وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم: قانون العام **المرجع:**

مذكرة نهاية الدراسة لنيل شهادة الماستر

الإطار القانوني والمؤسساتي لمواجهة الجريمة السيبرانية في الجزائر

الشعبة: الحقوق. **التخصص:** قانون جنائي وعلوم جنائية

من إعداد الطالبة: **تحت إشراف الأستاذة:**

رمضان يسرى سي مرابط شهرزاد

أعضاء لجنة المناقشة

الأستاذ(ة)..... طواولة امينة .....رئيسا

الأستاذة: ..... سي مرابط شهرزاد .....مشرفا مقررا

الأستاذ(ة)..... زعيمش حنان .....مناقشا

السنة الجامعية: 2024-2025

نوقشت يوم: 22-06-2025

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: رمضان يسرى الصفة: طالبة جامعية

الحامل لبطاقة التعريف الوطنية رقم: ..... والصادرة بتاريخ: 2021.08.07

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون العام

والمكلف بإنجاز مذكرة ماستر بعنوان:

الإطار القانوني والمؤسساتي لمواجهة الجريمة السيبرانية في الجزائر

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: نظرا لتصديق على إمضاء

إمضاء المعني

السيد: رمضان يسرى

ب بـ

الصادرة

بلدية

للسنة

2025 جوان 26

نائب رئيس المجلس الشعبي البلدي
وبتفويض منه : عربية بن ذهيبة
متصرف القسم رئيسي

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

بسم الله الرحمن الرحيم

الإهداء

بسم الله الرحمن الرحيم

والحمد لله الذي لا هادي إلا هو ولا معينا إلا سواه له الفضل والشكر على كل من طلب بعلمه مرضاة الله

أهدى ثمرة جهدي ونجاحي إلى ملاكي الحامي ومملكة حياتي سعادتي إلى من كانت قوتي وعزمي وسندي إلى أحسن امرأة في العالم ودعائها كان سيلا الإنارة دربي أمي الغالية

والى من علمني العطاء إلى من تحت شخصيتي ووقف وراء ظهري دائما أبي العزيز

إلى من بذلوا جهدا في مساعدتي وكانوا خير سند إخواني الأعزاء والأخواتي الغاليات

وأتقدم بخالص تحياتي وتقديري وإشادتي لجميع الأساتذة المحترمين على كل ما قدموه لمساعدتي في أن أصبح ما أنا عليه اليوم.

إلى كل من ساهم ولو بحرف في مشواري الجامعي أصدقائي وزملائي

إلى كل هؤلاء : أهدي هذا العمل، أسأل الله تعالى أن يتقبله خالصا.

رمضان يسرى

الشكر و التقدير

بعد الحمد والثناء على الله سبحانه وتعالى ، بمنه علينا، بتوفيقنا في إتمام هذا البحث، لا يسعنا إلا أن نتقدم بجزيل الشكر والتقدير الى الأستاذة الفاضلة الدكتورة سي مرابط شهرزاد على تفضلها بالإشراف على هذا العمل وما قدمته لنا من توضيحات و تصويبات خلال إعداد هذه المذكرة فجزاها الله عنا خير جزاء وجعل مجهوداتها في ميزان حسناتها.

كما نتقدم بالشكر الجزيل للأساتذة الدكاترة أعضاء لجنة المناقشة على تكبدهم عناء مناقشة هذه الرسالة داعين المولى عز وجل أن يوفقهم في مشوارهم العلمي و المهني و الإجتماعي.

كما نتقدم بالشكر الجزيل الى كل من ساعدنا في إنجاز هذا العمل.

قائمة المختصرات

ج ر ج ج : جريدة رسمية للجمهورية الجزائرية

ق.ع:قانون العقوبات

ص: صفحة

ط: طبعة

مج: مجلد

ب س ن: بدون سنة نشر

ع:العدد

ج: الجزء

د ب ن:بدون البلد النشر

ص ص:من الصفحة إلى الصفحة

مقدمة

تميز القرن العشرين باختراعات هائلة على المستوى التقني، خاصة بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات، حتى أصبح يعرف بقرن المعلوماتية. أصبحت المعلوماتية وأدواتها وسائل ضرورية في العمليات البنكية، سجلات الشركات وعلاقات الدولة مع الأفراد، حيث ترك الحاسب الآلي بصمات واضحة في تطوير العديد من الأنشطة اليومية من حيث المضمون والشكل والزمن والمسافة.

شهد القرن العشرين تطوراً كبيراً في أجهزة الكمبيوتر بدءاً من الحواسيب التماثلية في بدايات القرن، مروراً بأجهزة الكمبيوتر التي استخدمت الترانزستورات في الخمسينيات والستينيات، ثم الدوائر المتكاملة التي أدت إلى ظهور الحواسيب الشخصية في الثمانينيات والتسعينيات، وصولاً إلى الحوسبة المتنقلة والإنترنت في أواخر القرن والعقد الأول من القرن الحادي والعشرين.

كما ساهم تطور الكمبيوتر في جعل المعلومات متاحة بسرعة ودقة عالية، مما غير حياة الناس وطرق عملهم وتواصلهم بشكل جذري، وأدى إلى ظهور شبكة الإنترنت التي فتحت فضاءات جديدة للحوار والتواصل عبر الفضاء الافتراضي.

باختصار القرن العشرين كان عصر انفجار المعلومات وثورة الاتصال، حيث أصبحت تكنولوجيا المعلومات والاتصالات عنصراً لا غنى عنه في كل النشاطات السياسية، الاقتصادية الاجتماعية والعلمية.

وعلى الرغم من أهمية الوسائل الإلكترونية وإيجابيات إستعمالها، إلا أن الإستخدام غير المشروع لها، قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية – أو الجرائم المعلوماتية أو جرائم الأنترنت ، وهذه المصطلحات كلها تعبر عن مجموعة الجرائم المرتبطة بالأنظمة الإلكترونية والشبكة المعلوماتية وخصوصا على شبكة الأنترنت[1].

وفي عصر التكنولوجيا أصبحت مسائل الدفاع السبيراني هي أحد أولويات الدفاع الوطني، حيث أصبح الأمن المعلومات أهمية كبرى في الدفاع على الدولة من أي هجوم الكتروني قد

[1]– عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة دكتوراه جامعة نايف للعلوم الأمنية، كلية الدراسات العليا،2010،ص12

تتعرض الأنظمة التشغيلية لها من أي قرصنة إلكترونية، وقد أعلنت 130 دولة حول العالم عن قيامها بتخصيص بعض الأقسام للأمن السيبراني، هذا بالإضافة إلى بعض الطرق الأخرى التي تفرضها الدول كعقاب للجرائم الإلكترونية, وتعتبر الجرائم السيبرانية من أكثر الجرائم خطورة على الأمن القومي للدول، وهي من الجرائم التي تباينت تسميتها عبر المراحل الزمنية نظرا لتطورها، فكان يعبر عنها بداية بمصطلح إساءة استخدام الكمبيوتر أو الحاسب الآلي، مرورا باصطلاح احتيال الكمبيوتر، والجريمة المعلوماتية أو الإلكترونية، فاصطلاح جرائم الكمبيوتر ، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الإنترنت، إلى آخر المصطلحات الجرائم السيبرانية.

في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى من حزمة من التشريعات والآليات القانونية والمؤسساتية للتصدي لهذه الجريمة التي أصبحت تسمى في الأدبيات الأكاديمية بالجريمة الالكترونية أو الجريمة السيبرانية.

والجزائر إحدى هذه الدول التي لم تكن في منأى من تداعيات هذه الظاهرة، حيث انتشرت في الآونة الأخيرة جرائم تمس بالحياة الشخصية للمواطن وتمس أيضا بأمن واستقرار البلاد وبكل جوانب الحياة الأخرى اقتصاديا سياسيا ثقافيا، ومست حتى البناء المجتمعي في تركيبته وبنايته.

من هذا سعى المشرع الجزائري إلى سن العديد من التشريعات والقوانين للتصدي لهذه الجرائم السيبرانية وأهم هذه التشريعات القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وغيره من التشريعات التي تدعم الحد من انتشار هذه الجرائم . وصولا إلى تعديل قانون العقوبات رقم 24-06 الذي تطرق بدوره الى بعض الجرائم الالكترونية.[1]

تم إجراء هذا البحث لتوضيح الأسس العامة والأفكار التفصيلية المتعلقة بظاهرة الجريمة السيبرانية. **يهدف البحث** إلى فهم المفهوم العام للجريمة السيبرانية، وطبيعتها، ومكوناتها الفريدة، بالإضافة إلى الأسس الأساسية للمكافحة الجنائية لهذه الظاهرة وكيفية الوقاية منها. يتناول البحث

[1]- عمر بن محمد العتيبي،المرجع السابق،ص13

دراسة البيئة التي يحدث فيها الجرم السيبراني وأشكاله وصوره في الساحة العملية. كما يسلط الضوء على المفاهيم الجديدة المرتبطة بهذه الظاهرة، مثل المجني السيبراني والمجني عليه السيبراني ، والبيئة السيبرانية (بيئة الجريمة السيبرانية)، والسلوك الجنائي التقني. يتناول البحث أيضا التحليل الشامل للأنماط والأشكال التي تتبعها جرائم الإنترنت.

فهذا البحث يسعى إلى تحقيق اهداف التالية:

– التعرف بواقع الجرائم السيبرانية وانماطها المرتكبة، ومن ثم التعرف على مخاطرها والآثار التي نجمت عنها.

–اقتراح الآليات المناسبة لرفع كفاءة الأجهزة المختصة وفاعليتها في مواجهة الجرائم السيبرانية.

قد تكمن **أهمية هذا الموضوع** في أن الجرائم السيبرانية تعتبر من الجرائم المستحدثة التي تمثل خطرا وتهديدا كبيرا على الفرد والمجتمع وكذلك على الأجهزة الأمنية للدولة، مما يجب علينا أن نتطرق لدراستها لمكافحة هذه الجرائم من وضع الأنظمة والعقوبات الرادعة، والتصدي لهجمات المجرمين ومحاكمتهم أمام القضاء.

ومن أسباب اختيار الموضوع:

–الأسباب الذاتية:

–أن مجرد اسمها يكتسي جانب من الغموض خصوصا في إطار مكافحتها.

–حب الاستطلاع في هذا النوع من الجرائم التي لم يكن لها سبق في القرون السابقة والتي ارتبطت بشكل كبير بظهور تكنولوجيا الإعلام الآلي وانتشار شبكات التواصل الاجتماعي وبكل أنواعها.

–الرغبة في الوقوف على حقيقة التعامل مع الجريمة الإلكترونية من الناحية الإجرائية فالكثير من الدراسات التي تطرقت هذه الجرائم بائت تركز عن الجانب الموضوعي فقط.

-والأسباب الموضوعية:

- كون أن الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش.

-الجريمة الالكترونية تجدها تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية

-معرفة آليات المشرع الجزائري للتصدي للإجرام الإلكتروني.

وعليه تتمحور الاشكالية الاساسية لدراستنا في:

ماهية الجريمة السيبرانية؟ وفيما تتمثل الآليات القانونية والمؤسساتية التي تعتمدها الجزائر لمكافحة هذا النوع من الجرائم؟

بناء على ما تقدم فقد اعتمدنا في دراستنا هذه على **مناهج** نرى أنها تتلاءم مع طبيعة الموضوع، حيث استعنا **بالمنهج الإستقرائي** والذي يظهر في استقراءنا للمواد القانونية ذات العلاقة التي تفرض بعد ذلك تحليلها من خلال استعانتنا **بالمنهج التحليلي** تباعا، أما **المنهج الوصفي** فيظهر في تناولنا الاطار المفاهيمي الموضوع الدراسة.

للإجابة على الإشكالية الرئيسية للموضوع، مع ما ينبثق عنها من إشكالات فرعية، قمنا بتقسيم الدراسة إلى مقدمة، فصلين، خاتمة.

خصصنا **الفصل الأول** لدراسة كل ما يتعلق **الإطار المفاهيمي للجريمة السيبرانية** من خلال مبحثين حيث تناولنا في المبحث الأول ماهية الجريمة السبيرانية ، أما المبحث الثاني فتناولنا تصنيفات الجريمة السيبرانية .

أما **الفصل الثاني** فقد تطرقنا فيه **إلى الأحكام القانونية و الأجهزة المختصة لمكافحة الجريمة السيبرانية** وذلك من خلال تقسيمه إلى مبحثين في المبحث الأول بعنوان مكافحة جريمة السيبرانية من خلال النصوص القانونية، وفي المبحث الثاني مكافحة جريمة السيبرانية من خلال الأجهزة المختصة بها.

وأنهيت البحث بخاتمة تضمنت النتائج المتوصل إليها ثم ما تراء لنا بعد الدراسة من اقتراحات

الفصل الأول:

الإطار المفاهيمي للجريمة السيبرانية

لقد أثبت الواقع العملي أن الدولة لا تستطيع وحدها القضاء على الجريمة المعلوماتية بسبب تطورها السريع وعبر الحدود الدولية، مما يستدعي وجود كيان دولي يتولى هذه المهمة ويعزز التعاون بين الأجهزة الأمنية في الدول المختلفة لتبادل المعلومات بسرعة وتعقب المجرمين الهاربين.

هناك اتفاقيات دولية مثل الاتفاقية الجديدة المعنية بمكافحة الجريمة السيبرانية التي اعتمدتها الأمم المتحدة لتعزيز التعاون الدولي في هذا المجال[1]، كما توجد معاهدات ثنائية وإقليمية ومتعددة الأطراف تسهل تبادل الأدلة والمساعدة القانونية المتبادلة وتسليم المجرمين، مثل الاتفاقية العربية لجامعة الدول العربية واتفاقية الاتحاد الأفريقي للأمن السيبراني.

كما يلعب الانتربول دوراً محورياً في تسليم المجرمين المطلوبين دولياً وتتبعهم، مما يعزز مكافحة الجرائم الإلكترونية العابرة للحدود ، مما يؤكد أن التعاون الدولي هو ركيزة أساسية لمكافحة الجرائم المعلوماتية بفعالية، من خلال تبادل المعلومات بسرعة وحماية الأدلة الرقمية، وتسليم المجرمين، وهذا يتطلب مؤسسات دولية متخصصة وآليات تعاون قانونية وتقنية متطورة.[2]

ان الجريمة السيبرانية، المعروفة أيضاً بجرائم التكنولوجيا الرقمية أو الجرائم الالكترونية تشير إلى الأنشطة الإجرامية التي تتم باستخدام التكنولوجيا الرقمية وشبكات الإنترنت من خلال الأنشطة غير القانونية التي تستهدف الأفراد الشركات، والحكومات ،[3] نتناول في هذا الفصل الخاص بالاطار المفاهيمي للجريمة السيبرانية: في (المبحث الأول) **ماهية الجريمة السيبرانية** حيث يتم تعريفها وتوضيح خصائصها وأنواعها وفي (المبحث الثاني) نستعرض **الجوانب الإجرائية للمسؤولية الجنائية في الجريمة السيبرانية**، من خلال تحديد الاستدلال في الجريمة السيبرانية والتطرق إلى التحقيق في الجريمة السيبرانية وإجراءات المحاكمة فيها المطلب الثاني.

---

[1] – اتفاقية الامم المتحدة لمكافحة الجرائم السيبرانية ، مؤرخة في 25ديسمبر 2024.

[2]- سليمان أبو نمر ،يوسف بوكشريدة،مكافحة الجريمة المعلوماتية في إطار القانون الدولي،تخصص قانون دولي عام ،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد خيضر بسكرة،2020-2021،ص1

[3]– نورهان محمد الربيعي ،الجريمة السيبرانية و آليات مكافحتها (دراسة مقارنة)،مجلة الفارابي للعلوم الإنسانية ،مج 3،ع 1، 2024، الإمارات العربية المتحدة ،ص73

المبحث الأول : ماهية الجريمة السيبرانية

باتت الجرائم السيبرانية نوع جديد من أنماط الجريمة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم ، إذا ما تركت على الأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية المواجهة تلك الجرائم والعمل على محاربتها خاصة جهود الأمم المتحدة، منها اتفاقية بودابست لمكافحة الجرائم السيبرانية، واتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم نظرا لما تتمتع به تلك الجريمة من خاصية اللاحدودية.[1]

فالجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة.

إذ أنها تتقدم بوتيرة سريعة باستخدام المجرمون أحدث التقنيات في تنفيذ هجماتهم السيبرانية ، لذا كان علينا مواكبة القضاء السيبراني والتعرف على طرق التصدي لهذه الجرائم المستحدثة بسن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية وفرض العقوبات على المجرمين[2].

سنتطرق في المطلب الأول مفهوم الجريمة السبيرانية وفي المطلب الثاني الطبيعة القانونية للجريمة السيبرانية و أركانها.

المطلب الأول : مفهوم الجريمة السيبرانية

ان مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات.

---

[1]– قطاف سليمان ، بوقرين عبد الحليم،مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية،مجلة البحوث القانونية و الاقتصادية،مج 5،ع2،الأغواط. الجزائر. 2022،ص62

[2]– روان بنت عطية الله الصحفي ،الجرائم السيبرانية،المجلة الإلكترونية الشاملة متعددة التخصصات،ع24،جدة المملكة العربية السعودية.2020، ص1.5.6

وكذلك نجد كلمة سيبراني قد ارتبط بالأمن الالكتروني فأصبحنا نعتمد مصطلح الأمن السيبراني وذلك انطلاقا من مسمى الهيئة الوطنية للأمن السيبراني.

لذلك فإن مصطلح الجرائم السبيرانية في المجتمع العربي هو مصطلح عصري وحديث الجرائم الانترنت، فكان من الضروري التطرق له في الأبحاث والرسائل الأكاديمية[1].

الفرع الأول:تعريف الجريمة السيبرانية

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها ، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر ، مرورا باصطلاح احتيال الكمبيوتر ، والجريمة المعلوماتية ، فاصطلاحات جرائم الكمبيوتر ، والجريمة المرتبطة بالكمبيوتر ، وجرائم التقنية العالية ، إلى جرائم الهاكرز ، فجرائم الإنترنت ، إلى آخر المصطلحات الجرائم السيبرانية.

أولا: تعريف الجريمة السيبرانية لغة:

- **الجريمة** في اللغة لها معنيين هما:

الأول : الذنب ، نقول جرم وأجرم ، وأجترم بمعنى واحد.

الثاني : الجناية ، كقولهم جرم إليهم وعليهم جريمة ، أجرم جني جناية وجرم إذا عظم جرمه أي أذنب[2].

- **الجريمة السيبرانية لغة:**

(cyber) هي كلمة انجليزية ، حيث عرف قاموس أكسفورد كلمة سيبراني أو Cyber ، بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي[3].

---

[1]– عبد العزيز بن غرم الله آل جار الله ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة ويليه آثار العولمة على مستخدمي الإنترنت ، دار الكتاب الجامعي ، الرياض ، ط الأولى ، 2018م،ص 80

[2]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج الخضر، باتنة ، الجزائر ، 2013،ص65

[3] – سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية ، بدون طبعة ، 2008 ، ص12 4

ثانيا: التعريف الجريمة السيبرانية إصطلاحا

يستعمل مصطلح السيبرانية لوصف فكرة جزء من الحاسوب أو عصر المعلومات، أما الجريمة السيبرانية هي التجاوزات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة، وبقصد تشويه سمعة الضحية أذى مادي أو عقلي، مباشر أو غير مباشر، باستخدام شبكات الاتصال ومواقع المتواصل الاجتماعي مثل الانترنت (غرف الدردشة والبريد الإلكتروني والموبايل).[1]

كما تعرف الجريمة الإلكترونية بأنها: "مجموعة من الأفعال والأنشطة المعاقب عليها قانونا، والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"[2]

ومن التعريفات كذلك نذكر: "أنها كل فعل ضار بالآخرين عبر الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصال الهاتفية، شبكة نقل المعلومات، شبكة الانترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموما"[3].

ثالثا : التعريف الشرعي للجريمة:

تعرف الجريمة بأنها " إتيان فعل محرم معاقب على فعله ، أو ترك فعل محرم معاقب على تركه ، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه[4].

– [1] ذياب موسى البداينة، ورقة علمية بعنوان: الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، المملكة الأردنية الهاشمية،2013 ص: 03.

–3 محمود مدين: الجريمة الإلكترونية وتحديات الأمن القومي، دكتوراه في القانون الدولي العام، ط2، المصرية للنشر والتوزيع، ص:[2]59

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة الإلكترونية، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، 2013، ص: 51.

[4] – عبد العزيز بن غرم هللا ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة، (ويليه آثار العولمة على مستخدمي الإنترنت ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، 2018 ، ص 71.

رابعا : التعريف القانوني للجريمة السيبرانية:

عرف الجريمة من الناحية القانونية بعدة تعريفات منها : " هي إتيان فعل أو تركه عن إرادة جنائية إضرارا بمصلحة اجتماعية حماها المشرع بقواعد تجرمه وتعاقب عليه جزائيا .[1]

ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفا جديدا، ففقهاء القانون لم يستقروا على تعريف واحد ، فنحن لا نستنكر ذلك أبدا لأنه من الطبيعي جدا أن يكون هذا الاختلاف وهذا التنوع في المفاهيم والآراء، وذلك يرجع الحداثة الجرائم السيبرانية و لاختلافات الثقافات والقوانين بين الدول ، وأيضا خشية في أن يحضروا المصطلح في نطاق ضيق أو محدد.

فمنهم من عرف الجرائم السيبرانية : بأنها هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما.

والبعض الآخر عرفها : بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"

ومنهم من عرفها بأنها : " هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية فهي جرائم العصر الرقمي التي تطال بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية[2]."

وبناء على هذا التعاريف السابقة أصبح تعريف الجريمة السيبرانية أكثر توسعا فإنه يشمل دخول الأجهزة الالكترونية المعاصرة غير الكمبيوتر ضمن الحاسب الآلي ، وكذلك ارتباطها بالشبكات الخاصة والعامة والعالمية أيضا ، إلا أن هناك من ميز جرائم الإنترنت عن الهواتف الخلوية من حيث العالم الافتراضي فجرائم الانترنت لا تقع إلا عن طريق الفضاء السيبراني بالاعتداء على

[1]– روان بنت عطية الله الصحفي ،المرجع السابق، ص6.7.8.9

[2]– بدري فيصل ، مكافحة الجريمة في القانون الدولي والداخلي ، أطروحة دكتوراه في القانون العام كلية الحقوق، جامعة الجزائر – 2018،ص ص87.88

البيانات أما الهواتف الخلوية فإن وقوع الجريمة قد يتعدى من عالم البيانات إلى العالم المادي الواقعي ، ويكون محل الجريمة أو المجني عليه هو كيان مادي ملموس[1].

الفرع الثاني : خصائص الجريمة السيبرانية

الجرائم السيبرانية تتميز بخصائص فريدة تجعلها مختلفة عن الجرائم التقليدية تلك الفروقات تعود إلى سماتها الفريدة والعناصر التي تشكلها، بالإضافة إلى الأدوات والوسائل التي يستخدمها الجرائم السيبرانية في تنفيذها، وتتمثل هذه الخصائص بأنها جرائم تتم عبر التقنيات التكنولوجية الحديثة، وعلى رأسها شبكة الانترنيت التي تعتبر كوسيلة ارتكابها.

أولا: من حيث الهدف.

تستهدف الجرائم السيبرانية الأنظمة المعلوماتية من خلال اختراقها بهدف تلاعب أو تشويه المعلومات والبيانات الخاصة بمستخدمي البيئة الرقمية، على غرار ما يحدث في الجرائم التقليدية.

الجريمة السيبرانية تعتبر جريمة ناعمة بسبب خفتها وصعوبة اكتشافها، حيث قد لا يلاحظ الشخص المتضرر ارتكابها الثناء تواجده على الشبكة الجاني يمتلك مهارات تقنية متقدمة تسمح له بالقيام بتلك الجرائم دون أن يتم الكشف عنها، مثل سرقة الأموال أو إرسال فيروسات ضارة إلى البرامج وأجهزة الكمبيوتر.

ثانيا: صعوبة اكتشافها

تعتبر الجريمة السيبرانية من الجرائم التي يصعب اكتشافها ولذلك لعدم تركها الآثار مادية يمكن من خلالها كشف مرتكبها هذه الأخيرة مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية، مما يجعل أمر طمس هذا الدليل الإلكتروني ومحوه كليا من قبل الفاعل أمر في غاية السهولة .[2]

[1]– نورهان محمد الربيعي ،المرجع السابق، ص ص67.68

[2]– قطاف سليمان ، المرجع السابق ، ص ص69.70

ثالثا:جريمة ذات بعد دولي تعد الجريمة السيبرانية.

جرائم عابرة للحدود لا تعترف بعنصر الزمان والمكان، فهي تتميز بالتباعد الجغرافي واختلاف التواقيت بين الجاني والمجنى عليه، وهذا راجع الى المجتمع الذي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح على الشبكات تخترق الزمان والمكان دون أن تخضع الحرس الحرس الحدود.

تعتبر جرائم السيبرانية من بين الجرائم التي يتطلب المام مرتكبها بجوانب التقنية وكذلك الخبرة الفائقة في استخدام الحاسبة الآلي.

رابعا: صعوبة ضبط وتوصيف الجرائم السيبرانية.

أن من بين الصعوبات التي تواجه ضباط الشرطة القضائية والمحققين وكذا القضاء خاصة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية وإضفاء الوصف القانوني المناسب لها، ولعل المراد ذلك إلى الطبيعة الخاصة التي تتميز بيها هذه الأخيرة[1].

الفرع الثالث: أنواع الجريمة السيبرانية

تتنوع الممارسات التي تهدد الأمن السيبراني، يتنوع أهدافها، كما ويتنوع الجهات التي تعتمدها ويمكن ايراد بعضها على الشكل الآتي:

أولا- التعرض لسرية الاتصالات:

من خلال الدخول إلى الأنظمة للاطلاع على المعلومات دون اذن ويشابه هذا التنصت على المخابرات الهاتفية والاطلاع على البريد الشخصي ودخول المنازل لتفتيشها، ما يتطلب عادة وبحسب القواعد القانونية اذنا مسبقا من قبل السلطات المختصة في البلاد التي تقوم على احترام القاعدة القانونية، وتعتبر هذه الأعمال في غير تلك الحالة سواء قام بها الأفراد أو قامت بها السلطات العامة جرائم اعتداء على الحريات والحقوق الشخصية.

ثانيا: التلاعب بالمعلومات الموجودة في نظام معين وتشويهها أو اتلاقها:

[1]- قطاف سليمان ، المرجع نفسه،ص70

وذلك سواء عبر الاقتحام اليدوي أو عبر ارسال برامج وفيروسات متخصصة بذلك، ففي هذا اعتداء على الملكية وعلى حقوق التمتع والتصرف بها يضاف إلى ذلك التعرض لسلامة عمل المواقع الشخصية منها والتجارية عندما تتوفر نية الأضرار بغض النظر عن تحقق الضرر المرجو أم لا، الجرائم العادية التي تستخدم الانترنت في تنفيذها، كالسرقة والغش والخداع والتغرير بالقاصرين وتسهيل الدعارة والترويج لنشاطات مخالفة للقانون والاعتداء على الملكية الفكرية، فكل هذه جرائم تعاقب عليها القوانين الوضعية ويميل إلى القول هنا انها لا تتطلب بالضرورة إقرار نصوص جديدة بل تعديل ما هو موجود ليتناسب مع العناصر المادية الجديدة التي يدخلها الفضاء السيبيري من خلال طبيعته الخاصة[1].

ثالثا: الجرائم التي تندرج في إطار الجريمة المنظمة:

هي الجرائم التي تهدد أمن الأفراد والدول على السواء في الفضاء السيبراني وفي الفضاء التقليدي، وتأتي في هذا الإطار جرائم تبييض الأموال والإرهاب والجرائم السيبرانية .[2]

رابعا: الاعتداء السيبراني على حقوق الملكية الفكرية:

ويكون بالاعتداء على العلامات التجارية وبراءات الاختراع ، وكذلك نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص فهو اعتداء على الحقوق المالية والحقوق الأدبية[3].

خامسا : الانتحال والتغرير السيبراني.

أ-انتحال شخصية فردية : بسبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ

[1]- سعيداني نعيم، المرجع السابق،ص70

[2]- غانم مرضي الشمري، الجرائم المعلوماتية ، الدار العلمية الدولية ، عمان ، ط الأولى ، 2016م ، ص 52

[3]- روان بنت عطية الله الصحفي ،المرجع السابق، ص19.21

رمزي لجهة خيرية، وهذا يتطلب الإفصاح عن معلومات سرية الأمر الذي يؤدي الى استيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو الاساءة إلى سمعة الضحية.

ب-انتحال شخصية المواقع : و يكون باختراق حاجز أمني وتتم عملية الانتحال بهجوم يشته المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور[1] .

سادسا : الابتزاز والتهديد السيبراني

من خلال نشر صور أو معلومات صحيحة أو غير صحيحة عن المجني عليه بهدف الحصول على المال أو علاقة غير مشروعة.

سابعا:الاعتداء السيبراني على الأمن

كإنشاء موقع المنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات ، أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية ، والدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني[2].

المطلب الثاني : الطبيعة القانونية للجريمة السيبرانية وأركانها

باتت الجرائم السيبرانية نوع جديد من أنماط الجريمة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم ، إذا

[1]- سعيداني نعيم، المرجع السابق،ص71

[2]- قطاف سليمان ، بوقرين عبد الحليم،المرجع السابق،ص62

ما تركت على الأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها خاصة جهود الأمم المتحدة، منها اتفاقية بودابست لمكافحة الجرائم السيبرانية، واتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين[1] .

الفرع الأول : الطبيعة القانونية للجريمة السيبرانية ووسائل ارتكابها

إن طبيعة الجرائم السـيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى الوسـط الذي ترتكب فيه الجريمة وهي الأداة أو الوسـيلة التي اسـتخدمها الجاني في ارتكاب فعله غير المشـروع، وتتطلب توفر معرفة أو حد ادني من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي ينشـأ بارتكاب فعل حرمه القانون أو الامتناع عن فعل أمر به القانون، وتتجه إرادة الجاني إليه رغم وجود نص قانوني يجرم السلوك.[2]

أولا: الطبيعة القانونية للجريمة السيبرانية

الحديث حول الطبيعة القانونية للجريمة السيبرانية يركز على الوضع القانوني للبرامج والمعلومات وما إذا كانت لها قيمة في ذاتها أم تعتبر مستحدثة من القيم القابلة للاستئثار يشير إلى أن الجرائم السيبرانية تختلف عن الجرائم العادية بسبب ارتباطها بالقانون الجنائي السيبراني، حيث تتم داخل نطاق المعالجة الإلكترونية للبيانات. يذكر أن هذه الجرائم تشمل تجميع وتجهيز وإدخال البيانات للحصول على معلومات، وتحدث في مجالات مثل معالجة الكلمات والنصوص. ويشير إلى أن الجاني يتعامل مع برامج وبيانات جديدة كمحل للاعتداء أو وسيلة له يؤكد على أهمية تحديد الطبيعة القانونية للجريمة السيبرانية بسبب المال المعلوماتي وتقسيمه إلى نوعين معلوماتية ذات طبيعة معنوية ومعلوماتية ذات طبيعة مادية. يشير إلى أن شبكة المعلومات الإنترنت تطرح تساؤلات حول نظام المسؤولية والتشريع لخدمات نشر المواقع وتبادل المعلومات فيها. ويشدد على أن القانون الملائم للجرائم السيبرانية يهدف إلى معرفة النصوص القانونية التي يجب تطبيقها على

[1]– نورهان محمد الربيعي ،المرجع السابق،ص81

[2]– مهدي رضا ،الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث و الدراسات، مج 6. ع 02 ،جامعة محمد بوضياف المسيلة،2021،ص114

خدمات نشر المواقع والمعلومات، ويشير إلى تحديات مثل مسألة الإثبات وصعوبة محاكمة المتجاوزين في حالة وجود تشفير للبيانات. يختتم بالتأكيد على ضرورة تحديد الطبيعة القانونية للجرائم السيبرانية بناءً على المجال الذي يمكن أن تحدث فيه أو المحل الذي يقع عليه الاعتداء[1].

ثانيا: وسائل ارتكاب الجرائم السيبرانية:

أ- التجسس التقني والمعلوماتي: تشكل أسلحة حرب سيبرانية مهمة تهدد الدول، وتتضمن أشكالا متعددة مثل التجسس على المعلومات من أجهزة الحواسيب والأقمار الصناعية والهواتف المحمولة[2] .

ب- الإختراق الإلكتروني: هي جريمة الكترونية تشمل إنشاء نظام أو برنامج للاستيلاء على معلومات الخصم وتدميرها، مع فساد النظام الحاسوبي والآلي، بهدف التفوق في الجوانب الأمنية والعسكرية والاقتصادية والسياسية.

ج- القرصنة الإلكترونية: هي سلاحا فتاكا في الفضاء الرقمي، حيث يتضمن هذا السلاح تقنيات الصراع الإلكتروني الحديثة، وتعتمد على تجنيد أفراد ماهرين في التعامل مع الحواسيب والأنظمة التقنية، لاختراق الأنظمة التكنولوجية، يُطلق على هؤلاء الأفراد الماهرين باسم الهاكرز[3].

د- الرسائل الصامتة: هي برامج تقنية تستخدم في الهواتف المحمولة من الجيل الرابع والخامس، ترسل دون أن يلاحظ صاحب الهاتف وتساعد على تحديد موقعه بدقة.

هـ- شبكات التواصل الاجتماعي: هي منصات رقمية تربط الأفراد والمجتمعات مع بعضها البعض في مجالات مثل العمل والدين وغيرها، تجمع بين مختلف الفئات العمرية والاجتماعية

---

[1]- عبد الصادق عادل، الحروب السيبرانية تصاعد القدرات والتحديات للأمن العالمي المركز العربي لأبحاث الفضاء الإلكتروني، د.دار النشر، القاهرة، 2017، ص2

[2]- جلعود وليد غسان سعيد . دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، أطروحة ماجستير في التخطيط والتنمية السياسية، بكلية الدراسات العليا، جامعة نابلس، فلسطين.2013.ص111

[3]- هادفي تاج الدين ،إستراتيجية الجزائري في مواجهة الجرائم السيبرانية التي تهدد أمنها السيبراني ،ملتقى الوطني الأمن السيبراني و رهانات الأمن الشامل في الجزائر ،مخبر التنمية الاجتماعية و خدمة المجتمع ،كلية العلوم الإنسانية و الإجتماعية ،جامعة الشهيد حمه لخضر الوادي ،يوم 13.14ماي2024،ص6

والاقتصادية والثقافية والتعليمية، وتلعب دوراً هاماً في الصراع التقني عبر الإنترنت بما يسمى الجرائم السيبرانية.

و- **الحقيبة الكهروستاتيكتة:** هي عبارة عن تكنولوجيا عسكرية تشكل أجهزة صغيرة تولد نبضات كهرومغناطيسية فائقة القوة، تستخدم لتعطيل الوحدات الإلكترونية في أي نظام أو محطة إرسال، مما يؤدي إلى فقدان قدراتها العلمية والإنتاجية والتشغيلية.

ر- **الأسلحة النانو تكنولوجية:** تشمل تصميم أجهزة دقيقة جدا في المجال العسكري تتسلل إلى أنظمة الحواسيب والتقنيات، حيث تستخدم لتدمير البنية المعلوماتية بسرعة عالية. مثل آليات عمل الفيروسات، بواسطة ما يُعرف بالميكروبات الرقمية[1]

الفرع الثاني : أركان الجريمة السيبرانية

وفقا للمفوضية الأوروبية فان الجرائم السيبرانية تشمل عدة أركان يمكن إيجازها فيما يلي:

أولا : الركن المادي

ويُعرف بأنه : " النشاط المادي الذي يصدر عن الجاني متخذا مظهرا خارجيا يتدخل من أجله القانون بتقرير العقاب. "

ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية [2]، بمعنى أن الركن المادي يتكون من ثلاث عناصر:

أ- **السلوك الإجرامي** : وصوره متعددة كالسلوك الإجرامي الإيجابي وذلك بمخالفته نصا ينهي عن الإتيان بهذا الفعل كسرقة بيت أو جهاز معين ، سواء كان التحرك الإيجابي بحركة واحدة كالقتل بالرصاص ، أو بحركات متعددة كالمشاجرة التي تنتهي بالوفاة.

وقد يكون سلبيا بمخالفة نص يأمر بإتيان فعل معين ، كامتناع ممرضة عن إعطاء جرعة الدواء لمريضها العاجر بما يؤدي لوفاته.

---

[1]- روان بنت عطية الله الصحفي ،المرجع السابق، ص22.23

[2]- سعيداني نعيم، المرجع السابق، ص72.73

وقد يكون السلوك الإجرامي بصورة بسيطة كما في جريمة القذف ، وقد تكون بصورة معقدة كما في جريمة الإرهاب أو السطو المسلح.

فالقانون الجنائي لا يعول كثيرا على الوسيلة التي ارتكبت بها الجريمة أو وقع بها السلوك الإجرامي ولا يعتد بزمان أو مكان وقوع الجريمة إلا عند تقديره للظروف المشددة أو المخففة ،

فيستوي القتل أن يكون بمسدس أو بالسكين ، أو حتى عن طريق الريموت كنترول أو بواسطة أجهزة الحاسوب.

فأهمية هذه الصور المجرمة والظروف المصاحبة لها تظهر مدى توافر القصد الجنائي[1].

ب- النتيجة الإجرامية : بناء على ما تم طرحه، نرى أن الجريمة السيبرانية تعتبر من فئة الجرائم ذات السلوك المجرد، حيث لا تتطلب نتيجة محددة ليتم تحقيقها بل تحدث بمجرد وقوع السلوك ذاته على سبيل المثال، يمكن اعتبار الإبلاغ عن جريمة سيبرانية كفعل جرمي بمفرده دون الحاجة إلى انتظار النتيجة مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل[2].

ج- علاقة السببية: يراد بعلاقة السببية، الصلة التي تربط بين الفعل السلوك الإجرامي والنتيجة الإجرامية، إذ يثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة[3] ، والسببية هذه أهميتها فهي التي تربط بين عنصري الركن المادي فتقيم بذلك وحدته وكيانه، فإذا انتفت هذه العلاقة كانت مسئولية مرتكب الفعل تقتصر على الشروع إذا كانت الجريمة عمدية وتوافرت عناصر هذا الشروع أما إذا كانت الجريمة غير عمدية فلا يسأل مرتكب الفعل لأنه لا شروع في الجرائم غير العمدية.

---

[1]- مرابطين حياة ، الجريمة الالكترونية في التشريع الجزائري، رسالة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية – جامعة عبد الحميد بن باديس2018.2019.ص13

[2]- محمود نجيب حسني، الفقه الجنائي الإسلامي، دار النهضة العربية، 2008.ص279

[3]- هدى سالم محمد الأطرقجي، التكيف القانون للجرائم في القانون العقوبات العراقي، رسالة لنيل درجة دكتوراه كلية القانون جامعة الموصل ،2000،ص101

وعلاقة السببية تبحث بشكل عام بالنسبة للجرائم المادية وليس الشكلية، وذلك الحصول النتيجة في الجرائم الشكلية بمجرد وقو السلوك الإجرامي في هذه الجرائم[1].

نظرا لأن الجريمة السيبرانية تندرج ضمن فئة الجرائم ذات السلوك المجرد، حيث يفرض المشرع عقوبة بمجرد وقوع الفعل، ويأتي ذلك نتيجة لتكامل النتيجة والعلاقة السببية في هذا النوع من الجرائم. وبمعنى آخر، لا يتوجب وجود العناصر الأخرى للجانب المادي كالنتيجة الجنائية والعلاقة السببية لتحقيق هذا النوع من الجرائم وتتطلب النتيجة دائما إسنادا ماديا ومعنويا . فالإسناد المادي يقتضي نسبة الجريمة لفاعل معين ونسبتها إلى الفعل، بالإضافة لنسبة الفعل إلى فاعل.

أما الإسناد المعنوي، فهو نسبة الجريمة إلى شخص متمتع بالأهلية اللازمة لتحمله المسئولية الجنائية، ويقتضى ذلك أن يتوافر لدي الفاعل الإدراك وحرية الاختيار، ويلاحظ أن الإسناد المادي والمعنوي من عناصر المسئولية الجنائية، إذ بغيرهما لا تقوم لها قائمة. ولا يختلف مفهوم علاقة السببية في الجرائم السيبرانية عن الجرائم العادية، لأن رابطة السببية – كما هو معلوم – ارتباط الفعل التقني غير المشروع بالنتيجة المجرمة ارتباط السبب بالمسبب ومن ثم فهي مرتبطة بالواقع الافتراضي الذي يتم عبر شبكة الإنترنت وترتب اثارها في الواقع المادي[2].

أولا: الركن المعنوي للجريمة السيبرانية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وبالنظر لما للركن المعنوي من أهمية أساسية في النظرية العامة للجريمة، إذ الأصل أنه لا جريمة بدون ركن معنوي، فهذا الركن هو سبيل المشرع إلى تحديد المسئولية عن الجريمة فإنه يتعين توافر الركن المعنوي في الجريمة السيبرانية بالرغم من أنها لا ترتكب في عالم مادي وإنما في عالم افتراضي، فيجب أن يكون الجاني عالما بأن الفعل الذي يأتيه أو سلوكه المادي يحرمه القانون.

[1]– رؤوف عبيد، السببية في القانون الجنائي ، مطبعة الاستقلال، الأردن، 1996.ص3

[2]– يوسف الصغير، الجريم المرتكبة عبر الأنترنيت، رسالة مقدمة لنيل درجة ماجستير في كلية الحقوق والعلوم السياسة، جامعة مولد معمر، الباري وزي 2003.ص321

وعلى الرغم من توافر هذا العلم لديه تتجه إرادته إلى إتيان هذا الفعل قاصدا تحقيق نتيجته المري، وقوام الركن المعنوي، هو الأصول النفسية الماديات الجريمة والسيطرة النفسية عليها، ومن ثم كان الركن المعنوي في جوهره قوة نفسية، وهذه القوة هي الإرادة إلا أن هذا الركن لا يتحقق بهذه الإرادة وحدها ما لم تتجه إلى إتيان فعل جرمه القانون إذن الإرادة هي جوهر الركن المعنوي، كما أنها دليل على خطورة شخصية الجاني، وهي مظهر لهذه الشخصية[1]، فإذا اتخذت هذه الإرادة صورة القصد الجنائي وصفت الجريمة بأنها عمدية، أما إذا اتخذت صورة القصد غير العمدي؛ فإن الجريمة توصف بأنها غير عمدية .

ويعتمد هذا التقسيم على أن الفاعل في الجريمة العمدية قد قام باقتراف فعله قاصدا ارتكاب السلوك المجرم الذي أتاه، كما أراد النتيجة الإجرامية التي حصلت منه أو أية نتيجة أخرى، بينما أن الفاعل في الجريمة غير العمدية لم يقصد سوى ارتكاب السلوك دون إرادة تحقيق النتيجة الإجرامية. وعلى هذا الأساس يتبين أن الركن المعنوي في ضوء القواعد العامة يتخذ صورتين "القصد الجنائي" و "الخطأ غير العمدي"، [2]وسنحاول تطبيق هاتين الصورتين على عناصر الركن المعنوي في الجريمة السيبرانية، وذلك على النحو الآتي:

أ- **الجريمة سيبرانية كجريمة عمدية** :بناء على ما تم ذكره سابقا، يتضح أن القصد الجنائي يشير إلى معرفة عناصر الجريمة، ووجود إرادة موجهة نحو تحقيق تلك العناصر والموافقة عليها. يمكن تطبيق هذا التعريف على القصد الجنائي بجميع أشكاله، سواء كان القصد مباشرا أو احتماليا. ويوضح هذا التعريف، أن القصد الجنائي يقوم على عنصرين، وهما العلم» و «الإرادة»، غير أن العنصر الإرادة أهمية تفوق أهمية عنصر العلم لكون الإرادة هي جوهر القصد وليس العلم متطلبا لذاته وإنما باعتباره مرحلة في تكوين الإرادة وشرطا لتطورها. ويتوافر القصد الجنائي بتوافر هذين العنصرين معا، فالعنصر الأول يمثل إرادة النشاط الذي ينتهي إلى وضع إجراسي معين في القانون، والعنصر الثاني هو العلم والإحاطة بحقيقة هذا الوضع الإجرامي من حيث الوقائع وماهيته من حيث القانون وذلك في معنى الإدراك.

---

[1]- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية .1992.ص66

[2]- نورهان محمد الربيعي ،المرجع السابق،ص79

هذا ويعد القصد الجنائي هو أخطر صور الركن المعنوي، إذ تنصرف إرادة الجاني إلى السلوك الإجرامي وإلى ما يترتب عليه من نتيجة إجرامية . الفرق بين الجريمة العمدية وغير العمدية يتمحور، بشكل عام، حول النتيجة الجنائية الناتجة. إذ كلما كانت النية للوصول إلى تلك النتيجة وكان الجاني قد وجه جهوده نحو تحقيقها، تعتبر الجريمة عمدية. أما إذا لم يكن الجاني يقصد يفعلها ولم يتوقعها، أو قد قام بتقدير خاطئ بشأنها دون التصرف لتجنبها، فإن الجريمة تصنف عادة كغير عمدية[1].

ب- الجريمة السيبرانية كجريمة غير عمدية :إرادة تحقيق النتيجة الإجرامية عن طريق النص القانوني، فالجريمة غير العمدية هي الجريمة الناشئة أو الناتجة عن خطأ غير صدي، شريط أن ينص عليه القانون وقد أغفل قانون العقوبات المصري إيراد تعريف الخطأ غير صدي، واكتفى بذكر صوره في القسم الخاص في معرض بيانه للجرائم غير العمدية لاسيما جرائم القتل والإصابة الخطاء ولعل السبب في ذلك يرجع إلى الصعوبة التي يجدها المشرع الجنائي، إذا وضع تعريف عام للخطأ في الإحاطة بكل الحالات الموجودة والتي ستوجد في المستقبل. ناهيك من أن ذلك سيكون فيدا على حرية القاضي في التعامل مع الوقائع المتغيرة والمعقدة التي تعرض عليه المجيد. إذا أردنا تقييم إمكانية تطبيق هذا المعيار الشخصي على الأفراد في جرائم السيبرانية، يمكننا تصور أن الجرائم الجديدة قد تظهر كأخطاء غير متعمدة. على سبيل المثال، يمكن للموظف المسؤول (الفاعل) تدمير أجهزة المؤسسة بناء على فرضيات شخصية، مثل استخدام جهاز الحاسوب الخاص به في إجراءات غير مشروعة بناء على مهاراته في إنشاء فيروسات، أو استخدام قرص مرن في جهاز الحاسوب الخاص بالمؤسسة لنقل فيروسات، مما يؤدي إلى تدميرها جزئيا أو كليا. يظل هذا السيناريو ممكنا طالما يشارك الإنسان في عمليات معالجة البيانات[2].

[1]- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي .2008.ص99

[2]- نورهان محمد الربيعي ،المرجع السابق،ص80

المبحث الثاني: تصنيفات الجريمة السيبرانية

المشرع الجزائري واقتداء بأغلب دول العالم وأمام قصور القواعد القانونية التقليدية في مواجهة الجريمة المستحدثة، وجد نفسه امام حتمية استحداث قوانين تنسجم وحداثة الجريمة، مما ادى الى تعديل القانون الجنائي بشقيه الموضوعي والإجرائي من خلال التحلي بنصوص آمرة مستحدثة[1].

ولتصنيف القواعد القانونية بشكل عام أهمية كبيرة في مجال العمل القانوني؛ فهو يسهل مهمة الباحثين المختصين في البحث عن حكم القانون لحل قضية قد تكون محل النزاع، و يختصر الوقت والجهد على الباحثين عن حلول لمسائل القانونية المختلفة، ويعتبر كذلك من الوسائل الهامة لفهم المصطلحات الخاصة بقضية معينة، بالإضافة إلى ساهمته في ربط الظواهر الاجتماعية المتشابهة وإعطائها الوصف القانوني، فهو بمجمله عملية تسهل إيجاد الحلول القانونية لمختلف القضايا المتنازع عليها[2].

إذن سنتطرق في هذا البحث إلى الجرائم المعلوماتية تبعا لنوع المعطيات و محل الجريمة المطلب الأول أما المطلب الثاني فخصصناه لجرائم تبعا لدور الحاسب الآلي في الجريمة .

المطلب الأول: الجرائم المعلوماتية تبعاً لنوع المعطيات ومحل الجريمة.

يعكس هذا التصنيف التطور التاريخي لظاهرة الجرائم المعلوماتية وفق مجموعة من التقسيمات التي سنتطرق اليها.

الفرع الأول:الجرائم الماسة بقيمة المعطيات الحاسوب.

تنقسم هذه الجرائم على فئتين :

أولا: الجرائم الواقعة على نظام المعالجة الآلية للمعلومات

---

[1]– عقباش بريزة،مبارك حنان ،آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري،تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد البشير الإبراهيمي،برج بوعريريج،2021–2022،ص53

[2]– محمد بدوسي،تصنيف الجرائم الإلكترونية وفقا لطبيعة الحق المعتدى عليه دراسة مقارنة بين التشريع الفلسطيني و الإماراتي،مجلة جامعة العين لأعمال و القانون ، جامعة الإستقلال فلسطين ،ص124

تعرف الجريمة عموما في القانون الجنائي بأنها كل فعل أو امتناع عن فعل جرمه الشيء و حدود له عقوبة أو تدبير أمن في قانون العقوبات أو القوانين المكلمة له .[1]

أما مصطلح المعلومات فهو كثيرا ما يترادف مع مصطلح تكنولوجيا المعلومات أو تقنية المعلومات على الرغم من الاختلاف الموجودة بينها، فالمعلومات هي المضمون أو الرسالة الناتجة عن معالجة البيانات التي تم إدخالها بينما تكنولوجيا المعلومات هي الوسط المستخدم لاقتناء أو حفظ أو نقل المعلومات وقد وضعت اليونسكو تعريفا لتكنولوجيا المعلومات Technologie de l'information بأنها الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات و في تطبيقها والمتعلقة بالحواسيب وتفاعلها مع الإنسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية و ثقافية[2].

في عام 1962 اقترح الأستاذ (Drefus) مصطلح المعلوماتية informatique حيث تبنته الأكاديمية الفرنسية في عام 1966، والتي قامت بدورها بوضع تعريف له بأنه علم المعالجة المنطقية للمعلومات التي تعتبر بمثابة دعامة للمعارف الإنسانية و الاتصالات في المجالات الفنية و الاقتصادية والاجتماعية وذلك باستخدام معدات آلية[3] .

إلا أن جانب من الفقه يرى بأن تعبير معلوماتية يدل على المزاوجة ما بين الحواسيب و الاتصالات و قد استخدم هذا المصطلح من طرف الفقه الفرنسي في وصف الظاهرة الإجرامية المستحدثة تحت إسم الجرائم المعلوماتية أو الإجرام المعلومات بينما ذهب البعض الآخر إلى استخدام تعبير العش المعلوماتي أو الاحتيال المعلوماتي و غش الحاسوب إلا أن هذه التعابير في حقيقة الأمر تدل على جريمة واحدة من بين جرائم المعلوماتية لذلك فإن التعبير الأكثر شيوعا و الأعمق دلالة للتعبير عن هذه الظاهرة الإجرامية المستحدثة هو الجرائم المعلوماتية.

---

[1]– يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت، 14 ، دار العدالة ، عمان ، 2011 ، ص ص 26-27

[2]– بلال أمين زين الدين، المرجع السابق.ص100

[3]– د سامي الشوا " ثورة المعلومات وانعكاساتها على قانون العقوبات "، ط الثانية، دار النهضة العربية للنشر، القاهرة ، 1998، ص 4

و قد كثرت الآراء والشروح الفقهية لوضع تعريف قانوني محدد و منضبط للجريمة المعلوماتية أمام تحفظ المشرع في الدول التي تبنت تشريعات لذلك من الخوض في وضع تعريف قانوني محدد هو منهج سليم نظرا الحداثة الظاهرة إضافة إلى التباين حول استخدام المصطلح الدال على هذا النوع من الجرائم.

فمن التعريفات التي وضعت للجريمة المعلوماتية ما ذهب إليه الخبير الأمريكي من أن الجريمة المعلوماتية ما هي إلا فعل إجرامي ، أيا كانت صلته بتقنية المعلومات فيه يتكبد المجني عليه خسارة ويحقق الفاعل ربحا عمديا و يعرفها.

الأستاذ (sheldon hecht) بأنها واقعة تتضمن تقنية الحاسب و مجني عليه يتكبد أو

يمكن أن يتكبد خسارة وفاعل تحصل عن عند أو يمكنه الحصول على مكتب.. و يعرف خبراء منظمة التعاون الاقتصادي والتنمية الأوروبية (OECD) الجرائم المعلوماتية بأنها كل سلوك غير مشروع أو منافي للأخلاق أو غير مسموح به والذي يرتبط بالمعالجة الآلية للبيانات أو بنقلها.

وقد اعتمد هذا التعريف على معيارين الأول وصف السلوك وثانيها اتصال هذا السلوك بالمعالجة الآلية للبيانات أو نقلها.[1]

و من خلال كل ما تقدم يمكن تعريف جرائم المعلوماتية بأنها كل فعل أو امتناع ينشأ نتيجة الاستخدام غير المشروع التقنية المعلومات و يهدف للأضرار بالمصالح المادية و المعنوية التي يحميها قانون العقوبات ويطلق على المعلومات في العصر الحديث اسم البترول الرمادي Petrole grisأو باللغة الانجليزية petrol grayish نسبة إلى المادة الرمادية في المخ و أصبحت المعلومات إحدى أهم هذه المصالح المستهدفة [2].

[1]– بلال أمين زين الدين، المرجع السابق.ص101

[2]– زياد القاضي و اخرون: مبادي تحليل نظم الحامون والتصميم ، ط الأولى – دار الصفاء للنشر. 13 عمان، 1997،ص13

ثانيا :جريمة إتلاف برامج الحاسوب ومعلوماته

والمقصود هنا هو الإتلاف المنطقي أي إتلاف معلومات الحاسوب و بياناته باستخدام الطرق المنطقية والمعلوماتية وتنوع أساليب الاعتداء على المعلومات بحسب.

الهدف الذي يرمي الجاني إلى تحقيقه ومن ابرز هذه الاعتداءات : الفيروس المعلوماتي الدودة المعلوماتية ، القنابل المنطقية.

أ-الفيروسات:

وهو برنامج معلوماتي أعطي تسمية فيروس لتشابهه الكبير مع الفيروس البيولوجي من حيث الانتقال والتكاثر و وظائفه التدميرية للأنظمة المعلوماتية والقدرة على تعديل البرامج الأخرى التي يرتبط بها، كما يستطيع الفيرسات التمييز بين البرامج السليمة و البرامج التي سبق وأن أصبحت بالفيروس.

ولعل أهم العوامل التي ساعدت على انتشار السريع للفيروسات داخل الأنظمة المعلوماتية هي القرصنة المعلوماتية وتوافق الأجهزة وكذلك الانتشار الواسع الشبكة. الانترنيت.

وبالرغم من إنتاج العديد من البرامج المضادة للفيروسات تبقى هذه الأخيرة قادرة على اختراق النظم المعلوماتية وتدعيم البيانات مهما كانت المواقع والحصون[1].

ب- القنبلة المعلوماتية

و تنقسم إلى قسمين:

1-القنبلة المنطقية: و يهدف هذا الفيروس إلى تدمير المعلومات عند حدوث ظرف معين مثل تدمير نظام تسيير الموارد البشرية المؤسسة معينة عند شطب اسم أحد الموظفين من القائمة.

2- القنبلة الزمنية: يعمل هذا الفيروس في ساعة محددة من يوم معني و من أبرز الأمثلة عن ذلك فيروس Michael anglo مايكل انجلوا وفيروس Macmag و فيروس شرنوبيل

[1]- سعيداني نعيم، المرجع السابق،ص80

shernobel و يتميز هذا الأخير بأنه فيروس الأول الذي يصيب المكونات المادية بالخراب و التلف إلى جانب المكونات المعنوية (المعلومات) حيث اكتشف هذا الفيروس سنة 1998.[1]

3-الدودة المعلوماتية : هي عبارة عن نظام معلوماتي يمتاز بقدرته على التنقل عبر شبكات نقل المعلومات بهدف إعاقة عملها، والتشويش عليها عبر شل قدرتها على التبادل .. الخ و أهم ما تتميز به هذه الفيورسات ، الانتشار ، عبر الشبكات عن طريق توليد نفسها و من أشهرها الدودة التي أطلقها الطالب الأمريكي في جامعة كورنال Cornell university . روبيرت موريس سنة 1988 عبر شبكات الجامعات والشبكات العسكرية في الولايات المتحدة بتدمير الآلاف من الحواسيب وتعطيل الشبكات وكان هدفه من هذا هو إظهار ضعف مقاييس امن الشبكات قائلا : أردت أن أعرف إذا كان بإمكاني كتابة برنامج يستطيع قدر الإمكان الانتشار بشكل واسع على شبكة الانترنيت ، و قد حكم على روبرت سنة 1995، عملا بأحكام المادة 1/5من قانون إساءة استخدام الحاسوب الصادر سنة 1986 بالمراقبة لمدة ثلاثة سنوات وبالعمل بالخدمة الاجتماعية لمدة 400 ساعة.

ولقد أصبح مجرموا المعلوماتية يتفاخرون باستخدامها كوسيلة لاختراق الأنظمة و من الأمثلة الواقعية على ذلك ما حدث في صفحة إدارة الدفاع الأمريكية DOD الخاصة بالقوات الجوية الأمريكية التي تعرضت واجهتها المرحبة بزوار الموقع إلى اعتداء أجبر المسؤولين على إغلاق المواقع التي تمكنها إدارة الدفاع الأمريكية ، ليتم تريب برنامج وقاية اشد أمنا .[2]

[1]- عامر بزرا فايز أو أبو علي – فيروسات الكمبيوتر دار ضنين للنشر، عمان .ط الأولى، 1994.ص23

[2]- رامي حليم ،جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات،محاضرات جامعية ،جامعة سعد دحلب ،بليدة،ص350

الفرع الثاني: الجرائم الماسة بالمعطيات الشخصية البيانات المتصلة بالحياة الخاصة

وتشمل هذه الفئة الجرائم الاعتداء على المعلومات والبيانات الشخصية المتعلقة بالحياة الخاصة[1] وتعد هذه الجرائم من أخطر الصور لانها تنطوي على الاعتداء على المعلومات المخزنة في الحاسوب واستغلالها بأمور مشروعة بصور مختلفة.

وقد تأخذ جرائم المعلوماتية الماسة بالمعطيات الشخصية صورة نقل أو تسجيل المحادثات الخاصة وسائط الاتصال والتصنت عليها وهذا يمثل اعتداء على الحياه الخاصة، كذلك بعد انشاء البيانات الشخصية السرية سواء تم من قبيل الخطأ أو بقصد التشهير أو تهديد من صور

الاعتداءات الحياه الخاصة لان قيام شخص بإيداع بياناته لدى مؤسسه تحوز على ثقته وقيام تلك المؤسسة بإفشائها باي وسيله من الوسائل سالفة الذكر تعد من الجرائم التي تمس حياته الخاصة ولا يشترط القانون في بعض الدول ان تكون هذه البيانات حقيقيه أو مزورة بل يكفي ان تمس بشرف.

اما بالنسبة للأشخاص الاعتبارية فانقسم الفقه بشأن وجوب حماية خصوصيتها الى رأيين:

أولا-الرأي الأول.

أنكر عليها هذا نظرا لعدم تمتعها بالشخصية القانونية حيث حصر الشخصية القانونية في الشخص الطبيعي[2].

[1]- يوسف المصري، المرجع السابق، ص 26-27

[2]- ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996 ص 288.

ثانيا–الرأي الثاني

أقر لها بالحماية استنادا إلى أن هؤلاء الاشخاص تمنح لها حق الجنسية كالشخص الطبيعي وبالتالي كل ما يتمتع بالجنسية يمكن اعتباره مواطن فله الحماية القانونية للمعلومات الخاصة به [1].

الفرع الثالث: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه

التي تشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع.

وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن العرض المباشر المحرك للاعتداء النصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية البرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج[2].

هذا من جهة، ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات.

[1]– سمير شعبان، الجريمة الإلكترونية ،مقاربة تحليلية لتحديد مفهوم الجريمة و المجرم ،محاضرات جامعية ،جامعة باتنة ،ص120

[2]– بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي – دراسة مقارنة – أطروحة دكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة ، كلية الحقوق بجامعة محمد خيضر بسكرة ، الجزائر ، 2018،ص67

التي تشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع.

وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن العرض المباشر المحرك للاعتداء النصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية البرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.[1]

أولا- النص القانوني باعتبار المعلوماتية ضمن حقوق المؤلف في التشريع المقارن والجزائر

وقع الجدل الفقهي في البداية حول اعتبار المعلوماتية حقا للمؤلف وكانت بداية الاعتراف بذلك من خلال موافقة حقوق المؤلف الأمريكية copyright office لسنة 1964 على إيداع البرامج لديه كمصنفات ، وكذلك الحال في فرنسا بموجب القانون 86 66 المؤرخ في 03/07/1986 حيث أضيفت برامج الكمبيوتر ضمن حقوق المؤلف ولا الأمر 97-10 المؤرخ في 06/03/1997 المتعلق بحقوق المؤلف والحقوق المجاورة صراحة على اعتبار حقوق المؤلف معلوماتية.

لكن الأمر 03-05 المؤرخ في 09/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة " اعتبر صراحة من خلال نص المادة 4 منه على أن برامج الحاسوب تعتبر كمصنفات محمية.

[1]- سليمان أبو نمر ،يوسف بوكشريدة،المرجع السابق،ص16

ثانيا- الجرائم المعلوماتية في نطاق حق المؤلف والعقوبات المقررة عليها

تضمنت المواد من 151 إلى 160 من الأمر 03-05 العقوبات المقررة في مجال حق المؤلف لكن الأمر 03-05 المؤرخ في 09/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة " اعتبر صراحة من خلال نص المادة 4 منه على أن برامج الحاسوب تعتبر كمصنفات محمية[1].

المطلب الثاني: تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة و الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال.

يشتمل هذا التصنيف أهم الجرائم التي تتصل بالحواسيب ، حيث يعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية و مضاعفا لجسامتها.

تتعدد صور جرائم الحاسوب المرتكبة باستخدام الحاسب بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها[2]، وهي كالآتي:

الفرع الأول: تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة.

عرضنا فيما تقدم لدور الكمبيوتر في الجريمة، فقد يكون هدف الاعتداء، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق للجرائم الإلكترونية، وقد يكون الكمبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم الجرائم المرتبطة بالكمبيوتر، وقد يكون الكمبيوتر أخيرا بيئة الجريمة أو وسطها أو مخزنا للمادة الجرمية، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور جرائم التخزين[3].

---

[1]- بن دراح علي إبراهيم ،المرجع السابق، ص63.64

[2]- جوالي عبد الستار،جرائم الحاسوب (دراسة مقارنة بين الشريعة الإسلامية و القانون الجزائري)،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص شريعة و قانون ،شعبة العلوم الإسلامية ،كلية العلوم الإجتماعية و الإنسانية،جامعة الشهيد حمه لخضر الوادي،2014-2015،ص11

[3]- سمير شعبان،المرجع السابق،ص121

ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها.

والثاني جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانوني، والاصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الانترنت، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الالكتروني للأموال وغيرها، باعتبار أن مواقع الانترنت تتصل بشكل رئيس بهذه الأنشطة، والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها.

وهذا التقسيم شائع بجزء منه وهو تقسيم الجرائم الى جرائم هدف ووسيلة لدى الفقه الاجنبي ، وتبعا له تنقسم الجرائم الإلكترونية إلى جرائم تستهدف نظام المعلوماتية نفسه، كالاستيلاء على المعلومات واتلافها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر. أما تقسيمها كجرائم هدف ووسيلة ومحتوى فإنه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا، وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام 2001، ذلك أن العمل منذ مطلع عام 2000 يتجه إلى وضع إطار عام لتصنيف جرائم الكمبيوتر والانترنت وعلى الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة هذه الجرائم، وهو جهد تقوده دول أوروبا بالأساس، لكن وبنفس الوقت بتدخل ومساهمة من قبل أستراليا وكندا وأمريكا.[1]

لقد أوجد مشروع الاتفاقية الأوروبية تقسيما جديدا نسبيا يضم أربع طوائف رئيسة لمختلف الجرائم الإلكترونية.

الأولى :

-الجرائم التي تستهدف عناصر السرية والسلامة وموفورية المعطيات والنظم وتضم:

-الدخول غير قانوني (غير المصرح به).

[1]- سعيداني نعيم، المرجع السابق،ص81

-الاعتراض غير القانوني.

-تدمير المعطيات.

-اعتراض النظم[1].

اساءة استخدام الاجهزة.

الثانية : الجرائم المرتبطة بالكمبيوتر وتضم:

- التزوير المرتبط بالكمبيوتر.

-الاحتيال المرتبط بالكمبيوتر.

الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الاباحية وغير الأخلاقية.

الرابعة : الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة.

- قرصنة البرمجيات.

هذه هي هم نظريات التصنيف، وغيرها كثير، غير أن المقام لا يسمح بإيرادها كاملة، ولأننا أوردنا ملاحظاتنا حول بعض منها، فإننا تكتفي في معرض تقديرها بالقول أن أكثر التقسيمات الضبطية هو معيار تصنيف هذه الجرائم تبعا لدور الكمبيوتر في الجريمة[2].

الفرع الثاني تصنيف الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال.

يمكن تقسيم الجرائم المعلوماتية طبقا لهذا المعيار الى ما يلي:

أولا :الجرائم التي تستهدف الاشخاص

وتضم هذه الفئة نوعين رئيسين من الجرائم :

[1]- سمير شعبان،المرجع السابق،ص121

[2]- سمير شعبان،المرجع نفسه،ص122

أ – القذف و الإهانة والسب والاعتداء على حرمة الحياة الخاصة للأفراد عبر الانترنت:

تضمنت المواد 296 و 297و 298 من قانون العقوبات المساس بشرف واعتبار الأشخاص والسب والقذف، لكن لم يتناول إلى استعمال مختلف الوسائل المعلوماتية للقيام بهذه الجرائم.

كانت بداية تجريم هذه الأفعال من قبل المشرع بداية بموجب القانون رقم 01-09 المؤرخ في 26 جوان 2001 الذي أضاف المادة 144 مكرر التي نصت على العقوبة بالحبس من 3 أشهر إلى 12 شهرا وبغرامة من 50.000 دج إلى 250.000 دج أو بإحدى هاتين العقوبتين فقط كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا[1].

سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا في حالة العود، تضاعف عقوبات الحبس والغرامة المنصوص عليها في هذه المادة، والتي عدلت بموجب القانون رقم 11-14 المؤرخ في 2 أوت 2011 والتي تم من خلالها التخلي عن فكرة مضاعفة عقوبة الحبس والاكتفاء بمضاعفة الغرامة. إذا فإذا كانت هذه العقوبات حصرها المشرع في الأفعال المرتبطة ببعض الشخصيات في الدولة ، فانه يمكن استعمالها قياسا في الجرائم المرتكبة على باقي الأشخاص هذا من جهة ، كما أن نصوص المواد الثلاث المذكورة سابقا جاءت بصيغة العموم ولا لم تأت تفصيلا[2].

ما تجدر الإشارة إليه أن الجرائد الالكترونية وشبكات التواصل الاجتماعي تعد مجالا خصا لهذا النوع من الجرائم ، ومن الواضح أن قيام هذه الجرائم مكتملة الأركان لكونه يبقى ثابتا من خلال الكتابات التي تظهر أو التعليقات التي يمكن الاحتفاظ بها والتي تشكل مساسا أو قذفا لبعض الأشخاص ومنه توفر القصد الجنائي لدى المتهم، فاستعمالها من طرف الغير يعد من قبيل النشر الافتراضي.

[1]- بن دراح علي إبراهيم ،المرجع السابق،ص51

[2]– بعقيقي عبير، المرجع السابق،ص68

ب – الاستغلال الجنسي للأطفال عبر الانترنت: على عكس الجريمة السابقة المتعلقة بالسب والقذف غير الانترنت فقد سارع المشرع بموجب القانون رقم 14-01 [1]المؤرخ في 04 فيفري 2014 المتضمن تعديل قانون العقوبات على إضافة مادة خاصة تجرم كل استغلال جنسي للأطفال القصر بكل الوسائل، والتي تندرج من ضمنها الوسائل المعلوماتية بكافة أنواعها ، وهي المادة 333 مكرر والتي على نصت على العقوبة بالحبس من 5 سنوات إلى 10 سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، لكل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر[2].

كما أضافت نفس المادة وحماية لحقوق الأطفال الضحايا انه في حالة الإدانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لارتكاب الجريمة والأموال المتحصل عليها بصفة غير مشروعة مع مراعاة حقوق الغير حسن النية.

وكذلك من صور الاستغلال الجنسي للأطفال القصر هو التحريض على الفسق والدعارة وهو الأمر الذي تناوله القسم السابع من الفصل الثاني المتعلق بالجنايات والجنح ضد الأسرة والآداب العامة والمخصص لتحريض القصر على الفسق والدعارة، فقد نصت المادة 342 المعدلة على أنه من حرض قاصرا لم يكمل 18 سنة على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له ولو بصفة عرضية، يعاقب بالحبس من 5سنوات إلى 10 سنوات وبغرامة من 20.000 دج إلى 100.000 دج. ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة، حيث فتحت المادة 343 المجال واسعا في مجال الآليات

---

[1]– قانون رقم 01-14 مؤرخ في 20 جمادي الأولى عام 1422 الموافق 18 تخت سنة 2001 يتعلق بتنظيم حركة المرور عبر الطرق وسلامتها وامتها، ج ر ج ج،ع46

[2]– قارة آمال ، الجريمة المعلوماتية ، ماجستير تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق بجامعة الجزائر 2005،ص ص12.13

المستعملة لذلك ، حين نصت على امتداد العقوبة لكل شخص ساعد أو عاون أو حمى دعارة الغير أو أغرى الغير على الدعارة بأية طريقة كانت.

ج-انتهاك الآداب العامة عبر الانترنت: ما يقال عن جرائم السب والقذف عبر الانترنت يقال على هذا النوع من الجرائم لأنه لا يوجد نص واضح باستثناء جرائم استغلال الأطفال جنسيا التي أدرجها المشرع ضمن مجال انتهاك الآداب العامة ، وعليه فإن كل الجرائم التي تتدرج ضمن هذا الباب وتم فيها استخدام وسائل معلوماتية فإنها تكون مدعاة لقيام جريمة معلوماتية[1].

ثانيا : الجرائم المعلوماتية الواقعة على الأموال.

حيث سنتعرض إلى عديد الجرائم التي تناولها المشرع الجزائري ، والمتمثلة فيما يلي:

أ – النصب الالكتروني : تعتبر الجرائم المعلوماتية التي تستهدف المال من أشهر الجرائم وأخطرها خاصة مع انتشار وسائل الانترنت والحواسيب ، فأصبح المجرم المعلوماتي يبحث عن كل الطرق للبحث عن المال المعلوماتي في محاولة منه للوصول إليه مستعملا طرقا غير مشروعة ، وعليه طرح التساؤل بداية عن المال المعلوماتي المعني بالحماية القانونية ؟

يعتبر المال المعلوماتي المعني بالحماية القانونية كل مال الكتروني قابل للنقل والتملك كما يمكن تعريفه بأنه المال الموجود في الحاسوب سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية ، فهو بذلك كل المدخلات الالكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية[2].

عرف الأستاذ الأمريكي سكويرز جريمة النصب الالكتروني على أنها إساءة استخدام نظام الحاسوب بحيث ينطوي سلوك على حيلة أو خدعة مظللة 63 كما يمكن تعريفه على انه التحويل غير الشرعي للأموال المعلوماتية.[3]

---

[1]– بن دراح علي إبراهيم ،المرجع السابق، ص ص52.53

[2]– ناير نبيل، عمر الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية دار الجامعة الجديدة ، مصر ، 2012 .ص32

[3]– قارة آمال ، المرجع السابق،ص 15

وبالرجوع إلى تعريف المشرع الجزائري لجريمة النصب من خلال ما تضمنته المادة 372 ق ع فنجده عرفها على صيغة العموم، ولم يحدد جريمة النصب الالكتروني في حد ذاتها ، حيث عرف جريمة النصب على أنها " كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار. وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أذونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200.00 دج.

وعليه فإن كان المشرع لم يربط جريمة النصب بالجريمة المعلوماتية ، ولم يحدد وسيلة بعينها ، ولكن يمكن إسقاطها إذا ما تم توفر شروطها[1].

ب- جرائم التزوير : لقد انتشر استخدام الحاسوب انتشارا واسعا في شتى المجالات في التعامل بين الأفراد ويمكن القول أنه حل محل الأوراق العادية في أغلب نظم المعالجة الآلية للمعلومات ومع تزايد حجم الاعتداءات الواقعة على البيانات والمعلومات التي تمس الأفراد في حقوقهم وأموالهم، وفي مقابل ذلك تزايدت فرص الأشخاص للعبث والتلاعب في معطيات الحاسوب بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد، وبات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من هذا التبديل والتزوير.

ان جريمة التزوير، التي كانت في السابق مقتصرة على التلاعب بالمستندات المادية، أصبحت الآن تتخذ أشكالًا إلكترونية مع تطور التكنولوجيا، مما يجعلها جريمة سيبرانية، التزوير

[1]- بن دراح علي إبراهيم ،المرجع السابق،ص54

الإلكتروني يشمل التلاعب بالبيانات والمعلومات المخزنة رقميًا، ويمكن أن يشمل تزييف المستندات الرقمية، والتوقيعات الإلكترونية، وغيرها من أشكال التلاعب بالبيانات[1].

التزوير كجريمة سيبرانية في التشريع الجزائري لا يوجد قانون خاص للتزوير المعلوماتي (السيبراني) بشكل منفصل، بل يعتمد على القوانين العامة المتعلقة بالتزوير في قانون العقوبات أو في قانون مكافحة التزوير واستعمال المزور بشكل عام، وبالأخص أن الجريمة السيبرانية لها خصوصية متميزة عن باقي الجرائم لاستخدامها لتقنيات المعلوماتية.

فإذا كانت بعض التشريعات قد أوردت تعريفا للتزوير في نصوصها كالقانون العقوبات الفلسطيني رقم 74 لعام 1936 مثلا الذي نص في المادة (332) على تعريف التزوير بأنه تحريف معدل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي، وغيرها من القوانين إلا أنه هناك تشريعات أخرى لم تورد تعريفا للتزوير كالقانون الجزائري والمصري فأنها تبقي الباب مفتوحة لدخول أنماط مستحدثة من الأفعال التي قد تعد تزوير بخلاف الاتجاه الأول الذي يعتبر مفيدا. ويمكننا القول أن جريمة التزوير الإلكتروني يمكن أن تشمل تزوير البريد الإلكتروني الخاص بفرد أو مؤسسة معينة أو تزوير للوثائق والسجلات وأيضا تشمل تزوير الهوية.[2]

[1] – بن دراح علي إبراهيم، المرجع السابق، ص: 65

[2]– سليمان أبو نمر ،يوسف بوكشريدة،المرجع السابق،ص21

خلاصة الفصل الأول:

في ختام هذا الفصل الاول الموسوم بالاطار المفاهيمي للجريمة السيبرانية، نخلص بالقول أننا في عصر التكنولوجيا الحديثة، حيث أصبحت الجرائم السيبرانية، تُرتكب عبر الإنترنت باستخدام الأجهزة الرقمية كالهواتف الذكية وأجهزة الكمبيوتر، تشكل تهديدًا متزايدًا يؤثر على مختلف جوانب حياتنا، ورغم أن التكنولوجيا تُعد وسيلة لتعزيز فرص التعلم والتواصل، إلا أنها تمثل في الوقت نفسه خطرًا حقيقيًا على الأفراد والمؤسسات وامن الدول ككل، الذين قد يكونون عرضة لأنواع متعددة من الجرائم الإلكترونية.

مما يستوجب وضع إطار قانوني ومؤسساتي للوقاية من هاته الجريمة المعلوماتية المستحدثة من جهة وللحماية والتصدي لكل من يتعدى على أمن وخصوصية الأفراد والمؤسسات وأمن الدولة من جهة أخرى، هذا ما سنتطرق له في الفصل الثاني لهاته المذكرة .

الفصل الثاني:

الأحكام القانونية و الأجهزة المختصة لمكافحة الجريمة السيبرانية

شهد العالم في الألفية الأخيرة تحولات عميقة على كل المستويات الاقتصادية والاجتماعية والثقافية وبخاصة التكنولوجية ، حيث تحولت المجتمعات من مجتمعات استهلاكية إلى مجتمعات صناعية إلى مجتمعات الكترونية سيبرانية بفضل ما قدمته التكنولوجية الحديثة من خدمات رقمية سريعة قليلة التكاليف بدقة متناهية وبمردودية أكبر، وعلى الرغم من ايجابيات هذه التقانة والتكنولوجية إلا أنها بالمقابل شكلت هاجسا لكل المجتمعات بسبب إفرازها لمجموعة من السلبيات أهمها ما يعرف بالجرائم السيبرانية.

ونظرا لخصوصية هذه الجرائم باعتبار أنها جرائم عابرة للجغرافيا ولا تميز بين مجتمعات و أخرى ، فإن الجزائر تعتبر هي الأخرى من الدول التي عرفت في السنوات الأخيرة ارتفاع مؤشر هذه الجرائم بشكل ملموس، حسب التقارير الأمنية والعلمية أيضا ، وهو ما جعل المشرع يفكر في من مجموعة من التشريعات للتصدي لهذه الظاهرة السيبرانية[1].

ان المشرع الجزائري واقتداء بأغلب دول العالم وأمام قصور القواعد القانونية التقليدية في مواجهة الجريمة المستحدثة ، وجد نفسه امام حتمية استحداث قوانين تنسجم وحداثة الجريمة، مما ادى الى تعديل القانون الجنائي بشقيه الموضوعي والإجرائي من خلال التحلي بنصوص امرة مستحدثة، لتجريم الظاهرة وتحديد سبل واليات مكافحتها وذلك باستصدار قوانين خاصة تتلاءم والطبيعة الخاصة للجريمة الإلكترونية، كما تضمنت التعديلات المختلفة لقانون الإجراءات الجزائية الجزائري عدة قواعد اجرائية مستحدثة تتماشى وحداثة الجريمة.[2]

ومن خلال هذا الفصل سنتطرق الى مبحثين فالمبحث الأول سنخوض فيه مكافحة جريمة السيبرانية من خلال النصوص القانونية أما المبحث الثاني سنستعرض مكافحة جريمة السيبرانية من خلال الأجهزة المختصة بها.

[1]– مهدي رضا،المرجع السابق،ص111

[2]– عقباش بريزة، مبارك حنان،المرجع السابق،ص53

المبحث الأول: مكافحة الجريمة السيبرانية من خلال النصوص القانونية

نتيجة التطور المتسارع والانفتاح العالمي والعولمة ، فقد بات العديد من الجرائم يتم ارتكابها من خلال شبكة الإنترنت، ونتيجة التنظيم الإلكتروني لهذا النمط من الجرائم فقد أضيفت صفة التعقيد، وصعوبة الملاحقة لمرتكبي هذه الجرائم، وكان لا بد من وجود إطار تشريعي قانوني لمواجهة هذه الجرائم في الوطن العربي[1] .

لقد وضعت الجزائر الأمن السيبراني أحد أولوياتها من أجل المحافظة على السياسة الأمنية وذلك بإدراجها مجموعة من الآليات والميكانزمات والأجهزة من اجل مكافحة القضاء على الجريمة السيبرانية ، وكرس لها قواعد قانونية مختصة بها من اجل معاقبة مرتكبيها و هي عقوبات سالبة للحرية و بغرامات مالية نافذة للدولة[2].

المطلب الأول: مكافحة جريمة السيبرانية على ضوء القانون العقوبات والقانون الإجراءات الجزائية

في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى حزمة من التشريعات والآليات القانونية والمؤسساتية للتصدي لهذه الجريمة التي أضحت تسمى في الأدبيات الأكاديمية بالجريمة الالكترونية أو الجريمة السيبرانية.

والجزائر إحدى هذه الدول التي لم تكن في منأى من تداعيات هذه الظاهرة، حيث انتشرت في الآونة الأخيرة جرائم تمس بالحياة الشخصية للمواطن وتمس أيضا بأمن واستقرار البلاد وبكل جوانب الحياة الأخرى اقتصاديا، سياسيا، ثقافيا، ومست حتى البناء المجتمعي في تركيبته وبنايته.

من هنا سعى المشرع الجزائري إلى من العديد من التشريعات والقوانين للتصدي لهذه الجرائم السيبرانية وأهم هذه التشريعات القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم

---

[1]– مخلد إبراهيم الزعبي ،فاعلية القوانين و التشريعات العربية في مكافحة الجرائم الإلكترونية دراسة مقارنة ،المجلة العربية للنشر العلمي ،ع37.2021.قطر ،ص286

[2]– واجعوط سعاد ،مكافحة الجريمة السيبرانية على المستوى الوطني،المجلة دفاتر البحوث العلمية،مج12،ع2.2024. الجزائر ،ص421

المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1] وغيره من التشريعات التي تدعم الحد من انتشار هذه الجرائم[2].

الفرع الأول: مكافحة جريمة السيبرانية في قانون العقوبات

ركزت إستراتيجية المشرع الجزائري في التصدي للإجرام المعلوماتي[3] في القسم السابع مكرر من قانون العقوبات رقم 04-15 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات " جملة من قواعد قانونية موضوعية حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء و عقوبة، وتأخذ هذه الأفعال وصف الاعتداء على معطيات نظام المعالجة الآنية كما يمكن لها أن تأخذ وصف الاعتداء على سير نظام المعالجة الآلية.

أولا: تجريم الاعتداء على نظام المعالجة الآلية للمعطيات.

لقد جعل المشرع الجزائري من وجود نظام المعالجة الآلية شرطا أساسيا للبحث عن مدى تحقق الاعتداء على نظام المعالجة الآلية للمعطيات[4] تتحقق في صورتين الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات إضافة إلى الصورة المشددة للاعتداء على نظام المعطيات تتضمن جريمتي الدخول والبقاء غير المرخص بهما في النظام.

أ- الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات :

1 -الدخول غير المرخص: تقوم هذه الجريمة بتحقيق فعل الدخول إلى النظام المعلوماتي، ومدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات والمعلومات التي يتكون منها. ويقصد بالدخول أيضا الدخول إلى

---

[1]- قانون رقم 09 - 04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.ج ر ج ج ،ع47

[2]- مهدي رضا،المرجع السابق،ص112

[3]- - راضية عيمور ، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية المبحوث القانونية والسياسية، العدد 202201، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة الأغواط، الجزائر، ص 98

[4]- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 للعدل والمتمم للأمر 06/156، للتضمن جرائم المساس بأنظمة المعالجة الآلية للمعضوات ج.ر ، عدد71 لسنة2004.

محتويات جهاز الكمبيوتر ذاته، أي إجراء اتصال بالنظام محل الحماية بالطرق الفنية اللازمة لذلك، وليس معنى الدخول المادي كدخول القاعة أو الصالة الموجود بها جهاز الكمبيوتر مثلا.

ويجب أن ينظر إليه كظاهرة معنوية تشابه تلك التي تعرفها عندما تقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.

وتقع هذه الجريمة من كل إنسان أيا كانت صفته، أي أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة مثل الرشوة أو الاختلاس أو الزنا، وإنما ترتكب من أي شخص سواء كان يعمل في مجال الأنظمة أو لا يعمل، وسواء كان يفهم أو ولا يفهم أسلوب تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أولا وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، وإنما يتخذ هذا الفعل وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو بمعنى آخر دون تصريح.

فالأصل في جريمة الدخول إلى النظام هي جريمة نشاط وليست جريمة ضرر في غالبية التشريعات المقارنة ما دام أنه لا يلزم لوقوعها تحقق ضرر من نوع معين، ويتمثل هذا النشاط في الاتصال بنظام الكمبيوتر بأي طريقة كانت وعادة ما يقصد الفاعل بذلك الاطلاع على المعلومات التي يحتويها النظام .[1]

2 –البقاء غير مرخص: يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وكما قد يجتمعان[2].

[1]– المفتيحة مهري، جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي ، الجزائر 2016/2015، ص ص 10.11.12

[2]– المختن، عبيد صالح . سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية. مجلة الفكر الشرطي .مج، 24، ع4. 2015، ص31

وتعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي بشكل عام عن الجرائم التي يصعب تقديم دليل على إثباتها، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الانفصال عن النظام المتعدي عليه، وهذه الجريمة لا تترتب إلا على الجريمة السابق ذكرها وهي جريمة الدخول غير المشروع للنظام المعلوماتي، وتعد هذه الجريمة من الجرائم الشكلية كالجريمة السابقة، كما أنها تعد من الجرائم المستمرة، فتبقى الجريمة قائمة طالما أن الجاني مازال باقيا على الاتصال بنظام المعلومات الذي تم بدون قصد[1].

وهذا الركن المادي يظهر في صورتين وهما:

الصورة الأولى : تتمثل في تحقق فعل البقاء غير المرخص بها داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويتجسد هذا عندما يكون فعل الدخول إلى نظام المعالجة مشروعا، كأن يدخل الشخص صدفة أو خطأ إلى نظام ما أي دون قصد ففي هذه الحالة يتعين على المتدخل أن ينسحب ويغادر فورا النظام، أما إذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء الغير مرخص به.

الصورة الثانية: تتمثل في تحقق فعل البقاء غير المرخص به مجتمعا مع فعل الدخول، ويتجسد هذا الوضع حينما يكون الدخول غير مشروعا، مثال عن ذلك كان يدخل الجاني نظام ما دون إذن مسبق من صاحب هذا الأخير، ثم يستمر في البقاء داخله، وهذا يتحقق الاجتماع والتداخل المادي بين الجريمتين.[2]

فالفرق بين الصورتين السابقتين إبراز النطاق الزماني لكل واحدة منهما لها أهمية كبيرة في حساب مدة التقادم كل جريمة وتحديد الاختصاص فيها، خاصة إذا علمنا بأن جريمة البقاء داخل

---

[1]– الغافري، حسين، دراسة في الجهود الدولية في مواجهة جرائم الإنترنت، من منشورات المنشاوي للدراسات والبحوث.2007.ص 90

[2]– بيكة باكة ،موساوي لمياء،آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري ،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و العلوم الجنائية ،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الشيخ أمود بن مختار إيليزي،2022–2023، ص ص7.8

النظام هي جريمة مستمرة، وهذا ما أراده المشرع الجزائري على ما أعتقد تحقيقه من خلال نص المادة 394 مكرر عندما تطرق للدخول ثم البقاء.

ب- الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات: تشدد "الفقرتين الثانية والثالثة من المادة 394 مكرر من قانون العقوبات[1]، في عقوبة جريمة الدخول أو البقاء غير المصرح بها إذا نجم عن هذا الدخول أو البقاء داخل النظام غير المصرح بهما، إما محو أو تعديل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام الأداء وظائفه المترفع العقوبة إلى ضعف تلك المقررة في الجريمة البسيطة، سواء في حدها الأدنى الذي تضاعف من ثلاثة أشهر إلى سنة أشهر، أم في حدها الأقصى الذي تضاعف كذلك من سنة واحدة إلى سنتين، أما الغرامة فثبت حدها الأدنى عند 50.000 دج وارتفع حدها الأقصى إلى 150,000 دج وذلك في حالة ما إذا أدى الدخول والبقاء إلى حذف أو تغيير للمعطيات، أما إذا أدى الدخول أو البقاء إلى تخريب النظام فالغرامة تشدد إلى الضعف أي تتراوح من 100.000 إلى 200.000 دج.

انطلاقا مما سبق يتبين أن جريمة الدخول أو البقاء غير المصرح بهما لقيامهما لابد أن يكون النظام مفتوحا لأشخاص محددين، كما أن نصر " المادة 394 مكرر من قانون العقوبات سالف الذكر " تضمن صورتين للركن المادي هذه الجريمة هي الصورة البسيطة للمدخول أو البقاء غير المشروع، وكذا صورة مشددة للعقاب عليها تتضمن ضعف العقوبة المقررة للجريمة في صورتها البسيطة[2].

ثانيا: تصنيف الجرائم الإلكترونية.

تضاربت الآراء لتحديد أنواع جرائم الأنترنت وتعددت التصنيفات، فهناك من عددها بحسب موضع الجريمة وآخر قسمها بحسب طريقة ارتكابها، ويتمثل التصنيف في مايلي:

[1] – قانون العقوبات رقم 04-15 ، المرجع السابق.

[2]– بيكة باكة ،موساوي لمياء،المرجع السابق، ص ص8.9

الصنف الأول: يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة[1].

الصنف الثاني: تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور فيدعم جرائم غسيل الأموال، المخدرات المتاجرة بالأسلحة واستعمال الشبكة كسوف للترويج غير المشروع في هذه المجالات.

الصنف الثالث: بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب [2].

الصنف الرابع: فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستعمال ثغرات شبكة الانترنت.

وأخيرا صنفت الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية[3] .

يمكن تقسيم الجرائم المعلوماتية كالتالي: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي، والجرائم الواقعة على الأموال إضافة إلى الجرائم الواقعة على أمن الدولة.

---

[1]– الغافري حسين،المرجع السابق،ص 92

[2]– جميلة غربي، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية قسم القانون العام كلية الحقوق والعلوم السياسية، جامعة أكلي محمد أولحاج البويرة، الجزائر، 2020–2021، ص ص 16 – 17

[3]– الغافري حسين،المرجع السابق،ص ص93.94

أ- **الجرائم الواقعة على الأشخاص:** فرغم الإيجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك ومنها الجرائم المستحدثة في قانون العقوبات رقم 24-06 [1]والمتمثلة في :

1-جريمة النشر الإلكتروني أو التهديد به دون إذن صاحبه :

يعتبر هذا العنصر الإجرامي الجديد في قانون العقوبات بمثابة مواكبة للتطورات التكنولوجية الإلكترونية التي أصبحت حديث الساعة والمعاملات، والواقع الملموس التي شهدته التبليغات لدى مصالح الشرطة وعدد القضايا المرفوعة لدى المحاكم القضائية، للانتشار الواسع في مشاركة خصوصيات المرء لدى مواقع التواصل الإلكتروني وبالأخص بدون إذن أو رخصة من صاحبها[2].

مما دفع بالمشرع الجزائي بتجريم هذا النوع من الاعمال حفاظا على النظام العام وكيان الدولة بحماية رعاياها وتوفير الأمن السيبراني في ظل التهديدات والمخاطر الإلكترونية العديدة، وعليه نص المشرع في نص المادة 333مكرر 4[3]على أنه كل من يلتقط أو يتحصل على صور أو فيديوهات أو رسائل إلكترونية أو أي معلومات خاصة لأي شخص بأي طريقة كانت، وقام بإذاعتها أو نشر محتواها لأي شخص بأي طريقة كانت، وقام بإذاعتها أو نشر محتواها أو هدد بذلك دون إذنه أو رضاه، جعل عقوبته بالحبس من 3 ثلاث سنوات إلى 7 سبع سنوات كل شخص يستعمل صورا إلكترونية للغير أو يقوم بتحويرها أو نقلها أو نسخها أو نشرها قصد الإضرار به.

2-جريمة النشر الإلكتروني أو التهديد به اثناء قيام الرابطة الزوجية او الخطوبة:

جاءت نص المادة 333 مكرر 05 [4]واضحة بهذا الخصوص حيث نصت على أنه كل زوج أو خاطب أو مخطوبة يذيع او ينشر بأي وسيلة صورا خادشة لزوجه او خطيبته أو خاطبها أو هدد

---

[1]- القانون رقم 24-06 المؤرخ في 28أفريل2024 المتعلق بقانون العقوبات، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8جويلية 1966 والمتضمن قانون العقوبات.

[2]- الجميلة غربي، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، المرجع السابق، ص ص 18.17

[3]- المادة 333 مكرر 4 من قانون العقوبات سالف الذكر.

[4] القانون رقم 24-06 المتعلق بقانون العقوبات، المرجع السابق.

بنشرها أو إذاعتها سواء تم ذلك أثناء قيام رابطة الزوجية أو الخطوبة أو بعد انتهائها، يعاقب بالحبس من خمس سنوات5 إلى عشر سنوات 10 وبغرامة مالية من 500.000دج إلى 1.000.000دج.

3-جريمة منصوص عليها قانونيا ترتكب او يسهل ارتكابها تكنولوجيات الإعلام والاتصال:

كآخر جديد بخصوص ضبط الإطار القانوني الخاص بالتجريم الإلكتروني وضبط النظام العام وحفظ عدالة وكيان الدولة، زاد المشرع الجزائي بتوسيع دائرة الجرائم الإلكترونية ، وأفاد في نص المادة 333 مكرر 6 [1]على أن زيادة على العقوبات الأشد تضاعف العقوبات المقررة لجرائم التهديد والقذف والسب والإهانة وإفشاء السر المهني وذلك عندما ترتكب الجريمة أو يسهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال.

4-انتحال شخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شاعتها من أجل الحصول على بطاقات الائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية وتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت.

5- التشهير وتشويه السمعة : يقوم المجرم بنشر المعلومات التي قد تكون سرية أو مضللة عن الضحية، والذي قد يكون فردا أو مؤسسة تجارية أو سياسية، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم الإجزاء هذه الوسائل يتم إنشاء موقع على الشبكة يحوي المعلومات المطلوب

[1] المادة 333 مكرر 6 من القانون رقم 24-06 المتضمن قانون العقوبات، نفس المرجع السابق.

نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين لذلك يضم هذه الجرائم تشويه السمعة.[1]

ب- الجرائم الواقعة على الأموال: وتشمل أنشطة الاستيلاء على الأموال والمصاريف عن طريق الاحتيال التجاري والاحتيال عن طريق أوراق مالية والتزوير، والاقتحام بهدف اغتصاب الملكية ونقلها عبر النظم والشبكات، واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص، وتشمل جرائم الاحتيال التلاعب بالمعطيات والنظم واستخدامها في تدمير الكمبيوتر والبطاقات المالية للغير دون ترخيص[2].

ج- الجرائم الواقعة على أمن الدولة :تقع هذه الجرائم باستعمال النظام المعلوماتي سواء الإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني، أو الإرهاب الإلكتروني، التجسس.

الجرائم المعلوماتية الواقعة على النظام المعلوماتي: وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية النظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي[3].

الفرع الثاني : مكافحة جريمة السيبرانية في قانون الإجراءات الجزائية

وهذا بالتعديلات القانونية المتوالية لقانون الإجراءات الجزائية للأسباب الموضحة سابقا في جميع مراحل سير الدعوى العمومية، ابتداء من مرحلة التحقيق بنوعيه الابتدائي والتحقيق القضائي الابتدائي الذي تتوسطه مرحلة المتابعة الى مرحلة المحاكمة و العقوبة المقررة.

---

[1]- عمر بن ياسين. المعالجة القانونية للجرائم الإلكترونية في التشريع الجزائري والتشريعات المقارنة التشريع المغربي والإماراتي الموذجا، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 3 .2019.ص227

[2]- الطيب بلواضح، الجريمة في القضاء الإلكتروني، دار وائل للنشر والتوزيع، (د.م.د) (د ب ن)، (ط1)، 2020 ،ص 60

[3]- الجميلة غربي، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، المرجع السابق، ص ص 22-23

قانون رقم 04-14 والمتضمن قانون الإجراءات الجزائية[1] ، القانون رقم 06-22 والمتضمن قانون الإجراءات الجزائية الذي يضمن اساليب جديدة في التحري[2] ،المرسوم رئاسي رقم 21-439 يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3] ،الأمر رقم 21-11والمتضمن قانون الإجراءات الجزائية بباب سادس عنوانه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[4].

وعليه سنبين في هذا الفرع كيف شملت هذه التعديلات التي اجراها المشرع الجزائري على مدار 18 سنة سبل مكافحته للجريمة الالكترونية من الناحية القانونية الإجرائية على مستوى مراحل الدعوى العمومية وعليه سنتطرق الى التعديلات الاجرائية التي شملت مرحلة التحقيق والمتابعة ومرحلة المحاكمة وتقرير العقوبة .[5]

أولا: مرحلة التحقيق والمتابعة

أ- مرحلة التحقيق:

1 - التحقيق الابتدائي: يقصد بالضبط القضائي جميع الإجراءات التي تهدف الى التحري عن الجريمة والبحث عن مرتكبيها، وجمع كافة العناصر والدلائل اللازمة للتحقيق في الدعوى العمومية للتصرف على ضوئها، وهي اجراءات يتم اتخاذها منذ لحظة وقوع الجريمة نظرا بما تمتاز به

---

[1]- قانون رقم 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 يعدل ويتمم الأمر 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية جريدة رسمية عدد 71 أهم ما جاء فيها بالنسبة لموضوع الدراسة هو تمديد الاختصاص المحلي

[2]- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006والمتضمن قانون الإجراءات الجزائية الذي يضمن اساليب جديدة في التحري

[3]- مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق ل 07 نوفمبر سنة 2021 يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جريدة رسمية عدد 86

[4] - الأمر رقم 21-11 المؤرخ في : 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية جريدة رسمية رقم 65 يتمم الكتاب الأول من الأمر 155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 بباب سادس عنوانه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يتضمن المواد 211 مكرر 22 الى المادة 211 مكرر 29

[5]- عقباش بريزة،المرجع السابق، ص ص70.71

الجريمة الالكترونية من خصائص والتطور التكنولوجي لوسائل الإعلام والاتصال المبهر والسريع تلاه استحداث المشرع الجزائري الأساليب تحري خاصة تتناسب ومتطلبات ضبط الوجه الجديد للإجرام، حتى يسمح للقضاء وجهات التحقيق أن تتكيف بدورها في مهامهما مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر هذه الأساليب المرخص بها فقط الا في بعض الجرائم المعينة على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية استدركها المشرع بموجب تعديل قانون الاجراءات الجزائية[1].

-الإجراءات الجديدة التي جاء بها قانون رقم04-14 [2]تمديد الاختصاص في الحدود التي يباشرون ضمنها وظائفهم المعتادة : يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة نص المادة 16 الفقرة 1 من قانون الإجراءات الجزائية في كافة دائرة اختصاص المجلس القضائي الملحقين به في حالة الاستعجال : يباشرون مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به نص المادة 16 الفقرة الثانية من قانون الإجراءات الجزائية وعليهم ان يخبروا مسبقا وكيل الجمهورية الذين يباشرون مهمتهم في دائرة اختصاصه من نفس القانون[3].

-الاجراءات الجديدة في قانون 06-22 والذي نص على أساليب التحري الخاصة بالجريمة الإلكترونية[4]:

اعتراض المراسلات والتقاط الصور والصوت: من خلال المواد 65 مكرر 05 إلى المادة 65 مكرر 10 من قانون الإجراءات الجزائية نجد أن المشرع قد منح الضباط الشرطة القضائية وكل من له صفة الضبطية القضائية امكانية اعتراض المراسلات وتسجيل الأصوات والتقاطها، وهذا في الجرائم المصنفة ضمن الجرائم الخطيرة ويجوز لوكيل الجمهورية السماح للضبطية القضائية باعتراض المراسلات بواسطة استعمال الاتصال السلكي واللاسلكي ووضع اجهزة التنصت

[1]- عمر بن ياسين. المرجع السابق.ص228

[2] - القانون رقم 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 يعدل ويتمم الأمر 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

[3]- عقباش بريزة،المرجع السابق، ص ص71.72

[4] - القانون 06-22، والمتضمن قانون الإجراءات الجزائية ، المرجع السابق.

وتسجيل المكالمات والتقاط الصور، وحسب المادة 65 مكرر 05 من قانون الإجراءات الجزائية يمنح الإذن عن طريق وكيل الجمهورية أو قاضي التحقيق من أجل القيام بهذه الوظيفة يمكن استعمال معرفة ودراية اعوان المصلحة العمومية بحكم اختصاصهم في مجالهم .

-الاجراءات الجديدة التي جاء بها قانون 09-04 : مراقبة الاتصالات في اطار مكافحة الجريمة الإلكترونية[1]:

كما يمكن الاستعانة بالهيئة الوطنية للوقاية من الجرائم المتصل بتكنولوجيات الإعلام والاتصال ومكافحتها في مجال مراقبة الاتصالات الإلكترونية وهذا وفقا لما يلي:

نص المادة 4/3 : مراقبة الاتصالات الإلكترونية لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية نص المادة 4/4 : مراقبة الاتصالات الإلكترونية كإجراء مكافحة في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

2-التحقيق القضائي الابتدائي:

-الإجراءات الجديدة التي جاء بها قانون رقم 04-14 تمديد الاختصاص:

الاختصاص بناء على نص المادة 40 من قانون الإجراءات الجزائية : يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل اقامة احد الاشخاص المشتبه في مساهمتهم في اقترافها ، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر نص المادة 40 الفقرة الأولى 1[3].

[1] – القانون رقم قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– صالح بن منصور، وأنيسة كوش . السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة عبد الرحمان ميرة الجزائر .2015،ص22

[3]– القانون رقم 04-14، المتضمن تعديل قانون الإجراءات الجزائية، المرجع السابق

ب-المتابعة:

-**الإجراءات الجديدة التي جاء بها قانون رقم 04-14:** الاختصاص بناء على نص المادة 37 من قانون الإجراءات الجزائية : يتحدد اختصاص وكيل الجمهورية محليا بمكان وقوع الجريمة أو محل اقامة احد الاشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر تمديد الاختصاص الى المحكمة المختصة حسب نوع محدد من الجرائم من بينها الجريمة الالكترونية المادة 37 الفقرة الثانية.[1]

ثانيا: المحاكمة والعقوبة المقررة

أ المحاكمة : تضمن دستور الجزائر لسنة 2020 [2]نصوصا فيما يتعلق المحاكمة تتلخص مجملها فيما يلي : يصدر القضاء احكامه باسم الشعب المادة 166 تعلل الأحكام والأوامر القضائية . ينطق بالأحكام القضائية في جلسات علنية المادة 169 يحمي القانون المتقاضي من أي تعسف يصدر من القاضي المادة 174 الحق في الدفاع معترف به ، الحق في الدفاع مضمون في القضايا الجزائية المادة 175 تسيير المحاكمة بأكثر فاعلية من حيث سرعة تسيير والتصدي للملفات القضائية من حيث عامل التخصص للقضاة و الوسائل المتاحة[3].

1-الاختصاص النوعي والإقليمي للمحكمة: حيث أن المشرع الجزائري نص على جريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات من خلال المواد 394 مكرر 7 ، واعتبرها جنحا في جميع الأحوال ولم يقم المشرع الجزائري بتعريفها كما وضحنا سابقا واكتفى فقط بالإشارة إلى بعض الأفعال التي تبلور الركن المادي للجريمة[4].

---

[1]- القانون رقم 04-14، المتضمن تعديل قانون الإجراءات الجزائية، المرجع السابق.

[2] - دستور الجزائر 2020، مرسوم رئاسي رقم20-442 مؤرخ في30 ديسمبر 2020 ،يتضمن التعديل الدستوري

[3]- قربة سيد على عصماني سعيد، الطبيعة القانونية للأقطاب الجزائية المتخصصة وإجراءات سير الدعوى أمامها مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية قسم القانون العام، جامعة العقيد اكلي محمد أولحاج البويرة 2019 ، ص 47

[4] - القانون رقم 09-04، المتضمن تعديل قانون العقوبات، المرجع السابق.

2-سير محاكمة مرتكبي جريمة الكترونية : يخضع نظام المحاكمة امام المحاكم ذات الاختصاص الموسع للقواعد المقررة في القانون العام سواء تعلق الأمر بتلك المبادئ التي تحكم المحاكة أو الإجراءات المتبعة الى غاية صدور حكم فاصل في موضوع الجريمة المبادئ التي تقوم عليها اجراءات المحاكمة : وهي علانية الجلسة، شفافية المرافعة حضور الخصوم ، التدوين يناط لأمين الضبط مهمة تدوين الإجراءات والأحكام حيث يدخل في تشكيلة الجلسة ولا تنعقد الا بحضوره[1].

ب-العقوبات المقررة:

1- عقوبة الشخص الطبيعي : تخضع العقوبات الجزائية لمبدأي الشرعية والشخصية المادة 167 كل اجهزة الدولة المختصة مطالبة في كل وقت وفي كل مكان وفي جميع الظروف بالسهر على تنفيذ احكام القضاء المادة 178 ، يعاقب القانون كل من يمس باستقلالية القاضي أو يعرقل حسن سير العدالة وتنفيذ قراراتها .والعقوبات المقررة للجريمة الإلكترونية نوعان:

عقوبات اصلية :خاصة بكل جريمة الكترونية على حدى وفق نصوص قانون العقوبات سواء بعقوبة سالبة للحرية أو غرامة مالية ابتداء من نص المادة 394 مكرر الى 394 مكرر 5.

-**عقوبات تكميلية** : نصت عليها المادة 394 مكرر 6 من نفس القانون تتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة مع الحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها[2].

-**نظام ايقاف تنفيذ العقوبة** : وتنص المادة 592 من قانون الإجراءات الجزائية[3] : يجوز للمجالس القضائية والمحاكم في حالة الحكم بالحبس أو الغرامة اذا لم يكن المحكوم عليه قد سبق الحكم عليه بالحبس الجناية أو جنحة من جرائم القانون العام أن تامر بحكم مسبب بالإيقاف الكلي أو الجزئي التنفيذ العقوبة الأصلية .

---

[1]- الحاج علي بدر الدين ، جرائم الفساد واليات مكافحتها في التشريع الجزائري ، دار الأيام للنشر والتوزيع ، ج 1 ، ط1 2017 ص394.

[2]- صالح بن منصور، وأنيسة كوش . المرجع السابق ،ص24

[3] - القانون رقم 04-14 المتضمن تعديل قانون الإجراءات الجزائية، المرجع السابق

2- عقوبة الشخص المعنوي : نصت عليها نص المادة 394 مكرر 4 غرامة مالية تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي.[1]

المطلب الثاني: مكافحة جريمة السيبرانية على ضوء القانون رقم 09-04

وهو القانون الذي عرف الجريمة الإلكترونية وإدراجها ضمن الأعمال المعاقب عليها قانونا في المادة 02[2]، كما نص على مراقبة الاتصالات الإلكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتيه. [3]

الفرع الأول: آليات مكافحة الجرائم السيبرانية في قانون 09-04.

يتميز هذا القانون بأنه قانون أكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام والاتصال فنجد المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للمتصدي الجرائم المعلوماتية.

تتمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها ورصيد مرتكبيها وتدابير أخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية[4].

---

[1]- سحنين امال وموساوي خالد ، دوز المؤسسات العقابية في معالجة الجريمة في الجزائر، مذكرة لنيل شهادة الماستر المهني في تسيير المؤسسات ، كلية الحقوق والعلوم الإنسانية ، جامعة احمد دراية ادرار، 2018 .ص 39

[2] – المادة الثانية من القانون رقم 09-04، المتضمن تعديل قانون العقوبات، يشير إلى القانون رقم 09-04 المؤرخ في 5 غشت 2009، الذي يحدد القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[3]- قيطة فاطمة الزهراء ،صالحي دليلة،تعزيز الأمن السيبيراني في الجزائر ،المجلة الجهود القانونية العلمية و العملية ،ع 2019.3. ص8

[4]- المقدم عز الدين عز الدين ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية بسكرة في 16/11/2015.ص55

أولا : التدابير الوقائية المستحدثة.

لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، وهي كانت كالتالي:

-مراقبة الاتصالات الالكترونية التي نصت عليها المادة 04 من القانون رقم 09-04 [1]

فنجد الفصل الثاني منه بعنوان مراقبة الاتصالات الالكترونية فالحالات التي تسمح باللجوء إلى المراقبة الالكترونية فتنص المادة 04 من نفس القانون : تمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه كالحالات الآتية:

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

-في حالة توفر معلومات عنه احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو المؤسسات الدولة أو الاقتصاد الوطني.

-المقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تحمي الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية[2].

-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

-إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية : وذلك من خلال فرض عليهم من الالتزامات مذكورة في المواد 10 و 11 و 12 من نفس القانون.

[1] – القانون رقم 09-04، المتضمن تعديل قانون العقوبات، المرجع السابق.

[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.ص12

فحسب المادة 10 من قانون 09-04 من الفصل الرابع تحت عنوان التزامات مقدمي الخدمات مساعدة السلطات[1].

المادة 10: في إطار تطبيق أحكام هذا القانون ، بتعيين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية.

زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات الانترنت ما يأتي:

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

-وضع ترتيبات تقنية تسمح بحضر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها[2].

ثانيا: التدابير الإجرائية.

إضافة إلى التدابير الوقائية السالفة الذكر تبنى المشرع في القانون رقم 09-04 إجراءات تبنى بدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام والاتصال تتلخص فيما يلي:

-السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لفرض التفتيش ولو عن بعد المنظومة المعلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها.

-إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.

---

[1]- بيكة باكة ،موساوي لمياء،المرجع السابق، ص ص24.25

[2]- بوهرين فتيحة ، الجريمة المعلوماتية في الشريع الجزائري ، مجلة الحقوق والعلوم الإنسانية ، جامعة قسنطينة ، الجزائر ، العدد 04،ص66

في الأخير يتضح أن أحكام القانون رقم 09-04 جاءت عامة ومطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال، حيث يجرم كل الأفعال المخالفة للقانون التي تكن بوسائل الإعلام والاتصال ويطبق على كافة التكنولوجيات القديمة و الجديدة ، مما يجعله قانونا فعالا ويساير التطور التكنولوجي السريع .[1]

الفرع الثاني: القوانين اللاحقة المدعمة للقانون 09-04 للحد من الإجرام السيبراني

أدى التطور الكبير في عالم تكنولوجيا المعلوماتية وأجهزة الاتصال لاسيما منها الحواسيب وشبكة الانترنت إلى احتلالها مكانة خاصة في الحياة اليومية للمواطنين، لكن في المقابل ساهمت في بروز العديد من الجرائم المتصلة بهاء التي أصبحت تشكل هاجسا حقيقيا للكثير من الدول باعتبارها باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل على مكافحتها، سواء من خلال إبرام اتفاقيات الثانية ودولية أو وضع التشريعات وطنية للحد منها ومكافحتها، ولأن إفراد قانون خامس للحد ومكافحة الجرائم الالكترونية بات اليوم أكثر من ضرورة، حاولت الجزائر استحداث اليات قانونية تسمح بالحد من انتشار هذه الجرائم، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الجزائية، وتم تدعيمها بالقانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

أولا: القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية[3].

حيث استحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي منها، استحداث سلطة ضبط من بين مهامها السهر على احترام متعاملي البريد والاتصالات الالكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الالكترونية والأمن السيبراني

---

[1]- بيكة باكة ،موساوي لمياء،المرجع السابق، ص ص25.26

[2]- شيخ عبد الصديق،الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04،على الموقع الإلكتروني https://asjp.cerist.dz/en/article/116847:التاريخ الولوج:2025-04-23على الساعة 13:45

[3]- قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.ج ر ج ج،ع27

المادة 13 من القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر عدد 27 الصادرة بتاريخ 13 مايو 2018،ص10

-تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة، وسنت مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون[1].

ثانيا: القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2].

وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي يمكن إيجازها في عدة نقاط :

- ان استحداث سلطة وطنية الحماية المعطيات ذات الطابع الشخصي.

-وضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.

-اتحاد السلطة الوطنية المجموعة إجراءات إدارية في حالة حرق أحكام القانون من طرف المسؤول عن المعالجة.

-يمكن للسلطة الوطنية القيام بالتحريات ومعاينة المحلات و الأماكن التي تتم فيها المعالجة باستثناء محلات السكن، كما يمكنها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها.

[1]- مهدي رضا،المرجع السابق،ص121

[2]- قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو2018 ، ج ر ج ج،ع34

-تأهيل أعوان رقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات طابع شخصي تحت إشراف وكيل الجمهورية[1].

-يمكن للمدعي بالمساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية الحاد أي إجراءات تحفظية للحد من التعدي أو للحصول على تعويض.

-تختص الجهة القضائية الجزائرية بمتابعة هذه الجرائم التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية المادة 53 من القانون رقم 18-07 المؤرخ في 10 يونيو 2018،ص22.

-تجريم الاعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية و أخرى سالبة للحرية وفقا للمواد من 54 إلى 74 من هذا القانون[2].

ثالثا: قانون العقوبات في التعديل الأخير رقم 24-06

نتيجة الهجمات السيبرانية المتكررة سواء بالنسبة للأفراد أو على المؤسسات أو امن الدولة، وكثرة الشكاوى والقضايا المتواجدة على رفوف العدالة، خطى المشرع خطوة جديد من خلال إصداره لمجموعة من المواد تجرم بعض الأفعال المعلوماتية التي كانت في السابق أفعال عدائية دون تجريم، حيث تطرقنا لها في تصنيف الجرائم السيبرانية من خلال المواد 333 مكرر 3 ومايليها[3] ، من خلال جرائم التهديد، التشهير وتشويه السمعة...الخ من الجرائم السيبرانية.

[1]- بوهرين فتيحة ، المرجع السابق،ص68

[2]- مهدي رضا،المرجع السابق،ص122

[3] - القانون رقم 24-06 المتضمن قانون العقوبات المعدل والمتمم، المرجع السابق.

المبحث الثاني: مكافحة جريمة السيبرانية من خلال الأجهزة المختصة بها

تتزايد التهديدات السيبرانية بشكل مستمر مع تطور التكنولوجيا واعتماد المجتمع على الأنظمة الرقمية في مختلف المجالات. هذا التطور جعل من الجرائم السيبرانية تهديدا جديا للأمن الوطني، مما يستدعي تكوين هيئات متخصصة في البحث والتحري المكافحة هذه الجرائم. تلعب هذه الهيئات دورا حاسما في الكشف عن الأنشطة غير القانونية التي تستهدف الأفراد والمؤسسات والبنية التحتية الحيوية من خلال تزويدها بأحدث التقنيات وأفضل الكفاءات، تسعى الدول إلى تعزيز قدراتها على مواجهة الجرائم السيبرانية، حماية أمنها القومي، وضمان سلامة القضاء الرقمي[1].

و بالرغم أن الجريمة السيبرانية إلا أن الجزائر خصصت لها أجهزة و آليات فعالة من اجل اكتشاف مرتكب الجريمة على المستوى الوطني والدولي، وتسعى للانضمام إلى الاتفاقيات الدولية لمكافحة الجريمة السيبرانية والانضمام إلى اتفاقيات تسليم المجرمين الدوليين نظرا لخطورة هذا النوع من الجرائم و الذي قد يمتد أثرها إلى عدد كبير من دول العالم[2].

المطلب الأول: الأجهزة الأمنية العامة

إن أبرز الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم المعلوماتية، والتي ما تسند إليها عادة مهام الوقاية ومكافحة الجرائم المعلوماتية، نظرا لتشكيلتها البشرية الخاصة والتي تضم محققين من نوع خاص تجتمع لديهم صفة ضابط شرطة قضائية إضافة إلى المعرفة الواسعة بمجال النظم المعلوماتية والإجرام المعلوماتي، مما يسمح لهم ويؤهلهم لتولي مهام البحث والتحقيق في ميدان الجرائم المعلوماتية، سواء تمثلت في شخص وكيل الجمهورية أو قاضي التحقيق نظرا

[1]– لعور مرزوق،تازولت أكرم سيف الإسلام ،الجرائم الإلكترونية و الأمن السيبراني في الإتفاقيات الدولية و التشريع الجزائري، مذكرة نهاية الدراسة للحصول على شهادة ماستر، تخصص قانون جنائي، جامعة عباس لغرور خنشلة، 2023-202،ص83

[2]– واجعوط سعاد،المرجع السابق،ص421

لقلة خبرتهم بميدان النظم المعلوماتية وعلم تحكمهم في تقنيات البحث والتحقيق بواسطة وسائل معلوماتية خاصة تتطلب المعرفة والدقة في مجال استخدامها[1].

الفرع الأول: الهيئة الوطنية لمكافحة الجرائم المتعلقة بالتكنولوجية الإعلام.

استحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون رقم 09-04[2]، الذي يتضمن القواعد الخاصة بالوقاية من هذه الجرائم ومكافحتها. حيث نصت المادة 13 من هذا القانون على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن يتم تحديد تشكيلتها وتنظيمها وكيفية سير عملها عن طريق التنظيم.

وفيما يتعلق بتنظيم الهيئة وتشكيلتها وكيفية سيرها، أحال المشرع الجزائري ذلك إلى التنظيم من خلال نص المادة 13 المذكور أعلاه، وقد تم ذلك من خلال المرسوم الرئاسي رقم 19-172 الذي ألغى المرسوم الرئاسي رقم 15-261[3] واعتبر المشرع الجزائري الهيئة بموجب هذا المرسوم مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، وتوضع تحت سلطة وزارة الدفاع الوطني.

وفيما يخص تنظيم الهيئة، أشارت المادة 4 من المرسوم الرئاسي رقم 19-172 إلى أن الهيئة تتشكل من مجلسين مجلس توجيه ومديرية عامة. يترأس مجلس التوجيه وزير الدفاع أو ممثله، وتتألف الهيئة من ممثلين عن الوزارات التالية: وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

---

[1]- بوعجاجة بلال ،عراب ربيعة،الجريمة المعلوماتية و سبل مكافحتها في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة عباس لغرور،خنشلة ،2023-2024،ص46

[2]- قانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية، العدد 47، الصادرة بتاريخ 25 شعبان 061430 الموافق لـ 16 أوت 2009، ص6

[3]- مرسوم رئاسي رقم 19-172 مؤرخ في 06-06-2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها و تنظيمها وكيفيات سيرها جريدة رسمية رقم 37 لسنة 2019

أما عن كيفية سير عمل الهيئة، فقد نصت المادة 7 [1]من المرسوم الرئاسي رقم 19-172 على أن مجلس التوجيه يجتمع في دورة عادية مرتين في السنة بناءً على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا بناءً على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

وبخصوص مهام الهيئة تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 04/09 تحت رقابة السلطة القضائية، وفقا لأحكام قانون الإجراءات الجزائية والقانون رقم 04/09 وتشمل هذه المهام:

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بالجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

-تبادل المعلومات مع نظيراتها في الخارج لجمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم.

الفرع الثاني : جهازي الأمن الوطني و الدرك الوطني.

سعت المديرية العامة للأمن الوطني و جهاز الدرك الوطني في إنشاء فرق خاصة المكافحة الجرائم المعلوماتية، وكذا تكوين عناصر في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي متخصصة بالإضافة إلى توافر هادين الجهارين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام.

أولا : الوحدات التابعة لسلك الأمن الوطني.

تعد الجريمة الالكترونية وجه جديد للجرائم يستلزم استحداث هياكل جديدة وتدعيم الهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة لألمن الوطني، وعلى هذا الأساس قررت القيادة العليا للأمن الوطني استحداث مخابر وفصائل وحاليا مختصة في مكافحة

[1]- مرسوم رئاسي 15-261 مؤرخ في 2015/10/08، تعدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53 الصادرة بتاريخ 2015/10/08

الجرائم الالكترونية، وتقوم بعمليات التحسس والنوعية من خلال المشاركة في الملتقيات الوطنية و الدولية و جميع التظاهرات التوعية المواطن بالإضافة إلى دروس توعية في مختلف الأطوار الدراسية[1] .

أ- نيابة المديرية للشرطة العلمية على المستوى المركزي: قامت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية من خلال إنشاء وحدات متخصصة تعمل على مكافحة نوع معين من الجرائم دون سواها، وهذا باستحداث أربعة وحدات نيابية متخصصة تتمثل في:

-نيابة الشرطة العلمية والتقنية.

-نيابة مديرية الاقتصادية والمالية.

-نيابة القضايا الجنائية.

-مصلحة البحث والتحليل[2].

-الآليات المؤسساتية لمواجهة الجريمة الالكترونية: وما يهم في دراستنا هذه هي مديرية نيابة الشرطة العلمية والتقنية التي تتألف من مختبر مركزي على مستوى الجزائر العاصمة. و ثلاثة مخابر جهوية، ويحتوي كل مخير من دائرتين دائرة المشترطة العلمية وأخرى تقنية، وتتمثل المهمة الرئيسية للمخير المركزي بالمساهمة إلى جانب أجهزة العدالة في إظهار الحقيقة عن طريق تقديم المساعدات التي تطلبها الهيئات القضائية فيما يتعلق تفسير وتحليل الآثار المادية التي يعثر عليها في مسرح الجريمة أثناء عملية التحري والتحقيق[3].

ب- دائرة الأدلة الرقمية والآثار التكنولوجية على المستوى الجهوي: بالإضافة إلى المخبر المركزي الذي يتواجد بالجزائر العاصمة يوجد أيضا مخبرين جهويين على مستوى كل من قسنطينة ووهران يتوليان أعمال البحث والتحري في الجرائم، بما فيها الجريمة الالكترونية وهذا تحت تسمية

[1] -لامية وعلى كاهنة سعودي، إجراءات مكافحة الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية القسم القانون الخاص، كلية الحقوق والعلوم السياسية جامعة عبدا الرحمان ميرة بجاية الجزائر 2018/2019، ص ص 12 و 13

[2]

[3]- بوهرين فتيحة ، المرجع السابق،ص69

دائرة الأدلة الرقمية والآثار التكنولوجية والتي لم تكن سوى قسم عند استحداثها سنة 2004 ، وسبب الارتفاع المتزايد لقضايا الجرائم الالكترونية باستعمال تقنية

المعلومات تم ترقيتها إلى دائرة تصم ثالثة أقسام:

-قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات.

-قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

-قسم تحليل الأصوات.

في سنة 2010 تم حلق ما يقارب 23 خلية لمكافحة الجرائم الالكترونية موزعة على كل ربوع الوطن شرق، وسط، عرب و جنوب، وتكلف الدائرة بعدة مهام، من بينها البحث والتحري[1].

ثانيا: الوحدات التابعة للدرك الوطني.

اهتمت قيادة الدرك الوطني بمكافحة الجريمة الالكترونية بمختلف أشكالها وأنواعها، وهذا من خلال استخدام هياكل تابعة لها من أجل التصدي للإجرام المعلوماتي الذي بات يشكل تحديدا على أمن الدولة وسلامة المجتمع، فتم إنشاء أربعة وحدات تنشط في مجال الوقاية من الجريمة الالكترونية ومكافحتها.

فتعمل مؤسسة الدرك الوطني حادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا تسهيل مهمة البحث و المعاينة و التفتيش في أنظمة الحواسيب و العمل على مراقبة مختلف الشكات، وذلك حسب الاختصاص و الصلاحيات و طبيعة الجريمة إلى ثلاث 13 مستويات مركزية جهوية ، محلية[2].

أ- **على المستوى المركزي** : تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية و دعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

---

[1]- بيكة باكة،موساي لمياء،المرجع السابق،ص33

[2]- سعيدة يوزنون ، مكافحة الجريمة الالكترونية في التشريع الجزائري ، مجلة العلوم الإنسانية ، جامعة الإخوة منثوري قسنطة 09/07/2019 العدد 52،ص76

-**مديرية الأمن العمومي و الاستغلال** : هي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية و المركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

1-المصلحة المركزية للتحريات الجنائية : هي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة تكنولوجيا الإعلام والاتصال.

2 -المعهد الوطني للأدلة الجنائية وعلم الإجرام : مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 04/183 المؤرخ في 26جوان 2004[1]، في إطار عصرنة قطاع الدرك الوطني، مهامه تحليل الأدلة الخاصة بالجرائم المعلوماتية ، و ذلك بتحليل الدعامات الإلكترونية ، إنجاز المقاربات الهاتفية ، تحسين التسجيلات الصوتية و الفيديو و الصورة و ذلك التسهيل استغلالها[2].

وهذا فإن المعهد الوطني للأدلة الجنائية وعلم الإحرام يساهم بشكل فعال في مكافحة الجرائم المعلوماتية من خلال مهامه الخاصة بمتابعة أو دعم إجراءات البحث والتحقيق في الجرائم المعلوماتية فهو يتولى في هذا الشأن:

-القيام بالخبرات العملية أو الخيرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح، بما فيها تلك المتعلقة بالجرائم المعلوماتية.

-مساعدة المحققين للسير الحسن للمعاينات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.

-ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية .

- مشاركة ومساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإحرام في وضع سياسة مكافحة الإجرام.

[1] - المرسوم رئاسي رقم 04/183 المؤرخ في 26جوان 2004، المتضمن انشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام

[2]- بيكة باكة، موساي لمياء،المرجع السابق،ص34

3 –مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية[1] : أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية، ويقوم بالمهام التالية:

–ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

–القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون الفائدة وحدات الدرك الوطني و الجهات القضائية.

–مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال و البحث عن الأدلة في شبكة الانترنت.

–المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصباح الأمن و الهيئات الوطنية[2].

ب– على المستوى الجهوي : تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

ج– على المستوى المحلي : يجوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذوو خبرة واختصاص وامتعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية.

وذلك عن طريق القيام بتحقيقات تطلب تحريات معقدة ، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني.

[1] – مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية هو هيئة جزائرية تتبع وزارة الدفاع الوطني، ومهمتها الأساسية هي الوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– بيكة باكة،موساي لمياء،المرجع السابق،ص35

من خلال ما سبق عرضه ينضح لنا مدى تكاتف و تعزيز الجهود المتعلقة بترقية و دعم أعمال البحث والتحقيق بشأن الجرائم المعلوماتية ، من خلال تصنيفها على حدى وتخصيص أجهزة أمنية خاصة بمباشرة الأعمال المتعلقة بالبحث و التحقيق بشأنها ، وذلك نظرا لخصوصيتها من جهة والخصوصية مرتكبيها و أدلتها من جهة أخرى.[1]

المطلب الثاني: الاجهزة الأمنية المختصة

أدرجت الجزائر الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الالكترونية والارهاب الالكتروني، بل أصبح يشكل جزء لا يتجزأ من استراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال. أثبتت أن النجاعة في التطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان[2].

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

الفرع الأول: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

استحدثت بموجب القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي [3]، تقوم بمهام :

-وضع مجموعة التزامات على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.

-اتخاذ إجراءات إدارية في حالة حرق أحكام القانون من طرف المسؤول عن المعالجة أو من ينوبه.

---

[1]- بيكة باكة،موساي لمياء،المرجع السابق،ص36

[2]- جمال بوزدية،الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات و الأفاق المستقبلية "،مجلة العلوم القانونية و السياسية ،مج 10. ع 1.2019.ص1277

[3] - القانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات لذات الطابع الشخصي

-القيام بالتحريات و معاينة المحلات والأماكن التي تتم فيها المعالجة.

-تأهيل أعوان الرقابة للقيام بالبحث ومعاينة الجرائم المتعلقة بالمعطيات ذلت الطابع الشخصي تحت إشراف وكيل الجمهورية الرسمية، قانون 18-07 المتعلق بتحديد قواعد الأشخاص الطبعين في معالجة المعطيات ذات الطابع الشخصي،[1].

الفرع الثاني: الأقطاب القضائية الجزائية المتخصصة لمكافحة الجرائم الالكترونية.

بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية ، تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للمواد 9،32،40،37 منه، تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 384/06 المؤرخ في 5 جانفي 2006[2] حاليا في محكمة مقر المجلس وفقا للمادة 211 مكرر 22 و حاليا متواجد في محكمة دار البيضاء بالجزائر ، تختص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى و لو كان مرتكبيها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني .[3]

الفرع الثالث: مديرية المراقبة الوقائية واليقظة الالكترونية.

يتم تعيين مديرها بموجب مرسوم رئاسي موقع من رئيس الجمهورية كما يتم إنهاء مهامه بموجب نفس الطريقة، تتكفل مديرية المراقبة بالقيام بالعديد من المهام الضمان فعالية الهيئة نذكر منها على وجه الخصوص القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناءا على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، وإرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، بالإضافة لتنفيذ طلبات

---

[1]- بوهرين فتيحة ، المرجع السابق،ص84

[2] - المرسوم تنفيذي رقم 06 - 348 مؤ رّخ في 12 رمضان عام 1427 االوافق 5 أكتوبر سنة r2006 يتضمن تمديد الاختصاص. المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق

[3]- واجعوط سعاد،المرجع السابق،ص423

المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم[1] .

تتولى أيضا مهمة جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والعمل على تنظيم أو المشاركة في عمليات التوعية حول كيفية استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها ناهيك عن تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرة وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيره والحفاظ على الحالة الجيدة لمنشاته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة.[2]

الفرع الرابع : مديرية التنسيق التقني.

يتم تعيين مدير المديرية وإنهاء مهامه بموجب مرسوم رئاسي صادر عن رئيس الجمهورية ، تتولى بدورها مهام عديدة لكفالة أداء الهيئة بكافة فروعها وأجهزتها واجباتها وتحقيق الغرض من إنشائها حيث تتولى المديرية ممارسة المهام المتمثلة في انجاز الخبرات القضائية في مجال الجريمة الإلكترونية وآليات الرقابة المجتمعية في الجزائر اختصاص الهيئة، وكذا تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها وإعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

بالإضافة للقيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها[3].

[1] – بوهرين فتيحة، المرجع السابق، ص: 59.

[2] – سعيد زيوش .ظاهر بومدفع. الجريمة وآليات الرقابة المجتمعية في الجزائر، المجلة الجزائرية للعلوم الاجتماعية والانسانية، المجلد 09 العدد 02 جامعة حسيبة بن بوعلي الشلف الجزائر، 2021 ص 242

[3] – سعيد زيوش . المرجع السابق،ص243

الفرع الخامس: السلطة الوطنية لحماية المعطيات

تطورت المعطيات الشخصية بشكل متواتر مع تطور الانترنت، فمن التعرف على اسم الشخص وعنوانه الالكتروني، إلى صورته وصوته وهويته وبياناته المالية والاجتماعية والبيو مترية، الأمر الذي يجعل منها بيانات غاية في الأهمية والحساسية باعتبارها ترتبط بالحياة الخاصة للشخص[1].

في ظل هذا الواقع أصبحت المعطيات ذات الطابع الشخصي متداولة بشكل واسع وسهل خاصة مع تطور والاتصال والتخزين للملفات، مما استدعى كبرى الدول إلى صياغة تشريعات الحماية المعطيات ذات سي، ومن بينها المشرع الجزائري الذي لا طالما شدد على حماية الحق في الخصوصية لكل شخص، حيث أشار في التعديل الدستوري لسنة 2016 إلى أنه لا يجوز بأي شكل المساس بانتهاك حرمة الحياة الخاصة للمواطن، وحرمة شرفه وسرية المراسلات والاتصالات الخاصة، دون أمر معلل من السلطة القضائية الذي ويعاقب القانون على انتهاك ذلك، كما أدرج لأول مرة حق حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الذي يحميه القانون ويعاقب على انتهاكه.[2]

[1]– سعيدة يوزنون ، المرجع السابق،ص78

[2]– بوعجاجة بلال ،عراب ربيعة ،المرجع السابق، ص ص50.51

خلاصة الفصل الثاني:

في ختام هذا الفصل الثاني الموسوم بالأحكام القانونية و الأجهزة المختصة لمكافحة الجريمة السيبرانية، نخلص بالقول أن موضوع الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري من خلال البحث عن مدى توفيق المشرع الجزائري في قانون العقوبات عن مختلف انواع وصور هذه الجريمة المعلوماتية، وإدراج عقوبة لكل نوع، وذلك من خلال المواد 394 مكرر الى غاية 394 مكرر 7 من قانون العقوبات المعدلة والمتمم الى غاية القانون 16- 02 المؤرخ في 19/06/2016، وكذا أركانها وسبل مكافحتها.

الخاتمة

إن الجريمة السيبرانية باعتبارها من الجرائم المعلوماتية المعاصرة، التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية انترنت"، بسبب التقدم العلمي الحاصل ساعد على انتشار و تنوع هذا السلوك الإجرامي والذي أصبح يهدد الإنسان في مختلف المجالات لا سيما الاقتصادية والاجتماعية والثقافية والأخلاقية وحتى المعتقدات الدينية لذلك وأمام الانتشار الواسع لهذا النمط الإجرامي الجد متطور والذي تستخدم فيه أحدث التقنيات التكنولوجية العالية والمتطورة وسرعة وحيلة وبداهة مرتكبيها التي تجعلهم دائما يفلتون من العقاب في ظل غياب الدليل المادي للجريمة إضافة إلى غياب منظومة تشريعية وطنية تحدد الفعل، تجرمه، ثم تحدد العقوبة المناسبة لمرتكبة انعكس ذلك سلبا على المستوى الدولي، فعلى الرغم من وجود العديد من الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية التي سبق التطرق إليها إلا أنها تبقى غير كافية في غياب تظافر للجهود الدولية والتي تسعى في مجملها إلى اتخاذ التدابير اللازمة للحد من هذه الجرائم بالنظر إلى الطبيعة الخاصة لها كونها من

الجرائم الدولية العابرة للحدود.

و في السياق الجزائري، يعكس التشريع الوطني التزام الحكومة بمكافحة الجريمة السيبرانية وحماية الأمن المعلوماتي، من خلال تطوير قوانين متخصصة وتحديثها بما يتماشى مع التطورات العالمية. ورغم ذلك، تظل هناك حاجة لتعزيز التنفيذ الفعلي لهذه القوانين وتوفير التدريب اللازم للجهات المعنية.

على هذا الأساس استخلاصنا من خلال هذه الدراسة إلى صياغة مجموعة من النتائج و المقترحات.

أولا: النتائج

-الجريمة السيبرانية جعلت من كل الأنظمة المعلوماتية للمؤسسات السيادية، الشركات الكبرى المراكز المالية والحسابات الخاصة للأفراد عرضة للاختراق والتهديد من أجل الابتزاز المساومة والتجسس، رغم ما توفره الدولة من وسائل مادية التقنية والبشرية للحماية.

–الصراعات الدولية أصبحت حافز رئيسي لطغيان الجريمة السيبرانية على جميع مجالات الحياة الدرجة أن المخاطر الآنية والمستقبلية قد بلغت مستويات من شأنها المساس بالأمن الوطني، القومي والعالمي مما يستدعي إطلاق صفرات الإنذار لإعادة النظر في المنظومة الأمنية.

–ردود الافعال المطالبة بإرساء آليات فعالة للتعاون. تأكد أهمية الضغوط المجتمعية الحمل الحكومات على تجاوز حواجز الصراع للحد من المخاطر. وما تبذله الدول من مجهودات إنما هو استجابة لهذه المطالب للحد من مخاطر الهجمات السيبرانية، إلا أن العقبات المصلحية والصراعات بين الفاعلين في المجال وقفت عائقا، مما جعل من القابلية العطب ترافق كل المبادرات منذ اطلاقها.

–الجرائم السيبرانية تزداد خطورة في ظل التطور التكنولوجي و الالكتروني الرقمي و الشبكة الانترنت و استخدام مواقع التواصل الاجتماعي.

–عدم النوعية و النشر بثقافة الأمن السيبراني ومعاقبة المرتكبين لها يؤدي إلى زيادة انتشار هذه الجرائم.

–تزايد الجرائم الإلكترونية تشهد العقدان الأخيران نمواً كبيراً في وتيرة الجرائم الإلكترونية، مما يستدعي استجابات قانونية وتقنية فعالة لمواجهتها. هذا الازدياد يبرز الحاجة الملحة لتعزيز الأمن السيبراني الحماية الأفراد والمؤسسات.

–الاتفاقيات الدولية لعبت الاتفاقيات الدولية، مثل اتفاقية بودابست، دوراً هاما في وضع معايير عالمية لمكافحة الجرائم الإلكترونية، مما يعزز التعاون بين الدول المواجهة هذه التحديات المشتركة. هذه الاتفاقيات تسهم في تعزيز الأمن السيبراني من خلال وضع أسس قانونية موحدة تسهل تبادل المعلومات والتنسيق بين الدول.

–وتبقى الجريمة السيبرانية أكثر أنواع الجرائم تعقيدا وخطرا، إلى جانب صعوبة ضبطها بفعل التحديث الهائل في تقنياتها وأساليبها وأشكالها المتفردة والمتعددة، إلا أن ذلك لم يمنع من محاولات ناجحة دولية ووطنية والحد من مخاطرها ولو بشكل جزئي، فهي كانت ولازالت تسعى دائما لإجاد الحلول المناسبة من خلال التحري والبحث وتوفير الإمكانيات اللازمة ومن التشريعات المطلوبة.

ثانيا : الاقتراحات

– تحديث التشريعات الجزائرية : يجب على الجزائر تحديث قوانينها المتعلقة بالجرائم السيبرانية بما يتماشى مع المعايير الدولية والتطورات التقنية، لضمان فعالية التصدي للتهديدات السيبرانية وحماية الأمن السيبراني.

–تعزيز التعاون الدولي توسيع نطاق التعاون مع الدول الأخرى والمنظمات الدولية لتبادل المعلومات والخبرات في مجال مكافحة الجرائم الإلكترونية، مما يعزز الجهود المشتركة في تعزيز الأمن السيبراني العالمي وتنسيق الاستجابات للتهديدات العابرة للحدود.

–العمل على استحداث ضبطية قضائية متخصصة في مجال الجرائم السيبرانية.

–الاهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة المطلوبة منهم.

–يتعين بشكل حاسم إيجاد وسائل فعالة لتعزيز التعاون الدولي في مواجهة الجريمة الإلكترونية، وذلك من خلال تحقيق توافق بين التشريعات المتعلقة بها من خلال الاتفاقيات الدولية. يكمن أهمية ذلك في الاستفادة من مصادر المواقع العلمية التي تعتبر ذات قيمة في فهم أوجه التواصل الاجتماعي وتحليلها.

– تحديث وتعديل وسائل البحث والتحقيق يصبح ضروريا، خاصة في مجال الجرائم الإلكترونية حيث لا تترك آثارا واضحة. يشدد على أهمية تقليص أو تجاوز الإجراءات الروتينية الطويلة التي تستهلك وقتا كبيرا.

–تمكين وحدات عسكرية وأمنية خاصة تتولى بالتعاون على المستوى الخارجي، مع الهيئات العاملة على مكافحة المخاطر والحد منها ومن أثارها.

–يجب الإستفادة من التجارب الدولية الرائدة في هذا المجال.

–على جميع الدول أن تعمل على حماية الشبكات وأنظمة تقنية المعلومات وإنشاء هيئة وطنية للأمن السيبراني في كل دوله، يكون من أبرز أهدافها مكافحه هذه الجريمة قبل وقوعها.

تم بعون الله

قائمة المصادر والمراجع

المصادر:

1. القواميس:

- قاموس أكسفورد تحيين 2019

2. الدساتير:

- الدستور الجزائري لسنة 2020

3. النصوص القانونية:

– القانون رقم 04–15 المؤرخ في 10 نوفمبر 2004 للعدل والمتمم للأمر 06/156، للتضمن جرائم المساس بأنظمة المعالجة الآلية ج.ر ، عدد71 لسنة2004

– قانون 24–06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2004، يعدل ويتمم الأمر رقم 15646 المؤرخ في 18 صفر عام 1386 الموافق 3 يونيو سنة 1966 والمتضمن قانون العقوبات،ج ر رج،ع 30

–القانون رقم 01–14 مؤرخ في 20 جمادي الأولى عام 1422 الموافق 18 تخت سنة 2001 يتعلق بتنظيم حركة المرور عبر الطرق وسلامتها وامتها، ج ر ج ج،ع46

–قانون رقم 09 – 04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.ج ر ج ج ،ع47

–قانون رقم 18–04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.ج ر ج ج،ع27

–قانون رقم 18–07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو2018 ،المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ج ر ج ج،ع34

ب-الأوامر

- الأمر رقم 21-11 المؤرخ في : 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية جريدة رسمية رقم 65 يتمم الكتاب الأول من الأمر 155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 بباب سادس عنوانه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يتضمن المواد 211 مكرر 22 الى المادة 211 مكرر 29

ج -النصوص التنظيمية

-مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق ل 07 نوفمبر سنة 2021 يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جريدة رسمية عدد 86

-مرسوم رئاسي 15-261 مؤرخ في 2015/10/08، تعدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53 الصادرة بتاريخ 2015/10/08

-مرسوم رئاسي رقم 19-172 مؤرخ في 06-06-2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها و تنظيمها وكيفيات سيرها جريدة رسمية رقم 37 لسنة 2019

- المرسوم التنفيذي رقم 348/06 المؤرخ في : 12 رمضان عام 1427 الموافق 05 / اكتوبر سنة 2006 يتضمن تمديد الاختصاص المحلى البعض المحاكم ووكلاء الجمهورية وقضاة التحقيق جريدة رسمية رقم : 63

المؤلفات

أ-الكتب

1-العامة:

-الحاج علي بدر الدين ، جرائم الفساد واليات مكافحتها في التشريع الجزائري ، دار الأيام للنشر والتوزيع ، ج 1 ، ط1 2017

-الطيب بلواضح، الجريمة في القضاء الإلكتروني، دار وائل للنشر والتوزيع، (د.م.د) (د ب ن)، (ط1)، 2020

-الغافري، حسين، دراسة في الجهود الدولية في مواجهة جرائم الإنترنت، من منشورات المنشاوي للدراسات والبحوث.2007.

-بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي .2008.

-رؤوف عبيد السببية في القانون الجنائي ، مطبعة الاستقلال.1996.

-غانم مرضي الشمري، الجرائم المعلوماتية ، الدار العلمية الدولية ، عمان ، الطبعة الأولى ، 2016م

-محمود نجيب حسني، الفقه الجنائي الإسلامي، دار النهضة العربية، 2008.

-ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996

-ناير نبيل، عمر الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية دار الجامعة الجديدة ، مصر ، 2012

-يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والانترنت، 14 ، دار العدالة ، عمان ، 2011

-عبد الصادق عادل ، (2017) الحروب السيبرانية تصاعد القدرات والتحديات للأمن العالمي المركز العربي لأبحاث الفضاء الإلكتروني، د.ش، القاهرة

2-المتخصصة:

- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية .1992

-د سامي الشوا " ثورة المعلومات وانعكاساتها على قانون العقوبات "، الطبعة الثانية، دار النهضة العربية للنشر، القاهرة ، 1998

-عامر بزرا فايز أو أبو علي - فيروسات الكمبيوتر دار ضنين للنشر، عمان الطبعة الأولى، 1994.

-زياد القاضي و اخرون: مبادي تقليل نظم الحامون وتصميا ، الطبعة الأولى - دار الصفاء للنشر. 13 عمان، 1997

-عبد العزيز بن غرم الله آل جار الله ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة ويليه آثار العولمة على مستخدمي الإنترنت ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، 2018م

ب- الأطروحات والرسائل والمذكرات

1-أطروحات:

- بدري فيصل ، مكافحة الجريمة في القانون الدولي والداخلي ، أطروحة دكتوراه في القانون العام كلية الحقوق، جامعة الجزائر - 2018

- بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي - دراسة مقارنة - أطروحة دكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة ، كلية الحقوق بجامعة محمد خيضر بسكرة ، الجزائر ، 2018

- هدى سالم محمد الأطرقجي، التكيف القانون للجرائم في القانون العقوبات العراقي، رسالة لنيل درجة دكتوراء كلية القانون جامعة الموصل ،2000

-جلعود وليد غسان سعيد . دور الحرب الإلكترونية في الصراع العربي الإسرائيلي.أطروحة ماجستير في التخطيط والتنمية السياسية، بكلية الدراسات العليا، جامعة نابلس، فلسطين.2013.

-عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة دكتوراه جامعة نايف للعلوم الأمنية، كلية الدراسات العليا،2010

2-رسائل ماجستير:

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج الخضر، باتنة ، الجزائر ، 2013

- صالح بن منصور، وأنيسة كوش . السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة عبد الرحمان ميرة الجزائر.2015

- قارة آمال ، الجريمة المعلوماتية ، ماجستير تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق بجامعة الجزائر 2005

- يوسف الصغير، الجريم المرتكبة عبر الأنترنيت، رسالة مقدمة لنيل درجة ماجستير في كلية الحقوق والعلوم السياسة، جامعة مولد معمر، الباري وزي 2003

-مرابطين حياة ، الجريمة الالكترونية في التشريع الجزائري، رسالة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية - جامعة عبد الحميد بن باديس2018.2019

3-مذكرات الماستر:

- المفتيحة مهري، جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي ، الجزائر 2016/2015

- بوعجاجة بلال ،عراب ربيعة،الجريمة المعلوماتية و سبل مكافحتها في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة عباس لغرور،خنشلة ،2023-2024

- بيكة باكة ،موساوي لمياء،آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري ،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و العلوم الجنائية ،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الشيخ أمود بن مختار إيليزي،2022-2023

- جميلة غربي، آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية قسم القانون العام كلية الحقوق والعلوم السياسية، جامعة أكلي محمد أولحاج البويرة، الجزائر، 2020-2021

- سحنين امال وموساوي خالد ، دوز المؤسسات العقابية في معالجة الجريمة في الجزائر، مذكرة لنيل شهادة الماستر المهني في تسيير المؤسسات ، كلية الحقوق والعلوم الإنسانية ، جامعة احمد دراية ادرار، 2018

- سليمان أبو نمر ،يوسف بوكشريدة،مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة نهايةالدراسة للحصول على شهادة ماستر.تخصص قانون دولي عام ،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد خيضر بسكرة،2020-2021

- عقباش بريزة،مبارك حنان ،آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة نهايةالدراسة للحصول على شهادة ماستر .تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد البشير الإبراهيمي،برج بوعريريج،2021-2022

- قربة سيد على عصماني سعيد، الطبيعة القانونية للأقطاب الجزائية المتخصصة وإجراءات سير الدعوى أمامها. مذكرة لنيل شهادة الماستر في القانون .تخصص قانون جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية .قسم القانون العام، جامعة العقيد اكلي محمد أولحاج البويرة .2019

– لامية وعلى كاهنة سعودي، إجراءات مكافحة الجريمة الالكترونية، مذكرة مقدمة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية القسم القانون الخاص، كلية الحقوق والعلوم السياسية جامعة عبدا الرحمان ميرة بجاية الجزائر 2018/2019

– لعور مرزوق،تازولت أكرم سيف الإسلام ،الجرائم الإلكترونية و الأمن السيبراني في الإتفاقيات الدولية و التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي،قسم،جامعة عباس لغرور خنشلة،2023–2024

–جوالي عبد الستار،جرائم الحاسوب (دراسة مقارنة بين الشريعة الإسلامية و القانون الجزائري)،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص شريعة و قانون ،شعبة العلوم الإسلامية ،كلية العلوم الإجتماعية و الإنسانية،جامعة الشهيد حمه لخضر الوادي،2014–2015

ج– المقالات

– المختن، عبيد صالح . سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية. مجلة الفكر الشرطي .مج، 24، ع4. 2015

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

– جمال بوزدية،الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات و الأفاق المستقبلية "،مجلة العلوم القانونية و السياسية ،المجلد 10.العدد 2019.1

– راضية عيمور الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية المبحوث القانونية والسياسية، العدد 202201، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة الأغواط، الجزائر

– سعيد زيوش .ظاهر بومدفع. الجريمة وآليات الرقابة المجتمعية في الجزائر، المجلة الجزائرية للعلوم الاجتماعية والانسانية، المجلد 09 العدد 02 جامعة حسيبة بن بوعلي الشلف الجزائر، 2021

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

– عمر بن ياسين. المعالجة القانونية للجرائم الإلكترونية في التشريع الجزائري والتشريعات المقارنة التشريع المغربي والإماراتي الموذجا، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 3 .2019.

– قطاف سليمان ، بوقرين عبد الحليم،مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية،مجلة البحوث القانونية و الاقتصادية،المجلد 5،العدد 2،الأغواط. الجزائر. 2022

– قيطة فاطمة الزهراء ،صالحي دليلة،تعزيز الأمن السيبيراني في الجزائر ،المجلة الجهود القانونية العلمية و العملية ،العدد3 .2019.

– محمد بدوسي،تصنيف الجرائم الإلكترونية وفقا لطبيعة الحق المعتدى عليه دراسة مقارنة بين التشريع الفلسطيني و الإماراتي،مجلة جامعة العين لأعمال و القانون ، جامعة الإستقلال فلسطين

– مخلد إبراهيم الزعبي ،فاعلية القوانين و التشريعات العربية في مكافحة الجرائم الإلكترونية دراسة مقارنة ،المجلة العربية للنشر العلمي ،العدد ،37.2021.قطر

– واجعوط سعاد ،مكافحة الجريمة السيبرانية على المستوى الوطني،المجلة دفاتر البحوث العلمية،المجلد 12،العدد2.2024. الجزائر

–روان بنت عطية الله الصحفي ،الجرائم السيبرانية،المجلة الإلكترونية الشاملة متعددة التخصصات،العدد24،جدة المملكة العربية السعودية.2020

–مهدي رضا ،الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري،مجلة إيليزا للبحوث و الدراسات،المجلد 6.العدد 02 ،جامعة محمد بوضياف المسيلة،2021

–نورهان محمد الربيعي ،الجريمة السيبرانية و آليات مكافحتها (دراسة مقارنة)،مجلة الفارابي للعلوم الإنسانية ،المجلد 3،العدد 1،الإمارات العربية المتحدة،2024

–هادفي تاج الدين ،إستراتيجية الجزائري في مواجهة الجرائم السيبرانية التي تهدد أمنها السيبراني ،ملتقى الوطني الأمن السيبراني و رهانات الأمن الشامل في الجزائر ،مخبر التنمية الاجتماعية و خدمة المجتمع ،كلية العلوم الإنسانية و الإجتماعية ،جامعة الشهيد حمه لخضر الوادي ،يوم 13.14ماي2024

د–الملتقيات

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

– 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

هـ– المحاضرات

– سمير شعبان،الجريمة الإلكترونية ،مقاربة تحليلية لتحديد مفهوم الجريمة و المجرم ،محاضرات جامعية ،جامعة باتنة

–رامي حليم ،جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات،محاضرات جامعية ،جامعة سعد دحلب ،بليدة

و–المواقع الإلكترونية

–شيخ عبد الصديق،الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09–04،على الموقع الإلكتروني: https://asjp.cerist.dz/en/article/116847

الفهرس والمحتويات

الفهرس	الصفحة
الإهداء	
الشكر والتقدير	
قائمة المختصرات	
مقدمة	1
الفصل الأول: الإطار المفاهيمي للجريمة السيبرانية	7
المبحث الأول : ماهية الجريمة السيبرانية	8
المطلب الأول: مفهوم الجريمة السيبرانية	8
الفرع الأول: تعريف الجريمة السيبرانية	9
الفرع الثاني: خصائص الجريمة السيبرانية	12
الفرع الثالث: أنواع الجريمة السيبرانية	13
المطلب الثاني: طبيعة القانونية للجريمة السيبرانية وأركانها	16
الفرع الأول : الطبيعة القانونية للجريمة السيبرانية و وسائل تهديداتها	16
الفرع الثاني : أركان الجريمة السيبرانية	18
المبحث الثاني: تصنيفات الجريمة السيبرانية	24
المطلب الأول : الجرائم المعلوماتية تبعاً لنوع المعطيات ومحل الجريمة.	24
الفرع الأول : الجرائم الماسة بقيمة المعطيات الحاسوب.	24
الفرع الثاني : الجرائم الماسة بالمعطيات الشخصية البيانات المتصلة بالحياة الخاصة	29

الفرع الثالث: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه	30
المطلب الثاني : تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة و الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال.	32
الفرع الأول : تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة.	32
الفرع الثاني : تصنيف الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال.	34
خلاصة الفصل الأول	40
الفصل الثاني: الأحكام القانونية و الأجهزة المختصة لمكافحة الجريمة السيبرانية	42
المبحث الأول : مكافحة جريمة السيبرانية من خلال النصوص القانونية	43
المطلب الأول: مكافحة جريمة السيبرانية على ضوء القانون العقوبات و القانون الإجراءات الجزائية	43
الفرع الأول: مكافحة جريمة السيبرانية في قانون العقوبات	44
الفرع الثاني: مكافحة جريمة السيبرانية في قانون الإجراءات الجزائية	52
المطلب الثاني: مكافحة جريمة السيبرانية على ضوء القانون 09-04	57
الفرع الأول: آليات مكافحة الجرائم السيبرانية في قانون 09-04.	58
الفرع الثاني: القوانين اللاحقة المدعمة للقانون 09-04 للحد من الإجرام السيبراني	60

المبحث الثاني: مكافحة جريمة السيبرانية من خلال الأجهزة المختصة بها	64
المطلب الأول: الأجهزة الأمنية العامة	65
الفرع الأول: الهيئة الوطنية لمكافحة الجرائم المتعلقة بالتكنولوجية الإعلام	66
الفرع الثاني: جهازي الأمن الوطني و الدرك الوطني	71
المطلب الثاني: الاجهزة الأمنية المختصة	71
الفرع الأول: سلطة وطنية لحماية المعطيات ذات الطابع الشخصي.	72
الفرع الثاني: الأقطاب القضائية الجزائية المتخصصة لمكافحة الجرائم الالكترونية.	72
الفرع الثالث: مديرية المراقبة الوقائية واليقظة الالكترونية.	72
الفرع الرابع : مديرية التنسيق التقني.	73
الفرع الخامس: السلطة الوطنية لحماية المعطيات	74
خلاصة الفصل الثاني	75
الخاتمة	77
قائمة المراجع	82
الفهرس والمحتويات	91

ملخص مذكرة الماستر

إن تطور التكنولوجيا واتجاه الجزائر نحوى رقمنة جميع القطاعات يساعد في نشر الجريمة السيبرانية ونظرا لخصائصها التي تتميز وتنفرد بها و أبعادها الخطيرة ، أدى بالمشرع الجزائري إلى وضع آليات قانونية من اجل الوقاية ومكافحة الجريمة السيبرانية وكذلك و تكريس مجموعة من القاعد القانونية التي تعاقب مرتكبيها على المستوى الوطني.

باتت الجرائم السيبرانية نوع جديد من أنم اط الجريمة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم ، إذا ما تركت على الأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها خاصة جهود الأمم المتحدة، منها اتفاقية بودابست لمكافحة الجرائم السيبرانية، واتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم نظرا لما تتمتع به تلك الجريمة من خاصية اللاحدودية.

الكلمات المفتاحية

1-الجريمة السيبرانية 2- الأجهزة الأمنية 3- العقوبات الجريمة 4- الوسائل العلمية التقنية 5- الأدلة الرقمية.

Abstract of The master thesis

The development of technology and Algeria's move toward digitizing all sectors contributes to the spread of cybercrime. Given its unique characteristics and dangerous dimensions, this has led Algerian lawmakers to establish legal mechanisms to prevent and combat cybercrime, as well as to establish a set of legal rules that punish its perpetrators at the national level.

Cybercrime has become a new type of crime, characterized by its transnational nature. This has led the international community to cooperate to combat these crimes, which, if left unchecked, threaten national security in all aspects. Therefore, countries have sought to take joint measures to combat these crimes, by concluding international agreements and conventions to combat them, particularly the efforts of the United Nations, including the Budapest Convention on Cybercrime, the League of Arab States Convention, and bilateral and multilateral extradition agreements, which are among the most important methods of combating these crimes, given their transnational nature.

Reintegration of detainees :

1-Cybercrime 2- Security agencies 3- Crime penalties 4- Scientific and technical means 5- Digital evidence.