبات المقررة لها الا ان النص عليها في قانون العقوبات او في القانون 04/09 فقط لا يكفي لمواجهة الانتشار الرهيب و

التطور السريع لهذا النوع من الجرائم الالكترونية ، بل يجب إصدار قانون خاص بها حيث ينص في الفصل الأول منه على المصطلحات الخاصة بهذه الجرائم و مرتكبيها ووسائل ارتكابها نظرا لخصوصية مرتكبيها ووسائل ارتكابها وتخص الفصول اللاحقة أنواع هذه الجرائم والعقوبات المقررة لها، مع ضرورة تشديد عقوباتها نظرا للآثار السلبية التي تخلفها على أموال المؤسسات العامة وعلى خصوصية الأشخاص وشرفهم وعلى امن الدولة.

من هذا المنطلق حاولنا وضع جملة من الاقتراحات التي من شانها المساهمة في تدعيم الآليات القانونية عامة والعقابية خاصة لمكافحة الجريمة الالكترونية في الجزائر ، هذا و نختم هذه الدراسة ببعض الاقتراحات وهي كما يلي:

1. وجوب تعديـــل قانون العقوبات وقانون الإجراءات الجزائية بما يتـــلاءم مع أنواع الجرائم الالكترونية أو إصدار قانون خاص بالجرائم الالكترونية وطرق مكافحتها كما هو الحال بالنسبة لقانون الفساد رقم 06-01 .
2. إنشاء محاكم متخصصة بالجرائم الالكترونية في كل المجالس القضائية لمجابهة هذه الظاهرة.
3. ضـــــرورة تخصيص شرطة جنائيـــــة خاصة بجرائم الانترنت في كل ولاية ، مع تكوين لجان خبراء لهذا الشأن.
4. تعزيـــــز التعاون و المساعدة الوطنية و الدولية في مجال جرائم الانترنت مع فتح مجال التعاون الدولي والحرص على الاستفادة من خبرات الدول الرائدة والسباقة في مجال مكافحة الجريمة الالكترونية و الوقاية منها.
5. الحرص على تكوين كفاءات من القطاع الأمني متخصصة في مراقبة التجاوزات والكشف المبكر عن الجرائم الالكترونية خاصة وأنها جرائم غير مادية ولا ملموسة كما سبق ووضحنا، ونادرا ما يتم الكشف عنها في مراحل متقدمة من ارتكابها و إرسالهم للتكوين في كل من الولايات المتحدة الأمريكية و بريطانيا وفرنسا كدول ساهمت في مكافحة هذا النوع من الجرائم.

6. تكوين هيئة وطنية لمراقبة ومتابعة جرائم الانترنت، وتزويد البرلمان بكل التطورات الحاصلة، أي هيئة استشارية في المجال القانوني و الإجرائي في مجال مكافحة الجرائم الالكترونية.
7. توفير الحماية التامة من الدولة لمستخدمي الانترنت من مخاطر الجرائم المعلوماتية وتوفير أجهزة خاصة بذلك خاصة المعطيات ذات الطابع الشخصي للأفراد.
8. العمل في مقابل وضع الآليات العقابية على تدعيم برامج مكافحة الجريمة الالكترونية ببرامج تثقيفية يكون الهدف الرئيسي منها نشر ثقافة التعامل الالكتروني ورفع مستوى وعي الأفراد بمخاطر الانترنت للحد من التجاوزات والجرائم التي ترتكب بسبب الجهل في استخدام تكنولوجيات الاعلام والاتصال.
9. التركيز إلى جانب الآليات العقابية على وضع آليات ردعية والحرص من خلالها على فتح المجال لأصحاب الخبرات من خارج القطاع الأمني للمشاركة في هذه البرامج والسياسات والعمل في نفس الوقت على تطوير المؤسسات العمومية والخاصة الناشطة في مجال تكنولوجيات الإعلام والاتصال بصورة تساهم في خلق قاعدة أمنية الكترونية صعبة الاختراق.
10. وفي الأخير ضرورة التفكير جديا في إعادة النظر في أحكام القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي أصبح يثبت قصوره في تغطية الكثير من الجزئيات المتعلقة بالجريمة الالكترونية والتي وضحنا سابقا بأنها جريمة متجددة و دائمة التطور لارتباطها المباشر بتكنولوجيات الإعلام والاتصال التي تعتبر في المجالات سريعة التطور والتقدم و هو الأمر الذي يفرض تطور القانون الناظم للجرائم الالكترونية بنفس الوتيرة لتجنب وقوع أي ثغرات قانونية من شانها أن تفتح المجال للمجرمين للإفلات من العقاب. هذا فضلا عن ضرورة تفعيل دور الهيئات المستحدثة في مجال مكافحة الجريمة الالكترونية بصورة من شانها توسيع مساهمتها في مجال مكافحة الجريمة الالكترونية إلى جانب الهيئات الأمنية والقضائية بنجاعة وفعالية وعوض أن تكون مجرد هيئات مفرغة من أي محتوى وليس لها أي صلاحية الأمر الذي يجعلها عبء لا فائدة منه .

قائمة المصادر والمراجع

القران الكريم.

أولا/ النصوص القانونية:

1/ الدستـــــــور:

1- الدستور الجزائري

2/ القوانين الداخلية:

1- القانون رقم 04-15 المؤرخ في: 10نوفمبر 2004 المعدل والمتمم للامر 156/66 المتضمن الجرائم المساس بأنظمة المعالجة الآلية للمعطيات ،ج،ر عدد 71.

2- القانون رقم 09-04 مؤرخ في:5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، ج،ر عدد 47.

3- القانون رقم 05-10 مؤرخ في: 20 جوان 2005 المعدل والمتمم لامر 75-58 المؤرخ في:26 سبتمبر 1997 المتضمن القانون المدني ،ج،ر عدد 44، .

4- - مولود ديدان، قانون العقوبات ،الجزائر، دار بلقيس ، طبعة 2009.

5- قانون رقم 2000-03 المؤرخ في: 2000/08/05، والذي يحدد القواعد العامة المتعلقة بالبريد و المواصلات، السلكية واللاسلكية.

6- قانون رقم 08-01 المؤرخ في: 2008/01/23، المتمم لقانون رقم 83-01 المتعلق بالتأمينات.

7- القانون رقم 04-14 المؤرخ في: 10 نوفمبر 2004 المعدل والمتمم للامر 155/66 المتضمن قانون الإجراءات الجزائية، ج،ر، عدد 71.

8- المرسوم التنفيذي رقم 06-348 المؤرخ في: 5 اكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، ج،ر عدد 63.

9- الأمر رقم 66- 156 الصادر بتاريخ في: 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري،ج ر عدد 48.

10- المرسوم الرئاسي 15- 261 المؤرخ في: 08 اكتوبر 2015 ،ج ر عدد 53 المحددة لتشكيلة و تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.

ثانيـــا/ الكتـــــــب:

1/ الكتب العامـــة:

1- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط18 ، 2019 .

2- أحسن بوسقيعة ، قانون العقوبات في ضوء الممارسة القضائية ، برتي للنشر ، طبعة جديدة 2015 .

3- على عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلـي ، دار الجامعية للطباعة والنشر ، بيروت ، د ط ، 1999.

4- عبد الرحمان خلفي ، محاضرات في القانون الجنائي العام، دار الهدى للنشر و الطباعة و التوزيع، الجزائر.

5- نـــائلة فريد عادل محمد قورة، جـرائم الحاسب الآلـي الاقتصادية، منشـورات الحلبي الحقوقية، الطبعة1، 2005

6- محمد زكي أبو عامر، الإجراءات الجنائية، دار منشاة المعارف، الإسكندرية، الطبعة الثانية،(د،ت).

7- إبراهيم حامد طنطاوي، سلطات مأمور الضبط القضائي، مطبعة دار التأليف، القاهرة، 1991 .

2/ الكتب المتخصصة:

1- نهلة عبد القادر المومني، الجرائم المعلوماتية،ماجيستيرفي القانون الجنائي المعلوماتي،دار الثقافة للنشر والتوزيع 1429 هـ- 2008 م، الطبعة الاولى ، الاصدار الاول ،2008.

2- خالد ممدوح ابراهيم ،امن الجريمة الالكترونية،دار الجامعة، الاسكندرية، عنوان84 شارع زكرياء غنيم الابراهيمية الاسكندرية ،2008.

3- محمد عبد الله ابو بكر سلامة، موسوعة جرائم المعلومات، جرائم الكمبيوتر و الانترنت، منشاة المعارف الاسكندرية، 2006 .

4- سامي علي حامد عباد ، الجريمة المعلوماتية و اجرام الانترنت ، ماجيستر في القانون ، دار الفكر الجامعي 30 شارع سوتر ، الاسكندرية 2008.

5- عبد الفتاح بيومي حجازي، الاثبات الجنائي في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، مصر، سنة النشر 2007 .

6- علي حسن الطوالبة، الجرائم الالكترونية، مؤسسة فخراوي للدراسات و النشر، مملكة البحرين، الطبعة الاولى 2008 م .

7- محمد علي العريان ، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الاسكندرية، 2004.

8- غنيــة باطــلي، الجريمة الالكترونيـة، دراسة مقارنة، الدار الجزائرية للنشر و التوزيع، الجزائـــر، 2015

9- أمـــير فـــرج يوســـف، الجرائم المعلوماتية على شبكـــة الانترنت، دار المطبوعات الجامعية ، امام كلية الحقوق، ت 4126869 الاسكندرية 2009.

10- علي عدنان الفيل ، الاجرام الالكتروني،دراسة مقارنة ،منشورات زين الحقوقية،الطبعة الاولى 2011.

11- عمـــر محمد ابو بكر بن يونـــس ، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية 2004.

12- احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية 2006.

13- خالد دوادي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، طبعة 2018.

14- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي 30 شارع سوتير، الإسكندرية،2013.

15- عبد الفتاح مراد، دور الكمبيوتر في مجال ارتكاب الجريمة الالكترونية، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية.

16-زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى ، عين مليلة ، الجزائر ،د ط ،2001.

17- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق ، جامعة الإسكندرية ، 2006.

18- أمـــال قـــــارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة 2، 2007.

19- خالد ممدوح ابراهيم، فن التحقيق في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2009.

20- محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، اهمم صورها، والصعوبات التي توجهها، ط1، دار المناهج، الاردن، 2005.

21- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الالي والانترنت، دار الكتب القانونية، القاهرة، 2002 .

22- لينا محمد الاسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط1، دار الحامد، الاردن، 2015 .

23- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006 .

24-عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الالي، ط2، دار النهضة العربية، القاهرة، 2002 .

25- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998.

26- أسامة احمد مناعسة، جلال محمد صايل فاضل الهواوشة، جرائم الحاسب الالي والانترنت، ط1، دار وائل للنشر، 2001.

27- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، 2014 .

28-غانم مرضي الشمري ،الجرائم المعلوماتية (ماهيتها، خصائصها، كيفية التصدي لها قانونيا)، الطبعة الاولى 2016 م- 1437 هـ ، الدار العلمية الدولية للنشر و التوزيع، عمان ، الاردن.

29- خالد ممدوح ابراهيم ،الجرائم المعلوماتية،دار الفكر الجامعي، الاسكندرية،الطبعة الثانية 2019

30-..عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، دراسة في الظاهرة الاجرامية المعلوماتية، دار الفكر الجامعي ، الاسكندرية،2008 .

31- محمد امين الشوابكة ،جرائم الحاسوب و الانترنت – الجريمة المعلوماتية- دار الثقافة للنشر و التوزيع،عمان ، الطبعة الاولى الاصدار الثالث ، 2009.

32- امير فرج يوسف ، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر و الانترنت، الناشر مكتبة الوفاء القانونية ،الاسكندرية ،الطبعة الاولى ، 2011.

ثالثـــا/ الرسائل العلمية و الملتقيـــات:

1/ الرسائل العلمية:

1-يوسف الصغير، الجرائم المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجيستر، كلية الحقوق جامعة مولود معمري، تيزي وزو الجزائر.

2-ادهم باسم نمر بغدادي ، وسائل البحث والتحري عن الجرائم الالكترونية ، اطروحة بدرجة ماجيستر في القانون العام بكلية الدراسات العليا ، جامعة النجاح الوطنية ، نابلس، فلسطين 2018.

3-داود وسيلة ، الجريمة الالكترونية على ضوء قانون العقوبات الجزائري ، كلية الحقوق و العلوم السياسية ،جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2018 - 2019

4-لعقال فريال ، الجريمة المعلوماتية في ظل التشريع الجزائري ، مذكرة لنيل شهادة الماستر في القانون العام ، تخصص القانون و العلوم الجنائية ، جامعة اكلي محند الحاج ، البويرة ، السنة الجامعية 2014 – 2015.

5-سعيد نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية ، جامعة الحاج لخضر ، باتنة 2013/2012.

6-معتوق عبد اللطيف ،الاطـــار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقـــارن، مذكرة لنيل شهادة الماجستير في العلوم القانونيـــة ،جامعـة العقيـد الحـــاج لخضر ، باتنـــة ، السنـــة الجامعية 2011 – 2012.

7-شهرة عبد القادر ، تطور التنظيم القضائي الجزائري في مكافحة الجريمة الالكترونية، مذكرة لنيل شهادة الماستر تخصص القوانين الاجرامية و التنظيم القضائي.كلية الحقوق و العلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2017- 2018.

8-ماشوش مراد، مكافحة الجرائم في التشريع الجزائري، مذكرة مقدمة لنيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، سنة 2014/2013.

9-عبد الرحمن محمد بحر، معوقات التحقيق في جرائم الانترنت (دراسة مسحية على ضباط الشرطة في دولة البحرين)، رسالة مقدمة الى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجيستر في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، 1999.

10- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الاول لعلوم الادلة الجنائية والطبي الشرعي، جامعة نايف العربية للعلوم الأمنية، 12-2007/11/14،

2/ الملتقيـــــات و المقالات و المداخلات:

1- نشناش مونيـــة ، مداخلة حول الركن المفترض في الجريمة الالكترونية ، جامعة بسكرة 2015 / 2016 – ص من 1 الى 16 .

2- نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر ، الجرائم الالكترونية ، طرابلس 24 – 25 مارس 2017 ص من 1 الى 20 .

3- جميل عبد الباقي الصغير، مدى كفاية نصوص العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الانترنت، الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، أبو ظبي من 15 إلى 2008/11/19.

4- المقدم عز الدين عز الدين ، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية ، بسكرة ، 2015/11/16 .

5- – نعيمـة دوادي، الجريمة الالكترونية (خصائصها ومجالات استخدامها، واهم سبل مكافحتها) ، جامعة علي لونيسي ، البليدة الجزائر مقال منشور بمجلة معهد اللغات المجلد 2 العدد 1 / 2020 تاريخ النشر:2020/08/20 ،ص من 45 الى 53 .

6- حمزة عشاش، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، جامعة محمد بوضياف المسيلة، مقال منشور بمجلة الدراسات القانونية و السياسية ، المجلد 06 العدد 02 جوان 2020 تاريخ النشر:05 /06 /2020 .

7- سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مقال منشور في مجلة العلوم الإنسانية ،جامعة الإخوة منتوري قسنطينة 1 الجزائر 2019 ، عدد 52 ديسمبر 2019

8- سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد .

9- هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الاجرام، جامعة بسكرة، كلية الحقوق، 2016.

10- حملاوي عبد الرحمان . مداخلة بعنوان "دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية " . جامعة محمد خيضر . بسكرة. كلية الحقوق. 2016.

11- موسى مسعود ارحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الاول حول المعلوماتية والقانون، اكاديمية الدراسات العليا، طرابلس، 28-2009/10/29 .

12- فريق الخبراء المعني بالجريمة السيبرانية وتدابير التصدي لها، فينا 21/17/يناير/2001 .

13-براء منذر كمال عبد اللطيف، ناظر احمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009 .

خامسا/ المواقــع الالكتــرونيـــة:

1- مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، انظر الرابط hrdoegypt.org/wp-content/uploads/2014/12 تقرير الجريمة الالكترونية، تاريخ الزيارة 2021/04/18 على الساعة 14:52سا.

2- موقع جزا يرس، جرائم الالكترونية تهدد امن الجزائريين، نشر في أخبار اليوم يوم 2018/04/10 من الرابط https- //www.djazairess.com/akhbarelyoum/240271 تاريخ الزيارة 2021/04/18 بتوقيت الساعة 15 سا11د.

3- إحصائيات مصالح المديرية العامة للأمن الوطني المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منشورة على الرابط: https://www.algeriepolice.dz – تاريخ الزيارة: 2021/04/28 الساعة: 10:00 .

4- علي محمود علي حمـــودة، الأدلـــــة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، مقال منشور على شبكة الانترنت:https://www.mohamah.net/law/ تاريخ الدخول الى الموقع: 2021/05/05 على الساعة: 10:46.

5- ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد 2، كانون الثاني، جامعة النهرين، 2016، مقال منشور على شبكة الانترنت: https://iasj.net/iasj/search?query=au تاريخ الدخول الى الموقع: 2021/05/05 الساعة: 11:00 .

حسـين بن سعيـد بن يوسف الغافـــري، الجهـود الدوليـــة في مواجهـــة جرائم الانترنت، ص 55، مقال منشور على شبكة الانترنت: http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=12005, 80014، تاريخ الدخول الى الموقع: 2021/05/05 على الساعة: 10:20 .

الفهـــــرس

شكر وعرفان.

إهداء.

مقدمة:.....أ-ه

الفصل الأول: ماهية الجريمة الالكترونية

المبحث الأول: مفهوم الجريمة الالكترونية 06

المطلب الأول: تعريف الجريمة الالكترونية.....06

الفرع الأول: تعريف المصطلحات و المفاهيم المتعلقة بالجريمة الالكترونية.....06

الفرع الثاني: تعريف الجريمة الالكترونية.....10

المطلب الثاني: خصائص و أسباب الجريمة الالكترونية.....19

الفرع الأول: خصائص الجريمة الالكترونية.....20

الفرع الثاني: أسباب و دوافع الجريمة الالكترونية.....25

المطلب الثالث: التطور التاريخي للجريمة الالكترونية.....29

الفرع الاول:مرحلة استخدام الحواسيب من الستينات إلى التسعينات من القرن الماضي.....30

الفرع الثاني:مرحلة استخدام الحواسيب ما بعد الثمانينات.....30

الفرع الثالث:مرحلة شيوع استخدام الحواسيب ما بعد التسعينات.....31

المبحث الثاني : مفهوم الجريمة الالكترونية في التشريع الجزائري..... 32

المطلب الأول : تعريف المشرع الجزائري للجريمة الالكترونية.....32

الفرع الأول : التعريف الفقهي.....32

الفرع الثاني: التعريف الأكاديمي.....33

الفرع الثالث: التعريف القانوني.....34

المطلب الثاني: الطبيعة القانونية للجريمة الالكترونية.....36

المطلب الثالث: أركان الجريمة الالكترونية في التشريع الجزائري..... 38

الفرع الأول: الركن الشرعي للجريمة الالكترونية.....38

الفرع الثاني: الركن المادي للجريمة الالكترونية.....43

الفرع الثالث: الركن المعنوي للجريمة الالكترونية.....52

الفصل الثاني: الجريمة الالكترونية بين المعالجة و المعوقات

المبحث الاول: معالجة الجريمة الالكترونية في التشريع الجزائري.....58

المطلب الاول: تجريم الأعمال الالكترونية في التشريع الجزائي الجزائري 58

الفرع الاول: تجريم الاعمال الالكترونية في قانوني العقوبات و الاجراءات الجزائية.....58

الفرع الثاني: القوانين التي نصت على الجريمة الالكترونية في الجزائر.....61

المطلب الثاني: قواعد الاختصاص و الإجراءات الخاصة بمتابعة الجريمة الالكترونية.....64

الفرع الاول:قواعد الاختصاص النوعي والمحلي في الجريمة الالكترونية حسب القانون الجزائري.....65
الفرع الثاني:قواعد المتابعة الخاصة بالجريمة الالكترونية حسب القانون الجزائري.....67
الفرع الثالث: إجراءات متابعة الجريمة الالكترونية في التشريع الجزائري.....69
الفرع الرابع: إجراءات المتابعة في مرحلة التحقيق التمهيدي أمام الضبطية القضائية.....69
الفرع الخامس: إجراءات المتابعة في مرحلة التحقيق القضائي.....74
الفرع السادس: إجراءات المتابعة في مرحلة المحاكمة.....75
المطلب الثالث: الآليات المختصة في متابعة الجريمة الالكترونية في التشريع الجزائري.....77
الفرع الاول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....78
الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.....80
الفرع الثالث: المعهد الوطني للأدلة الجنائية وعلم الجرائم.....81
الفرع الرابع: المديريـة العامـة للأمـن الوطـني.....82
المبحـث الثـاني:معوقات مكافحة الجريمة الالكترونية و انعكاسها على التشريع الجزائي الجزائري.....85
المطلب الاول: المعوقات المتعلقة باكتشاف و إثبات الجريمة الالكترونية 87
الفرع الأول: معوقات اكتشاف الجريمة الالكترونية.....87
الفرع الثاني: معوقات إثبـات الجريمة الالكترونية.....91
المطلب الثاني: المعوقات المتعلقة بالجانب القضائي.....95
الفرع الأول: المعوقـات المتعلقة بالتعـاون الدولي.....96
الفرع الثاني: المعوقـات المتعلقة بالمحكمة المختصة والقانون الواجب التطبيق.....98
خاتمة.
قائمة المصادر والمراجع.
الفهرس.
ملخص الدراسة.

ملخص:

يعرف العصر الحالي العديد من التطورات العلمية، ومن بينها التطور الحاصل الذي تشهده الثورة المعلوماتية و الالكترونية والانتشار الواسع للشبكة العنكبوتية، والتي ساهمت بشكل كبير في تطور العديد من مجالات الحياة. غير انه في المقابل أنتجت هذه الثورة نمط جديد من أنواع الجريمة وهي الجريمة الالكترونية والمعلوماتية، وهي جريمة تمس في صميمها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول فتسارعت العديد من الدول لإيجاد الحلول لها من خلال التشخيص العلمي الدقيق لمختلف العوامل الكامنة وراءها والتعرف على مختلف الاستراتيجيات والآليات التي تؤدي إلى الحد منها، ومن هنا يقترح الباحث مداخلة نتطرق فيها إلى استعراض جملة من المفاهيم المتعلقة بالمشكلة والمتمثلة في مفهوم الجريمة الالكترونية لدى مجموعة من العلماء. وتعريفها في التشريع الجزائري، وكذلك خصائص هذا النوع من الجرائم ومرتكبها، بالإضافة إلى مجالات استخدامها، وأخيرا أهم الآليات والسبل التي يمكن استغلالها من اجل التصدي لها.

مما لا شك فيه أن الصعوبات التي تعترض سبل مكافحة الجريمة المعلوماتية متعددة، وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمه للعدالة، أو خلال ملاحقة الجناة وكشف جرائمهم عبر الحدود.

لذلك تثور العديد من المشكلات والتي تقف عائقا أمام مكافحة الجريمة المعلوماتية، منها ما يتعلق بالكشف عن الجريمة المعلوماتية، كما قد يبرز للوجود صعوبات متعلقة بالتعاون القضائي الدولي وتحديد قواعد الاختصاص.

الكلمات المفتاحية: الجريمة الالكترونية، أنظمة المعالجة الآلية للمعطيات. صعوبات مواجهة الجريمة الالكترونية – اكتشاف واثبات الجريمة الالكترونية – التعاون الدولي في مجال الجريمة الالكترونية.

Abstract :

The current era is known for many scientific developments . one of wich is development in the information and electronic revolution and high prevalence of the web that contributed greatly to the progress of many areas of life. On the other hand , this revolution produced a new type of crime, namely electronic or informatoin crime. The latter, at its core, affects the fundamental values of individuals, institutions and even countries. Consequently, many countries have accelerated to find solutions through accurate scientific diagnosis of the various factors behind it, and identify the different strategies and mechanimsms to reduse it. This research paper attempts to describe cybercrime and provide definitions and related concepys set by scholars, and its definition in the Algrian legislation. The paper also illustrates of this crime, its perpetrators, areas of use and the most important mechanisms and ways to confront it.

Undoubtedly, there are many problems hampering the process of fighting cybercrime . Thay are all due to the fact that these crimes are totally diffrent from ordinary crimes. This raises some legal and operational challenges for the systems in charge of its fight. The challenges may intervene at the stage of gathering evidence and investigating through the virtual space to detect criminals and prosecute them, or at stage of tracking criminals and detecting their crossborder crimes.

Thus , many problems arise in the way of fighting cybercrimes, some of them are related to the detection of the crime and the identification of criminals and other are related to proving the cybercrime. Other problems may arise in relation to difficulties in the international judicial cooperation and the determination of jurisdictional rules.

Key words : Cybercrime, Automatic data processing systems.

– difficulties in fighting cybercrimes – detection and confirmation of cybercrimes – international judicail cooperation in matters of cybercriminality.