جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة لنيل شهادة ماستر في القانون

تخصص: قانون جنائي وعلوم جنائية

والموسومة بـ:

المكافحة الموضوعية للجريمة الالكترونية في التشريع الجزائري

من إعداد الطالبتان:

- بن بوجمعة نجلاء سرور
- بن قيط سارة

إشراف الأستاذة :

الفحلة مديحة

أعضاء لجنة المناقشة:

د/ النحوي سليمان	رئيسا
د/ خطوي مسعود	مناقش
د/ فحلة مديحة	مشرف

2024/2023

قال الله تعالى " فاذكروني أذكركم و أشكروني و لا تكفرون " و عملا بقوله صلى الله عليه و سلم: " من لم يشكر الناس لم يشكر الله "

الحمد لله العظيم الكريم أحمده وأشكره وأسترضيه على فضله وجزيل بذله، الذي وفقني لإنجاز هذا العمل.

أتقدم أولا بالشكر الجزيل إلى من مد يد المساعدة وساهم معنا في تذليل ما واجهنا من صعوبات الأستاذة المشرفة " " ذات القلب الحنون والصوت الرنان على مساعدتها لنا دون أن تبخل علينا بتوجهاتها ونصائحها القيمة، ولها منا خالص التقدير والاحترام كما نتقدم بالشكر إلى كل أساتذتنا الكرام طول مسارنا العلمي منذ كان وبالأخص أسرتي الجامعة القانونية كما نتقدم باسمي الطلبة نجلاء سرور وباسم زميلتي سارة نتقدم بأحرى الثناء والاطراء الى الأساتذة:

قاوي، عبدي، طهاري، خضرون، بركات، بوحاق، بوقرين، رابحي، خطوي، بالحسن، ملياني.

ونشكر كل من ساعدنا من قريب أو من بعيد ولم نذكره .

إهداء

" و قضى ربك ألا تعبدوا إلا اياه و بالوالدين احسان "

الحمد لله رب الفضل والنعمة على توفيقه لنا لبلوغ قدر من حكمة، فأي أبواب الثناء سندخل وأي أبيات الشعر سنشعر وأي الأسطر ستكفي وتقدر ثم أي الأقلام ستحظى وأي الكلمات ستوافي وتعبر.

أتفضل الى الجوهرتين النفيستين والداي الكريمين عبارات شكري التي لا توافيكم وحروف الحب لا تساوي عطائكم ومساعيكم مهما تغنت بكم نفحات النسيم وأريج الأزاهير لن تتم اطراء حبكم لنا ولا قدر دعاويكم.

بذرة تعبكم وتربيتكم زرعتموها واليوم في ابنتكم البكر أنتم تحصوها أول خريجة لأهلها اليوم باذن ربها ستنقش على هيئتكم الفخر والسرور ان شاء الله طول الدهور

الى أبي سندي ومسندي، عزوتي ومعزتي، رفيقي وقدوتي.

الى منبع الجب والعطاء الى مفتاح الجنة اخرتي ودنياي الى أمي الماسة النفيسة وهبة الباري أدام الله عزكم وأطال في بركة أعماركم وأدام لي عطائكم طول الدهور والعصور وعملي هذا أهديه لكم عطرا بين باقات الزهور.

الى اخوتي التوأمين الى أختي وعائلتي بوجمعة ودندان.

بن بوجمعة نجلاء سرور

إهداء

الى أمي وأبي، أهدي اليكما تمرة تعلمي، هذا العمل هو نتاج تضحياتكما ودعواتكما.

فأنتم من أوقدتم شعلة العلم في، شكرا على كل ما قدمتماه لي من علم ومعرفة، أدعو الله أن يوفقكما وأن يجزيكما خير الجزاء.

وأن يمنحكما الصحة والسعادة.

الى أمي التي غرست في حب العلم والسعي نحو النجاح والتي علمتني معنى المثابرة والصبر.

أدعو الله أن يحفظكما وأن يمنحني القدرة على رد الجميل

وكذلك اخوتي أدامهم الله وحفظهم والى خالتي التي أعطتني يد العون وساعدتني في هذه المذكرة.

والى زميلتي في المذكرة لما قدمته من مساعدة في كل مرحلة من مراحل هذه المذكرة والى أستاذتي المشرفة الفحلة مديحة لتفضلها بالاشراف

ولكل من له يد العون من قريب وبعيد.

بن قيط سارة

مقدمة:

الإنسان مخلوق كرمه الله بالعقل والوجدان بهما استطاع المضي في الحياة بكل ثقه واتزان وبالرغم من كل التحديات التي قد تمت مواجهتها إلا أننا وصلنا الى ما لم يكن متوقعا حدوثه في زمن كان فيه الناس همهم الوحيد لقمة العيش ومسكن يحيطه الأمان مهما انجر عن ذلك من أثمان تبسط فيه سلطة القوي على الضعيف المهان وبذلك ظهر مصطلح الجريمة والاجرام موضوع يعبر في طياته عن الانحراف عن مسار المقاييس الجماعية التي تتميز بدرجة عالية من النوعية الجبرية والكلية ابتغاء تحقيق تلك الرغبات الشخصية ما يترتب عنها اقتراف سلوكات مادية إجرامية تنافي المبادئ والأسس الاجتماعية حيث مرت هذه الأخيرة بعدة مراحل وأطوار تلازمت مع تطور نمط حياة الأفراد.

فمع تطور الأزمنة والعصور أضحت الخدمات بالتقدم والازدهار وسيما اهتمام كل فرد منا إلى بناء ذاته والنمو باجتهاداته بما يناسب أسس مبتغياته سواء من الناحية العلمية أو العملية الروتينية أو المستقبلية هذا من انجر عنه القيام بمستوى الفطنة والنضوج للإنسان مستحضرا في طياته عدة اختراعات وابتكارات اقتحمت الحياة اليومية لجلب المجتمعات حيث بلغت ذروتها بعد انبثاق فكره الثورة الصناعية وتباعيتها التكنولوجية ما أحدث انتفاضة هائلة تجسدت في عالم يتسارع فيه ازدهار الخدمات متباينة الأنواع والسمات بشكل غريب مريب لتصبح ضرورة لا غنى عنها من الضروريات بعد أن كانت من الكماليات اختزلت جل المسافات والأزمان لتصبح مجتمعا يعيش بين أربعة جدران تحيط بنا كل من العولمة التكنولوجيا التقدم والابتكار

ومع استبيان غرة القرن العشرين كانت جل دول العالم تشهد رقي غير مسبوق في مختلف المجالات والميادين نتج عنه ظهور طفرة جديدة تسمى بالمعلوماتية تقنية إلكترونية تجاوزت كل المعارف التقليدية التي تعتبر سمة العصر الانتقالية والمقياس الذي يحدد مدى تقدم المجتمعات البشرية إذ أضحت أجهزة الكمبيوتر والهواتف الذكية على رأسهم الشبكة العنكبوتية من الضروريات المعيشية التي كان لها فضل تسهيل وتيسير الاتصالات والمعاملات البشرية بمختلف أقطار الدول اللغات العالمية حيث أنه كما كان هناك ما يسمى بالثورة الصناعية ظهرت انتفاضات أخرى شاملة تجتاح العالم الآن ألا وهي الثورة المعلوماتية والتي ارتقت بالإنسان من عصر الصناعة إلى عصر الرفاهية الإلكترونية.

وتماشيا مع هذا العصر كان لزاما عن الدول ضمان نهضتها مواكبة هذا التقدم التكنولوجي بغض النظر عن الجانب الآخر الذي يخفيه هذا التقدم من سوء استغلال لهذه التقنيات وإساءة استعمال تلك المعلومات بما يخدم الأهداف الإجرامية لطائفة معينة يصطلح عليهم تسمية مجرمي المعلوماتية فئة حاولت هي الأخرى الاستثمار من هذا الازدهار التقني من استخدام

الفكر والسلوك الإجرامي ليشهد بعدها الفقه الجنائي ولادة جيل جديد من المجرمين المستحدثين التي لا تمد بأي صلة للمجرم التقليدي الذي يتخذ من الفضاء الافتراضي مسرحا لسلوكاته معبرا من خلالها عن غضبه ثأره وانتقامه وحتى ابتغاء اثبات مهاراته التقنية والمعرفية وبما أن هذه الافعال تعد من الجرائم العصرية المستحدثة فقد تزامن ظهورها مع ظهور أعظم اختراع في العالم الحديث ألا وهو الحاسب الآلي وشبكة الإنترنت وهي إفرازات لما نعيشه اليوم من ثورة إلكترونية رقمية فبالرغم من حداثتها إلا أنها تشكل تهديدا حقيقيا لاقتصادات الدول وخصوصيات أفرادها فمع تدفق هذا الكم الهائل من سيول المعلومات أصبح من الصعب إدراك حجمها قدرتها وتنوعها في عالم افتراضي غامض أعماق.

واستفادة لما سبق ونتيجة لتأثر الجزائر بإفرازات الثورة التقنية وتباعياتها التكنولوجية الجريمة لم يبقى المشرع أيضا عن هذه التحولات الجارية في مجال تكنولوجيا المعلومات التي مست جل الخصوصيات لمختلف الفئات والمؤسسات وحتى سيادة الدول وسرية المعسكرات ومع هذا التصعيد الغير مسبوق كان لابد من تكاتف المجهودات العالمية والقوانين المنتجة التقنية لصد وردع هذه السلوكات الإجرامية وتلبية لهذه الاحتياجات وعلى غرار باقي الدول والتشريعات لجأ المشرع الوطني والجزائري هو الآخر إلى بناء أسس للتصدي لهذه الظاهرة الشاملة تداركا للفراغ التشريعي القائم في مجال الاجرام الإلكتروني والاستعانة بمختلف الآليات القانونية الخاصة منها والعامة مجابهة لهذه الظاهرة الإجرامية واحتوائها ومراعاة طبيعتها المتميزة فأمام قصور القواعد التقليدية في التصدي لهذه الجريمة وجد المشرع نفسه أمام حتمية استحداث تلك القوانين بما ينسجم مع حداثة هذا التجريم من إضافة إلى استحداث تقنيات خاصة متخصصة لمواكبة هذا التنوع المستحدث من الاجرام، والتي من خلالها قد يتسنى له سن أحكام رادعة ووقائية وبغية الحفاظ على المصالح التقنية الإلكترونية لمختلف الفئات الشخصية منها والدولية وضمان سلامته وأمن الفضاء الرقمي في العالم الافتراضي.

وعلى ضوء ما سبق تبرز أهمية دراسة هذا الموضوع المستجد المتمثلة في الجرائم المعلوماتية وليدة العصر مواكبة لجل تطورات أساليب هذا الدهر ومهما أحيط بها من دراسات فإنها لا توافي ولم تغص في أعماق تقنياتها وأساليب ارتكابها من طرف من يقف وراءها وكيف كان للتشريعات الوطنية دورا في مواجهتها والصعوبات الكامنة في تطبيق النصوص التقليدية على هذه الجرائم العصرية بغية تحليل الإستراتيجية التشريعية الوطنية ومواكبتها لمتطلبات عصرنا الحالي من الناحية العلمية والعملية وما ينجر عنها من تباعيات جد وخيمة بأساليب ناعمة وبسيطة.

- الرغبة الملحة لتفسير وتحليل طيات هذا الموضوع

- محاولة التقصي عن حيثيات وعناصر هذا الموضوع بين طيات القانون الوطني

- الرغبة في الكشف عن أساليب تواكب ابتكار ازدهار هذه التقنيات التكنولوجية

- الإحاطة بالمنحنيات الخفية للجريمة الإلكترونية من خلال النظام الجزائري

عدم وجود اجتهادات قضائية تساعد في تحليل بعض النصوص الغامضة القانونية الافتقار لتطبيقات عملية في هذا المجال خاصة من الناحية الوطنية لإضفاء لمسة تمثيلية على أساس القوانين الوطنية، وفي سبيل تحقيق مبتغيات دراستنا بما يتناسب والطابع التقني لموضوعنا سنطرح الإشكالية الجوهرية المحورية المتمثلة في إلى أي مدى كانت مجابهة الشارع الوطني للجريمة الإلكترونية ناجحة ؟ وتندرج تحت هذه الإشكالية مجموعة من الفرضيات نجملها فيما يلي :

- ما هي الجريمة المعلوماتية

- كيف ساهمت التقنيات مختلفة في مكافحة الجرم المعلوماتي

- هل تعتبر الإجراءات والتدابير المتاحة كفيلة لمواجهة هذه الجرائم المعلوماتية

وللإجابة على هذه الإشكاليات وتلك التساؤلات فقد ارتقينا إلى تقسيم دراستنا القانونية إلى فصلين الفصل الأول فصل تمهيدي جاء تحت عنوان المدخل الجريمة الإلكترونية من خلالها تطرقنا إلى مبحثين المبحث الأول خصص لماهية هذه الجريمة المستحدثة كيف ظهرت أبرز مميزاتها و تصنيفاتها ثم تطرقنا إلى أبرز الاستثناءات الخاصة بأركانها أما المبحث الثاني جاء بعنوان ماهية المجرم المعلوماتي هذا المجرم من خلال هذا المبحث غصنا في أعماقه للتعرف أكثر عن طبيعته الشخصية ودراسة تلك الفئات الجرمية التي يتبناها إسمه أهم سماته دوافع إجرامه أما عن الفصل الثاني فهو ذلك الفصل العملي والنظري والذي أدرج تحت عنوان المكافحة التشريعية للجريمة المعلوماتية حيث انشطر هذا الأخير إلى مبحثين أساسيين حتى تناولنا في المبحث الأول تقنيات وآليات مواجهة هذا الاجرام الرقمي من خلال مجموعة القوانين العامة الوطنية وما تبعها من استحداثات تواكب مجال التقنية المعلوماتية ثم انتقلنا في الأخير إلى المبحث الثاني من الفصل النظري بعنوان مكافحة الجريمة بقوانين الخاصة في هذا الإطار خصصنا دراستنا القانونية المنهجية لاستقراء تلك القوانين والتقنيات المتخصصة في مجال التقنية الالكترونية وكيف تشعب في بعض المجالات العملية والحياة اليومية وحتى السيادة الوطنية للدولة كل ذلك بغية ضمان الحماية الرقمية للأنظمة الإلكترونية داخل بحر التقنيات السيبرانية.

ولبلوغ أهداف الدراسة تم الاعتماد على مجموعة من المناهج العلمية التي ساعدت في بلورة هذه الدراسة القانونية تمثلت في كل من المنهج الوصفي والمنهج التحليلي واللذان يتناسبان وموضوع الدراسة من حيث توضيح وتبين أسس هذه الجريمة المعلوماتية ومن يكون مرتكبها، من خلال إبانة مبتغياته سماته وحتى دوافعه وفي أثناء ذلك نستطيع إيضاح الصورة متكاملة للجريمة المعلوماتية والمجرم الإلكتروني بالإضافة إلى تحليل الإستراتيجية الوطنية التشريعية وكل القوانين الخاصة والعامة الجلية ويمكننا إكمال ذلك بدون اعتماد على المنهج الاستقرائي والذي كان له دور استقرائنا واطلاعنا على فحوى ومضمون القوانين الوطنية في الإطار العام أو الخاص منها وكيف كانت مجابهة الشارع الوطني للجريمة في حد ذاتها أو لمرتكبيها.

الفصل الأول

مدخل الى الجريمة الالكترونية

الفصل الأول: مدخل الى الجريمة الاكترونية

لقد اضحى بروز وانتشار الخدمات التقنية المعلوماتية من السمات المألوفة في العصر الحالي عصر التطور والازدهار وفي ظل هذا التقدم أتاحت الثورة الصناعية والتكنولوجية استحداث وسائل وكذا سبل للتعايش بروتين السهل الممتنع بدون بذل أي جهد يذكر عن طريق الحواسيب الآلية والشبكة العنكبوتية ورغم كل ما قدمه هذا المجال للجنس البشري في جل مجالات الحياة إلا أن إساءة الاستخدام والاستغلال جعلت من هذا التقدم التكنولوجي احدى اخطر الأوجه السلبية التي نتجت عن التقدم السريع الذي يمس بغالبية المجالات العلمية والحياتية في العصر الحالي وما جعل طائفة من المجرمين يحاولون الاستفادة من هذا التقدم التقني وتبعا لذلك فإنه من البديهي ظهور أنماط مستحدثة من الجرائم غير مسبوقة العهد ومنه ظهر ما يسمى بالجرائم الالكترونية جرائم انجرت وراء استغلال آخر ما توصلت اليه التكنولوجيا المعلوماتية وفق ما يخدم مبتغياتهم الجرمية متبنية مختلف فئات المجتمع صغار سن بالغين شباب وحتى الفئات الفاعلة في المجتمع كل تحت غطاء القدرة والمعرفة الممتازة بشبكة الانترنت والبيانات التكنولوجية المتعلقة بها ومن خلال ما سبق حاولنا في هذا الفصل التطرق إلى أهم ما يميز الجريمة المعلوماتية والمسؤولون عن اقتراف هذه الجرائم وكل هذا انشطر في مبحثين المبحث الأول الذي خصص إلى ماهية الجريمة المعلوماتية خصائصها وكيف تم تصنيفها والاستثناءات الخاصة بأركانها اما المبحث الثاني فقد خصص لدراسة الفئات الجرمية المسؤولة عن ارتكاب مثل هذه الأفعال وما الدافع الأساسي لهم.

المبحث الأول: ماهية الجريمة المعلوماتية

تنوعت أساليب ارتكاب الجريمة في الآونة الأخيرة بشكل غير مسبوق بمناسبة الازدهار التكنولوجي ما أنجب ما يسمى بجرائم الكمبيوتر وليده شبكة الانترنت جرائم شهدت صعوبة في مواجهتها نظرا للتطور المواكب لها.

وتعقدت تقنيات تفسيرها بسبب اختزالها لكل الحدود الجغرافية والحواجز الإدارية بل تعد الامر الى أن أصبح بعد المسافات واختلاف اللغات لا يعد عائقا أمام مرتكبيها كل ذلك تحت طائلة ما يسمى بالثورة العالمية التكنولوجية تضاهي في قوتها الثورة الصناعية وعلى ضوء ما سبق تم تقسيم هذا المبحث الى أربعة مطالب خصص الأول لتعريف الجريمة الإلكترونية وبيان خصائصها والثاني لتطورها التاريخي اما المطلب الثالث تم التطرق فيه لمحل الجريمة الالكترونية والرابع الاخير خصص لدراسة أركانها القانونية.

المطلب الأول : مفهوم الجريمة الالكترونية

تعددت مصادر الدراسات واختلفت غالبية التعريفات ولم يتفق الفقه الجنائي على ايراد مفهوم معين في إطار موحد للجريمة الإلكترونية فهناك تقسيمات واتجاهات عده تناول تحليل وتفسير هذه الجريمة والخوض في خصوصيتها الفريدة.

الفرع الأول : التعريف الفقهي

تباين الفقهاء بشأن التعريف الضيق والمتسع في معنى الجريمة الإلكترونية وذلك تبعا للدور الذي يقوم به النظام المعلوماتي او المعيار الذي يعتمد في التعريف كالتالي :

أولا: تعريف يستند الى أداة ارتكاب الجريمة: يرى أصحاب هذا الاتجاه انه لقيام الجريمة المعلوماتية لابد من وجود وسيلة فلا يتصور ارتكابها بدون مساعدة من الحاسب الآلي وعبر شبكة الإنترنت ما يمثل دور المساعد والمساهم الرئيسي في تنفيذ الاعتداء ومن أصحاب هذا الاتجاه الفقيه تايدمان Tiedeman «الذي عرفها على أنها كل أشكال السلوك الغير مشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب» وعرفها بعض أصحاب هذا الاتجاه بأنها الفعل الغير مشروع الذي يتورط في ارتكابه الحاسوب او هو الفعل الاجرامي الذي يستخدم في اقترافه الحاسوب كأداة رئيسة[1] وقد عرفها الاستاذ "محمد البشري" بأنها نشاط اجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة أو كهدف لتنفيذ العمل الإجرامي المقصود وعرفها "عبد الرحمن الشنيفي" بأنها أي نوع من أنواع الجرائم التي ترتكب بإستخدام الحاسوب وهي أيضا

[1] الدكتور عمار عباس الحسيني، أستاذ القانون الجنائي، جرائم الحاسوب و الانترنت، جرائم المعلوماتية، منشورات زين الحقوقية، بيروت ، لبنان ، الطبعة الأولى ، 2017 ، ص37.

اي جريمة تنطوي بطريقة او بأخرى على استعمال تكنولوجيا المعلومات والاستفادة من تكنولوجيا شبكة الانترنت.[1]

وقد كان لبعض السياسيين الدور في تعريف هذه الجريمة كما هو الحال بالنسبة لوزير الداخلية الفرنسي والذي عرفها على أنها المصطلح المستخدم لوصف جميع الجرائم الجنائية التي ترتكب عبر شبكات الكمبيوتر ولا سيما عبر الانترنت كما عرفها الأستاذان" روبرت ج. ليند كويست" "Robert Lindquist" و"جاك بولوفنا" "jack Bologne" «بأنها جريمة يستخدم فيها الحاسب كوسيلة او أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها».[2]

وقد عرف المشرع السعودي الجريمة المعلوماتية بأنها «الجريمة المعلوماتية اي فعل يرتكب متضمنا الحاسب الالي والشبكة المعلوماتية بمخالفة لأحكام هذا النظام».[3]

كما نص عليها أيضا القانون المصري والنموذجي الموحد الخاص «بمكافحة سوء واستخدام التكنولوجيا المعلومات والاتصالات والذي عرفها بأنها كل فعل مؤثر يتم ارتكابه عبر أي وسيط الكتروني».[4]

ثانيا: التعريف الذي يستند ألى المعرفة التقنية لدى مرتكب الجريمة: يرى اصحاب و أنصار هذا الاتجاه أن من أساسيات قيام الجريمة الالكترونية أن يكون الفاعل ملما بتقنية المعلومات فهم لا يعتمدون على الحاسب الآلي بل على الشخص الذي يستخدمه فبدون المعرفة المعلوماتية لا يمكنه استخدام الحاسوب ولا أن يقوم بارتكاب جريمة أصلا فقد عرفها الأستاذ "David thomson"أنها «أي جريمة يكون متطلب لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب هنا يظهر المعيار المعتمد المتعلق بالسمة الشخصية لدى الجاني إذ تتم متابعة وملاحقة مقتلف الفعل غير المشروع في حالة واحدة وهي علمه بتكنولوجيا الحاسب الآلية»[5] وتعرف موسوعة "بريتانيكا" هذه الجرائم بأنها «أي جريمة ترتكب عن طريق معرفة

---

[1] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية دراسة مقارنة ، منشورات الحلبي الحقوقية الطبعة الأولى ، 2018 ، ص44-45.

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ، الطبعة الأولى، 2022 ، ص14-15

[3] المادة 8 من النظام السعودي بشان المكافحة المعلوماتية ، 1428-2008

[4] المادة الأولى من قانون العقوبات المصري النموذجي الموحد الخاص بمكافحة سوء استخدام تكنولوجيا المعلومات

[5] مذكرة مقدمة لاستكمال متطلب طلبات اثنين شهادة ماستر أكاديمي في الحقوق، تخصص قانون إعلام آلي والانترنت جامعة محمد البشير الابراهيمي برج بوعريريج، 2022/2021 ، ص08

خاصة أو استخدام الخبراء لتكنولوجيا الحاسوب وهي الجرائم التي تتضمن أي فعل غير قانوني تكون المعرفة بتكنولوجيا الحاسوب أساسية لارتكابها وقد عرفها الاستاذ "عبد الله يوسف" بانها «الجريمة التي يتم ارتكابها اذا قام الشخص باستخدام معرفته بالحاسوب لإنجاز عمل غير قانوني».[1]

ثالثا: التعريف الذي يستند إلى موضوع الجريمة: يرى جمع آخر من الفقهاء ان تعريف الجريمة المعلوماتية لا يستند الى الوسيلة المستعملة أو الفاعل الذي يرتكبها بل تقوم على أساس موضوعها أي الأفعال الغير مشروعة التي تقع ضد الحاسبات الآلية او النظم المعلوماتية ما يؤدي الى الحاق الضرر بالمجني عليه لذلك عرفها " Kenneth Rosenblatt" بانها «نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزونة أو المنقولة بواسطة الحواسيب» كما يرى الأستاذ "محمد عوفي" بأنها الجرائم المرتكبة ضد المال المرتبط بالمعالجة الآلية للبيانات كما عرفت أيضا على أنها كل عمل أو امتناع عن عمل يأتيه الانسان إضرارا لمكونات الحاسب أو شبكات الاتصال به المحمية قانونا والمعاقب على هذا الفعل بموجب القانون»[2]

رابعا: التعريف الذي يستند إلى تعاريف متعددة: حاول أنصار هذا الاتجاه دمج عدة معايير للحصول على تعريف شامل وكامل للجريمة المعلوماتية على عكس الاتجاهات السابقة التي اعتمدت على معيار واحد وفريد لذلك نجد الفقيه"Donn parker" يعرف الجريمة المعلوماتية بأنها جميع الافعال المقترنة بالحواسيب واتصالات البيانات بوضوح يتعرض بموجبها المجني عليه او يمكن ان يتعرض فيه اي شخص اخر لخسارة لا إرادية فيما يحقق مرتكبيها أو يمكن أن يحقق مكسب وعرفت أيضا بأنها أي سلوك غير مشروع يرتكب بواسطة شبكة حواسيب أوفيها يتعلق بنظام حاسوبي أو شبكة حاسوبية بما في ذلك الجرائم من قبيل المعلومات أو عرفها أو توزيعها بصورة غير مشروعة بواسطة نظام او شبكة حواسيب».[3]

الفرع الثاني : تعريف الاتفاقيات الدولية

ذهبت المنظمة الأوروبية للتعاون الاقتصادي والتنمية إلى وضع تعريف للجريمة الالكترونية لغرض استخدامها أساسا للدراسات التي تجري في هذا المجال منذ عام 1983 بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها وقد تبنى هذا التعريف الفقيه Vllich Siber اما مكتب المحاسبة العامة للولايات

---

[1] الدكتور مشتاق طالب وهيب النعيمي، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، مرجع سابق ،ص47-48

[2] الدكتور مشتاق طالب وهيب النعيمي، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، مرجع سابق ، ص46-47

[3] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، نفس المرجع ، ص49-50

المتحدة الأمريكية فقد عرفها بأنها الجريمة الناجمة عن إدخال بيانات مزورة في الانظمة وإساءة استخدام المخرجات إضافة الى افعال اخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية».[1]

أما من جهة أخرى عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية (GCA)بأنها الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج والمعلوماتية دورا رئيسيا في ارتكابها»[2]

كما عرفت وزارة العدل الأمريكية الجرائم المعلوماتية في عام 1989 بأنها كل فعل غير مشروع تتطلب لارتكابها إلماما وعلما بتقنيات الحاسب الالي لارتكابها والتحقيق فيها ومقاضاتها.

ومن جهة أخرى عرفت منظمة التعاون الاقتصادي والتنمية والخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي كل فعل أو امتناع من شأنه الاعتداء على الأمور المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات».[3]

ولقد أخذت منظمة الأمم المتحدة في مؤتمرها العاشر لمنبع الجريمة ومعاقبة المجرمين والذي عقد في فيينا بتعريفها للجريمة المعلوماتية بأنها ايه جريمة يمكن ارتكابها بواسطه نظام حاسوبي او شبكه حاسوبيه او داخل نظام حاسوبي والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية».[4]

الفرع الثالث : التعريف القانوني

رغم انفراد الجرائم الإلكترونية بخصوصية تميزها عن باقي الجرائم التقليدية المألوفة الارتكاب إلا أنها في التشريع الوطني كانت تصنف ضمن جرائم النظام العام مثلها مثل الاختلاس وخيانة الأمانة وتكتسي نفس العقوبات المقررة لنظيرتها سابقة الذكر وذلك قبل أن يخطو المشرع الجزائري خطى التشريعات والتعريفات الحديثة من خلال تصنيف إطار قانوني يلائم طبيعة وخصوصية الجريمة المعلوماتية من خلال تعديل قانون العقوبات الجزائري لسنة 2009 الموافق ل1430هـ من خلال قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها بينما عرفت المادة الثانية الفقرة "أ"

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق ، ص40-41

[2] الدكتور مشتاق طالب وهيب النعيمي، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، مرجع سابق ، ص44-45

[3] الدكتورة خنيش دليلة ، الجريمة الإلكترونية و الأمن الاجتماعي ديوان المطبوعات الجامعية ، 2023 ، ص22

[4] ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية ، جامعة أبي بكر بلقايد ، تلمسان ، 2016-2017 ، ص24

«منه الجريمة المعلوماتية بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات واي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية»[1] والملفت للانتباه أن المشرع الجزائري اصطلح على تسمية الجريمة المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على غرار ما ادرج عليه الفقه والتشريعات المقارنة من تسميات كالجرائم الإلكترونية جرائم الانترنت الجرائم السيبرانية والجرائم المعلوماتية وذلك بهدف فتح مجال تجريم وعقاب هذا الصنف من الجرائم في القانون الجزائري الى أبعد الحدود الممكنة لأن هذه الجرائم قد تتجاوز حدود المساس أو التلاعب بالمعطيات التالية الى استعمال الوسائل الالكترونية والتكنولوجية في ارتكاب جرائم تقليدية مثال ذلك القتل من خلال فصل المريض عن أجهزة التنفس الاصطناعي والإنعاش القلبي وما إلى ذلك من أجهزة إلكترونية تساعد المريض على إبقائه على قيد الحياة كما عرفت المادة الثانية من القانون نفسه فقرتيها "ب" و"ج" كل من المنظومة المعلوماتية والمعطيات المعلوماتية على النحو التالي:

أولا: المنظومة المعلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض او المرتبطة يقوم واحد منه او اكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين

ثانيا: المعطيات المعلوماتية: أي عملية عرض للوقائع او المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها.[2]

الفرع الرابع : خصائص ومميزات الجريمة المعلوماتية

تعد الجريمة السيبرانية أو ما يطلق عليها بالجريمة الإلكترونية ظاهرة اجتماعية إجرامية معاصرة تنفرد عن الجريمة التقليدية بمميزاتها وتتشارك معها بأخرى ما أحاط بها الكثير من الغموض وذلك لطبيعتها الخاصة المرتبطة بالحاسب وأنظمة المعلومات الإلكترونية وما تتمتع به من أمور فنية وتقنيات علمية في معظم جوانبها ونتيجة لذلك اكتسبت هذه الجرائم شكل وزمرة مستحدثة ومن أبرز سمات هذه الجريمة ما يلي:

أولا: جريمة عابرة للحدود: لعل أبرز ما يميز الجريمة المعلوماتية أنها جريمة عالمية فقدت معها الحدود الجغرافية للدول سلطتها في الفضاء الشبكي متشعب المسارات ومجتمع التقنية المعلوماتية الالكتروني لا يعترف بالحدود الدولية ولا يتقيد بها فهو ذلك المجتمع المنفتح عبر

---

[1] المادة 02 منا القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة المتعلقة بالرقابة ومكافحة الجرائم المتصلة بتكنولوجيا إعلام واتصال ومكافحتها.

[2] المادة 02 من نفس القانون رقم 09-04

الزمان والمكان دون أن يخضع للجانب التقليدي في الحراسة الدولية حرس الحدود فهذه التقنية تسمح لمستخدميها بالتنقل المعنوي الافتراضي بين الدول والقارات دون أي تعقيد أو صعوبة او حتى عوائقها انطلاقا من سهولة حركة المعلومات وتبادلها وهو ما جعل من اليسر ارتكاب السلوك الإجرامي في دولة وتحققها في دولة أخرى فهي شبكة اتصال لا متناهية متاحة لأي شخص في العالم مثال ذلك جريمة تبييض الأموال وتمويلها عبر الإنترنت وسرقة البنوك دون الحاجة إلى السطو الفعلي عليها او اختراق نظام إلكتروني لقاعدة عسكرية نووية بهدف استخدام عتادها لتدمير دولة أخرى.[1]

ثانيا: جريمة هادئة قليلة المخاطرة: يعتبر ذكاء ودهاء المجرم المعلوماتي كافي لإتمام الجرم بدون الحاجة لاستخدام العنف أو السلاح كونها جرائم ترتكب في الخفاء من خلال نظام رقمي للشبكة العنكبوتية وهذا ما يجعلها تتسم بالهدوء عكس ما هو مألوف في الجرائم التقليدية والتي تحتاج إلى جهد فعلي فركنها المادي قد لا يتجاوز مجرد لمسة بسيطة لمفاتيح التشغيل الخاص بجهاز الحاسب الآلي أو ملحقاته[2] مثال ذلك من يتلقى رسالة الكترونية فبمجرد فتحها يفتك بالحاسب الآلي وبنظامه المعلوماتي لأنها تحمل بداخلها فيروس خطير.

ثالثا: جريمة خفية عن الأنظار: تعتبر هذه الجرائم شديدة الخفية مستقرة الأفعال إذ أنها ممكنة الوقوع أثناء المعالجة الآلية للحاسوب أو نظامه الداخلي وذلك بدون إدراك المجني عليه حتى ولو وقعت هذه الجريمة أثناء تواجده داخل الشبكة أو نظامه الحاسوبي الخاص بالرغم من أن الجاني يرتكب جرمه من خلال جهاز كمبيوتر مثله مثل الضحية الا أن هذا الأخير يتمتع بقدرات فنية عالية في أغلب الأحيان تمكنه من تنفيذ جريمته بكل دقة وغموض بدون معرفه مالك النظام ولعل ما يزيد من خفاء هذه الجرائم هو أن غالبية ضحاياها لا يتواصلون ببرامج وأنظمة الحماية الفنية لحماية انظمة المعلوماتية غالبا ما يمكنهم من ارتكاب جرائمهم ببرامج وتقنيات تيسر عملهم الخفي من اختراق جدران الحماية الأمنية تلك[3] من اتلاف ومحو وحذف وغيرها مثال ذلك بغية التجسس وسرقة معلومات أو شفرات خاصة وحتى تحويل الاموال إلكترونيا.

رابعا صعوبة اكتشاف وإثبات الجريمة: من مميزات الجريمة الالكترونية انها تقع في بيئة افتراضية من خلالها لا يمكن العثور على اية آثار مادية محسوسة على غرار الحالات

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق ، ص49

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ، مرجع سابق ، ص20

[3] ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، مرجع سابق ، ص61

المكتشفة فعليا بها والتي لا تكاد تذكر مقارنة بالجرائم التقليدية وذلك لعدة اسباب أبرزها الطابع التقني الذي يضفي عليها كما من الغموض والتعقيد ما يزيد هوية إثباتها كما أن نقص الخبرة الفنية والتقنية لدى الشرطة وجهل الادعاء العام وكذا القضاة إذ أن هذا النوع من الجرائم يتطلب تدريبا وتأهيل الأفراد هذه الجهات في مجال التقنية الحديثة من حيث كيفية جمع الأدلة وإجراء التفتيش والملاحقة في بيئة النظام المعلوماتي مما يجعل من الجهود المبذولة في هذا المجال غير متناسقة[1] فغالبا ما تكون فيها الأدلة نادرة وذلك راجع لطبيعة المعلومات المتواجدة على مستوى الانترنت المتكونة في شكل رموز مخزنة على وسائط ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي ما يسهل عملية اخفائها والتخلص منها والذي يتم من خلال نبضات كهربائية حيث تتغير وتسمى الدلالات الارقام المعلومات من ذاكرة الحاسب بدون صعوبة وهذا ناتج عن الانتقال من الفضاء القانوني مبني على أساس جغرافي إلى فضاء قانوني مبني على الارتباط بالفضاء الالكتروني.[2]

خامسا خطورة الجريمة المعلوماتية : تتعاظم خطورة هذه الجرائم من نواحي عدة تمس بحقوق الأفراد المؤسسات الاقتصادية وحتى أمن الدول وسيادتها وذلك حسب نوع الهدف المقصود التسلية أو الفضول وقد يكون بغرض الابتزاز أو التخريب أو الاختلاس الرقمي التشهير وتشويه السمعة ويمكن أن تزداد خطورتها أكثر إذا طالت مؤسسات مالية أو تنظيمات حكومية وغير حكومية بشكل قد يمس الأمن القومي لهذه الدول والحكومات وذلك بسبب التجسس الصناعي والعسكري أو التخريب المعلوماتي والتعرض للإرهاب السيبراني ويعزى هذا النمو الجنائي الغريب المرتبط بتكنولوجيا الاتصالات والمعلومات الى عدة عوامل أبرزها:

- النمو التكنولوجي السريع

- التوافر السهل لأدوات الجريمة وتقنيات البرمجة

- سرعة الاتصالات

- الدرجة العالية لانتشار الانترنت وزيادة الاعتماد على تكنولوجيا الحواسيب[3]

سادسا: أحجام الضحايا عن التبليغ : تتسم الجريمة الإلكترونية في الغالب بالتكتم وعدم الإعلان أو الإبلاغ عنها لدى المصالح المختصة وعدم الكشف عنها ينجم عن أسباب عدة إما لعدم اكتشاف الضحية لها أو للإكتشاف المتأخر لها أو التستر عنها لحساسية المعلومات

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق ، ص54

[2] الدكتور مشتاق طالب وهيب النعيمي، أستاذ القانون الجنائي، الجرائم المعلوماتية ، مرجع سابق ، ص28-29

[3] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية دراسة مقارنة ، مرجع سابق ، ص28

المخترقة (معلومات أمنية أرصدة مالية معلومات سرية) بالإضافة لعدم جدوى التبليغ عن ذلك صعوبة واستحالة تحديد مصدر التهديد[1] كل ذلك يتأتى من خوف الضحية وخشيته من الوقوع في الفضيحة أو التشهير خاصة إذا كانت تلك الاعتداءات تمس بخصوصية الأفراد كما أن خوف الشركات التجارية من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة من الزمن مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق عطفا على ما قد تسببت الجريمة في خسارتها أصلا والواقع ان اجراءات التحقيق الخاطئة في بعض الاحيان قد تسبب خسائر مادية تفوق تلك التي نجمت عن الجريمة في المقام الاول كما قد يكون سبب امتناع المؤسسات او الأشخاص عن التبليغ هو القلق من فقدان الزبائن وتدني ثقتهم بهم أو حتى احجامهم عن التعامل معها خوفا على مصالحهم الشخصية.

سابعا: وقوع الجريمة في بيئة الكترونية تقنية : على عكس الجريمة التقليدية فإنه يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من أجل معالجتها الكترونيا بما يمكن للمستخدم من إمكانية تصحيحها أو محوها أو تخزينها أو استرجاعها أو طباعتها و هذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية وعلى الرغم من ارتكابها أثناء أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي(ادخال معالجة أو اخراج) فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن النظر الى طبيعة ارتكابها إلا في وقت معين كما يمكن أن تتضمن مثل هذه العمليات بيانات ومعلومات على وسائط التخزين المادية مثل الأقراص الصلبة وبطاقات الفلاش للتخزين وكذا البيانات والمعلومات المخزنة في نظام البث المعلوماتي سواء السلكية أو البصرية او تردد الراديو.[2]

المطلب الثاني التطور التاريخي للجريمة المعلوماتية

بعد ظهور وانتشار جهاز الحاسوب والشبكة العنكبوتية انتقالة غير مسبوقة في حياة البشرية إذ أن التطور الهائل والسريع لتقنية المعلومات فتحت منعرجا جديدا لنشر ثقافة تكنولوجية غير مألوفة العهد بالنسبة للكثير من المجتمعات وذلك نتيجة للانفتاح الذي فرضه ازدهار العصر الحالي.

---

[1] الدكتورة شنتير خفرة، دكتورة قانون جنائي، الآليات القانونية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص 23

[2] الدكتور يعيش تمام شوفي ، سلسلة مطبوعات المنبر ، الجريمة المعلوماتية ، دراسة تأصيلة مقارنة جامعة محمد خيضر بسكرة ، الطبعة الأولى ، جانفي 2019 ، ص 26-27-28

نظام التقنية المعلوماتي مثل ما يمكن استخدامها في تحقيق مصلحة البشرية فان لها اضرار وخيمة تعد من أبرز أسباب انتشار الافعال غير المشروعة والسلوكات المنحرفة فإما ان تقع على الكمبيوتر ذاته أو بواسطة وهو ما يعد لعبة في يد الجاني يستخدمها بهذا في تحقيق أغراضه الإجرامية وهو ما يسمى بالجريمة المعلوماتية جريمة مر تطورها بأربع مراحل أساسية تتمثل في:

الفرع الأول: المرحلة الأولى في الستينات

بظهور استخدام الكمبيوتر وربطه بشبكة الانترنت في ستينات إلى سبعينات القرن الماضي برزت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر وكذا التجسس المعلوماتي حيث شكلت موضوعا للتساؤل والنقاش اذا ما كانت هذه الجرائم مجرد حاله عابره او ظاهرة إجرامية مستجدة ؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال النظم المعلوماتية ومع هذا أو ذاك بقيت محصورة في اطار السلوك اللاأخلاقي دون النطاق القانوني فمع توسع الدراسات تدريجيا خلال سبعينات القرن الماضي بدأ الحديث عنها كظاهرة اجرامية جديدة[1] يجب الأخذ بها بكل جدية

كما شهدت هذه الفترة الزمنية أيضا بداية لظهور بعض التشريعات والقوانين التي تجرم بعض الممارسات ذات الصلة بإساءة استخدام الحاسوب حيث قررت لها عقوبات محددة كما حصل في السويد التي اعتبرت بذلك أول دوله يصدر بها قانون يجرم بعض الأفعال والممارسات المرتبطة بالحواسيب ورغم استمرار تطور ظاهرة الجريمة الإلكترونية خلال حقبة السبعينات إلا أن الحالات التي سجلت في تلك الفترة الزمنية كانت جد قليلة وقد تعود أسباب تلك القلة إلى كون أن إمكانية الخطر كان داخليا ويكاد أن يكون الخطر ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطيع الوصول إلى تلك الأنظمة بصورة مباشرة ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي كما أن سبب قلتها أيضا يعود إلى عدم الابلاغ عن الكثير من تلك الجرائم لكون الشركات وكذا الوكالات كانت تحرص على عدم اهتزاز الثقة بها وبأنظمتها الحديثة.[2]

خلال سنة 1966 سجلت أول قضية في الولايات المتحدة الامريكية تتعلق بارتكاب أفعال إساءة استعمال الحاسوب أين تمت محاكمة مهندس يعمل في البنك من أجل قيامه بالتحايل

---

[1] الدكنورة خنيش دليلة ، الجريمة الإلكترونية و الأمن الاجتماعي ، مرجع سابق ، ص 24

[2] الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015 ، إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى ، عمان ، ص25-26

على برنامج الإعلام الآلي لاختلاس مبلغ مالي كما تم تسجيل عده قضايا مماثلة تتعلق بالدخول خلسة إلى الانظمة المعلوماتية للاطلاع على محتواها وكان القضاء يتعامل مع هذه القضايا على أساس قضية سرقة بالإكراه وأحيانا يعتبرها إخلالا بالتزامات المسؤولية العقدية وفي اليابان سجلت أول قضية خلال سنة 1970 تتعلق بالمساس بالأنظمة المعلوماتية على إثر اكتشاف عملية سرقة ونشر معطيات شخصية لزبائن شركة تجارية.

ونظرا لصعوبة التعامل مع هذا النوع من الجرائم بسبب خصائص البيئة المعلوماتية الإفتراضية تبلورت فكرة ضرورة وضع نصوص قانونية خاصة حيث بادرت عدة دول إلى إصدار تشريعات تجرم إساءة استعمال جهاز الكمبيوتر ونذكر على سبيل المثال:

- الولايات المتحدة الامريكية في سنة 1970 صدر أول قانون خاص بحماية البيانات وحق الوصول اليها ثم في سنة 1977 صدرت أول تشريع فيدرالي خاص بجرائم الحاسوب

- السويد في سنة 1973 أصدرت قانون المعطيات المعلوماتية[1]

- فرنسا في سنة 1978 أصدرت قانون يتعلق بالمعلوماتية والحريات[2]

الفرع الثاني: المرحلة الثانية في الثمانينات

في حقبة الثمانينات حدث تغيير ملحوظ في التعامل مع ظاهرة الجريمة الإلكترونية وذلك من جانب الباحثين والعامة على سواء بسبب ارتفاع مؤشر عدد القضايا ذات الصلة بإساءة إستخدام الحاسوب ولا سيما بعد اهتمام الصحافة وإبرازها لتلك القضايا حيث أصبح بعضها يؤرق المجتمع الدولي كقضايا الإختراق وقرصنة البرمجيات والتلاعب في أنظمة النقد الالكتروني وانتشار العديد من أنواع الفيروسات كما شهد ذلك العهد الانطلاقة الأولى للقوانين والتشريعات الخاصة بحماية البرامج الحاسوبية والتي اطلق عليها قوانين حماية الملكية الفكرية واعتبرت من القوانين الأكثر وضوحا ونضجا[3] كما أنه في الثمانينيات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والإنترنت وارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج حيث شاع اصطلاح "الهاكرز" المعبرين عن مقتحمي النظم لكن الحديث عن الدوافع لارتكاب

---

[1] الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها" مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18/01/2022, ص 04-05

[2] الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها"،االمرجع السابق ، ص05 ،تاريخ الدخول أفريل 2022

[3] الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015، مرجع سابق، ص26 تاريخ الدخول أفريل 2024

هذه الافعال ظل محظورا في رغبة المحترفين تجاوز أمن المعلومات واظهار تفوقهم التقني لكن هؤلاء أصبحوا في الاخير أداة إجرام وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة و القدرة على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والإقتصادية والاجتماعية والسياسية وكذلك العسكرية[1]

كما تم في تلك الفترة الزمنية ظهور الاهتمام العربي بظاهرة الجريمة الإلكترونية وتمثل ذلك في إصدار العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة الإلكترونية وعقد عده ندوات ذات الصلة بذلك حيث عقدت في ندوة أمن المعلومات في الحسابات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية.[2]

كما أنه في سنة 1988 أصدرت فرنسا قانون يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات GODFRAIN[3].

كما أنه في مطلع الثمانينات تبنى مجلس أوروبا اتفاقية حماية المعطيات الشخصية والمعالجة الآلية لها رقم 108.[4]

الفرع الثالث المرحلة الثالثة في التسعينات

شهدت فترة التسعينات من القرن الماضي تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بالفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات بحيث ظهرت أنماط جديدة وخطيرة في ذات الوقت ففي هذه الفترة نمت الإنترنت بشكل مذهل بعدما كانت مجرد شبكة أكاديمية صغيرة وتحولت الى بيئة متكاملة للإستثمار والعمل والانتاج وكذا الإعلام والحصول على المعلومات ففي البداية لم يكن ثمة إهتمام بمسائل الامن بقدر ما كان الإهتمام ببناء الشبكة وتوسيع نشاطها دون مراعاة تحديات أمن المعلومات فالإهتمام الأساسي تركز على الربط والدخول فلم يكن الامن من بين

---

[1] بصرة سعيدة , الجريمة الإلكترونية في التشريع الجزائري, دراسة مقارنة مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق, جامعة محمد خيضر بسكرة. 2015-2016 ، ص16-17

[2] الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015، مرجع سابق ،ص26

[3] الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها"،االمرجع السابق ، ص05

[4] الاتفاقية رقم 108 المؤرخة في 28/01/1981 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي, رابط الموقع الرسمي لمجلس أوروبا www.intcoe

الموضوعات الهامة في بناء الشبكة هذه الثغرة التي شجعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة الامر الذي أدى الى لفت النظر إلى حاجة شبكة الانترنت وتوفير معايير عدة من الأمن حيث بدأ التفكير مليا في الثغرات ونقاط الضعف وعليه قد يكون الكمبيوتر هدفا للجريمة غايته المعلومة المخزنة من أجل السيطرة على النظام دون. ... ثم السرقة والاعتداء على مختلف جوانب الملكية الفكرية.[1]

وخلال التسعينات أيضا من القرن العشرين ومع انتشار الحواسيب والاعتماد عليها في شتى المجالات الحياتية الخاصة منها والعامة حيث بدأت الجريمة الإلكترونية في النمو والبروز أكثر فأكثر حيث سجلت ظهور عدة حالات للجريمة ذات الصلة بالحواسيب كان من أبرزها جريمة السرقة بنك مينيسوتا الأمريكي في سنة 1966 والتي اعتبرت أول سرقة إلكترونية تقع على بنك وبعد ذلك توالت بعض المقالات الصحفية في الظهور متناولة بعض الحالات التي أطلق عليها آنذاك جرائم الحاسوب computer crime

أو الجرائم ذات الصلة بالحاسوب[2]computer related crime

الفرع الرابع: المرحلة الرابعة في العصر الحالي

شهدت السنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الإلكترونية حيث ارتبط ذلك بتحول شبكه الإنترنت في ذلك الوقت من شبكة أكاديمية إلى شبكة تعنى بخدمة المجالات التجارية والفردية حيث بلغ مستخدميها في عام 1996 ما يقارب ب 40 مليون مستخدم وفي عام 2014 تجاوز عدد المستخدمين أكثر من 3 مليارات مستخدم الأمر الذي أدى إلى خلق عبء كبير على المختصين بمكافحة الجريمة الإلكترونية ولذلك وجد مفهوم جديد عرفها بالجرائم العابرة حيث يستطيع المجرمون تنفيذ مخططاتهم الإجرامية في دول متعددة دون الاكتراث بأية حدود دولية.[3]

وقد استمر التطور التشريعي لمعالجة هذا النوع من الجرائم في العديد من الدول عبر العالم حيث برزت الحاجة إلى ضرورة التعاون الدولي في هذا المجال اين أصدرت عدة اتفاقيات إقليمية ودولية من بينها اتفاقية بودابست المتعلقة بمكافحة الجرائم الإلكترونية[4] حيث صادقت على هذه الاتفاقية عدة دول حيث اعتبرت الإطار الدولي الوحيد الى غاية اليوم في مجال

---

[1] الدكنورة خنيش دليلة ، الجريمة الإلكترونية و الأمن الاجتماعي، مرجع سابق ، ص24-25

[2] الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015، مرجع سابق ،ص26

[3] الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015، مرجع سابق ، ص26-27

[4] الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية ببودابست سنة 23/11/2001

مكافحة الجرائم المعلوماتية هدفها الأساسي توحيد الجهود والمساعي الدولية وتوطيد التعاون من أجل التصدي لمثل هذا النوع من الجرائم [1]ونذكر على سبيل المثال بعض الاتفاقيات الدولية والقوانين المتعلقة بهذا المجال أبرزها:

- اتفاقية الأمم المتحدة الخاصة بالجريمة العابرة للحدود الوطنية المؤرخة في 2000/15/11

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21

- القانون الغربي للاسترشاد لمكافحة جرائم تقنية المعلومات والذي اعتمدته جامعة الدول العربية[2]

قانون الانترنت بالقاهرة في سبتمبر 2004

- المؤتمر الدولي الأول قانون الإنترنت بمدينة الفردقة في أوت 2005

- القانون التونسي المتعلق بالتجارة الإلكترونية رقم 83 الخاص بالمبادلات الإلكترونية المؤرخ في تاريخ 2000/8/9[3]

المطلب الثالث: محل الجريمة الإلكترونية

تتجسد الجريمة المعلوماتية في أشكال عدة وتنسب عبر مجالات لا حصر لها تحت غطاء رقمنة وعولمة العصر الحالي ذلك ضمن نطاق ما يسمى بالمعالجة الآلية للبرمجيات الالكترونية من خلال جهاز الحاسب الآلي وشبكة الإنترنت وما ينجر عنها من تجهيزات تكنولوجية حديثة أين اتسمت هذه الاخيرة بطبيعة قانونية خاصة تختلف كل الاختلاف عما كان متعارف عليه في القواعد التقليدية ولم يتوقف الامر هنا بل انتقل الى تطور المهارات السلوكية والمعرفية والتقنية الإجرامية للجاني مما جعل معظم هذه الأفعال الغير مشروعة تشكل محل إساءة واعتداء لما يسمح به القانون ومما سبق نجد أن محل الجريمة المعلوماتية يظهر من خلال ما سنتناوله في العناصر تالية الذكر.

---

[1] الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها"،االمرجع السابق ، ص05

[2] الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها"،االمرجع السابق ، ص12 متضمن الإطار القانوني ببجريمة المعلوماتية في التشريع الجزائري الاتفاقيات الدولية و الاقليمية

[3] بصرة سعيدة , الجريمة الإلكترونية في التشريع الجزائري, دراسة مقارنة مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، مرجع سابق ، ص27-28

الفرع الاول :المعلومة كمحل للجريمة الإلكترونية

تعتبر المعلومة من ناحية كميتها ونوعيتها وكذا سرعة تدفقها سمة هذا العصر الى الحد الذي لا يمكن معه تصور نشاط اجتماعي ناجح لا يقوم على توظيف المعلومة والمعلومة هي احدى تلك المفردات المشتقة من مصدر علم ولهذه المشتقات العديد من المعاني منها ما يتصل بالعلم أي إدراك طبيعة الأمور المعرفية أي القدرة على التمييز التعليم التعلم الإحاطة اليقين الإتقان الإرشاد والتوعية وغيرها من المعارف يعود«information» مصطلح إلى أصله اللاتيني والذي يعني عملية الاتصال[1] وهو نفس ما تعنيه مفردة المقابل لها في اللغة الصينية «Xinxi» وعلى العموم فالمعلومة في أبسط تعريفاتها الاصطلاحية تعني المعطيات الأولية التي تتعلق بنشاط أو قطاع ما أما الأستاذ«parker» فقد عرفها بأنها «مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محطا للتبادل والإتصال أو التفسير والتأويل والمعالجة سواء بواسطة أفراد أو الأنظمة الإلكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة»[2]

ومنه يتجلى محل الجرائم المعلوماتية إما سرقة أو حذف أو تغيير للمعلومات والتي غالبا ما يكون لها قيمة معنوية ومادية لدى مالكها لذلك نجد المشرع الجزائري شدد العقوبة المقررة لتغيير أو حذف هذه المعلومات لما تحمله من خصوصية إتجاه صاحبها أو ذلك من خلال الفقرتين 02 و03 من نص المادة 394 مكرر من القانون رقم 04/ 15[3] وكذلك فعل المشرع الفرنسي في الفقرة الثالثة من المادة 323 من القانون الفرنسي والمشرع الامريكي حيث أصدر سنه 1974 قانون الخصوصية «PA privacy ACT» وقانون خصوصية الاتصالات الإلكترونية لسنة 1986

«COPA electtoni communication privacy ACT»

ومما سبق نفهم أن حقوق الملكية الفكرية كانت ولا زالت تحظى باهتمام عديد التشريعات فالمبادرة الأولى للمشرع الجزائري في هذا الخصوص كانت في سنه 1973 بموجب الامر رقم 1973 المتعلق بحق المؤلف[4] والذي تم إلغائه بعد ذلك بموجب الأمر رقم 10 97 المتعلق

---

[1] الدكتورة شنتير خفرة، دكتورة قانون جنائي، الآليات القانونية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص 26

[2] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص79

[3] القانون 04-15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 الصادر في 08/06/1966

[4] الأمر رقم 73-14 المؤرخ في 03/04/1973 المتعلق بحق المؤلف الصادر في الجريدة الرسمية عدد 29

بحقوق المؤلف والحقوق المجاورة حيث أنه ولأول مره يعتبران أن برامج الحاسب الآلي تعد من قبيل المصنفات المحمية قانونا إضافة إلى إدراج الحقوق المجاورة لحق المؤلف ومنحها الحماية القانونية. [1]

ونظرا لما للمعلومة من أهمية فقد أكد على ذلك الكثير من الفقهاء والدكاترة فالفرق اليوم بين مختلف المجتمعات هو في استثمارها فهي شجون الحاضر وغموض المستقبل خاصة في ظل الرهانات والمتغيرات الحالية التي أفرزت لنا مجتمعا إلكترونيا محضا انتقلت تجلياته إلى مختلف المجالات الحياتية تاركة وراءها تغييرا جذريا في نمط الحياة إذ أجبرت مختلف الدول بالأخذ بها بهذا المبدأ سعيا للتطور ولتقليص الفجوة المعرفية[2] فقد باتت المعلومة هي اداة محاربة الجريمة وفي نفس الوقت مسرح الجريمة نفسه وهذا ما خلفه لنا العالم الرقمي وعصر العولمة ونجد من أبرز صور المعلومات ما يلي:

أولا: المعلومات الاسمية: هي تلك المعلومات الشخصية التي تتعلق بالشخص كاسمه ولقبه أو جنسيته وحالته الاجتماعية أو هي تلك المعلومات الإسمية الموضوعية التي تكون منسوبة إلى شخص معبرا بها عن رأيه اتجاه الغير كالمقالات في الصحف أو التقارير الخاصة بالعاملين لدى مؤسسة ما.

ثانيا: المعلومات المتعلقة بالمصنفات الفكرية: وهي تلك التي تتعلق ببراءة الاختراع وحقوق المؤلف كما سبق الذكر وغيرها من الحقوق الملكية الأدبية والفنية والصناعية والتي يتمتع أصحابها بحقوق مالية وأدبية عليها.

ثالثا: المعلومة المباحة: هي التي يحق للجميع الحصول عليها والاستفادة منها دون إذن من صاحبها كالنشرات الجوية وأخبار البورصة .

رابعا: المعلومة السرية: هي المعلومة التي يكون الاطلاع عليها وحيازتها تقتصر على الأشخاص المصرح لهم ذلك دون بقية الأشخاص ويكون محظورا على غيرهم المساس بها وفي حال الحصول عليها من غير المصرح لهم بها سيمثل ذلك نشاطا إجراميا غير مشروع

خامسا: المعلومة التجارية والصناعية: تتمثل على سبيل المثال في الدراسات الخاصة بالأسواق التجارية والصناعية ومشروعات الاستثمار والتصنيع والإنتاج والتوزيع والتجارة وكذا الأسعار ومراكز البيع والقطاع الصناعي للانتاج سادسا المعلومة العسكرية هي المعلومات

---

[1] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية ، مرجع سابق ، ص 29

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية ، مرجع سابق ، ص 25

التي تتعلق بالنشاط العسكري للدولة ومنها على سبيل المثال الأسرار العسكرية وتحديث الأسلحة والمشروعات النووية وكذا المعدات.[1]

الفرع الثاني: الأجهزة كمحل للجريمة الإلكترونية

يعد جهاز الحاسوب ونظامه المعلوماتي من أساسيات تنفيذ الجريمة المعلوماتية ما يسهل عملية التوغل والانسياب إلى مختلف شبكاته الداخلية ومن ثم تقنياته الإلكترونية لا يمكن للجاني اقتراف فعله الجنائي إلا بعد الاستعانة بالإمكانيات التي يتيحها له الحاسب الآلي ومن خلال هذه الأخيرة يتاح له تخريب البرمجة الآلية للحاسب ما ينتج عن ذلك التعطيل الكلي أو الجزئي المحتوم للجهاز.

لهذا حين نقول الأجهزة كمحل للجريمة الإلكترونية فإننا لا نعني بها فقط الأشياء المادية كجهاز الكمبيوتر أو المعدات الملحقة به من أسطوانات وشرائط ممغنطة وكابلات وغيرها لأن كل هذه المكونات قد تكون محلا للسرقة أو الإتلاف العمدي كتكسيرها أو حرقها وما إلى ذلك من جرائم تعد من قبيل الجرائم التقليدية بل إننا نعني الجرائم التي تتسبب في تعطيل أجهزة الكمبيوتر ومن في حكمها أو تخريبها عبر إرسال الفيروسات أو البرامج التي تحتوي على أنظمة هجومية قد تسبب تلفا في هذه الاخيرة مما يؤدي إلى شلل كل الأنشطة المرتبطة بهذه الأجهزة وتزداد خطورة هذه الجرائم حينما تقع على البرامج وليس على المكونات المادية لها وذلك نظرا لقيمة ما تحتويه هذه البرامج من معلومات وبيانات حيث يستلزم هذا النمط من الجرائم معرفة فنية عالية في مجال البرمجة.[2]

وفي ظل التشريعات التي جرمت تعديل أو إزالة المعطيات التي تتضمنها نظام المعالجة الآلية للمعطيات نجد أن المشرع الفرنسي بالحماية الجنائية من الجرائم الائتلاف المعلوماتي بأشكاله المختلفة من خلال تدشين عدد من النصوص التشريعية في القانون الجنائي الفرنسي فقد تم تخصيص فقرتين بالمادة(323) والمادة(3/323)[3] وهذا ما أخذ به المشرع الجزائري هو الآخر في تجريم هذه السلوكيات الغير قانونية من خلال نص المادة 94 3 مكرر من قانون العقوبات الجزائري[4] والهدف الأساسي من تجريم هذه الأفعال هو حماية الأجهزة ونظام التشغيل المعلوماتي من التخريب أو الإتلاف أو حتى الإعتداء

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص82-83

[2] الدكتورة شنتير خفرة، دكتورة قانون جنائي، الآليات القانونية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص 31

[3] المركز العربي لأبحاث القضاء الإلكتروني http://accronline.com article detail (تاريخ الدخول في 17/04/2024)

[4] المادة 394 ثلاثة مكرر 01 من القانون رقم 04/15 المعدل والمتمم لقانون العقوبات 2004

وما يهم هو اذا حدث الإعتداء ضد أحد المكونات أو العناصر المعنوية التي منها يتكون منها الحاسب كالمعلومات أو البرامج إذ أن هذه المسألة تثير صعوبات تتمثل في عجز النصوص القائمة عن معالجة هذه الجرائم كالاتلاف والتخريب في قوانين مختلفة نظرا للطبيعة المادية التي تتطلبها هذه النصوص في الأشياء التي تكون موضع لهذه الجرائم في حين أن المعلومات المبرمجة آليا بواسطة نبضات كهربائية تفتقر إلى الطبيعة المادية إلا في الحالات التي فيها إتلاف للمكون المعنوي ما يؤدي في نفس الوقت إلى إتلاف أحد المكونات المادية للحاسب وكذلك الحال بالنسبة إلى الأفعال التي تسبب عرقلة نظام الحاسب وتمنعه من أداء مهامه أو ما يسمى بإنكار الخدمة إذ إنه من الواضح في هذا المجال أن المظاهر المطلوبة لاعتبار الحاسب هدفا في حقل التصرفات الغير قانونية تظهر عندما تكون السرية والسلامة في أنظمة المعلومات هي موضوع الاعتداء.[1]

ولعل أبرز الجرائم الواقعة بواسطة الحاسب الآلي أو الأجهزة الملحقة به أو عن طريق الاستعانة بالنظم المعلوماتية نذكر على سبيل المثال ما يلي:

أولا: جرائم وإفشاء الأسرار: من الممكن أن يكون جهاز الحاسب والإنترنت اداة فاعلة في إفشاء الأسرار لا سيما مع اتساع عدد المستخدمين لهذه التقنية ولعل أبرز الأسرار المستهدفة في هذه الجرائم هي أسرار الدفاع الوطني وأسرار الاتصالات والصناعة والأسرار المهنية الأخرى بالإضافة إلى الأسرار الشخصية.

ثانيا: جرائم الاعتداء على حق الملكية: يمكن أن يكون حق الملكية محلا لجرائم معلوماتية متعددة وأبرزها جرائم الاحتيال المعلوماتي والجرائم الناشئة عن إساءة استخدام البطاقات البنكية المصرفية.

ثالثا: جرائم الإعتداء على حقوق الملكية الفكرية: حقوق الملكية الفكرية أو حقوق المؤلف فإنه يتم إستخدام الحاسب والإنترنت في الاعتداء والسطو على بنوك المعلومات التي تتضمنها بعض البرامج في حاسب آخر أو سرقة مؤلفات معينة موجودة في موقع إلكتروني لم يأذن صاحبها بنشرها ولم يجعلها متاحة للمستخدمين فالاعتداء في هذه الأحوال يعد انتهاكا مزدوجا فهو من جهة إعتداء على القيمة المالية التي تمثلها المعلومة ومن جهة أخرى اعتداء على الحقوق المعنوية لأن لها قيمة معتبرة.

رابعا: جرائم الإعتداء على الحقوق الشخصية: في هذه الاحوال يستخدم الحاسب والإنترنت للاعتداء على الحقوق الشخصية كما لو استهدف الاعتداء حرمة الحياة الخاصة للإنسان أو

[1] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية، مرجع سابق ،ص117

الحريات العامة للأفراد وتتحقق هذه الحالة على وجه الخصوص في حالة تكوين ملف يحتوي معلومات اسمية أو ما تسمى بالبيانات الشخصية التي تخص أحد الأفراد دون علمه أو موافقته أو كما في حالة تجميع هذه المعلومات بعلم الشخص موافقته ولكن الاحتفاظ بها قد تم على نحو غير مشروع أو تم الاطلاع عليها من قبل من لم يأذن لهم القانون والإطلاع عليها دون إذن الشخص المعني وقد تبنه المشرع الفرنسي إلى خطورة هذه المعلومات فأصدر بذلك قانون المعلومات والبطاقات والحريات الصادر في 6 يناير 1972 الذي اعتنى بمعالجة مختلف صور الإعتداء على هذه البيانات.[1]

الفرع الثالث: الأشخاص أو الجهات كمحل للجريمة الالكترونية

في ظل عصر العولمة والتقدم التكنولوجي شهدت الجريمة انتقالة غيرت منحى الحياة البشرية من خلال عدة أصعدة ليظهر لنا نوع جديد مستحدث ارتقى بالأفعال الغير مشروعة إلى مستوى جد متطور وعالي ألا وهي ما يسمى بالجرائم الالكترونية جرائم مجردة من الطابع المادي المألوف لتصبح ذات طابع افتراضي يتم توقيع الاعتداءات بها بواسطة الشبكة العنكبوتية وهذا ما ألحق بكل من الأشخاص والكيانات اعتداءات وتبعات جد وخيمة

وبالرغم من دقة وذكاء وسرعة الحاسب في معالجة البيانات إلا إنه آلة عمياء وهذا ما يعني أنه لا يمكن لها أن تقوم بأي عمل أو مهمة ما لم تتلقى الأوامر من بيانات ومعلومات اللازمة لتنفيذ أي وظيفة معينة وهذا بطبيعة الحال يفترض وجود العامل البشري وذلك بمقتضى أن الحاسب لا يمكنه العمل بصورة مستقلة وأن البدء بتنفيذ أي عمل جنائي يتطلب منذ البداية تدخل العامل البشري في إنشاء التهديدات الإلكترونية التي تكون في أغلبها برامج معينة تصمم خصيصا لمهاجمة المعلومات المقصودة والمخزنة ضمن نطاق إلكتروني[2] فمن المتوقع أن يقع ضحيتها جميع فئات المجتمع العامة منها والخاصة الطبيعية كانت أو المعنوية وهذا ما أشار اليه المشرع الجزائري في نص المادة 394 مكرر رقم 03 «تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاصة الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد»[3] فالشخص الذي يتعامل مع هذه الالة لا نقول إنه يتمتع بذكاء مطلق ولكن على الأقل سيكون له القدرة والمعرفة الكافية بالجوانب المرتبطة بطرق عمل الجهاز والأنظمة المتصلة به وبالمفردات

---

[1] الدكتور عمار عباس الحسيني، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، مرجع سابق،ص94-95-96

[2] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية، مرجع سابق ،ص123

[3] المادة 394 ثلاثة مكرر 03 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات 2004

الأخرى التي يتعامل معها فالمجرم المعلوماتي لا يستطيع على سبيل المثال إختراق أي نظام معلوماتي مصرفي أو مالي ما لم يستخدم جهاز الحاسوب كون أن هذا الجهاز هو الأداة التي يمكن من خلاله الدخول إلى النظام المقصود وبنفس الوقت هو يحتاج المعرفة المطلوبة لتشغيل هذه الالة بواسطة البرامج والأنظمة والتطبيقات في طريق محدد والذي يتيح تحقيق الهدف الجنائي.[1]

ومن بين الجرائم التي باتت تهدد أمن المواطنين والدول على حد سواء الإرهاب الإلكترونية والذي ساعدت التقنية الحديثة على استفحاله وسرعة انتشاره وتطبيقه مما توفره من معلومات ووسائل وقلة التكاليف فباستعمال شبكة الإنترنت تتمكن المنظمات الإرهابية المتفرقة من الاتصال مع بعضها البعض والتنسيق فيما بينها فعدم وجود زعيم ظاهر للجماعة الإرهابية اصبحت سنة جوهرية للتنظيم الإرهابي الحديث مختلفا بذلك عن النمط الهرمي القديم للجماعات الإرهابية لذا اصبح الإرهاب الإلكتروني أو ما يسمى بالإرهاب السيبراني « le cyberterrorisme» هو السائد حاليا معتمدا على اقتحام المواقع «storming sites» وتدميرها وتغيير محتوياتها به بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا[2] مثال ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين والاطباء أو من المحاسبين أو غيرهم من المهنيين وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة بالشخص أو تسجيل مكالمات أو فيديو أو مراقبته بل قد يتعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها خاصة المتمثلة في الإرهاب والجريمة المنظمة كما سبق الذكر بل الأخطر من ذلك إتاحة تقنية الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى كالاطلاع على الأسرار العسكرية أو الاقتصادية خاصة فيما يتعلق بالدول التي يكون بها نزاعات ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الإنترنت حيث تعطي هذه الاخيرة فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.[3]

---

[1] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية، مرجع سابق ،ص123-124

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية ، مرجع سابق ، ص 34-35

[3] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, جامعة محمد بوضياف المسيلة, مجلة الأستاذ الباحث للدراسات القانونية والسياسية, العدد الحادي عشر ,سبتمبر ,2018 ،ص357-378

لذا خص المشرع الجزائري مرتكبي مثل هذه الأفعال بعقوبات تتراوح بين 5 الى 10 سنوات سجن إضافة إلى غرامة مالية[1] ولا شك أن التقدم الكبير الذي لحق بالاتصالات وصناعة الحواسيب أسفر عن إيجاد وسائل أكثر فعالية في التجسس ومن الأمثلة على ذلك ما قام به هاكرز حين الإغارة على شبكة معلومات تابعة لوكالة ناسا ومواقع اسلحة ذرية تابعة لحكومة الولايات المتحدة الامريكية.[2]

المطلب الرابع: أركان الجريمة المعلوماتية

كأصل عام متعارف عليه فإن المشرع الجزائري يشترط لقيام أي جريمة توافر عناصر أساسية وبدونها لا يمكن تصور الفعل الجنائي إلا وهي الركن الشرعي يليه الركن المادي وأخيرا الركن المعنوي أساسيات تقوم الجريمة بقيامها وتنعدم بانعدامها إلا أن ذلك يختلف شيئا ما فيما يتعلق بالجريمة الإلكترونية جريمة بتطور تقنياتها وحداثة أساليبها اتخذت من الفضاء الافتراضي مسرحا لها ومن التقنيات الالكترونية .....لسلوكاتها ومن النظام الالكتروني وأصحابه ضحية لها ومن خلال ما سبق سوف نتطرق إلى تبيان الاركان القانونية التي تقوم عليها هذه الجريمة.

الفرع الأول: الركن الشرعي

لقد شهد الزحف الذي عرفته الجرائم الماسة بالنظام المعلوماتي والاعتداءات التي شملت خصوصية الأفراد ومختلف الهيئات انتقالة غير مسبوقة حيث لجأت أغلب التشريعات الوطنية والدولية التي فرض رقابتها وسلطتها إتجاه تجريم مختلف أوجه الجريمة المعلوماتية [3]فقد بذلت هيئة الأمم المتحدة بالإضافة إلى المجلس الأوروبي جهودا مضنية لاقناع الدول بضرورة وضع التشريعات الملائمة لمواجهة الجرائم الإلكترونية وتعزيز التعاون الدولي في هذا المجال[4] حيث تعتبر الجريمة بصفة عامة عمل غير مشروع يجرمه القانون ويعاقب عليه وذلك بالنظر لما يقرره القانون الجنائي والقوانين المكملة له من أوامر ونواهي تجرم وتعاقب على كل سلوك أو فعل ترى فيه السلطة المختصة بالتشريع أنه يرقى لدرجة التجريم بما يشكله من مساس

---

[1] القانون رقم 16/02 المؤرخ في19/02/2016 المتمم للأمر 66-156 رقم المؤرخ في و المتضمن قانون العقوبات جاءت المادة 02 منه لتتمم قانون العقوبات بثلاث مواد منها المادة 87 مكرر 12

[2]الدكتورة شنتير خفرة، دكتورة قانون جنائي، الآليات القانونية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص 37

[3] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, معهد الحقوق و العلوم السياسية , المركز الجامعي افلو 2020/2021،ص12-13

[4] بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني, مذكرة نهاية الدراسة لنيل شهادة الماستر, جامعة عبد الحميد بن باديس, مستغانم, 2022/2023،ص10

بمصالح الجماعة بوجه عام للخطر[1] ومنه فإن الركن الشرعي يتمثل في ذلك النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له تطبيقا لنص المادة الاولى من قانون العقوبات بقوله لا جريمة ولا عقوبة أو تدبير أمن بغير قانون وهو ما يقابل المادة 160 من دستور 2016 التي تنص في فحواها على «وجوب خضوع العقوبات الجزائية إلى مبدأ الشرعية والشخصية.[2]»

ولقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفعل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والتي اشتملت على ثمانية مواد تضمنت كل أنواع الاعتداءات على الأنظمة المعلوماتية بمحتوى المادة 394 مكرر إلى 394 مكرر 07 بمقتضى القانون رقم 04 15 المؤرخ في 10 نوفمبر 2004 ولم يكتفي المشرع الجزائري لذلك فرض حمايه جنائية على الحياة الخاصة للأفراد من خلال القانون رقم 06 23 المؤرخ في 20 ديسمبر 2006 والذي جاء بمحتوى المادة 303 مكرر إلى المادة 3 مكرر 07 وهذا كله تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة[3] كما تجدر الإشارة إلى أنه لا يجوز متابعة الشخص قضائيا عن فعل ارتكبه قبل صدور نص التجريم أو عن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها أو أفعال أخرى ورد في حقها نص قضائي مهما يكن بينهما من تشابه من حيث الدوافع أو الفعالية النتائج أو حتى فيما يخص العناصر ذلك إنه من غير المقبول التوسع في تفسير النصوص الجزائية وعلى كل القضاة التقيد بمدلول القاعدة القانونية والالتزام الكلي المطلق بمقاصدها ذلك أنه قد يترتب على إهمال قاعده شرعية الجرائم و العقوبة نتائج جد مهمة تتمثل في عدم رجعية القاعدة الجنائية أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي إلا إذا نص القانون على ذلك، صراحة في نص قانوني أو إذا ما عملت قاعدة تطبيق القانون الأصلح للمتهم وبما أن الركن الشرعي والصفة الغير مشروعة للفعل الذي يقوم به الجاني فإن له ركنين أساسيين هما:

---

[1] غريبي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي و علوم جنائية ,جامعة آكلي محند أولحاج, البويرة 2020-2021،ص14

[2] المادة 160 الصادرة بموجب قانون رقم 16/01 المؤرخ في 06/03/2016 المتضمن التعديل الدستوري من الجريدة الرسمية العدد

[3] إيمان بغدادي, أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية, جامعة قسنطينة مجلة آفاق البحوث والدراسات السياسية, العدد 04, جوان, 2019،ص188

– مطابقة الفعل لنص التجريم يقصد به تطابق الأفعال التي يجرمها القانون مع النصوص التجريبية الموجودة.

– خضوع الفعل لسبب من أسباب الإباحة يقصد به حسب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة.[1]

الفرع الثاني: الركن المادي

لقد ذهب بعض الفقهاء القانونيين إلى القول بأن الركن المادي للجريمة المعلوماتية يتمثل في كل فعل ينتج عنه توقيف نظام المعالجة الآلية للمعطيات عن أداء أعماله الطبيعية وبالرغم من الجدل الفقهي الواسع الذي صاحب مفهوم النظام المعلوماتي حول شموله لجل عناصره من عدمه إلا أن غالبية الفقه ترى بضرورة عدم اشتراط أن يقع فعل التعطيل أو الإضرار بالنظام الإلكتروني كله بل يكفي أن يؤثر على أحد من عناصره فقط كجهاز الحاسوب نفسه أو شبكات الاتصال أو المساس بالبرامج والمعطيات المعلوماتية[2] فالقول أن الجريمة الإلكترونية قامت بسبب قيام السلوك المادي الذي يتطلب هو الآخر وجود بيئة رقمية وجهاز كمبيوتر والاتصال بشبكة الانترنت ومن الضروري أيضا معرفة بداية هذا النشاط والشروع النتيجة المبتغاة منها على سبيل المثال يقوم الجاني بتجهيز الكمبيوتر لكي يسهل عليه اقتراف فعله الجنائي فيقوم هذا الأخير بتحميل جهاز الحاسب ببرامج اختراق متنوعة ويقوم بإعدادها بنفسه كذلك قد يحتاج الى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف كما يمكنه القيام بإعداد فيروسات تمهيدا لبثها[3] وهذا ما يطلق عليه بالأعمال التحضيرية ذلك ما جاء به المشرع الجزائري في نص المادة الثانية من القانون رقم 09 04 والذي جاء في فحواه وهو يعرف بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأن « جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات

---

[1] عمار حشمان, الجريمة المعلوماتية في التشريع الجزائري, مذكرة مقدمة لاستكمال متطلبات شهاده الماستر المهني الطور الثاني, ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير, جامعة قاصدي مرباح ورقلة ,2018-2019، ص 13

[2] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية,مرجع سابق ، ص14

3بوديسة بجاد عبد الرؤوف, آليات التحري عن الجريمة الإلكترونية في القانون الجزائري, مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر مهني في الحقوق ,تخصص قانون إعلام آلي والانترنت, جامعة محمد البشير الابراهيمي, برج بوعريريج,2021-2022،ص19

الإلكترونية»[1] ومنه فإن الركن المادي للجريمة المعلوماتية هي تلك الصور التي تضمنها المشرع الجزائري من خلال القانون رقم 04/ 15 المعدل والمتمم لقانون العقوبات لسنة 2004 منها ما يلي:

– جريمة الدخول والبقاء في النظام المعلوماتي والتي نصت عليها المادة 394 مكرر وما يلحقها من سلوكيات تتمثل في الحذف والتغيير والتخريب...

– جريمة التلاعب بالمعطيات المعلوماتية والتي نصت عليها المادة 394 مكرر 01 والتي تحتوي هي الأخرى على أفعال غير مشروعة مكونة لها كالإدخال والإزالة والتعديل للمعطيات والمعلومات في النظام المعلوماتي بصفة كلية أو جزئية.

– جريمة التعامل الغير شرعي بمعطيات النظام المعلوماتي المنصوص عليها بالمادة 394 مكرر 02 هي الأخرى اشتملت على العديد من السلوكيات التي من خلالها حاول المشرع الوطني التوسيع من نطاق التجريم والإحاطة بكافة الجوانب بأي قدر ممكن جمعت عدة أعمال نذكر منها التصميم والبحث التجميع والتوفير الحيازة والافشاء النشر والاستعمال لمعطيات المنظومة المعلوماتية بالإضافة إلى ما نص عليه القانون رقم 04 15 من أحكام خاصة بالجريمة المعلوماتية من خلال نص المواد 394 مكرر 03 394 مكرر 04 394 مكرر 05 394 مكرر 07 ولتمام الركن المادي للجريمة الالكترونية لابد من توافر عناصر ثلاثة وهي:

أولا :السلوك الإجرامي: يبرز هذا السلوك بصورتين فقد يكون بفعل إيجابي الذي يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة كما قد يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع بنص القانون أما فيما يخص الجريمة المعلوماتية يمكننا أن نجد هذا السلوك بنوعية الإيجابي والسلبي ولا ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الجاني والذي استحدثه بعقليته الذكية التي استطاعت الانتقال من تقليدية السلوك الجرمي إلى مساحات أكثر اتساعا وتعقيدا أوجدت بلا شك صعوبات عدة[2] خاصة فيما يخص متابعة هذا السلوك وتحقيقه.

---

[1] القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها, الجريدة الرسمية ,العدد 47

[2] عمار حشمان, الجريمة المعلوماتية في التشريع الجزائري,مرجع سابق ، ص14

جمع أدلة إثباته وهي ما أظهرت نمطا مستحدثا من الاجرام أدى إلى انقلاب في النظرية العامة للجريمة من خلال المحاور التالية:

- طبيعة السلوك والنتيجة والعلاقة بينهما زمنيا ومكانيا.

- نسبة السلوك إلى الفاعل والمساهمين.

- عجز النمو عجز النصوص التقليدية عن استيعاب القوالب الجريمة المستحدثة.[1]

ثانيا: النتيجة الإجرامية : يقصد بها كل فعل ينجم من جراء السلوك الاجرامي الغير مشروع تؤدي بالمساس بالمصالح الفردية والجماعية في المجتمع وقد يتعدى ذلك إلى اختراق نظام الدولة وسيادتها حيث كان الفقه قديما يشترط لقيام الركن المادي حصول نتيجة إجرامية كيف ما كانت إلا أن التوجه الحديث في تجريم الافعال لم يعد يشترط حصول نتيجة الجريمة خاصة فيما يتعلق بنوع معين من الافعال الغير مشروعة التي يطلق عليها تسميه جرائم الخطر من بينها الجريمة المنظمة على نحو ما هو منصوص عليه في اتفاقية الامم المتحدة لعام 2000 والتي عاقبت على مجرد الاتفاق لارتكاب إحدى الجرائم المنصوص عليها ولو لم تتحقق النتيجة الإجرامية به.[2]

ثالثا : العلاقة السببية : لقيام المسؤولية الجنائية كأي جريمة تقليدية فإنه من الضروري قيام العلاقة السببية التي تصل بين الفعل الغير مشروع والنتيجة الإجرامية والتي من خلالها يثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وتكمن أهمية الرابطة السببية إلى إسناد هذه الأخيرة الى الفعل المجرم والذي يعتبر شرط أساسي لتقرير المسؤولية الجنائية تجاه الجاني كما أنها تحقق تلازما ماديا بين الفعل والنتيجة ما يؤدي إلى وقوف مسؤولية الفاعل عند حد الشروع إذ لا يعد مسؤولا عما حدث أو ما تخلف عنه أما اذا كانت غير عمدية فان نفي الرابطة السببية يؤدي إلى انتفاء المسؤولية بصفة كلية ذلك أنه لا شروع في الجرائم العمدية.[3]

الفرع الثالث: الركن المعنوي

تعد الجرائم المعلوماتية وكغيرها من الجرائم التي تفترض بالأساس وجود الركن المعنوي هذا العنصر الذي يعبر عن المسلك النفسي للجاني باعتباره محور القانون الجنائي ذلك أنه في إطار هذا الركن تتوفر كافة مقومات المسؤولية الجنائية من علم وإرادة آثمة وقصد جرمي مع اقرار العقاب الذي يبنى على هذه المقومات لذلك يمكن تعريف الركن المعنوي بأنه العلاقة التي

---

[1] بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني,مرجع سابق ، ص15-16

[2] بوديسة بجاد عبد الرؤوف, آليات التحري عن الجريمة الإلكترونية في القانون الجزائري،مرجع سابق ،ص20

[3] عمار حشمان, الجريمة المعلوماتية في التشريع الجزائري,مرجع سابق ، ص14-15

تربط بينما ماديات الجريمة وشخصية الجاني وهذه العلاقة يطبق عليها القانون والعقاب الذي يقرره كما يمكن تعريفه أيضا لأنه العلم بعناصر الجريمة وإرادة ارتكابها وبالتالي فيتكون هذا الركن من عنصريين كما سبق القول وهما العلم والإرادة فالعلم هو إدراك الامور على نحو مطابق للواقع أما الإرادة فتتمثل في الاتجاه من أجل تحقيق السلوك الإجرامي. [1]

ويتخذ القصد الجنائي عدة صور منها القصد الخاص والقصد العام فهذا الأخير هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم فلا يكفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أي أنه ينبعث في نوايا المجرم فما هو القصد الذي يجب أن يتوفر في الجريمة المعلوماتية.

يعتبر القصد الجنائي متوافر في جميع الجرائم المعلوماتية دون اي استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم الإلكترونية التي تتطلب توافر القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنت أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الظروف المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص فبعض المجرمين يبررون أفعالهم لأنهم مجرد فضوليين إلا أنه كان عليهم أن يتراجعوا بمجرد دخولهم ولا يستمرون ببقائهم داخل النظام الخاص بالأفراد أو المؤسسات فمثل هذه الأفعال تتطلب مهارات عقلية ومعرفية كبيرة[2] **وبذلك يقوم القصد الجنائي في حق الجاني بحالات ثلاث تتمثل فيما يلي:**

– الحالة الأولى: إن كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة.

– الحالة الثانية: إذا نجم على الفعل او الامتناع ضرر أو خطر أكثر جسامة مهما كان يقصده الفاعل وهي في حالة جواز القصد الذي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف.

– الحالة الثالثة الحالات التي ينص فيها القانون الفصل إلى الفاعل نتيجة لفعله أو امتناعه أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضا وهو مستمد من أن

---

[1] مهداوي حنان, التنظيم القانوني في الجريمة الإلكترونية في التشريع الجزائري, جامعة محمد لمين دباغين سطيف 2, مجلة الفكر القانوني والسياسي (ssn:2588-1620/), المجلد السادس, العدد الثاني, 2022 ،ص1066

[2] غريبي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري,مرجع سابق، ص16

النتيجة الجسيمة التي تحققت نشأت عن فعل الجاني فمقتضى ذلك أن هذا الفعل كان صحيحا فإحداثها ولكونه كذلك فإن الجاني يجب أن يتحمل نتائجها توقعها أم لم يتوقعها.[1]

أما عن الاثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات و تصحيحها بمالها من صلاحيه باعتبارها صاحبة القرار النهائي بالفعل في الدعاوى المرفوعة أمامها.[2]

المبحث الثاني: ماهية المجرم المعلوماتي

المجرم والجريمة ومصطلحان متلازمان فلا يمكن تصور أي مجتمع خال منهما فلولا المجرم لما كانت الجريمة والعكس صحيح هذا وصاحب النمو البشري ازدهار في معدلات الاجرام ورقي مخططات الأشرار بما يواكب عصر العولمة والإبتكار ليشهد بعدها الفقه الجنائي ولادة جيل جديد من مجرمين هذه الفئة التي لا تمد بأي صلة للجاني والسلوك الإجرامي المعهود . الذي من خلاله يعبر المرأ عن غضبه ثأره وانتقامه من شيء ما تجاه أمر وهم من اصطلح على تسميتهم بمجرمي المعلوماتية مجرمين اتخذوا من الواقع الافتراضي والنظام المعلوماتي مسرحا لجرائمهم وذلك يرجع لتطورات التقنية والثورة التكنولوجية التي شهدها العالم في جل مجالات الحياة ومختلف مسارات المعاملات لكافة فئات طبقات المجتمعات بحيث شكلت قفزة نوعية من الحياة التقليدية إلى حياه أكثر عصرنة وحداثة هذا ولم يكن حكرا على طائفة من المجرمين الذين حاولوا استغلال التقنيات التكنولوجية والشبكات الالكترونية في تحسين واستحداث سلوكياتهم الإجرامية إذ لم تعد الاعتداءات موجهة ضد الأشخاص أو الكيانات المادية بل انتقل الأمر إلى العنف ضد النظام المعلوماتي هذا ما جعل من مرتكبي هذه الأفعال يتسمون بطبيعة إجرامية خاصة ببعدهم عن كل مظاهر العنف المادي واعتمادهم الكلي على الذكاء الإلكتروني والمهارات التقنية في التعامل مع التكنولوجيا المعلوماتية وللفهم العميق للجرائم ذات الطبيعة المعلوماتية فإنه لابد من دراسة المجرم الالكتروني حيث أن جل تبعيات هذه الجرائم سابقة الذكر ترتبط ارتباطا وشيكا بالصفة البيولوجية والدوافع الإجرامية النفسية للجاني المعلوماتي هذا ما يجعل من البحث وتحليل شخصية هذا الأخير أمر ضروري لفهم الظاهرة الإجرامية بشكل أكثر دقة ووضوح وبناء على ما تقدم سنستعرض في هذا المبحث دراسة طبيعة المجرم المعلوماتي من حيث مفهومه في المطلب الاول من ثم تبيان تقسيماته الفقهية في المطلب

---

[1] بوديسة بجاد عبد الرؤوف, آليات التحري عن الجريمة الإلكترونية في القانون الجزائري, مرجع سابق، ص355

[2] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, مرجع سابق، ص355

الثاني أما المطلب الثالث فسوف نتطرق فيه إلى الخصائص التي تميز هذا الأخير عن المجرم التقليدي وما أبرز السمات التي ينفرد بها عن غيره ومن ثم المطلب الرابع والأخير الذي خصص لدراسة مسببات ودوافع مرتكبي الجريمة المعلوماتية.

المطلب الأول: مفهوم المجرم المعلوماتي

إن ارتباط هذا العصر بالحاسب وتكنولوجيا المعلومات أنتج ما يسمى بالمجرم المعلوماتي طائفة ظهرت كفكرة جديدة نوعا ما على الفقه الجنائي ففي الجريمة المعلوماتية كما عرفناها سابقا و بمناسبة الطبيعة الخاصة التي تنفرد بها فإننا لا نكون بصدد مجرم عادي بل أمام مجرم ذي مهارات تقنية وخبرة عالية في مجال الأنظمة الإلكترونية عامة والحاسب الالي خاصة ما أسفر عن أوامر مستحدثة في أذهان مرتكبيه ليحولوا نواياهم من أفعال مادية إلى اللغة الرقمية باستخدام التقنية المعلوماتية وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع المحلي والدولي نتيجة مخالفة قواعد الضبط الاجتماعي محليا أو دوليا بحيث أن هذا الصنف من المجرمين لديهم تأثير خطير جدا على الأشخاص الطبيعيين صغارا كانوا أو كبارا أو على الاشخاص المعنويين في المؤسسات والدول.

المجرمون الالكترونيون أو ما يطلق عليهم البعض تسمية المخترقون ويسميهم آخرون بالقراصنة والمقصود بالقرصنة هي عملية التوصل إلى كافة المعلومات في الكمبيوتر بصورة غير مشروعة ونسخ برامج بدون وجه حق أي الحصول على المعلومات بطرق ملتوية وهناك نوعين من القراصنة الصنف الأول يطلق عليه اسم الهواة وهم الشباب الفضوليين الذين يسعون تسلية ولا يشكلون خطورة على الصناعات وأنظمة المعلومات والصنف الثاني وهم المحترفون وهم الأكثر خطورة من الصنف الاول بحيث أنهم يحدثون أضرارا كبيرة كما يمكن وأن يؤلفوا أندية لتبادل المعلومات فيما بينهم[1] فشخصية المجرم المعلوماتي سواء كان طبيعيا أو معنويا وآلية ارتكاب الجريمة تجعل منه شخصا يتسم بسمات خاصة تضاف إلى الصفات الاخرى التي يجب ان تتوافر في المجرم العادي ولعل أهم ما يتميز به الشخص المذكور أنه يتوافر لديه خبرة بالمسائل المعلوماتية ومعرفة كافية بآلية عمل الحاسب الآلي وتشغيله باعتبار أن الاجرام المعلوماتي ينشأ من تقنيات التدمير الهادئة التي تتمثل في التلاعب بالمعلومات والكيانات المنطقية وذلك لا يعني إمكانية تصور الصنف الموجه ضد النظام المعلوماتي فقد يكون محل الجريمة إتلاف الحاسب الآلي ذاته أو وحدة المعالجة المركزية أي أن ما يمكن الاعتداء عليه قد يكون لهيكلة الحسابات لا بمعلوماتها المتنقلة عبر شبكة

[1] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية ،مرجع سابق، ص37-38

المعلومات[1] ففي هذا النوع من الجرائم نحن لسنا بصدد سارق أو محتال أو مزور عادي ولكن مجرم ذو مهارة تقنية في أغلب الأحيان ودراية بتقنيات المستخدم في الحاسب والنظام المعلوماتي فهو قادر على استخدام قدراته لاختراق كود المعلومات السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام هذه التقنية.[2]

هناك من يتوسع في تحديد فئات المجرم المعلوماتي تبعا الخطورة الإجرامية الكامنة فيه أو من خلال ما إذا كان الشخص المجرم طبيعي أو معنوي وذلك كما يلي:

الفرع الأول:«Hackers»: هم فئة المجرمين الأقل خطورة والذين تتوفر لديهم خبرة معتبرة في مجال الحاسب الالي ووظائفه ومكوناته والنظم المعلوماتية و معرفة البرامج التي يجري العمل بها كالبرامج المحاسبية وبما أن هؤلاء يمارسون مواهبهم بغرض الولوج إلى نظم المعلومات بدافع الفضول أو اللهو فهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة لذلك فإن هذه الفئة تعد أقل خطورة ولكن مع ذلك يلاحظ أن ازدياد الأعداد المستخدمة لتكنولوجيا الإعلام والاتصال وما يتبعه من ازدياد نسب جرائم في هذا المجال فلا يستبعد معه احتمال انزلاق هذه الفئة من مجرد هواة لهذه الأفعال الغير مشروعة إلى محترفين[3] كما يعتبرون أولئك الذين يتحدون إجراءات أمن النظم والشبكات دون أن تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية إنما ينطلقون من دوافع التحدي وإثبات المقدرة.[4]

الفرع الثاني: «crackers»: أصحاب هذه الفئة يتمتعون بمستوى مهاري عالي يسمح لهم بالدخول واقتحام الأنظمة المحاسبية بكل سهولة واقتدار رغم احتياطات الأمن المتعددة ورغم قلة العناصر القادرة على اكتشافها مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة اذ غالبا ما تكون جرائم التحويل والنسخ والإضافة للمعلومات على البرامج وتغيير محتواها من جانب هذه الفئة جد ضخمة وتبعا لذلك يميز بين مصطلحي «cracher» و «cracker».

---

[1] بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني, مرجع سابق،ص19

[2] الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، مرجع سابق،ص74

[3] الدكتور يعيش تمام شوفي ، سلسلة مطبوعات المنبر ، الجريمة المعلوماتية ، دراسة تأصيلة مقارنة جامعة محمد خيضر بسكرة ، الطبعة الأولى ، جانفي 2019 ، ص 22

[4] الدكتور عمار عباس الحسيني، أستاذ القانون الجنائي، جرائم الحاسوب و الانترنت، جرائم المعلوماتية، مرجع سابق،ص58

من حيث نتيجة الفعل الإجرامي في الأول يلج داخل النظام ويحطم المعطيات بدافع الرغبة أما الثاني فيدخل إلى النظام للتحريف في هذه المعطيات أو محوها أو إدخال معلومات أخرى كما يطلق على فئة «cracker» ب «spiders»لأنهم يعملون في الخفاء ولا يتركون آثار مادية لأفعالهم وقد يصبحون أشد خطورة إذا ما تم تبادل تقنياتهم فيما بينهم كما ذكرنا سابقا حيث يشكلون ما يعرف بالجماعات والفرق المتخصصة أو العمل عن طريق الوساطة[1] وهم من تعكس اعتداءاتهم ميولا اجراميا خطيرا وهذا المعيار ما تعتمد عليه التشريعات الامريكية في التمييز بين النوعين من المجرمين فيما يميل البعض إلى تسمية المجرم المعلوماتي بالمجرم الالكتروني الرقمي ويعرفه بأنه من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني أو الرقم أو ملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي أو المحلي.

الفرع الثالث: المجرم المعلوماتي الطبيعي :لا شك أن الشخص الذي يرتكب الفعل الغير مشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظر القانون مجرما ويتعرض للعقاب إذا ما اقترف جريمته ولذلك فإن العقوبة لكي تحقق هدفها المباشر أو غير المباشر أي تحقيق هدفها في مجال الردع العام والخاص أما في مجال الإجرام المعلوماتي من حيث الظروف التي دفعته لارتكاب جريمته وأسبابها وصفاتها وذلك حقا يمكننا إعادة تأهيله اجتماعيا ويعود إلى حظيرة المجتمع كمواطن صالح ينفع المجتمع ولا يضره.

وقد عرفه الدكتور مصطفى يوسف كافي على أنه «مجرم متخصص على مستوى عالي من المهارة والحرفية ولابد أن يكون كذلك على مستوى عالي من التعليم إلا أن ذلك كله لا ينفي عنه صفة الاجرام» فهذا الصنف من المجرمين يحتاج لممارسة جريمته إلى الولوج الغير مشروع لذاكرة الحاسب الآلي لكي يختطف المعلومات المخزنة أو يعدل فيها ولا طالما ارتبطت شخصية المجرم بصورة الطالب في مجال العلوم المعلوماتية وذلك الشخص المهووس بالتقنية المعلوماتية غير أن التحول الجذري من حيث مدى خطورة هذه الأفعال دفع و بصفة تدريجية إلى تصنيفها ضمن مجال الاعتداءات التي تندرج في صنف الجريمة المنظمة.

[1] عامر محمد الحبيب عبد القادر, المجرم المعلوماتي, مذكرة نهاية الدراسة لنيل شهاده الماستر, جامعة عبد الحميد بن باديس, مستغانم,2018-2019،ص44-45

الفرع الرابع: المجرم المعلوماتي المعنوي: ليس هناك ما يمنع ان يكون المجرم المعلوماتي شخصا معنويا ومع الخلاف الدائر بين الفقه وبعض التشريعات في مدى إقرار المسؤولية الجنائية للشخص المعنوي إلا أن الأمر بات محسوما في ظل التشريع العراقي بل والعديد من التشريعات الأخرى التي أقر في نص المادة 80 من قانون العقوبات العراقي رقم 111 لسنة 1969 التي نصت على «أن الأشخاص المعنوية فيما عدا مصالح الحكومة ودوائرها الرسمية وشبه الرسمية مسؤولة جزائيا عن الجرائم التي يرتكبها ممثلوها أو مديروها أو وكلائها لحسابها وباسمها ولا يجوز الحكم عليها بغير الغرامة والمصادرة والتدابير الاحترازية المقررة للجريمة قانونا فإذا كان القانون يقرر للجريمة عقوبة أصلية غير الغرامة أبدلت بالغرامة ولا يمنع من معاقبة مرتكب الجريمة شخصيا بالعقوبات المقررة للجريمة في القانون».

ويمكن تصور ارتكاب الجريمة المعلوماتية من قبل الشخص المعنوي كما في حالات قيام شركة أو مصرف أو مؤسسة بارتكاب جريمة الاحتيال المعلوماتي أو سرقة البيانات الإلكترونية أو ممارسة الإرهاب الإلكتروني وما شابه ذلك.[1]

كما نص المشرع المصري في نص المادة 76 من قانون العقوبات المصري على أنه «يعاقب المسؤول عن الإدارة الفعلية للشخص الاعتباري بذات العقوبات المقررة عن الأفعال التي ترتكب مخالفة لأحكام هذا القانون إذا ثبت علمه بها وكان اخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة».

وقد تطرق المشرع الجزائري إلى العقوبات التكميلية للشخص المعنوي بالنسبة لجرائم اتلاف نظم المعلومات من خلال نص المادة 18 مكرر (معدلة) ولم يخرج المشرع الجزائري صراحه عن نظيره الفرنسي حيث أقر هذا الأخير في نص المادة 313-39 من قانون العقوبات الفرنسي سوف نذكر:

- **حل الشخص المعنوي.**
- **منع ممارسة نشاط أو عدة أنشطة مهنية أو اجتماعية سواء لمدة غير محددة أو لمده خمس سنوات أو أكثر.**
- **الوضع تحت المراقبة القضائية لمدة خمس سنوات أو أكثر.**
- **الغلق لمدة خمس سنوات أو أكثر للمؤسسة أو عدة مؤسسات ارتكبت هذه الجرائم.**
- **المنع من التعامل مع الأسواق العامة لمدة غير محددة أو لمدة خمس سنوات.**
- **المنع من دخول في المناقصة العامة لمدة غير محددة أو لمدة خمس سنوات.**

[1] الدكتور عمار عباس الحسيني، أستاذ القانون الجنائي، جرائم الحاسوب و الانترنت، جرائم المعلوماتية، مرجع سابق،ص57

وبالتالي نتوصل أن المشرع الجزائري سلك نهج المشرع الفرنسي في وضع نصوص تشريعية خاصة لمواجهة المجرم المعلوماتي الاعتباري بهدف التصدي لآثارها السلبية على المجتمع والدولة.[1]

كما يتصف المجرم المعلوماتي بأنه يملك سلطة ما على النظام المعلوماتي المستهدف بحيث تكون هذه السلطة مباشرة مثل من يملك الشفرة الخاصة بالدخول إلى النظام المعلوماتي المحتوي على المعلومات وقد تكون سلطة غير مباشرة مثل من يملك التصريح بالدخول إلى غرفة الأنظمة المعلوماتية المتمثلة في الحسابات الآلية وأدواتها دون حق في الولوج إلى نظام معلوماتي معين كما قد يكون فاعلا أصليا أو شريكا في ارتكاب هذه الجريمة فصفات الفاعل الأصلي قد ترتبط بأحد العاملين أو المستخدمين في منشأة تدار بالنظام المعلوماتي بغض النظر عن المستفيد من ارتكاب هذه الأفعال وبما أن هذه الجريمة تتطلب الدقة والتفسير للعمليات الغير مشروعة فإنه يستلزم وجود مشاركة أو مساعدة أشخاص آخرين سواء كانوا فنيين أو مجرد وسطاء يساعدون في حدوث وإنجاح العملية الغير مشروعة.[2]

المطلب الثاني: أقسام المجرمين المعلوماتيين

الجريمة المعلوماتية تلك الظاهرة المستحدثة التي احتوت جملة فئات المجتمع وكل مستويات الموظفين والطلبة هذا ما جعل العديد من الدراسات والكثير من التساؤلات تحوم حول ماهية هذا المجرم ومن له القدرة أو صلاحية ارتكاب مثل هذه الأفعال الغير مشروعة هذا ما جعل جملة من أساتذة القانون الجنائي والفقهاء إلى تقديم دراسات تحليلية من أجل الوصول إلى تقسيمات متعددة ومتباينة وفي بعضها شبه متداخلة والهدف السامي الأساسي منها هو التعريف بالأنماط المختلفة للمجرم المعلوماتي من عدة نواحي وجوانب كل هذا وأكثر سيتضح عند استعراضنا التقسيمات التالية.

الفرع الأول: تقسيم المجرمين المعلوماتيين من حيث السن والخبرة

أولا: «Pranksters»: يمثلون فئة من صغار سن دون سن الأهلية بحيث أنهم متحمسين بالحاسوب ودافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب فالإجرام الإلكتروني يتسم بالذكاء دون الحاجة إلى استخدام القوه والذكاء لديهم هو مفتاح المجرم الالكتروني لاختراق

[1] عامر محمد الحبيب عبد القادر, المجرم المعلوماتي, مرجع سابق،ص46-47

[2] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, للسنة أولى ماستر, تخصص قانون جنائي وعلوم جنائية ,جامعه زيان عاشور, الجلفة,2021-2022، ص03

البرامج المحصنة[1] ويسميهم البعض صغار نوابغ المعلوماتية حيث تضم الأشخاص الذين يرتكبون الجرائم المعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية إحداث أي ضرر للغير وذلك عن طريق استخدام الحاسبات الآلية المحمولة الخاصة بهم أو الحاسبات الآلية الخاصة بمدارسهم ومن بينهم فئة لم تبلغ بعد سن الأهلية فتونين كثيرا بالتقنيات الرقمية على الرغم من صغر سنهم إلا أنهم قادرين على اقتحام بعض أنواع الأنظمة الرقمية البنكية والشركات والمؤسسات المالية.[2]

ثانيا: «Hackers»: تتألف هذه الطائفة من المراهقين والشباب في حالة دراسة أو عاطلا عن العمل تتراوح أعمارهم ما بين 18 و 35 سنة بارعين في استخدام الحاسب الآلي وبرامجه يتحدون اجراءات أمن الشبكات بدافع إثبات الذات دون أن تتوفر لديهم أي دوافع حاقدة أو تخريبية [3]فهي تضم الأشخاص الذين يهدفون إلى الدخول لأنظمة الحسابات الآلية غير المصرح لهم بالدخول اليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف اكتساب الخبرة أو الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة[4] كما أن هذا القسم من القراصنة يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية وهذه الطائفة غالبا ما تكون من هواة الحاسوب ويقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا أو مجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى. [5]

ثالثا: «Crackers»: هم أخطر طائفة من بين مجرمي الكمبيوتر والانترنت تتراوح أعمارهم بين 25 الى 40 سنة تهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم لارتكاب جرائم الحاسوب كما تهدف لتحقيق أغراض سياسية أو التعبير عن موقف فكري او نظري أو فلسفي كما أنهم أفراد يتسمون بالتكتم فلا يتبادلون المعلومات بشأن أنشطتهم ويطورون معارفهم دون الكشف عن طرقهم التقنية لارتكاب جرائمهم طائفة استفادت

---

[1] حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري, مذكرة لنيل شهادة الماستر في القانون الخاص ,جامعة عبد الرحمان ميرة, بجاية,2021-2022 ،ص26.

[2] رزيقة بونار, الجريمة المعلوماتية في التشريع الجزائري, مذكرة مكملة لنيل شهادة الماستر, جامعة محمد الصديق بن يحيى ,جيجل,2020-2021،ص17-18.

[3] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, مرجع سابق ، ص03-04.

[4] لعاقل فريال, الجريمة المعلوماتية في ظل التشريع الجزائري, مذكرة لنيل شهادة ماستر في القانون العام, جامعة آكلي محند أولحاج , البويرة,2014-2015،ص22.

[5] رزيقة بونار, مرجع سابق ، ص15.

كثيرا من التقنيات المطورة من قبل فئة الهاكرز باستخدامها في اعتداءات ذات ميولات إجرامية بحيث يقومون بالتسلل إلى نظم الحاسوب للاطلاع على معلوماته المخزنة أو لإلحاق الضرر أو العبث بها أو سرقتها.[1]

الفرع الثاني: تقسيم المجرمين المعلوماتيين إلى مستخدمين ومبرمجين

أولا: المبرمجين المستخدمين «computer user criminals»: هذه الطائفة من المجرمين المعلوماتيين هم مستخدمين فقط ممن تتوافر لديهم المعلومات الكافية عن آلية عمل الحاسوب ومكوناته ووظائفه الأساسية ومعرفتهم ببعض البرامج التي يجري بها العمل كالبرامج المحاسبية والتطبيقية والتعليمية المختلفة ولديهم أيضا معرفة بعمل الشبكة المعلوماتية حيث يرتكبون جرائمهم دون أن تكون لهم علاقة بالنظم المعلوماتية سوى الاستخدام فحسب ومن أمثلتهم الموظفين في المؤسسات المالية كالبنوك وهذه الفئة من المجرمين في تزايد واتساع وانتشار تبع لتطور نظم تقنية الحاسوب وتعدد استخداماته في مختلف المجالات كما أن طريقه ارتكاب هذه الفئه للجرائم المعلوماتية تتم إما بالدخول إلى مراكز الحاسب الآلي المركزي مباشرة أو بأية وسيلة أو باستخدام إحدى وحدات الحاسوب الآلي الفرعية المرتبطة بجهاز الكمبيوتر المركزي سواء أتم ذلك باستخدام كلمة السر أو باستخدام البطاقات الممغنطة أو بأية وسيلة أخرى تسمح بذلك [2]كما تضم هذه الفئة مجموعة من الأفراد الذين يرتكبون الجريمة خطأ وبدون عمد أي المجرم في هذه الحالة يرتكب فعلا ما ولكن هذا الفعل يؤدي إلى إحداث ضرر بالآخرين كمبرمج الحاسوب الذي غير البرنامج المسؤول عن تحديد مسار الطائرة ولكنه لم يتمكن من إبلاغ قائد الرحلة مما أدى إلى اصطدام الطائرة بأحد الجبال.[3]

ثانيا: المجرمين المبرمجين: نظرا للمستوى المالي الذي يتمتع به المبرمجين وقدرتهم على دخول واقتحام الأنظمة الحاسوبية بكل سهولة على الرغم من أن الاحتياطات الأمنية المتعددة فإن الخطورة واضحة هنا بصورة كبيرة إذ غالبا ما تكون الجرائم المرتكبة من هذه الفئة ضخمة وذات أهمية كبرى ولعل ما يزيد من خطورة هذه الجرائم قلة العناصر القادرة على اكتشافها وهؤلاء مبرمجون قادرون على القيام بتعديل وتحويل ونسخ وإضافة أي معلومات على البرامج بالإضافة إلى قدرتهم على اتلافها وتغيير محتواها لتحقيق أغراض مشروعة بنظرهم كل ذلك يتم باستغلال المساحات الخالية بين أوامر برامج الحاسب الآلي مع الاستفادة من الأوامر الأخرى المحققة لأغراضهم ومن أشهر القضايا بهذا الشان القضايا المتعلقة بإضافة أوامر

---

[1] الدكتورة خلدون عائشة, مرجع سابق ، ص04

[2] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص70-71

[3] الدكتور مشتاق طالب وهيب النعيمي، تزوير المعلومات احد صور الجرائم المعلوماتية ،مرجع سابق،ص83

البرامج المحاسبية في البنوك حيث تضاف أوامر تعالج حالات يترتب عليها جبر كسور عشرية للمبالغ النقدية الموجودة في حسابات العملاء عند كل عملية تجري عليها ثم تحول هذه المبالغ إلى حساب آخر[1] بحيث تعتبر هذه الفئة الأكثر خطورة كونهم مدفوعون بالقوة أو الغضب أو الكراهية وليس لديهم أي مخاوف كما يقومون بتدمير بيانات الشبكة التي يخترقونها فهم عبارة عن قراصنة يتمتعون بمهارات حوسبة ممتازة وجد عالية ينجذبون بحكم أفعالهم للأنشطة الخبيثة بغية تحقيق دوافعهم المتمثلة في إحداث الضرر وسرقة المعلومات بالإضافة إلى تدمير البيانات وكسب المال[2] كما تعتبر هذه الطائفة من المجرمين الأكثر طلبا ورواجا نظرا للخبرة التقنية العالية والمستخدم التي يتمتع بها هؤلاء فقد يستخدمون من قبل أفراد و مؤسسات أو حكومات لاقتحام برامج ونظم حاسوبية معينة لتدميرها أو سرقة ما فيها أو تشويهها مقابل مبلغ من النقود.[3]

الفرع الثالث: تقسيم المجرمين المعلوماتيين من حيث أماكن عملهم:

أولا: المجرمين المعلوماتيين من داخل المؤسسة: يطلق على هذه الفئة عدة تسميات أبرزها الحاقدون أو الموظفون الساخطون هم طائفة غير محددة الأعمار ولا تتوفر لديهم نفس أغراض وأهداف الجريمة المتوفرة لدى الطائفتين السابقتين إنما تحركهم الرغبة بالانتقام من صاحب العمل كونهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة أو بدافع الانتقام كغرباء عن المنشأة المستهدفة في نشاطهم ورغم عدم اكتسابهم المعرفة التقنية الاحترافية إلا أنهم يسعون للاحتراف في أنشطتهم الإجرامية[4] بحكم ارتباط هؤلاء بالنظام المعلوماتي كونه مجال عملهم الأساسي ونظرا لمهاراتهم التقنية المحدودة فإنهم يرتكبون الجرائم المعلوماتية بغية تحقيق أهدافهم الشخصية بحيث تكون غايتهم القصوى في تحقيق الكسب المادي ومنه نستنتج أن العلاقة الوظيفية هي التي تربط بين المجني عليه والموظف الجاني ولحكم العلاقة. بينهما فإنه يسهل عملية ارتكاب الجريمة السيبرانية هذا من جهة ومن جهة أخرى نجد أن هناك فئة من الحاقدين على عملهم وعلى الشركات التي يعملون فيها وهنا تكون العمليات الإجرامية ليس بهدف تحقيق الكسب المادي كما قلنا سابقا بل بدافع الثأر

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص71

[2] الدكتورة أمينة بضافة, الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة, جامعة الجزائر 03 ,حوليات جامعة الجزائر 01 ,المجلد 37/العدد1-2023 ، ص102

[3] الدكتور مشتاق طالب وهيب النعيمي، تزوير المعلومات احد صور الجرائم المعلوماتية ،مرجع سابق،ص83

[4] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, مرجع سابق ، ص04

والانتقام[1] وبالرغم من أن سمات هذه الطائفة صنفها من حيث الخطورة في مؤخرة جميع الطوائف الا أن ذلك لا يمنع من أن تكون الأضرار التي ألحقت خسائر فادحة بالمؤسسات المستهدفة.[2]

ثانيا: المبرمجين المعلوماتيين من خارج المؤسسة: تجمع هذه الفئة بين ثلاثة أصناف أولهم مخترق الشبكات وصانعو الفيروسات «Bwders Virus» وناسخو البرامج « Software crackers» هذه المجموعة تميل أساسا إلى استغلال نقاط الضعف التي اكتشفها المبرمجون الالكترونيون من مختلف الفئات ثم طرق البرمجة لتستفيد من عيوب الكمبيوتر ويطلق البعض على هذه المجموعة من المجرمين إسم «Hacktarst» هذا الإسم المشتق من الجمع بين الكلمتين النشاط والقرصنة والتي تعد من القراصنة الأسرع نموا يتم تحفيزها لتشويه مواقع الويب وشن خدمات رفض الخدمة «DOS» لتلبية الأجندات السياسية أوالدينية أو الاجتماعية أو حتى الشخصية أو يتعاقدون لإختراق الأسرار التجارية أو الدولية أو حتى العسكرية[3] كما تعد هذه الطائفة متخصصة بفك شفرات البرامج وليس تخريب الشبكة إذ يقومون بخرق مقاييس الحماية التي تمنع من استنساخ البرامج أو ما يعرف بكسر رقم التسلسل «serial number» حيث ينطوي تحت هذه الفئة أيضا الأشخاص الذين يقومون بهذه العملية بقصد تحقيق الربح بأنواعه.[4]

الفرع الرابع: تقسيم الأستاذ «parker» للمجرمين المعلوماتيين:

لقد اتجه الأستاذ باركر إلى تقسيم فئة المجرمين المعلوماتيين إلى سبعة أصناف أساسية والتي من الممكن أن يكون المجرم الواحد يتسم أو ينتمي لأكثر من صنف واحد وعلى حسب ما سبق فإن هذه الفئات تتمثل في ما يلي:

أولا: «pranksters»: وهم الأشخاص الذين يرتكبون جرائمهم المعلوماتية بهدف التسلية واللهو وقضاء الوقت دون ان يكون في نياتهم الإضرار بالغير و أبرز من يمثل هذه الطائفة هم صغار مجرمي المعلوماتية أي الأحدث.

---

[1] حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري، مرجع سابق ،ص25

[2] عامر محمد الحبيب عبد القادر, المجرم المعلوماتي, مرجع سابق ،ص63

[3] الدكتورة أمينة بضافة, الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة, مرجع سابق ،ص103

[4] الدكتور مشتاق طالب وهيب النعيمي، تزوير المعلومات احد صور الجرائم المعلوماتية ،مرجع سابق،ص82

ثانيا: «hackers»: هي طائفة تضم المجرمين الذين يقومون بكسر الحواجز الامنية لغرض الدخول الى أنظمة الحاسب التي لم يصرح لهم بالدخول إليها وكل ذلك يتم بغرض اكتساب الخبرة او بدافع الفضول أو التحدي.

ثالثا: «Malicious hackers»: هي طائفة تهدف إلى إلحاق الخسائر بالمجني عليهم وأن يكون هدفها الحصول على مكاسب مادية ومن أمثلتها هؤلاء صانعي الفيروسات وموزعيها

رابعا: «Personal problem solvers»: مجرمي هذه الطائفة هم الأكثر شيوعا بين المجرمين المعلوماتيين حيث أنهم يتمتعون بقدر معقول من الخبرة في هذا المجال و يترتب على ارتكاب جرائمهم خسائر كبيرة تلحق المجني عليهم دون أن يكون الباعث من هؤلاء المجرمين تحقيق أرباح مادية إنما يهدفون إلى إيجاد حلول لمشكلات مادية تواجههم دون أن يستطيعون حلها بوسائل أخرى بما فيها اللجوء إلى الجريمة التقليدية بحيث يبررون أفعالهم لأن المجني عليهم في جرائمهم وهي في الغالب مؤسسات مالية يستطيعون تحمل الخسائر الناجمة عن أفعالهم.

خامسا: « Career criminals»: يمكن القول أن المجرمين الذين ينتمون إلى هذه الطائفة يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة وهم يعملون في الغالب بطريقة منظمة بحيث يمكن أن ينطبق على أفعالهم ومن الجريمة المنظمة إذ يقترب فاعل هذه الجريمة من المجرم التقليدي لاسيما بعد أن أصبحت الجرائم والمعلوماتية تجتذب إهتمام العديد من الجماعات الإجرامية المنظمة لما تدره من عائدات هائلة.

سادسا: «Extreme Advoctes»: تضم هذه الطائفة الجماعات الإرهابية المتطرفة مدفوعين بغايات سياسية أو دينية أو اجتماعية يرغبون في فرضها ويبدو نشاط مجرميها في تحقيق العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إليهم.

سابعا: «The criminally negligent»: وهم طائفة المهملون الذين كثيرا ما يترتب على جرائمهم الواقعة بطريق الخطأ ولا سيما بصورة الإهمال أضرارا قد تؤدي في الكثير من الأحيان إلى حد إزهاق الأرواح.[1]

الفرع الخامس: التقسيم الثلاثي "الإنجليزي" للمجرمين المعلوماتيين:

ذهب بعض الأساتذة في إنجلترا وهم"David Icove" و "karel seger" إلى تقسيم المجرمين المعلوماتيين إلى ثلاثة أصناف أساسية تتمثل حسبهم في التالي:

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص74

أولا: المخترقون أو المتطفلون: ذهب أصحاب هذا التقسيم إلى الجمع بين طائفتي «Hackers» و «crackers» تحت هذه الطائفة من المجرمين المعلوماتيين وذهبوا أيضا إلى طائفة «Hackers» وهم متطفلون يتحدون إجراءات أمن النظم والشبكات دون أن تتوافر لديهم دوافع حاقدة أو تخريبية إنما ينطلقون من دوافع التحدي وإثبات المقدرة أما«crackers» فعلى العكس إذ تتوافر لديهم دوافع إجرامية واعتداءاتهم تنبئ عن خطورة إجرامية ورغبة في إحداث التخريب.

ثانيا: المحترفون: أفراد هذه الطائفة يتميزون بالخبرة وسعة الإدراك للمهارات التقنية والتنظيم والتخطيط للأنشطة المركزية لهذا تعد هذه الطائفة الاخطر بين المجرمين المعلوماتيين بحيث تهدف اعتداءاتهم إلى الكسب المادي لها أو للجهات التي كلفتها بارتكاب الجريمة وفي بعض الأحيان تهدف اعتداءاتهم إلى تحقيق أغراض سياسية أو التعبير عن موقف فكري أو فلسفي كما يتميز أطراف هذه المجموعة بصفة التكتم على أفعالهم الإجرامية فلا يتبادلون الخبرات التقنية فيما بينهم بل يعمدون إلى تطويرها بشكل ذاتي وتجدر الإشارة إلى أن أعمار هذه الطائفة من المجرمين تتراوح بين 20 الى 40 سنة.

ثالثا: الحاقدون: أطراف هذه الطائفة لا يسعون إلى إثبات مقدرتهم أو مهاراتهم التقنية كما أنهم لا يسعون إلى مكاسب مادية أو سياسية بل يرتكبون انشطتهم الإجرامية بدافع من الثأر والانتقام ولهذا فهم مقسمون إلى مجرمين على علاقة بالنظام وآخرين غرباء عن النظام وقد يتطور إجرام هؤلاء إلى المستوى الدولي حيث تشن دولة ما حربا إلكترونية على دولة أخرى بدافع الإنتقام لتعطيله أو تخريب أنظمتها الإلكترونية الخدمية في ظل ما يعرف اليوم ب«الحكومة الإلكترونية».[1]

في الأخير وبعد تعرضنا إلى دراسة العديد من تقسيمات الفقهاء القانونيين نخلص إلى أن المجرم المعلوماتي مجرم ذو طبيعة خاصة مميزة ليس له نطاق واحد معين يحصره بل نجد له عدة تفرعات في البيئة الإفتراضية التكنولوجية بحيث يتنوع مجرم هذا المجال بحسب نوع الجريمة التي يختلفونها ومن حيث السن والخبرة التي يتمتع بها الجناة أو بحسب اعتمادهم على معيار المعرفة بالنظم الإلكترونية مستخدمين كانوا أو مبرمجين أو حتى من حيث أماكن عمل هؤلاء المجرمين وغيرها الكثير ففي إظهار التخصص الواحد نجد طوائف فرعية جمة تضم مجموعة معينة من الجناة الالكترونيين بالرغم من أن المجرم الواحد قد ينتمي إلى أكثر من

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،الجرائم المعلوماتية، مرجع سابق،ص75-73-77

طائفة وتخصص وهذا جزء بسيط مما يخفيه المجرم المعلوماتي من خطورة وغموض أثناء اقترافه بعض السلوكيات الغير مشروعة.

المطلب الثالث: خصائص وسمات المجرم المعلوماتي

لقد انجر عن ما شهده العصر الحديث من جرائم معلوماتية حديثه العهد نقلة نوعية في جل المجالات ومختلف المجتمعات ولعل أبرز ما لفت الإنتباه هو ولادة جيل جديد من المجرمين المعلوماتيين مجرمين يختلفون إختلاف جذري عن باقي طوائف المجرمين التقليديين وهذا راجع للبيئة الرقمية التي ترعرع بها وأصبحوا جزءا لا يتجزأ منها ما لفت انتباه أكبر عمداء وأساتذة الفقه الجنائي بغية دراسة هذه الفئة إضافة إلى تحديد أهم وأبرز ما يميزه هؤلاء المجرمين عن غيرهم من طوائف الحياة الجنات العاديين سواءا من ناحية السمات الخاصة التي ينفردون بها عن البقية أو من حيث الصفات العامة التي قد يشتركون بها مع باقي المجرمين التقليديين وعليه يمكننا إجمال أهم وأبرز ما يتسم ويختص به المجرم المعلوماتي في نطاق الجريمة الإلكترونية وذلك على النحو التالي:

الفرع الأول: مجرم معلوماتي ذكي

يتصف المجرم الإلكتروني بالذكاء العالي وقدر كبير من سرعة الفهم وسرعة الإطلاع بالإضافة إلى النشاط الذهني المتقدم الذي يسعى إلى خداع مختلف الأجهزة الرقمية حيث يستغل مهاراته النفسية في اختراق الشبكات وكسر كلمات المرور أو الشفرات كما يستطيع أن يكون تصور كامل لجريمته قبل تنفيذها وما يمكن ملاحظته في العديد من القضايا المطروحة على مختلف المحاكم أن المجرم الإلكتروني متخصص فقط في الجريمة الإلكترونية دون الجرائم العادية ولا تكون لديه له أي علاقة بهذه الاخيرة لأنه ينتمي إلى إجرام الحيلة[1] والذي يعتبر نوعا معين من القدرات الذهنية والدراية بأحدث ما توصلت إليه التقنية الرقمية وما يجعله يمتلك القدرة على التفكير وفهم العلاقات بين العناصر المكونة لموقف ما فالمجرم في هذا المجال يمتلك القدرة على الإدراك بطرق جديدة بمعنى أن يكون مبدعا ما يتضمن الطلاقة والمرونة والأصالة الإلكترونية الرقمية بالإضافة إلى امتلاكه القدرة على معرفة ذاته وارضائها والقدرة على التعامل مع الأرقام واستخدامها بما يحقق أهدافه الإلكترونية الإجرامية هذا ما يمكنه من رؤية علاقة الأشكال أو الأشياء مع بعضها البعض في الفضاء الإلكتروني[2] وما يجعل سنة الذكاء من أبرز صفات مرتكبي الجرائم الإلكترونية وما تتطلبه جرائمهم من المعرفة التقنية الكافية و

---

[1] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, جامعة محمد لمين دباغين, سطيف 02,2022-2023،ص08

[2] الدكتور مشتاق طالب وهيب النعيمي، تزوير المعلومات احد صور الجرائم المعلوماتية ،مرجع سابق،ص75

الاحترافية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج بطريقة تمكنهم من ارتكاب جرائم السرقة والنهب وغيرها من الجرائم بطريقة أسهل وأكثر أمانا[1]

الفرع الثاني: مجرم معلوماتي محترف

يتمتع هذا النوع من المجرمين بالاحترافية الكبيرة في تنفيذ الجرائم بالكمبيوتر الأمر الذي يقتضي الخبرة والمهارة التقنية بحيث أنه لا يمكن لأي شخص ارتكاب هذا النوع من الجرائم دون المعرفة التامة بكيفية التعامل مع الجهاز والإنترنت وكذا الهواتف الذكية المستعملة بشبكة الإنترنت ومختلف البيانات والمعلومات بشكل منهجي دقيق الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر[2] كما تمكنه هذه المهارات والقدرات التقنية على توظيفها في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال[3] كما يتطلب هذا النوع من الإجرام مهارة فنية عالية لا يستطيع الشخص العادي المبتدئ القيام بها إذ تتطلب هذه الجريمة قدرا من الدقة والتخصص لتجاوز العقبات الإلكترونية وهذا الإحتراف أو المهارة يكتسبه المجرم المعلوماتي إما من خلال الدراسة في مجال تكنولوجيا المعلومات عن طريق الخبرة العملية في هذا المجال أو من خلال التفاعل الاجتماعي مع الآخرين.[4]

الفرع الثالث: مجرم معلوماتي غير عنيف

يقال في العادة ان المجرم المعلوماتي مجرم غير عنيف مقارنة بالمجرم التقليدي الذي يميل في إجرامه إلى العنف كالضرب والقتل والجرح فإذا كان من الممكن تصور قيام العنف في جرائم الاعتداء على الحاسب أي ماديات الحاسب غير أن هذا النوع من الإجرام المعلوماتي كإتلاف المعلومات مثلا لا يتطلب عنفا ماديا محسوسا كونه من تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات او الكيانات المنطقية أو حتى البيانات ومثل ذلك يقال أيضا بالنسبة لسرقة البيانات أو الاحتيال المعلوماتي أو ما شابه من الجرائم المعلوماتية التي يتمثل سلوك الجاني فيها بشكل معالجة فنية هادئة للمعطيات الإلكترونية والتي تتم بكل هدوء وروية وبدون أي عنف يذكر كما أن هذا النوع من المجرمين يتمتع باحترافية جد عالية في

---

[1] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ،مرجع سابق، ص38

[2] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, ،مرجع سابق، ص08

[3] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص62

[4] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص61

تنفيذ أفعالهم الغير قانونية إلا أنهم لا يلجأون إلى العنف الجسدي وإنما قد ينتج عن فعلتهم الإجرامية عنف معنوي كجريمة السب والقذف عبر مواقع التواصل الإجتماعي بالإضافة للجرائم الإرهابية الإلكترونية التي تهدف إلى بث الخوف والرعب وسط المواطنين وإذا نجم عن فعله قتل فلا يكون قد لجأ فيه إلى العنف الجسدي بل مجرد حيل تقنية كالألعاب الإلكترونية التي خلفت الكثير من الضحايا ودفعت بهم إلى قتل أنفسهم أو ذويهم دون لجوء المجرم فيها إلى العنف الجسدي[1] ولعل أبرز الأمثلة التي شهدها المجتمع هي بعض الألعاب الإلكترونية الدخيلة على مجتمعنا والتي أدت بالكثير منهم للهاوية أبرزها ما يلي:

- لعبة مريم الإلكترونية.

- لعبة الحوت الأزرق التي تؤدي للإنتحار لعبة الشيطان الحزين

- لعبة البوكيمون جو

- لعبة جنية النار التي تقتل الأطفال بواسطة الألغاز

الفرع الرابع: مجرم المعلوماتي اجتماعي

يقال أن المجرم الإلكتروني شخص إجتماعي لكونه لا يضع نفسه في حالة عداء سافر مع المجتمع المحيط به بل هو إنسان متوافق مع من حوله فمعدل الذكاء المرتفع لديه يساعده على عمليه التكيف داخل الوسط الإجتماعي فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف ولا يعني التقليل من شأن المجرم الإلكتروني بل أن خطورته الإجرامية قد تزداد إذا ما زاد تكيفه واندماجه الإجتماعي مع توفر الشخصية الإجرامية لديه[2] كما أن هذا التكيف يحتوي على حقيقتين.

- الأولى تتمثل في تكيف المجرمين المعلوماتيين فيما بينهم حيث تعتبر هذه الخاصية امتداد لسمات التخطيط والتنظيم مثل التكيف الاجتماعي لمجموعة لها صفات مشتركة مثل نوابغ صغار المعلوماتية ولا شك أنهم يتكيفون في أفكارهم وهذه الروابط تتعدى النطاق المحلي إلى المجال الدولي.

- أما الحقيقة الثانية وتكمن في تكيف المجرم المعلوماتي الذي لا يضع في نفسه حالة عداء مع محيطه كما أن تكيفه مع نفسه يزيد الثقة بأنه خارج إطار الشبهات وهذا الشعور يدفعه إلى التمادي في ارتكاب جريمته. [3]

---

[1] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, ،مرجع سابق، ص08

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ،مرجع سابق، ص39

[3] مرابطن حياة, الجريمة الإلكترونية في التشريع الجزائري, ،مرجع سابق، ص26

فهذا المجرم المعلوماتي وعند شعوره أنه محل ثقة وخارج إطار الشبهات كما ذكرنا سابقا قد يدفعه إلى التمادي بصورة كبيرة في اقتراف أفعاله الغير مشروعة والتي قد لا تنكشف مطلقا أو تواجه صعوبة في الإثبات ونقص الأدلة وكذا الخبرة لدى المحققين ورجال القضاء والملاحظ أن تكيف هؤلاء الأشخاص داخل الوسط الاجتماعي يكون محدودا وغالبا ما يكونون منعزلين عن الناس.[1]

الفرع الخامس: مجرم معلوماتي عائد للإجرام

يعمد الكثير من مجرمي المعلوماتية في الغالب إلى العودة مرة أخرى إلى ارتكاب جرائمهم انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم ومن ثم كشف جرائمهم وتقديمهم إلى المحاكمة[2] ورغم تميزه بأنه عائد للجريمة دائما الا أنه يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين المعلومات والبيانات بالإضافة إلى التحكم في أنظمة الشبكات من حيث الدخول الغير مصرح به لمرات ومرات فهو لا يحقق جريمته في الإختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في إختراق مختلف الأنظمة الحاسوبية

وقد تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم دون غيرها من الجرائم التقليدية مما تبين أن المجرم في الغالب متخصص في هذا النوع من الإجرام فقط [3]ومن الأمثلة الشهيرة على ذلك ما قام به الهاكرز البريطاني جاري ميكنون "Gary mckinnon" الذي إخترق حسابات وكالة الفضاء الامريكية ناسا "nasa" بين سنتي 2001 و 2002 حيث تم القبض عليه للمرة الأولى سنة 2002 ولكن السلطات أفرجت عنه لعدم كفاية الأدلة الموجهة ضده ثم تم القبض عليه مرة أخرى في سنة 2005 حيث حكم عليه بالوضع تحت المراقبة وبالحرمان من إستخدام شبكة الإنترنت مرة أخرى[4]

الفرع السادس: مجرم معلوماتي متخصص

المجرم المعلوماتي مجرم متخصص أو محترف في تنفيذ جريمته الإلكترونية حيث أن ارتكابها يتطلب التغلب على تقنيات الحماية لأنظمة الكمبيوتر خلافا على المجرم العادي المجرم

---

[1] غربي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, ،مرجع سابق، ص28

[2] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص62

[3] مرابطن حياة, الجريمة الإلكترونية في التشريع الجزائري, ،مرجع سابق، ص24-25

[4] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ،مرجع سابق، ص40

المعلوماتي مجرم ذكي يتمتع بالمهارة والمعرفة بدرجة عالية من الثقافة[1] كما له قدرة هائلة في مهارة التقنية عن طريق إستغلال مداركه ومهاراته في إختراق الشبكات وكسر كلمات المرور أو الشفرات ويصبح في عالم الإلكترونيات ليحصل على كل غالي ونفيس من البيانات والمعلومات الموجودة على أجهزة الحواسيب ومن خلال الشبكات الرقمية[2] حيث أثبتت العديد من الدراسات في هذا المجال أن المجرمين المعلوماتيين وهم في الغالب لا يرتكبون أفعال إجرامية سوى هذا النوع من الجرائم لتخصصهم فيه [3]وهذه الخاصية تعد من أبرز وأهم سمات المجرم المعلوماتي التي ينفرد بها عن غيره من طوائف المجرمين.

الفرع السابع: المجرم المعلوماتي شخص حذر جدا

يتسم المجرم الإلكتروني بأنه شخص حذر بدرجة عالية وذلك خشية إكتشاف أمره فهو وبقدر تكيفه مع المجتمع الحقيقي إلا أنه قادر كذلك على التكيف وبشكل موازي مع عالم الجريمة الالكترونية والذي يعتبر مجالا خاصا به فالحذر الدائم للمجرم المعلوماتي يدفع به إلى اتباع أسلوب تدمير ومحو كل الدلائل الناتجة عن فعله من خلال محو بيانات[4] كما يتصف مجرمو المعلوماتية من كشف جرائمهم بالرغم من أن هذا الحذر يصاحب المجرمين على إختلاف أنماطهم إلا أن أغلب ما يتميزون به هم مجرمي المعلوماتية بصفة خاصة وذلك لما يترتب على كشف أمرهم من ارتباك مالي وفقد للمركز الوظيفي وإن وجد في الكثير من الأحيان.

كما ان طبيعة الأنظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله ذلك أن كثيرا ما يعرض المجرم إلى إكتشاف أمره هو أن يطرأ أثناء تنفيذ جريمته عوامل غير موفقة في حين أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي الحواسيب إنما تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها فخوف المجرم المعلوماتي وحذره والجديد منك من إنكشاف أمره عائد إلى انتمائه في الغالب الى الوسط الاجتماعي سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل[5]

---

[1] رزيقة بونار, الجريمة المعلوماتية في التشريع الجزائري, ،مرجع سابق، ص15

[2] الدكتور محمد شرقي, الدكتور صلاح الدين جبار, تأثير تطور تكنولوجيا المعلوماتية على تنامي الجريمة, جامعة لونسي علي, البليدة 02 ،ص04

[3] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص63-64

[4] بن يونس محمد الأمين بن مصطفى, خير الناس عمر بن إبراهيم, حماية الأطفال من الجريمة الإلكترونية, مذكرة مقدمة لاستكمال نيل شهادة الماستر, جامعة غرداية,2022-2023،ص27

[5] غربي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, ،مرجع سابق، ص29

الفرع الثامن: المجرم المعلوماتي متسلط

يعني بالسلطة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي من خلالها يستطيع القيام بالسلوك الإجرامي فالمجرم الإلكتروني يتمتع بالسلطة المباشرة أو غير المباشرة في مواجهة المعلومات محل الجريمة المتمثلة في الرقم السري الخاص للدخول إلى النظام الذي يحتوي على جملة من المعلومات والتي تمد الجاني بمزايا كفتح الملفات ومحو المعلومات أو تعديلها وقراءة الملفات وكتابتها وقد تتمثل هذه السلطة في حق إستعمال الأنظمة المعلوماتية وكذا الدخول إلى الأماكن التي تحتوي على الأنظمة الإلكترونية كما أن نظام التخطيط والتنظيم في علم الإنترنت والشبكات الإلكترونية يقوم بمعظم أعمالها الإجرامية أفراد أو مجموعات صغيرة كما هو الحال في الواقع المادي حيث ترتكب أغلب الجرائم من طرف مجموعات متكونة من عدة أفراد يحدد لكل شخص دوره ويتم ذلك وفقا لتنظيم وتخطيط مسبق من رئيس المجموعة[1] وأيضا قد تتمثل هذه السلطة في الحق في إستعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة[2] وقد يستغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها فيضيف بيانات وهمية وغير صحيحة ويطلب الحاسوب اعتمادها عند إجراء بعض العمليات ومثالها الموظف المشرف على الموظفين في مصالح المحاسبة وصرف الأجور ما يمكنه من إدراج بعض أسماء الموظفين الوهميين ضمن القائمة ثم يمرر عملية صرف الرواتب ويتولى إيداع الرواتب للموظفين الوهميين في حسابه الخاص[3] كما يتصف المجرم المعلوماتي أيضا بأنه يملك سلطة ما على النظام المعلوماتي المستهدف العبث به ما تجعله مسيطرا ومتحكما نوعا ما بحيث تكون هذه السلطة مباشرة مثل من يملك تصريح بالدخول إلى غرفة الأنظمة المعلوماتية المتمثلة في الحسابات الآلية وأدواتها دون حق في الولوج إلى نظام معلوماتي معين.[4]

الفرع التاسع: السمات التي أوردها الأستاذ "باركر"

يعد الأستاذ باركر واحدا من أبرز الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصه إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص غير التي

---

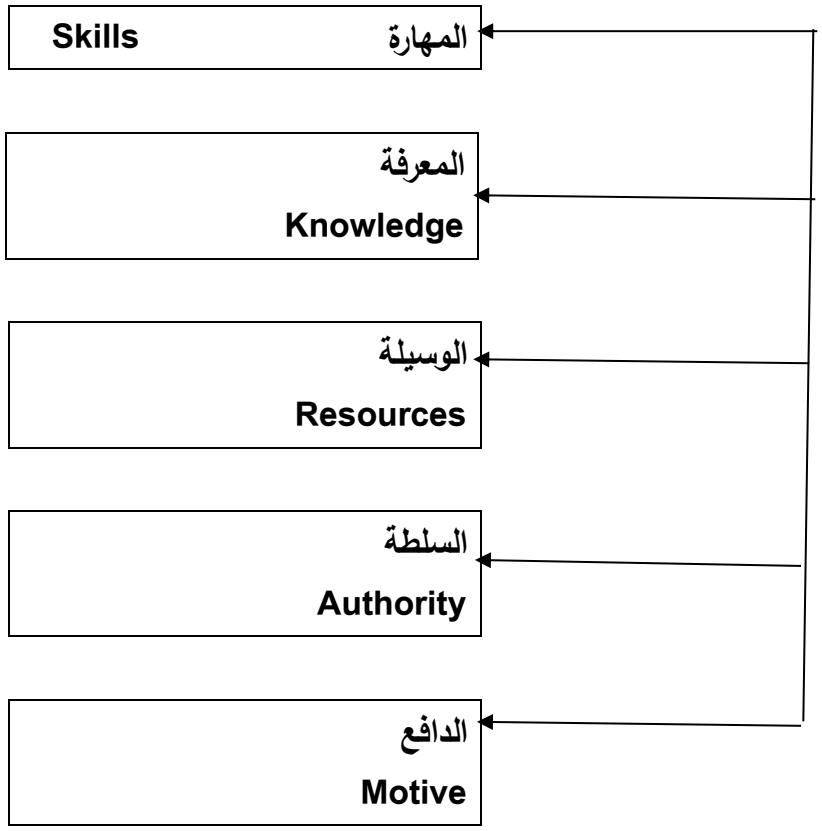
[1] حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري ، مرجع سابق، ص23-24

[2] غربي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, ،مرجع سابق، ص29

[3] عامر محمد الحبيب عبد القادر, المجرم المعلوماتي, ،مرجع سابق، ص57-58

[4] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, ،مرجع سابق، ص03

ذكرناها سابقا والتي تميزه بصفة عامة عن غيره من المجرمين بحيث يرمز لها الاستاذ باركر بكلمة S.K.R.A.M والتي تعني:[1]



S.K.R.A.M[2]

أولا: المهارة «Skills»: تعد هذه السمة من أبرز خصائص المجرم المعلوماتي والتي تعد متطلبة لتنفيذ النشاط الإجرامي بحيث قد يكتسبها الجاني عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات أو بمجرد التفاعل الإجتماعي مع الاخرين إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال بل أن الواقع العلمي قد أثبت أن بعض انجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.[3]

[1] لعاقل فريال, الجريمة المعلوماتية في ظل التشريع الجزائري, ،مرجع سابق، ص19-20

[2] الدكتورة بوقرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري ، مرجع سابق ، ص53

[3] لعاقل فريال, الجريمة المعلوماتية في ظل التشريع الجزائري, ،مرجع سابق، ص20-21

ثانيا: «Knowledge»: المعرفة تعني هذه الخاصية تصرف الجاني على كافة الظروف والملابسات المحيطة بجريمته التي يروم تنفيذها واحتمالات نجاحها أو حتى فشلها إذ أنه من البديهي أن يتعرف الجاني على المحيط الذي تدور فيه حتى لا يواجه ما لا يتوقعه بما يؤدي إلى فشل جريمته إذ يقوم مجرم المعلوماتية في تجربة جرائمه على محيط مفترض في الحاسب أو شبكة الإنترنت قبل الشروع بها فعلا للتعرف على مدى نجاحها.[1]

ثالثا: الوسيلة «Resources»: يراد بها الإمكانية التي يتزود بها الفاعل لإتمام جريمته المعلوماتية وفيما يتعلق بالمجرم المعلوماتي فان الوسائل المتطلبة للتلاعب بأنظمة الحسابات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وسهولة الحصول عليها أبرزها جهاز الحاسب الآلي.[2]

رابعا: الباعث الدافع «Motive»: لا يختلف الباعث في الجريمة المعلوماتية في الغالب عن الباعث في الجرائم الأخرى التقليدية إذ تارة تكون الرغبة في الإنتقام وتارة أخرى يكون بسبب تحقيق الربح المادي وأخرى في تحدي الأنظمة لحماية جهاز الحاسوب أوشبكة الإنترنت أما الحقيقة هي أن الباعث أيا كان فإن الشعور الذي يخالج معظم المجرمين المعلوماتيين يتمثل في أنهم ليسوا بالمجرمين وأنما يقومون به لا يدخل في عداد الجرائم. [3]

خامسا: السلطة «Authority»: يقصد بالسلطة الميزة او الحق الذي يمكن المجرم المعلوماتي من ارتكاب جريمته إذ أن غالب مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة وهذه السلطة قد تتمثل في الشفرة الرقم السري الذي يمكنه من فتح الملفات المخزنة ومن ثم نسخها او تعديلها أو اتلافها أو حتى سرقتها كما قد تكون السلطة التي يتمتع بها الجاني غير حقيقية كشفرة الدخول الخاصة بشخص آخر.[4]

---

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص63

[2] لعاقل فريال, الجريمة المعلوماتية في ظل التشريع الجزائري, ،مرجع سابق، ص21

[3] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص63

[4] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص64

المطلب الرابع: دوافع مرتكبي الجريمة المعلوماتية

تتباين الدوافع المؤدية لارتكاب الجريمة الإلكترونية تبعا لطبيعة المجرم ومدى ثقافته ومعرفته بمجال الحاسب الآلي[1] هذا ما يجعل دوافع هذا النوع من الإجرام لا تكاد تختلف كثيرا عن الإجرام التقليدي من حيث المبدأ مع الاشارة إلى أن هذه البواعث لا تؤثر في التكييف القانوني للجريمة في ظل العديد من التشريعات الجنائية إذ لا عبرة منها ولكن تظل دراسة هذه البواعث والأسباب امرأ مهما من الناحية العلمية لعله يفيدنا في تحديد أهم المعالجات التشريعية لجرائم المعلوماتية من حيث تشديد العقوبة في بعض الجرائم او تنظيم أحكام المواد وتشريع العقوبات الملائمة[2] على أساس ما سبق تتجلى أبرز هذه الدوافع سواء كانت شخصية أو موضوعية فيما يلي:

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية

تعتبر الدوافع الداخلية للإنسان والمرتبطة بشخصيته الذاتية السبب الرئيسي والأول في إقدامه نحو السلوك الإجرامي بغية تحقيق أهداف ذاتية خاصة سواء كانت مادية أو معنوية و سنبين ذلك على النحو التالي:

أولا: الدافع المادي: يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية ذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم إلى تطوير نفسه حتى يواكب كل حديث يطرأ على مجال المعلوماتية واستغلال الفرص والسعي إلى الإحتراف بغية تحقيق مكاسب بأقل جهد دون ترك أي أثر يذكر فالإنسان بغية تلبيته حاجياته الأساسية الفيزيولوجية كانت أو الاجتماعية فإنه يحتاج إلى المال الذي يعد عصب الحياة هذا ما يجعل مرتكبي الجريمة الإلكترونية يوفرون الكثير من المعلومات التي يمكنهم من خلالها إستخدامها واستغلالها وبيعها في ظل عصر بيع المعلومات التي ساهمت في تطور سوق المعلومات بإختراق أنظمة وبيانات الدول والهيئات والمؤسسات وهذا ما مثل دافعا أساسيا لإرتكاب مثل هذه الجرائم بل يعد المحرك الأول والأساسي لها[3] ففي دراسة الفقيه البريطاني باركر الصادرة في احد المجلات المتخصصة بخصوص موضوع الأمن المعلوماتي تبين أن:

- **34% من جرائم الغش المعلوماتي من أجل اختلاس الأموال**
- **23% من أجل سرقة المعلومات**

---

[1] الدكتورة شنتير خفرة، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية،مرجع سابق ،ص40

[2] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص64

[3] حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري،, ،مرجع سابق، ص14

- 19% من اجل الاتلاف

- 15% من اجل سرقة وقت الحاسوب لأغراض شخصية

وإذا انتقلنا لدراسات حديثة فسنجد أن الدافع المادي يسود على غيره ويعكس استمرار إتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية وفي مقدمة هذه الدراسات المسحية والاحصائية الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية [1]وغالبا ما يكون الدافع لارتكاب هذه الجرائم وقوع الجاني بمشاكل مادية كعجزه عن سداد ديونه المستحقة أو لوجود مشاكل عائلية تعود إلى عدم توفر الأموال أو شراء المخدرات حيث يسعى الجاني للخروج من هذا المأزق إلى عمليات التلاعب بالأنظمة المعلوماتية للبنوك المؤسسات المالية وذلك بواسطة إختراق الأنظمة لها واكتشافه لفجواتها الأمنية.[2]

ثانيا: دافع التحدي وقهر النظام المعلوماتي: هناك طائفة عريضة من الناس يخالجهم الشعور بالفخر إذا ما تمكنوا من إختراق مواقعها على شبكة الإنترنت أو وصلوا إلى قاعدة بيانات محمية حيث يعد ذلك من الأمور التي يتباهون بها أمام أقرانهم ويشبعون بها فضولهم ويثبتون بها قدراتهم على إختراق البرامج ويسعون من خلالها إلى تحقيق شهرة ما مع العلم أنهم قد لا يملكون المعرفة الحقيقية لشن الهجمات الإلكترونية ولكنهم يستعينون ببرامج موجودة على شبكة الإنترنت وهم من يسميهم المتخصصون في مجال أمن المعلومات بأطفال البرامج الجاهزة «seiht kidders»[3] هذا ما جعل جملة من إدارة المواقع الإلكترونية تذهب الى تأمين مواقعها بشكل محكم من خلال تعقيد الأرقام السرية وتغييرها باستمرار وهذا ما زاد من تحفيز الكثير من المجرمين المعلوماتيين المحترفين على الدخول في تحدي مع أنفسهم أولا وأنظمة تلك المواقع ثانيا من أجل قهر نظم الحماية تلك واختراقها والغالب في هذه الفئة عدم الخطورة إنما هم يلجأون إلى هذه الأفعال بدافع التحدي وإثبات الذات.[4]

ثالثا: دافع التسلية والمزاح: يعتبر هذا الدافع من الدوافع التي تجعل الشخص يقوم بتصرفات لا يقصد من ورائها إحداث جرائم وإنما بغرض مزاح إلا أن هذه التصرفات قد تنتج عنها نتائج

---

[1] لعاقل فريال, الجريمة المعلوماتية في ظل التشريع الجزائري, ،مرجع سابق، ص24-25

[2] غربي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, ،مرجع سابق، ص34

[3] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية،مرجع سابق ،ص41-42

[4] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص66

ترقى إلى درجة الجريمة[1] كما قد يتداخل هذا الدافع مع الدافع السابق وقد يكون صورة من صوره حيث يعمد بعض المجرمين المعلوماتيين ممن لديهم شغف وولع بالأنظمة المعلوماتية إلى محاولة إظهار تفوقهم أو مستوى براعتهم التقنية وهم غالبا ما يكونون مدفوعين بدافع التسلية.[2]

الفرع الثاني: الدوافع الموضوعية لإرتكاب الجريمة الإلكترونية

تتمثل الدوافع الخارجية في جملة من العوامل والأسباب التي ليس لها علاقة بالذات الشخصية للأفراد بل تنسب إلى الواقع المحيط بالإنسان وما يتعرض له من مواقف قد تدفع به لإتيان فعل إجرامي إلكتروني لا يسعى من خلالها المجرم والمعلوماتي لمكاسب شخصية بل إلى الإنتقام وإبعاد الضغوطات العامة المحيطة به والتي سنتناولها في العناصر التالية:

أولا: دافع الانتقام: يعد دافع الانتقام من أخطر الدوافع التي تدفع بالشخص لارتكاب الجريمة وغالبا ما يصدر هذا الفعل من شخص يملك معلومات كبيرة عن الشركة أو المؤسسة التي يعمل بها إذ أن أسباب هذا الدافع تتعلق بالوظيفة التي يشغلها وذلك حيث يشعر بالحرمان من الحقوق المهنية أو التعرض للطرد من الوظيفة حيث يتولد لدى المجرم المعلوماتي الرغبة في الإنتقام من رب العمل ومن أمثلة ذلك ما قام به شاب هندي يبلغ من العمر 16 سنه قام بإنشاء موقع إباحي على شبكة الإنترنت للانتقام من زملائه في الدراسة الذين كانوا يسخرون منه حيث تضمن الموقع نصوصا بأسماء بعض من زملائه وزميلاته ومعلميه بها تعليقات غير أخلاقية بجانب إسم كل واحد منهم بتاريخ 2001/04/27 علقت عليه الشرطة القبض وقدم للمحاكمة فحكمت عليه محكمة الجنح الهندية بالحبس[3]

ثانيا: الدوافع السياسية: يتميز العصر الحالي بظهور الكثير من المنظمات التي تتبنى بعض الأفكار والآراء السياسية والدينية والإيديولوجية والتي تدافع عنها بارتكاب أفعال إجرامية ضد معارضيها مثل مناداة أحد التجمعات في أواخر الثمانينات بضرورة الإعتراف بحق جديد للإنسان يتمثل في حق التواصل بين مختلف الأطياف الإنسانية عبر العالم دون قيود[4] كما شهدت أيضا السنوات المنصرمة وجود حرب سياسية إلكترونية بين العديد من الدول لا سيما في حالات الحرب والاختلافات السياسية كإختراق المواقع الإلكترونية لدولة أخرى والتجسس

---

[1] بن يونس محمد الأمين بن مصطفى, خير الناس عمر بن إبراهيم, حماية الأطفال من الجريمة الإلكترونية، مرجع سابق، ص29

[2] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص66

[3] الدكتورة شنتير خفرة، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية،مرجع سابق، ص43

[4] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, ،مرجع سابق، ص06

عبر الإنترنت الذي بات من أبرز الوسائل المخابراتية أو تدمير بعض المواقع الرسمية لإيقافها عن العمل ناهيك على أن بعض المجرمين المعلوماتيين غير المنتمين إلى جهات سياسية أو حكومية قد يقومون بدوافع سياسية وطنية بإختراق المواقع الإلكترونية لبلدان معادية لبلدانهم[1] فمثالها ما قام به بعض القراصنة المتواجدين على الأراضي السورية بإختراق الحسابات الحكومية في الولايات المتحدة الأمريكية لمدة عام كامل حيث قاموا بسرقة معلومات غير سرية ولكنها حساسة من أجهزة الحواسيب عسكرية الأمريكية.[2]

ثالثا: دافع التعاون والتواطؤ: هذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية يقوم بالجانب الفني من المشروع وآخر من المحيط أو خارج المؤسسة المجني عليها لتغطية التلاعب وتمويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة [3]أو يشكلون جماعات للإجرام في هذا المجال بحيث يتعاونون من أجل إتيان الأفعال الإجرامية بدقة لتحقيق أهداف مشتركة بينهم وهذا النوع يتكرر كثيرا في المجال الالكتروني.[4]

[1] الدكتور عمار عباس الحسيني ، جرائم الحاسوب و الانترنت ،, ،مرجع سابق، ص66

[2] الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية،مرجع سابق ،ص44

[3] الدكتورة بوقرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري ، مرجع سابق ، ص54

[4] حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري، مرجع سابق ، ص18

الفصل الثاني

المكافحة التشريعية للجريمة الالكترونية

الفصل الثاني: المكافحة التشريعية للجريمة الالكترونية

في إطار الإتجاه نحو التحول الرقمي والتقني وبعد استفحال ظاهرة الجرائم الإلكترونية وما إنجر عنها من خسائر لا تعد ولا تحصى أضحت الجرائم ترتكب بمجرد لمسة زر واحدة أو إدخال رمز ما يعد كفيل بخلق فوضع عارمة وهذا يتجسد في إظهار حجم التغيير الحاصل في مجال السلوك الإجرامي فالجريمة بمفهومها المتداول هي تلك الظاهرة الاجتماعية التقليدية التي تتضمن أفعالا مجرمة قانونا غير أن العصر الحالي خالف ذلك مع إستبيان الجريمة الإلكترونية الحديثة و المستحدثة جريمة تستغل التطورات التكنولوجية المعاصرة لارتكاب أفعال لم تكن موجودة قبلا مع هذا التصعيد الغير مسبوق كان لابد من تكاثف المجهودات والخبرة المختصة في هذه المجالات على رأسهم مجال الأمن المعلوماتي تحت سقف قانوني واحد بقصد رصد ومكافحة هذه السلوكيات الغير مشروعة قانونا وهذا ما دفع بالمشرع الجزائري شأنه شأن باقي النظم القانونية في العالم لمواجهة تحديات جمة في مواكبة التطورات المتسارعة في مجال التكنولوجيات المعلومات وما صاحبها من ولادة جيل جديد من الجرائم الخفية ذات الطبيعة المعقدة، وتلبية لهذه الإحتياجات لجأ المشرع الوطني الجزائري للاستعانة بآليات تشريعية متنوعة من خلالها يتسن له سن أحكام رادعة وعقوبات صارمة بغية مكافحة هذا النوع الجديد من الجرائم مع ضمان الحفاظ على مصالح الأفراد وصيانته حقوقهم مستندا في ذلك إلى مجموعة من القواعد العامة وكذا الخاصة منها لبناء أساس يحتوي على هذه الأفعال الجنائية بهدف مكافحة الجريمة الإلكترونية وضمان أمن وسلامة الفضاء الرقمي في العالم الإفتراضي وعلى ضوء ما سبق تطرقنا في هذا الفصل لأهم وأبرز القواعد والركائز القانونية لمكافحة الجريمة المعلوماتية وهذا ما قمنا بدراسته من خلال مبحثين المبحث الاول والذي خصص للقوانين العامة المتمثلة في الدستور وقانون العقوبات من ثم القانون المدني وقانون الإجراءات الجزائية وكيف احتوت هذه التشريعيات كل على طريقته صد وردع هذه السلوكيات أما المبحث الثاني فقد خصصت لدراسة القوانين والنظم الخاصة التي جاءت بحلة إستثنائية لقمع ومواجهة أبرز الأسس والأعمدة التي تقوم عليها الجريمة المعلوماتية.

المبحث الأول: مكافحة الجريمة في القوانين العامة

تداركا للفراغ التشريعي القائم في مجال الإجرام الإلكتروني وما صاحبها من تبعيات وخيمة مست كل من أفراد المجتمع والدولة منذ أواخر الألفيات الفارطة حيث باتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم الإلكترونية وتجاوبا مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال عمد المشرع الجزائري إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية سواء من جانب التنظيم أو من جانب الحماية والتحرير والتجريم بهدف التصدي للأسباب الجوهرية المسؤولة عن تكوين السلوك الاجرامي وهي من الأمور التي أولاها المشرع أهمية قصوى من خلال القوانين الوطنية العامة وعليه قسمنا هذا المبحث إلى أربعة مطالب أولهم خصص لعمدة القوانين و هو الدستور أما المطلب الثاني فقد تناول قانون العقوبات وأبرز ما عدل فيه ثم المطلب الثالث تحت عنوان القانون المدني أما المطلب الرابع والأخير فيه قمنا بدراسة قانون الإجراءات الجزائية.

المطلب الأول: مكافحة الجريمة بموجب الدستور.

حاول المشرع الجزائري إصدار العديد من القوانين العامة من أجل التصدي للجريمة المعلوماتية فقام بعدة جهود لمحاربة قراصنة الإنترنت وكيفية القبض عليهم وإحالتهم على الجهات القضائية المختصة متأثرا بذلك بمختلف التشريعات ومن أبرز المسائل التي أولها المشرع اهتمام في هذا النوع من الإجرام تلك التي تستهدف الاشخاص والاموال وكذا أمن الدولة ومنه كفل الدستور الجزائري لسنة 1996 وكذا مختلف التعديلات الطارئة عليه خاصة دستور 2020 م[1] عدة حقوق وحريات جوهرية أحاط بها المشرع الموان الجزائري وكرامته الشخصية.

الفرع الأول: دستور 2016: كفل تعديل الدستور الجزائري لسنة 2016.

وكذا التعديل الطارئ عليه بموجب القانون المعدل له لسنة 2016 حماية الحقوق الأساسية والحريات الفردية على أن تضمن الدولة عدم استسهال حرمة الانسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والاجراءات الجنائية وقوانين خاصة أخرى والتي تحضر كل مساس بهذه الحقوق من أبرز هذه المبادئ الدستورية العامة نذكر:

[1] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص11

- المادة 38: «الحريات الأساسية وحقوق الانسان والمواطن مضمونة»

- المادة 44: «حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن حقوق المؤلف يحميها القانون»

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.

الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة»[1]

- المادة 46: «لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميهما القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه» [2]

ويفهم من سياق المواد السابقة أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها كما أن القانون يحمي حقوق المؤلف في كل مجالاتها [3]

الفرع الثاني : دستور 2020

كفل دستور 2020 ومن خلال المرسوم الرئاسي رقم 20-442 المؤرخ في تاريخ 2020/12/30 المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020 في الجريدة الرسمية رقم 82 في:

- المادة 35: « تضمن الدولة الحقوق الأساسية والحريات»

- المادة 47: « لكل شخص الحق في حماية حياته الخاصة وشرفه لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت لا مساس بالحقوق المذكورة في

---

[1] مدرك ناريمان , الآليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري, مذكرة نهاية الدراسة لنيل شهادة الماستر, جامعة عبد الحميد بن باديس, مستغانم,2022/2023, ص56-57

[2] المادة 46 من الدستور الجزائري بموجب تعديل 6 مارس سنة 2016 , الفعل الرابع تحت عنوان الحقوق والحريات, ص 14

[3] مدرك ناريمان , الآليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري, مرجع سابق ،ص57

الفقرتين الاولى والثانية إلا بامر معلل من السلطة القضائية حماية الاشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي يعاقب القانون كل انتهاك لهذه الحقوق».

– المادة 73 في الفقرتين 01 و 03: « تسهر الدولة على توفير الوسائل المؤسساتية والمادية الكفيلة بتنمية قدرات الشباب وتحفيز طاقاتهم الابداعية تحمي الدولة الشباب من الآفات الاجتماعية».

– المادة 81 : «يمارس كل شخص جميع الحريات في إطار احترام الحقوق المعترف بها للغير في الدستور لا سيما منها احترام الحق في الشرف والحياة الخاصة وحماية الأسرة والطفولة والشباب» وبهذا عمل المشرع على حماية حرمة الحياة الخاصة للأفراد من كل اعتداء مهما كانت الوسيلة المستخدمة ولو كانت إلكترونية كما أكد على حق الأشخاص في سرية مراسلتهم واتصالاتهم في أي شكل كانت كما أن المشرع جعل من حرمة حياة الأشخاص وحمايتهم عند معالجة المعطيات ذات الطابع الشخصي حق أساسي كما يستشف من نص المادة المذكورة أعلاه أن المشرع أقر على أن هناك حماية يقوم بها الأشخاص وكذا حماية توفرها الدولة للأشخاص من خلال معاقبة كل شخص قام بانتهاك تلك الحقوق بأي نوع من أنواع الاعتداءات بما في ذلك التي تستعمل فيها الوسائل الإلكترونية.[1]

المطلب الثاني: مكافحة الجريمة بموجب قانون العقوبات

تطرق المشرع الجزائري في أحكام قانون العقوبات إلى تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام مما دفع به الى تعديل قانون العقوبات بتاريخ 2001/06/26 بموجب القانون رقم 09/01 المعدل والمتمم للقانون 155/66 المتضمن قانون العقوبات من الفصل الخامس تحت عنوان الجنايات والجنح التي يرتكبها الأشخاص ضد النظام العمومي في القسم الأول تحت عنوان الإهانة والتعدي على الموظفين ومؤسسات الدولة[2] حيث ذكرت الجريمة المعلوماتية لأول مرة كما ذكر أول تجريم لها في جريمة القذف وسب وإهانة رئيس الجمهورية من خلال نص المادة " 144 مكرر" وكذا جريمة الاساءة لرسول الله صلى الله عليه وسلم والأنبياء وبقية الأديان على رأسهم الدين الإسلامي من خلال نص المادة" 144 مكرر 02 " [3] أو ضد

---

[1] عقباش بريزة, مبارك حنان, آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري , مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي, جامعة محمد البشير الإبراهيمي, برج بوعريريج,2022/2021,ص 35

[2] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص13

[3] خاليدة بن بعلاش , جامعة تيارت, علي عثماني, المركز الجامعي آفلو–الأحكام الموضوعية والإجرائية مكافحة الجريمة الإلكترونية في التشريع الجزائري, مجلة أبحاث قانونية وسياسية, المجلد 06 العدد 02 ديسمبر 2021/710–698,ص702–703

الهيئات والمؤسسات العمومية ومن أبرز خصوصيات المادة 144 مكرر أنها أدرجت لأول مرة مصطلح (وسيلة إلكترونية ومعلوماتية...) والتي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلوماتية والإنترنت، فيما بعد أحدث قسم خاص في قانون العقوبات وذلك من خلال القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من الفعل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال بموجب القانون رقم 04 15 المؤرخ بتاريخ 2004/11/10 المعدل والمتمم لقانون العقوبات حيث حدد المشرع الجزائري من خلال كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة أما وصف:

- الاعتداء على نظام المعالج الآلية للمعطيات

- الاعتداء على معطيات نظام المعالج الآلية

- الاعتداء على سير نظام المعالجة الآلية

مع عدم إغفال النص على عقوبات الأشخاص المعنوية المرتكبة للجرائم الإلكترونية وكذا عقوبات الشروع والاشتراك في الإجرام الالكتروني وذلك من خلال نص المواد 394 الى نص المادة 394 مكرر 07 وهذه الاعتداءات تتطلب وجود نظام معالجة آلية للمعطيات كشرط أساسي مسبق بخلاف الاعتداءات على منتوجات النظام وسنتعرض إليها بتفصيل فيما يلي:

الفرع الأول: جريمة الدخول والبقاء في النظام المعلوماتي عن طريق الغش

أولا: الركن الشرعي: نصت المادة 394 مكرر على الاعتداءات الواقعة على نظام المعالجة الآلية للمعطيات من القانون رقم 04-15 بما يلي:

« يعاقب بالحبس من 3 أشهر إلى سنة ب بغرامة من 50,000 دينار جزائري الى 100,000 دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير المعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون عقوبة الحبس من 06 أشهر إلى سنتين وغرامة من 50,000 دينار جزائري إلى 150,000 دينار جزائري.[1]

ثانيا: الركن المادي: بالرجوع إلى نص المادة 394 مكرر سالفة الذكر يتضح أن الركن المادي لهذه الجريمة يتكون من عنصرين هما الدخول إلى نظام المعالجة أو البقاء فيه والذين سنشرحهما كما يلي:

[1] المادة 394 مكرر من القانون رقم 04 15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

1- فعل الدخول: هو التواجد داخل نظام المعالجة الآلية للمعطيات دون إذن أو ترخيص من مدير النظام أو صاحبه بمعنى التواجد ضد إرادة من له الحق في السيطرة عليه[1] ويتحقق هذا السلوك المجرم عن طريق قيام الجاني الإلكتروني باختراق أنظمة المعلوماتية والتي يمكن ان نتصور:

- الدخول اليها وفق فرضيات نوجزها فيما يلي:

- الدخول عن طريق تشغيل حاسب آلي مغلق

- الدخول باستعمال حاسب آلي مفتوح الدخول عن طريق الاختراق

- الدخول عن طريق خطوط الاتصالات الدخول إلى نظام الحاسب الآلي باستعمال بطاقة الغير،[2] ولقيام هذه الجريمة يتوجب وجود شرطان هما:

- الولوج المادي للمعلومات والمعطيات المخزنة

- عدم وجود تصريح أو إذن بالدخول

2- فعل البقاء: هو استمرارية التواجد داخل نظام المعالجة الآلية دون إذن من صاحبه أو من له السيطرة عليه بمعنى آخر هو بقاء الشخص داخل نظام المعالجة ملك الغير بعد الدخول إليه خطأ أو صدفة رغم علمه بأن بقائه فيه غير مرخص[3] كما يعتبر البقاء جريمة لاحقة بجريمة الدخول ولا يمكن تصور البقاء دون الدخول ويتحقق هذا الفعل بالشروط التالية:

- التواجد داخل النظام بدون رضا من يملكه.

- البقاء في جزء او كل من النظام المعلوماتي.

ثالثا: الركن المعنوي: جريمة الدخول إلى النظام المعلوماتي أو البقاء فيه من الجرائم العمدية التي تقوم بتوفر القصد الجنائي العام بعنصريه العلم والإرادة[4] كما لا تقوم الجريمة إذا انعدم الركن المعنوي إذا كان دخول الجاني او بقائه داخل النظام مسموح به أو مشروع أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو الحق في البقاء أو كان

---

[1] الدكتور حسين طاهري ، الجرائم الالكترونية ، مرجع سابق ، ص.128

[2] ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية مرجع سابق ،ص.178

[3] راضية عيمور, الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري, جامعة الاغواط, المجلة الاكاديمية للبحوث القانونية والسياسية, 2022 المجلد السادس, العدد الأول,ص100

[4] ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية مرجع سابق ،ص184

يجهل وجود حظر الدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول إلا إذا توفر القصد الإجرامي فإنه تقوم الجريمة في حق الجاني.[1]

وتكملة لجريمة الدخول والبقاء تتواجد هناك ظروف مشددة المنصوص عليها بموجب نص المادة 394 مكرر سالفة الذكر والتي تتمثل في:

1- جريمة حذف أو تغيير معطيات النظام المعلوماتي: هذه الجريمة تم النص عليها في المادة 394 مكرر في فقرتها 02 [2]ومنها نجد أن الظروف المشددة لهذه الجريمة تتمثل في:

- حذف لمعطيات المنظومة المعلوماتية.

- تغيير لمعطيات المنظومة المعلوماتية.

وعليه فإن المشرع فرق بين عملية حذف البيانات وعملية تغييرها الذين يعتبران كنتيجة لفعل الدخول الغير شرعي أو البقاء كما اعتبرهما جريمتين مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما. [3]

2- جريمة تخريب النظام المعلوماتي: هذه الجريمة تم النص عليها في المادة 394 مكرر فقرتها 03 [4]ومنه نجد أن الظروف المشددة لهذه الجريمة تتمثل في:

- إعاقة وعرقلة كل أو جزء من أعمال النظام (تؤدي إلى توقف او اتلاف عمل النظام)

- الإخلال بحسن سير النظام (يكون من خلال استعمال القنبلة المعلوماتية أو استخدام فيروس ما ينتج عنه عدم القدرة على الاستعمال الصحيح والسليم للنظام).

على هذا الأساس لم يعتبر المشرع جريمة تخريب النظام جريمة مستقلة بذاتها على غرار الدخول الغير شرعي والبقاء بل اعتبرهما نتيجة للجرائم السابقة وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداءا دون توفر القصد الجنائي إلا عندما يكون نتيجة لجريمة سابقة.[5]

---

[1] الدكتور حسين طاهري ، الجرائم الالكترونية ، مرجع سابق ، ص133

[2] تنص المادة 394 فقرتها 02 على «...تضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة..»

[3] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, مرجع سابق ،ص47

[4] تنص المادة 394 فقرتها 03 على «... وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...»

[5] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, مرجع سابق ،ص47-48

الفرع الثاني: جريمة التلاعب بمعطيات المنظومة المعلوماتية

أولا: الركن الشرعي: نصت المادة 394 مكرر 01 على الاعتداءات الواقعة على معطيات نظام المعالجة الآلية من القانون رقم 04-15 كما يلي:

« يعاقب بالحبس من 6 أشهر الى 03 سنوات وبغرامة مالية من 500,000 دينار جزائري إلى 2.000000 دينار جزائري كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».[1]

ثانيا: الركن المادي: بالرجوع إلى نص المادة 394 مكرر 01 يتضح أن الركن المادي لهذه الجريمة يتكون من ثلاثة عناصر تتمثل في:

1- الإدخال: هو إدخال معطيات في النظام المعلوماتي عن طريق الغش باستخدام برامج خبيثة كإدخال أسماء وهمية في كشوف المرتبات الشهرية ولا يشترط وقوع الضرر.

2- الازالة: المحو الكلي أو الجزئي للمعلومات أو نقلها وتخزينها في منطقة خاصة فالإزالة هي عملية لاحقة عن الإدخال.

3- التعديل: هو تغيير المعلومات الموجودة داخل النظام واستبدالها بمعلومات أخرى مخالفة للأصلية كالتزوير.

ثالثا: الركن المعنوي: هذه الجريمة من الجرائم العمرية لا تقوم إلا بتوفر القصد الجنائي العام المتمثل في علم وإرادة الجاني والملاحظ أن المشرع أورد مصطلح بطريق الغش أي أن هذه الأفعال يجب أن تتم بطريق الغش وبالتالي توفر سوء النية لدى الجاني عند إدخاله لمعطيات جديدة أو محوها أو تغيير هذه المعطيات لأن ذلك قد يتم برضا صاحبها وعلمه أو عن طريق الخطأ وهنا تنتفي المسؤولية. [2]

الفرع الثالث: جريمة التعامل الغير شرعي بمعطيات النظام المعلوماتي

أولا: الركن الشرعي: نصت المادة 394 مكرر 02 على الاعتداءات الواقعة على سير النظام المعالجة الآلية للمعطيات من القانون رقم 04 -15 بما يلي:

« يعاقب بالحبس من شهرين الى ثلاث سنوات وبغرامة من 1.000000 دينار جزائري إلى 5.000000 دينار جزائري كل من يقوم عمدا أو عن طريق الغش بما يلي تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في المعطيات المخزنة أو معالجة او مرسلة عن طريق

---

[1] المادة 394 مكرر 01 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

[2] مليايني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية مرجع سابق ،ص195

منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم حيازة أو افشاء أو نشر او استعمال لأي غرض كان للمعطيات المتحصل عليها من أحد الجرائم المنصوص عليها في هذا القسم ».[1]

ثانيا: الركن المادي: بالرجوع إلى نص المادة 394 مكرر 02 يتضح أن الركن المادي لهذه الجريمة يتكون من مجموعتين وفق ما يلي:

1- التعامل في المعطيات الصالحة لارتكاب جرائم ماسة بالنظام المعلوماتي: تتمثل في كل من التصميم البحث التوفير التجميع التوفير النشر الانجاز.

2- التعامل في المعطيات المتحصل عليها من الجرائم الماسة بالنظام المعلوماتي: تتمثل في كل من الحيازة الإفشاء النشر الاستعمال.

ثالثا: الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي هو علم وإرادة الجاني بالفعل الغير مشروع كما يشترط القصد الجنائي الخاص المتمثل في نية الجاني لاستعمال هذه المعطيات في ارتكاب إحدى الجرائم الماسة بالنظام المعلوماتي [2]

الفرع الرابع: الأحكام الخاصة بالجرائم المعلوماتية

أولا: الاتفاق الجنائي: نصت عليه المادة 394 مكرر 05 بما يلي:

« كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبة المقررة للجريمة ذاتها».[3]

ولقيام الاتفاق الجنائي يجب توفر شروط التالية :

- **المشاركة في الاتفاق.**
- **العقد الجنائي العام.**
- **الاعداد وتحديد الجريمة.**

ثانيا: الشروع الجنائي: نصت عليه المادة 394 مكرر 07 بما يلي:

---

[1] المادة 394 مكرر 02 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

[2] ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية مرجع سابق ،ص201

[3] المادة 394 مكرر 05 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

« يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات للجنحة ذاتها».[1]

ولقيام الشروع الجنائي يجب توفر الشروط التالية:

- البدء بالتنفيذ والأعمال التحضيرية.

- عدم إتمام الجريمة لظروف خارجة عن إرادة الجاني.

- استحالة الجريمة.

- القصد الجنائي العام.

ثالثا: العقوبات التكميلية: نصت عليها المادة 394 مكرر 03 بما يلي:

« تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو المؤسسات العمومية».[2]

وهدف المشرع من هذه المادة هو حماية الهيئات والمؤسسات العمومية والدفاع الوطني بكل أسلاكه ومجالاته بصفة عامة والدولة ككل بصفة خاصة من اعتداءات قد تمس بأمن وسلامة النظم المعلوماتية لهذه الجبهات.

رابعا: عقوبة الشخص المعنوي: نصت عليه المادة 394 مكرر 04 بما يلي :

« يعاقب الشخص المعنوي إذا ارتكب أحد الجرائم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة لشخص طبيعي».[3]

ومن ضمن ما اعتمد عليه المشرع الجزائري في التصدي للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات في سنة 2009 ست قواعد خاصة في قانون العقوبات حيث تهدف هذه القواعد إلى الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وذلك بموجب القانون رقم 09 -04 أما سنة 2016 وبموجب القانون رقم 16 -02 المؤرخ في 2016/06/19 أضاف المشرع ماده قانونية تحمل رقم 394 مكرر 08 وقد بين من خلالها العقوبات التي تطبق على مقدم خدمة الانترنت على ثبوت مسؤوليته الجنائية ذلك أن دور هذه الفئة يعتبر أساسيا في تشغيل الإنترنت.[4]

---

[1] المادة 394 مكرر 07 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

[2] المادة 394 مكرر 03 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

[3] المادة 394 مكرر 04 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

[4] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص13

المطلب الثالث: مكافحة الجريمة بموجب القانون المدني

يسعى القانون المدني كغيره من التشريعات العامة إلى إرساء قواعده وأسسه الخاصة في مجال مكافحة الجريمة المعلوماتية وتباعياتها من خلال ضمان حق جميع أفراد المجتمع في العدالة والمساواة بغض النظر عن ماهيتهم عرقهم ودينهم ما داموا مواطنين جزائريين ولعل أبرز ما يلفت الانتباه في هذا القانون هو المسؤولية المدنية والتعادل الوظيفي في علاقتهما بالتصدي للأجرام الرقمي

الفرع الأول: المسؤولية المدنية في الجرائم الإلكترونية

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد بين المشرع الجزائري ان كل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصه أن يطلب وفق هذا الاعتداء غير المشروع التعويض عندما يكون قد لحقه من ضرر وذلك وفقا لمقتضيات المادة 124 من القانون المدني:

« كل عمل أي كان يرتكبه يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض»

فقد جاء هذا النص عاما شاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخص بما فيها الحق في الحياة الخاصة وقد تطرق هذا النص لمبدأ هام هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر و عليه فإن المسؤولية المدنية ترتب الحق في الحكم بالتعويض فالفعل الضار هو أساس المسؤولية وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوة القضائية عن الاعتداءات الإلكترونية التي تمس الحياه الخاصة على شبكة الإنترنت والضرر عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبة في الإثبات وتحديد لهوية المعتدي[1] وفي هذه المسألة نجد أن المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الاثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل إعتداء قابل للاثبات وإن وقع على الشبكة.[2]

---

[1] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص11-12

[2] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, مرجع سابق ،ص362

الفرع الثاني: مبدأ التعادل الوظيفي في الجريمة الإلكترونية

نصت المادة 323 مكرر 01 من القانون المدني على أنه يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وإن تكون معدة ومحفوظة في ظروف تضمن سلامتها وتأسيس ا على ذلك أسس المشرع من خلال هذا النص مبدأ التعادل الوظيفي بين الكتابة في الشكل الإلكتروني والكتابة على الدعامة الورقية كما قد اعترفت المادة السالفة بالكتابة الإلكترونية في اثبات التصرفات والعقود من جهة وجعلتها معادلة في حجيتها الوثيقة المخطوطة على دعامة ورقية في حجيتها وصحتها[1] واستخلاصا لما سبق فإنه في حالة ارتكاب فعل غير مشروع الكتروني فيما يخص تدوين تصرفات أو عقود ما بزيادة أو نقصان فإنها ترتقي إلى جريمة يعاقب عليها القانون

المطلب الرابع: مكافحة الجريمة بموجب قانون الإجراءات الجزائية

لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بالجريمة المعلوماتية محاولة منه لتطبيقها والقضاء عليها أو على الأقل الحد من انتشارها حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها وقد أوردت هذه الأساليب في قانون الإجراءات الجزائية [2]وهذا ما أدركه المشرع الجزائري بأن هذه المواجهة لا تكون فقط بإرساء قواعد موضوعية ذات الطبيعة الردعية وإنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية تحفظية والتي من شأنها تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر ما يسمح بتدارك مخاطرها

ومن أهم ما جاء به في مكافحة هذا النوع من الاجرام تعديل قانون الإجراءات الجزائية لسنة 2006 بموجب القانون رقم 22 -06 الذي جاء بإجراءات مستحدثة تطبق على هذه الجريمة لعل من أهمها ما يلي:

الفرع الأول: تمديد الاختصاص

إذا تم تعديل الاختصاص لوكيل الجمهورية ولضباط الشرطة القضائية إلى كل ربوع الوطن في هذا النوع من الجرائم[3] وذلك من خلال نص المادة 37 من قانون الإجراءات الجزائية [1]

---

[1] الدكتورة ناني لحسن , التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018,ص31

[2] بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني, مرجع سابق ،ص53-54

[3] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص13-14

الفرع الثاني: التفتيش

التفتيش في الجريمة العادية ليس كالتفتيش في الجريمة المعلوماتية حيث يقوم بها ضباط الشرطة القضائية إلى جانب الجهات القضائية التي يؤول إليها الاختصاص للتحقيق في هذه الجريمة كما يمكن اللجوء إلى أشخاص مؤهلين كالخبراء والتقنيين في الإعلام الآلي لإجراء هذه العمليات التفتيش على المنظومة المعلوماتية وتزويد الجهات القضائية بالمعطيات التي تحتاجها هذا وتجدر الإشارة الى أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في الجريمة العادية وذلك من حيث الشروط الشكلية والموضوعية وفقا لما جاء في نص المادة 45 في فقرتها 07 من قانون الاجراءات الجزائية.

وإن كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن التفتيش هنا لا يتم إلا بطلب المساعدة من السلطات الاجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل. [2]

الفرع الثالث: التوقيف للنظر

تختلف إجراءات التوقيف للنظر بالنسبة للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات عن الجريمة العادية إذ يمدد هذا التوقيف مره واحدة فقط وهذا ما جاء في نص المادة 51 في فقرتها 06 من قانون الإجراءات الجزائية.

الفرع الرابع: اعتراض المراسلات

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع التخزين الاستقبال والعرض التي تتم عن طريق القنوات أو وسائل الاتصالات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء إلى هذا الإجراء من خلال نص المادة 65 مكرر 06 من قانون الإجراءات الجزائية فبموجب هذه المادة سمح المشرع لسلطات التحقيق الاستدلال إذا استدعت الضرورة في الجريمة المتلبس بها أو التحقيق في الجرائم الالكترونية اللجوء إلى اجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول لكشف ملابسات الجريمة واثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة.

---

[1] المادة 37 من قانون الإجراءات الجزائية, من الفعل الثاني مكرر تحت عنوان: الوساطة من الكتاب الأولى في مباشرة الدعوى العمومية إجراءات التحقيق, ص24

[2] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص14

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الاجراء بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد[1] فكل ذلك انشئ بموجب القانون رقم 14-04 المؤرخ في تاريخ 2004/11/10 المعدل لقانون الاجراءات الجزائية والأقطاب القضائية الجزائية المتخصصة في هذا النوع من الجرائم.[2]

الفرع الخامس: حجز المعطيات المعلوماتية

يتم اللجوء إلى هذا الإجراء عندما يتم اكتشاف معطيات من قبل السلطة التي تباشر التفتيش في المنظومة المعلوماتية هذه المعطيات تكون مخزنة كما تكون مفيدة في الكشف عن الجرائم أو مرتكبيها كما أنه ليس من الضروري حجز كل المنظومة بل يكفي نسخ المعطيات اللازمة لفهمها على دعامة تخزين الكترونية حيث تكون قابلة للحجز والوضع في ..... وفقا للقواعد المقررة في قانون الإجراءات الجزائية.[3]

الفرع السادس: إجراء التسرب

نصت عليها المادة 65 مكرر 11 إلى المادة 65 مكرر 18 من قانون الإجراءات الجزائية وقد عرفه المشرع الجزائري في نص المادة 65 مكرر 18 من نفس القانون بكونه قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو الجنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو نافذ.... وأجاز المشرع اللجوء إلى هذه الوسيلة التي تعد أسلوبا من أساليب التحري الخاصة في بعض الجرائم المنصوص عليها على سبيل الحصر في المادة 65 مكرر 05 كما يتم التسرب بعد الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق لضمان شرعيته وعدم مساسه بخصوصية الأفراد المكفولة دستوريا ويكون عبر استعمال العون المتسرب هوية مستعارة في مواقع الانترنت التي تشكل أو يشتبه في قيام أصحابها بعمليات النصب والاحتيال. [4]

---

[1] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, مرجع سابق ،ص364

[2] الدكتورة ناني لحسن , التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018,ص37

[3] الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, مرجع سابق ، ص15

[4] خاليدة بن بعلاش , جامعة تيارت, علي عثماني, المركز الجامعي آفلو-الأحكام الموضوعية والإجرائية مكافحة الجريمة الإلكترونية في التشريع الجزائري, مرجع سابق ،ص708

المبحث الثاني: مكافحة الجريمة في القوانين الخاصة

مع استفحال ظاهرة النمو السريع في استخدام النظم المعلوماتية وانتهاك حرمة البيانات الشخصية والوطنية لم يقف المشرع الجزائري بمنع عن هذه التجاوزات بل تصدى لها بالعديد من التشريعات على رأسها قانون العقوبات وقانون الإجراءات الجزائية غير أن هذه القوانين التقليدية ورغم استحداثها لم تكن كافية وقادرة على استيعاب ضغوطات الجرائم المعلوماتية وطبيعتها الإلكترونية المعقدة هذا ما عزز التعاون بين الجهات القضائية والخبراء المختصين في مجال المعلوماتية ما أدى إلى خلق واستحداث قوانين أخرى خاصة بهدف ضمان الحماية الجنائية للمعاملات الإلكترونية من الناحية الشخصية أو الاجتماعية أو الدولية والحد من الاعتداءات الصادرة ضد الأنظمة والشبكات الرقمية الخاصة بالفرد أو الدولة وكل تلك المواد التي بدأت تتجلى للعيان كل ذلك أجملناه من خلال أربعة مطالب أساسية فمن خلال المطلب الاول تناولنا القانون الخاص بالوقاية من الجرائم المتعلقة بتكنولوجيا إعلام والاتصال 09-04 والمطلب الثاني تعلق بقانون البريد والمواصلات السلكية واللاسلكية 03-2000 أما المطلب الثالث فكان تحت عنوان القانون الخاص بحماية المؤلف والحقوق المجاورة 03-05 ثم المطلب الرابع والأخير الذي تطرقنا فيه لدراسة القانون الخاص من بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني 15-04 بالإضافة إلى قانون التأمينات.

المطلب الأول: القانون الخاص المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا إعلام والاتصال

عمدت معظم الدول إلى استحداث وحدات خاصة لمواجهة الجريمة الإلكترونية كما تم انشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الانتربول اليوروبول والأفريبول أما في الجزائر فقد تم تسخير هيئات ووحدات مختصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا إعلام والاتصال[1] هذه الهيئة التي أنشئت بموجب القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 سبتمبر 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [2]حيث تضمن هذا القانون 19 مادة أهم النقاط التي جاء بها هو استحداث المراقبة الإلكترونية للاتصالات هذا الإجراء نظمته المادة 04 منه كما أدرج قواعد إجرائية جديدة تمثلت في تفتيش المنظومة المعلوماتية طبقا لنص المادة 05 في حين نصت المواد 06 إلى 09 عن عملية حجز المعطيات المعلوماتية كما حدد القانون التزامات مقدمي الخدمات بنص المواد 10 إلى 12 وحدد عقوبات في حال مخالفة هذه

[1] عقباش بريزة, مبارك حنان, آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري, مرجع سابق،ص43-44

[2] الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 47, ص05

الالتزامات في حين تم النص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا إعلام والاتصال ومكافحتها بموجب المادتين 13 و 14 وأخيرا حدد أطر وإجراءات التعاون الدولي والمساعدة القضائية الدولية بموجب نص المواد من 15 إلى المادة 18 منه[1] وفي المجمل يحتوى هذا القانون على 6 فصول تناولت التعريف بالجريمة مراقبة الاتصالات الإلكترونية القواعد الإجرائية والاختصاص القضائي في نص المادة 19 من هذا القانون ومنه[2] فإن هذا القانون قد شمل مواضيع ومجالات أخرى أوسع نطاقا من التي أوردناها سابقا وذلك من خلال ما يلي:

الفرع الأول: عناصر الجريمة المعلوماتية في إطار القانون 09-04

أولا: المنظومة المعلوماتية: أي نظام متفاعل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة حيث يقوم واحد منها أو أكثر لمعالجة إليه للمعطيات تنفيذا لبرنامج معين

ثانيا: المعطيات المعلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها.

ثالثا: مقدم الخدمات: وهم صورتين:

- أي كان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات.

- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

رابعا: المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات حيث توضح مصدر ووجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم و مدة الاتصال ونوع الخدمة.

خامسا: الاتصالات الإلكترونية: حيث تراسل أو ارسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.[3]

الفرع الثاني: مكافحة الجريمة الإلكترونية من خلال القانون 09-04

[1] الدكتورة ناني لحسن , التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018,ص38

[2] بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني, مرجع سابق ،ص53-54

[3] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, مرجع سابق ،ص79-80

أولا: مراقبة الاتصالات الإلكترونية: حددت المادة 04 من القانون 09-04 الحالات التي تسمح باللجوء إلى هذه الإجراء:

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

- في حالة توافر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام.

- لمقتضيات التحريات والتحقيقات القضائية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة غير أن المشرع الجزائري أو من خلال نفس النص القانوني أكد على أنه لا يجوز إجراء عمليات مراقبة في الحالات السابقة المذكورة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.

ثانيا: القواعد الإجرائية: تضمنت المواد من 05 إلى 09 من القانون رقم 09-04 مجموعة من القواعد الإجرائية التي تهدف إلى الوقاية من الجرائم الإلكترونية ومكافحتها وتتمثل هذه الإجراءات في:

- تفتيش المنظومة المعلوماتية من خلال المادة 05.

- حجز المعطيات المعلوماتية من خلال المادة 06.

ثالثا: إلزام مقدمي الخدمات بضرورة المساهمة في الوقاية من الجرائم الالكترونية: فرض القانون 09-04 على مقدمي الخدمات مجموعة من الالتزامات تساهم بدورها في الوقاية من الجرائم الإلكترونية أو مكافحتها وتتمثل أهم هذه الالتزامات في:

- تقديم المساعدة للسلطات المكلفة بالتحريات القضائية.

- حفظ المعطيات المتعلقة بحركة السير.

- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

- وضع ترتيبات تقنية تسمح بحصر امكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.[1]

الفرع الثالث: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا إعلام والاتصال

[1] مهداوي حنان , التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري, مجلة الفكر القانوني والسياسي, جامعة محمد لمين دباغين , سطيف 02 , المجلد السادس, العدد الثاني 2022 , ص 1069-1070-1071

نصت على انشاء هذه الهيئة المادة 13 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا إعلام والاتصال ومكافحتها حيث نصت على « تنشأ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم» أما مهامها فقد أوردتها المادة 14 من نفس القانون ومن خلال اسمها فان لهذه الهيئة دوران أساسيان يمكن ان تلعبهما في تأسيسها والتي تكمن فيما يلي:

أولا: الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بنوعية مستعملي تكنولوجيا الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون ويستعملون هذه التكنولوجيات ومن أبرز هذه الجرائم على سبيل المثال نذكر:

- التجسس على الاتصالات والرسائل الإلكترونية.

- التلاعب بحسابات العملاء أو بطاقات ائتمانهم.

- اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية.[1]

ثانيا: مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: بحسب نص المادة 14 من القانون 09-04 تمت مراقبة السلطة القضائية وطبقا لأحكام التشريع الساري المفعول تكلف الهيئة بما يلي:

- تنشيط وتنسيق الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

- مساعدة السلطة القضائية ومصالح الشرطة القضائية في مكافحة هذا النوع من الجرائم.

- تنفيذ عمليات مراقبة وقائية للاتصالات الالكترونية بعد إذن من السلطات القضائية.

- جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم الإلكترونية.

- تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناءا على طلبها بمعلومات ومعطيات تتعلق بالجريمة الالكترونية.

- القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية.

- تطوير التعامل مع المؤسسات والهيئات الوطنية المعنية في نفس المجال.

- تنفيذ طلبات المساعدة القضائية الأجنبية في جمع المعطيات وتحديد مكان الجناة.

- تبادل المعلومات واتخاذ أي اجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة أو الاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.[1]

---

[1]الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مرجع سابق ،ص368

وفي الاخير فإن أهمية هذا القانون رقم 09-04 تبرز في كونه يجمع بين القواعد الإجرائية المكملة لقانون الاجراءات الجزائية وبين القوانين الردعية الوقائية والتي من خلالها أتاح المشرع للسلطات القضائية المختصة بمكافحة هذا النوع المستحدث من الجرائم بما يناسبها من إجراءات التدخل السريع والفوري بغية ردع مرتكبي هذه الجرائم وتطويق سلوكاتهم الإجرامية بوسائل وتقنيات إلكترونية قضائية تسمح بالرصد المبكر لهذه الاعتداءات المحتملة.

المطلب الثاني: قانون البريد والمواصلات السلكية واللاسلكية 03-2000

بغية التصدي لظاهرة الإجرام الإلكتروني ومكافحة مرتكبيه سعى المشرع الجزائري ومنذ الألفية إلى إبراز دور القوانين الوطنية والهياكل القانونية الخاصة في مكافحة الجريمة الإلكترونية وذلك من خلال تعديل بعضها واستحداث البعض الآخر وهذا ما ظهر جليا بموجب القوانين الخاصة لعل أبرزها القانون الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية من خلال القانون رقم 2000-03، تضمن هذا القانون سالف الذكر القواعد العامة المتعلقة بالبريد والمواصلات والذي تم تعديله بموجب القانون 03-22 الممضى عليه في تاريخ 2003/12/28 من قبل وزارة المالية والقانون 06-24 الممضى عليه في تاريخ 2006/12/26 من قبل وزارة المالية وقد تلاه أكثر من 20 نص تطبيقي حيث يضم هذا القانون 151 مادة أدرجت لتنظيم الاتصالات السلكية واللاسلكية وكذا البريد كما يحتوي على نصوص عقابية وذلك من المادة 127 منه إلى المادة 144 ومن بين أهم السلوكيات المجرمة بنص هذا القانون نذكر:[2]

« يعاقب بالحبس من 03 اشهر إلى 05 سنوات وبغرامة مالية من 100,000 دينار جزائري إلى 1.000000 دينار جزائري كل من يقطع عمدا كاملا بحريا أو يسبب له تلفا قد يوقف أو يعطل المواصلات السلكية واللاسلكية كليا أو جزئيا»

« يعاقب بغرامة مالية من 10,000 دينار جزائري إلى 50,000 دينار جزائري كل شخص يقوم بإشهار لغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون أن يكون متحصلا على الاعتماد المسبق المنصوص عليه في المادة 41 من هذا القانون»

---

[1] عقباش بريزة, مبارك حنان, آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري , مرجع سابق ،ص46-48-47

[2] الدكتورة ناني لحسن , التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018,ص34-35

« يعاقب بالحبس من 3 اشهر إلى سنة كل شخص يقوم بإرسالات لاسلكية كهربائية باستعمال عمدا رمز نداء في السلسلة الدولية المخصص لإحدى محطات الدولة أو لكل محطة أخرى مرخص بها».

« يمنع تقليد واستعمال المطبوعات المستعملة من طرف المستغل العمومي او من طرف كل متعامل اخر مرخص له».[1]

وباستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات نلاحظ أيضا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي لذلك بات من السهولة إمكان إجراء التحويلات المالية عن الطريق الإلكتروني وذلك لما نصت عليه المادة 87 من القانون 2000-03 كما نصت المادة 84 في فقرتها 02 من نفس القانون على استعمال حوالات دفع عادية أو إلكترونية أو برقية كما نصت في المادة 105 منه على احترام المراسلات بين ما أتت المادة 127 منه بإجراء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من 5 إلى 10 سنوات.[2]

المطلب الثالث: القانون الخاص بحماية حق المؤلف والحقوق المجاورة 05-03

مع النمو المتسارع في مجال التكنولوجيا الرقمية والتي طغت على غالبية مجالات الحياة الإنسانية ومسايرة لثوره المعلوماتية لم يكن الجانب الفكري مستثنى من هذه القفزة الرقمية قفزه كان لها أثر بالغ من ناحية الملكية الفكرية والحقوق المتعلقة بشخص المؤلف ومن هنا بدا الجدال الفقهي بصفة عامة وفي الفقه الجنائي بصفة خاصة فيما يتعلق بمدى مساس السلوكات الإجرامية الإلكترونية بمجال الابداعات الشخصية للأفراد والانطلاقة كانت من خلال موافقة حقوق المؤلف الامريكية «copyright office» لسنة 1964 على إيداع البرامج لديه كمصنفات وكذلك الحال في فرنسا بموجب القانون 86-66 المؤرخ في تاريخ 1986/07/03 حيث أضيفت برامج الكمبيوتر ضمن حقوق المؤلف أما في التشريع الجزائري فلم ينص الأمر73-14 المؤرخ في تاريخ 1973/04/03 المتعلق بحق المؤلف ولا الأمر 97-10 المؤرخ في تاريخ 1997/03/06 المتعلق بحقوق المؤلف والحقوق المجاورة

---

[1] المادة 130 المادة 133 المادة 136 المادة 144 من القانون رقم 2000 03 المؤرخ في 5 غشت سنة 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية, الجريدة الرسمية للجمهورية الجزائرية, العدد 48, ص24-25-26

[2] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, مرجع سابق ،ص364

صراحة على اعتبار حقوق المؤلف معلوماتية إلا أن الأمر صفر 03-05 المؤرخ في تاريخ 2003/07/09 المتعلق بحقوق المؤلف والحقوق المجاورة اعتبر صراحة من خلال نص المادة 04 من نفس القانون على أن برامج الحاسوب تعتبر مصنفات محمية قانونا[1] مثل الروايات والبحوث العلمية والاجتهادات القضائية برامج والعاب الحاسوب وغيرها فالحقوق المالية أو المادية هي الإطار الذي يمكن صاحب البرنامج من استغلاله بأي طريقة دون غيره أو لمن يخول له هو نفسه هذا الحق وله وذلك وفقا لأحكام المادة 27 من الأمر 03-05 بإبلاغه للجمهور بأية منظومة معالجة معلوماتية حيث يترتب عن ذلك حقوقا مادية للمؤلف صاحب هذا البرنامج بالاستغلال التجاري له ولورثته بمختلف الطرق وهذا ما يستخلص من نص المادة 03 من نفس الأمر.

كما بسط المشرع الجزائري حمايته على برامج الحسابات الآلية مدرجا إياها تحت نطاق حقوق المؤلف تماشيا مع اتفاقية برن الدولية التي صادقت عليها الجزائر بموجب المرسوم الرئاسي 97-341 المؤرخ في تاريخ 1997/09/13 حيث أنه بموجب هذه الاتفاقية تبسط الحماية على حقوق المؤلف وبالتالي على البرامج مدة 50 سنة ابتداءا من مطلع السنة الميلادية التي تلي نشر المصنف وهذا ما نصت عليه المادة 58 في فقرتها 01 من الأمر 03-05 ومدة 50 سنة أيضا ابتداءا من مطلع السنة الميلادية التي تلي تاريخ وفاة المؤلف تماشيا مع نص المادة السابقة من اتفاقية "برن".[2]

وفي سبيل تقرير حماية جنائية فعالة في هذا المجال عمد المشرع الجزائري إلى تصنيف جملة من الأفعال المجرمة قانونا والعقوبات المقررة لها بهدف ردعها والحد منها وذلك ما تضمنته المواد من 151 من المادة 160 من الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة وذلك من خلال ما يلي:

الفرع الأول: الجرائم المعلوماتية الواقعة في نطاق حق المؤلف

يعد مرتكبا لجنحة التقليد كل من يقترف السلوكات التالية:

- **الكشف الغير مشروع للمصنف أو المساس بسلامته أو الأداء لفنان مؤد أو عازف.**
- **استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.**
- **استيراد أو تصدير نسخ مقلدة لمصنف أو أداء ما.**
- **بيع لنسخ مقلدة لمصنف أو أداء ما.**
- **تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء ما.**

[1] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, مرجع سابق ،ص63

[2] غربي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, مرجع سابق ،ص54-55

– كل من ينتهك الحقوق المحينة قانونا فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني أو البث الإذاعي السمعي أو السمعي البصري أو التوزيع بواسطة الكابل أو بأية وسيلة نقل أخرى لإشارات تحمل أصوات فقط أو صورا وأصواتا أو بأي منظومة معالجة معلوماتية

– كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة.

– كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو أي مالك حقوق مجاورة آخر للحقوق المعترف بها قانونا.[1]

الفرع الثاني: العقوبات المقررة لجريمة التقليد

حدد المشرع الجزائري صنفين من العقوبات المقررة على جنح تقليد المصنفات المعلوماتية والتعدي على حقوق الشخصية للمؤلف والتي تتمثل في العقوبات الأصلية والتكميلية.

أولا: العقوبات الأصلية: حددت هذه العقوبات في نفس المادة 153 من الأمر 0 3 0 5 على النحو التالي:

« للقاضي أن ينطق بعقوبة أصلية تتمثل في الحبس من 06 أشهر الى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيه المصنفات المعلوماتية.

علاوة على عقوبة الحبس يمكن للقاضي أن يحكم بغرامة مالية تتراوح بين 500,000 دينار جزائري إلى 1.000000 دينار جزائري».[2]

وأوردت المادتان 151 و 152 من نفس الأمر لمرتكبي جنحة التقليد لمصنف أو أداء في عقوبة تتمثل في نفس العقوبة الواردة في المادة 153 من نفس القانون.

ونصت المادة 154 على معاقبة الشريك في ارتكاب جريمة التقليد سواءا بأعماله أو بوسائله بنفس عقوبة المادة 153.

وتضمنت المادة 156 نفس العقوبة المقررة في المادة 153 لكل من يمتنع عن دفع المكافأة المستحقة للمؤلف.

تشدد العقوبة المقررة في المادة 153 في حالة العود.

ثانيا: العقوبات التكميلية: تتم عن طريق ما يلي:

– الغلق المؤقت لمدة لا تتعدى 6 اشهر لمؤسسة يستغلها مقلد أو شريكه وإن يكون الغلق نهائي عند الاقتضاء من طرف محكمة الموضوع.

---

[1] الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, مرجع سابق ،ص64-65

[2] راضية عيمور, الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري, جامعة الاغواط, المجلة الاكاديمية للبحوث القانونية والسياسية, 2022 المجلد السادس, العدد الأول,ص100

– المصادرة سواءا كانت للمبالغ التي تمثل الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي أو إتلاف العتاد وهي مصادرة وجوبية بحيث تؤول الأموال والوسائل المصدرة للمؤلف أو مالك الحقوق أو ذوي حقوقهما كتعويض عن ما لحقهم من ضرر.

– نشر ملحق الحكم أي التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية وما يتم مصادرته من نسخ وايرادات وأقساط تأمر الجهة القضائية المختصة بتسليمها للمؤلف أو لأي مالك للحقوق أو لذويهم وذلك بموجب شكوى لدى الجهة القضائية المختصة من طرف مالك الحقوق أو من يمثله قانونا طبقا للمادة رقم 160 من الأمر 03-.05[1]

وفي الأخير تجدر الاشارة إلى أن معظم الفقه يرى بأن الموقع الإلكتروني مصنف متعدد الأغراض يتم استخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتهم المعروضة للتسويق أو الدعاية عن غيرها من شبكه الإنترنت أو كاسم تجاري أو شعار لجذب الجمهور كما يمكن ان يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو وغيرها وفي كل حالة يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم هذه الخدمات على الشبكة وبمجرد تسجيل إسم الموقع سيحظى بحماية قانونية المقررة لحق الملكية الفكرية الذي يتضمنه أي تحديد القانون الواجب التطبيق حسب الطبيعة القانونية للموقع فعند تسجيل الموقع كمصنف أدبي أو فني فإنه لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد كالاستعمال الاسم الكامل لشخص معين معروف دون إذنه أو استغلال صورة شخص ما دون موافقته وغيرها الكثير[2] وهذا ما أقره المشرع الجزائري من خلال دستور 1996 ودستور 2016 من خلال نص المواد 38- 40- 41 44 -46.

المطلب الرابع: قوانين أخرى خاصة

الفرع الأول: قانون التأمينات 80-01

على غرار التشريعات السابقة العامة منها والخاصة وتماشيا مع متطلبات العصر الحالي تطرق القانون رقم 08-01 المؤرخ في تاريخ 2008/01/23 المعدل والمتمم للقانون رقم

[1] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, مرجع سابق ،ص47

[2] الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, مرجع سابق ،ص365

01-83 المتعلق بالتأمينات الاجتماعية لتنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص عديدة تخص كل من:[1]

- المادة 93 مكرر 02 « دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من 02 الى 05 سنوات وبغرامة من 100,000 دينار جزائري إلى 200,000 دينار جزائري كل من يسلم أو يستلم بهدف الاستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة».

- المادة 93 مكرر 03 « دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500,000 دينار جزائري إلى 1.000000 دينار جزائري كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة.

يعاقب بنفس العقوبة كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لمهني الصحة يعاقب بنفس العقوبة على المحاولة في ارتكاب الجنح المذكورة في الفقرتين الأولى والثانية أعلاه ».

- المادة 93 مكرر04 « دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين الى خمس سنوات وبغرامة من 500,000 دينار جزائري إلى 5.000000 ملايين دينار جزائري كل من ينسخ أو يصنع أو يحوز أو يوزع بطريقة غير مشروعة البطاقات الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل للعلاج او المفتاح الالكتروني لمهني الصحة».

- المادة 93 مكرر 05 « يعاقب كل شخص معنوي يرتكب احدى الجنح المنصوص عليها في المادتين 93 مكرر 03 و93 مكرر 04 أعلاه بغرامة تساوي خمس مرات المبلغ الأقصى للغرامة المقررة للشخص الطبيعي».

- المادة 93 مكرر 06 « دون الإخلال بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والوسائل المستعملة وكذا إغلاق المحلات وأماكن الاستغلال التي تكون محل الجنح

[1] الدكتورة خلدون عائشة, محاضرات في الجريمة المعلوماتية, مرجع سابق ،ص56

المنصوص عليها في المادتين 93 مكرر 03 و93 مكرر 04 أعلاه في حالة ما إذا كان المالك على علم بذلك ».[1]

ومن خلال ما سبق يفهم أن قانون التأمينات رقم 08-01 هو الآخر أحاط بالجريمة المعلوماتية وتباعياتها التي قد تلحق بالمؤمن الاجتماعي أو البطاقة الالكترونية الخاصة به وذلك بهدف صيانة وحماية هذا المجال.

الفرع الثاني: القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين 15-04

تفضل المشرع للدور الذي تلعبه الوسائل التي أفرزتها تكنولوجيات الاتصال كالتوقيع والمحرر الالكترونيين وضرورة توفير أمان قانوني من خلال إنشاء هيئات التصديق الالكتروني تطبيقا للمادة 33 من القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين حيث استحدث هذا القانون بهدف مسايرة التطور التكنولوجي على المستوى العالمي لا سيما في الجانب الاقتصادي إضافة إلى تفعيل مشروع الحوكمة الالكترونية الذي تسعى الدولة الى تجسيده في أقرب وقت فمن جهة حدد القانون مجمل الإجراءات الواجب اتخاذها في هذا الصدد والجهات المكلفة بذلك من جهة ثانية نص على مختلف التعريفات والأحكام المنظمة لعمليتي إنشاء واستغلال كل من التوقيع والتصديق الإلكترونيين من خلال 82 مادة إجمالا وتم من خلالها تخصيص فصل للأحكام الجزائية وهو الفعل الثاني على مستوى المواد من 66 إلى المادة 75 مستحدثا بذلك أحكام جزائية جديدة من بينها:

- المادة 66 :« الإدلاء بإقرارات كاذبة للحصول على شهاده تصديق إلكتروني موصوفة».

- المادة 74 : « استعمال شهادة تصديق إلكتروني الموصوفة لغير الأغراض التي منحت لها».

- المادة 69 : « الإخلال عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة».

[1] القانون رقم 08-01 المؤرخ في 23 يناير 2008 المتعلق بالتأمينات الاجتماعية, الجريدة الرسمية للجمهورية الجزائرية, العدد 04,ص05

الخاتمة :

من خلال طرح موضوع دراستنا المكافحة الموضوعية للجريمة الإلكترونية في التشريع الجزائري موضوع ينطوي على قدر كبير من الأهمية العلمية والعملية حيث يبرز الهدف السامي من هذه الدراسة القانونية ألا وهي اهتمام المشرع الوطني بالجريمة المعلوماتية ومستجداتها الإجرامية الواقعة على النظم والبيانات وجل البرمجيات الحاسوبية ثم يتجلى ذلك من خلال تسميتها وصولا إلى الطبيعة الخاصة الداخلة ضمن دائرتها و ما يميزها من شمولية عالمية وسلوكيات خفية فرغم تطور الوسائل الحديثة إلا أن سلبيات وإجرام هذه التقنيات كانت ولا زالت جد كثيفة مست بجل طبقات والمستويات الأمنية الفردية منها والدولية هذا ما جعل من مجرمي المعلوماتية ينفذون اجرامهم بكل دقة حرفية وسرية بعيدا عن أنظار المتابعات الأمنية والقضائية ما جعلها تتخطى قدرات الدولة وحواجزها السيادية على عكس تلك الجرائم المحلية ثم تطويع كل تلك السلوكات لصالحه المجرم المعلوماتي من أجل ممارسة نشاطاته الإجرامية التي عجزت عن مواكبتها النصوص العادية ولمواكبة هذه التكنولوجيات اضطرت غالبية الدول والمنظمات لإيجاد سبل بغية مواجهتها من خلال تعديل التشريعات التقليدية واستحداث تقنيات أخرى اختصاصية حيث قام الشارع الوطني والجزائري بتعديل واستحداث الجوانب الموضوعية قصد التصدي لهذه الظاهرة الإجرامية من خلال ما تبناه من قوانين أبرزها القانون رقم 04-15 والأمر 03-05 والقانون رقم 09-04 وبذلك يكون المشرع الجزائري قد تدارك وأحاط بالنقص التشريعي الواقع في المجال العقابي التقني التكنولوجي بتأسيس منظومة عصرية قانونية ومؤسساتية من أجل ردع هذه الاعتداءات الرقمية وضمان الحماية الإلكترونية للفرد والدولة رغم انتشارها وقوه استفحالها وبما أننا دولة متجهة إلى رقمنة الحكومة والإدارة الجزائرية وكذا المعاملات الاجتماعية كان لابد من الغوص في هذه المجالات العلمية لتفادي المشكلات المستقبلية وعلى هذا الأساس خلصت هذه الدراسة لجملة من النتائج والتوصيات تمثلت في:

نتائج الدراسة:

- عدم وجود مفهوم جامع مانع للجريمة المعلوماتية رغم العديد من الاتجاهات والدراسات العلمية منها والقانونية.

- مرتكب هذه الأفعال قد يكون من أي طبقة اجتماعية أو فئة عمرية او مستوى علمي.

- تمييز مرتكبي هذه السلوكيات الإجرامية المعلوماتية بمؤهلات علمية وكفاءات تقنية جد عالية تعود لكياسة ونبوغ حجم الإدراك لديهم مقابل المجرم العادي.

- الجريمة المعلوماتية جريمة ذات طبيعة جنحية إلا أنها قد ترقى إلى السلوك الجنائي كالقتل بطريقة غير مباشرة مثال ذلك فصل جهاز الإنعاش القلبي والجهاز التنفسي عن مريض في حالة حرجة.

- تعد الجرائم المعلوماتية جرائم خطر أكثر من كونها جرائم ضرر.

- الجريمة الالكترونية جريمة مستمرة ويرجع الفضل في ذلك لطبيعتها الخاصة المميزة.

- نقص المعرفة بالتقنيات الإلكترونية أدى بشكل كبير إلى الوقوع في فخ الجرائم المعلوماتية.

- طبيعة مسرح الجريمة لهذا النوع من الجرائم صعب عملية المكافحة الاستباقية لها.

- إحجام غالبية الضحايا عن التبليغ بالرغم من حجم الأضرار البالغة اللاحقة بهم حيث تقدر هذه الاعتداءات في اليوم الواحد بكم لا يعد ولا يحصى.

- تعد الدوافع المادية والانتقامية النفسية من أبرز الأسباب الرامية لاقتراف هذا الاجرام.

- قلة التطبيقات والاجتهادات القضائية في هذا المجال.

- إغفال المشرع على العديد من السلوكيات الخطيرة التي قد يكون لها أثر جسيم على المجتمع وسيادة الدولة كخيانة الأمانة وغسيل الأموال المعلوماتي والجرائم الاباحية والماسة بالشرف والاعتبار المعلوماتي الشخصي.

- تنفذ هذه الجرائم في غالب الاحيان عن بعد دون حاجة الجاني للتواجد الشخصي أو التواجد المادي الملموس المباشر مع الضحية عكس الجرائم التقليدية.

-عدم اتجاه المشرع الوطني للمجال الوقائي بل اتجه مباشرة إلى مجال التجريم والعقاب

- تقاعس واحجام مواكبة التشريعات القانونية لهذه الظاهرة الإجرامية.

المقترحات:

- تضمين ودمج جل القواعد القانونية والتشريعية المختصة في مكافحة الإجرام الإلكتروني تحت غطاء نظام واحد موحد ذات عنوان الاعتداءات الرقمية في مجال الأنظمة المعلوماتية.

- اخضاع كل القطاعات والمعاملات لمبدأ الحماية التقنية لضمان الرقابة والوقاية من السلوكات الإجرامية غير الشرعية.

- تعمق وإفاضة المشرع الوطني في سنه القواعد القانونية فيما يخص هذه الجريمة السيبرانية.

- مضاعفة و تشديد القواعد الردعية والعقابية بما يناسب طبيعة هذه الجرائم التقنية.

- خلق إطار قانوني كفيل بحصر كل السلوكيات الإجرامية ذات الطبيعة الرقمية.

- إيجاد آليات مكافحة خاصة ومتخصصة أكثر لاستيعاب هذه التقنيات الحديثة.

- اعتماد جهات بحث وتحري مدربة متمكنة خبيرة في مجال التقنية المعلوماتية.

- إنشاء أقطاب ومحاكم قضائية مكرسة خصيصا لهذا النوع من السلوكات تتكون من تشكيلة قضائية محنكة متمكنة جيدا من معطيات وخبايا الواقع الافتراضي.

- تفعيل التعاون والتكاتف الدولي وتوحيد نظام عالمي مختص في هذا النوع من الإجرام كونها من السلوكيات العابرة للحدود الجغرافية الدولية.

- تشجيع البحث العلمي في المجال الإلكتروني من طرف الطلبة والباحثين الأخذ بعين الإعتبار الاجتهادات والتطبيقات العلمية في مجال التكنولوجيا الرقمية.

المصادر:

الجريدة الرسمية:

1. **المادة 8 من النظام السعودي بشان المكافحة المعلوماتية ، 1428-2008.**
2. **المادة الأولى من قانون العقوبات المصري النموذجي الموحد الخاص بمكافحة سوء استخدام تكنولوجيا المعلومات.**
3. **القانون رقم 16/02 المؤرخ في19/02/2016 المتمم للأمر 66-156 رقم المؤرخ في و المتضمن قانون العقوبات جاءت المادة 02 منه لتتمم قانون العقوبات بثلاث مواد منها المادة 87 مكرر 12.**
4. **المادة 02 منا القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة المتعلقة بالرقابة ومكافحة الجرائم المتصلة بتكنولوجيا إعلام واتصال ومكافحتها.**
5. **القانون 04-15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 الصادر في 08/06/1966.**
6. **المادة 394 ثلاثة مكرر 01 من القانون رقم 04/15 المعدل والمتمم لقانون العقوبات 2004.**
7. **المادة 394 ثلاثة مكرر 03 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات 2004.**
8. **المادة 46 من الدستور الجزائري بموجب تعديل 6 مارس سنة 2016, الفعل الرابع تحت عنوان الحقوق والحريات.**
9. **القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها, الجريدة الرسمية ,العدد 47.**
10. **تنص المادة 394 فقرتها 02 على «...تضاعف العقوبة إذا ترتب على الدخول أو البقاء حذف أو تغيير لمعطيات المنظومة..».**
11. **تنص المادة 394 فقرتها 03 على «... وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...».**
12. **المادة 394 مكرر 01 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.**

13. المادة 394 مكرر 02 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

14. المادة 394 مكرر 05 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

15. المادة 394 مكرر 07 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

16. المادة 394 مكرر 03 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

17. المادة 394 مكرر 04 من القانون رقم 15/04 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

18. المادة 37 من قانون الإجراءات الجزائية, من الفعل الثاني مكرر تحت عنوان: الوساطة من الكتاب الأولى في مباشرة الدعوى العمومية إجراءات التحقيق.

19. المادة 160 الصادرة بموجب قانون رقم 16/01 المؤرخ في 06/03/2016 المتضمن التعديل الدستوري من الجريدة الرسمية.

الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 47.

20. المادة 130 المادة 133 المادة 136 المادة 144 من القانون رقم 2000 03 المؤرخ في 5 غشت سنة 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية, الجريدة الرسمية للجمهورية الجزائرية, العدد 48.

21. القانون رقم 08-01 المؤرخ في 23 يناير 2008 المتعلق بالتأمينات الاجتماعية, الجريدة الرسمية للجمهورية الجزائرية, العدد 04.

22. المادة 394 مكرر من القانون رقم 04 15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

23. القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها, الجريدة الرسمية ,العدد 47.

الكتب والمجلات:

24. **الدكتور عمار عباس الحسيني، أستاذ القانون الجنائي، جرائم الحاسوب و الانترنت، جرائم المعلوماتية، منشورات زين الحقوقية، بيروت ، لبنان ، الطبعة الأولى ، 2017.**
25. **الدكتور مشتاق طالب وهيب النعيمي ، أستاذ القانون الجنائي ، الجرائم المعلوماتية ، تزوير المعلومات كأحد صور عن جرائم المعلوماتية دراسة مقارنة ، منشورات الحلبي الحقوقية الطبعة الأولى ، 2018.**
26. **الدكتورة شنتير خفرة ، دكتورة قانون جنائي ، الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة ، الطبعة الأولى، 2022.**
27. **الدكتورة خنيش دليلة ، الجريمة الإلكترونية و الأمن الاجتماعي ديوان المطبوعات الجامعية ، 2023.**
28. **خاليدة بن بعلاش , جامعة تيارت, علي عثماني, المركز الجامعي آفلو–الأحكام الموضوعية والإجرائية مكافحة الجريمة الإلكترونية في التشريع الجزائري, مجلة أبحاث قانونية وسياسية, المجلد 06 العدد 02 ديسمبر 2021.**
29. **راضية عيمور, الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري, جامعة الاغواط, المجلة الاكاديمية للبحوث القانونية والسياسية, 2022 المجلد السادس, العدد الأول.**
30. **الدكتورة ناني لحسن, التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018.**
31. **الدكتورة ناني لحسن , التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018.**
32. **مهداوي حنان , التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري, مجلة الفكر القانوني والسياسي, جامعة محمد لمين دباغين , سطيف 02 , المجلد السادس, العدد الثاني 2022.**
33. **الدكتورة ناني لحسن, التحقيق في الجرائم المتصلة بتكنولوجيا المعلومات بين النصوص التشريعية والخصوصية التقنية, النشر الجامعي الجديد, 2018.**
34. **راضية عيمور, الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري, جامعة الاغواط, المجلة الاكاديمية للبحوث القانونية والسياسية, 2022 المجلد السادس, العدد الأول.**

35. الدكتور يعيش تمام شوفي ، سلسلة مطبوعات المنبر ، الجريمة المعلوماتية ، دراسة مقارنة جامعة محمد خيضر بسكرة ، الطبعة الأولى ، جانفي 2019.

36. الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015 ، إعداد مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى ، عمان.

37. الباحثة سويسي فتيحة, قاضية باحثة بمركز البحوث القانونية والقضائية, "التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها" مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18/01/2022.

38. الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها ، مسابقة جائزة الأمير نايف بن عبد العزيز، البحوث الأمنية لعام 2015.

39. الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية ببودابست سنة 23/11/2001

40. الدكتورة بوضياف أسمهان, الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر, جامعة محمد بوضياف المسيلة, مجلة الأستاذ الباحث للدراسات القانونية والسياسية, العدد الحادي عشر ,سبتمبر ,2018.

41. الدكتور بن دراح علي ابراهيم , محاضرات في الجرائم المعلوماتية, معهد الحقوق و العلوم السياسية , المركز الجامعي افلو 2020/2021.

42. إيمان بغدادي, أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية, جامعة قسنطينة مجلة آفاق البحوث والدراسات السياسية, العدد 04, جوان, 2019.

43. مهداوي حنان, التنظيم القانوني في الجريمة الإلكترونية في التشريع الجزائري, جامعة محمد لمين دباغين سطيف 2, مجلة الفكر القانوني والسياسي (1620-2588:ssn/), المجلد السادس, العدد الثاني, 2022.

44. الدكتور يعيش تمام شوفي ، سلسلة مطبوعات المنبر ، الجريمة المعلوماتية ، دراسة تأصيلة مقارنة جامعة محمد خيضر بسكرة ، الطبعة الأولى ، جانفي 2019.

45. عائشة, محاضرات في الجريمة المعلوماتية, للسنة أولى ماستر, تخصص قانون جنائي وعلوم جنائية ,جامعه زيان عاشور, الجلفة,2021-2022.

46. الدكتورة أمينة بضافة, الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة, جامعة الجزائر 03 ,حوليات جامعة الجزائر 01 ,المجلد 37/العدد1- 2023.

47. الدكتورة بوراس نادية, محاضرات مقدمة في مقياس الجريمة الإلكترونية, جامعة محمد لمين دباغين, سطيف -2023.
48. الدكتور محمد شرقي, الدكتور صلاح الدين جبار, تأثير تطور تكنولوجيا المعلوماتية على تنامي الجريمة, جامعة لونسي علي, البليدة 02.

المذكرات:

49. بن يونس محمد الأمين بن مصطفى, خير الناس عمر بن إبراهيم, حماية الأطفال من الجريمة الإلكترونية, مذكرة مقدمة لاستكمال نيل شهادة الماستر, جامعة غرداية,2022-2023.
50. مدرك ناريمان , الآليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري, مذكرة نهاية الدراسة لنيل شهادة الماستر, جامعة عبد الحميد بن باديس, مستغانم,2022/2023.
51. عقباش بريزة, مبارك حنان, آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري , مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي, جامعة محمد البشير الإبراهيمي, برج بوعريريج,2022/2021.

52. مذكرة مقدمة لاستكمال متطلب طلبات اثنين شهادة ماستر أكاديمي في الحقوق، تخصص قانون إعلام آلي والانترنت جامعة محمد البشير الابراهيمي برج بوعريريج، 2022/2021.
53. ملياني عبد الوهاب ، رسالة لنيل شهادة الدكتوراه في القانون العام ، أمن المعلومات في بيئة الأعمال الالكترونية ، جامعة أبي بكر بلقايد ، تلمسان ، 2016-2017.
54. بصرة سعيدة , الجريمة الإلكترونية في التشريع الجزائري, دراسة مقارنة مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق, جامعة محمد خيضر بسكرة. 2015-2016.
55. بقدار شيماء , آليات مكافحة الجريمة الالكترونية على المستويين الدولي والوطني, مذكرة نهاية الدراسة لنيل شهادة الماستر, جامعة عبد الحميد بن باديس, مستغانم, 2022/2023.
56. غريي جميلة , آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري, مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي و علوم جنائية ,جامعة آكلي محند أولحاج, البويرة 2020-2021.

57. عمار حشمان, الجريمة المعلوماتية في التشريع الجزائري, مذكرة مقدمة لاستكمال متطلبات شهاده الماستر المهني الطور الثاني, ميدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير, جامعة قاصدي مرباح ورقلة, 2019.

58. بوديسة بجاد عبد الرؤوف, آليات التحري عن الجريمة الإلكترونية في القانون الجزائري, مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر مهني في الحقوق ,تخصص قانون إعلام آلي والانترنت, جامعة محمد البشير الابراهيمي, برج بوعريريج,2021-2022.

59. حرزون ليلى هدروق أسماء, التنظيم القانوني في الجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري, مذكرة لنيل شهادة الماستر في القانون الخاص ,جامعة عبد الرحمان ميرة, بجاية,2021-2022.

60. رزيقة بونار, الجريمة المعلوماتية في التشريع الجزائري, مذكرة مكملة لنيل شهادة الماستر, جامعة محمد الصديق بن يحيى ,جيجل,2020-2021.

61. لعاقل فر يال، الجريمة المعلوماتية في ظل التشريع الجزائري, مذكرة لنيل شهادة ماستر في القانون العام, جامعة آكلي محند أولحاج , البويرة,2014-2015.

المواقع الالكترونية:

62. المركز العربي لأبحاث القضاء الإلكتروني article detail http://accronline.com (تاريخ الدخول في 17/04/2024).

63. الاتفاقية رقم 108 المؤرخة في 28/01/1981 لمجلس أوروبا المتعلقة بحماية الأشخاص اتجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي, رابط الموقع الرسمي لمجلس أوروبا www.intcoe.

الفهرس

الفهرس

الفهرس

الفهرس

الفهرس