وزارة التعليم العالي والبحث العلمي
المركز الجامعي صالحي أحمد – النعامة –
معهد الحقوق
قسم القانون

مذكرة مقدمة لنيل شهادة الماستر – ل.م.د –
الشعبة : حقوق
التخصص: قانون أعمال

تحت عنوان :

آليات مكافحة الجريمة الالكترونية

من إعداد الطالبتين :
شرويلي فاطمة
ديدي فضيلة

تحت إشراف :
د. مولاي محمد الأمين

المناقشة من طرف اللجنة المكونة من :

اسم ولقب الأستاذ	الرتبة العلمية	الصفة
د. مولاي بلقاسم	محاضر	رئيسا
د. مولاي محمد الأمين	محاضر	مشرفا ومقررا
د. بن حبيبة إيمان	محاضر	مناقشا

السنة الجامعية : 2023/2022

إهـــداء

أهدي ثمرة جهدي إلى :

من جرع الكأس فارغا ليسقيني إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم إلى روح والدي الطاهرة رحمه الله تعالى

وإلى أمي الكريمة أطال الله في عمرها وإلى أخواتي وأصدقاء دربي وزملائي

و إلى زوجي قرة عيني وسندي ومن كان سببا في تحفيزي لتكملة دراستي وإلى بناتي حفظهم الله لي.

وإلى كل من ساهم في إنجاز هذا العمل من قريب و بعيد.

فاطمة

إهـــــداء

بسم الله الرحمن الرحيم و الحمد لله الذي لا هادي إلا هو ولا معينا إلا سواه له الفضل والشكر على كل من طلب بعلمه مرضاة الله.

أهدى ثمرة جهدي ونحاجي إلى ملاكي الحامي وملكة حياتي سعادتي إلى من كانت قوتي وعزمي وسندي إلى أحسن امرأة في العالم ودعائها كان سيلا لإنارة دربي أمي الغالية وإلى من علمنى العطاء إلى من تحت شخصيتي ووقف وراء ظهري دائما " أبي العزيز"

وإلى من وهبني الله بنعمة وجودهم في حياتي وكانوا عونا أخي علي وأخواتي سارة وسماح وإلى أخوالي خالدي الذين كانوا سندا لي في هذه الحياة.

وكل صديقاتي وأصدقائي الذين جمعتني بهم الحياة ولأساتذتي الذين سايروني في مشواري الدراسي وبأخص أستاذي المشرف " مولاي أمين ".

إلى كل هؤلاء أهديهم هذا العمل المتواضع ، سائلة الله العلي القدير أن ينفعنا به ويمدنا بتوفيقه.

فضيلة

شكـــر وعرفان

الحمد لله رب العالمين خلق اللوح والقلم ، وخلق الخلق من عدم ودبر الأرزاق والآجال بمقادير ، أشكره سبحانه وتعالى على حسن توفيقه و منه علينا بإنجاز هذه المذكرة.

ونتقدم بالشكر الجزيل إلى أستاذنا الفاضل والمشرف علينا في هذا العمل الأستاذ / مولاي محمد أمين ، والذي لم يبخل يوما بوقته وبجهده علينا .

و إلى كل من ساعدنا في إنجاز هذا العمل,

قائمة المختصرات :

- **ق.د** : القانون الدستوري.
- **ق.إ.ج.ج** : قانون الإجراءات الجزائية الجزائرية.
- **ق.م** : القانون المدني.
- **ق.ع.ج** : قانون العقوبات الجزائري.
- **ج.ر** : الجريمة الرسمية.
- **د.ط** : دون طبعة.

مقدمة

المقدمة

نظرا للتطور الهائل في مجال الإعلام والاتصال ، المصحوب بالتطور الهائل في تكنولوجيا الكمبيوتر والأجهزة الذكية ، مما أدى إلى ظهور أدوات واختراعات وخدمات جديدة ، مما نتج عنه ظاهرة تسمى المعاملات الإلكترونية ، والتي تشير إلى المعاملات من خلال أجهزة الكمبيوتر والإنترنت والهواتف المحمولة (الهواتف الذكية) وغيرها من الأجهزة الإلكترونية ، بسبب النطاق الواسع والتطور السريع لهذه الأجهزة ، مع ضعف قدرات المصاحبة والرصد والتحكم ، ظهر نوع جديد من الجريمة يعرف باسم المعلومات الإلكترونية. أو الجريمة التكنولوجية ، وهي استخدام تكنولوجيا الكمبيوتر أو الأنشطة الإجرامية التي ترتبط فيها الهواتف الذكية بشكل مباشر أو غير مباشر بالإنترنت لارتكاب أعمال إجرامية تهدد حاليًا سلامة وأمن الأفراد والمؤسسات ، وحتى الحكومات بحاجة إلى تسريع الإجراءات الضرورية للحد من خطورة مثل هذه الجرائم.

الجريمة الإلكترونية أو الجرائم الإلكترونية هي جرائم يتم ارتكابها باستخدام تقنيات الحاسوب والإنترنت، وتندرج هذه الجرائم تحت مجموعة واسعة من الأنشطة المختلفة المتعلقة بالإنترنت، مثل الاحتيال، والتزوير الإلكتروني، والتجسس، والاختراق، والتحريض على الكراهية والإرهاب، والتنمر الإلكتروني، وغيرها من الأفعال الإلكترونية التي تسبب الأذى للأفراد والمؤسسات.

وعلى الرغم من أن الإنترنت قد جعل الحياة أكثر سهولة وإيجابية في كثير من الأحيان، إلا أنه في الوقت نفسه، أدى إلى زيادة الجرائم الإلكترونية والمشاكل الأمنية المتعلقة بها، وهذا يتطلب منا جميعًا حماية أنفسنا وأجهزتنا الإلكترونية، واتخاذ إجراءات وقائية لحماية أنفسنا من مخاطر الإنترنت والجرائم الإلكترونية.

تكمن أهمية موضوع الجريمة الإلكترونية في الانتشار الواسع لمثل هذه الجرائم والتي يصاحبها من ناحية انتشار استخدام المعاملات الإلكترونية على المستوى الدولي والإقليمي والوطني هذا من ناحية.

ومن ناحية أخرى أصبحت الجريمة الإلكترونية حديث العصر ، نظرًا للتقدم الهائل في استخدام شبكة الويب العالمية (الإنترنت) ، ظهرت الجريمة الإلكترونية في أشكال مختلفة وأصبحت تهديدًا لأمن المعلومات للأفراد والمؤسسات والحكومات.

وما دفعنا لاختيار هذا الموضوع الشيق هو تزايد أهمية البحث في الجرائم الالكترونية مع كثرة استخدام التكنولوجيا والإنترنت في حياتنا اليومية. كما أنها تندرج تحت فئة الجرائم السيبرانية وتشمل الاحتيال الإلكتروني، السرقة الإلكترونية التجسس، واختراق النظام الإلكتروني وغيرها ، هذا من جهة.

ومن جهة أخرى نملك دوافع ذاتية لخصناها في الرغبة الكبيرة في الإثراء المعرفي الخاص بهذا الصنف من الجرائم الفتاكة والتي انتشرت في الآونة الأخيرة انتشارا مخيفا في وسط المجتمعات العالمية خصوصا الجزائر ، وما يطرحه هذا الموضوع من تساؤلات عدة في النفوس.

الدراسات السابقة التي تعرضت لموضوع الجريمة الالكترونية هي قليلة بالمقارنة بغيرها من المواضيع الأخرى.

ولتسليط الضوء أكثر على الموضوع نطرح الاشكالية التالية:

ماهي الآليات والتدابير الكفيلة لمكافحة الجرائم الإلكترونية؟

ومن هذه الإشكالية نتفرع الى عدة تساؤلات منها:

- ما المقصود بالجريمة الإلكترونية؟ والإجراءات المتبعة؟
- وماهي الآليات المتخدة لمواجهة الجريمة الإلكترونية على الصعيد الدولي والعربي والوطني؟

وللإجابة على الإشكالية الرئيسة والأسئلة الفرعية المطروحة اعتمدنا على المنهج الوصفي لوصف أسلوب الجرائم الالكترونية وصفا دقيقا ، و كذا المنهج التحليلي لتحليل النصوص القانونية المتعلقة بالموضوع ، وأيضا استعنا بالمنهج المقارن وذلك بغية معرفة موقف المشرع الجزائري مقارنة مع التشريعات الأخرى وذلك للاستفادة من تجارب الدول وفهم النصوص القانونية وتطبيقاتها.

ومن أهم الصعوبات التي واجهتنا في بحثنا هذا هي صعوبة جمع المعلومات المتعلقة بهذا الموضوع من نذرة للمراجع والمصادر التي تسلط الضوء على الجريمة المعلوماتية. وتقريبا جل المصادر تطرق إلى الموضوع بشكل جد وجيز ومختصر.

ومن أجل دراسة موضوع البحث بطريقة ممنهجة ومحكمة ارتأينا من خلال هذه الدراسة إلى تقسيم الموضوع إلى فصلين :

حيث سنتناول في الفصل الأول ماهية الجريمة الالكترونية وقسمناه الى مبحثين تناولنا في المبحث الأول مفاهيم الجريمة الالكترونية والمبحث الثاني أركان وأحكام الجريمة الالكترونية والإجراءات العامة.

بينما تكلمنا في الفصل الثاني عن التحديات القانونية لمكافحة الجريمة الالكترونية وقسمناه الى مبحثين ، تناولنا في المبحث الأول الآليات والسبل للحد من الجريمة الالكترونية على المستوى الدولي ، أما في المبحث الثاني المكافحة التشريعية للجريمة الالكترونية في الجزائر ، وخلصنا هذه الدراسة بخاتمة أجبنا فيها عن الإشكالية المطروحة ومجمل النتائج التي توصلنا اليها.

الفصل الأول :

ماهية الجريمة الالكترونية

تعتبر الثورة التكنولوجية ، ولا سيما ثورة الاتصالات ، أهم تطور في العالم اليوم ، ثورة الاتصالات هي المحرك الرئيسي للتطورات التي تحدث حاليًا ، لكنها ليست المحرك الوحيد لهذه التطورات ، لأن التطور الهائل لقد سهلت تكنولوجيا الكمبيوتر بشكل كبير الاتصال وسرعة التقدم في مجال المعلومات.

وقد كان من نتاج التطور فى الجانبين ظهور أدوات واختراعات وخدمات جديدة فى مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

المبحث الأول : مفاهيم الجريمة الالكترونية.

الجريمة الإلكترونية هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله الأجهزة الإلكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد .

المطلب الأول : تعريفات الجريمة الالكترونية

لقد تعددت التعاريف واختلفت الآراء كلا حسب وجهة نظره إلى الجريمة الالكترونية وعليه يجب علينا أولا تعريفها (الفرع الأول) ثم تعريفها في التشريع الجزائري والمقارن (الفرع الثاني).

الفرع الأول : تعريف الجريمة الالكترونية

البند الأول: التعريف الضيق

تعرف الجريمة المعلوماتية على أنها : " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لإرتكاب من ناحية لملاحقته وتحقيقه من ناحية أخرى."

يرى الأستاذ Mass أن المقصود بالجريمة المعلوماتية : " الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح."

الفقيه الألماني Tiedemann أن : " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام الحاسب. فهو يرتكز في تعريفه على وسيلة إرتكاب الجريمة.[1]

البند الثاني : التعريف الواسع

هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالأتي : كل فعل أو امتناع عمدي ، ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال أو الأشياء المعنوية الخبير الأمريكي parker مفهوما واسعا للجريمة المعلوماتية أنها : كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه ، أو كسب يحققه الفاعل

كما يعرفها الأساتذة Vivant وLestanc الجريمة المعلوماتية أنها : " مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب."

كما أن الخبير الأمريكي Parker تبنى مفهوما واسعا للجريمة المعلوماتية على أنها : "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل ". [2]

[1] بعرة سعيدة ، الجريمة الالكترونية في التشريع الجزائري ، دراسة مقارنة ، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، بسكرة ، 2016/2015 ، الصفحة 11.

[2] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط 1 ، دار الثقافة للنشر والتوزيع ، عمان ، 2008 ، الصفحة 49.

كما عرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة ثم غير مباشرة عن تدخل التقنية المعلوماتية ". كما تعرف أيضا : " تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية أو المعلوماتية."

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية ، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها ، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية. فهذه التعاريف تتبنى المفهوم الموسع للجرائم الالكترونية والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها أو عن طريق شبكة الانترنت أو بأي وسيلة الكترونية أخرى تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها. [1]

جرائم الكمبيوتر فهو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء أداة الجريمة أو كان هدف الجريمة ويدخل من ضمنها جرائم معلوماتية وجرائم الإنترنت ، كما يدخل من ضمنها الإعتداء على الشبكات المحلية خاصة بالهيئات والمنشات الخاصة والعامة.

جريمة الإلكترونية هي ببساطة استخدام التقنيات الرقمية لإخافة الآخرين. [2]

[1] يزيد أبو حليط ، الجرائم الالكترونية والوقاية منها في القانون الجزائري ، في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة ، د.ط ، دار الجامعة الجديدة للنشر الإسكندرية 2019 ، الصفحة 51.

[2] بعرة سعيدة ، المرجع السابق ، الصفحة 10.

الفرع الثاني : تعريف الجريمة الالكترونية في التشريع الجزائري والمقارن

سنسلط الضوء في هذا الفرع على تعريف الجريمة الالكترونية في التشريع الجزائري تعريفا فقهيا وأكاديميا وقانونيا.

البند الأول : التعريف الفقهي

إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلا في الجرائم التقليدية فلهذا ظهر اختلاف في تعريف قائما من هذه التعاريف ما يلي : " بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال ".

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

أو أنها " استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي و الهاتف النقال ، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضيها المجتمع". [1]

ومن خلال هذه التعاريف تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية ، جميع الجرائم التي بمكن ارتكابها في بيئة إلكترونية. [2]

البند الثاني : التعريف القانوني

تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي

---

[1] زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، د ط ، 2011 الصفحة 42.

[2] زبيحة زيدان ، المرجع السابق ، الصفحة 43.

لا بد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث. [1]

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات. [2]

حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. [3] مسميا إياه : " المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة ، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين ". [4]

المطلب الثاني : خصائص وصور وأنواع الجريمة الالكترونية

لا شك أن المعلوماتية عادت على الإنسان بالخير الكثير، وطبعت مختلف جوانب حياته بطابع لم يكن ليحلم به قبل وقت قريب، فهذا التقدم العلمي الكبير في مجال المعلوماتية يسر حياة الإنسان ووفر عليه جهداً كبيراً وطبع شتى معاملاته بالسرعة الفائقة والتي لولا هذا التطور لاستغرقت من الوقت الكثير، كما أن هذه المعلوماتية وفرت على الإنسان الكثير من المال الذي كان سينفقه في قضاء حاجات أصبح يمكنه أن يقضيها في بيته بكبسة زر، لكن وفي المقابل فقد ارتبط استعمال هذه الوسائل الفنية الحديثة بظهور جرائم جديدة لم تكن معروفة من قبل، فهذه التقنية أوجدت ألوانا جديدة من الجرائم طبعتها بطابعها وأسبغت عليها خصائص ميزتها عن غيرها من الجرائم، سواء تعلقت هذه الخصائص بالشخص الذي يقدم على هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت

[1] قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 ، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، الجريدة الرسمية عدد 47 بتاريخ 2009/08/16 ، الصفحة 5.

[2] نفس المرجع ، الصفحة 5.

[3] المادة 2 الفقرة ب من القانون رقم 09-04 ، المرجع السابق.

[4] نشناش منية ، مداخلة حول الركن المفترض في الجريمة المعلوماتية ، جامعة بسكرة 2015 -2016 ، الصفحة 4.

بالجريمة ذاتها وصعوبة اكتشافها وإثباتها أو ما يلعبه الضحية من دور فيها، أو تعلق الأمر بالنطاق المكاني لهذه الجريمة أو الخسائر التي تخلفها.

الفرع الأول: خصائص الجريمة الالكترونية

تنفرد الجريمة الالكترونية بخصائص عدة تميزها عن بقية الجرائم ، في هذا الفرع سنتطرق إلى هذه الخصائص المتعلقة بالجريمة الالكترونية وهي كالتالي : الجرائم التي تدفع على المعطيات ، الجرائم العابرة للحدود ، سهولة ارتكابها ، صعوبة معرفة مرتكب الجريمة سهولة إخفاء وطمس آثارها وأخيرا جرائم متطورة ومتعددة الأشكال.

البند الأول : الجرائم التي تدفع على المعطيات

نظرا لما تشهده الدول بصفة عامة بما فيها الجزائر، فيما تعلق بالتحول الرقمي للمعلومات المتعددة الاستعمالات والإستخدامات عامة كانت أو خاصة ، مسموح بتداولها أو غير مسموح ذات قيمة أو ليست ذات قيمة ، والمهم أن تلك المعلومات المتداولة آليا ينبغي حمايتها من الإعتداء عليها، لهذا تدخل المشرع لإضفاء حماية لها تكرس لدى الأشخاص جانب من الأمن القانوني لمالك تلك المعلومة أو بالأحرى أمن قانوني للمعلومة في حد ذاتها من مختلف الإعتداءات الواقعة عليها، فإذا كان هذا الإهتمام بالمعلومة الإلكترونية بوجه عام فالأمر يزداد أهمية بالنسبة للمعلومات الشخصية التي تتميز بطابعها الحساس، وهذا لإرتباطها بحرمة الحياة الخاصة للأفراد، فبالرغم من صدور عدة نصوص قانونية ، سواء كانت متعلقة بالمعلوماتية أو بحرمة الحياة الخاصة، إلا أنها لم تشر إلى المعطيات الشخصية كحق يستوجب حمايته هذا الفراغ القانوني استمر إلى غاية صدور القانون رقم 18/07 [1] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10 يونيو سنة 2018 والصادر بالجريدة الرسمية عدد 34 المؤرخة بتاريخ 10 يونيو 2018، والذي تضمن في فصله الثاث أحكام جزائية متعددة وما يهمنا في هذه الدراسة هي تلك الجرائم المتعلقة بالمساس بالمعطيات الشخصية التي سنحاول تسليط

[1] القانون 18/07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الضوء عليها وفق دراسة قانونية تحليلية نقف من خلالها على صور تلك الجرائم متعمقين في أركانها والجزاءات المترتبة عنها. [1]

البند الثاني : الجرائم العابرة للحدود

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحاسبات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان في دولة معينة علي مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت، خاصة في مجال التجارة الإلكترونية وازدياد اعتماد البنوك عليها.

الجريمة الإلكترونية ذات بعد دولي، أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، كما ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية. [2]

وتثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصلة عليها في دولة ما أمام قضاء دولة أخرى [3] وتذكر في هذا المجال قضية Thompson RN وفيها قام مبرمج انجليزي يعمل لدى بنك بالكويت بالتلاعب في معطيات بنظام الحاسب الآلي الخاص بالبنك، وذلك عن طريق الخصم من أرصدة العملاء ثم الإيداع في حسابه الخاص، وبعد عودته لانجلترا طلب من البنك تحويل الحساب الخاص إلي عدة حسابات بنكية في انجلترا فقام البنك بذلك ، حوكم الفاعل بتهمة

[1] ملياني عبد الوهاب ، جرائم المساس بالمعطيات الشخصية على ضوء القانون رقم 18/07 ، مجلة البحوث القانونية والاقتصادية ، الطبعة 6 ، العدد 1 ، بتاريخ 2023/01/28 ، الصفحة 272.

[2] ابراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مجلة كلية الشريعة والقانون بطنطا، الجزء الثاني، العدد 30 ، الصفحة 374.

[3] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة 2003 الصفحة 49.

الحصول على أموال الغير بطريق الاحتيال وحكم عليه بعقوبة السجن، طعن في الحكم استنادا إلى عدم اختصاص القضاء الإنجليزي لأن فعلي السحب والإيداع قد تما في الكويت لا في إنجلترا لكن محكمة الاستئناف رفضت طعنه وردت بأن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية.

البند الثالث : سهولة ارتكابها

لا تتطلب جرائم الأنترنت عنفا لتنفيذها أو مجهودا كبيرا ، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء ، كما هو الحال في جريمة القتل أو الاختطاف ، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة. [1]

تتميز جرائم الأنترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة ، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الأنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو الغرير بالقاصرين ، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الانترنت من الجرائم النظيفة فلا آثار فيها لأي عنف أو دماء ، وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي. [2]

البند الرابع : صعوبة معرفة مرتكب الجريمة

تتميز الجريمة الالكترونية بصعوبة اكتشافها وإثباتها ، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة ، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه

[1] يوسف صغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة لنيل شهادة الماجستير في القانون الخاص ، كلية الحقوق جامعة مولود معمري ، تيزي وزو ، 2013 ، الصفحة 16.

[2] يوسف صغير ، المرجع السابق ، الصفحة 16.

الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية ، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الالكترونية وإثباتها إلى عدة عوامل منها : [1]

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

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

3- تحتاج الجريمة الالكترونية لاكتشافها إلى خبرة فنية ، حيث تتطلب جريمة الكمبيوتر إلمام معلومات واسعة سواء لارتكابها أو التحقيق فيها ، كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الالكتروني ، فقد يتسبب المحقق دون قصد في إتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنيين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الالكترونية. [2]

البند الخامس : سهولة إخفاء وطمس آثارها

يعتبر إخفاء وطمس آثار الجريمة الإلكترونية من الأمور الصعبة جداً وغير القانونية حيث يمكن للسلطات الإلكترونية والمتخصصين في الجرائم الإلكترونية استخدام تقنيات متطورة لتحديد مصدر الهجوم ومعرفة المتورطين فيه، كما يمكن للشرطة القضائية استخدام أدوات الرصد والتحليل الجنائي الرقمي لتحديد منفذ الهجوم ومسار الجريمة الإلكترونية.

[1] حسين فريجة ، الجرائم الالكترونية والانترنت ، مجلة المعلوماتية ، العدد 36 ، أكتوبر 2011 ، الصفحة 3.

[2] يوسف صغير ، المرجع السابق ، الصفحة 16.

لذلك، يجب على الأشخاص عدم الاعتماد على تقنيات إخفاء الآثار الإلكترونية لأنها يمكن أن تؤدي إلى اكتشاف دلائل عليها وتعريض صاحبها للمساءلة القانونية. [1]

البند السادس : جرائم متطورة ومتعددة الأشكال

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات لا يوجد لها مثيل لدى غيره، كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنده أيضا، فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي، أي انه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أن هذا المجرم إنسان ذكي، إذ أنه يستغل ذكاءه في تنفيذ جريمته، ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا، ويفسر هذا أن هذا المجرم من ذوي المستويات العلمية العالية غالبا.

وما يميز مجرم المعطيات أيضا هي الدوافع التي تدفعه لارتكاب الجريمة، فهي متعددة ومختلفة فقد تكون السعي لتحقيق الربح وقد تكون الرغبة في الانتقام من رب العمل وقد تكون الرغبة في قهر النظام والتفوق علي وسائل التقنية وتعقيدها. وقد يرتبط الدافع بحب التعلم والاستكشاف، كما قد يرتبط بالسياسة والايديولوجيا .. إلى غير ذلك من البواعث كما يتميز مجرم المعطيات أيضا بفئاته وأنماطه المختلفة وهو ينقسم إلى نوعين رئيسيين :

- الأول : هم الهواة المولعون بالمعلوماتية.
- والثاني : هم محترفو الجرائم المعلوماتية وأساس التمييز بين النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة، بينما هو ساذج لدى النوع الأول لا يتعدى الرغبة في الاستطلاع والاستكشاف، فهو خبيث لدى النوع الثاني، والذي قد يكون ماليا أو سياسيا أو غيره. [2]

---

[1] يوسف صغير ، المرجع السابق ، الصفحة 18.

[2] د, عبد الله حسين محمود ، شرقة المعلومات المخزنة في الحاسب الآلي ، دار النهضة العربية ، ط 2 ، القاهرة 2002 الصفحة 36.

الفرع الثاني : المجرم المعلوماتي

يعتبر المجرم المعلوماتي أساس ارتكاب الجريمة في المجال المعلوماتي ، وتتطلب السياسة الجنائية بداية التعرف على هذا النوع الخطير من المجرمين بالإضافة إلى التعرف على الدوافع التي تؤدي بهم إلى ارتكاب هذه الجرائم ، حتى يستطيع المشرع معرفة أسباب هذا الإجرام ومحاولة مكافحته والوقاية منه وعلى هذا الأساس ، سوف يتم التعرف على تصنيفات المجرم المعلوماتي (البند الأول) ، وصفاته (البند الثاني) ودوافعه (البند الثالث).

البند الأول : تصنيفات المجرم المعلوماتي

مما لا شك فيه أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير يعد في نظر القانون مجرما ويتعرض للعقاب إذا ما اقترف جريمته. ولذلك، ولكي تحقق العقوبة هدفها المباشر أو غير المباشر أي تحقيق الردع العام أو الخاص فيجب النظر إلى المجرم المعلوماتي من حيث صفاته، والظروف التي دفعته إلى ارتكاب جريمته وأسبابها وذلك حتى يمكن تأهيله .اجتماعيا وقد تم تصنيف المجرم المعلوماتي إلى ثلاثة أنواع :[1]

1- **هواة ارتكاب الجرائم المعلوماتية** : ويطلق على هذه الطائفة مصطلح (الهاكرز) Hacker's ويعني المتطفل، وهو ذلك الشخص الذي يدخل على شبكات وحاسبات الآخرين دون حق يتميزون بقدر عال التقنية، ويتفاخرون بإلمامهم بعلوم الحاسوب وبقدرتهم على اختراق شبكات الحاسب الآلي وبجهدهم الذاتي، ودون الاستعانة بأي تعليمات من أي مصادر، وأغلبهم صغار السن؛ مراهقون وشباب طلبة وتلاميذ ثانويات وشباب عاطل عن العمل.

ويهدف هاوي ارتكاب الجرائم المعلوماتية إلى الحصول على المعلومات بشتى الوسائل ويسخر قدراته في هذا المجال. [2]

[1] د. بن مكي نجاة ، السياسة الجنائية لمكافحة الجرائم المعلوماتية ، منشورات دار الخلدونية ، 2017 ، الصفحة 39.

[2] بن مكي نجاة ، المرجع نفسه ، الصفحة 39-40.

2- **محترفو ارتكاب الجرائم المعلوماتية :** ويطلق على هذه الطائفة مصطلح Cracker's ويتميز أفراد هذه الطائفة بالتخصص العالي في مجال الحاسب الآلي، وتعد هذه الطائفة الأخطر من بين مجرمي المعلوماتية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب

المادي لهم أو للجهات التي كلفتهم و سخرتهم لارتكاب جرائم الحاسوب، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي وأفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم.

وتشير الدراسات إلى أنهم من الشباب الأكبر سنا من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين 25 و 40 سنة، وغالبا ما يتم ارتكاب هذه الجرائم المعلوماتية في هذه المرحلة من أشخاص يعملون في منشأة ما، أو مسؤولين عن أنظمة معلوماتية، فهم يملكون المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسبات الآلية، وعندئذ يقومون بتنفيذ أفعالهم غير المشروعة بأنفسهم أو بمشاركة أو مساعدة أشخاص آخرين سواء كانوا فنيين أم مجرد وسطاء، ومما يساعد على نجاح عملياتهم غير المشروعة. وهنا يكمن الخطر الحقيقي، أنهم كثيرا ما ينظر إليهم بوصفهم مستخدمين مثاليين، والغالبية العظمى فيهم يشغلون مراكز قيادية هامة، ويتمتعون لذلك بثقة كبيرة في مجال عملهم. [1]

ويتشابه مرتكبو هذه الأفعال الآثمة مع المجرمين ذوي الياقات البيضاء من حيث كونهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة مع تقنية الإلكترونيات وعلى قدر من الذكاء. [2]

يكتسب هذا النمط المستحدث من الإجرام المرتبط بالاستخدام التعسفي للحاسب الآلي خطورة خاصة، نظرا إلى تقنيته العالية من جهة ولتعدد أنواع مرتكبيه وغموض شخصيتهم من جهة أخرى في الهاكرز يتحدون إجراءات نظم المعلومات، ولكن لا تتوافر لديهم دوافع

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 40.

[2] بن مكي نجاة ، المرجع نفسه ، نفس الصفحة.

تخريبية بل لهم دافع التحدي وإثبات قدراتهم وتفوقهم على عكس الكراكرز الذين تعكس اعتداءاتهم الميول الإجرامي الخطير في إحداث التخريب.

3- **المتطرفون من ذوي المثل العليا** : تتألف هذه المجموعة من أشخاص يدافعون عن قضية أو غاية ليس لها علاقة بمصالحهم الشخصية المباشرة وهم على استعداد للانخراط في أنشطة إجرامية من شأنها أن تسبب أضرارا جسيمة بالآخرين أو بقطاعات كاملة في المجتمع، وقد يكون وراء ذلك اسباب ذات طابع سياسي أو اقتصادي أو ديني أو تتعلق بحقوق الإنسان. [1]

البند الثاني : صفات المجرم المعلوماتي

يتميز مرتكب الجرائم المعلوماتية بصفات خاصة غيره من مرتكبي الجرائم وذلك من حيث :

- إنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنه إنسان متوافق معه، وتزداد خطورته الإجرامية إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه. [2]
- إنه إنسان محترف وذكي يكفي أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه البيانات أو يعطل استخدام البرامج وليس عليه سوى اللجوء إلى زرع الفيروسات في هذه البرامج أو استخدام القنابل المنطقية أو الزمنية لكي يشل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه الطبيعية. وقد يصل الأمر إلى حد احتراف الإجرام ، مما يشمل خطرا كبيرا على المجتمع ، سواء كان فردا أو جماعة منظمة أو غير ذلك. [3]

كل هذه الصفات ساعدت هؤلاء المجرمين على اتركاب جرائمهم دون ترك أي أثر مادي يمكن من خلاله الكشف عن جرائمهم ومساءلتهم جنائيا.

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 41.
[2] بن مكي نجاة ، المرجع نفسه ، الصفحة 41-42.
[3] بن مكي نجاة ، المرجع نفسه ، الصفحة 42.

البند الثالث : دوافع ارتكاب الجرائم المعلوماتية

ثمة دوافع عديدة تحرك مجرمي المعلوماتية لارتكاب أفعال الاعتداء المختلفة المنضوية تحت مفهوم الإجرام المعلوماتي ، ويمكن تلخيص هذه الدوافه فيما يلي :

1 – الدوافع الذاتية :

أ– الرغبة الأكيدة في الانتقام : الانتقام موجود داخل النفس البشرية ، فكثير من الأفراد يفصلون تعفسيا أو بغير وجه حق من شركة أو منظمة حكومية أو حتى مصرف ، وهم يملكون المعلومات اللازمة والمعرفة الكافية بخفايا هذه الجهة ، لذلك يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا بأس به. [1]

ب– الرغبة في إثبات الذات والتفوق على تعقيد وسائل التقنية : الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، إلى درجة أنه إزاء ظهور أي تقنية مستحدثة، فإن مرتكبي هذه الجرائم لديهم شغف الآلة فيحاولون إيجاد الوسيلة لتحطيمها، أو التفوق عليها، وليسوا على جانب كبير من الخطورة الإجرامية، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوافر لديهم أي نوايا سيئة. [2]

ج– الولع في جمع المعلومات وتعلمها : يرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألا يكون عليه أي قيد، فالقرصان يكرس جهده في تعلم كيفية اختراق المواقع الممنوعة وغالبا ما يكون القراصنة مجموعات يكون الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار.

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 42–43.

[2] بن مكي نجاة ، المرجع نفسه ، الصفحة 43.

كما يفضل القراصنة أن يكونوا مجهولين حتى يتمكنوا الاستمرار في الوجود داخل الأنظمة لأطول فترة ممكنة. [1]

د– ارتكاب الجرائم كوسيلة للتسلية والدعابة : يعتبر دافع المزاح والدعابة من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة من الملفات من جهاز شخص آخر. وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعابة، بل إن هذا التصرف في حقيقته جريمة إتلاف وتخريب متعمد في حالة ما إذا كان هناك قانون يجرم هذا الفعل.

2 – الدوافع المادية :

تعتبر الدوافع المادية من أهم البواعث على ارتكاب الجرائم المعلوماتية لما تحققه من ثراء فاحش حيث يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية أو الخسائر الضخمة من العاب القمار أو إدمان المخدرات وقد تكون جميع الوسائل بالنسبة إلى البعض مشروعة في مثل هذه الحالات فالغاية تبرر الوسيلة. [2]

فالطمع وحب الثراء السريع يدفع الفرد إلى القرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع غير المكلف بالإضافة إلى تحقيق أغراض معنوية مقصودة وذلك من خلال عمليات الجوسسة واختراق المواقع.

نتيجة تنوع اصناف الأشخاص مرتكبي الإجرام المعلوماتي، وما يتميزون به من معرفة وتقنية كافية للتلاعب بالحاسبات الآلية وفقا لهواهم أخذوا يشكلون خطرا على أنظمة الحاسب بما يشمله من معلومات وكذا على الحياة الخاصة للأفراد وأموالهم. [3]

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 43.

[2] بن مكي نجاة ، المرجع نفسه ، الصفحة 44.

[3] بن مكي نجاة ، المرجع السابق ، الصفحة 44.

هذه بصفة عامة أهم الصفات والدوافع الخاصة بالمجرم المعلوماتي، خاصة أنه لم تتضح الصورة جلية في شأن تحديد صفات مرتكي جرائم الحاسوب واستظهار سماتهم وضبط دوافعهم نظرا إلى قلة الدراسات الخاصة بالظاهرة برمتها من جهة ، ونظرا إلى صعوبة الإلمام بمداها الحقيقي ، بفعل عدم التبليغ عن جرائمها غير المكتشفة من جهة أخرى ، حيث يستخدم منتهكو القوانين الإمكانيات والأساليب المعلوماتية لارتكاب هذه الجرائم وكذا التهرب من المساءلة بالإضافة إلى كونها من الجرائم التي يكون فيها الاشتراك أو المساعدة ضرورية.

المبحث الثاني : أركان وأحكام الجريمة الالكترونية والإجراءات العامة

سبق وأن تطرقنا في بداية بحثنا إلى مفهوم الجريمة الالكترونية ولقد سلطنا الضوء تاليا إلى خصائصها وسماتها وكذا الدوافع الخاصة بها. سنعرض في هذا المبحث ، أركان الجريمة الالكترونية وأحكامها (المطلب الأول) و الإجراءات العامة هذه الأخيرة (المطلب الثاني).

المطلب الأول: أركان الجريمة الإلكترونية وأحكامها

الفرع الأول : أركان الجريمة الالكترونية

ونتناول في هذا الفرع أركان الجريمة الالكترونية الأساسية والمتمثلة في الركن الشرعي (أولا) والمتمثل في نصوص القانونية والركن المادي (ثانيا) والمتمثل في السلوكات المادية المجرمة والركن المعنوي (ثالثا) المتمثل في القصد الجنائي للجريمة الإلكترونية.

البند الأول: الركن الشرعي للجريمة الالكترونية

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان ، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه. [1]

القاعدة الأساسية الناتجة عن مبدء الشرعية وهي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون [2] وهذا ما نصت عليه المادة 1 من قانون العقوبات "*لا جريمة ولا عقوبة أو تدبير أمن بغير نص قانوني* ". [3]

ويتميز هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره تفسيرا ضيقا ، بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي

[1] أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط 10 ، 2011 ، الصفحة 27.

[2] أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط 2 ، 2006 ، الصفحة 78.

[3] مولود ديدان ، قانون العقوبات ، قانون رقم 09-01 المؤرخ في 25 فبراير 2009 ، د ط ، الصفحة 4.

الجنـائي إلى قياس فعل لم يرد نص بتجـريمه على فعل ورد نص بتجـريمه فيقـرر القـاضي الجنـائي للأول عقـوبة الثـاني للتشـابه بين الفعـلين. [1]

البند الثاني : الركن المادي للجريمة الالكترونية

لا بد من فعل أو إمتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لآخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر ، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها ، وهذا ما يدعو للتدخل التشريعي. [2]

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

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب (مثلا: جريمة الغش المعلوماتي : الركن المادي فيها هو تغيير الحقيقة في التسجيلات الالكترونية أو المحررا الالكترونية. [3]

---

[1] معتوق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة مكملة لنيل شهادة الماجستير وعلوم الجنائية ، 2011-2012 ، الصفحة 25.

[2] بن غدفة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها أعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29مارس 2017 ، الصفحة 48

[3] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الإلكترونية " ، طرابلس، بتاريخ 25-24 مارس 2017 ، الصفحة 118.

البند الثالث : الركن المعنوي للجريمة الالكترونية

تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم، والإرادة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو إرتكاب الجريمة.

يتكون الركن المعنوي للجريمة الالكترونية من عنصرين هما العلم والإرادة.

العلم : هو إدراك الفاعل للأمور.

أما الإرادة : فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا القصد الجنائي العام: هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود إرتكاب الفعل.

أما القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بإرتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة (مثال: في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه) وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الالكترونية ؟

الأصل إن الفاعل في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية يتوافر فيها القصد الجنائي الخاص (مثال: جرائم

تشويه السمعة عبر الأنترنت، وجرائم نشر الفيروسات عبر الشبكة). وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي. [1]

أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا، و المحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات تمحيصها بما لها من صلاحية بإعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها. [2]

الفرع الثاني : أحكام الجريمة الالكترونية

تشترك جميع صور الجريمة الالكترونية في أحكام مشتركة بينها فيما يتعلق بالشروع (أولا) والمساهمة الجنائية (ثانيا) والاتفاق الجنائي (ثالثا) والتي سنعرضها فيما يلي :

البند الأول: أحكام الشروع في الجريمة الالكترونية

يتنازع الشروع من حيث التعريف والتجريم مذهبين هما المذهب المادي الذي يشترط في الشروع أن يبدأ الجاني بارتكاب أحد الأفعال المكونة للركن المادي للجريمة ، ولا يعتد بما سبق من أفعال بحيث يدخلها أنصار هذا المذهب ضمن المرحلة التحضيرية للجريمة.

أما المذهب الثاني فهو المذهب الشخصي الذي يعتد بالنية الإجرامية ويعد شروعا وفقا لهذا المذهب ارتكاب الفاعل فعلا معينا بنية ارتكاب فعل لاحق له يؤدي إلى تحقيق النتيجة الإجرامية التي يستهدفها [3] وقد تناول المشرع الجزائري مسألة الشروع في المادة 30 من قانون العقوبات التي تنص على أن كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يكن بلوغ الهدف

[1] فضيلة عاقلي ، المرجع السابق ، الصفحة 120.

[2] لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها" دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن، 2016/08/13 ، ص 24.

[3] د. عبد القادر عميمر ، التحديات القانونية لإثبات الجريمة المعلوماتية ، النشر الجامعي الجديد ، تلمسان ، 2021 الصفحة 94-95.

المقصود بسبب ظرف مادي يجهله مرتكبها" والمادة الواحدة والثلاثين من قانون العقوبات التي تنص على أن: " *المحاولة في الجنح لا يعاقب عليها إلا بناء على نص صريح في القانون*... ".

فطبقا للمشرع الجزائري فإذا تجاوز الجاني مرحلة التحضير للجريمة يعتبر أنه قد بدأ في تنفيذها وبذلك يدخل في مرحلة جديدة تسمى الشروع، ويتحقق الشروع في حالتين: الحالة الأولى هي عدم تحقق النتيجة ويكون ذلك في الجريمة الخائبة والجريمة الموقوفة؛ أما الحالة الثانية فتكون عند تحقق النتيجة وانقطاع علاقة السببية بتدخل عامل غير مألوف بين النشاط والنتيجة أو وجود عامل غير متوقع في أثناء النشاط، وبالتالي فإن مرحلة الشروع هي المرحلة التي يتجاوز فيها الجاني مرحلتي التفكير والتحضير لارتكاب الجريمة، ولكن لا يصل إلى التنفيذ الكامل للجريمة، وبالتالي لا يعد شروعا مجرد العزم على ارتكاب الجريمة أو الأعمال التحضيرية لها أو محاولة ارتكابها.

أما في الجريمة المعلوماتية فقد نصت المادة الحادية عشر من اتفاقية بودابيست على الشروع في الجريمة المعلوماتية بالقول: " يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم وفقا لقانونه الداخلي ، كل شروع عمدي لارتكابه إحدى الجرائم المشار إليها في المواد 3-5-7-8-9 فقرة 1-أ ".

أما المشرع الجزائري فقد عاقب على الشروع في الجريمة المعلوماتية بمقتضى المادة 394 مكرر 7 من ق.ع.ج بالقول : " *يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هدا القسم بالعقوبة المقررة للجنحة ذاتها*". [1]

البند الثاني : أحكام المساهمة الجنائية في الجريمة الالكترونية

يقصد بالمساهمة الجنائية حالة تعدد الجناة الذين يساهمون في إبراز الجريمة وظهورها إلى الوجود [1] ومن ثم تكون هذه الأخيرة ثمرة لنشاط عدة أشخاص ، بمعنى أن الجريمة لم

[1] عبد القادر عميمر ، المرجع السابق، الصفحة 95-96.

ترتكب من طرف فرد واحد فقط وإنما ارتكبت من طرف عدة أشخاص لكل منهم دور قام به ومن هذا نستنتج أن المساهمة الجنائية تقوم على عنصرين وهما تعدد الجناة ووحدة الجريمة فإذا انتفى أحد هذين الركنين أو كلاهما تنتفي فكرة المساهمة الجنائية، وقد استخدمت عدة مصطلحات للدلالة على ذلك منها مصطلح المساهمة الجنائية، ومصطلح الاشتراك في الجريمة

وبالنظر إلى الدور الذي يلعبه المساهمون في الجريمة والذي يتفاوت من فاعل لآخر فإن ذلك أثار مشاكل قانونية في تحديد أثر هذا التفاوت، فالأصل أن يضطلع لشخص واحد أو عدة أشخاص بارتكاب كافة العناصر المكونة للنشاط الإجرامي يأخذوا فيها دورا أساسيا ويطلق عليهم في هذه الحالة وصف الفاعلين للجريمة رحيبها تعد المساهمة الجنائية مساهمة أصلية، كما قد يشترك آخرون في الوصول بهذا النشاط إلى غايته عن طريق القيام بدور ثانوي أو تبعي لا يدخل في التنفيذ المباشر الجريمة كالمساعدة مثلا، وحينها تأخذ المساهمة الجنائية في هذه الحالة صورة المساهمة التبعية، وفي حالة المساهمة الأصلية في الجريمة لا يطرح أي جدل نظرا لوجود أحكامها ، إلا أن الخلاف يطرح إذا تعلق الأمر بالمساهمة التبعية وهو ما المساهمة الأصلية نظرا للعلاقة القوية بينهما وهنا الحصر الخلاف في رأيين هما : مذهب يرى تعدد الجرائم بتعدد المساهمين، ومذهب يقرر وحدة الجريمة رغم تعدد المجرمين.

ولقد نظم المشرع الجزائري أحكام المساهمة الجنائية في المواد 41 إلى 46 من الفصل الأول من الباب الثاني من الكتاب الثاني من الجزء الأول من ق.ع.ج تحت عنوان " المساهمون في "الجريمة" فالمادة 41 المشار إليها أعلاه تعتبر كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكابها يعتبر فاعلا، فيما تعتبر المادة 42 من نفس القانون شريكا في الجريمة من لم يشترك اشتراكا مباشرا. [2]

[1] عبد القادر عميمر ، المرجع نفسه، الصفحة 96-97.

[2] عبد القادر عميمر ، المرجع السابق، الصفحة 98

البند الثالث : أحكام الاتفاق الجنائي على ارتكاب الجريمة الالكترونية

يقصد بالإتفاق انعقاد إرادتين للجناة أو أكثر على ارتكاب الجريمة، ويتكون لهذه الجريمة الركن المادي لهذه الجريمة من الاتفاق بين شخصين فأكثر على إرتكاب الجناية أو المنحة ويتحقق هذا الأمر من خلال قيام أحد المساهمين بالتعبير سواء بالقول أو بالكتابة أو بالإشارة أو بالإيحاء بحيث يصل التعبير إلى سائر المساهمين ويلقى قبولا لديهم فلا بد من قبول سائر المساهمين على نحو يمكن معه القول بوجود اتفاق، وهي من الجرائم العمدية التي يتعين أن يتوافر لقيامها القصد الجنائي لدى الجناة المتكون من عصرين وهما عنصر العلم بموضوع الاتفاق الذي يجب أن يشمل ماهية الفعل أو الأفعال المتفق عليها ومالها من خصائص يعتمد عليها الشارع في إسباغ الصفة الإجرامية على هذا الفعل. [1]

والعنصر الثاني هو الإرادة بمعنى أن تتجه إرادة الشخص إلى الدخول في الاتفاق ويصبح طرفا فيه، وأن يقوم بالدور المعهود به إليه فإذا لم تتجه الإرادة على هذا التحو يكون الشخص في هذه الحالة غير جاد هدفه مجرد استطلاع أمر أعضاء الاتفاق أو نه كان يريد العبث بهم فلا يتوافر القصد الجنائي لديه، ولا يشترط شكل معين هازلا . الاتفاق الجنائي كان يكون في شكل منظمة أو جمعية بل يكفي الإتفاق البسيط.

ولهذه الجريمة خصوصيات تتميز بها بحيث لا يتصور وجود الشروع في جريمة الاتفاق وذلك لأن الاتفاق حالة نفسية تتم بتلاقي الإرادات ولا تحتمل بداية ونهاية لهذه الجريمة إما أن تقع أو لا تقع ولا يتصور وجود بدء في التنفيذ كما يذهب في ذلك غالبية الفقه، وبالتالي فهي من الجرائم الشكلية، كما أن جريمة الاتفاق الجنائي تتعقد بمجرد الاتفاق على ارتكاب جناية أو جنحة وبالتالي فالعدول بعد هذا لا يعفي من العقوبة لأن الركن المادي لهذه الجريمة قد اكتمل. [2]

[1] عبد القادر عميمر ، المرجع السابق، الصفحة 99.

[2] عبد القادر عميمر ، المرجع نفسه، الصفحة 99-100.

المطلب الثاني : الإجراءات العامة لمتابعة الجريمة الالكترونية

إن الجريمة الالكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قوانين العقوبات والقوانين الأخرى ، فلذلك تتسع الجريمة الالكترونية بدعوى عمومية وهذه الدعوة تتم بمراحل وهي عمل دراستنا ، مرحلة جمع الأدلة (الفرع الأول) ومرحلة وسائل الاثبات (الفرع الثاني).

الفرع الأول : جمع الأدلة

إن هذه المرحلة من اختصاص ضباط الشرطة القضائية وهم نوعان النوع الأول : هم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات ، أما النوع الثاني : فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر هؤلاء المشار اليهم في المادة 21 من قانون الإجراءات الجزائية وسلطتهم كذلك محددة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني أو الأماكن المحاطة بأساور إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي وتعد محاصرتهم ذات حجية وقوة إثبات كما استقر عليه القضاء الوطني. [1]

البند الأول : المعاينة

هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

وتعتبر المعاينة إجراءا من إجراءات التحقيق التي تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها . كما يمكن للمحكمة أن تقوم بإجراءات معاينة إذا

[1] زبيحة زيدان ، المرجع السابق ، الصفحة 116-117.

رأت ذلك يستدعي لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناءا على طلب من الشخص المعني بعد موافقة القاضي المختص بناءا على طلب عريضة. [1]

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

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

ب- المسرح الافتراضي: يقع داخل البيئة الالكترونية ، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله. [2]

البند الثاني: التفتيش

إن التفتيش المنصب على منظومة المعلوماتية يختلف عن التفتيش المتعارف عليه ، في القواعد الإجرائية العامة من حيث الشروط الشكلية والوضعية وموضوع التفتيش.

على الرغم من أن المشرع الجزائري اعتبر التفتيش إجراء من إجراءات التحقيق وإحاطته بقواعد صارمة إلا أنه لم يورد تعريفا خاصا ودقيقا وقد إهتم الدستور الجزائري بعدم مساس بحرية الأشخاص وكرامتهم وأكد ذلك في المادة 40 منه بالقول : " *فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه ، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة*".

[1] عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006 ، الصفحة 84

[2] عائشة بن قارة مصطفى ، المرجع السابق ، الصفحة 85-86.

وفي الأخير أن التشريعات العربية تتفق على تعريف التفتيش بأنه إجراء من إجراءات التحقيق غايته ضبط الأدلة الجريمة موضوع التحقيق وكل مايفيد الحقيقة في شأنها. [1]

البند الثالث : الضبط

إن الضبط في قانون الإجراءات الجزائية هو وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها. [2]

إن الضبط في الجريمة الإلكترونية يختلف عن ضبط في الجرائم الأخرى من حيث المحل لأن الجريمة الإلكترونية يردالضبط على الأشياء ذات طبيعة معنوية وهي البيانات والمراسلات والإتصالات الإلكترونية من جعة ولها طبيعة مادية كالورق والكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرنة وأقراص الليزر البطاقات الممغنطة. [3]

الفرع الثاني : وسائل الاثبات

الاثبات هو إقامة الدليل على وقوع الجريمة ونسبتها إلى المتهم وذلك وفق طرق مشروعة ومحددة قانونا ، والإثبات في مجال الجرائم الالكترونية ينطبق عليه المفهوم العام للاثبات وتبعا لذلك فهو يواجه العديد من الإشكاليات بغية استخلاصه نظرا للخصوصيات المتعلقة بطبيعة الجريمة باعتبارخا غير مرئية ويسهل نحو آثارها ويصعب الوصول إلى أدلة إدانتها والسمات المتعلقة بخصوصية التحقيق في هذه الجرائم نظرا لصعوبة التحري في كشف غموضها.

سنعرض فيما يلي جملة من وسائل الاثبات والمتمثلة في الخبرة (أولا) ، الشهود (ثانيا) الاستجواب (ثالثا).

[1] زبيحة زيدان ، المرجع السابق ، الصفحة 130-131.

[2] عائشة بن قارة مصطفى ، المرجع السابق ، الصفحة 201.

[3] بوكثير خالد ، استئناف الأحكام القضائية الصادر عن هيئات القضاء الإداري في ظل التعديل الدستوري لسنة 2020 مذكرة لنيل شهادة الماستر في الحقوق ، جامعة عبد الرحمان ميرة ، بجاية ، 2021-2022 ، الصفحة 26.

البند الأول: الخبرة

لابد أن يكون الخبير صاحب مقدرة وإمكانيات العلمية والفنية في مسألة موضوع الخبرة ويستطيع القيام بدوره وللقيام بهذا الأخير عليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئتها والأثار الإقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية وكيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها. [1]

البند الثاني : الشهود

يطلق عليه اسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات فلذلك نجد أن الشاهد المعلوماتي ينحصر في عدة طوائف تتمثل في: مشغلة الحاسب الآلي ، خبراء البرمجة ، المحللون ، مهندسو الصيانة والإتصالات ، مديرو النظم. [2]

و للشاهد إلتزامات لا بد منالتقيد بها مثل : طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطبعها وتسليمها إلى سلطات التحقيق والإفصاح عن كلمات المرور السرية و الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة. [3]

البند الثالث : الاستجواب

والإستجواب ماهو إلا مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما ، وذلك قصد محاولة كشف الحقيقة وإستظهارها بالطرق القانونية.

---

[1] زبيحة زيدان ، المرجع السابق ، الصفحة 169.

[2] الأمر 04-14 ، المعدل والمتمم للأمر 26-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية العدد 71 المؤرخ في 10 نوفمبر 2004.

[3] بوكثير خالد ، المرجع السابق ، الصفحة 23.

أحالت التشريعات استجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الإستعانة بمحام أثناء الإستجواب وتمكينه من الإطلاع على ملف والإتصال به. [1]

خلاصة الفصل :

من خلال دراستنا لماهية الجريمة الالكترونية في الفصل ، نستخلص ما يلي :

- لم يتفق الفقهاء على تعريف جامعا مانعا للجريمة الإلكترونية.
- إن الجرائم المعلوماتية من أخطر الجرائم، فالشخص الذي يرتكبها هو مجرم غير تقليدي له مميزاته الخاصة، وهي جرائم يصعب اكتشافها وإذا ما اكتشفت يصعب إثباتها، وما يزيد من خطورة هذه الجرائم أن للضحية دور مهم فيها.
- تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.
- قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.
- بشكل عام، فإن استخدام وسائل الإثبات الإلكترونية في إثبات الجرائم الإلكترونية يعتمد على التكنولوجيا والتقنيات المتاحة والقانون الذي يحكم الدولة.

[1] بوكثير خالد ، المرجع نفسه ، الصفحة 24.

الفصل الثاني :

التحديات القانونية لمكافحة الجريمة الالكترونية

تعد الجرائم الالكترونية ذات طابع عالمي فهي جرائم عابرة للحدود كما أنها تترك أثرا ماديا في مسرح الجريمة، وهناك العديد من الأليات والإجراءات المعمول بها لقمع الجريمة المعلوماتية على المستوه الوطني والدولى لما تشكله من خطر على أمن الدولة والأفراد والمصالح الخاصة . ولقد خصصنا هذا الفصل لآليات مكافحة الجريمة الإلكترونية من خلال عرضنا الآتي:

المبحث الأول : الآليات والسبل للحد من الجريمة الإلكترونية على المستوى الدولي

أضحت الجرائم الإلكترونية كإحدى الجرائم المعلوماتية في العصر الراهن التي رافقت عمر التقدم التكنولوجي، خاصة بعد ظهور شبكة المعلومات الدولية. بسبب تقدم العلمي من خلاله ساعد على انتشار وتنوع السلوك الإجرامي الذي أصبح يهدد الأفراد في مختلف المجالات، فأصبح اهتمام بعض الدول والمنظمات الدولية للبحث عن الثغرات لمكافحة الجريمة الإلكترونية.

ومن هنا ستحاول عرض في هذا المبحث الجهود الدولية والعربية لمكافحة الجريمة.

المطلب الأول : الجهود الدولية لمكافة الجريمة الالكترونية

توجد العديد من الهيئات والمنظمات تلعب دورها ما في إبرام اتفاقيات في محاولة اقامة تعاون دولى لتحقيق أهداف مجتمع دولى ويردع من مقرها الجرائم. سنتطرق في هذا المطلب إلى التعاون الدولى وجهود المبذولة لمكافحة الجريمة المعلوماتية من خلال فروع.

الفرع الأول : التعاون الدولي

إن التعاون الدولي في المسائل الجنائية وفقا للإلتزامات الدولية والقوانين الوطنية هو حجز الزاوية في الجهود التي تبذلها الدول لمنع الجريمة، لا سيما في أشكالها عبر الوطن

مثل جرائم المعلومات، ومحاكمة ومعاقبة مرتكبيها، ويشجع دول العالم على مواصلة وتعزيز هذه الأنشطة على جميع المستويات. [1]

التعاون القضائي:

تتطلب إجراءات التحقيق في الجرائم الإلكترونية وملاحقتها تتبع النشاط الإجرامي ى والأمر الذي يسلزم نقص أثار الجريمة من مصدرها إلى نهاية تنفيذها وتحديد مواقع الضرر الذي تسببت فيه الجريمة. هناك نوع من التعاون بين السلطات القضائية فى هذه الدول من أجل توسيع نطاق الاختصاص. وستعرض أهم صورتين فى مجال التعاون القضائي.

البند الأول : التعاون الأمني

من الواضح أن الحدود الجغرافية ومشكلة الاقتصاص الإقليمي نفق حاجر أمام الإجراءات الجنائية لمعالجة مرتكبي الجرائم، وخاصة في جرائم الأنترنت والتي تتميز بأنها جريمة عابرة للحدود. و الحاجة الماسة إلى توحيد الجهود فيما يتعلق بتبادل البيانات والمعلومات المتعلقة بالجريمة التي تتيح الكشف عن هوية المجرمين ، حيث يستحيل على الدولة وحدها القضاء على هذه الجريمة. [2]

فأجهزة الشرطة لا يمكنها تعقي مرتكبي الجرائم وملاحقتها إلا من نطاق حدودها أي أنه من أنه من فر المجرم خارج حدود الدولة فإنه يبقى في مأمن من المتابعة ونجد في هذا الإطار أن هناك ثلاثة أوجه الإقامة هذا التعاون :

أولا/ انشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الأنترنت ونشرها قصد فها هي تنمية التعاون بين سلطات الدول القضائية في مجال مكافحة الجريمة وملاحقة المجرمين بإضافة إلى تقديم المعونة وتبادل الخبرات عند الاقتضاء .

[1] د.مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات ط 1439هـ – 2018 م دار الجلدونية الجزائر جانفي 2018 ، الصفحة 263.

[2] قزران مصطفى، زرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المركز الجامعي، أفلو.المركز الجامعي في تمثيل.المجلد الثامن ، العدد 02 ، تاريخ النشر 2022/06/16 , ص 1225.

ثانيا / التعاون في إطار المنظمة الدولية للشرطة الجنائية الأنتربول: وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة فى الدول الأطراف بطرق فعالية في مكافحة الجريمة من خلال جمع البيانات والمعلومات المتعلقة بالجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أراضي الدولة. المنظمة إليها و تبادل فيما بينها بالإضافة ان التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في دول الأطراف.

ثالثا / القيام بعمليات أمنية مشتركة : عندما يتم تعقب الجريمة المعلوماتية، يتم تتبع الأدلة الرقمية ومصادرتها و يتم إجراء عمليات التفتيش عبر الحدود بواسطة أجهزة إعلام الآلي والأنظمة المعلوماتية وشبكات الاتصالات بحثا عن الأدلة والبراهين وكل هذه الإجراءات تتطلب تعاونا دوليا. [1]

البند الثاني : المساعدات القضائية بوجه عام

المقصود بالمساعدة القضائية الدولية هو كل إجراء قضائي تتخذه دولة ما من شأنه تسهيل عملية المتابعة والمحاكمة الجزائية في بلد ما فيما يتعلق بجريمة ما . وبناء على هذا التعريف, تظهر الحاجة الملحة للمساعدة القضائية الدولية في عملية مكافحة الجرائم بوجه عام والجريمة الإلكترونية بوجه خاص. [2]

وتتخذ المساعدة القضائية صور نذكر منها:

أولا: التبادل المعلومات ، يتم ذلك عن طريق تبادل البيانات و الوثائق والمواد الإستدلالية التي تطلبها سلطة قضائية أجنبية أثناء قيامها بعملية التحقيق في الجريمة التي يتم فيها رفع دعوى ضد أحد رعاياها أو مواطني دولة أخرى ، والتي يشمل تبادل السوابق القضائية لأتباع

[1] قزران مصطفى، زرقين عبد القادر، المرجع السابق ، الصفحة 1226.

[2] براهيمي جمال (التحقيق الجنائي في الجرائم الإلكترونية)، أطروحة لنيل شهادة الدكتواه في العلوم ، جامعة مولود معمري – تيزي وزو كلية الحقوق والعلوم السياسية 2018/06/27, الصفحة 314 – 315.

مثل هذه الجرائم وتجد عد ائم ونجد عدة تطبيقات لهذه الصورة وورد فى الفقرات 3 و4 من المادة الثامنة من اتفاقية الأمم المتحدة. لمكافحة الجريمة المنظمة عبر الوطنية. [1]

ثانيا: نقل الإجراءات :نعني أن قيام دولة ما بناء على اتفاقية أو معاهدة تتخذ إجراءات جنائية أثناء قيامها بعملية ارتكابات جريمة فى أراضي دولة أخرى ولصالح هذا البلد عند استفاء شروط معينة من أهمها التجريم المزدوج ويعنى أن الفعل المنسوب إلى شخص يشكل جريمة في البلد الطالبة، والدولة المطلوبة إليها نقل الإجراءات.

وبالاضافة الى شرعية الإجراءات المطلوبية اتخادها ، بمعنى أن الإجراءات الواجب إتخادها مقررة فى قانون الدولة المطلوب منها من نفس الجريمة ، كما أن أحد الشروط التي يجب استفاؤها هو أن الإجراءات المطلوب اتخادها مهمة جدا بحيث تلعب دوراً مهما في الوصول إلى الحقيقة. [2]

ثالثا: الإنابة القضائية الدولية، يقصد بالإنابة القضائية الدولية طلب اتخاذ إجراء قضائى من اجراءات الدعوى الجنائية ، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة ويتعذر عليها القيام بنفسها.

فالإنابة القضائية تعبر عن قيام دولة ما لمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمة لدولة أخرى نيابة عنها، بناء على طلب تلك الدولة المناب عنها ، ووفقا لما تقرره بنود الإتفاقية الدولية بين الدولتين في هذا الشأن.

[1] قزران مصطفى، زرقين عبد القادر، المرجع السابق ، الصفحة 1227

[2] مناصرة يوسف ، المرجع السابق ، الصفحة 312 – 313.

وهدفها هو نقل الإجراءات الجنائية لمواجعة التطور الحاصل في الظواهر الإجرامية وتذليل العقبات التى تعترض سير الإجراءات الجنائية المتعلقة بالقضايا التي تتجاوز الحدود الوطنية. [1]

رابعا: تعليم المجرمين : حيث يعتبر من صور المساعدة القضائية الدولية المتياد لة فى تسليم المجرمين، والمقصود بالتسليم هو تخلي الدولة عن أي شخص موجود على أراضيها إلى دولة أخرى تتم ملاحقته أو الحكم عليه فيها، وبناء على طلب الدولة وينطبق على هذا المفهوم كل من عبارات تسليم المجرمين ، الإسترداد أو نقل الأشخاص.

وتستخدم معظم الشريعات الثنائية والمتعددة الأطراف والاتفاقيات القضائية عبارة التسليم والاسترداد لأن كل واحدة تهدف الى نفس المعنى ، أما فيما يتعلق ينقل الأشخاص فهو يستخدم في مجال المحكوم عليهم لتنفيذ الأحكام الصادرة بحقهم.

فإن التسليم أو الإسترداد نجد أساسه القانوني في التشريعات الداخلية والإتفاقيات الثنائية والمتعددة الأطراف التي تنظم القواعد المتعاقدة بشأن تبادل المجرمين سواء كانوا في طور الملاحقة أو المحكومين . بحيث تطبق الإتفاقية التي تعلو عى القانون من حيث التطبق. [2]

الفرع الثاني : الاختصاص القضائي الدولى والداخلي.

البند الأول: الاختصاص القضائي الدولي

تثار مشكلة الاختصاص القضائي الدولي فيما يتعلق بالجرائم المرتكية في نطاق المعلوماتية إلى حد أكبر مما هي عليه على مستوى إقليم دولة واحدة، حيث يمكن للدولة وضع حد للمشكلة على مستوى الوطني أو المحلي، من خلال النصوص القانونية التي يمكن

[1] خراشي عادل عبد العال إبراهيم ، إشكاليات التعاون الدولى في مكافحة الجرائم المعلوماتية د,ط ، دار الجامعة الجديدة ، الإسكندرية ، سنة 2015 ، الصفحة 209 – 210.

[2] برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية مجلة البحائر للدراسات القانونية والإقتصادية جامعة جيلا لي ليابس سيدي بلعباس، الجزائر، المجلد 01 ، العدد 01 ،2021/03/25 ، الصفحة 97.

الموافقة عليها في هذه الدولة أوتلك, لأن الجريمة محصورة فى النطاق الإقليمي للدولة ومعالجتها مرتبطة بكل دولة على حدى ، على عكس مشكلة الاختصاص على المستوى الدولى لأن الجريمة في الأخير لا ترتبط بالحدود الإقليمية لدولة ما بل بالعكس هي جريمة عابرة للحدود, بإضافة إلى اختلاف التشريعات والأنظمة القانونية من دولة إلى دولة أخرى في مواجهة هذه الجرائم، وقد يحدث أن الجريمة ارتكبت فى إقليم دولة معينة من قبل أجنبي ، وفى هذه الحالة تخضع الجريمة للإختصاص الجنائي للدولة الأولى على أساس مبدأ الإقليمية، وتخضع أيضا لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكونا هذه الجريمة احدى الجرائم التي تهدد أمن وسلامة دولة أخرى، ثم تتدخل في اختصاصها بناء على مبدأ العينة.

البند الثاني : الاختصاصية الفضائي الداخلي

يطلق على هذا النوع من الاختصاص القضائي بالإختصاص الإقليمي أو الداخلي ، نظراً لأن القضاء الوطني هو المختص بالفصل في القضايا الجزائية، ويستند إلى تحديد إطار الجغرافي ، أو دائرة الاختصاص مكاني في منطقة معينة من أراضي الدولة، ويستند هذا التقسيم إلى ثلاث معابر هي : مكان وقوع الجريمة، أو مكان الإقامة المتهم ، أو مكان القبض على المتهم. [1]

وبهذا الخصوص تحت المادة 37 ق.إ.ج.ج يقولها (يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في ، مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حي ولو حصل هذا القبض لسبب آخر.

[1] فايز محمد راجح غلاب ، (الجرائم المعلوماتية في القانون الجزائر اليمني) ، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية جامعة الجزائر كلية الحقوق , سنة المناقشة 2009 / 2010 الصفحة 374 و379

وكما نصت المادة 329 ق إ ج ح : "*تختص محليا بالنظر في الجنحة محكمة محل الجريمة ، أو محل إقامة أحد المتهمين أو شركائهم ، أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبا آخر*". [1]

ومن خلال النصين السابقين يتضح أن الاختصاص القضائي يتطلب توافر حالة من الحالات الثلاثة التالية:

1/ أن تكون الجريمة قد أركيت في مجملها، أو أن أحد عناصرها مادي، أو تم تحقيق شكل من أشكال الاستمرارية للجريمة المستمرة، أو أي فعل اعتيادي أو متسلسل فيما يتعلق بالجريمة المركبة فعل من أعمال الشروع في التنفيذ فى منطقة الإختصاص المكاني لعضو النيابية العامة أو قاضي التحقية

2/ أن تكون إقامة المتهم أو المثنية به، أو إقامة أحد المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، ويتحدد مكان الإقامة بوقت إيتيان الجريمة.

3/ أن يكون قد ألقى القبض على أحد المتهمين أو المشبة بهم في نطاق تلك الدائرة .

وقد مدد المشرع الجزائري الاختصاص القضائي بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وغيرها من الجرائم [2] مما نصت المادة (37) و المادة (80) والمادة (329) ق.إ.ج.ج.

حيث نصت المادة (37 – 2) على أنه : " يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى ، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتسريع الخاص بالصرف".

[1] أنظرالمادة 37ق1 والمادة 329 من الأمر رقم 04 – 14 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 71 ، المؤرخ في 10 نوفمبر 2004.

[2] فايز محمد راجح غلاب ، المرجع السابق، ص 375 376.

كما نصت المادة (80) على: " يجوز لقاضي التحقيق أن ينتقل صحبة كاتبه بعد إخطار وكيل الجمهورية بمحكمته إلى دوائر اختصاص المعالم المجاورة للدوائر التي يباشر فيها و ظيفته للقيام بجميع إجراءات التحقيق إذا ما أستلزمت ضرورات التحقيق أن يقوم بذلك وعلى أن يخطر مقدم وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها وينوه في محضره إلى الأسباب التي دعت إلى انتقاله".

وكذلك تحت المادة (329-5) على: " بحور تحديد الاختصاص المحلي للمحكمة إلى الدائرة اختصاص محاكم أخرى عن طريق تنظيم ، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية. للمعطيات وجرائم شبييض الأموال والإرهاب الجرائم المتعلقة بالشريع الخاص بالصرف". [1]

وعليه فإن المشرع الجزائري قد حسم مشكلة تنازع الإختصاص بين السلطات القضائية المتواجدة فى إقليم الدولة ، وهو اختصاص يتم تحديده بـ:

1/ بنطاق ضرورة التحقيق حيث أجازت المادة (80) ق.إ.ج.ج لقاضي التحقيق أن يقوم بكل إجراءات التحقيق في نطاق الإختصاص المحاكم المجاورة لنصاق اختصاصته وفق شروط:

- أن تكون هناك ضرورة للانتقال خارج نطاق اختصاصه المكاني.
- أن يُخطر وكيل الجمهورية الذي يعمل فى نفس الدائرة اختصاصه
- اخطار وكيل الجمهورية فى نطاق الإختصاص الدعائم التمديد اليه
- تحديد الأسباب التى جعلته يمدد دائرة اختصاصه المكانية فى محضر المعانية

2/ كما يتم تمديد الاختصاص وفقا للقضايا الأخرى التي تشمل جرائم معينة تشكل تهديد أكبير الأمن المجتمع، بما فى ذلك الجرائم التي تؤثر على أنظمة معالجة البيانات الآلية ، حتي يتمكن وكيل الجمهورية من توسيع نطاق اختصاصه المحلى إلى اختصاص المحاكم

[1] أنظر المادة 37 ف 2 و 80 والمادة 329 ف 5 من قانون 04 – 14 المتضمت قانون الإجراءات الجزائية، المرجع السابق.

الأخرى ، ويمكن تقاضي التحقيق إجراء أي تفتيش أو حجز على امتداد الأراضى الوطنية، ويسكن أيضا توسيح اختصاص المحكمة ليشمل اختصاص المحاكم الأخرى. [1]

الفرع الثالث: الجهود الأمم المتحدة والأوربية لمكافحة الجريمة

البند الأول: جهود الأمم المتحدة لمكافحة الجريمة الإلكترونية :

تبذل الأمم المتحدة جهوداً كبيرة فى مجال مواجعة الجرائم المعلوماتية ، وتؤكد على ضرورة تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وثفاقم آثارها [2] ، أصدرت منظمة الأمم المتحدة فى مؤتمرها الثامن لمنع الجريمة ومعاملة المجرمين قراراً بشأن الجرائم المتصلبة بالحاسوب وتبين من هذا القرار أن إجراء الدولى لمكافحة الجرائم المعلوماتية يتطلب من الدول الأعضاء إتحاد إجراءات وتتلخص في :

– تحديث القوانين والأغراض الجنانية الخاصة بها، بما في ذلك الإجراءات المتخدة لضمان إجراء التعديلات ويتم تطبيق القوانين الجنائية الراهنة (التحقيقاً ، قبول ، الأدلة) بالشكل المناسب إذا دعت الضرورة.

– مصادرة العائدات من الأنشطة غير مشروعة .

– إتحاد الإجراءات الأمنية والوقائية مع مراعاة خصوصية الأفراد و احترام حقوق الإنسان.

– حماية مصالح الدولة وحقوق ضحايا جرائم المعلوماتية وكذال التعاون مع المنظماتالمهتمة بموضوع جرائم الأنترنات, وتدريس الآداب المتبعة في أستخدام الحاسوب ضمن المناهج المدرسية.

فتزايد الجرائم المرتكبة عبر الأنترنت و المشكلات التى تثيرها أدى إلى قيام الأمم المتحدة بإبرام اتفاقية الخاصة بمكافحة إساءة استخدام التكنولوجيا للأغراض الإجرامية في عام 2000، حيث أكدت على ضرورة تعزيز التكنولوجيا التنسيق والتعاون بين الدول، وكذلك

[1] فايز محمد راجح غلاب ، المرجع السابق، الصفحة 377 ، 378.

[2] د. فاروق خلف (الآليات القانونية لمكافحة الجريمة المعلوماتية)، مجلة الحقوق والحريات كلية الحقوق جامعة حمة لحضر الوادي ، العدد الثاني , 2015, الصفحة 11.

تم عقد منظمة الأمم المتحده المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل أيام 12 ، 19 أفريل 2010, وبناء على ذلك ناقشت في دول الأعضاء بعض التطورات الحديثة في استخدام العلم والتكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحة جرائم الحاسوب. [1]

البند الثاني: جهود الأوروبية لمكافحة الجريمة الإلكترونية

تشكل الجرائم المعلوماتية مصدر قلق كبير للدول الكبيرة وتمثل تحديا جديدا للمجتمع الدولي, خاصة في ظل التطور السريع والمتعاقب والذي يصاحبه تطور سريع فى هذه الجرائم فتعددت الجهود المبذولة المواجهة هذه الجرائم سواء كانت من طرف منظمة التعاون الإقتصادي والتنمية أو من طرف المجلس الأوروبي.

أولا : منظمة التعاون الاقتصادي والتنمية

اهتمت منظمة التعاون الاقتصاديا و التنمية بالمشكلات التى أثارها ظهور نظم المعلومات في الحياة الاقتصادية عام 1977 ، وقد بدأ هذا الاهتمام في البداية يميل إلى حماية الخصوصية من التهديد المعلوماتي لها ، وهذا الإهتمام أنتج قواعد ارشادية وتوصيات للدول الأعضاء فى تشريعها الوطنية . حيث نصت على عقوبة جنائية في حالة مخالفة هذه الإرشادات والتوصيات ، فهذه التوصيات والتعليمات تتعلق بحماية الأدلة ذات طابع شخصى (البينات الشخصية) ، وتتمثل هذه القواعد والإرشادات في :

- تحديد الهدف الذي يتم جمع البينات من أجليه.
- يجب مراعاة القواعد الشكلية للمحافظة على البيانات.
- الإنفتاح وهذا يتطلب أن يكون على ما يتعلق بالحياة الشخصية، من حيث السياسة العامة للتطوير والتخطيط والتنفيد ويكون متاحا للجميع معرفتها .

[1] بن علية بن جدو ، (تحديات الأمن السيبراني المواجهة الجريمة الإلكترونية)، المجلة الجزائرية للأمن الإنساني، جامعة بومرداس ، المجلد 07 ، العدد 02 ، تاريخ 03/01/ 2022، الصفحة 308 – 309.

– المشاركة الفردية تتطلب أن يكون للناس حق فى الوصول إلى بياناتهم و معرفتها و الحق في الرد عليها.

فهذه القواعد لا تعد إلزامية بل هي إرشادات و توصيات فقط، وتغطي على الأشخاص العادين وتطبق أيضا عل القطاع العام والخاص وتتعلق المعالجة آليا.

وبداية من عام 1983 بدأت المنظمة بإهتمام بجرائم المعلوماتية من خلال اجتماعات مؤتمرات للبحث عن هذه الظاهرة الإجرامية وفي 1985 تم تشكيل لجنة الدراسة الجريمة المعلومائية من خلال إجراء مسح لهذه الجريمة لكل دول أعضاء المنظمة ، وفي 1986 تم صدور تقرير بعنوان جرائم الحاسب الآلي وأوصينا اللجنة في تقريرها بعد تحليل للنظم القانونية بالدول الأعضاء بضرورة مراجعه المشكلات الناجمة عن الجرائم الالكترونية فى قوانيتها الداخلية . وبعد ذلك اتجهت المنظمة إلى الإهتمام بحماية أنظمة وشبكات المعلوماتية وذلك بإصدار التوصيات الخاصة بالتدابير و الإجراءات المفروضة على أعضاء لحماية أنظمة المعلومات. [1]

ثانيا : جهود المجلس الأوروبي في مكافحة الجريمة الإلكترونية : (المعاهدة الأروبية):

حيث وقعت اللجنة الخاصة بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية للمعاهدة وهدفها مساعدة الدول في مكافحة الجرائم الإلكترونية وبعد إتمام المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدات ومنها المعنية ، يستلزم منها سن القوانين الضرورية بالحد الأدنى لتعامل مع جرائم التقنية العالمية بما في ذلك الدخول الغير المصرح به وتلاعب بالبيانات و الاحتيال والتزوير التي لها علاقة بالكمبيوتر.

وتضمنت المعاهدة والتي تم تعديلها 27 مرة قبل الموافقة عليها، حيث تتكفل الحكومات بحق المراقبة وتلزم الدول بمساعدة بعضها في جمع الأدلة وفرض القانون

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 117 – 119.

فصلحيات الدولية الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومة من استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يسوء استخدامها. [1]

الفرع الرابع: أهم الإتفاقيات والمنظمات المواجهة الجرائم المعلوماتية

البند الأول: اتفاقية بودابست : هي من أبرز الاتفاقيات الدولية التي أبرمت لمكافحة الجريمة الالكترونية ووقعت في العاصمة بودابست في عام والمعروفة بإتفاقية الدولية لمكافحة الإجرام عبر الأنترنت حيث تتكون الإتفاقية من ديباجة وثماني وأربعون مادة موزعة على أربعة فصول:

الأول : يعالج استخدام ستخدام المصطلحات، أما الثاني. يعين الإجراءات الواجب إتخادها على مستوى الوطني ، و الفصل الثالث. يتضمن التعاون الدولى ، والفصل الرابع يحدد الأحكام الختامية. [2]

فالهدف من الإتفاقية هو السعى لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للإتفاقية، وتم تأكيد على التعاون الإقليمي و الدولى في مواجهة الجرائم الكمبيوتر وايجاد دليل للتدابير التشريعية الوطنية. وتهدف أيضا تحقيق التوازن بين حماية حقوق الإنسان الأساسية (المعترف بها بموجب اتفاقية مجلس أوربا لحماية حقوق الإنسان 1950 والاتفافية العالمية الأخرى في ميدان حقوق الإنسان) و تحديد الحقوق المتصلة بالرأي وحرية الوصول للمعلومات وحرية البحث والتنقل للمعلومات والأفكار. [3]

[1] جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات ، دج، الطبعة الأولى ، دار البداية ناشرون وموزعون ، عمان 2010 ، الصفحة 228 – 229

[2] أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الإلكترونية، دج، دط، دار الجامعة الجديدة ، الإسكندرية، سنة 2015 الصفحة 98.

[3] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت ، دج، الطبعة الأولى، منشورات الحلبي الحقوقية ، لبنان 2007 ، الصفحة 126 – 127.

البند الثاني : إتفاقية برن لحماية المصنفات الأدبية والفنية .

في القرن التاسع عشر بدأ الحديث عن الإيطار التشريعي لقوانين الملكية الفكرية بصفة عامة، وعندما اشتدت الحركة الدولية التي تطالب بحماية حقوق الملكية القدرية فتم عقد معاهدة برن بسوسرا في 9 سبتمبر 1886 والمكملة بباريس في 4 ماي 1896 والمعدلة ببرلين في 13 نوفمبر 1908 ، والمكملة ببرن في 20 مارس 1914 والمعدلة بروما فى 2 جوان 1971 والمعدلة في 28 سبتمبر 1979 – حيث أقرت الإتفاقية لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية والعلمية أيا كانت طريقة التعبير عنها

و بموجب مرسوم رئاسي رقم 97 – 341 المؤرخ في 13 سبعمر 1997 انضمت الجزائر بتحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية فإنها تعتبر البحر الأساسى فى مجال الحماية الدولية لحق المؤلف

و يستلزم من أعضاء الإتفاقية توفير الحد الادني لحماية حقوق المؤلف لفترة زمنية، ويستنتج أن اتفاقية برن هي أول اتفاقية عالمية وضعت مبادئ عامة لحقوق الملكية الفكرية وكذا اهتمامها بالقواعد الموضوعية وتعتمدها كل الاتفاقيات اللاحقة كمرجع ، ولكن من الجانب الآخر لم تتطرق الى حماية برامج الحاسب الآلي بصورة مباشرة ولكن هذا لا يعنى عدم الحاجة إلى إتفاقيات أخرى تعنى أكثر بيرامج الحاسوب وتخضعها للتنظيم وهذا ما حاول الجهد الدولي بلوغه. [1]

البند الثالث : جهود منظمة الانتربول Interpol :

أنشأت منظمة الأنتربول نظاما خاصا للتعاون ، ويعتبر نظام وطني والمرجعية المركزية، ويوجد فى كل دولة من الدول الأعضاء فى منظمة الأنثربول مكتب مركزي وطني يمثل نقطة الاتصال مع الإدارات الأجنبية التى تجرى تحقيقات خارج حدودها.

[1] بن مكي نجاة ، المرجع السابق، الصفحة 96/92/91.

وتضم شبكة من المحققين العاملين فى الوحدات الوطنية المعنية بالجرائم لإجراء الاتصالات الميدانية بين الدول الأعضاء والاسع فيه قدر الامكان ، و من مهام هذا النظام تطوير الإستراتيجيات والمعلومات المتعلقة بأحداث الأساليب الإجرامية فى مجال جرائم تقنية المعلومات.

كما قامت المنظمة بوضع برنامج خاص لمكافحة الإجرام المعلوماتي يتركيز على التدريب والعمليات ويعمل عل مواكبة التهديدات ويهدف هذا البرنامج إلى :

- تقديم دورات تدريبية لوضع معايير معينة والتزام بها.
- تنسيق ودعم العمليات الدولية .
- مساعدة الدول الأعضاء على التحقيق في الهجمات أو الجرائم الالكترونية من خلال تقديم خدمات في مجال التحقيق وقواعد البيانات
- تحديد التهديدات وتبادل المعلومات الاستخبار فى هذا المجال مع دول الأعضاء.
- إنشاء بوابة آمنة على شكبة الأنترنت لنشر المعلومات والوثائق العملياتية. [1]

البند الرابع: جهود الاتحاد الافريقي ومجموعة الدول الثمانية G8:

أولا : جهود الاتحاد الافريقي :

قام الاتحاد الافريقى بطلب انعقاد مؤتمر استثنائي لوزارة الاتحاد الأفريقى المسؤولة عن تكتولوجيا المعلومات والإتصالات، الذي أنعقد في جنوب افريقيا فى فترة 02 إلى 05 نوفمبر 2009,من مفوضية الاتحاد الإفريقي باشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا لإعداد اتفاقية حلول التشريع القضائي القائمة على حاجيات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية، وأوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر قيمة بالنسبة للمجتمع مما يجعل سن التشريعات ضذ الجريمة الإلكترونية في جوان 2014 ، حيث اجتمع

[1] مراد مشوس، الجهود الدولية لمكافحة الإجرام السيبراني ، مجلة الواحات للبحوث والدراسات جامعة غرداية ، العدد 02 20/ 12/ 2019 ، دون ترقيم.

مجموعة من القادة الاتحاد الإفريقى مكون من 54 حكومة افريقة ووافقوا اعلى اتفاقية الاتحاد الافريقى فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.

ثانيا : جهود مجموعة الدول الثماني "G8":

تبنت وزارة العدل والداخلية لبلدان الثمانية فى اجتماعهم المختلفة سياسات لمكافحة العديد من الجرائم الالكرونية على أساس المبادئ التالية:

وهي عدم توفير الملاذ الآمن المعتدى على تقنية المعلومات والتنسيق بين جميع الدول المعنية في ملاحقة ومقاضات مرتكبي الجرائم الإلكترونية وتدريب العاملين فى مجال تنفيد القانون وتجهيزهم بالمعدات اللازمة للتعامل مع الجرائم التكنولوجيا العاليه, وعليه دعت الدول الثامنية المواصلة العمل للوصول إلى حلول دوليه ناجحة و من خلال عقد اتفاقية دولية, ومن توصيات "G8" بالنسية للجرائم الالكترونية موجودة فى إطار الباب "D"من معاهدة وتتلخص في:

وجب على الدول أن تجرم الانتهاكات على حقوق الغير على شبكة العنكبوتية التي يستوجب فرض عقوبات جزائية التي تعالج مشاكل المتعلقة بالتحقيقات القضائية لمنع الجريمة وإقامة تعاون دولى يتعلق بمكافحة هذه الإنتهاكات و اتحاد خطوات لمنع الجريمة ذات التقنية عالية. [1]

وجدير بالذكر فقد تطرقت سابقا إلى جهود منظمة التعاون الاقتصادي والتنمية فهي أيضا اهتمت بالمجال الجرائم المعلوماتية وحاولت تصدي لها من خلال قواعد و ارشادات.

[1] فاروق خلف ، المرجع السابق ، الصفحة 13-14.

المطلب الثاني الجهود العربية المبذولة لمواجهة الجريمة الالكترونية:

انتشرت الجريمة الالكترونية في المنطقة العربية كما انتشرت في بقية العالم و فى ظل غياب أطر قانونية واضحة وشاملة تضمنت مكافحة الجرائم المتعلقة بحماية المعاملات الالكترونية فبادرت العديد من الدول العربية إلى تبني تشريعاك لمكافحة الجرائم المعلوماتية ، ومن هذا المنطلق فقد تطرقنا إلى :

الفرع الأول: مكافحة الجريمة الالكترونية على مستوى الدول العربية

إن أبرز ما يمكن قوله من الجهود العربية المبذولة للحماية من جرائم المعلوماتيك وهو اعتماد قانون الجزائر العربي الموحد كقانون نموذجي بموجب قرار رقم 229 لسنة 1996، حيث صدرفيه النموذج العربي أو القانون الاسترشادي في موضوع المكافحة الجرائم المعلومات تتجه العمل المشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن اتضح أن كلاهما قدم مشروعا بهذا الشأن وبالفعل تم اجتماعهما المشترك فى 21 – 21 / 05 / 2003 فتم النظر فى المسودتين اللتين تم إعدادهما في إطار الغرفتين، وتم إعداد مشروع قانون مشترك ثم عرضه على المجلسين في الجلسة العادية لكل منهما حيث تمت الموافقة عليه. بعد الموافقة على هذا المشروع لايوجد أي عذر لأي مشروع عربي للتقاعس عن الشروع فى إصدار تشريعات وطنية تتضمن مواجعة الجرائم المعلوماتية التى تجد تطبيقها في جميع أنحاء العالم وفى أي دولة بغض النظر عن تصنيفها من حيث الاستخدام الحاسوب و الأنترنت ومهما كانت درجة تقييمها. [1]

وبالرجوع إلى المذكرة الايضاحية لهذا القانون و مراجعة الفصل السابع الخاص بالجرائم ضد الأشخاص تجد أن هذا القانون قد تضمن فعلا فاها بالاعتداء على حقوق الأشخاص الناتجة عن معالجة المعلومات وذلك في المواد (461 461) وأشارت المواد

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 130-131.

(من 461 إلى 463) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآليه وكيفية جمع المعلومات والاطلاع عليها . أما المادة (464) نصت على عقاب كل من يقوم بفعل الدخول عن طريق الغش إلى أنظمة المعلوماتية وعرقلتها وتغير المعلومات داخل النظام، وتزوير الوثائق المعالجة الآلية، وسرقة المعلومات.

وتحدث جرائم المعلومات بجميع أشكالها وتتراوح من جرائم الاحتيال الحاسب الآلي من خلال اختراقها وسرقة المعلومات المخزنة عليها أو إتلافها ، إلى الجرائم الأكثر خطورة مثل التزوير المعلوماتي ، سرقة الأموال عن طريق الوسائط الإلكترونية وكذلك الجرائم كالتجار بالبشر وغيرها من أصناف الاجرام المستحدثة. [1]

الفرع الثاني: إتفاقية العربية لمكافحة جرائم التقنية المعلومات.

تعرف الإتفاقية العربية لمكافحة الجرائم الثقنية المعلوماتية بأنها اتفاقية إقليمة الدوليه المبرمة بين الدول العربية فى نطاق جامعة الدول العربية بصورة خطية في أكثر من وثيقة، وقد وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعها الذي عقد في مقر الأمانة العامة لجامعة الدول العربية بتاريخ 2010/01/21 القاهرة وتسمية الاتفافية "الإتفاقية العربية لمكافحة الجرائم التقنية المعلومات" وتتكون الإتفاقية من ديباجة وثلاثه وأربعين مادة موزعة على خمسة فصول. [2]

وتصدق الاتفاقية إلى تعزيز وتقوية التعاون بين الدول العربية في مجال مكافحة جرائم الثقنية المعلومات حفاظا على أمن و مصالح الدول العربية، وتعتبر هذه الإتفاقية مهمة من حيث وجودها، والأهم أن هذه الاتفاقية تنفد لحماية أمن الدول العربية من جرائم التقنية بسبب انتشار هذه الجرائم ووجود تعاون بيت الدول العربية يساهم في الحد من انتشارها، ووجود نوع

[1] بن مكي نجاة ، المرجع السابق ، الصفحة 131-132

[2] أحمد حيمي ، أصور جرائم تقنية المعلومات وفقا للاتفاقية العربية (2014) ، مجلة العلوم القانونية والسياسة ، المركز الجامعي لتامنعست الجزائر، المجلد 10 ، العدد 01 الصفحة 778 – 779.

من هذه الاتفاقيات بين الدول لتسليم المجرمين أو عمل ما بين الشريعات الوطنية والاتفاق العربية حتى لايكون هناك تعارض في تطبيق العقوبة بين تشريع والاتفاقية.

وتجدر الإشارة أن الاتفافية كان لها الأصل في وضع الجرائم فى الفصل الثاني منه مثل فى حالة الاعتداء على سلامة البيانات، وجريمة الترويرر, جريمة الاحتيال ، الشروع والاشتراك فى ارتكاب الجرائم...

وأما على المستوى الإجرائي تضمنت الاتفاقية مجموعة من القواعد الإجرائية في بيئة الجرائم المعلوماتية ، وأعتبرت هذه الإتفاقية أن كل دولة تبنت في قوانينها الداخلية والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة فى الفصل الثالث الذي يحتوي على أحكام إجرائية. [1]

الفرع الثالث : نظام الملكية الفكرية العربية بوجه عام

إهتمت الدول العربية بقضايا الملكية الفكرية، حتى تجد أن بعضها ساهم في الجهد الدولي لحماية الملكية الفكرية منذ القرن التاسع عشر، كما هو الحال في الجمهورية التونسية على سبيل المثال ، وأن عددا من الدول العربية من بيت الدول الرئيسية في عضويتها في عدد من إتفاقيات الملكية الفكرية الدولية .

ان استجابة الدول العربية لحماية الملكية الفكرية عالية في ظل موجات التشريعات التي تظهر فيها ، فى الخمسينات مشاهدت موجة واسعة من التشريعات في غالبية الدول العربية في مجال حماية براءات الاختراع و العلامات التجارية والرسوم والنماذج الصناعية، فقد شهدت في الثمانينيات والتسعينيات موجه واسعة من الإجراءات التشريعة في مجال حماية حق المؤلف. [2]

[1] أدهم باسم نمر بغدادي، (وسائل البحث والتحري عن الجرائم الإلكترونية)، أطروحت ماجستر في القانون العام ، كلية الدراسات العليا، جامعة النجاح الوطنية 2018.

[2] مروة زين العابدين صالح ، الحماية القانونية الدوليه للبيانات الشخصية عبر الأنترنت ، ط الأولى ، مركز الدراسات العربية ، مصر ، 2016، الصفحة 172.

وشهدت أوائل التسعينات إعتماد عدة قوانين وتعديلات لقوانين القائمة فيما يتعلق بحماية برامج الكمبيوتر و قواعد البيانات ضمن قوانين حقوق النشر .

والجدير بالملاحظة فإن الإتفاقية تلزم الدول الأعضاء بإتباع سياسات عامة فيتعين اتفاق مع الاتجاه العام ولكن قد تختلف في تفاصيل مع دولة أخرى. وموقف الدول العربية من الاتفاقيات الدولية في حفل الملكية الفكرية فإن غالبية الدول العربية هي أعضاء في إتفاقيات منها اتفاقية انشاء منظمة العالمية للملكية الفكرية، وإتفاقية ببرن للملكية الأدبية وإتفاقية باريس للمليلة الصناعية .

وتتضمن قوانين حماية الملكية الفكرية العربية نصوصا تحمى برامج الحاسوب وقواعد البيانات وفقا لحق المؤلف – بوجه عام – طيلة حياة المؤلف ولمدة خمسين عاما بعد وفاته. [1]

[1] مروة زين العابدين صالح ، المرجع السابق ، الصفحة 173–179.

المبحث الثاني: المكافحة التشريعة للجريمة الالكترونية في الجزائر

مع التطور المتصل الحاصل فى المجال العلمي أصبحت المعلومات والبرامج الكمبيوتر تهيمن على العديد من جوانب حياتنا المعاصرة، وبأبعادها الثقافية والاجتماعية والإقتصادية، فالواقع العلمي الكبير ومعقد يصعب التحكم والسيطرة عليه.

فسرقة المعلومات الإلكترونية واتلافها و تعدي على حقوق و قيم التى تهدد الأمن والإساءة إلى الآداب والنظام العام. وفى هذا العدد باشرت الجزائر كغيرها من دول العالم إلى حماية هذا الفضاء الإلكترونيا مستعملة جملة من القوانين ، سواء تعلق بالقوانين العامة أو القوانين الخاصة.

ومن خلال هذا المبحث سنتطرق إلى:

المطلب الأول: التصدي للجريمة الإلكترونية بموجب قوانين عامة

سنتناول في هذا المطلب القوانين العامة والمتمثلة في القانون الدستوري والقانون المدني والعقوبات لمواجهة الجرائم الالكترونية.

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني.

لقد تضمن القانون الدستوري لسنه 1996 و كذا تعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 و أيضا تم تعديله سنة 2020 حماية حقوق الأساسية والحريات الفردية ، وتكفل الدولة عدم المساس بحرمة الإنسان وكرست هذه المبادئ الدستورية في تطبيق النصوص التشريعية وأسسها فى قانون العقوبات وإجراءات الجنائية بشكل خاص والتي تمتنع على اعتداء على هذه الحقوق ومن أهم المبادئ الدستورية العامة. [1]

[1] د.بوضياف اسمهان الجريمة الإلكترونية والإجراءات التشريعة لمواجهة في الجزائر)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلية، العدد 11 ، بتاريخ 2018/05/09, الصفحة 361.

نصت المادة 38 : "*الحريات الأساسية وحقوق الإنسان والمواطن مضمونة* ". المادة 44 "حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون

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

الحريات الأكادمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون ". [1]

وتم تعديل الدستور سنة 2022 منها المادة 47 والتي تنص على :

لكل شخص الحق فى حماية حياته الخاصة من سرقة.

لكل شخص الحق في سرية مراسلاته وإتصلاته الخاصة فى أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات طابع شخصي حق أساسي بجانب القانون على كل إنتهاك لهذه الحقوق.

و أيضا نصت المادة 47 في الفترة الأولى "*حرية الإبداع الفكري بما في أبعاده العلمية والفنية مضمونة*."

وفي الفقرة الثالثة : يحمي القانون الحقوق المترتبة على الإبداع الفكري. [2]

وتماشيا مع ما تم ذكره فى المواد سواء فى دستور 2016 و في دستور المعدل 2020 إذ لا يجوز المساس بحرمة حياة الشخصية للمواطن وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة و القانون أيضا يحمي حقوق

[1] المادة 38 والمادة 44 ، مرسوم رئاسي ، رقم 16 – 01 ، تاريخ 06 مارس 2016، يتضمت قانون الدستور ج.ر العدد 14 ، بتاريخ 07 مارس 2016.

[2] المادة 47, صادرة بموجب مرسوم رئاسي ، رفع 20 –442 بتاريخ 30–12–2020 يتصمن قانون دستور ج.ر العدد 82 ,بتاريخ 2020.

المؤلف ولايجوز حجز أي مطبوع أو تسجيل أو أي وسيلة من وسائل التبليغ والإعلام إلا بأمر قضائي. [1]

وانسجاما مع الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع إلى النص على أنه يجوز لكل من تعرض لاعتداء غير مشروع على حق من الحقوق الملازمة للإنسان أن يطلب وقف الاعتداء مع التعويض عن الضرر الذي تعرض [2] له طبق لنص المادة 124 ق م ج *"الفعل أيا كان يرتكبه الشخصا بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعريض"* [3] وقد جاء كنص عام وشاملا لأي اعتداء يقع على حق من الحقوق الملازمة الشخصية بما في ذلك الحق في الحياة الخاصة ، وجاء فى هذا النص مبدأ مهما و هو حق من وقع إعتداء على حياته الخاصة في التعويض كما لحقه من ضرر فالمسؤولية المدينة ترتب الحق في الحكم فى بالتعويض . فالفعل الضار هو أساس المسؤولية" فهو الركن الأساسي الذى يؤسس عليه الحق فى رفع دعوى القضائية عن الاعتداءات الإلكترونية التي تمس الحياة الخاصة على شبكة الأنترنت. [4]

الفرع الثاني: مواجهة الجريمة الإلكترونية بموجب قانون العقوبات

وضع المشرع عدة آليات تشريعية لمكافحة الجرائم الالكترونية والحد منها وذلك من خلال إضفاء تعديلات على قانون العقوبات بموجب القانون رقم 15/04 والمعدل والمتمم للأمر 155/66 و المؤرخ فى 10 نوفمبر 2004 فى قسم السابع مكرر من الفصل الثالث

[1] بوضياف اسمهان ، المرجع السابق، الصفحة 361-362.

[2] د. حسين نوارة ، آليات تنظيم المشرع الجزائر لجريمة الإعتداء على حق الحياة الخاصة، أعمال الملتقى الوطني : آليات مكافحة الجرائم الالكرونة في التشريع الجرائري، جامعة مولود معمري تيزي وزو الجزائر 29 مارس 2017 الصفحة 121

[3] المادة 124 الأمر رقم 75-58 المورخ في 26 سبتمبر 1975 المتضمن القانون المدني.

[4] د.حسين نوارة, المرجع السابق ، الصفحة 121.

الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات : جاء التعديل فى المواد 394 مكرر إلى المادة 394 مكرر 7ق ع ج. [1]

و يلاحظ من نص المادة أن المشرع الجزائري قسم الجرائم الالكترونية إلى أربع فئات تتنوع بحسب المصالح المحمية ، التي تتمثل بشكل أساسي فى سرية هذه البيانات، كما أضاف المشرع فى سنة 2006 تعديلات جديدة مست قسم السابع مكرر منه وجاء لتسديد العقوبة المقرة لهذه الجرائم دون المساس بنص المادة وجاء التعديل لزيادة الوعي بخطورة مثل هذه الجرائم المستحدثة فإنما تؤثر على إقتصاد الوطني وبمؤسسات الدولة بدرجة الأولى وشيوع ارتكابها ليس من الطبقة المثقفة يل من قبل جميع الفئات و بمختلف الأعمار وذلك لتبسيط وسائل التكنولوجيا المعلومات كوسيلة و تبادل المعلومات. [2]

في المادة 334 مكررة ق ع ج نصت : " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألفا إلى مائة ألف دينار لكل من يدخل أو يبقي عن طريق الغش فى كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حدف أو تغير المعطيات المنظومة إذا ترتب على الأفعال المذكورة أعلاء تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنئين وغرامة من خمسين ألف إلى مائة وخمسون ألف دينار ".

وفي مستهل النص نلاحظ أن المشرع جرم كل دخول الغير المصرح به والغير مشروع إلى منظومة المعالجة الآلية للمعطيات، وما يخص جريمة البقاء غير مشروع داخل النظام المعلوماتي ويقصد بها التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو

[1] أنظر المواد من 394 إلى 394 القانون رقم 04-15 المؤرخ في 10 توقير 2004 ، المتضمن قانون العقوبات ، ج ر 71 ، 2004

[2] د. سي حميدي عبد المومن ، د قيرة سعاد الجريمة الإلكترونية وآليات التصدي لما في القانون الجزائري) ، مجلة البيبان للدراسات القانونية والسياسية، جامعة البشير الابراهمي ، برج بوعريريج الجزائر، المجلد 07 ، العدد 01, جوان 2022 ، الصفحة 63 – 64.

من له سيطرة عليه وتتحقق في هذه الحالة التى يجد الشخص فيها نفسه داخل النظام عن طريق الخطأ أو الصدفة إلى أنه يقرر البقاء داخل النظام وعدم قطع االإتصال به.

أما جريمة الاعتداء على المعطيات نصت المسادة 394 مكرر 1 قاع ج يعاقب بالحيس من شهرين على ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 كل من يقوم عمدا وعن طريق الغش :

فالمشرع حصر صور الاعتداء على المعطيات في ثلاث صور تتمثل في إدخال معطيات جديدة وغير صحيحة إلى المعطيات الموجودة داخل النظام التي تتم معالجتها آليا. وإزالة معطيات كانت موجودة أو تعديل أو تغير المعطيات و إستبدالها بأخرى من خلال برامج معينة تعمل على إتلاف المعطيات. [1]

فجريمة الإستلاء على المعطيات تعد هذه الجريمة من بين أكثر الجرائم وقوعا فى العالم الاقتراضي وهي ما أقرته المادة 394 مكرر 2 ق.ع.ج.

وفى نفس العدد أنشطة الأنترنت المجسدة بجرائم المحتوى الضار والتعرف الغير القانوني نصت مواد القسم السابع مكرر من ق ع ج وخاصة المادة 394 مكر 2/ 2 على تجريم أفعال الحيازة ، وإفشاء والنشر التي ترد على المعطيات الآليه بأهداف المنافسة غير مشروعة، الجوسسة .. الإرهاب ، التحريض على الفسق، وجميع الأفعال الغير المشروعة . وذلك بعقوبة الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر6 ق ع ج بتوقيع عقوبة تكميلية في غلق المواقع التى تكون محلا للجريمة من الجرائم المنصوص عليها من قاع ج. [2]

بإضافة الى ق إ ج ج فقد أدرك المشرع الجزائري بأن المواجهة الفعالة للإجرام الالكروني لا تكون فقط بإرساء قواعد قانونية موضوعيه ذات طبيعة ردعية ، و إنما لابد من

[1] سي حميدي عبد المومن د. قيرة سعاد ، المرجع السابق ، الصفحة 64.

[2] بن علية بن جدو ، المرجع السابق ، الصفحة 314-315.

إضافة قواعة اجرامية وقائية تحفظية لتفاد وقوع الجرائم الإلكترونية، وهو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل والمتمم لقانون إج ج تدابير اجرائية مستحدثة تتعلق بالتحقيق فى الجرائم المعلوماتية والتى تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها والتسرب.

ويقصد بإعتراض المراسلات أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوتريع والتخزين الاستقبال والعرض) التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الادلة عنها. [1]

وقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء وهذا في المادة 65 مكرر 5 ق إ ج ج ، فيموجب هذه المادة فإن المشرع أجاز السلطات التحقيق والإستبدال إذا استدعت ضرورة التحري فى الجريمة المتلبس بها أو التحقيق فى الجريمة الإلكترونية، اللجوء إلى اجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والتقاط الصور و الاستعانة بكل الترتيبات التقنية اللازمة من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها. [2]

المطلب الثاني: مواجهة الجريمة الالكترونية بموجب قوانين وهيئات خاصة.

بعد التطرق إلى مكافحة الجرائم الالكترونية من خلال قوانين عامة، سوف نتناول في هذا المطالب إلى تصدى للجرائم الالفرونه موجب قواتنا وهيئات خاصة وسنعرفها كالآتي :

الفرع الأول : الحماية الجزائية المعلوماتية من خلال نصوص الملكية الفكرية

يتم تحديد العلاقة بين الجرائم المعلوماتية وحقوق الملكية الفكرية بشكل عام من ناحيتين من خلال اعتبار نظام المعلومات صورة و تطبيقات متطورة لبرامج الحاسوب

[1] بوضياف اسمهان ، المرجع السابق ، الصفحة 363.

[2] بوضياف اسمهان ، المرجع نفسه ، الصفحة 364.

معطياته واعتباره من الإبداعات الفكرية ذات طبيعة التقنية وكفل المشرع الجزائري حمايتها بموجب الأمر 03-05 المؤرخ 19-07 - 2003 .

حيث يشكل هذا الاعتداء على برامج جريمة معلوماتية، ومن جهة أخرى فإن ظهور نوع جديد من المصنفات يعرف بالمصنفات الرقمية تتجة للتطوير التي عرفها مجال التكنولوجيا الإعلام والإتصال الذي أدى إلى ظهور وسائل وطرق جديدة لإستغلال المصنفات الفكرية عن طريق المنظومك المعلوماتية مما يجعل الاعتداء على حقوق المؤلف والحقوق المجاورة في بعض حلاته من صور الجريمة المعلوماتية. [1]

وعليه من خلال استقراء الأمر 10/97 المعدل والمتمم بالأمر 05/03 المتعلق بحق المؤلف والحقوق المجاورة نستنتج ما يلي :

- قام المشرع بتوسيع قائمة المؤلفات المحمية ويدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصيلة بموجب 04 من الأمر 97/ 10 التى عبر عنها لمصنفات قواعد البيانات وبرامج الإعلام الآلي التي تمكن من القيام بنشاط علمي أو نشاط آخر، أما القواعد البيانات فهي عبارة عن مجموعة من المصنفات والأساليب والقواعد. كما يمكن أن تشمل الوثائق المتعلقة بسير ومعالجة المعطيات بموجب المادة 05 من الأمر 10/97
- وأن المدة الحماية تحدد من 25 سنة إلى 50 سنة بعد الوفاة المبدع مسبقا للمادة 58 من الأمر 05/03. [2]

عند المساس بحقوق المؤلفين لاسيما مؤلفى المصنفات المعلوماتية تشدد العقوبات وهذا بموجب أحكام المادة 153 من الأمر 05/03 وتقابلها المادة 151 من الأمر 10/97

[1] عبد القادر عيمر، التحديات القانونية لإتيات الجريمة المعلوماتية ، دط، النشر التشر الجامعي الجديد, تلمسان الجزائر ، 2021، الصفحة 78 – 79.

[2] المادة 4 و5 والمادة 58 ، 153 أمر رقم 10/97 المعدل والمتمم بأمر جر العدد : 44 ، تم 05/03 تاريخ 19 جوان 2003 المتضمت حق المؤلف والحقوق المجاورة ج ر العدد 44 , تم نشرها 23 جوان 2003.

– اعتمد المشرع الجزائر فيما يتعلق بحماية المصنفات الجزائرين المعيار الشخصي إذ نص أن الحماية تشمل مصنفات الجزائرين سواء نشرت فى الجزائر أو الخارج.

أما بالنسبة لمؤلفات الأجانب اعتمد على المعيار الإقليمي حيث شملها بنفس الحماية التي يتمتع بها مؤلفات الجزائرين .

وأشارت معاهدة الويبو بشأن حق المؤلف المؤرخة في 1996/06/20 في مادتها الرابعة على أن برامج الحاسوب تتمتع بالحماية باعتبارها من المصنفات أدبية حسب مفهوم المادة الثانية من اتفاقية بارن ، تطبيق الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أوشكلها . وأضافت أيضا المادة الخامسة منها أن مجموعات البيانات تتمتع بالحماية فإنها تعتبر ابتكارات فنية بسبب اختيار محتوياتها. [1]

الفرع الثاني : مكافحة الجرائم الالكترونية وفق قوانين 04/09 و 04/15 وقانون 04/18 و 07/18

البند الأول: قانون 04/09 المتعلق بالوقاية من جرائم المتعلقة بإعلام واتصال

وتماشيا مع التطورات التي عرفتها الجزائر في مجال التكنولوجيا لأنها أصبحت كثيراً من الأحيان مسرح للجريمة ومع تفاقم الاعتداءات على معطيات الحاسب الالي مع ضعف الحماية الفنية، استدعى تدخلا تشريعيا صريحا فإستدرك المشرع الجزائري الفراغ القانوني من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. ومكافحتها ، يحتوي هذا القانون على 19 مادة فى ستة فصول فالفصل الأول يحدد الأهداف القانون ومفهوم المصطلحات الثقنية الواردة فيه والأحكام المتعلقة بمجال تطيبقية مع تأكيد على احترام مبدأ المحافظة على سرية الإتصالات الإلكترونية و تجميع وتسجيل ، أما الفصل الثاني يتضمن مراقبة الإتصالات الالكترونية فى نطاق

[1] سوير سفيان ، (جرائم المعلوماتية) ، مذكرة الماجستير، جامعة أبوبكر بلقايد تلمسان ، كلية الحقوق والعلوم الساسية سنة 2010 – 2011 ، الصفحة 72-73-74.

الإتصالات المنطوية على خطورة التهديدات وثم تأكيد على عدم جواز إجراء عمليه المراقبة إلا بإذن السلطة المختص والفصل الثالث من هذا القانون تضمن القواعد الإجرائية المعلقة بتفتيش المنظومة المعلوماتية، أما الفصل الرابع يحدد الإلتزامات التي تقع على عاتق المتعاملين فى مجال الاتصالات الإلتكرونية ، الفصل الخامس يتضمن انشاء هيئة وطنية للوقاية من الإجرام المتصل بالتكنولوجيا الإعلام و الاتصال ومكافحته وأخيراً الفصل السادس تضمن التعاون والمساعدة القضائية الدولية. [1]

البند الثاني : قانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونين

جاء فى القانون رقم 04/15 و المتعلق بالقواعد التوقيع والتصديق الإلتكروني بتجريم بعض الأفعال المرتبطة بالبينات و والمعلومات ذات طابع الشخصي التي تشكل الاعتداء عليها و يعد جريمه يعاقب مرتكبها بأحكام جزائية تتمثل في:

– جريمة إفشاء البيانات الشخصية أو اساءة استعمالها حسب نص المادة 68 من نفس القانون حيث يعاقب الشخص بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة مالية أو بإحدى هاتين العقوبتين، فكل من يقوم حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني موصوف خاص بالغير.

جريمة الإخلال بسرية البيانات وهذا ما نصت عليه المادة 42 من ق 04/15 [2] وجب على مؤدي خدمات التصديق الإلكتروني أن يحافظوا على سرية البيانات والمعلومات المتعلقة بشهدات التصديق الإلكتروني فإذا تم الإخلال بهذا الواجب يعاقب بالسجن من 3 أشهر إلى سنتين وبغرامة مالية أو بإحدى هاتين العقوبتين وأراد المشرع أن يضفي حمايته على المعلومات الشخصية التي تؤخد من الأفراد وأضاف صفة السرية لما لها من خصوصية معينة وجرم الإخلال بسرية هده البيانات

[1] بن مكي نجاة، المرجع السابق ، الصفحة 228 ,229 230.

[2] المادة 68 و المادة 42 : قانو نا رقم 04/15 المؤرخ في 01 فبراير 2015 ، يتضمن قواعد المتعلقة بالتوقيع والتصديق الإلكترونين ، ج ر العدد 06 . بتاريخ فبراير 2015.

– جريمة جمع البيانات الشخصية للمعنى دون موافقته : تنص المادة 43 منه لا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع البيانات الشخصية للمعنى إلا بموافقته الصريحة، وإذا أخل بهذا الواجب يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية أو بإحدى هاتين العقوبتين فقط. [1]

البند الثالث: القانون 04/18 والمتعلق بالقواعد العامة بالبريد والإتصالات الإلكترونية وقانون رقم 07/18 والمتضمن حماية الأشخاص الطبيعين في مجال معالجة المعطيات

– كل القوانين سالفة الذكر التي أصدرها المشرع الجزائري لمكافحة الجرائم الإلكترونية لم تكن كافية لمجابهته ، لهذا أصر المشرع القانون رقم 04/18 والذي ألغى بموجب رقم 03/2000 الذى أكد فيه على وجوب عدم المساس استعمال شبكات وخدمات الإتصال الإلكترونية بحفظ الحياة الخاصة وإذا تم المخالفة يتعرض للأحكام الجزائية. في حالة انتهاك سرية المراسلات الالكتروبة يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية طبقا لنص المادة 164 من قانون 04/18 .

وأيضا فى حالة تحويل المراسلات الصادرة عن طريق البريد حسب نص المادة 165 من قانون 04/18 فإنه يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة مالية أو إحداهما. [2]

أما القانون المتعلق بتحديد قواعد الحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصى الذى أصدر حديثا القانون رقم 07/18 المؤرخ في 10 جوان 2018 ويقصد بالمعطيات ذات الطابع الشخصى وفقا لأحكام هذا القانون هي كل معلومة متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة لاسيما بالمرجوع إلى

[1] سي حيدي عبد المومن, د قيرة سعاد ، المرجع السابق، الصفحة 66.

[2] المادة 164 ، 165 قانون رقم 18–04 المؤرخ 10 مايو 2018 الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية ، ج ر العدد 27 بتاريخ 13 مايو 2018

رقم التعريف أو عنصر من عناصر خاصة بهويته البدنية أو الجينية أو البيومترية أو الثقافية أو الإجتماعية.

وتجدر الإشارة أن مخالفة الأحكام لهذا القانون يعرض للأحكام الجزائية كخرق الحياة الخاصة عند معالجة المعطيات حيث يعاقب بالحبس من ستتين إلى خمس سنوات بغرامة مالية ، وأيضا فى حالة الإستعمال الغير الشرعي للمعطيات الشخصية التى يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد و واضح فلا يجوز وصول هذه المعلومات إلى شخص آخر إذ تم إلحاق الضرير فالمشرع وضع عقوبة الحيس من ستة أشهر إلى سنة وبغرامة مالية أو بإحدى هاتين العقوبتين. [1]

الفرع الثالث : الهيئات الخاصة لتصدي الجرائم الإلكترونية.

تتوفر مجموعة من الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية نذكر منها:

– الهيئة القضائية الخاصة للبث في الجرائم الإلكترونية : شرعت الجزائر فى إصلاح العدالة سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية وهي دعم حقوق الإنسان وتسهيل حق اللجوء إلى القضاء وإعادة لإعتبار النظام التكوين والتأهيل بإحداث تغير جديرية في قطاع العدالة واستحداث قواتن تنسجم مع قوانين أخرى .

فالمشرع الجزائري استحدث الأقطاب الجزائية المختصة وهي المحاكم ذات اختصاص إقليمي موسع بموجب قانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم في ق إ ج ج الذى أجاز توسيع اختصاص لبعض المحاكم. ووكلاء الجمهورية وقضاء التحقيق فى جرائم محددة على سبيل الحصر. [2]

[1] سي حيدي عبد المومن, د قيرة سعاد ، المرجع السابق، الصفحة 66–67.

[2] سعيدة بوزنون (مكافحة الجريمة الإلكترونية في التشريع الجزائري مجلة العلوم الإنسانية ، جامعة الإخوة منشوري قسنطينة ، المجلدب ، العدد 52 بتاريخ 2019/07/09.

– الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال: تم إنشاء هذه الهيئة بموجب القانون رقم 04/09 في 5 أوت 2009 والذي حددت المادة 14 [1] منه مهام الهيئة والمتمثلة في :

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مكافحته.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية فى التحري الجرائم التي لها صلة بتكنولوجيا الإعلام والإتصال.

– تبادل المعلومات مع الدول فى الخارج قصد جمع المعلومات و المعطيات المفيدة في التعرف على مرتكبي الجرائم والمتصلة بتكنولوجيات إعلام والإتصال وتحديد تواجدهم .

أما المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي أنشىء بموجب مرسوم رئاسي رقم 04 – 183 المؤرخ في 26 جوان 2004 وهي مؤسسة ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي ويوضع تحت وصاية وزير الدفاع الوطني. [2]

يتكون هذا المعهد من إحدى عشر دائرة متخصصة في عدة مجالات مثبانية، تقدم المساعدات التقنية وتقوم دائرة الإعلام الآلي والالكتروني المكلفة بالمعالجة وتحليل وتقديم كل دليل رقمي يساعة العدالة .

أما مركز الرقابة من الجرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني أنشىء سنة 2008 ومن أهدافه هو تأمين المنظومة المعلومات لخدمة الأمن العمومي ، وهو بمثابة توثيق فدوره قيام بتحليل المعطيات والبينات للجرائم المعلوماتية المرتكبة ومحاولة تحديد هوية أصحابها، مما يؤمن الأنظمة المعلوماتية للمؤسسات و البنوك ... الخ ، فإنه يعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى.

[1] المادة 14 قانون 09–04 المؤرخ 5 اغسطس 2009 يتضمت القواعد الخاصة للوقاية من الجرائم التكنولوجيا الإعلام والإتصال ومكافحتها ، ج ر العدد 47 بتاريخ 16 أغسطس 2009.

[2] بزهرينً فتيحة ,(الجريمة المعلوماتية فى التشريع الجزائري) ، مجلة الحقوق والعلوم الإنسانية، جامعة قسنطية 2, الجزائر، المجلد 14 ، العدد 04, الصفحة 57.

والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني تم انشائها سنة 2011 وأضيف للهيكل التنظيمي حيث احتلت الجزائر المرتبة 23 عالميا والعاشرة عربيا حسب إلتزامها بتلك التدابير التي يحددها الرقم القياسي للأمن السيبراني. [1]

ملخص الفصل الثاني :

حاولنا في الفصل الثاني دراسة الجوانب لآليات المساعدة لمكافحة الإجرام الالكتروني والتي تعد حديثة وخطيرة في ة في نفس الوقت ، وقد سجلت عددا كبيرا في مختلف دول العالم ومن بينها الجزائر لهذه الجرائم المعلوماتية ، مما جعل أهل الاختصاص في ايجاد حلول عصرنة لمكافحتها والحد من انتشارها من خلال التعاون الدولي و المنظمات الدولية والجمعية العربية وأيضا الجزائر كان لها دور فعال من خلال وضع قوانين ردعية للحد ومواجهة الإجرام الإلكتروني.

[1] بن علية بن جدو ، المرجع السابق ، الصفحة 316-317.

خـاتمـة

الخـــاتمــة

من خلال دراستنا لموضوع الجرائم الالكترونية والتي هي من أخطر الجرائم، فالشخص الذي يرتكبها هو مجرم غير تقليدي له مميزاته الخاصة، وهي جرائم يصعب اكتشافها وإذا ما اكتشفت يصعب إثباتها، وما يزيد من خطورة هذه الجرائم أن للضحية دور مهم فيها، وأنها جرائم ناغمة شديدة الإغراء للمجرمين وأنها جرائم عابرة للحدود وجرائم فادحة الأضرار.

الجرائم الإلكترونية تشمل أي نوع من الأنشطة الإجرامية التي تنطوي على استخدام التكنولوجيا الحديثة، مثل الإنترنت والشبكات الحاسوبية والأجهزة الذكية والهواتف الذكية والبريد الإلكتروني وغيرها، للقيام بأنشطة إجرامية مثل الاحتيال والتزوير والتهديد والتحيّز والتجسس والاختراق والإبتزاز والتحريض والدعارة الإلكترونية والتحرش الإلكتروني وسرقة الهوية الإلكترونية والتعرّض للأطفال. ويؤدي القيام بالأنشطة الإجرامية هذه إلى ارتكاب جريمة تحت رقابة القانون، وتعرض المجتمع والأفراد إلى خطر.

ومن بين أهم النتائج المتوصل إليها في هذه الدراسة ما يأتي فيما يلي :

- لحد الساعة لم يتفق الفقهاء على تعريف جامع مانع للجريمة الالكترونية.
- تبين من خلال دراسة خصائص الجريمة الالكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.
- القصور التام والكامل للقوانين التقليدية أمام هذه الجرائم المستحدثة.
- إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية ، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في بيئة الرقمية الحديثة.
- المشرع الجزائري لم يخصص قانونا خاصا للجريمة الالكترونية.

في ضوء النتائج والاستخلاصات السابقة التي أظهرتها الدراسة تخلص إلى بعض التوصيات والاقتراحات تتمثل فيما يلي :

- ضرورة إعطاء تعريف موحد للجريمة الالكترونية يشمل فيه كل سلوكيات المجرمة.
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحقيق التعاون مع التقنيين من أصحاب الخبرة.

– ضرورة مراجعة التشريعات الوطنية من خلال تشديد الوصف الجنائي والعقوبات المقررة للأنماط الإجرامية للجريمة المعلوماتية ، بغية تحقيق الردع والقضاء على الإجرام المعلوماتي.

– الحرص على تعديل بعض التشريعات الجزائرية الحالية وخاصة في مجال الملكية الفكرية بما يتلائم مع طبيعة جرائم الأنترنت والتقنية ، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل مفصل ودقيق.

– الإسراع في إصدار القوانين التنظيمية ، من خلال وضع مدونة قواعد السلوك في مجال المعلوماتية ، تتناسب مع التطورات التي يعرفها الإجرام الالكتروني.

– ضرورة إبرام اتفاقات عربية ودولية في مجال مكافحة الجرائم المعلوماتية وذلك لتحديد إطار الاختصاص القضائي الدولي والتعاون في كشف وإثبات الجريمة المعلوماتية.

– التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم.

– الاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن وجه.

– عقد دورات مكثفة للكوادر البشرية العاملين في حق التحري والتحقيق ، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب والجرائم المرتبطة بها والنظر في تضمين مناهج التحقيق الجنائي في كليات ومعاهد تدريب الشرطة موضوعات عن جرائم الأنترنت.

– ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا : المصادر.

– 1/ قانون المدني الجزائري المعدل والمتمم لأمر 75–58 المؤرخ 26 سبتمبر 1975.

– 2/ قانون 03–05 أمر رقم 97–10 بتاريخ 19 جوان 2003 المتضمن حق المؤلف والحقوق المجاورة ج ر العدد 44.

– 3/ قانون العقوبات الجزائري 04–15 بتاريخ 10 نوفمبر 2004 .ج ر العدد 71.

– 4/ قانون 04–14.المعدل والمتمم للأمر رقم 26 – 155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية العدد 71 ، المؤرخ 10 نوفمبر 2004.

– 5/ قانون 09–04 المؤرخ 5 أغسطس 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، ج ر عدد 47 بتاريخ 2009/08/16.

– 6/ قانون دستوري المعدل والمتمم رقم 01–16 تاريخ 6مارس 2015م العدد 14.

– 7/ قانون 18–04 المؤرخ 10 مايو 2018 يحدد قواعد العامة المتعلقة بالبريد والاتصالات الالكترونية العدد 27.

– 8/ القانون 18/07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

– 9/ قانون الدستور المعدل رقم 20 – 442 بتاريخ.30–12–2020، العدد 82.

ثانيا : الكتب.

– 1/ أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومة ، الجزائر ، ط 10 2011

– 2/ أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط 2 2006

– 3/ أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية الجامعة الجديدة الإسكندرية 2015.

– 4/ بن مكي نجاة ، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية الجزائر 2017

– 5/ جعفر حسن جاسم الطائي، الجرائم تكنو لوجيا المعلومات ط 1، دار البداية ناشرون الموزعون ، عمان 2010

– 6/ حسين فريجة ، الجرائم الالكترونية والانترنت ، مجلة المعلوماتية ، العدد 36 ، أكتوبر 2011

– 7/ خراشي عادل عبد العال إبراهيم، استكاليات التعاون الدولى فى مكافحة المعلوماتية، دار الجامعة الجديدة ، 2017.

– 8/ زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر ، د ط ، 2011

– 9/ عبد القادر عمير ، التحديات القانونية الإتيات الجريمة المعلومانية النشر الجامعي الجديد ، تلميات الجزائر 2021.

– 10/ د. عبد الله حسين محمود ، شرقة المعلومات المخزنة في الحاسب الآلي ، دار النهضة العربية ، ط 2 ، القاهرة 2002

– 11/ عبد الله عبد الكريم عبد الله ، الجرائم المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، ط1 ، لبنان ، 2007 .

– 12/ مروة زين العابدين صالح، الحماية القانونية الدولية للبينانات الشخصية عبر الأنترنت ، ط1 ، مركز الدراسات العربية، مصر 2016 .

– 13/ مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية ، الجزائر 2018

– 14/ نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط 1 ، دار الثقافة للنشر والتوزيع عمان ، 2008

– 15/ يزيد أبو حليط ، الجرائم الالكترونية والوقاية منها في القانون الجزائري ، في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات – قانون الإجراءات الجزائية – قوانين خاصة ، د.ط ، دار الجامعة الجديدة للنشر الإسكندرية 2019

ثالثا : مذكرات

– 1/ بعرة سعيدة ، الجريمة الالكترونية في التشريع الجزائري ، دراسة مقارنة ، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، بسكرة ، 2016/2015

– 2/ بوكثير خالد ، استئناف الأحكام القضائية الصادر عن هيئات القضاء الإداري في ظل التعديل الدستوري لسنة 2020 مذكرة لنيل شهادة الماستر في الحقوق ، جامعة عبد الرحمان ميرة ، بجاية ، 2021–2022

– 3/ عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006

– 4/ معتوق عبد اللطيف ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة مكملة لنيل ش‌هادة الماجستير وعلوم الجنائية ، 2011–2012

– 5/ د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة 2003

– 6/ نشناش منية ، مداخلة حول الركن المفترض في الجريمة المعلوماتية ، جامعة بسكرة 2015 –2016

– 7/ يوسف صغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة لنيل شهادة الماجستير في القانون الخاص ، كلية الحقوق جامعة مولود معمري ، تيزي وزو ، 2013

رابعا : المقالات العلمية والمجلات.

– 1/ ابراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، مجلة كلية الشريعة والقانون بطنطا، الجزء الثاني، العدد 30

– 2/ أحمد حيمين, صور جرائم التقنية المعلومات وقف للإتفاقية العربية مجلة العلوم القانونية والسياسة، المركز الجامعي لتمنراست الجزائر، 2014 العدد 01

– 3/ برقوق يوسف المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية, مجلة البصائر للدراسات القانونية ، جامعة جيلالي ليابس سيدي بلعباس الجزائر 2021/03/05 العدد 01

– 4/ بن علية بت جدو, تحديات الأمن السيراني لمواجعة الجريمة الإلكترونية مجلة الجزائرية للأمن الإنساني، جامعة بومرداس ، تاريخ 2024/03/01 العدد 02.

– 5/ بوضياف إسمهان، الجريمة الإلكترونية و الإجراءات التشريعية لمواجهة في الجزائر مجلة الاستاد الباحث للدراسات القانونية والسياسة، جامعة محمد بوضياف المسيلة ، بتاريخ 2018/05/09 العدد11.

– 6/ بوهرين فتيحة ، الجريمة المعلوماتية في الشريع الجزائري ، مجلة الحقوق والعلوم الإنسانية ، جامعة قسنطينة ، الجزائر ، العدد 04.

– 7/ سعيدة يوزنون ، مكافحة الجريمة الالكترونية في التشريع الجزائري ، مجلة العلوم الإنسانية ، جامعة الإخوة منثوري قسنطة 2019/07/09 العدد 52.

– 8/ د. سي حمدي عبد المومن ، د. قيرة سعاد ، الجريمة الالكترونية وآليات التصدي لها في القانون الجزائري ، مجلة البيان للدراسات القانونية والسياسة ، جامعة البشير الإبراهيمي، جوان 2022 ، العدد 01.

– 9/ د. فاروق خلف ، الآليات القانونية لمكافحة الجريمة المعلوماتية ، مجلة الحقوق والحريات ، كلية الحقوق جامعة جمة الخضر الوادي ، 2015 العقد الثاني

– 10/ قرزان مصطفى, زرقين عبد القادر ، الاليات الدولية لمكافحة الجرائم الالكتروني مجلة الصوت القانون، المركز العاصمي تسمسيلت 16/04/2022 العدد 02

– 11/ مراد مشوش ,الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات جامعة غرداية ، 20/12/2019 العدد 02

– 12/ ملياني عبد الوهاب ، جرائم المساس بالمعطيات الشخصية على ضوء القانون رقم 18/07 ، مجلة البحوث القانونية والاقتصادية ، الطبعة 6 ، العدد 1 ، بتاريخ 2023/01/28

– 13/ لورنس سعيد الحوامدة، " الجرائم المعلوماتية أركانها وآلية مكافحتها " دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن، 2016/08/13

خامسا : المؤتمرات والملتقيات العلمية.

– 1/ المقدم عز الدين عز الدين ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية بسكرة في 2015/11/16

– 2/ بن غدفة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها أعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017

– 3/ حسين نوارة ، آليات تنظيم المشرع الجزائري لجريمة الإعتداء على حق الحياة الخاصة، أعمال الملتقى الوطني، جامعة مولود معمري ، تيزي وزو ، الجزائر ، بتاريخ 29 مارس 2017.

– 4/ فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الإلكترونية " ، طرابلس، بتاريخ 25-24 مارس 2017

سادسا : الرسائل العلمية.

– 1/ براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية ، أطروحة لنيل شهادة الدكتوراه في العلوم ، جامعة ميلود معمري ، تيزي وزو ، كلية الحقوق و العلوم السياسية ،2018/06/27.

– 2/ سويسر سفيان ، جرائم المعلومماية ، مذكرة الماجستير ، جامعة أبو بكر بلقايد تلمسان كلية الحقوق والعلوم السياسية، سنة 2010-2011

– 3/ فايز محمد راجح غلاب ، الجرائم المعلومانية في القانون الجزائري و اليمني أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق ، فرع القانون الجنائي والعلوم الجنائية جامعة الجزائر ، كلية الحقوق ، سنة 2009-2010.

الفهرس

الفهرس

الاهداءات	
شكر وعرفان	
قائمة المختصرات	
المقدمة	أ – د
الفصل الأول : ماهية الجريمة الإلكترونية.	9
المبحث الأول: مفاهيم الجريمة الإلكترونية	10
المطلب الأول: تعريفات الجريمة الإلكترونية	10
الفرع الأول: تعريف الجريمة الإلكترونية	11
البند الأول: الضيق	11
البند الثاني: الموسع	11
الفرع الثاني: تعريف الجريمة الإلكترونية في التشريع الجزائري والمقارن	13
البند الأول: التعريف الفقهي	13
البند الثاني: التعريف القانوني	14
المطلب الثاني: خصائص الجريمة الإلكترونية وصورها وأنواعها	15
الفرع الأول: خصائص الجريمة الإلكترونية	15
البند الأول: الجرائم التي تدفع على المعطيات	15
البند الثاني: الجرائم العابرة للحدود	16
البند الثالث: سهولة ارتكابها	17
البند الرابع: صعوبة معرفة مرتكب الجريمة	18
البند الخامس: سهولة إخفاء وطمس آثارها	19

البند السادس: جرائم متطورة ومتعددة الأشكال	19
الفرع الثاني: المجرم المعلوماتي	20
البند الأول: تصنفات المجرم المعلوماتي	20
البند الثاني: صفات المجرم المعلوماتي	22
البند الثالث: دوافع ارتكاب الجرائم المعلوماتية	23
المبحث الثاني: أركان وأحكام الجريمة الإلكترونية والإجراءات العامة	26
المطلب الأول: أركان الجريمة الإلكترونية وأحكامها	26
الفرع الأول: أركان الجريمة الإلكترونية	26
البند الأول: الركن الشرعي للجريمة الالكترونية	26
البند الثاني: الركن المادي للجريمة الالكترونية	27
البند الثالث: الركن المعنوي للجريمة الالكترونية	28
الفرع الثاني: أحكام الجريمة الإلكترونية	29
البند الأول: أحكام الشروع في الجريمة الالكترونية	29
البند الثاني: أحكام المساهمة الجنائية في الجريمة الالكترونية	30
البند الثالث: أحكام الاتفاق الجنائي على ارتكاب الجريمة الالكترونية	31
المطلب الثاني: إجراءات متابعة الجريمة الإلكترونية	33
الفرع الأول: جمع الأدلة	33
البند الأول: المعاينة	33
البند الثاني: التفتيش	34
البند الثالث: ضبط الأدلة	35

الفرع الثاني: وسائل الاثبات	35

البند الأول: الخبرة	35
البند الثاني: الشهود	36
البند الثالث: الاستجواب	36
الفصل الثاني : التحديات القانونية لمكافحة الجريمة الإلكترونية.	38
المبحث الأول: الاليات والسبل للحد من الجريمة الإلكترونية على المستوى الدولي	38
المطلب الأول: الجهود الدولية لمكافحة الجريمة الإلكترونية.	38
الفرع الأول: التعاون الدولي .	38
التعاون القضائي	39
البند الأول : التعاون الأمني	39
البند الثاني : المساعدات القضائية	40
أولا: تبادل المعلومات	40
ثانيا: نقل الإجراءات.	41
ثالثا: الإنابة القضائية الدولية.	41
رابعا: تسليم المجرمين.	42
الفرع الثاني: الإختصاص القصائي الدولى والداخلي	42
البند الأول : الاختصاص القصائى الدولى	42
البند الثاني: الاختصاص القصائى الداخلي	43

الفرع الثالث : الجهود الأمم المتحدة والأروبية لمكافحة الجريمة الالمكرونة	46

البند الأول : الجهود الأمم المتحدة لمكافحة الجريمة الإلكتروني	46
البند الثاني: جهود الأوروبية لمكافحة الجريمة الإلكترونية.	47
أولا: منظمة التعاون الاقتصادي والتنمية	47
ثانيا: جهود مجلس الأوروبي (معاهدة الأوروبية)	48
الفرع الرابع: أهم الإتفاقيات والمنظمات لمواجهة الجرائم المعلوماتية	49
البند الأول : اتفاقية بودابست	49
البند الثاني : اتفاقية برنا لحماية المصنفات الأدبية والفنية	50
البند الثالث: جهود منظمة الأنتربول.	50
البند الرابع: جهود الاتحاد الإفريقي و مجموعة الدول الثمانية G8	51
أولا : جهود الإتحاد الإفريقي	51
ثانيا: جهود مجموعة الدول الثمانية G8	52
المطلب الثاني : الجهود العربية المبذولة لمواجهة الجرائم الإلكترونية	53
الفرع الأول : مكافحة الجرائم على المودى مستوى الدول العربية	53
الفرع الثاني: اتفاقية العربية لمكافحة الجرائم التقنية المعلومات	54
الفرع الثالث : نظام الملكية الفكرية العربية بوجه عام.	55
المبحث الثاني: المكافحة التشريعية للجريمة الإلكترونية فى الجزائر	57
المطلب الأول : مواجهة الجرائم المعلوماتية بموجب قوانين عامة	57
الفرع الأول: مواجهة الجريمة الإلكترونية من خلال قانون الدستوري والقانون المدني	57
الفرع الثاني : مواجهة الجريمة الإلكترونية من خلال قانون الدسوري وقانون المدنى من حلال في العقوبات	59
المطلب الثاني: مواجهة الجرائم الإلكترونية بموجب قوانين وهيئات	62

خاصة	
الفرع الأول: الحماية الجزائية المعلوماتية من خلال نصوص الملكية الفكرية	62
الفرع الثاني : مكافحة الجرائم الإلكترونية وفق قوانين 04/09 و15/ 04.وقانون 04/18 و07/18.	64
البند الأول: قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة با الإعلام والإتصال	64
البند الثاني : 15/ 04 المتعلق بالتوقيع والتصديق الالكتروني	65
البند الثالث : 04/18 المتعلق بالقواعد العامة بالبريد و التصالات – قانون رقم 18/07 المتضمن حماية الأشخاص الطبيعين في مجال معالجة المعطات	66
الفرع الثالث : الهيئات الخاصة لتحدى الجرائم الإلكترونية	67
– الهيئة القضائية الخاصة للبث في الجرائم إلى الإلكترونية	67
– الهيئة الوطنية للوقاية من جرائم المتصلة بالتكنولوجيا الإعلام والاتصال	67
الخاتمة	71
قائمة المصادر والمراجع	74
الفهرس	80

الملخص:

مرت الجريمة السيبرانية بعدة مراحل تاريخية مختلفة ووصلت إلى مستوى عالٍ من التطور ومع تطور التكنولوجيا وتغيرها بات من الصعب إيجاد مفهوم موحد لها في التشريع فتعريفها يتأرجح بين واسع وضيق ، لكن الأحدث لا توجد تفرقة من حيث طرق معالجتها ومكافحتها.

أما المشرع الجزائري فقد تناول تعريف الجريمة الإلكترونية ووصفها بأنها جريمة ضد أنظمة معالجة البيانات الآلية. أما بالنسبة للعناصر المكونة لهذه الجريمة ، فلا فرق فيها عن العناصر الإجرامية التقليدية المعروفة والمتجسدة في الأركان القانونية ، أي النصوص القانونية ذات الأدلة الجنائية. أما الركن المادي فهو فعل إجرامي منصوص عليه في النص القانوني ويدور ركنه المعنوي حول القصد الجنائي لهذه الجريمة.

وفي الأخير نقول إن الجريمة الالكترونية مهما تمت مكافحتها فهي متطورة بتطور وسائل التكنولوجيا.

الكلمات المفتاحية: الجريمة الإلكترونية،اثبات الجريمة الإلكترونية،التعاون الدولي في مجال الجريمة الإلكترونية.

Abstract :

Cybercrime has gone through several different historical stages and has reached a high level of development. With the development and change of technology, it has become difficult to find a unified concept for it in the legislation.

As for the Algerian legislator, he dealt with the definition of electronic crime and described it as a crime against automated data processing systems. As for the constituent elements of this crime, there is no difference in them from the traditional criminal elements known and embodied in the legal pillars, that is, the legal texts with forensic evidence. As for the material element, it is a criminal act stipulated in the legal text, and its moral element revolves around the criminal intent of this crime.

At the end, we say that cybercrime, no matter how much it is combated, is advanced with the development of technology.