وزارة التعليم العالي والبحث العلمي

Ministry of High Education and Scientific Research

جامعة محمد البشير الإبراهيمي برج بوعريريج

University of Mohamed el Bachir el Ibrahimi–Bba

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في الحقوق

تخصص: قانون الإعلام الالي والانترنت

الوقاية من الجريمة الالكترونية في التشريع الجزائري

إعداد الطالبتين:

- ضيف حياة
- بلقرع نور الهدى

إشراف:

الدكتور:دريسي عبد الله

لجنة المناقشة

بن محمود بوزيد	استاذ محاضر أ	رئيسا
دريسي عبد الله	أستاذ محاضر ب	مشرفا ومقررا
صديقي سامية	أستاذ محاضر أ	ممتحنا

السنة الجامعية: 2024 / 2025

* الملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا المعضي أسفله،

السيد(ة): ..... الصفة: طالب، أستاذ، باحث .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: ..... والصادرة بتاريخ .....

المسجل(ة) بكلية / معهد: ..... قسم: .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: .....

.....

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

التاريخ: .....

توقيع المعني (ة)

شوهد لأجل التصديق

الوحيد: .....

بطاقة التعريف الوطنية رقم: .....

سلمت في: .....

العناصر في: .....

رئيس المجلس الشعبي البلدي ينوب عنه

ضابط الحالة المدنية

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): بلقرع نور الهدى الصفة: طالب، أستاذ، باحث

الحامل(ة) لبطاقة التعريف الوطنية رقم: 121011164033870005 والصادرة بتاريخ: 2019/08/24

المسجل(ة) بكلية / معهد: العلوم السياسية قسم: الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الوقاية من الجريمة الإلكترونية في التشريع الجزائري

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

التاريخ: .....

توقيع المعني (ة)

شوهد لأجل التصديق
الرئيس المحلي البلدي و بتفويض منه
رئيس مصلحة الحالة المدنية
2020 Dec 24


بسم الله الرحمن الرحيم

التشكرات

كل الامتنان لمن قدّم لي يد العون في لحظات الحاجة وكان دعمُه الصادق سببًا في تجاوز الصعاب وتحقيق هذا الإنجاز.

كما أخصّ بالشكر أستاذي الفاضل، لما أبداه من صبر وتفهّم وما قدّمه من توجيه طوال هذه الرحلة.

إهداء

إلى العزيز الذي حملت اسمه فخرًا، وإلى من كلّله الله بالهيبة والوقار، إلى من حصد الأشواك عن دربي وزرع لي الراحة بدلًا منها... إلى أبي.

لم يحْنِ ظهر أبي ما كان يحمله، بل انحنى ليحملني حبًّا لا حِملًا. وكنت أحجب عن نفسي مطالبها، فكان يكشف عني ما اشتهى الحجب، وشكرًا لكونك أبي.

إلى من علّمتني الأخلاق قبل تعلّمها، إلى الجسر الصاعد بي إلى الجنة، إلى اليد التي أزالت عن طريقي العقبات، ومن ظلّت دعواتها تحمل اسمي ليلًا ونهارًا... أمي، محبوبتي وملهمتي.

وإلى من وهبني الله نعمة وجودهم، وإلى مصدر قوتي وأرضي الصلبة وجدار قلبي المتين... إخوتي.

وإلى من ضاقت بي الدنيا، فسَعَتْ بي خُطاهم، وإن سقطتُ كانوا أول من رفعني بكلماتهم، إلى من رافقني بالقلب قبل الدرب... أصدقائي وأحبتي.

ها أنا اليوم طويت صفحة من التعب، وسجّلت في تاريخي فخرًا لا يُنسى. لم أعد أتساءل عن ملامح الوصول، فقد رأيتها في عيوني.تلاشت غيوم التعب وابتسم الأفق بعد عتمة الانتظار، وها هي الخطى التي كانت تتعثّر أحيانًا وجدت مستقرّها في قمّة الإنجاز. وبين طيّات الطريق، تنفّستُ سلامًا وفرحًا وامتنانًا.

وآخر دعوانا أنِ الحمد لله رب العالمين.

حياة

إهداء

إلى من غرسا في قلبي حبّ العلم،

وسهرا من أجلي الليالي،

إلى نبض حياتي... والديّ العزيزين،

أهديكما ثمرة جهدي ونجاحي، فبفضل دعائكما وصلت.

نور الهدى

قائمة المختصرات:

ص: صفحة

ق إ ج ج : قانون الإجراءات الجزائية

إ أ م إ م : الاتفاقية الاوروبية لمكافحة الاجرام المعلوماتي

ق إ ج ف : قانون الاجراءات الجنائية الفرنسي

ج ر ج ج : الجريدة الرسمية للجمهورية الجزائرية

مـقدمـــة

مقدمة :

أدى التطور الهائل في عالم تكنولوجيا المعلوماتية ووسائل والاتصال إلى تعاظم دورها بشكل كبير في شتى مجالات الحياة، وأصبحت الحواسيب وشبكة الأنترنت تحتل مساحة هامة في الحياة اليومية للمواطن وبات يعتمد عليها بشكل شبه كلي في تسيير شؤونه اليومية، وتسيير مختلف المرافق الإدارية والعلمية والاقتصادية، الأمر الذي يتطلب توفير أقصى درجات الحماية لهذه الوسائل الحديثة وما يحيط بها تجنبا لتعطيل سير تلك المرافق الحيوية أو الاعتداء عليها بما يؤثر على المصالح والخدمات التي بانت تقدمها في عالم اليوم .

رغم الإيجابيات والفوائد الكثيرة لهذا التطور في التكنولوجيات الحديثة، فلقد إلى بروز العديد من المشكلات والسلبيات التي ظهرت نتيجة الاستعمال الواسع للحواسيب ووسائل الاتصال المختلفة ابرزها على الإطلاق الجرائم الإلكترونية المقترفة من بعض مستخدمي هذه الوسائل الحديثة التي التميز بخطورتها وسهولة استعمالها، وبذلك فقد ساهم الانتشار الواسع لتكنولوجيا المعلوماتية واتاحة استعمال التقنيات الحديثة دون ضوابط صارمة في ظهور هذه الجرائم وهي تعد من الجرائم الخطيرة التي يصعب اكتشافها ومكافحتها لاسيما بعد اتساع استعمال الأجهزة ومختلف الوسائط الإلكترونية بشكل كبير وغير مسبوق.

لقد أصبحت هذه الجرائم تشكل هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل بشكل جاد على مكافحتها، سواء من خلال إبرام اتفاقيات ثنائية أو وضع تشريعات وطنية للحد منها ومكافحتها .

كما أدى هذا التطور الذي عرفته تكنولوجيا المعلوماتية وتطبيقاتها المتعددة، إلى بروز مشاكل قانونية جديدة، تطلب حلها البحث في الأوضاع القانونية القائمة ومدى وملائمتها

المواجهة هذه المشاكل الأمر الذي دفع بالدول إلى العمل مليا للحد من هذه الجرائم من خلال التوعية والوسائل الوقائية الأمنية وغيرها.

بحيث بات لزاما أن يواكب تطور الجريمة وأساليبها تطورا في مجال السياسة التشريعية عموما والسياسة الجنائية على وجه الخصوص، بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية .

ساهم التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي، والزيادة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، من اشخاص طبيعية، أو هيئات واشخاص معنوية، كل ذلك أسهم في ظهور فئة جديدة من الجرائم، مرتبطة بالتكنولوجيا، ومنها جرائم المعلوماتية، ونظرا لتزايد اسباب ارتكاب هذه الجريمة في الآونة الأخيرة، الأمر الذي أدى إلى انعكاسها على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة الجريمة ومعطياتها، وآثارها.

وبناء عليه كانت الحاجة ملحة لوضع هذا الموضوع موضع الدراسة والتحليل، والتعريف الوسائل القانونية والوقائية للجريمة المعلوماتية.

اهداف الدراسة :

تتمثل أهداف دراسة هذا الموضوع في التعرف التطور التشريعي لوسائل الوقاية من الجريمة الإلكترونية

التعرف على الوسائل التقنية

التعرف على الهيئات والأجهزة المختصة لمكافحة الجريمة المعلوماتية.

التعرف على إجراءات التحقيق للكشف عن الجريمة المعلوماتية.

اهمية الموضوع :

تكمن اهمية دراستنا لموضوع الوقاية من الجريمة الالكترونية في التشريع الجزائري ، في بيان هذا النوع من المخاطر المستحدثة، والحد منها داخل المجتمع والتقليل من آثارها، وزيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة، وبأخذ الحذر والحيطة في الاستخدام كما تتجلى اهميته في تبيان الإطار التشريعي للوقاية من الجريمة المعلوماتية في القانون الجزائري.

اسباب اختيار الموضوع :

تظهر اهم الاسباب دفعتنا إلى اختيار هذا الموضوع في الأسباب الموضوعية وأخرى ذاتية تتمثل في مايلي:

الاسباب الذاتية :

تتمثل الاسباب الذاتية في رغبتنا في باهتماماتنا الشخصية بتأثير التطورات التكنولوجية على المجال القانوني، لا سيما في الجانب المتعلق بالأمن السيبراني، وهو ما دفعني إلى دراسة سبل الوقاية القانونية والأمنية التي أقرها التشريع الجزائري لمواجهة الجرائم الإلكترونية، ومحاولة استكشاف مدى فعاليتها على أرض الواقع، وكذلك ارتباط موضوع مذكرتنا بتخصصنا القانوني كطلبة قانون اعلام الي مما يسهم في اثراء زادنا المعرفي في مجال تخصصنا ويجعلنا على اطلاع بكل ماهو حديث في مجال تخصصنا .

الاسباب الموضوعية :

اما الاسباب الموضوعية تتمثل في تزايد انتشار الإنترنت وتصاعد الجرائم الإلكترونية، مما يستدعي البحث في سبل الوقاية، كما أن تعقيد الجريمة الإلكترونية فرض تطوير أدوات قانونية وتقنية للحد منها وقد زادت هشاشة الأمن السيبراني زادت الحاجة لوسائل وقائية فعالة.

خاصة في ضل تزايد الاعتداءات الرقمية يتطلب دراسة الإطار الوقائي في القانون الجزائري.

وكذلك الإجراءات المتخذة للكشف عنها وذلك في التشريع الجزائري، وبناء على كل ذلك، نطرح الاشكالية التالية :

ما هي اليات واجراءات الحماية من الجريمة الإلكترونية في التشريع الجزائري؟

وتحت هذا السؤال العام، تنبثق عنه مجموعة من التساؤلات الفرعية كالتالي:

- ✓ ما هي الإجراءات القبلية للوقاية من الجريمة الإلكترونية ؟
- ✓ ما الوسائل التقنية لحماية منها ؟
- ✓ هل يوجد آليات المؤسساتية المختصة للكشف عن الجريمة المعلوماتية؟
- ✓ ما هي إجراءات التحقيق في الجريمة المعلوماتية

المنهج المتبع :

اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي، حيث تمثل الجانب الوصفي في عرض الوسائل التشريعية الأمنية، التقنية والإجرائية المعتمدة في الوقاية القبلية والبعدية من الجريمة الإلكترونية. أما الجانب التحليلي، فتم من خلال دراسة النصوص القانونية وتحليل إجراءات التحقيق وآليات عمل الجهات المختصة بهدف تقييم مدى فعالية المنظومة الجزائرية في التصدي لهذا النوع من الجرائم.

الدراسات السابقة :

– عقباش بريزة وحنان مبارك ، أليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، وهي مذكرة مقدمة الاستكمال متطلبات نيل شهادة ماستر اكاديمي في الحقوق تخصص .

قانون اعلام الآلي والانترانت، والتي نوقشت بكلية الحقوق والعلوم السياسية ، جامعة بن بوعريريج سنة 2022

– غربي جميلة – اليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، وهي مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي و علوم جنائية والتي نوقشت بكلية الحقوق والعلوم السياسية ، جامعة البويرة،سنة 2021

الهدف من الدراسات السابقة:

> تهدف الدراسات السابقة المُدرجة في هذه المذكرة إلى دعم موضوع البحث من خلال الاطلاع على الجهود العلمية التي تناولت الجريمة الإلكترونية والوقاية منها في السياق القانوني الجزائري. فقد ساهمت هذه الدراسات في:

توفير خلفية نظرية ومعرفية مكّنتنا من فهم تطور معالجة هذه الظاهرة.

تحديد أوجه الاتفاق والاختلاف بين الباحثين حول نجاعة الإطار التشريعي والمؤسساتي المعتمد.

الكشف عن الثغرات التي لم تُغطِّها الدراسات السابقة، مما يبرز أهمية الدراسة الحالية في سدّ هذا الفراغ، لاسيما من حيث التركيز على البعدين الوقائي القبلي والبعدي في التشريع الجزائري.

وأخيرًا، تساعدنا هذه الدراسات في بناء تصور علمي واضح حول واقع الوقاية من الجريمة الإلكترونية، واختيار المنهج والأساليب المناسبة لمعالجة الإشكالية المطروحة.

خطة الدراسة :

وللإجابة على الاشكالية الرئيسية والتساؤلات الفرعية ودراسة الموضوع محل البحث اعتمدنا على الخطة التالية :

اذ قسمنا الدراسة الى فصلين ، حاولنا من خلال الفصل الأول دراسة ، الوقاية القبلية من الجريمة الالكترونية، عالجنا في المبحث الأول التطور التشريعي لوسائل الوقاية من الجريمة الالكترونية بينما خصصنا المبحث الثاني لدراسة الوسائل التقنية .

في حين خصصنا الفصل الثاني لدراسة الوقاية البعدية من الجريمة الالكترونية حيث عالجنا في المبحث الأول الوسائل الاجرائية المؤسساتية

كما تطرقنا في المبحث الثاني الى التدابير الاجرائية للكشف عن الجريمة المعلوماتية

وفي ختام دراستنا لموضوع البحث محل الدراسة ، تطرقنا الى اهم النتائج التي توصلنا إليها خلال بحثنا مع تقديم بعض الاقتراحات التي ارتأينا انها مدعمة لموضوع دراستنا.

الفصل الاول

الوقاية القبلية

من الجريمة الالكترونية

الفصل الاول:الوقاية القبلية من الجريمة الالكترونية

شهد العالم في العقود الأخيرة تحولًا جذريًا بفعل الثورة الرقمية، حيث أصبحت التكنولوجيا الحديثة جزءًا لا يتجزأ من الحياة اليومية للأفراد والمؤسسات على حدٍّ سواء، ما فتح آفاقًا واسعة أمام التطور، لكنه في المقابل أتاح مجالًا خصبًا لظهور أنماط جديدة من الإجرام. ولعلّ أبرز هذه الأنماط هي الجريمة الإلكترونية، التي باتت تمثل تهديدًا حقيقيًا لأمن الأفراد والدول، بالنظر إلى طبيعتها المعقدة وسرعة انتشارها وصعوبة تتبع مرتكبيها.

وفي ظل هذا الواقع، أصبحت الوقاية القبلية من الجريمة الإلكترونية ضرورة ملحة، إذ لم يعد بالإمكان الاعتماد فقط على الوسائل التقليدية في مواجهة هذا النوع من الإجرام، بل بات لزامًا على الدول سنّ تشريعات وتطوير آليات وقائية فعالة تسهم في تحصين المجتمع ضد مخاطره المتزايدة.

ولأن الجزائر جزء من هذا الفضاء الرقمي العالمي، فقد حرص المشرع الجزائري على تكييف المنظومة القانونية الوطنية بما يواكب تطورات الجريمة الإلكترونية، من خلال وضع أطر تشريعية وتنظيمية تهدف إلى الوقاية الاستباقية منها، سواء من خلال النصوص القانونية أو عبر تمكين الأجهزة الأمنية من آليات الكشف المبكر والتصدي الفعّال.

وللإجابة على الإشكال قسمنا هذا الفصل إلى مبحثين حيث تطرقنا في (المبحث الأول) إلى التطور التشريعي لوسائل الوقاية من الجريمة الالكترونية ، ويليها الوسائل التقنية في (المبحث الثاني).

المبحث الأول: التطور التشريعي لوسائل الوقاية من الجريمة الالكترونية

تُمثّل الوقاية الإجرائية أحد أهم الوسائل الاستباقية لمنع الجرائم الإلكترونية، ولذلك سنناقش في هذا المبحث الإطار التشريعي الجزائري المتعلق بالأمن السيبراني، ودور الأجهزة الأمنية في هذا المجال.

المطلب الاول :الإطار التشريعي للوقاية من الجرائم الالكترونية

لم يجد المشرع الجزائري بدأ من تعديل قانون العقوبات لما كان فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم والمعادل للأمر 156/66 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي.[1]

لذلك فقد آثار المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم. تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها . ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات

[1] عمار حشمان ،الجريمة المعلوماتية في التشريع الجزائري مذكرة لنيل شهادة ماستر في العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، 2019، ص. 17.

الإحعلام والإتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها [2]

الفرع الاول: القوانين الجزائرية المتعلقة بالجريمة الالكترونية والامن السيبراني

أ-الدستور: لاسيما المواد 41 50.51.47.43 52 54 55 المتعلقة أساسا بحماية الحريات الفردية حماية الحياة الخاصة الحق في سرية المراسلات والاتصالات الخاصة حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي

ب-الاتفاقيات الدولية والاقليمية:

الإعلان العالمي لحقوق الإنسان 1948

العهد الدولي الخاص بالحقوق المدنية والسياسية 1966.

العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية 1966.

اتفاقية الأمم المتحدة الخاصة بالجريمة المنظمة العابرة للحدود الوطنية المؤرخة في 15/11/2000 المصادق عليها بموجب المرسوم الرئاسي رقم 02/55 المؤرخ في 05/02/2002

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14/252 المؤرخ في 08 سبتمبر 2014.[3]

---

[2] عمار حشمان , المرجع السابق, ص. 17.

[3] سويسي فتيحة التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المرتبطة بها، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022 منشور على موقع وزارة العدل الجزائرية http://www.mjustice.dz تاريخ الاطلاع: 9 ماي 2025، ص 12

مرسوم رئاسي رقم 16-111 يتضمن التصديق على اتفاقية إنشاء المنظمة العربية لتكنولوجيات الاتصال والمعلومات المحررة بالقاهرة في 13/02/2002

القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات والذي اعتمدته جامعة الدول العربية.

ج-القوانين:

تعديل قانون العقوبات بموجب كل من:

2001 القانون رقم 01-09 المؤرخ في 26 جوان

القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 إضافة القسم السابع مكرر يتضمن مواد جديدة تعاقب على المساس بأنظمة المعالجة الآلية للبيانات.

القانون رقم 14-01 المؤرخ في 14 فيفري 2014 المعدل والمتمم لقانون العقوبات.

القانون رقم 16-02 المؤرخ في 10 يونيو 2016 المتمم لقانون العقوبات.

قانون رقم 20-06 مؤرخ في 28 أبريل 2020 يعدل ويتمم الأمر رقم 66-156 والمتضمن قانون العقوبات المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، أين تم إضافة مواد جديدة تعاقب على نشر وترويج أخبار أو أنباء تمس بالنظام والأمن العمومين لاسيما عبر وسائل الاتصال الحديثة

القواعد الإجرائية المقررة لمكافحة الجرائم الإلكترونية:

القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية.

القانون رقم 06-22 المؤرخ في 20/11/2006 المعدل لقانون الإجراءات الجزائية[4]:

[4] سويسي فتيحة ،المرجع السابق، ص،ص12-13

يهدف إلى وضع قواعد إجرائية أكثر تكيفا مع بعض أنواع معينة من الجرائم الجديدة أو الأكثر انتشارا، بما في ذلك الهجمات على أنظمة المعالجة الآلية للبيانات، ومن بين المستجدات التي تم إدراجها اعتراض المراسلات تسجيل الصوت وأخذ الصورة.

القانون رقم 06-01 المؤرخ في 20 فبراير 2006 يتعلق بالوقاية من الفساد ومكافحته.

القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هذا القانون يعكس السياسة الجديدة للجزائر في مكافحة الجريمة المتعلقة بتكنولوجيا الإعلام والاتصال ويتضمن تدابير إجرائية أهمها:

تعزيز صلاحيات أجهزة التحقيق.

إشراك المتعاملين التقنيين شركات الاتصالات و مقدمو خدمة الأنترنت».

تعزيز المساعدة القانونية والتعاون الدولي.[5]

القوانين الخاصة ذات الصلة:

القانون رقم 08-01 المؤرخ في 23 جانفي 2008، يتمم القانون رقم 83-11 المؤرخ في 2 جويلية 1983 المتعلق بالتأمينات الاجتماعية، تم بموجبه تحديد الجرائم الواقعة على البطاقة الالكترونية الشفاء

القانون العضوي رقم 12-05 المؤرخ في 12 جانفي 2012 المتعلق بالإعلام.

القانون رقم 15-12 المؤرخ في 15 جويلية 2015، يتعلق بحماية الطفل.[6]

---

[5] قانون رقم 04-09 المؤرخ في 5 أغسطس 2009 متضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا العلم والاتصال ومكافحتها الصادرة ب 5اغسطس 2009 ج،ر،ج،ج العدد 47 سنة 2009

[6] سويسي فتيحة ،المرجع السابق ، ص. 13.

القانون رقم 15-13 المؤرخ في 15 جويلية 2015، يتعلق بأنشطة وسوق الكتاب.

الأمر رقم 05-03 المؤرخ في 19 جويلية 2005 المتعلق بحقوق المؤلف والحقوق المجاورة

القانون رقم 16-03 المؤرخ في 19 جوان 2016 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية.

القانون رقم 04-08 المؤرخ في 14 أوت 2004 المتعلق بشروط ممارسة الأنشطة التجارية المعدل والمتمم.

القانون رقم 18-04 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

القانون رقم 18-05 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الإلكترونية.

القانون رقم 18-07 المؤرخ في 10 جوان 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

القانون رقم 09-03 المؤرخ في 25 فيفري 2009 المتعلق بحماية المستهلك وقمع الغش[7]

بعض النصوص التنظيمية ذات الصلة:

المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد

الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009، المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة.

القانون رقم 15-04 الذي يضع القواعد العامة للتوقيع والتصديق الإلكترونيين.

[7] سويسي فتيحة ،المرجع السابق ، ص،ص.13-14

المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، الذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الالكتروني وسيرها ومهامها[8].

الفرع الثاني: التعديلات التشريعية الحديثة

اولا:القانون رقم 24-06 المؤرخ في 28افريل2024

والجزائر كغيرها من دول العالم، سعت إلى التوجه نحو منظومة عقابية مواكبة التطورات التكنولوجية الحديثة للحد من العقوبات السالبة الحرية من جهة، ولتخفيف الضغط على المؤسسات العقابية من جهة أخرى، وهذا من خلال الأخذ بعقوبة الوضع تحت المراقبة الالكترونية لأول مرة بموجب القانون رقم 18-01 المؤرخ في 30 جانفي 2018)، المتمم(للقانون رقم 05-04 المؤرخ في 6 فيفري 2005 المتضمن قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين. لكن كأحد الأنظمة التكييف العقوبة

غير أنه في سنة 2021 تم تعليق العمل بهذا النظام بسبب معونات تقنية تتعلق اساسا باقتناء اساور مغشوشة

وبعد ثلاث سنوات من تعليق العمل به ،المشرع الجزائري يعود من جديد إلى تقنين الوضع تحت المراقبة الالكترونية، لكن بدلا من عقوبة الحبس القصير المدة، وذلك من خلال القانون رقم (24-06) المؤرخ في 200 أفريل 2024) المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات

جاء القانون رقم 24-06 المعدل والمني 1966 للأمر رقم 66-156 المؤرخ في 8 جوان المتضمن قانون العقوبات بأحكام قانونية جديدة تتعلق بشروط الاستفادة من عقوبة الوضع

[8] سويسي فتيحة ،المرجع السابق،ص 15

تحت المراقبة الالكترونية، بدلا من عقوبة الحبس إضافة إلى عدة أحكام أخرى تتعلق أساسا بتطبيقها[9]

ثانيا :الامر رقم 21-09 المؤرخ في 8جوان 2021

قصد حماية المعلومات والوثائق الإدارية المصنفة المتعلقة بالدولة ومؤسساتها ، وهيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية، وكل مؤسسة تملك الدولة كل أو بعض رأسمالها، بالإضافة إلى كل مؤسسة تقدم خدمة عمومية تدعى في النص بـ " السلطات المعنية سارع المشرع الجزائري إلى وضع تقنين يحمي المعلومات والوثائق المصنفة من خلال إصدارة للقانون رقم 21-09 المتعلق بحماية المعلومات والوثائق الإدارية الموضوعة تحت سلطة الموظفين في مؤسسات الدولة.[10]

المطلب الثاني: دور الاجهزة الامنية في مكافحة الجريمة الالكترونية

في المفهوم الحديث للعمل الأمني يعتبر المواطن لب العملية الأمنية ومحورها بل هو أهم طرف في أي معادلة أمنية من هذا المبدأ اتجهت الأجهزة الأمنية بمختلف دول العالم إلى بناء سياسات ومقاربات أمنية تسعى إلى إشراك المواطن في عملها الأمني، ففاعلية المواطن من خلال التبليغ الآني والفوري عن الأخطار والأحداث التي من شأنها أن تمس بالنظام العام هو مقياس نجاح المؤسسة، وسعياً إلى تحقيق هذا الهدف تقوم المؤسسات الأمنية ببناء علاقات إنسانية إجتماعية مع مختلف أطياف المجتمع، محاولة بذلك كسر جمود العلاقة التقليدية بين الأمن والمواطن أملاً في كسب تأييده لاسيما في ظل تطور الجريمة وظهور جرائم مستحدثة على غرار الجرائم السيبرانية حيث تستغل الأجهزة الأمنية وسائل

[9] القانون رقم 24-06المؤرخ في 28 افريل 2024 ، المعدل والمتمم للامررقم 66-156المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الصادر في 30 افريل 2024 ، ج رج، ج العدد 30 سنة 2024

[10] الامر 21-09المؤرخ في 8 جوان2021 يتعلق بحماية المعلومات والوثائق االدارية الصادر ب 9 جوان 2021 . ج ر ج ج العدد 2021

الإعلام والاتصال في إنجاح هذا المسعى من خلال الرهان على زيادة الوعي بالمخاطر المحدقة بالمجتمع وذلك في إطار ما أصلح على تسمية بـ "الإعلام الأمني.[11]

الفرع الاول:تفعيل دور الاعلام الامني في مكافحة الجريمة الالكترونية:

1-مفهوم الاعلام الرقمي والاعلام الامني:

أ-تعريف الاعلام الرقمي: يمكن القول أن الإعلام الرقمي هو عبارة عن نوع جديد من الإعلام يشترك مع الإعلام التقليدي في المفهوم، والمبادئ العامة والأهداف وما يميزه عن الإعلام التقليدي انه يعتمد على وسيلة مختلفة وهي الدمج بين كل وسائل الاتصال التقليدي، بهدف إيصال المضامين المطلوبة بأشكال متمايزة ومؤثرة بطريقة أكبر، وتتيح لأنترنت للإعلاميين قدرة كبيرة لتقديم موادهم الإعلامية المختلفة، بطريقة إلكترونية بحتة دون اللجوء إلى الوسائل التقليدية كمحطات البث المطابع وغيرها بطرق تجمع بين النص والصورة والصوت والتي ترفع الحاجز بين المتلقي والمرسل ويمكن أن يناقش الضامين الإعلامية التي يستقبلها، إما مع إدارة الموقعة و مع المتلقين آخرين (الفتاح 2014، صفحة (12:11)، فالإعلام الالكتروني هو الأسلوب المنظم للدعاية السياسية أو ترويج للأفكار في وسط مهيا نفسياً لاستقبال السيول الفكرية التي تقذفها المصادر التي تتحكم بالرأي العام وتمسك زمام الأمور بيد من حديد عن طريق وسائل إلكترونية كالكمبيوتر والأنترنت والوسائط الذكية التي أصبحت وسيلة اتصال عالمية مهيمنة في كثير من بقاع العالم، ففي زمن لا يزيد إلا قليلا عن عقد من الزمن أصبحت الشبكة الرقمية جزءا مهما من حياة كثير من الأفراد في المجتمعات حول العالم، إلا أن القليل فقط يعرف بخصوص استخدامات وإمكانات شبكة الإنترنت وتحدياتها (الجحافي،2013)

[11] ساعد محمد سيدي موسى ليلى ،الاعلام الامني ودوره في تعزيز الوعي الامني السيبراني ،الشرطة الجزائرية نموذجا-مجلة الرواق لدراسات الاجتماعية والانسانية .جامعة عبد الحميد بن باديس مستغانم (الجزائر) المجلد 9 ▪العدد 1-2023 ص 235

من هذا المنطلق أصبحت استخدامات شبكة الإنترنت كوسيلة اتصال جماهيرية تم استغلالها من قبل أجهزة الأمن من أجل زرع ثقافة أمنية عبر مواقعها للتعريف بنشاطاتها وإحصائيتها وتقديم بعض الخدمات الإرشادية التحسيسية والوقاية والإصغاء لانشغالاتهم عن طريق الشكاوي والبلاغات المرسلة عبر القضاءات الرقمية هذه الأخيرة التي أصبح لها جمهورها الخاص من حيث الكم والنوع.[12]

ب–تعريف الإعلام الأمني: يمثل الإعلام الأمني استخدام الوسائل والطرق المختلفة لبث الشعور بالأمن بين أفراد المجتمع وهذا الشعور يتطلب ضمان تحقق الأمن الداخلي للدولة والمجتمع بما يضمن نشر الثقافة والمعرفة الأمنية في المجتمع فالإعلام الأمني هو مجموعة العمليات المتكاملة التي تقوم بها أجهزة الإعلام المتخصصة لإيجاد نوع من التوازن في المجتمع والمحافظة على نظمه البنائية الاجتماعية والسياسية والثقافية لتحقيق أمن واستقرار [13]

2 –دور الاعلام الامني في مكافحة الجريمة الالكترونية: : تدعو الحاجة في الوقت الراهن إلى إرساء نوع من التعاون المستقبلي بين وسائل الإعلام والأجهزة الأمنية من جهة، وبين هذه الأخيرة والجمهور من جهة أخرى، في مجال مكافحة الجريمة ومن ثم يتوجب علينا تحديد دور وسائل الإعلام في الحد من ظاهرة الجريمة الإلكترونية كالتالي:

–**الدور الوقائي الإعلامي:** يتمثل دور الإعلام الأمني في هذا المجال من خلال تلك الخطط والبرامج الهادفة التي تبتها عبر وسائلها المختلفة، خاصة عبر القنوات الإعلامية والوسائط الرقمية بغرض وقاية المجتمع من مخاطر الجريمة الإلكترونية ومنعها من لوقوع

[12] خبزاوي مراد ، محمودي رقية ، الإعلام الأمني. الرقمي كممارسة آمنية استياقية في سبيل الوقاية الجريمة الإلكترونية. مجلة البحوث والدراسات العلمية ، جامعة يحيى فارس بالمدية (الجزائر)المجلد 18العدد 01 .2024 صفحة 5

[13] المرجع نفسه ،ص 6

-**الدور الإعلامي الاجتماعي:** يتصل دور الإعلام الأمني اتصالا وثيقا من خلال معالجة القضايا الأمنية من منظورها الاجتماعي المتمثل أساسا في تحديد الآثار السلبية التي تتركها الآفات الاجتماعية على السلوكيات الفردية داخل المجتمع خاصة مع الاختلاف الكبير بين الطبقات الاجتماعية والتي تجعل الضعيفة منها عرضة للانحراف والوقوع في دائرة الجريمة.

-**الدور الإعلامي القمعي** : يقوم الإعلام الأمني بدور بارز في مكافحة الجريمة، وذلك من خلال إخبار الرأي العام بمختلف النشاطات الإعلامية المتصلة بقمع الإجرام والمجرمين خاصة القضايا الأمنية التي تمت معالجتها والمحالة أمام المحاكم، والتصدي لكل أشكال الخروج عن الضوابط القانونية التي تنظم سلوكيات الأفراد، كما أنه يستقطب الرأي العام ويحميه بالتصدي للجريمة والوقاية منها، وبعد في حد ذاته عملا يجسد سياسة الوعي الأمني، هذا بالإضافة إلى حماية أفراد المجتمع من الوقوع في شبكات الإجرام والمجرمين.

ونظرا للتأثير الكبير للمواد الإعلامية في الرأي العام يمكن تحديد أدوار أخرى للإعلام الأمني وهي:

-**إطاعة القوانين والأنظمة:** تلعب وسائل الإعلام دور هام في توجيه الأفراد وتوعيتهم حول خطورة الإجرام من خلال عرس الثقافة الأمنية وجعلهم أكثر احتراما للقوانين والنظم، وبالتالي يساهم المجتمع بتدعيم الأجهزة الأمنية في التقليل من مخالفي القانون باحترام القوانين والأنظمة السائدة في المجتمع.

-**اتخاذ الإجراءات الكفيلة بمنع وقوع الجريمة:** تكسب وسائل الإعلام الجمهور مجموعة من الإجراءات الكفيلة بمنع وقوع الجريمة، ومحاربتها والتصدي لها، من خلال إبعاد خطر الجريمة وحثهم على الحرص لحفظ أموالهم وممتلكاتهم وتربية أبنائهم على الأخلاق الرفيعة والسلوك القيم الذي يقيهم من الجريمة[14]

[14] خبزاوي مراد،المرجع السابق،ص.11.

-**التبليغ عن الجرائم:** تخلق وسائل الإعلام لدى المواطن واجب التحصين ضد الجريمة وذلك بالتبليغ عنها والكشف عن مرتكبيها ويساعد الأجهزة الأمنية مواجهتها.

-**التقدم للشهادة:** يمكن لوسائل الإعلام المختلفة أن تلعب دورا كبيرا في تكوين اقتناع لدى أفراد المجتمع بأنه من واجبهم التقدم إلى مصالح الأمن للإدلاء بشهاداتهم ضد المجرمين تسهيلا لمعالجة القضايا الإجرامية وتسويتها أمام العدالة، باعتبار الجريمة دائمة الوقوع ومن الواجب على وسائل الإعلام أن توجه جمهور المتلقين توجيها سديدا، يحقق إعلاما أمنيا إيجابيا من خلال:

-أن يوجه الرأي العام توجيها مفاده خلق اقتناع بالوقوف ضد الجريمة، ويكون مؤيدا للقانون والأنظمة.

-خلق نقاط أمنية لدى المواطنين بأن الجريمة سلوك منحرف ويؤدي إلى تحقيق نتائج سلبية تضر بالمجتمع.

-ترقية وسائل الإعلام لمكانة المؤسسات التشريعية والمؤسسات القائمة على تنفيذ القانون باعتبارها جهات حازمة وعادلة، وأن المواطن من جانبه مساعدة هذه المؤسسات على تنفيذ القانون في منع الجريمة [15]

الفرع الثاني: تعزيز التعاون الامني الدولي في مكافحة الجريمة الالكترونية

1-مفهوم تعاون الأمني الدولي:

أ-المفهوم العام: يُعرف التعاون الأمني الدولي بأنه تبادل العون والمساعدة، وتكاثف الجهود المشتركة بين دولتين أو أكثر، لتحقيق منفعة أو مصلحة مشتركة في مجال مكافحة الجرائم وما يرتبط بها من مجالات كالأمن والعدالة الاجتماعية، أو لتذليل عقبات الحدود والسيادة

[15] خبزاوي مراد،المرجع السابق،ص،ص، 11 – 12.

التي قد تعيق المتابعة الوطنية للمجرمين ومصادر التهديد سواء أكان هذا التعاون قانونيا أم قضائيا أم شرطيا، وسواء شمل دولتين فقط أو اتسع نطاقه إقليميا أو عالميا[16]

ب-المفهوم القانوني: يعرف التعاون الأمني الدولي بأنه مجموعة الإجراءات التي تتخذها دولة أو منظمة دولية، بناء على طلب من دولة أو منظمة أخرى، في المجال الأمني والشرطي للتصدي للجريمة وتحقيق الأمن يهدف هذا التعاون إلى تعزيز القدرات الأمنية لمواجهة التهديدات العابرة للحدود، مثل الإرهاب والجريمة المنظمة[17]

2-صور تعاون الامني دولي:

اولا-ربط شبكات الاتصال والمعلومات: تحتاج الاتصالات الشرطية إلى وسائل للاتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين السلطات تحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية تطوير الاتصال وتبادل المعلومات في ما بينها.

ثانيا-القيام ببعض العمليات الشرطية والأمنية المشتركة : تعقب المجرم المعلوماتي و تعقب الأدلة الرقمية وضبطها ، و قيام بعملية تفتيش العابر للحدود المكونات الحاسب الآلي و الأنظمة المعلوماتية و شبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية ، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة، واشتراك الدول في ما بينها للقيام بعمليات شرطية وأمنية يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم و بتالي وضع حد لها.[18]

---

[16] سليمان ابو نمر، يوسف بوكشيدة ، مكافحة الجريمة المعلوماتية " في اطار القانوني الدولي ، مذكرة ماستر، جامعة محمد خيضر بسكرة 2021 ص.23

[17] جريدة العربي الافريقي،آليات التعاون الامني الدولي،htttps://arabafricanews.com تم الاطلاع عليه يوم 10\05\2025 على الساعة 8:48 مساءا

[18]قاضي حولة جباس منال التعاون الدولي في مكافحة الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق جامعة قاصدي مرباح ورقلة 2021، ص 23

3-دور المنظمات الأمنية الدولية والإقليمية في مكافحة الجريمة الإلكترونية:

1. التعاون الدولي في مكافحة الجرائم الإلكترونية (الإنتربول):

-يهدف الإنتربول إلى تعزيز التعاون بين دوله الأعضاء لمكافحة الجرائم الإلكترونية، مثل جرائم الإنترنت والصور غير الأخلاقية، من خلال تبادل المعلومات والبيانات بين المكاتب الوطنية.

- أنشأ الإنتربول وحدة خاصة للجرائم التكنولوجية عام 2004، وتعاون مع دول الـ G8 لوضع استراتيجيات مشتركة، بما في ذلك إنشاء مراكز اتصال تعمل على مدار الساعة.

- من إنجازاته توقيف مجرمين مثل طالب لبناني قام بنشر صور غير أخلاقية، وتفكيك شبكات إجرامية بالتعاون مع المباحث الفيدرالية الأمريكية.

2. شرطة الويب الدولية والتعاون القضائي:

-تأسست شرطة الويب في الولايات المتحدة عام 1986 لتلقي شكاوى المستخدمين ومتابعة القراصنة والمجرمين الإلكترونيين، بالتعاون مع فرق متخصصة من 61 دولة.

-على المستوى العربي، أنشئ المكتب العربي للشرطة الجانبية عام 2010 لتعزيز التعاون بين الدول الأعضاء في مكافحة الجرائم الإلكترونية.

-يركز التعاون القضائي الدولي على تسهيل الإجراءات القانونية المتبادلة، مثل التحقيقات وتسليم المجرمين، كما نصت عليه اتفاقيات الأمم المتحدة لضمان فعالية المكافحة.[19]

[19] فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق و العلوم السياسية، - جامعة البليدة 02 الجزائر المجلد 08 - العدد 01 2022، ص ،ص. 438-439

المبحث الثاني :الوقاية الموضوعية من الجريمة الالكترونية

مع التطور الكبير في وسائل التكنولوجيا، أصبحت الوقاية التقنية ضرورة لا غنى عنها في مواجهة الجريمة الإلكترونية. فلا يكفي الاعتماد على القوانين فقط، بل يجب تبني وسائل موضوعية تقوم على حماية الأجهزة والشبكات والمعلومات، وتطوير آليات فعالة لرصد التهديدات مبكرًا. يهدف هذا المبحث إلى إبراز أهم هذه الوسائل والآليات التقنية التي تساهم في التصدي لمخاطر الجرائم الإلكترونية.

المطلب الأول: الوسائل الوقائية التقنية

يُعد التأمين التقني من أهم الوسائل المعتمدة لتحقيق الوقاية الموضوعية في مجال حماية المعلومات. وسنعرض في هذا المطلب أبرز هذه الوسائل من خلال فرعين أساسيين.

الفرع الاول:تأمين شبكات المعلومات

اولا– تعريف امن شبكات المعلومات: ويمكننا تعريف "أمن شبكات المعلومات على أنه مجموعة من الإجراءات التي يمكن خلالها. توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

او هي مجموعة من المعايير التي تحول دون وصول المعلومات المخزنة في الشبكات إلى الأشخاص غير المخول لهم الحصول عليها[20]

[20] رجب عبد الحميد حسين ، آمن شبكات المعلومات الإلكترونية (المخاطر والحلول) مجلة Cybrarians Journal جامعة الحصن، أبو ظبي، العدد 30 ديسمبر 2012 ،ص،ص.77-78

ثانيا-التحديات الامنية التي تواجه امن نضم المعلومات:

1-تهديدات ناتجة عن الاعتداء:

-**البرامج الضارة**(الخبيثة):) وهي كل برنامج يدخل في النظام ويكون عمله ضارا، منها:

الفيروسات: الفيروس برنامج خبيث تم تصميمه من قبل أحد المبرمجين لتحقيق بعض الأهداف وحسب هذه الأهداف تكون النتائج، قد تكون غير مضرة كإظهار بعض الإعلانات قد تكون خطيرة نوعا ما كتعديل جزء من البرامج ، و أغلبها يكون مدمر كتعطيل وتدمير البرامج والأجهزة كلية ،و من سمات الفيروس قدرته على ربط نفسه بالبرامج وتسخ نفسه بنفسه دون علم المستخدم إضافة إلى قدرته على التخفي والانتشار السريع

-**الديدان Vers** : الديدان عبارة عن برامج مستقلة تنتقل من حاسب لآخر داخل الشبكة دون الحاجة لتدخلات بشرية، وتنتشر بسرعة أكبر من الفيروس، ويمكن أن تخفى معطيات وبرامج واتلافها، وإعاقة عمل شبكة معلوماتية فالديدان المعلوماتية تستقر في ذاكرة أنظمة المعلومات بنفس الطريقة التي تستقر فيها الدودة البيولوجية في تفاحة، وعلى عكس الفيروس، فهي قادرة على نسخ نفسها بدون تدخلات داخلية أو خارجية.

-**حصان طروادة Chevaux de Troie:** يعرف حصان طروادة على أنه " رمز حيث يختفي داخل برنامج تمظهرا بذلك براءته عن طريق تمثله في لعبة صغيرة أو بطاقة رغبات أو برنامج مشاهدة صور من أجل أن ينفذ لاحقا عمليات غير شرعية[21](Godart 2005, pp 65-66) فهو " برنامج غير خطير في الظاهر، ولكن تصرفاته غير متوقعة، ليس فيروس لأنه لا يتكاثر، ولكن يمكن أن يمرر فيروسات ورموز خبيثة أخرى من أجل أن يضمن دخوله في النظام المعلوماتي

[21] -فيلالي اسماء ،شليل عبد اللطيف ،تهديدات آمن المعلومات وسبل التصدي لها، - جامعة أبو بكر بلقايد ، تلمسان الجزائر،مجلة البشائر الاقتصادية المجلد الرابع تلمسان الجزائر، المجلد الرابع،العدد03، 2019.ص167

– **القنابل المنطقية Bombe logique:** القبيلة برنامج متخفي في انتظار حدث معين محدد من قبل المبرمج، ويشغل هذا البرنامج الخبيث عندما يحدث الحدث هذا الرمز الخبيث ينتظر عموما تاريخ معين من أجل أن يباشر العمل

ب–القرصنة المعلوماتية (التجسس على أنظمة المعلومات): القرصنة تعمل على كشف نقاط ضعف نظم حماية الأنظمة المعلوماتية، وغالبا ما يتم استغلال مختلف وظائف الانترنت التي تحوله إلى نظام مفتوح منهل الاختراق ، و عليه هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات والحصول على المعلومات السرية بأي طريقة وسنقوم بذكر أكثر الطرق انتشارا .

التصنت L'Ecoute : التصنت يكمن في التموقع على شبكة معلوماتية أو شبكة التوصل عن بعد ، و من ثم تحليل وتخزين المعلومات العابرة ، وترجمة التأمرات وكل ما يدور داخل الشبكة المعلوماتية.

إذ أنه وعلى مستوى الاتصال بالشبكة أو الانترنت العادية 99.9% من المعلومات التي تدور ليست مشفرة ويمكن اعتراضها من قبل أي أحد

ومن أكثر البروتوكولات عرضة التصنت بروتوكول (TCP/IP)، ومن الأدوات المستخدمة لتنفيذ التصنت برامج تحليل الشبكات وبروتوكولاتها كبرنامج " Sniffer الذي يعرف على أنه برنامج التصنت الالكتروني الذي يراقب المعلومة المنقولة داخل الشبكة (354 2006 Ladon et Laden) ويسمح بالتصنت على حركة الشبكة المعلوماتية التي تتصل مباشرة بالحاسب، ومن أولوياته البحث عن تحديد الحزم التي تضم كلمات login أو password[22]

سرقة الهوية l"usurpation d'identité: تكمن في انتحال هوية شخص آخر والاستفادة من امتيازاته عن طريق اغتصاب هويته والاستيلاء على العديد من العناصر

[22] -فيلالي اسماء ،شليل عبد اللطيف ،المرجع السابق، ،ص. 168

الخاصة به بصمة ، صوت ، بطاقة تعريف ، بطاقة الائتمان ، شريحة، كلمة سر، تاريخ ميلاد...)

رفض الخدمة : هذه الهجمة حتى وإن كان ظاهرها غير مخيف إلا أن تأثيرها كبير:

هي نشاط خبيث يترجم بانشغال أو عدم التاجة مؤقت أو دائم لعدة مكونات نظام الاتصال عن بعد

-هجمة رفض الخدمة هي تلك التي تعرقل وتمنع خدمة تطبيق ما وجعلها أحيانا غير مفيدة للمستعملين الشرعيين، باختصار هجمة رفض الخدمة تعمل على ازعاج الضحية، ولكن أيضا يمكن أن تتسبب في خسائر كبرى[23]

التزوير أو التعديل: تزييف وتعديل المعطيات خلال الارسال بتدخل حيث يحدث مشكل التكامل، فالتكامل المضمون عن طريق بروتوكولات النقل مثلا TCP تضمن أن يكون جريان المعطيات المستقبلة مماثلة تماما لجريان المعطيات المرسلة 14 2010 ,Vaucamps) ، وبالتدخل بينهما وتعديل الرسائل المرسلة لا تكون هذه الأخيرة نفسها هي المستقبلة، أما التعديل في البرامج يجعلها تؤدي عملها بطريقة مختلفة تلبية المصالح المهاجم

2 -التهديدات الناتجة عن ثغرات الامينة: تعتبر الثغرة الأمنية عبارة عن فجوة أو ضعف على مستوى نظام المعلومات، ومن الممكن استغلالها من طرف عناصر مهددة باستعمال مختلف طرق الهجوم، وعليه الثغرة الأمنية هي عبارة عن ضعف أو خطأ في نظام معين أو طريقة حماية معينة يتم استغلالها من قبل المهاجم الإحداث أضرار مختلفة، وتكون الأمنية على ثلاث مستويات الثغرات الأمنية على المستوى التنظيمي (الادارة)، الشعرات الأمنية على المستوى المادي، الثغرات الأمنية على المستوى التكنولوجي.

[23] -فيلالي اسماء ،شليل عبد اللطيف، المرجع السابق،ص. 168

ثالثا–طرق ضمان امن نضم المعلومات:

1–الحماية البرمجية للمعلومات وأنظمة المعلومات: الحماية البرمجية تتمثل في استخدام كل البرامج المتاحة والتي توفر حماية للمعلومات المنتقلة غير الشبكات أو المخزنة في الحواسيب.

أ–الجدار الناري: ويمكن تعريف الجدار الناري على أنه: "كل آلة موضوعة في شبكة معلوماتية وقادرة على تحقيق فريقة على التواصلات الداخلة والخارجة

ويعرف أيضا أنه : جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب ، و يكون أداة مخصصة أو برنامج على جهاز حاسوب آخر الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يقرر أحقية المرور ضمن قواعد معينة

أما بالنسبة الأشكال الجدار الناري، فهي تأتي على نوعين:

–برامج وهنا يكون الجدار الناري عبارة عن برنامج يتم تنزيله على الحاسب

–أجهزة وهو عبارة عن علبة أو صندوق مزود بواصلين انترنت، هاته العلبة تضم في نفس الوقت حاسب وبرنامج جدار ناري .[24]

ب– برامج مكافحة الفيروسات Anti virus:برنامج مكافحة الفيروس يتحقق من الأقراص والأنظمة من أجل تحديد تواجد فيروسات معلوماتية، ويستطيع عموما تنظيف المنطقة المصابة، ومن أجل أن يبقى البرنامج فعال يجب أن يحدث باستمرار[25]

[24] [24] المرجع السابق، -فيلالي اسماء ،شليل عبد اللطيف.ص169

[25] المرجع نفسة.ص 170

-**التشفير Chiffrement** : " هو مجموع التقنيات التي تهدف إلى تحويل بفعل اتفاقيات سرية، معلومات أو إشارات واضحة إلى معلومات أو إشارات غير واضحة من أجل تحقيق الفرضية المعاكسة عن طريق وسائل مادية أو برامج متخصصة لذلك

هو الاعتماد على خوارزمية لتحويل المعطيات الواضحة إلى معطيات مشفرة من أجل جعلها غير واضحة الشخص دخيل والهدف من التشفير هو جعل كل الملفات الرقمية الموجودة على التحاميل غير صالحة الاستعمال لمن لا يملك مفتاح الرمز.

وعليه فإن التشفير عبارة عن استخدام تقنيات أو برامج عملها هو تغيير مظهر المعلومات من معلومات واضحة يسهل فهمها إلى معلومات سرية يصعب فهمها، اعتمادا على :

خوارزمية التشفير : هي الصيغة الرياضية المطبقة على المعلومات المراد تشفيرها.

المفتاح التشفيري: وهو السر أو الأداة المستعملة في تشفير أو فك شفرة المحتوى

ت- مراقبة الدخول وأنظمة كشف التدخل:

1. **مراقبة الدخول (Contrôle d'acces)** : مراقبة الدخول هي كل السياسات والاجراءات المتحدة من قبل مؤسسة من أجل ايقاف أو إعاقة الدخول للأنظمة من قبل أشخاص ممنوعين، والدخول إلى النظام يتطلب التعريف بالهوية + التحقق من الهوية.
2. **أنظمة كشف التدخل IDS Intrusion Detection** Systems : أنظمة كشف التدخل هي عبارة عن أدوات مراقبة مستمرة موضوعة في أماكن أو نقاط الدخول الأكثر حساسية لشبكات المؤسسة من أجل كشف التدخلات، ومن ثم يطلق النظام إنذار في وقت حقيقي في حال حدث مهيب أو غير عادي[26]

[26] فيلالي اسماء ،شليل عبد اللطيف، المرجع السابق ،ص. 170

ث- الشبكة الافتراضية الخاصة :Virtuel Private Network VPN :هي تكنولوجيا حديثة يتم من خلالها حماية تبادل المعطيات بين موقعين متباعدين على الأقل، ضامنة بذلك هويات المرسل والمستقبل، إضافة إلى ضمان عدم انتهاك المعطيات وتكاملها وتأكيد عملية ارسالها واستقبالها فشبكة VPN تشفر حركة مرور الشبكة الحامة ، و عملها يتم من خلال خادم VPN الذي يمثل مقر المراقبة داخل المؤسسة

ج- التحديثات تجد نوعين من التحديثات : التحديث الآلي عن طريق قيام البرنامج المثبت في الحاسوب الاتصال بالشركة الأم للتحقق من وجود أي تحديثات، فإن وجد أي منها بادر البرنامج بتنبيه المستخدم إلى ذلك، ويتطلب هذا اتصال الحاسوب بالإنترنت، أما الثاني فهو التحديث اليدوي والذي يكون بمبادرة من المستخدم الذي عليه الذهاب إلى الموقع الالكتروني للشركة المصنعة للبرامج ويقوم بتحميل التحديثات اللازمة[27]

2-**الحماية المادية لممتلكات المؤسسة المادية (الأمن المادي)**:تحقيق الأمن المعلوماتي لا يكون بحماية المعلومات داخل الحواسب فقط، بل من الضروري تحقيق الأمن الخارجي والمادي للمنظمة وموقعها وتجهيزاتها.

أ-أمن موقع المنظمة: هو تحقيق الأمن المادي الموقع المنظمة والسيطرة الخارجية لسياسة وحمايتها من كل تدخل طبيعي أو متعمد من خلال عدة إجراءات :

الاختيار الأمثل الموقع المنظمة.

-تحديد نطاق المؤسسة وتقسيم المواقع الواجب حمايتها .

-تشييد آليات منع الدخول عن طريق تركيب سياج أو سور ملائم للمخاطر أو وضع الأبواب المغلقة بالرموز أو الابواب الدوارة

[27] فيلالي اسماء،وشليل عبد اللطيف ،المرجع السابق.ص.170.

– تركيب أجهزة إنذار في حال التدخل غير المسموح أو في المناطق الحساسة.[28]

الفرع الثاني :تأمين الاجهزة

أولا–تعريف الحاسب الالي: هو جهاز الكتروني يمكن برمجته ليقوم بإدخال ومعالجة البيانات وتخزينها واسترجاعها أو إظهارها للمستخدم بصورة أخرى وله القدرة على انجاز عمليات متعددة في ثواني بسيطة وإذا نظرنا إلى جهاز الحاسوب نظرة شاملة نجد ان وظيفته تتعدى معالجة البيانات المدخلة فيمكنه نقلها إلى جهاز حاسوب آخر أي تبادل معلومات مع الحواسيب الأخرى وذلك من خلال شبكة المعلومات.[29]

ثانيا–تطبيقات الحاسب الالي:

1–**التطبيقات الاصلية:**هي تطبيقات يتم برمجتها وتطويرها لتتوافق مع أحد نظم تشغيل الأجهزة الإلكترونية مثل (Google Android (Apple Windows Phone IOS ومستخدم اللغات برمجية متوافقة معها، فنظام IOSيدعم للغة Programing Objective C بينما يدعم نظام Android للغة Java Programmingوأخيرا يدعم نظام Windows Phone للغة Net Framework

2–تطبيقات الويب:هي تطبيقات تستند على متصفح شبكة الويب للأجهزة الإلكترونية في عملها، ويتطلب توافر تقنيات شبكة الويب مثل Java Script) ومن أهم عيوب هذه الفئة هو محدودية وصولها إلى البيانات الأساسية ونظم تشغيل الجهاز الذكي المستخدم.

كما إنها تستغرق وقت إضافي في تحميل وعرض محتوياتها ووظائفها كونها تعتمد على سرعة اتصال الجهاز المستخدم بشبكة الويب، إلا هذه الفئة تميزت بكونها لا تشترط تجهيزات محددة في الأجهزة الإلكترونية أو تتطلب من المستخدم تحميل تطبيقات أو ملفات تشغيل

---

[28] فيلالي اسماء،وشليل عبد اللطيف ،المرجع السابق، ص.171

[29] University of Babylon ,الحاسوب وتعريف الحاسوب، https://www.uobabylon.edu.iq ،تم الاطلاع عليه يوم 2025/5/10الساعة 7:54

على أجهزتهم المستخدمة في ذلك سوى أن يكون الجهاز مدعم للاتصال بشبكة الأنترنت اللاسلكية (Wireless)[30]

3-التطبيقات الهجينة:هي تطبيقات تحاول الجمع بين خصائص ومميزات كلا من التطبيقات الأصلية وتطبيقات الويب، بشكل يحقق توازن في استخدامها وسرعة تطويرها، فهي تطبيقات يتم تصميمها بلغة (HTML5) ويتم إدراجها داخل نطاق تطبيقي أصيل Container Native) ممثلا في منصة استخدام قائمة على بيئة الويب (Web-based) للإمكانات الفنية والوظيفية التي نتاج الواجهة فقط في شكل تطبيق أصيل قابل للعمل والتشغيل عبر نظم الأجهزة الذكية[31]

ثالثا-أنواع الفيروسات:

تقسم فيروسات الحاسوب إلى أنواع، وهي على النحو التالي:

الفيروسات المخادعة ذات قدرة تحويلية متعددة: وهي البرامج التخريبية التي تمتلك القدرة على الديناميكية في التحول والتخفي من خلال تغيير شفرتها عند بدء بانتقال عدوتها بين الملفات، وذلك لعدم الكشف عنها.

فيروسات قطاع التشغيل (Boot Sector):يتمركز هذا النوع من الفيروسات في المواقع التي يقرأها

جهاز الحاسوب من خلال القرص الصلب، ويبدأ مفعولها التخريبي بالسريان عند بدء إقلاع القرص الصلب وتستقر في ذاكرة جهاز الحاسوب وتبدأ بفك شفرتها وتنفيذ الأوامر يُعتبر

[30] معدي بن عبد الله الشهري، استخدام الأجهزة الإلكترونية وأثرها على سلوك الأطفال من وجهة نظر الوالدين دراسة وصفية على عينة من آباء وأمهات طلاب الصفوف العليا للمرحلة الابتدائية بمحافظة جدة، المجلة الدولية لنشر البحوث والدراسات العدد السابع والعشرون المجلد الثالث، يناير 2022، ص.363.

[31] المرجع نفسه.ص.364.

هذا النوع من أكثر أنواع الفيروسات خطورة ويهدد بشكل مباشر المقطع التشغيلي في القرص الصلب ويصيبه

فيروسات الماكرو Macro Viruses : يعتبر هذا النوع من أكثر أنواع الفيروسات الحاسوبية حداثة، ويعتمد المبرمجون على برنامج معالجة النصوص Microsoft word في كتابته، ويغزو الملفات التي تحتوي على البيانات ويشكل أدق ملفات الأوفيس.

الفيروسات ذات الملفات المتعددة: يدخل هذا النوع من الفيروسات إلى جهاز المستخدم بصبغة معينة وفور استقراره بالجهاز وتمكنه منه يبدأ بالتحول لأكثر من صيغة ليستهدف الملفات جميعها.

الفيروسات الخفية يستقر هذا النوع في ذاكرة جهاز الحاسوب، ويتولى مهمة إعاقة فحص نظام التشغيل وقطاعه ويرسل تقرير بسلامة الجهاز وعدم العثور على أي فيروسات.

فيروسات الملفات التنفيذية :File Infector Viruses: تجعل هذه الفيروسات من نفسها ملحقاً مع ملفات البرامج التنفيذية ومرافقاً لها باستمرار، ومن هذه البرامج التنفيذية Command.com

فيروسات ذات مهام متعددة: تغزو قطاع بدء التشغيل مع الملفات الموجودة على جهاز الحاسوب في أن واحد، أي أنها تغزو جميع محتويات الحاسوب.[32]

الفيروسات الطفيلية :تتطفل هذه الفيروسات على الملفات التنفيذية وتتمركز في الذاكرة، وتبدأ عملها فور استخدام المستخدم لأي من البرامج المصابة، وتبدأ بعدها يغزو أي برنامج يتم تشغيله.

[32] كلية المستقبل الجامعة ،فيروسات الحاسوب ومكونات الفيروس ،htttps://uonus.edu.iq تم الاطلاع عليه يوم 2025/5/10 ،الساعة 7:56

الفيروسات المتطورة: لديها القدرة على الانتقال من جهاز حاسوب إلى آخر من خلال التحول من شفرة إلى أخرى.

رابعا-طرق الحماية:

أ-أشكال الوقاية منها:ينصح المستخدم عادة بحماية جهازه من الفيروسات ووقايته منها، وذلك باتباع الخطوات التالية:

-عدم تحميل أي برامج دون إجراء فحص لها، وكذلك الأمر بالنسبة للملفات المحملة والمنقولة من الشبكة العنكبوتية فيتوجب الفحص قبل التشغيل.

-تحميل البرامج الخاصة للكشف عن وجود الفيروسات ومكافحتها في جهاز الحاسوب.

-الاحتفاظ بنسخ احتياطية (Backup) للملفات والبرامج.

-الاعتماد على برامج الجدار الناري التي تقف عائقاً في وجه الفيروسات.

-تنصيب أنظمة تشغيل أكثر أماناً كنظام التشغيل لينكس.

-عدم تشغيل ملفات وبرامج مجهولة المصدر.

-أخذ الحيطة والحذر من الرسائل التي تصل عبر البريد الإلكتروني والروابط المجهولة

ب-ازالة فيروسات الحاسب:ينصح المستخدم في حال اكتشافه وجود فيروسات بجهازه اتخاذ الإجراءات التالية:

-تنصيب برامج حماية من الفيروسات (Anti-Virus)

- البدء بعمل Scan لكل الملفات الموجودة.[33]

[33] كلية المستقبل الجامعة ، المرجع السابق.

المطلب الثاني :تطوير اليات الحماية من الجريمة الالكترونية

"ولمواجهة مختلف التهديدات الرقمية، برزت عدة آليات تهدف إلى تعزيز أمن المعلومات. ومن أبرز هذه الآليات نذكر التشفير كوسيلة لحماية سرية البيانات، وأنظمة الكشف المبكر عن حالات الاختراق لرصد التهديدات قبل تفاقمها. وسنُفصّل هذين الجانبين في الفروع التالية."

الفرع الاول :اهمية التشفير في حماية المعلومات

بعد التشفير علم قائم بذاته ولد منذ القدم كان يستعمل في الأمور العسكرية لضمان سرية الرسائل والمعلومات المرسلة، وأصبح يشكل وسيلة حديثة لحماية أمن المعلومات، ويستعمل أيضا حاليا كتدبير تكنولوجي المجابهة القرصنة نظرا لخصائصه وفاعليته العالية الكفيلة بضمان حماية المصنف الرقمي، وعليه سوف نتطرق في هذا المطلب إلى ما يلي:

أولا–تعريف التشفير الالكتروني للمعلومات:يعتبر التشفير من حماية المعلومات يتم عن طريقه تحويل النص الأصلي إلى نص آخر غير مقروء يدعى بالنص المشفر ولا يمكن فك تشفيره إلا من خلال مفتاح سري يملكه أشخاص محددين لتحويله إلى نص آخر مقروء

ومن بين الأهداف التشفير الالكتروني نذكر السرية أو الخصوصية، تكامل البيانات، التحقق وإثبات الهوية ، عدم الإنكار.[34]

[34]أحمد غريبي ، حورية قاسيمي ، دور سياسة التشفير الالكتروني في حماية نظم معلومات الإدارة الإلكترونية بمؤسسة بريد الجزائر فرع المدية، مجلة الاقتصاد الجديد، جامعة المدية، الجزائر، المجلد : 12 ، العدد: 1 ، 2021 ،ص.313

ثانيا–مستويات التشفير الالكتروني:

1 **نظام الشبكة الافتراضية:** تعتبر شبكة الأنترنت وسيط لتحويل البيانات والمعلومات من نقطة الإرسال إلى نقطة الموجهة لها، ويكن القول أنه وسيلة آمنة لتبادل تلك المعلومات والبيانات على جزء من هذه الشبكة .

2 **التشفير على مستوى الإرسال:** في هذا المستوى يتم تشفير جميع البيانات والمعلومات وذلك من نقطة الإرسال إلى غاية نقطة الاستقبال، ويعمل هذا المستوى بواسطة الشبكات الافتراضية الخاصة ".

3 **التطبيق المستخدم في تنفيذ:** يستخدم للتشفير الجزئي من أهم نماذجه نظام "SET" وهو نظام خاص لتشفير البيانات والمعلومات وتأمين المعاملات الالكترونية".

4 التشفير على مستوى التصفح أو التنقل: من أجل حماية البيانات والمعلومات أثناء تحويلها عبر الشبكة يتم تشفير جميع الاتصالات في هذا المستوى سواء تلك التي تتم بين فتحات الشبكة، أو برامج المواقع أو التصفح الموجودة عليها، مما يؤدي إلى حماية المعلومات والبيانات أثناء انتقالها ".

5 **التطبيق المستخدم في تنفيذ:** يستخدم للتشفير الجزئي من أهم نماذجه نظام "SET" وهو نظام خاص لتشفير البيانات والمعلومات وتأمين المعاملات الالكترونية[35]

ثالثا–أنواع التشفير الالكتروني:يسعى معظم الباحثين إلى الحصول على طرق تشفير تتناسب مع حجم المعلومات حيث تكون أكثر فاعلية في حفظها والوصول إليها بمستوى عالي من السرية والأمان

[35] -مرابط حمزة ، داودي منصور التشفير كلية لحماية المصفات الرقمية من القرصنة الإلكترونية، مجلة الحقوق والعلوم السياسية جامعة تيارت الجزائر، المجلد 10 العدد 01 2023، ص ، ص.42-43

–التشفير المتماثل :Symmetric Encryption يعرف أيضا بالتشفير بالمفتاح العام وهو يستخدم مفتاح واحد لعملية التشفير وفك التشفير للبيانات، حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات

–التشفير غير المتماثل Asymmetic Encrption:يعتمد على وجود مفتاحين أحدهما علني (عام) والآخر سري (خاص)، يحتفظ الشخص دائما بالمفتاح السري أما المفتاح العلني فيعطيه لمن يريد أن يرسل له رسالة والمفتاح العلني له القدرة على التشفير وليس فك الرسالة بعد إرسالها

بعد التشفير النظام المناسب الحماية البيئة الافتراضية إلا قوته وتقنياته مرهونة بمدى حسن استخدام البرامج والأجهزة لتحقيق عملية الحماية لنظم المعلومات[36]

الفرع الثاني: انضمة لكشف المبكر عن حالات الاختراق

1 تعريف انضمة كشف الاختراق:

– يمكن تعريف كشف الاختراق بأنه عملية معرفة وتحديد الاستخدام المؤذي أو غير المشروع، سوء الاستخدام، تجاوز الحد في استخدام أنظمة الحواسب.[37]

–كما يُعرف نظام كشف الاختراق كمنتج صلب أو برمجي يركز اهتمامه على الحوادث المحتمل حدوثها والناجمة عن نشاط المهاجمين، حيث يعتمد على مراقبة البيانات الخاصة بالاختراقات وتسجيلها وإرسال تقرير تفصيلي المسؤول أمن الشبكة في الزمن الحقيقي.[38]

[36] -أحمد غريبي، حورية قاسيمي، المرجع السابق، ص، ص .313-314

[37]- بشرى ديوب دراسة ومقارنة أنظمة كشف الاختراقات المفتوحة المصدر، مجلة جامعة تشرين للبحوث والدراسات العلمية، سلسلة العلوم الهندسية، المجلد : 37 العدد 5، 2015، ص .276.

[38]- حازم عدنان سلوم، تحسين نظم كشف الاختراق باستخدام تقنية مصائد الاختراق الهجينة، رسالة لنيل شهادة الماجستير في العلوم والتكنولوجيا المعهد العالي للعلوم التطبيقية والتكنولوجيا قسم الاتصالات، سوريا، 2017، ص.9

2-تصنيفات نضم كشف الاختراق:

اولا-حسب مصدر المعلومات التي تراقبها وتحللها إلى :

القمة كشف شبكية Network-Based OS : يراف النظام مقطع كامل من الشبكة.

أنظمة كشف على المضيف 105 Host-Based: تراف هذه الأنظمة المضيف الموضوعة عليه.

-أنظمة كلف على المضيف 105 Host:

-يستطيع تحليل ما يقوم به التطبيق.

-يمكنه التأكد من نجاح أو فشل الاختراق.

-يكشف الاختراقات التي لا تحتاج وجود شبكة.

لا تحتاج إلى عتاديات harthwan إضافية.

-لا تتأثر في حال الشبكات الموصولة بمبدلات switched networks

-Network-Based IDS أنظمة كشف شبكية:

- لا تؤثر على أداء أجهزة الشبكة

- غير مرتبة أبداً من قبل أجهزة الشبكة.

-يمكنها مراقبة أكثر من مضيف في الوقت نفسه

-أكثر مقاومة المحاولات التلاعب[39]

[39] -بشرى ديوب.المرجع السابق.ص.276.

-يمكنها كشف الاختراقات الشبكية التي من غير الممكن كشفها من وجهة نظر جهاز واحد.

ثانيا- حسب طريقة التحليل و الكشف إلى: وانظمة كشف الشذوذ Anomaly - Based: تعتمد على تعريف ما هو السلوك الطبيعي أو المسموح به في النظام و من ثم الإعلام عن أي فعل أو حدث يقع خارج حدود المسموح أو الطبيعي.

وأنظمة الكشف المعتمدة على التواقيع 105 Signature-Based و انظمة كشف سوء الاستخدام

Misuse-Based: النموذج الذي كتب التوصيف السلوك السين هو الفرضية الأساسية، بعد ذلك يقوم النظام بمقارنة تسلسل المعلومات مع هذا النموذج ليقرر ما هو جيد و ما ، تحتاج الأنظمة المعتمدة على المواقع الصيانة وتعديل بشكل دائم للتعرف على الاختراقات الجديدة، في حين تستطيع أنظمة كشف السعود الكشف عن الاختراعات الجديدة.[40]

-انظمة الكشف المعتمدة على التواقيعSignature-Based IDS:

-معدل كشف أعلى و انذارات خاطئة أقل.

-لا تحتاج إلى طور تعلم. من الصعب تجاوزها.

-تزود معلومات أكثر عن الاختراق.

Anomaly-Based IDS أنظمة كشف الشذوذ

-لا تحتاج إلى صيانة مستمرة

-يمكنها كشف الاختراقات الجديدة.[41]

[40] -بشرى ديوب،المرجع السابق،ص.276

[41] نفس المرجع . ص .ص 276- 277.

ثالثا-الأنظمة المعتمدة على القواعدRule-based systems:تفتقر هذه الأنظمة إلى قوة الأنظمة الخبيرة، ولكنها تتميز بوضوح نماذج الاختراق كل اختراق يتم توصيفه بقاعدة واحدة تأخذ الشكل التالي

condition, A condition, A condition actions)

يعتبر النظام أن هناك اختراق عندما تكون نتيجة تقييم كل الشروط true وعندها يجب القيام بالأفعال المحددة ب actions، ويتم تفعيل القاعدة من أجل الرد على هذا الاختراق

نظام Snort:

يعتبر هذا النظام من الأنظمة الشبكية التي تؤمن الوقاية من الاختراق Network Intrusion Prevention قادر Network Intrusion Detection System NIDS))(و نظام كشف للاختراقات الشبكية)NIPS) Systemعلى تحليل وتسجيل الرزم المتبادلة

يقوم Snort:بعملية تحليل للبروتوكولات، وعمليات مطابقة وبحث matching searching في محتويات الرزم packet payload، وتم استخدامه بشكل أساسي من أجل الكشف دون الرد) عن عدد كبير من الهجمات وعمليات السير Scan [42]

رابعا- وظائف أنظمة كشف الاختراق:هنالك العديد من المهام التي تقوم بها أنظمة كشف الاختراق نذكر منها [2] :

1- الرصد والمراقبة حيث تقوم برصد نشاط المستخدمين ومراقبة حركة البيانات ضمن الشبكة من أجل التقاط أي نشاط مشبوه.
2- التعرف على الأنماط حيث تملك أنظمة كشف الاختراق القدرة على التعرف على أنماط الهجومات المعروفة مسبقاً.

[42] -بشرى ديوب ,المرجع السابق،ص. 277

3- إنشاء تقارير عن الاختراقات تقوم أنظمة كشف الاختراق بإعداد تقرير تفصيلي عن الأحداث الملتقطة، ليتم فيما بعد الاستفادة منها من قبل مسؤولي الحماية في المنظومة التحليل سلامة النظام ومعرفة نقاط الضعف المستهدفة.

4-تعقب أداء المستخدمين حيث تقوم بتعقب محاولات تجاوز أو انتهاك السياسات المسندة إلى المستخدم لتقييم النظام والمحافظة على أصالة البيانات..

5-تنبيه مسؤولي أمن النظام عند حدوث أي اختراق تقوم بإرسال إنذارات إلى مسؤولي النظام عبر صفحات برمجية أو عبر البريد الالكتروني.

6- القدرة على كشف الهجوم في مراحله الأولية عندما يحاول المهاجم أن يبدأ بتفحص المنافذ المفتوحة لتحديد نقاط الضعف.

7-تسجيل الأحداث عند النقاط أي نشاط مشبوه تقوم هذه الأنظمة بتسجيل البيانات المتعلقة بهذا النشاط[43]

[43] -حازم عدنان سلوم ،المرجع السابق، ص.11

خلاصة الفصل

يستخلص من ختام هذا الفصل، أن الوقاية القبلية من الجريمة الإلكترونية أصبحت ضرورة حتمية تفرضها التحولات المتسارعة في العالم الرقمي، الأمر الذي يتطلب تبني مقاربة شاملة ومتكاملة تُدمج بين البُعد التشريعي، الأمني، والتقني.

فقد أظهر التحليل أن المشرع الجزائري عمل على تطوير المنظومة القانونية لمواجهة هذا النوع من الجرائم، من خلال تحديث القوانين وتكييف النصوص العقابية بما ينسجم مع طبيعة التهديدات السيبرانية. كما برز الدور الفاعل للأجهزة الأمنية في الكشف المبكر والاستجابة السريعة، إلى جانب مساهمة الإعلام الأمني في نشر الوعي وبناء ثقافة مجتمعية واعية بالمخاطر الرقمية.

من جهة أخرى، فإن حماية الفضاء السيبراني لم تعد مسؤولية داخلية فقط، بل باتت تتطلب تنسيقًا دوليًا واسع النطاق، خاصة أمام الطبيعة العابرة للحدود لهذه الجرائم. وقد شكلت الوقاية التقنية، من خلال آليات كالتشفير وتأمين الشبكات، دعامة أساسية لتعزيز أمن المعلومات والتقليل من فرص الاختراق.

وفي المجمل، خلُص الفصل إلى أن الوقاية الفعالة من الجريمة الإلكترونية لا تتحقق إلا بتكامل التشريع، الأمن، التقنية، والتعاون الدولي، وهو ما يشكل الأساس الحقيقي لبناء منظومة دفاعية قوية في وجه هذه الظاهرة المعقّدة.

الفصل الثاني

مكافحة الجريمة الإلكترونية في التشريع الجزائري

الفصل الثاني: مكافحة الجريمة الإلكترونية في التشريع الجزائري:

في ظل التطور التكنولوجي الهائل الذي يشهده العالم أضحت الجريمة الإلكترونية تمثل تحدياً حقيقياً للأمن القانوني والمجتمعي، لما تنطوي عليه من تعقيدات وصعوبة في الكشف عنها والتصدي لمرتكبيها. ومن هذا المنطلق، لم يعد من الكافي الاقتصار على وسائل الوقاية التقليدية، بل أصبح من الضروري اعتماد مقاربة شاملة تأخذ بعين الاعتبار خصوصية هذا النوع من الجرائم. لذا، يهدف هذا الفصل إلى تسليط الضوء على الوسائل المعتمدة في الوقاية البعدية من الجريمة الإلكترونية، سواء من الناحية الإجرائية أو القانونية، من خلال دراسة مختلف الأجهزة المكلفة بمكافحتها والإجراءات القانونية المتخذة في هذا السياق.

وفي هذا الفصل سنتناول اهم الوسائل البعدية التي اقرها التشريع الجزائري من خلال التطرق الى الوسائل الاجرائية المؤسساتية ،واعطاء نضرة حول الوحدات المختصة بتولي اجراءات البحث والتحقيق في الجريمة الالكترونية و الاشارة الى الوقاية في قانون العقوبات (المبحث الاول) وصولا الى التدابير الاجرائية للكشف عن الجريمة المعلوماتية وبيان الاجراءات القانونية للكشف عنها وكذا الاجراءات المستحدثة في مجال الجريمة الالكترونية وفق التشريع الجزائري (المبحث الثاني)

المبحث الاول: الوسائل الاجرائية لمكافحة الجريمة الالكترونية:

تعد الوسائل الإجرائية من أهم الركائز في الوقاية البعدية من الجرائم الإلكترونية، نظراً للدور المحوري الذي تلعبه في الكشف عن الجرائم وتعقب مرتكبيها وجمع الأدلة اللازمة لمقاضاتهم. ويبرز في هذا الإطار دور الوحدات المختصة في البحث والتحري، سواء على مستوى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو على مستوى الأجهزة الأمنية التقليدية. كما أن للقانون الجزائي دوره في هذا المجال من خلال ما يتضمنه من عقوبات أصلية وتكميلية تهدف إلى ردع الجناة ومنع تكرار مثل هذه الجرائم.

المطلب الاول: الوحدات المختصة بتولي اجراءات البحث والتحقيق في الجريمة الالكترونية:

تعتبر الجريمة المعلوماتية من ضمن الجرائم المستحدثة التي غزت الساحة العالمية تقدمت بسرعة مذهلة رغم الجهود الكبيرة التي بذلها الدول المتقدمة لمكافحة هذا المد الإجرامي، إلا أنها لا زالت مستمرة لاعتمادها على تكنولوجيات الاتصالات والمعلوماتية.

والمشرع الجزائري على غرار باقي الدول يسعى جاهدا من أجل مكافحتها والحد من آثارها الوخيمة بجملة من الوسائل منها التشريعية وذلك بالنص عليها في قانون العقوبات وتطبيق إجراءات خاصة للبحث والتحري عنها في قانون الإجراءات الجزائية أو القانون (09/04)[44].

[44] جبار فاطمة، "الخصوصية الإجرائية لمواجهة الإجرام الإلكتروني في التشريع الجزائري"، مجلة دراسات وأبحاث، المجلد 12، العدد 4، أكتوبر 2020 ،ص. 674

الفرع الأول : الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال

نص القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لمكافحتها، في الفصل الخامس منه على إنشاء هيئة وطنية للوقاية من الجرائم المعلوماتية أو كما تعرف عامة بالجرائم الإلكترونية.[45]

ويعتبر هذا التشريع نقلة نوعية في النصوص الإجرائية الجزائية بالنظر إلى نوعية الإجراءات التي نص عليها كمراقبة الاتصالات السلكية واللاسلكية والمراسلات الإلكترونية والاتصالات الهاتفية، وكذا مراقبة كل المعطيات الشخصية على الإنترنت، وهو ما قد يتخذ أحيانا بقصد أو دون قصد كطريق للمساس بحرمة حياة الأشخاص وأمن اتصالاتهم وبياناتهم الشخصية المالية والصحية والاجتماعية، لذلك تم إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا المعلومات ومكافحتها، تتكون هذه الهيئة هي الجهة الرقابية الخاصة بهذا النوع من الجرائم، حتى تضمن الحق الدستوري لكل مواطن في حرمة حياته ومراسلاته من المساس بها بداعي مكافحة الجرائم، ويقصد تفعيل نص المادة 13 من القانون 09-04 فقد صدر في البداية المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،غير أنه في 2019 صدر مرسوم رئاسي 19-172 المعدل بالإلغاء للأحكام المرسوم الرئاسي 15-261 وذلك نتيجة الظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة مما أفضى إلى ظهور مخاطر فعلية التعرض الأمن العمومي وكذا المؤسسات الدستورية للخطر فجاء هذا المرسوم ليغير

[45] قانون رقم 09-04 مؤرخ في 5اغسطس 2009 متضمن قواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الصادرة ب 5اغسطس 2009 ،ج ر،ج،ج العدد 47،سنة 2009

من الطبيعة القانونية للهيئة حيث نقل الإشراف عليها من وزارة العدل إلى وزارة الدفاع مما حولها إلى هيئة ذات طابع أمني.[46]

أولا-تشكيلة الهيئة الوطنية:في ظل المرسوم الرئاسي رقم 15-261 كانت الهيئة تضم مجموعة من الهياكل تتمثل في:لجنة مديرة – مديرية عامة – مديرية للمراقبة الوقائية واليقضة الالكترونية – مديرية للتنسيق التقني – مركز للعمليات التقنية – ملحقات جهوية

-**اللجنة المدبرة:** تتشكل من الوزير المكلف بالداخلية الوزير المكلف بالبريد وتكنولوجيات الاعلام والاتصال قائد الدرك الوطني المدير العام للامن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا يعنهما المجلس الأعلى للقضاء، ويعين ممثلا رئاسة الجمهورية ووزارة الدفاع الوطني بموجب مرسوم رئاسي برأسها الوزير المكلف بالعدل ".

الملاحظ أن تشكيلة اللجنة المديرة ادارية بحتة تعكس تبعية مطلقة للسلطة التنفيذية.

-**المديرية العامة:** نص المرسوم الرئاسي على رئاسة المديرية العامة من قبل مدير عام يعين بموجب مرسوم رئاسي. من دون تحديد وضبط تشكيلتها.

أما باقي الهياكل، فلم يحدد المرسوم الرئاسي رقم 15 261 تشكيلها ولا تنظيمها، محيلا الأمر الصدور قرار مشترك بين الوزراء المكلفين بالعدل والدفاع الوطني والداخلية.[47]

أما بعد صدور المرسوم الرئاسي رقم 19-172، فقد أصبحت الهيئة مكونة من جهازين اثنين هما: مجلس التوجيه ومديرية عامة، طبقا لنص المادة 4 من هذا المرسوم.

---

[46] بوكيحل حكيمة ، وسامية بن عبيد، "الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلومات"، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 1، 2021، ص. 1544

[47] -خريشي إلهام، "النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، مجلة الأبحاث القانونية والسياسية، المجلد 4، العدد 1، 2022،ص .63

-**مجلس التوجيه:** حددت المادة 5 من المرسوم الرئاسي رقم 19-172 تشكيلة مجلس التوجيه من ممثلي الوزارات الآتية: وزارة الدفاع الوطني الوزارة المكلفة بالداخلية وزارة العدل الوزارة المكلفة بالمواصلات السلكية واللاسلكية، برئاسة وزير الدفاع الوطني أو ممثله.

الملاحظ ان المرسوم الجديد حصر تشكيلة الهيئة في اربع وزارات واسقط عدة قطاعات أخرى كالامن والدرك الوطنيين والقضاة". وهو ما يعاب على المشرع عند اسقاطه عضوية القضاة ذوي الخبرة في مجال مكافحة الجرائم السيبرانية.[48]

-**المديرية العامة:** اكتفى المرسوم الرئاسي بوضعها تحت إدارة مدير عام وتضم مديرية تقنية مديرية للإدارة والوسائل، مجموعة من المصالح. من دون تحديد تشكيلها بدقة.

الملاحظ ان المرسوم الرئاسي الجديد قد لجأ إلى التقليص من الهياكل الرئيسية المكونة للهيئة على خلاف سابقه وعوضها بهياكل جديدة فرعية تعمل تحت سلطة المديرية العامة وتتمثل في:

مديرية تقنية مديرية للادارة والوسائل مصالح من دون تحديد تشكيلتها التي ترجع من دون شك للمدير العام بتفويض من وزير الدفاع بالنظر للمهام التي تقوم بها.

النتيجة التي تخلص الها أن المرسوم الرئاسي الجديد اتجه إلى تركيز هياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلال احلال نظام تدرج لصالح المديرية العامة بعد أن كان لصالح اللجنة المديرة في ظل المرسوم السابق.[49]

---

[48] المرسوم الرئاسي رقم 19-172 المؤرخ في 6جوان 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنضيمها وكيفيات سيرها ،الصادرة في 9جوان 2019 ،ج رج،ج العدد37 سنة 2019

[49] -خريشي إلهام، المرجع السابق ،ص .64

ثانيا-المهام: لقد سبق البيان أن القانون رقم 09-04 نص في المادة 14 على مجمل الاختصاصات التي منحها المشرع للهيئة، فهي تتولى على وجه الخصوص المهام الآتية:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي يجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات الفضائية.

-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

بما ان القانون المتضمن القواعد الخاصة المتصلة بجرائم الإعلام والاتصال ومكافحتها قد نص في المادة 14 منه على مهام الهيئة بصفة واضحة، إلا أنه في المرسوم الرئاسي السالف الذكر فصل في هذه المهام ووزعها على مجلس التوجيه والمديرية العامة[50]

-**مهام مجلس التوجيه:** يكلف المجلس على الخصوص بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية وتكنولوجيات الاتصال ومكافحتها، وكذا يتداول ويناقش مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة

بتكنولوجيات الإعلام والاتصال، إجراء تقييم دوري لحالة التهديد في مجال الجرائم والأهداف المرجوة منها، كما يقترح أي نشاط براه مناسبا يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المعلوماتية ومكافحتها، كما يقدم كل اقتراح في مجال اختصاص

[50] بوكحيل حكيمة ،المرجع السابق،ص. 1546

الهيئة وكذا يساهم في ضبط المعايير القانونية في مجال اختصاصه، ويدرس ميزانية الهيئة و يوافق عليه.

أما فيما يتعلق بتسييره فإنه يجتمع في دورتين عاديتين بناء على استدعاء من رئيسه كما يمكن أن يجتمع في دورة غير عادية بناء على استدعاء من رئيسه أو يطلب من أحد أعضائه أو من المدير العام للهيئة كلما كان لذلك ضرورة عملية وهو ما نصت عليه المادة 6 من المرسوم السالف الذكر، أما المادة 8 فقد حددت قواعد وكيفيات سير مجلس التوجيه بناء على قرار من وزير الدفاع الوطني.

– **مهام المديرية العامة:** تتولى المديرية السهر على حسن سير الهيئة وذلك من خلال تنشيط و تنسيق عمليات الوقاية المتصلة بجرائم تكنولوجيات الإعلام والاتصال ومكافحتها، وكذا تبادل المعلومات مع الهيئات الأجنبية التي تعمل في نفس المجال في إطار التعاون الأمني بغرض تجميع المعطيات المتعلقة بمرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك للتعرف عليهم وتحديد مكان تواجدهم بالإضافة إلى القيام بمهام إدارية بحتة ك إعداد مشروع ميزانية الهيئة، إعداد وتنفيذ برامج عمل الهيئة وكذا العمل تنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة تحضير اجتماعات مجلس التوجيه كون المديرية العامة تتولى مهام الأمانة العامة لمجلس التوجيه بموجب المادة 5 الفقرة الأخيرة من المرسوم السالف الذكر كما تقوم بإعداد التقرير السنوي النشاطات الهيئة حيث يمسك محاسبة الهيئة حسب قواعد المحاسبة العمومية وهو ما نصت عليه المادة 17 من المرسوم السالف الذكر.[51]

الفرع الثاني: الاجهزة الامنية المكلفة بالبحث والتحري

اولا–الضبطية القضائية

[51] -بوكحيل حكيمة ،المرجع السابق،ص. 1546

تعتبر الضبطية القضائية صاحبة الاختصاص الاصيل في كل الجرائم بما فيا الجريمة الالكترونية، وقد منحها القانون اساليب تحري جديدة نبينها فيما يلي :

1 على مستوى جهاز الشرطة:أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة ، ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف على جرائم الانترنت . بالإضافة لإنشائها ثلاث مخابر على مستوى بشار ورقلة وتمنراست قيد الإنجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن .. كما يظم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم دائرة الادلة الرقمية والآثار التكنولوجية والتي تضم ثلاث أقسام هي :

–قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات

–قسم استغلال الادلة الناتجة عن الهواتف النقالة

–قسم تحليل الأصوات، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الالكترونية 34

2 **على مستوى جهاز الدرك الوطني:** تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الاجرام الكائن مقره ببو شاوي التابع لقيادة الدرك العامة قسم الاعلام و الإلكترونيك الذي يختص بالتحقيق والكشف عن الجرائم الالكترونية ". وأيضا بواسطة مديرية الامن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية ، وهي هيئة ذات اختصاص وطني مهمتها التصدي للجريمة الإلكترونية [52]

[52] -فلاح عبد القادر، بن عبد المالك نادية، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الباحث للدراسات القانونية والسياسية، المجلد 4 ، العدد 2، 2019، ص ،ص. 1695-1696

ثانيا–مركز الوقاية من جرائم الاعلام الآلي والجرائم الإلكترونية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية عن طريق المرسوم الرئاسي رقم 15 261 و مقره بئر مراد رايس، وهو تابع المديرية الأمن للدرك الوطني. وقد حددت المادة الأولى منه تشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال " . وتمارس هذه الهيئة العديد من المهام في مجال التصدي للجريمة الإلكترونية ورد النص عليها في المادة 14 من القانون 09–04 سالف الذكر وهي

–ضمان المراقبة المستمرة لشبكة الانترنت

–القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني

–المشاركة في عمليات البحث والتحري عن الجرائم الإلكترونية

المطلب الثاني : الوقاية من الجريمة الالكترونية في قانون العقوبات الجزائري

بهدف تدارك الفراغ القانوني قام المشرع الجزائري بإدراج قسما كاملا في قانون العقوبات الجزائري رقم 04 15 متعلقا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات و هذا ضمن القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال حيث قام المشرع بسن جملة من القواعد القانونية الموضوعية و التي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة, وتأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الآلية أو وصف الاعتداء على معطيات نظام المعالجة الآلية كما يمكن لها أن تأخذ وصف الاعتداء على سير نظام المعالجة الآلية الجريدة الرسمية العدد 71/2004)[53]

[53] -بوخالفة سعاد ، "مكافحة الجرائم الإلكترونية في التشريع الجزائري"، ضمن أعمال الملتقى الوطني الافتراضي حول الجرائم الإلكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني، جامعة يحي فارس المدية ، 15 مارس 2022، ص. 119

الفرع الأول: العقوبات الأصلية

اولا – عقوبة جرائم الاعتداء على نظام المعالجة الآلية للمعطيات

طبقا للمادة (13) من الاتفاقية الدولية للإجرام المعلوماتي؛ فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية وسالبة للحرية، تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناء على تبني مبدأ مساءلة الشخص المعنوي الواردة في المادة (12) من الاتفاقية، كما نص المشرع الجزائري على مجموعة من العقوبات عن الجرائم الماسة بالنظام والمتمثلة في عقوبات أصلية وأخرى تكميلية بموجب المواد من 394 مكرر إلى 394 مكرر 5 ، كما نص على عقوبة الأشخاص المعنوية والأشخاص الطبيعية، وأيضا عقوبة المساهمة والشريك في الجريمة.

واعتمد المشرع أثناء وضعه لهاته الجرائم على معيار أساسه الخطورة الإجرامية لكل جريمة على حدا، بحيث اتبع مبدأ الهرمية في التدرج في سلم العقوبات، فنص على جريمة الدخول أو البقاء في الصورة البسيطة والمشددة، ثم نص على جريمة الاعتداء العمدي على المعطيات باعتبارها أشد خطورة من سابقتها، ذلك أنها تستهدف المعطيات الموجودة داخل النظام بما فيها البيانات والبرامج المعطيات وأي اعتداء عليها سيؤدي لا محالة إلى وقف النظام أو تعطيله أو تغيير سير وجهة هذا النظام .[54]

العقوبات المقررة لشخص الطبيعي

العقوبات الأصلية من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية: يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد

[54] بوزينة امنة امحمدي ، "الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري: دراسة تحليلية لقانوني العقوبات وحقوق المؤلف"، مجلة القانون والمجتمع، العدد 6، 31 ديسمبر 2015، ص .111.

الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات. إذ نجد سلم خطورة الجريمة يتضمن ثلاث درجات جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.

الدخول والبقاء بالغش الجريمة البسيطة العقوبة المقررة في 3 أشهر إلى سنة حبس و 50000 دج إلى .)100000 دج غرامة (المادة 394) مكرر

الدخول والبقاء بالغش الجريمة المشددة تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير المعطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة المادة 394 مكرر / (32).

الاعتداء العمدي على المعطيات طبقا لنص المادة (394) مكرر (1) فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام في الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى

2000000 دج. أما العقوبة المقررة لاستخدام المعطيات وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية العقوبة المقررة في الحبس من شهرين إلى ثلاث)2(سنوات وغرامة من (2) 1000000 دج إلى 5000000 دج (394) مكرر2[55]

[55] -امحمدي بوزينة امنة ، خصوصية قواعد التجريم عند الاعتداء على انظمة المعالجة الآلية للمعطيات في اطار التشريع الجزائري ، مجلة ببلوفيليا لدراسات المكتبات والمعلومات ، العدد 05 ، 30 مارس 2020، ص.82.

-2- العقوبات المقررة لشخص المعنوي :

أقر المشرع الجزائري مبدأ مساءلة الشخص المعنوي في القانون 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66، وذلك بنص المادة (51) مكرر) من هذا التعديل (200) ، كما تجدر الإشارة إلى أن المشرع الجزائري، قد أقر في التعديل الأخير القانون العقوبات المسؤولية الجزائية للشخص المعنوي، وذلك في نص المادة (18) مكرر) من القانون رقم 15/04 المتضمن قانون العقوبات .

أما بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة (394) مكرر (4) من قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي .

ثانيا : العقوبات المقررة لجريمة التقليد

قبل صدور قانون حماية المؤلف كان التعدي على الملكية الأدبية والفنية تحكمه المواد (390) إلى (394) من قانون العقوبات الجزائري، إلا أن أحكام هذه المواد الغيت بمقتضى المادة (151) من الأمر رقم 10/97 المؤرخ في 6 مارس (159)158((157) (156) (153) 1997، كما ألغي هذا الأمر بموجب الأمر 05/03، حيث تضمنت المواد العقوبات المقررة الجريمة التقليد وهي على قسمين عقوبات أصلية وتكميلية[56]

العقوبات الاصلية:

نصت المادة (153) من الأمر رقم 05/03 على عقوبة التقليد بقولها: " يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين (151) و (152) أعلاه بالحبس من سنة أشهر إلى ثلاثة سنوات وبغرامة مالية من خمسمائة ألف دينار إلى مليون

[56] امحمدي بوزينة امنة ،المرجع السابق، ص. 88.

دينار سواء كان النشر قد حصل في الجزائر أو في الخارج"، كما نصت المادة (154) من الأمر رقم 05/03، بقولها: "بعد مرتكبا الجنحة المنصوص عليها في المادة (151) من هذا الأمر ويستوجب العقوبة المقررة في المادة 153 أعلاه كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة، ونصت المادة (155) من الأمر رقم 05/03 بقولها: "بعد مرتكبا لجنحة التقليد ويستوجب نفس العقوبة المقررة في المادة 153 أعلاه كل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو لأي مالك حقوق مجاورة.. ونصت المادة (156) من الأمر رقم 05/03 بقولها: تضاعف في حالة العود

العقوبة المنصوص عليها في المادة 153 من هذا الأمر مما تجدر الإشارة إليه أن هذه العقوبات تسري على جميع صور التقليد .[57]

الفرع الثاني : العقوبات التكميلية

اولا – العقوبات التكميلية لجرائم الاعتداء على نظام المعالجة الآلية للمعطيات

– نصت المادة (394) مكرر (3) من قانون العقوبات على العقوبات التكميلية والمتمثلة في المصادرة وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

إغلاق المواقع والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

[57] -امحمدي بوزينة امنة , المرجع السابق، ، ص.88.

إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها .[58]

ثانيا – العقوبات التكميلية المقررة لجريمة التقليد

تتلخص هذه العقوبات في الغلق والمصادرة ونشر ملخص الحكم الصادر في الدعوى.

1 – الغلق نصت المادة (156) من الأمر رقم 05/03 ، بقولها: "يمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت لمدة لا تتعدى ستة أشهر للمؤسسة التي يستغلها المقلد أو شريكه او ان تقرر الغلق النهائي

بناء على هذه المادة، فإن للمحكمة الحكم بغلق المؤسسة التي يستغلها المقلد سواء كانت مملوكة لهم أم مستأجرة، ويجوز كذلك الحكم بالغلق المؤقت أو النهائي لهذه المؤسسة وذلك بالموازاة مع حجم الخسائر أو نوع الجريمة القائمة ويرجع الفصل فيها المحكمة الموضوع.

2 – المصادرة نصت المادة (159) من الأمر رقم 05/03، بقولها: "يمكن للجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي المصنف أو أداء محمي مصادرة، وإتلاف كل عناد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة. يتضح من خلال نص المادة أن المصادرة وجوبية، فالقاضي ملزم بأن يحكم بمصادرة وإتلاف جميع الوسائل والعتاد المستخدم في النسخ والتقليد، كما وأن المادة (159) حددت الجهة التي يمكن أن تؤول إليها هذه الأموال والوسائل محل المصادرة، بحيث قررت تسليمها للمؤلف أو مالك الحقوق أو ذوي حقوقها، وهي بذلك تعتبر بمثابة تعويض عن الضرر اللاحق بهم.

[58] -امحمدي بوزينة امنة , االمرجع السابق، ص.83.

-3 – نشر ملخص الحكم نصت على هذه العقوبة المادة (158) من الأمر رقم 05/03 على أنه للمحكمة بطلب من الطرف المدني أن تأمر بنشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها، ومن ضمن ذلك على باب مسكن المحكوم عليه على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها ..

ويقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، فهي ماسة بالشرف. والاعتبار وهي عقوبة تكميلية وجوبية يجب الحكم بها دائما في حال صدور حكم بالإدانة حتى ولو وقف تنفيذ الحكم .[59]

المبحث الثاني: التدابير الاجرائية للكشف عن الجرائم الالكترونية

تفرض الجريمة الإلكترونية تحديات جديدة على أجهزة العدالة، مما استدعى تطوير إجراءات قانونية خاصة تمكن من كشف هذا النوع من الجرائم المعقدة. ويهدف هذا المبحث إلى تسليط الضوء على أهم الوسائل الإجرائية المعتمدة، سواء التقليدية أو المستحدثة للكشف عن الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات في إطار قانوني بوازن بين الفعالية وحماية الحقوق...

المطلب الأول : الاجراءات القانونية للكشف عن الجرائم المعلوماتية

كشفاً للجرائم وتعقباً لمرتكبيها وبحثاً عن الأدلة الناتجة عنها، تقوم الجهات المختصة بإتباع أساليب البحث والتحري المختلفة من أجل الوصول إلى كل ما سبق ذكره، فالتحقيق في مجال القانون هو مجموعة الإجراءات التي تباشرها سلطة التحقيق عند وقوع جريمة أو حدث بهدف البحث والتنقيب عن الأدلة التي تفيد في كشف الحقيقة، فالإجراءات المتبعة

[59] -امحمدي بوزينة امنة ، المرجع السابق، ،ص. 83.

هي في الغالب التي ينص عليها قانون الإجراءات الجزائية، ومنها التي سيتم التطرق لها في هذا المطلب ؛ كالمعاينة والتفتيش عن الأدلة وضبطها وتحريزها وفقاً لما ينص عليه القانون وبالرغم من أن كل تلك الإجراءات تقليدية في غالبها، إلا أن طبيعة الجريمة الإلكترونية وخصائصها استوجبت التفتيش ، هو البحث في مستودع سر المتهم وهو إجراء من إجراءات التحقيق يتطلب أو امر قضائية لمباشرته ويجب على المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني بطمس معالم الجريمة وإخفاء كل ما يتعلق بها وهو يستطيع ذلك إذا اتسع له الوقت وسنحت الفرصة .[60]

الفرع الأول: اجراءات التفتيش ومعاينة مسرح جرائم الماسة بأليه المعطيات

أولا : معاينة مسرح جريمة الكترونية

تعد المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة ومن اهم المراحل على الاطلاق نظرا لما يمكن ان توفره من ادلة لاثبات الجريمة وتزداد اهميتها في الجرائم المرتكبة عبر الانترنت و ذلك راجع للطبيعة الخاصة للسلوك الاجرامي فيها بالاضافة الى اعتبارها من الجرائم المستحدثة مما استوجب ابتكار اجراءات خاصة بالمعاينة في هذا المجال

1- مفهوم المعاينة ومسرح الجريمة

تاتي المعاينة لغة بمعنى النظر وعاين الشئ اى راه بعينه ودلالتها في اللغة تشير الى بمعناه الواسع الى الرؤية و المشاهدة ودلالتها القانونية وخاصة في المجال الجنائي هي التي تعتمد على حاسة البصر وتبعا لذلك تعنى المعاينة رؤية اماكن ارتكاب الوقائع الجنائية كما

[60] -شنتير خضرة, الاليات القانونية لمكافحة الجريمة الالكترونية ، (دراسة مقارنة) ، اطروحة دكتوراة ، جامعة أحمد دراية ، ادرار ، كلية الحقوق والعلوم السياسية ، 2021، ص . 63.

تنصرف الى فحص جسم المجنى عليه و المتهم و اثبات ما يوجد بها من اثار . وعرفها جانب من الفقه بأنها مشاهدة و اثبات الحالة في مكان الجريمة ...[61]

غير أن المشرع الجزائري لم يحدد المقصود بالمعاينة ولكن قانون الإجراءات الجزائية أشار إلى إجراء المعاينة باعتباره إجراء من إجراءات السلطات التحقيقية بمختلف فئاتها وطوائفها، حيث نصت المادة 79 من الأمر رقم 155-66 المتضمن (ق.إ. ج. ج) على أنه يجوز القاضي التحقيق الانتقال إلى أماكن وقوع الجرائم الإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها ...»[62]

أ-**المسرح التقليدي** هو مسرح الجريمة الذي يقع خارج بيئة الحاسب الآلي ويمكن الرجل الضبط الجنائي العثور فيه على آثار مادية خلفها الجاني، كالأوراق والأقراص المرنة والصلبة وأشرطة تخزين المعلومات والقطع الإلكترونية وأجهزة المودم والبرامج المستخدمة والطابعات وأقراص الليزر والبطاقات المستخدمة ووسائل الحفظ، وأشرطة الحاسب الآلي وكابلاته وشاشة العرض الخاصة به ومفاتيح التشغيل والأسطوانات وغيرها من مكونات الحاسب ذات الطابع المادي المحسوس. وليس هناك صعوبة مادية لتقرير مدى صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبها إلى شخص معي [63]

فالمعاينة التي تتم على مستوى مسرح الجريمة التقليدي تتسم بالسهولة لوقوعها على عناصر مادية ملموسة .

---

[61] -منير محمد الجنبيهي ، صعوبات التحقيق واستخراج الادلة في جرائم المعلومات ، دار الفكر الجامعي ، الاسكندرية ، 2019 ,ص. 62.

[62] -بومحراث ليندة ، اجراءات التحقيق الخاصة بالجرائم السيبرانية " ، يوم دراسي حول الجريمة السيبرانية ، مجلس فضاء قسنطينة بالتعاون مع جامعة قسنطينة 1 ،2،3، وجامعة الأمير عبد القادر للعلوم الاسلامية،2022 ، ص. 11.

[63] -.بومحراث ليندة , المرجع السابق ، ص.12.

ب- المسرح الافتراضي هو المسرح الإلكتروني الذي يقع داخل النظام المعلوماتي أو العالم الافتراضي والذي قام فيه المجرم بجريمته أو قام بها بواسطته، ويصل إليه رجل الضبط الجنائي بطريقة فنية تستلزم الالمام بالتقنية والاتقان لها، ويمكن من خلال هذا المسرح استخلاص الدليل الجنائي الإلكتروني وغيره من الأدلة المعلوماتية التي تثبت وقوع الجريمة ونسبها إلى مرتكبيها وهذا المسرح يتكون من البيانات الرقمية التي تتواجد في ذاكرة الأقراص الصلبة الموجودة داخل الحاسوب.[64]

2 - إجراءات المعاينة التقنية:

تتمثل إجراءات المعاينة التقنية في الانتقال إلى مسرح الجريمة المعاينة وتأمينه.

اولا- الانتقال إلى مسرح الجريمة

كتم المعاينة في الجريمة الإلكترونية المرتكبة عبر الإنترنت أو بواسطة الحاسب الآلي كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني .ومن بين التدابير الفنية والتحفظية التي تساعد المحقق على المعاينة الإلكترونية هي كالآتي:

الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد وموقع الأجهزة الإلكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.

[64] -.بومحراث ليندة ،المرجع السابق،ص. 12.

توفي الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة يمكن الاستعانة بها في الفحص التشغيل الضبط والتأمين وحفظ المعلومات.

التحفظ على محتويات سلة المهملات ومستندات الادخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة الرفع ومضاهاة ما لقد يوجد عليها من بصمات .

– إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجيا الإعلام الآلي للاستعانة بهم عند الحاجة .[65]

ثانيا– تأمين مسرح الجريمة

من أجل ضمان حماية وتأمين المسرح الجريمة الواجب مراعاة بعض الضوابط التالية:

تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان النقاط كل صورة

إخطار الفيل الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة

المناسبة لضبط أدلة الجريمة حال معاينتها وتأمينها.

[65] عبد النور سعيداني ، ليندة بومحراث ، اجراءات البحث والتحري في الجرائم الالكترونية ضمن اعمال الملتقى الوطني الافتراضي حول الجرائم الالكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني) ، جامعة يحي فارس المدية ، 15 مارس 2022، ص. 140.

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

أن تقتصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر فيهم الكفاءة العملية والحيرة الفنية في مجال الحواسيب[66]

ثالثا- اهمية المعاينة

تعد المعاينة الأداة الرئيسية في كشف غموض الجريمة والوصول إلى الأدلة التي يخلفها الجاني بمسرح الجريمة، وهي من أهم وسائل الإثبات الجزائي لأنها تعبر عن الواقعة تعبيرا صادقا يخلو من المحاباة والخداع والكذب وتتبلور هذه الأهمية في أنها تساهم في إثبات صحة وقوع الجريمة من عدمه، ومنه صحة البلاغ من عدمه، كما تقوم بتحديد الوسائل المستعملة في ارتكاب الجريمة، ومكانها وعدد مرتكبيها مما يساعد على الوصف الصحيح للجريمة من خلال الظروف المحيطة بها، بالإضافة إلى توضح كيفية دخول الجاني لمكان الجريمة وخروجه منها، وتحدد شخصية الجاني وعاداته من خلال الآثار التي يتركها بمسرح الجريمة، كما أنها تنقل للقاضي صورة واضحة عن مكان وأطراف الواقعة بالإضافة إلى أنها تساند وتعزز باقي الأدلة.[67]

ثانيا -التفتيش

التفتيش ، هو البحث في مستودع سر المتهم وهو إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته ويجب على المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني

[66] عبد النور سعيداني ، ليندة بومحراث،المرجع السابق، ص. 140.
[67] عبد القادر عميمر، اليات اثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة) ، اطروحة دكتوراة ، جامعة الجزائر 1 (بن يوسف بن خدة ، كلية الحقوق ، 2020 ،ص. 232.

بطمس معالم الجريمة وإخفاء كل ما يتعلق بها وهو يستطيع ذلك إذا اتسع له الوقت وسنحت الفرصة

والتفتيش في مدلوله القانوني بالنسبة للجرائم الالكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية فيقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها.[68]

يمكن تعريف التفتيش بانه اجراء من اجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قاننا في محل يتمتع بالحرمة بهدف الوصول الى ادلة مادية الجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها الى متهم هذا في الجرائم التقليدية لكن التساؤل يثور عندما نكون بصدد تفتيش عن حيثيات جريمة مرتكبة عبر الانترنت حول قابلية مكونات وشبكات الحاسب الآلي للتفتيش

ان التفتيش في الجرائم الرقمية (المعلوماتية يكون محله كل مكونات الحاسب الآلى سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش وتشمل جميع مكوناته المادية، والمكونات المعنوية التي تشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقا لاحتياجات العميل، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة ومهارة تقنية في نظم الحاسب الآلي كمشغلي الحاسب الآلي وخبراء البرامج ومديري النظم المعلوماتية.[69]

[68] -منير محمد الجنبيهي ،المرجع السابق، ،ص. 67.
[69] المرجع نفسه ، ص. 69.

1 – شروط التفتيش في مجال البيئة الرقمية

ا – الشروط الشكلية

وهي شروط ذات طابع شكلي تجب مراعاتها عند ممارسة هذا الإجراء حفاظا على الحريات الفردية من التعسف أو الانحراف في استخدام السلطة وهي كالآتي:

1. الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية

يعتبر هذه الإجراء من أهم الشروط الشكلية التي يتطلبها القانون في الجانب حيث أن المتهم هو الشخص الذي يستوجب القانون حضوره عند إجراء التفتيش، إذ أن الإجراء المتحد يمسه هو، غير أنه قد لا ينسى للمتهم الحضور في حال كان محل التفتيش مسكنه فمن أجل ذلك أجاز القانون له أن يجيب . غيره ليجري التفتيش في حضوره وإلا وجب استدعاء شاهدين في بعض الأحوال كما يحق للمتهم أن يستعين كمحامية عند إجراء التفتيش، ومن ثم يجيز للمحامي الحضور أيضا، كذلك إذا جرى التفتيش لدى غير المتهم وجب إتاحة الفرصة لحائز المكان في الحضور رعاية لمصالحه، ويخول المشرع للنيابة العامة أيضا حق الحضور أثناء التفتيش الذي يجريه قاضي التحقيق[70]

2 – موعد إجراء التفتيش في الجرائم الإلكترونية

اختلفت التشريعات الإجرائية في وضع مبدأ موحد يخص الميعاد الزمني للتفتيش النظم المعلوماتية، فمنها من حظر القيام بهذا الإجراء في أوقات معينة في الليل مثلا، وهنالك من قرنه بوقت معين حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المساكن،

[70] -عبد النور سعيداني ، ليندة بومحراث ، اجراءات البحث والتحري في الجرائم الالكترونية ضمن اعمال الملتقى الوطني الافتراضي حول الجرائم الالكترونية في المجتمع الجزائري تشخيص الواقع وتحديات الأمن السيبراني) ، جامعة يحي فارس المدية ، 15 مارس 2022، ص. 141.

وهنالك من تركه على مطلقه يتم في أي ساعة من ساعات الليل والنهار وترك السلطة التقديرية في ذلك للقائم أو للسلطة المكلفة بالتفتيش .

أما عن المشرع الجزائري فقد تطرق إلى هذه الجزئية من خلال نص المادة 47 من قانون ! ، ج ، ج، والتي جاء فيها: "عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب وكذا الجرائم المتعلقة بالصرف فإنه تجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.[71]

3.محضر الفيش في الجرائم الإلكترونية

باعتبار أن التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسوب والانترنت بالفقه للاستعانة به في صباغة مسودة محضر التفتيش

ب الشروط الموضوعية:

وهي الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي السبب الحمل، والسلطة المختصة بالقيام بالتفتيش

[71] -عبد النور سعيداني ، ليندة بومحراث ،نفس المرجع ،ص . 141.

-1- سبب الفيش في البيئة الإلكترونية

الورق أو الأقراص، أو على أي دعامة أخرى كالفلاش ميموري (Hash Memory)، بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم الجريمة في مرحلة المحاكمة . فالسبب هو وقوع الجريمة جناية أو جنحة، وتوفر أمارات قوية وقرائن على وجوه دليل يعيد في كشف الجريمة لدى المتهم أو غيره وهذا السبب لا ينشأ إلا بعد وقوع الجريمة، والتجاه قرائن الاقام ضد شخص، أو وجود أمارات قوية ضد آخر على حياتيه ما يقيد في كشف الحقيقة .

2 - محل التفتيش.

يشترط كذلك لصحة ومشروعية التفتيش في الجريمة الإلكترونية أن ينصب على محمل بحيث يشترط أن يكون محددا أو قابلا للتحديد ويكون مشروعا يرد على محل حائز قانونا كالمكونات المادية والمعنوية للكمبيوتر وملحقاته وبالله الهاتف الذكي وشبكات الاتصال من بعده كما نشير إلى استثناء بعض الأشخاص والأماكن من التفتيش مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية، ومكاتب المحامين لتمتعه بالحصالة، وعليه فأي تفتيش لها بعد منافيا للقانون وماله البطلان.[72]

-3- السلطة المختصة بالقيام بالتفتيش.

إن التفتيش إجراء قاصر على السلطة المختصة به وهي قاضي التحقيق والنيابة العامة، فالنيابة العامة توجه الامام وقاضي التحقيق يباشر الإجراءات بما فيها القليل، كما أنه يجوز القاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء من شأنها أن تفيد التحقيق وإظهار الحقيقة وزيادة على ذلك له الحق في إثابة أحد ضباط الشرطة القضائية

[72] -عبد النور سعيداني ، ليندة بومحراث ،المرجع السابق، ص. 142.

للقيام بهذا التفتيش بشروط حدوثها المؤد من 138 إلى 142 من في إرج (ج) إذا استحال على قاضي التحقيق تنفيذه بنفسه.[73]

4- خصائص التفتيش

يتميز التفتيش بمجموعة من الخصائص تتمثل في :

أ- الخبر والإكراه : وهذا يعني أن الإنسان يخضع له عادة بحيراً، ذلك لأن التفتيش يفترض أنه تعرض قانوني ينطوي على انتهاك الحرمة سر الإنسان أيا كان وعاؤه، وقد يكون وعاء هذا السر هو الشخص ذاته أو ملابسه أو ما معه من أمتعة، وقد يكون مسكنه وما إليه من أماكن، كما قد يكون محل التفتيش رسائل المتهم وأوراقه.

ب- المساس بحق السرية إن التفتيش بما يتضمنه بعد انتهاك فضائي لحرمة الحياة الخاصة التي تعتبر مستودعا للاحتفاظ بالأسرار، إلا أن هذا الانتهاك محسوب، بحيث لا يتجاوز القدر الأدنى واللازم تكشف الحقيقة بشأن الجرائم والتوصل إلى الجناة فيها وتوقيع الجزاء المناسب بما يحقق أهداف العقاب.

ج- البحث عن الأدلة المادية للحريمة فالتفتيش يهدف كما قلنا إلى البحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول المعلومات بشأنها، إذ الهدف من هذا الإجراء يتمثل في الحصول على أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة من أجل إثبات ارتكابها ونسبتها إلى المتهم، وهذا يعني

ومفهوم المخالفة أنه لا يجوز إجراء التفتيش للتوصل إلى ضبط جريمة مستقبلية أي لم تقع بعد أو يخشى وقوعها.[74]

---

[73] عبد النور سعيداني، المرجع السابق،ص. 142.

[74] - لدغش رحيمة ، ضوابط تفتيش الحاسب الآلي "، مجلة الحقوق والعلوم الانسانية العدد 25 ، جامعة الجلفة ،ص. 138.

5- اجراءات التفتيش

يقع التفتيش على جانبين في الجرائم الإلكترونية على الجانب المادي وعلى الجانب المعنوي، وذلك من أجل فك ملابسات الجريمة .

أ- تفتيش منظومة الحاسب الآلي المادية.

يتكون الحاسوب من كيانات مادية، تتمثل في وحدة المدخلات، ووحدة الذاكرة الرئيسية، ووحدة الحاسوب والمنطق، وجدة التحكم، وحدة المخرجات ووحدات التخزين الثانوية، وفي الوقع أغلب الجرائم المعلوماتية تقع على معدات الحاسب الآلي ، وشاشة العرض ومفاتيح تشغيلها وغيرها، وإن الولوج إلى هذا النوع من الكيانات للبحث عن شيء يفيد في كشف الحقيقة، والبحث عن مرتكبها بشأن جريمة معلوماتية وقعت يخضع الإجراءات قانونية خاصة بالتفتيش ولا يثير أية صعوبة.[75]

ب- تفتيش مكونات الحاسب الآلي المعنوية.

يقصد ما أنظمة الكمبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات ، فالبيانات والمعلومات المخزنة في الحاسب الآلي تصلح لأن تكون محلا للتفتيش، ويمكن ضبطها واستنساخها على الورق أو الأقراص، أو على أي دعامة أخرى كالفلاش ميموري (Hash Memory)، بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم الجريمة في مرحلة المحاكمة .[76]

---

[75] -عبد النور سعيداني ، ليندة بومحراث ،المرجع السابق،،ص. 142.
[76] -نفس المرجع ،ص. 143.

الفرع الثاني : اجراء الحجز

في التشريع الجزائري نجد الحجز في الجريمة الالكترونية مؤطر بنص المادة السادسة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها التي تنص على أنه عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها ، وأنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين الالكترونية ، تكون قابلة للحجز ، ووضع في احراز وفقا للقواعد المقررة في القانون الاجراءات الجزائرية .

1 - تعريف الحجز الإلكتروني:

يعرف الحجز بأنه العثور على أدلة الخاصة بالجريمة التي تباشر التحقيق بشأنها والحفظ هذه الادلة ، والضبط هو الغاية من التفتيش و النتيجة المباشرة المستهدفة ولذلك عند اجرائه أن تتوفر فيه القواعد نفسها التي تنطبق بشأن التفتيش و يؤدي بطلان التفتيش الى بطلان الضبط وعليه يمثل محل الضبط في الجرائم الكترونية جدلا بين فقهاء القانون وانقسموا الى اتجاهين ، الاتجاه الأول يرى انصاره عدم ضبط المعلومات المعالجة في مجال الافتراضي الا بعد نقلها على كيان مادي ملموس اما تصوريا أو بواسطة دعائم التخزين الالكتروني أما الاتجاه الثاني يرى اتباعه عدم انكار المادي للمعلومات المعالجة الكترونيا لأنها قابلة للتسجيل والحفظ والتخزين[77]

-2- آليات الحجز المعلوماتي للمعطيات

[77] فلاح عبد القادر ، حجز وحفظ المعطيات في الجريمة الالكترونية ، مجلة صوت القانون ، المجلد الثامن ، العدد 1، 2021 ، ص. 180.

حجز المعطيات المعلوماتية عن طريق النسخ: تتم هذه العملية عن طريق أخذ نسخة من البيانات الالكترونية باستخدام برامج خاصة تفي بهذا الغرض، وقد نص القانون 0409 على هذا الإجراء في المادة السادسة منه التي جاء فيها عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وهذا الإجراء استحدثه المشرع الجزائري تماشيا مع ما جاءت به المادة التاسعة عشر من القسم الرابع من اتفاقية بودابيست التي جاء فيها: على سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة، وهو ما أخذ به المشرع الفرنسي في الفقرة الثالثة من المادة 1/157 من قانون الأمن الداخلي رقم 239 لسنة 2003 التي جاء فيها أن المعطيات التي يتم الحصول عليها في ظل الشروط المنصوص عليها في المادة السابقة، يتعين نسخها على دعامات، ثم يتم تحريز هذه الدعامات المعلوماتية في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون.[78]

3-الحجز عن طريق منع الوصول إلى المعطيات

يتم منع الوصول إلى المعطيات العملية بتجميد التعامل مع الحاسوب أو الجزء الذي استخدم في ارتكاب الجريمة، ويتم ذلك عن طريق ضغط محتويات القرص الصلب ونقل تلك المحتويات إلى أقراص صلبة أو ممغنطة ويستعمل هذا الإجراء في مواجهة الحاسبات الخادمة التي تحتوي مواقع الدعارة ، أو مواقع الهكر ، أو ملفات فيروسية، كما تستخدم في حالة احتواء القرص الصلب على ملفات مشفرة وتحتاج إلى فك شفرتها وقد كرس المشرع

[78] -عبد القادر عميمر, المرجع السابق ,ص. 302.

الجزائري هذا الإجراء في المادة السابعة من القانون 09-04 التي جاء فيها :" إذا استحال إجراء الحجز وفقا لما منصوص عليه في المادة 06 أعلاه الأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[79]

الفرع الثالث: مراقبة الاتصالات والالتزامات القانونية لمقدمي خدمات الإنترنت

اولا : مراقبة الاتصالات:

الجزائر أضفت حماية قانونية للبيانات الشخصية من خلال الدستور، حيث يضمن الدستور حقوق الأفراد في احترام حياتهم الخاصة وبياناتهم الشخصية. تنص المادة 77 على أن لكل فرد حرية ممارسة حقوقه، مع احترام حقوق الآخرين، بينما تؤكد المادة 46 أهمية حماية حرمة الحياة وخصوصية المراسلات والاتصالات. التعديلات الدستورية في 2016 ضمنت عدم المساس بهذه الحقوق إلا بأمر من السلطة القضائية، مع عقوبات على المخالفات.

هذه التعديلات تعكس التزام المشرع الجزائري بحماية البيانات الشخصية، وينتظر إصدار قانون خاص عن حماية البيانات قريباً بعد أن بدأت الوزارة المخصصة في نوفمبر 2014 بمشروعه الجزائر تعد الوحيدة بين الدول العربية التي تطرقت إلى حماية البيانات الشخصية في دستورها، بينما اقتصرت الدساتير الأخرى على حماية المراسلات.السلطة القضائية يمكنها فرض مراقبة الاتصالات الشخصية في حالات محددة، مثل مكافحة الجرائم الإرهابية أو لحماية أمن الدولة. هذه المراقبة الإلكترونية تعتبر وسيلة فعالة ومكلفة أقل، لكنها تكشف بيانات حساسة قد تنتهك خصوصية الأفراد. وقد وضع المشرع ضمانات لحصر الحالات

[79] -عبد القادر عميمر, المرجع السابق، ص. 302.

التي يمكن فيها اللجوء إلى المراقبة الإلكترونية، مما يسعى للتوازن بين الأمن وحماية الحياة الخاصة وهذه الحالات هي :

للوقاية من أفعال الإرهاب أو التخريب، يجب اتخاذ إجراءات عند توفر معلومات عن احتمال الاعتداء على نظم معلوماتية تهدد النظام العام أو الاقتصاد التحريات قد تحتاج إلى مراقبة الكترونية عندما تكون النتائج صعبة. المشرع الجزائري يسعى للاستفادة من التكنولوجيا بمراقبة المشتهين إلكترونياً، وهو أقل تكلفة وأكثر فعالية، ولكنه قد ينتهك الخصوصية.[80] لضمان حماية الحياة الخاصة، وضع المشرع ضمانات لتخفيف التأثيرات السلبية وتتمثل هذه الضمانات في :

1 حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية

هي الحالات التي أوضحتها المادة الرابعة من القانون ٠٤. على سبيل الحصر.

ا – للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

ج – المقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية

د– في إطار تنفيذ المساعدة القضائية الدولية المتبادلة .

[80] -رضا بوعافية ، اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية " ، ضمن اعمال الملتقى الوطني الافتراضي ، حول الجرائم الالكترونية في المجتمع الجزائري (تشخيص الواقع و تحديات الأمن السيبراني) ، جامعة يحي فارس المدية ، 15 مارس 2022، ص ، ص. 110- 111.

باستقراء الحالات هذه تجد أن الشرع في لص من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة" ج" والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.[81]

2- وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء

تضيف المادة 4/2 من القانون ٠٤٠ بأنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطات القضائية المختصة

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها ".

كما تنص المادة 41 من المرسوم الرئاسي رقم ٢٦٥/٩ المؤرخ في 10 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص

[81] -امحمدي بوزينة امنة اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لاحكام قانون الاجراءات الجزائية وقانون الوقاية من جرائم الاعلام) ، ضمن الملتقى الوطني ، اليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة ، 29 مارس2017، ص. 74.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسر المهني المادتين 27 و 28 المرسوم الرئاسية (٢٦/٨)

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانة حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق والزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد محرما، وهذا ما يسمى ضمانات المحاكمة العادلة[82]

3- تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في اعتراض المراسلات الإلكترونية"، تسجيل الأصوات النقاط الصور"، تقليش المنظومات المعلوماتية وحجزها المادة 5 و 7 من القانون ٠٤٠٩. إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها ؟

أجابت المادة 100 من القانون ٤٠ المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية

[82] -امحمدي بوزينة امنة, المرجع السابق ، ص. 75.

يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.[83]

4- سن عقوبات الجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة الأغراض شخصية، أو كل تجاوز الحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك[84]

ثانيا : التزامات مقدمي الانترانت

اولا : مفهوم مقدمي الانترانت

1 - تعريف مقدمي الخدمات

عرفت (إ.أ.م.إ.م) مقدمي الخدمات بموجب المادة (01/ج) التي تنص على: يقصد بمزودي الخدمات أي كيان عام أو خاص الذي يوفر المستخدميه القدرة على التواصل من خلال النظام المعلوماتي.

[83] امحمدي بوزينة امنة،المرجع السابق، ص. 75.
[84] المرجع انفسه، ص. 76.

أي كيان آخر يقوم بمعالجة أو تخزين البيانات الحاسوبية لخدمة الاتصالات أو الخدمة مستخدميه،وهو التعريف نفسه الذي خص به المشرع الجزائري مقدمي الخدمات بموجب المادة (202) من القانون رقم : 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها التي تنص على يقصد في مفهوم هذا القانون ما يأتي.[85]

د- مقدمو الخدمات

أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام اتصالات.

وأي كيان اخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

Internet Service Provider(هو اختصار لكلمة (ISP إن مزود خدمة الإنترنت ويسمى أيضا بموفر خدمة الاتصال بالإنترنت (AIP) هي الشركة التي توفر لعملائها إمكانية الوصول إلى الإنترنت ويرتبط مزود خدمة الإنترنت بعملائه باستخدام تقنية نقل البيانات المناسبة التوصيل حزم بيانات نظام الإنترنت مثل الاتصال الهاتفي خط المشترك الرقمي للاتصال (DSL) كابل المودم الاسلكية الوصلات المخصصة عالية السرعة .... إلخ. إن مزود خدمة الإنترنت قد يوفر حسابات البريد الإلكتروني للمستخدمين، والتي تسمح لهم بالتواصل مع بعضهم البعض عن طريق إرسال واستقبال الرسائل الإلكترونية من خلال خادم (server) مزود خدمة الإنترنت وكجزء من خدمة البريد الإلكتروني عادة ما يوفر مزود خدمات الإنترنت للمستخدم وعميل البريد الإلكتروني حزمة البرامج التي طورت داخليا

[85] - يزيد بوحليط ، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات قانون الاجراءات الجزائية ، دار الجامعة الجديدة ، 2019،ص. 317.

أو من خلال ترتيب عقد خارجي، كما يمكن المقدمي خدمات الإنترنت توفير خدمات أخرى مثل تخزين البيانات عن بعد نيابة عن عملائها[86]

2 – تعريف مقدمي خدمة الانترانت

تطرقنا سابقا إلى مفهوم مقدمي الخدمات وهو التعريف الذي جاء به نص المادة (102) من القانون رقم : 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على يقصد في مفهوم هذا القانون ما يأتي .

مقدمو الخدمات

أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات.

وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها". وعليه يدخل ضمن هذا التعريف مقدمو خدمة النفاذ الشبكة الإنترنت (Internet Service Provider)، حيث تتعدد طرق النفاذ إلى شبكة الإنترنت مثل خط اشتراك رقمي غير متماثل (ADSL) الخ، إلا أنه في كل الأحول يجب وجود مقدم خدمة الإنترنت (Intermet Service Provider) الذي يعرف على أنه الشركة التي تستضيف مواقع الإنترنت على خوادمها (Servers) حيث يكون مقدم الخدمة مؤجرا وصاحب الموقع مستأجرا ويسمى أيضا بموفر خدمة الاتصال بالإنترنت (AP) ، وهي الشركة التي توفر لعملاتها إمكانية الوصول إلى الإنترنت ويرتبط مزود خدمة الإنترنت بعملاته باستخدام تقنية

[86] يزيد بوحليط، المرجع السابق ،ص. 317.

نقل البيانات المناسبة لتوصيل حزم بيانات نظام الانترنت مثل الاتصال الهاتفي، كابل المودم..... إلخ . كما أن مزودي خدمة الإنترنت لا يجبرون على مراقبة المحتوى.[87]

من جهة أخرى، يوفر مزود خدمة الإنترنت حسابات البريد الإلكتروني المستخدمين، والتي تسمح لهم بالتواصل مع بعضهم البعض عن طريق إرسال واستقبال الرسائل الإلكترونية من خلال خاتم (server) مزود خدمة الإنترنت وكجزء من خدمة البريد الإلكتروني عادة ما يوفر مزود خدمات الإنترنت للمستخدم وعميل البريد الإلكتروني حزمة البرامج، كما يمكن توفير خدمات أخرى مثل تخزين المعطيات عن بعد نيابة عن زبائنها.[88]

2 – التزامات مقدمي خدمة الانترانت ومسؤولياتهم

فرض المشرع الجزائري التزامات على عاتق مزودي خدمة الإنترنت، ينجر عنها تحمل مسؤوليتهم في حال الإخلال بها، وذلك نظرا لحساسية هذا القطاع بالنسبة للدولة والمواطن على حد سواء، وما يشكله أيضا من بيئة خصبة لانتشار الجرائم الإلكترونية

اولا : التزامات مقدمي خدمة الانترانت

في إطار تنظيم المشرع الجزائري لخدمة الإنترنت في الجزائر، أخضع مزود و هذه الخدمة لعدة التزامات ضمانا لتقديم أحسن الخدمات وحفاظا على المجتمع من أخطار الإنترنت في هذا الصدد نصت المادة (14) من المرسوم التنفيذي رقم : 257-98 المؤرخ في 1998/08/25 يضبط شروط وكيفيات إقامة خدمات إنترانت واستغلالها على يلتزم مقدم خدمة إنترانت خلال ممارسة نشاطه بما يأتي:

تسهيل النفاذ إلى خدمات إنترانت حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجع الوسائل التقنية المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه

[87] يزيد بوحليط ،المرجع السابق،ص.324
[88] المرجع نفسه، ص. 324.

الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات إنترانت" ومساعدتهم كلما طلبوا ذلك عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أية طريقة غير مشروعة سواء اتجاه المستخدمين أو اتجاه مقدمي خدمات إنترانت" الآخرين تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها طبقا للأحكام التشريعية المعمول بها اتخاذ كل الاجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق.

وفي المجال نفسه، وإضافة للالتزامات السابق ذكرها بموجب نص المادة (14)، نصت المادة (11) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على مجموعة أخرى من الالتزامات، حيث تنص على مع مراعات طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ

ا- المعطيات التي تسمح بالتعرف على مستعملي الخدمة

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال

ج -الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ - المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها .[89]

[89] قانون رقم 04-09 المؤرخ في 5 أغسطس 2009 متضمن قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا العلم والاتصال ومكافحتها الصادرة ب 5اغسطس 2009 ج،ر،ج،ج العدد 47 سنة 2009

من جهة أخرى، حدد المشرع مدة حفظ المعطيات بسنة واحدة، وذلك بموجب نص المادة (7/11) من القانون 04-09 التي تنص على تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل قصد إعطاء الوقت اللازم لأجهزة البحث والتحري للرجوع إلى هذه المعطيات في حال الحاجة إليها.

ونظرا لأهمية هذا الفضاء الافتراضي فلمزودي خدمة الإنترنت مسؤولية كبيرة في الحد من المخاطر التي تعترض شبكة الإنترنت، لذا يجب عليهم اتباع سياسة تأمينية علمية لحماية أنظمة المعلومات من قبل مخترقي الأنظمة مثل تنظيم عمليات دخول مستخدمي النظام وتأمين الشبكة الداخلية والخارجية وتأمين التطبيقات وقواعد البيانات المستخدمة ... إلخ).

من جهة ثانية أضاف المشرع الجزائري التزامات أخرى بموجب نص المادة (12) من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص على زيادة على الالتزامات المنصوص عليها في المادة (11) أعلاه، يتعين على مقدمي خدمات الإنترنت ما ياتي:[90]

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

ب - وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها .

وعليه يلعب مزود خدمة الإنترنت دورا فعالا في مساعدة السلطات القضائية المكلفة بالتحريات والتحقيقات في ضبط الدليل الرقمي لإدانة المتهم، إذ يمكن عن طريق برامج متخصصة مثل برنامج (Carnivore) سبق التطرق إليه الوصول إلى الفاعل عن طريق

[90] يزيد بوحليط ، المرجع السابق، ص337.

تتبع خطواته عبر شبكة الإنترنت كما يقوم بدور وقائي قبل وقوع الجريمة، وذلك من خلال وضع ترتيبات تقنية تسمح بتوفير حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق حماية للمجتمع من الجرائم الإلكترونية.[91]

ثانيا : مسؤوليات مقدمي خدمة الانترانت

1 – المسؤولية العقدية لمزودي خدمات الانترانت

بمجرد ابرام العقد بين المشترك ومقدم خدمات الإنترنت ، يلتزم هذا الأخير بتخزين المادة المعلوماتية وإيصالها إلى مستخدمي الشبكة عن طريق تزويدهم بالوسائل الفنية التي تسمح بذلك، وبالمقابل يلتزم مستخدمو الشبكة والمستفيدون من هذه الخدمات بتأدية ما ترتب في ذمتهم من استحقاقات مالية، وكذلك باحترام القوانين والأنظمة السارية والأعراف، وقواعد السلوك الثابتة في هذا المجال فتثور المسؤولية العقدية لمزود خدمات الإنترنت في حال إخلاله بالتزامه بتقديم تلك الخدمة، حيث يحق لكل مشترك الحصول على خدمة الإنترنت المتعاقد عليه ، ففي حالة عدم تمكنه من الإتصال بالشبكة ، أو عدم وصوله إلى المادة المعلوماتية المطلوبة لأي سبب كان، تطبق مباشرة قواعد المسؤولية العقدية على مقدم الخدمة.

المقدم الخدمة يبذل في ذلك عناية الشخص العادي بمعنى أنه لا تطبق عليه قواعد المسؤولية العقدية إلا في حالة إخلاله ببنود العقد بسبب خطأ جسيم أو غش من جانبه[92]

[91] يزيد بوحليط المرجع السابق ،ص.337.

[92] مصطفي هنشور وسيمة ، النظام القانوني لمقدمي خدمات الانترانت في التشريع الجزائري ، مجلة البحوث القانونية والسياسية ، العدد الخامس ديسمبر 2015، ص. 136.

-2- المسؤولية الجزائية لمقدمي خدمات الإنترنت

لقد تناول المشرع الجزائري المسؤولية الجنائية المزودي خدمات الإنترنت في القانون 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، إذ تقوم هذه المسؤولية في حالة إفشاء أسرار التحري والتحقيق أو في حالة عدم حفظ المعطيات المتعلقة بحركة السير.

ا - جريمة إفشاء أسرار التحري والتحقيق

تقوم هذه الجريمة وفقا لنص المادة 10 فقرة 2 من القانون 09-04 في حالة عدم التزام مقدم خدمات الإنترنت بكتمان سرية المعلومات والعمليات التي يقوم بها بطلب من المحققين ، وذلك بنقلها وإذاعتها وإطلاع الغير عليها إذ تقوم مسؤوليته الجنائية في هذه الحالة بصفته مؤتمن على أسرار البحث والتحقيق.وتجب الإشارة إلى أن المشرع الجزائري لم يحدد عقوبة هذه الجريمة في القانون 09-04، بل أحال إلى المادة 301 من قانون العقوبات المخصصة لجرائم الإفشاء فيما يتعلق بالأشخاص الطبيعية أما بخصوص الشخص المعنوي فقد أشار إليه في المادة 303 مكرر 3 من قانون العقوبات.

ب - جريمة عدم حفظ المعطيات المتعلقة بحركة السير

أشار إليها المشرع الجزائري وفقا لمقتضيات المادة 11 فقرة من القانون رقم 09-04 ، بحيث تتمثل هذه الجريمة في عدم حفظ المعطيات المتعلقة بحركة السير ، أو عدم حفظها في المدة القانونية وتكمن هذه المعطيات في المعطيات التي تسمح بالتعرف على مستعملي الخدمة.[93]

[93] مصطفي هنشور وسيمة، المرجع السابق،ص. ص. 136- 137

المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال ، وكذا عناوين المواقع المطلع عليها .

على أن يؤدي عدم حفظ تلك المعطيات إلى عرقلة وتعطيل حسن سير التحريات القضائية، ويحدد هذا الحفظ لمدة سنة واحدة من تاريخ التسجيل. وقد حددت العقوبات المترتبة على عدم حفظ هذه المعطيات في الفقرة الرابعة من نفس المادة.[94]

المطلب الثاني: الاجراءات المستحدثة في مكافحة الجرائم المعلوماتية

تسمى هذه الإجراءات عادة بـ أساليب التحري الخاصة، وقد استحدثها المشرع الجزائري على إثر تعديله لقانون الإجراءات الجزائية، بموجب القانون رقم 05-22 المؤرخ في 20 ديسمبر 2006 المعدل لقانون الإجراءات الجزائية، تماشيا مع التطور المتسارع الذي تعرفه الجريمة في مجتمعنا، وفي إطار المكافحة الإجرائية لهذا النوع من الإجرام .

الفرع الاول:الكشف بواسطة اسلوب اعتراض المراسلات وتسجيل الصوت والصور

1 – مفهوم اعتراض المراسلات وتسجيل الصوت و التقاط الصور

يقصد باعتراض المراسلات عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه في ارتكابهم للجريمة أو مشاركتهم فيها. ويطلق على هذا الإجراء تسميات أخرى في الفقه

[94] -مصطفي هنشور وسيمة ، المرجع السابق،ص ،ص . 137 - 138

كمصطلح التنصت interception des) واعتراض المكالمات الهاتفية écoutes téléphoniques الهاتفي conversations téléphoniques)

ويقصد بتسجيل الأصوات مراقبة المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة، وفي مكان عام أو خاص، عن طريق التقاطها أو نقلها أو تسجيلها، أو أنه الاستماع خلسة للأحاديث دون علم صاحبها، بواسطة أجهزة إلكترونية.

كما يقصد بالتقاط الصور القيام بالتصوير الخفي لشخص أو عدة أشخاص يتواجدون في مكان خاص، كوضع ميكروفون في منزل المتهم أو مكتبه أو سيارته أو أي مكان يتردد عليه المشتبه فيه وحتى باستعمال التلفون المحمول الذي باستطاعته تسجيل الصوت والصورة على نحو متناه في الدقة.[95]

2- **إجراءات اعتراض المراسلات نتناولها وفق التقسيم الآتي:**

-1- تحديد مجال اعتراض المراسلات نصت المادة (65) مكرر (5) من (ق.إ. ج. ج) على الجرائم التي يجوز

القيام فيها بهذه العملية وهي:

- جرائم المخدرات.

الجريمة المنظمة العابرة للحدود الوطنية.

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جرائم تبييض الأموال.

---

[95] بطيحي نسمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية مطبوعة مقدمة لطلبة السنة الثانية ماستر ، تخصص إدارة الكترونية وخدمات رقمية، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين- سطيف 2، السنة الجامعية 2021/2022، ص ،ص. 15- 16.

- جرائم الإرهاب.

الجرائم المتعلقة بالتشريع الخاص بالصرف وهو الأمر رقم 96-22 المؤرخ في 1996/07/09

المتمم والمعدل بالأمر رقم : 03-01 المؤرخ في : 2003/02/19

جرائم الفساد المحددة بالقانون رقم : 06-01 المؤرخ في 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته.

-- الجهة القضائية التي يجوز لها بمنح الإذن للقيام بهذه العملية : حسب ما ورد في نص المادة (65) مكرر (5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

وكيل الجمهورية : يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة له.

- **قاضي التحقيق** : في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65) مكرر (05) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65) مكرر (6/5).[96]

2- **الأماكن التي يسمح فيها بالاعتراض:** لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية الاعتراض، بل جاء النص على عمومه، حيث نصت المادة (65) مكرر (05) على ... في أماكن خاصة أو عمومية .... دون استثناء فقد يكون منزلا أو مقهى للإنترنت أو شركة ... الخ مخالفا في ذلك المشرع الفرنسي الذي أورد استثناءات في هذا الشأن بموجب المادة (96706) من (ق.إ.ج.ف) مثل المحلات التي تحتوي على مؤسسات

[96] المادة 65 مكرر 5 من القانون رقم06-01 المؤرخ في 20 فيفري2006، المتعلق بالوقاية من الفساد ومكافحته، التي تجيز التقاط الصور في جرائم معينة كالمخدرات والإرهاب والفساد ، بشرط الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق، الجريدة الرسمية عدد 14 الصادرة بتاريخ 8 مارس 2006

إعلامية والمحلات ذات الطابع المهني للأطباء وسيارات النواب والمحامين ... إلخ (1). حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن ووضع الوسائل اللازمة لاعتراض المراسلات حتى بغير علم وموافقة أصحابها وحتى خارج الأجال المنصوص عليها في المادة (47) من (ق.إ . ج. ج) (1) بمعنى أنها تكون في أي وقت.[97]

3 **مضمون الإذن ومدته** : يتضمن الإذن المذكور في المادة (65) مكرر (5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء كانت سكنية أو غيرها، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65) مكرر (7) على يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

من خلال هذه المادة يمكن أن نستشف الشروط الشكلية والزمنية للإذن وهي :

أن يكون الإذن مكتوبا.

ذكر جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة، وذلك بالتحديد الدقيق للاتصال المراد مراقبته أو المراسلة التي سيتم اعتراضها وكذا المكان الذي يتم فيه وضع الترتيبات التقنية.

[97] - يزيد بوحليط ، المرجع السابق ، ص . 258.

– ذكر الجريمة التي تبرر اللجوء إلى هذه العملية وهي إحدى الجرائم المذكورة على سبيل الحصر في نص)المادة (65 مكرر (5) من (ق. إ. ج. ج

– ذكر المدة التي تتم خلالها العملية على ألا تتجاوز مدة أربعة (4) أشهر قابلة للتجديد بالشروط نفسها.[98]

4– كيف تتم العملية : يتم اعتراض المراسلات بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65) مكرر (8). يفرض على ضابط الشرطة القضائية المأذون له أو المناب من القاضي المختص، تحرير محضر لكل عملية اعتراض أو تسجيل مراسلات، بما في ذلك تفاصيل الترتيبات التقنية والالتقاط مع تحديد تاريخ وساعة بداية ونهاية العملية، وفقا للمادتين 65 مكرر و 65 مكرر 10 من قانون الإجراءات الجزائية، مع احترام السر المهني حسب المادة 45، واتخاذ التدابير المنصوص عليها في المادة 65 مكرر 6.

ويُعتبر البريد الإلكتروني وسيلة حديثة وفعالة للاتصال، لكنه يستغل أحيانا من قبل المجرمين، مما يجعله خاضعًا لعملية الاعتراض للكشف عن الجرائم الإلكترونية. ورغم أن هذا الإجراء يعد مساسا بالحياة الخاصة إلا أن المشرع أجازه استثناء لتحقيق الحقيقة، حيث يمكن لضباط الشرطة القضائية اعتراض هذه المراسلات عن بعد باستخدام وسائل تقنية متطورة لاستخلاص الأدلة الرقمية.[99]

3– اجراءات تسجيل الصوت : ويتم ذلك كما الآتي :

[98]- يزيد بوحليط ،المرجع السابق ، ص ،ص. 258- 259.
[99] المرجع نفسه،ص.ص. 259- 260.

-1- تحديد مجال تسجيل الأصوات نصت المادة 65 مكرر (5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي جرائم المخدرات الجريمة المنظمة العابرة للحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... إلخ.

2 منح الإذن للقيام بهذه العملية حسن ما ورد في نص المادة 65 مكرر (5) فإن منح

الإذن للقيام بهذه العمليات مقتصر على كل من:

- **وكيل الجمهورية** : يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها تحت مراقبته المباشرة.

- **قاضي التحقيق** : في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65 مكرر (5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65) مكرر (6/5) من(ق. إ . ج. ج)

-- أماكن تسجيل الأصوات لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية تسجيل الأصوات بل جاء النص على عمومه، حيث نصت المادة (65) مكرر (5) على ..... في أماكن خاصة أو عمومية . حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن ووضع الوسائل اللازمة لتسجيل الأصوات كتركيب الميكروفونات حتى بغير علم وموافقة أصحابها وحتى خارج الأجال المنصوص عليها في المادة (47) من(ق.إ. ج. ج)[100]

4 **مضمون الإذن ومدته** : يتضمن الإذن المذكور في المادة (65 مكرر (5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم، وكذا الأماكن المقصودة سواء كانت عامة أو خاصة وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص

[100] - يزيد بوحليط ، المرجع السابق ، ص. 263

المادة (65) مكرر (7) على يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

-5- كيف تتم العملية: تتم عملية تسجيل الأصوات بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر 8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية الماذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية تسجيل الأصوات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها.[101]

4- **إجراءات التقاط الصور** : نتطرق إليها كما يأتي:

أولا: تحديد مجال التقاط الصور : نصت المادة (65) مكرر (5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي:

- جرائم المخدرات .

- الجريمة المنظمة العابرة للحدود الوطنية

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جرائم تبييض الأموال. جرائم الإرهاب.

[101] - يزيد بوحليط ،المرجع السابق، ص. 263.

– الجرائم المتعلقة بالتشريع الخاص بالصرف.

– جرائم الفساد.

ثانيا : منح الإذن للقيام بهذه العملية : حسب ما ورد في نص المادة (65 مكرر (5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:[102]

– **وكيل الجمهورية** : يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس وتحت المراقبة المباشرة له.

– **قاضي التحقيق:** في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65 مكرر (5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65) مكرر (65)

–**أماكن التقاط الصور:** على خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة استثنى المشرع الجزائري التقاط الصور في الأماكن العمومية، غير أنه سمح بهذا التدبير في بعض القوانين الخاصة كالترصد الإلكتروني والاختراق بموجب المادة (56) من القانون 06–01 المتعلق بالوقاية من الفساد ومكافحته

ثالثا: مضمون الإذن ومدته: يتضمن الإذن المذكور في المادة (65 مكرر (5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط الصور لهم والأماكن المقصودة سواء كانت عامة أو خاصة، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65) مكرر

[102] يزيد بوحليط المرجع السابق ،ص. 265.

(7) على ... يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.[103]

رابعا: كيف تتم العملية : تتم عملية التقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65) مكرر (8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية التقاط الصور، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها، وهذا بموجب المادتين (9-10) من (ق .إ.ج.ج).[104]

الفرع الثاني : أسلوب التسرب

1 - **مفهوم التسرب :**

أ- التعريف الفقهي للتسرب

حاول العديد من الفقهاء وضع تعريف لإجراء التسرب، ولعلى أرجح التعريفات الفقهية هو التعريف الذي يعرف لنا التسرب بأنه : " تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل الجماعة الإجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة الأشخاص المشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية ويظهر كأنه الفاعل أو الشريك

ب- تعريف التسرب في القانون الجزائري

[103] يزيد بوحليط. المرجع السابق، ص. 266
[104] المرجع نفسه، ص. 266.

عرف لنا المشرع الجزائري إجراء التسرب في المادة 65 مكرر 12 من قانون الإجراءات الجزائية، وتنص هذه المادة

على أنه : " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.[105]

2 – شروط التسرب

يشترط قانون الإجراءات الجزائية للقيام بهذه العمليات الشروط الآتية :

ا – الشروط الشكلية

يستوجب قانون الإجراءات الجزائية شروط شكلية يجب مراعاتها عند ممارسة التسرب صونا للحريات الفردية من التعسف أو الانحراف في استخدام السلطة ، كالأتي :

1 **الإذن القضائي** : .جعل المشرع الجزائري بموجب المادة 65 مكرر 11 من ق إ،ج،ج الاختصاص بالإذن بإجراء التسرب الوكيل الجمهورية، وفي حالة فتح تحقيق قضائي يتم التسرب بناءً على إذن من قاضي التحقيق وتحت مراقبته المباشرة بعد إخطار وكيل الجمهورية .[106]

ويمكن تعريف الإذن بأنه عبارة عن تفويض يصدر من السلطة المختصة إلى احد ضباط الشرطة القضائية محولا إياه إجراء عملية التسرب .. أو هو أيضا محرر رسمي صادر من

[105] - تركية صيافة ، اسلوب التسرب في القانون الجزائري ، مجلة الدراسات القانونية والسياسية ، المجلد 09, العدد 02 . جوان 2023 ، ص. 272.

[106] - صالح شنين، التسرب في قانون الاجراءات الجنائية الجزائري حماية للنظام العام والحريات ام حماية للنظام العام ، المجلة الجزائرية للقانون المقارن،العدد 2،ص. 123.

جهة مختصة هي وكيل الجمهورية أو قاضي التحقيق مسلم إلى ضابط الشرطة القضائية ويشترط القانون بالمواد 65 مكرر 15 من ق إ. ج ج. في الإذن الشروط التالية ::

أن يكون مكتوبا تحت طائلة البطلان ، ذلك أن الأصل في العمل الإجرائي الكتابة ، وهو إجراء شكلي اشترطه المشرع في نص المادة 65 مكرر 15 . أن يكون الإذن مسببا ، إذ يعتبر التسبيب أساس العمل القضائي، ومن ثم كان لزاما عند إصدار الإذن بإجراء التسرب سواء من طرف وكيل الجمهورية أو قاضي التحقيق ، إظهار الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية .

أن يسلم لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري، أو التحقيق

ضمن نفس الشروط الشكلية والزمنة،يجب أن تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة

القضائية الذي تتم العملية تحت مسؤوليته .

يجب أن تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

أن يكون مصدره مختصا نوعيا ومكانيا أصلا بالبحث أو التحقيق في الجريمة التي صدر الإذن بشأنها، ووفقا للقواعد العامة يتحدد الاختصاص النوعي بحسب نوعية الجريمة ، أما الاختصاص المكاني بمحل الواقعة، أو ضبط المتهم، أو محل إقامته.[107]

2 – **تقرير عملية التسرب :**

[107] - صالح شنين ، المرجع السابق ،ص . 124.

استوجب المشرع الجزائري في المادة 65 مكرر 13 على ضابط الشرطة القضائية المكلف بتنسيق العملية أن يحرر تقريرا، يتضمن كل العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط أو

العون المتسرب، وكذا الأشخاص المسخرين طبقا للمادة 65 مكرر 14 .

ولا يكون لهذه المحاضر قوة في الإثبات إلا إذا كانت صحيحة في الشكل طبقا للمادة 214 والأدلة الواردة بها لها حجة نسبية أي صحيحة ما لم يقدم ما يخالفها على خلاف الأدلة الواردة بالمحاضر المنصوص عليها بالمادة 216 من قانون الإجراءات الجنائية ...

3 – الجهة المختصة بالقيام بعملية التسرب :وفقا للمادة 65 مكرر 12 يقوم بعملية التسرب ضابط الشرطة القضائية أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية .

كما يقوم بها الأشخاص المسخرين لهذا الغرض من قبل ضابط الشرطة القضائية المكلف بتنسيق العملية حسب المادة 65 مكرر 14 ...[108]

ب–الشروط الموضوعية:

بالإضافة إلى الشروط الشكلية يشترط القانون الشروط الموضوعية الآتية :

1 سبب التسرب :

نظرا لخطورة عملية الترب. فإن المشرع قرر في المادة 65 مكرر 11 أنه لا يجوز لوكيل الجمهورية أو قاضي التحقيق اللجوء إليه إلا إذا دعت الضرورة الملحة للتحري والتحقيق

[108] صالح شنين، المرجع السابق ، ص. 125.

ضمن الشروط المبينة في القانون ، وفي نطاق الجرائم المحددة حصرا في المادة 65 مكرر 15 من قانون الإجراءات الجنائية ..

وعليه فيجب على ضابط الشرطة القضائية أن يؤسس طلبه بالإذن بعملية التسرب على عدد من المبررات والحيثيات، من أجل إقناعهم بمنح الإذن الإجراء هذه العملية .

2 **نوعية الجرائم :**

حولت المادة 65 مكرر 11 من ق.إ.ج.ج لوكيل الجمهورية أو قاضي التحقيق عند ضرورة التحري أو التحقيق الإذن بإجراء عملية التسرب في الجرائم المنصوص عليها في المادة 65 مكرر 5 . وهي جرائم المخدرات أو الجريمة المنظمة العابرة للحدود أو الجرائم الماسة بأنظمة المعالجة الآلية المعطيات أو جرائم تبييض الأموال أو الإرهاب، أو جرائم الصرف أو جرائم الفساد .

وتجدر الإشارة إلى انه يترتب على تخلف احد شروط التسرب بطلان الإجراء وعدم الاعتماد بما قد ينتج عنه من دليل جنائي .[109]

[109] - صالح شنين, المرجع السابق،ص . 126.

خلاصة الفصل:

تُعد الوقاية البعدية من الجريمة الإلكترونية استجابة ضرورية لما قد يقع من اعتداءات رقمية رغم كل الجهود الوقائية القبلية، فهي تمثل مرحلة تدخل مؤسسات الدولة المختلفة لملاحقة الجريمة بعد تحققها، والتقليل من آثارها، والحد من تكرارها.

وقد تبيّن أن التشريع الجزائري قد أولى أهمية خاصة لهذا الجانب، من خلال تسخير آليات مؤسساتية وتشريعية متعددة، أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والأجهزة الأمنية المكلفة بالتحري والتحقيق. كما ظهرت جملة من الإجراءات القانونية الميدانية، كتفتيش ومعاينة مسرح الجريمة الإلكترونية، الحجز، وتتبع المراسلات الإلكترونية، وتسجيل الأصوات، واعتماد أسلوب التسرب، وهي تدابير تهدف جميعها إلى تعزيز فعالية الكشف عن الجريمة المعلوماتية.

خاتمة

خاتمة:

تبقى الحماية الفنية والتقنية مهما بلغت درجتها عاجزة عن التطور الرهيب الذي تشهده تقنيات اختراق الأجهزة الإلكترونية لاسيما الحواسيب، وهو ما أدى إلى استفحال الجريمة الإلكترونية وتسبب في أضرار مادية ومالية وحتى نفسية للعديد من الضحايا.

تبين لنا من خلال هذه الدراسة مدى خطورة الجرائم الإلكترونية وصعوبة اكتشافها، حيث وقفت مختلف النظم القانونية عاجزة عن مكافحتها، نظرا للعد الهائل من هذه الجرائم المتزايدة بشكل غير مسبوق.

كما أن الجهود الوطنية والدولية لمكافحة الجرائم الالكترونية لا تزال في بداياتها الأولى. ولا ترقى إلى المستوى المطلوب، وأمام هذه الوضعية حاول المشرع الحد من خطورة هذه الجرائم من خلال إدراجه لتعديلات هامة على قانون العقوبات وقانون الاجراءات الجزائية، وسن القانون رقم 04-09 للوقاية ومكافحة هذه الجريمة.

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي تعتمد على التقنية الحديثة والمتطورة، لذلك يتطلب مكافحتها والاعتماد على وسائل تقنية لا تقل حداثة عن الوسائل المستعملة في ارتكابها.

تظهر خطورة الجرائم الإلكترونية في كونها جرائم عابرة للحدود وصعبة الاكتشاف والإثبات ويصعب فيها تحديد الاختصاص القضائي نتيجة لكون شبكة الأنترنيت هي المجال الحيوي لارتكابها.

ترتكب الجرائم الإلكترونية في عالم افتراضي غير ملموس ماديا لكن له وجود حقيقي أهم خصائصه هي أنه غير مقيد بحدود زمنية ومكانية، وهو ما يتطلب ضرورة إعادة النظر في

الكثير من القواعد والمسلمات القانونية مثل قواعد الاختصاص القضائي وغيره من المبادئ القانونية.

قد توجهت دراستنا الموسومة –**الوقاية من الجريمة الالكترونية في التشريع الجزائري** – بجملة من النتائج والمقترحات نوجزها فيما يلي:

النتائج:

– تبين أن التشريع الجزائري لا يزال يشكو من بعض الفراغات القانونية التي تحد من فعالية مكافحة الجريمة الإلكترونية.

– تبين وجود قصور في الجانب المؤسساتي من حيث ضعف التنسيق بين الجهات المعنية بمكافحة الجريمة الإلكترونية.

– هناك ضعف في التكوين والتدريب الموجه لموظفي الجهات الأمنية والقضائية في المجال السيبراني.

– تبين محدودية الوعي المجتمعي بمخاطر الجريمة الإلكترونية وطرق الوقاية منها.

– عدم استغلال التعاون الدولي بالقدر الكافي في مواجهة الجرائم العابرة للحدود.

الاقتراحات:

– ضرورة الإسراع في سن قوانين جزائية خاصة بالجريمة الإلكترونية تكون واضحة ومتكاملة، وتغطي كل صور الاعتداءات الرقمية الحديثة.

– يجب العمل على تفعيل آلية التنسيق بين مختلف المؤسسات الأمنية والقضائية والتقنية، من خلال إنشاء هيئة وطنية موحدة تتولى تنسيق الجهود ومتابعة الجرائم الإلكترونية.

– ينبغي تعميم التكوين المتخصص والدوري في مجال أمن المعلومات والجرائم الإلكترونية لكافة الإطارات القضائية والأمنية والفنية.

– من المهم تكثيف حملات التوعية عبر وسائل الإعلام والمنصات الرقمية والتركيز على برامج الإعلام الأمني الموجهة لفئات المجتمع المختلفة.

– ينبغي تعزيز التعاون الأمني والقضائي الدولي، وتفعيل الاتفاقيات الدولية، خاصة المتعلقة بتبادل المعلومات وتسليم المجرمين الرقميين.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

اولا-المصادر:

1-القوانين:

- القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، المعدل والمتمم للامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الصادر في 30 افريل 2024 ، ج رج، ج العدد 30 سنة2024
- قانون رقم 09-04 مؤرخ في 5 اغسطس 2009 متضمن قواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها الصادرة ب 5 اغسطس 2009 ، ج رج، ج العدد 47 سنة2009
- القانون رقم 06-01 المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية، العدد 14، الصادرة بتاريخ 8 مارس 2006.

2-الاوامر:

- الامر 21-09 المؤرخ في 8 جوان 2021 يتعلق بحماية المعلومات والوثائق الادارية الصادر ب 9 جوان 2021 . ج ر ج ج العدد 45 سنة 2021

3-المراسيم:

- المرسوم الرئاسي رقم 19-172 المؤرخ في 6 جوان 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنضيمها وكيفيات سيرها الصادرة في 9 جوان 2019 ج ،ر،ج، ج العدد 37 سنة 2019

ثانيا-المراجع:

1-الكتب:

- د. بوحليط يزيد الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات -قانون الإجراءات الجزائية ،دار الجامعة الجديدة ،2019
- منير محمد الجنبيهي ،صعوبات التحقيق واستخراج الادلة في جرائم المعلومات ،دار الفكر الجامعي ،الإسكندرية ،2019

2-**الرسائل الجامعية:**

أولا -أطاريح الدكتوراه:

- شنتير خضرة ،الآليات القانونية لمكافحة الجريمة الإلكترونية ،دراسة مقارنة،**اطروحة دكتوراه** ،جامعة أحمد دراية ،ادرار ،كلية الحقوق والعلوم السياسية ،2021
- عميمر عبد القادر ،اليات اثبات الجريمة المعلوماتية في التشريع الجزائري دراسة مقارنة ،**اطروحة دكتوراه** ،جامعة الجزائر 1 بن يوسف بن خدة ،كلية الحقوق 2020

ثانيا-رسائل الماجستير:

- حازم عدنان سلوم ، تحسين نظم كشف الاختراق باستخدام تقنية مصائد الاختراق الهجينة ،**أطروحة الماجستير** ، المعهد العالي للعلوم التطبيقية والتكنولوجيا قسم الاتصالات ،سوريا 2017 .

ثالثا-مذكرات الماستر:

- ابو نمرة سليمان ، بوكشيدة يوسف ، مكافحة الجريمة المعلوماتية " في اطار القانوني الدولي ، **مذكرة ماستر**، جامعة محمد خيضر بسكرة،2021
- حشمان عمار ، الجريمة المعلوماتية في التشريع الجزائري **مذكرة ماستر** جامعة قاصدي مرباح ورقلة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير قسم علوم التسيير ،2019
- قاضي خولة، جباس منال، التعاون الدولي في مكافحة الجريمة الإلكترونية مذكرة **ماستر**، جامعة قاصدي مرباح ورقلة 2021

3-المقالات العلمية:

- امحمدي بوزينة امنة ، "الحماية الجنائية للمعطيات الإلكترونية في إطار القانون الجزائري: دراسة تحليلية لقانوني العقوبات وحقوق المؤلف"، **مجلة القانون والمجتمع**، العدد 31 ،6 ديسمبر 2015.
- امحمدي بوزينة امنة ،خصوصية قواعد التجريم عند الاعتداء على انظمة المعالجة الآلية للمعطيات في اطار التشريع الجزائري ،مجلة ببلوفيليا لدراسات المكتبات والمعلومات ،العدد05 30،مارس 2020
- بن عبد الله الشهري معدي ، الأجهزة الإلكترونية وأثرها على سلوك الأطفال من وجهة نظر الوالدين دراسة وصفية على عينة من آباء وأمهات طالب الصفوف العليا

للمرحلة الابتدائية بمحافظة جدة، المجلة الدولية لنشر البحوث والدراسات العدد السابع والعشرون المجلد الثالث، 3 يناير 2022

- بن عبد المالك نادية ،فلاح عبد القادر، ، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2019
- جبار فاطمة، "الخصوصية الإجرائية لمواجهة الإجرام الإلكتروني في التشريع الجزائري"، مجلة دراسات وأبحاث، المجلد 12، العدد 4، أكتوبر 2020
- خبزاوي مراد ، محمودي رقية ، العالم الامني الرقمي كممارسة امنية استباقية في سبيل الوقاية من الجريمة الإلكترونية. مجلة البحوث والدراسات العلمية ، جامعة يحيى فارس بالمدية (الجزائر)المجلد ،18العدد01 .2024
- ديوب بشرى ،دراسة ومقارنة أنظمة كشف الاختراقات المفتوحة المصدر ، مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الهندسية المجلد 37 العدد 1 ،2015
- داودي منصور ،مرابط حمزة ، التشفير كآلية لحماية المصنفات الرقمية من القرصنة الإلكترونية ، مجلة الحقوق والعلوم السياسية جامعة خنشلة ،جامعة تيارت، ابن خلدون، الجزائر ، المجلد 10 العدد01– 2023
- سيدي موسى ليلى ،ساعد محمد , ،العالم الامني ودوره في تعزيز الوعي الامني السيبراني الشرطة الجزائرية نموذجا–مجلة الرواق لدراسات الاجتماعية والانسانية .جامعة عبد الحميد بن باديس مستغانم الجزائر المجلد 9 ▪العدد202
- شنين صالح ، التسرب في قانون الإجراءات الجنائية الجزائري حماية للنظام العام والحريات ام حماية للنظام العام ،المجلة الجزائرية للقانون المقارن ،العدد2

- شليل عبد اللطيف ،فيلالي اسماء ، ،تهديدات آمن المعلومات وسبل التصدي لها، – جامعة أبو بكر بلقايد ، تلمسان الجزائر،مجلة البشائر الاقتصادية المجلد الرابع تلمسان الجزائر، المجلد الرابع،العدد03، 2019.
- صيافة تركية ،اسلوب التسرب في القانون الجزائري ،مجلة الدراسات القانونية و السياسية ،المجلد09,العدد02.جوان 2023
- عبد الحميد حسين رجب ،آمن شبكات المعلومات الإلكترونية : المخاطر والحلول : مجلة Journal Cybrarians جامعة الحصن ابو ظبي ،العدد30ديسمبر 2012
- فلاح عبد القادر ،حجز وحفظ المعطيات في الجريمة الإلكترونية ،مجلة صوت القانون ،المجلد الثامن العدد 1 ،2021
- غريبي أحمد، قاسيمي حورية ، دور سياسة التشفير الإلكترونية في حماية نظم معلومات الإدارة الإلكترونية بمؤسسة بريد الجزائر فر ع المدية : مجلة الاقتصاد الجديد ، جامعة المدية الجزائر المجلد 12 ، العدد ،1 .2021
- لدغش رحيمة ،"ضوابط تفتيش الحاسب الآلي "،مجلة الحقوق والعلوم الإنسانية العدد 25 ،جامعة الجلفة
- مصطفى هنشور وسيمة ،النظام القانوني لمقدمي خدمات الأنترانت في التشريع الجزائري ،مجلة البحوث القانونية و السياسية ،العدد الخامس ،ديسمبر ،2015

4-الملتقيات العلمية:

- امحمدي بوزينة امنة ،اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية دراسة تحليلية الحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم العالم الملتقى الوطني ،اليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ،الجزائر العاصمة ،29 مارس 2017

- بوعافية رضا ،"اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية "،ضمن اعمال الملتقى الوطني الافتراضي ،حول الجرائم الإلكترونية في المجتمع الجزائري ،(تشخيص الواقع و تحديات الأمن السيبراني)،جامعة يحي فارس المدية ،15مارس 2022
- بوخالفة سعاد ، "مكافحة الجرائم الإلكترونية في التشريع الجزائري "، ضمن: أعمال الملتقى الوطني الافتراضي حول الجرائم الإلكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني،جامعة يحي فارس المدية ،15 مارس 2022
- بومحراث ليندة، عبد النور سعيداني ،،"اجراءات البحث والتحري في الجرائم الإلكترونية "ضمن اعمال الملتقى الوطني الافتراضي حول الجرائم الإلكترونية في المجتمع الجزائري)تشخيص الواقع وتحديات الأمن السيبراني (،جامعة يحي فارس المدية ،15مارس 2022
- سويسي فتيحة "التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المرتبطة بها، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي ،2022

5-المحاضرات:

- بطيحي نسمة، محاضرات في مقياس الوقاية من الجرائم الإلكترونية، مطبوعة مقدمة لطلبة السنة الثانية ماستر، تخصص: إدارة إلكترونية وخدمات رقمية، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين – سطيف 2، السنة الجامعية 2021/2022

6-الأيام الدراسية:

- بومحراث ليندة ،إجراءات التحقيق الخاصة بالجرائم السيبرانية "،يوم دراسي حول الجريمة السيبرانية ،مجلس فضاء قسنطينة بالتعاون مع جامعة قسنطينة 3،2، 1 وجامعة الامير عبد القادر للعلوم الاسلامية ، 2022

7-المواقع:

- العربي الإفريقي، "آليات التعاون الأمني الدولي"، تم الاطلاع عليه بتاريخ 2025/05/10، الساعة 8:48 مساءً، من الموقع: https://www.arabafricanews.com

- University of Babylon، "الحاسوب وتعريف الحاسوب". تم الاطلاع عليه يوم 10 ماي 2025، الساعة 7:54 مساءً، من: https://www.uobabylon.edu.iq

- كلية المستقبل الجامعة. "فيروسات الحاسوب ومكونات الفيروس". تم الاطلاع عليه يوم 10 مايو 2025، الساعة 7:56 مساءً، من: https://www.uonus.edu.iq

فهرس

المحتويات

فهرس المحتويات

الشكر

الإهداء

المقدمة 2

الفصل الاول:الوقاية القبلية من الجريمة الالكترونية

المبحث الاول:التطور التشريعي لوسائل الوقاية من الجريمة الالكترونية.....10

المطلب الأول: الإطار التشريعي للوقاية من الجرائم الإلكترونية.....10

الفرع الأول: القوانين الجزائرية المتعلقة بالجريمة الالكترونية والأمن السيبراني.....11

الفرع الثاني: التعديلات التشريعية الحديثة.....15

المطلب الثاني: دور الأجهزة الأمنية في مكافحة الجريمة الإلكترونية 16

الفرع الأول : تفعيل دور الاعلام الأمني في مكافحة الجريمة الإلكترونية 17

الفرع الثاني: تعزيز التعاون الأمني الدولي في مكافحة الجريمة الإلكترونية 20

المبحث الثاني : الوقاية الموضوعية من الجريمة الالكترنية.....23

المطلب الأول: الوسائل الوقائية التقنية.....23

الفرع الأول : تأمين شبكات المعلومات.....23

الفرع الثاني : تأمين الأجهزة.....30

المطلب الثاني : تطوير اليات الحماية من الجريمة الالكترونية.....34

الفرع الأول : اهمية التشفير في حماية المعلومات.....34

الفرع الثاني: انضمة لكشف المبكر عن حالات الاختراق.....36

الفصل الثاني: مكافحة الجريمة الالكترونية **في التشريع الجزائري**

المبحث الأول : الوسائل الاجرائية لمكافحة الجريمة الإلكترونية 44

المطلب الأول : الوحدات المختصة بتولى اجراءات البحث والتحقيق في الجريمة الإلكترونية.....44

الفرع الأول : الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال.....45

الفرع الثاني: الأجهزة الأمنية المكلفة بالبحث والتحري 49

المطلب الثاني : الوقاية من الجريمة الإلكترونية في قانون العقوبات الجزائري.....51

الفرع الأول: العقوبات الأصلية 52

الفرع الثاني : العقوبات التكميلية 55

المبحث الثاني: التدابير الإجرائية للكشف عن الجرائم الإلكترونية 57

المطلب الأول : الإجراءات القانونية للكشف عن الجرائم المعلوماتية 57

الفرع الأول: اجراءات التفتيش ومعاينة مسرح جرائم الماسة باليه المعطيات 58

الفرع الثاني : اجراء الحجز 69

الفرع الثالث: مراقبة الاتصالات والالتزامات القانونية لمقدمي خدمات الإنترنت.....71

المطلب الثاني: الإجراءات المستحدثة في مكافحة الجرائم المعلوماتية.....83

الفرع الأول : الكشف بواسطة اسلوب اعتراض المراسلات وتسجيل الصوت

و الصور 83

الفرع الثاني : أسلوب التسرب 91

الخاتمة.....97

قائمة المصادر والمراجع 101

فهرس المحتويات.....109

ملخص 112

ملخص:

أدى تطور تكنولوجيا المعلومات والاتصالات إلى بروز الجريمة الإلكترونية كخطر عابر للحدود، ما استدعى استجابات تشريعية وأمنية وتقنية متكاملة. وقد تبنّى المشرع الجزائري وسائل قانونية وإجرائية للحد من اختراق الأنظمة وحماية المعطيات، مع تعزيز قدرات الأجهزة الأمنية، وتفعيل الإعلام الأمني، فضلًا عن إشراك المؤسسات المختصة والتدابير الإجرائية للكشف عن الجريمة وملاحقة مرتكبيها.

كما تم اعتماد وسائل تقنية متقدمة مثل التشفير، أنظمة كشف التسلل، الجدران النارية، وشبكات VPN لضمان حماية وقائية واستجابة فعالة. وقد أظهرت التجربة أن مواجهة هذا النوع من الإجرام تتطلب تنسيقًا متكاملًا بين القانون، الأمن، والتكنولوجيا ضمن رؤية استراتيجية تستجيب لتحولات الفضاء الرقمي.

Summary:

The evolution of information and communication technologies has elevated cybercrime into a transnational threat, prompting integrated legal, security, and technical responses. Algerian legislation adopted regulatory and procedural tools to protect systems and data, reinforced security agencies, and activated awareness through media, while also engaging institutional bodies and procedural measures to detect and prosecute cyber offenses.

Advanced tools such as encryption, intrusion detection systems, firewalls, and VPNs have been employed to ensure proactive protection. The experience confirms that effectively addressing cybercrime requires coordinated efforts across legal, security, and technological dimensions within a strategic framework responsive to digital developments.