وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم: القانون الخاص

المرجع:

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة المعلوماتية في التشريع الجزائري

ميدان الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: القانون القضائي

من اعداد الطالبة:

جلطي مختارية

تحت إشراف الأستاذة:

علاق نوال

أعضاء لجنة المناقشة

الأستاذ(ة): **حميدة فتح الدين** رئيسا

الأستاذ(ة): **علاق نوال** مشرفا مقررا

الأستاذ(ة): **بن سطاعلي جميلة** مناقشا

السنة الجامعية: 2024/2023

نوقشت في: 2024/06/13

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

UNIVERSITE Abdelhamid Ibn Badis MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات
الرقم :.....م.ت/

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية لإنجاز البحث

حررت هذه الوثيقة من طرف الموثق
عمار فاطمة

أنا الممضي أدناه،

السيد: خلصي مختارية الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 411604735 والصادرة بتاريخ: 2024/05/09

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون العام

والمكلف بإنجاز مذكرة ماستر بعنوان:

الحبس بمقابل المعلوماتية في التشريع الجزائري

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

التاريخ: 2024/06/12

إمضاء المعني

نظرا لسلطة الإمضاء
السيد
صيادة في:
12 JUIN 2024

ع/ رئيس المجلس الشعبي البلدي
و بتفويض منه
رئيس مصلحة الحالة المدنية
مت إمضاء : حمو شلوش

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

Scanné avec CamScanner

اهداء

بكل حب اهدي نجاحي وتخرجي الى:

من كلله الله بالهيبة والوقار يامن افتقدك منذ الصغر الى والدي العزيز الذي وافته المنية تغمده الله برحمته الواسعة.

من جعل الله الجنة تحت اقدامها، الى من كانت ملجئي ويدي اليمنى في هذه المرحلة الى من ابصرت بها طريق حياتي واعتزازي بذاتي الى من دعمتني وعلمتني ان هذه الحياة كفاح وسلاحها العلم والمعرفة الي امي العزيزة.

من كانت سندا لي في مخاض هذا العمل الى اختي العزيزة لن أنسى ابدا دعمك أتمنى ان نحقق معا المزيد من النجاحات في المستقبل.

السند والكتف الذي لا يميل اخي العزيز وائل.

صديقاتي العزيزات اللواتي كن دائما بجانبي في كل الأوقات شكرا لكن على الدعم المستمر.

شكر وعرفان

الحمد لله عز وجل على توفيقه لي في إنجاز هذه المذكرة حمدا يليق بجلالته وعظمته، فالحمد والشكر لله.

اتقدم بالشكر الجزيل إلى الأستاذة المشرفة علاق نوال التي لم تبخل علي بنصائحها وتوجيهاتها السديدة التي كان لها بالغ الأثر في إنجاز هذه المذكرة كما نحيي فيها روح التواضع والمعاملة الجيدة جزاها الله كل خير.

كما أتقدم بأسمى عبارات التقدير والاحترام لأعضاء لجنة المناقشة الذين قبلوا مناقشة هذه المذكرة.

كذلك اشكر جميع اساتذتي الكرام الذين تعلمت منهم ولو حرفا واحدا خلال مسيراتي الدراسة.

هذه كلمات الشكر تعبر عن خالص امتناني لكل من كان لي عونا من قريب او بعيد.

مـــقدمـــــة

مقدمة:

لقد شهد العالم تطورا هائلا لم يسبق له مثيلا في جميع مجالات الحياة الاجتماعية، السياسية الاقتصادية، الأمنية وغيرها من المجالات، حيث تحولت طريقة الحياة من كل ما هو تقليدي مادي الى ما هو حديث ورقمي بفضل الثورة المعلوماتية التي حدثت، والتي من خلالها تم كسر الحدود بين الدول والشعوب، وأصبحت دول العالم بمثابة قرية صغيرة، اذ أصبح من الشائع استعمال الحاسوب وكذا شبكات الاتصال بشكل يومي، اللذان كان لهما دور في تحقيق قفزة حضارية في حياة الأفراد وكذلك الدول.

أصبحت معظم القطاعات تستعمل الأنظمة المعلوماتية لأداء مهامها ذلك لأنها تقدم خدمات سريعة وبطريقة سهلة وأقل تكلفة وبدقة عالية، كما تقوم الأنظمة المعلوماتية بجمع المعطيات وتخزينها ومعالجتها ونقلها ومن ثم تبادلها مع الافراد والمؤسسات والشركات سواء داخل الدولة او بين عدة دول، فبدا من الصعب أن تقوم هذه القطاعات بأداء أعمالها دون الاعتماد الأساسي على هذه التقنية الحديثة، فأصبحت من لوازم الحياة المتطورة سواء على المستوى العام أم الخاص، حيث تعتمد المؤسسات الحكومية والخاصة على حد سواء في تسيير أعمالها بشكل أساسي على استخدام نظم المعالجة الآلية.

بالرغم من أن هذه الثورة المعلوماتية كان لها دور كبير في تسهيل حياة الافراد وكذلك الدول، الا انها بقدر ما كان لها من انعكاسات إيجابية، كان لها أيضا انعكاسات سلبية خطيرة ظهرت جراء الاستخدام السيئ للتقنية المعلوماتية، اذ انها كانت سببا في ظهور جريمة خطيرة تشكل انتهاكا على الافراد كما تشكل ايضا خسائر لاقتصادات الدول، الا وهي الجرائم المعلوماتية والتي سميت أيضا بالجرائم الالكترونية او الجرائم السيبرانية، هذه الجرائم مرتبطة بالأنظمة المعلوماتية وكذلك شبكة الانترنت.

والخطورة التي تتسم بها هذه الجريمة هي سهولة ارتكابها، كما أن آثارها ليست محصورة في نطاق إقليمي محدد لدولة بعينها، فضلا على أن مرتكبي الجريمة المعلوماتية يتميزون بالذكاء في التعامل مع مجال الأنظمة المعلوماتية والإلمام بالمهارات والمعارف التقنية، هذا الأمر اثار بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة المعلوماتية، خاصة انها متعودة على التعامل مع الجرائم التقليدية، والتي يمكن إدراكها بالحواس بحيث يخلف مرتكبو هذه الجرائم آثار مادية في مسرح الجريمة مثل بصمات أو بقع دم أو محررات مزورة.

من المشكلات الإجرائية التي ستواجه هذه الاجهزة عند تعاملها مع الجريمة المعلوماتية، هي انها ترتكب في بيئة افتراضية تقنية، كما أن هذه الجريمة ترتكب في الخفاء، فكثيرا ما يتعمد مرتكبي الجريمة المعلوماتية إخفاء نشاطهم الاجرامي وذلك عن طريق التلاعب بالبيانات والذي غالبا يعقد أمر كشفها وتحديد مرتكبها.

كما ان النصوص الخاصة بالبحث والتحقيق في مجال الجرائم التقليدية لا تصلح للتطبيق في مجال الجرائم المعلوماتية، فالنصوص المتعلقة بإصدار اوامر القبض والإحضار وعلى سبيل المثال لا يمكنها أن تجدي نفعا في مواجهة مجرمي المعلوماتية الذين قد يرتكبون فعلهم الإجرامي من نقطة تقع في أقصى بقاع الأرض، وذلك بسبب عائق مبدأ إقليمية النص الجنائي، وهو ما تسبب في شل أيدي العدالة عن ممارسة أعمال البحث والتحقيق بشأن الجرائم المعلوماتية.

تكمن **أهمية** دراستنا لهذا الموضوع في:

-ان الجريمة المعلوماتية من الجرائم الناجمة عن التطور التكنولوجي وتختلف عن الجرائم التقليدية.

-الجريمة المعلوماتية جريمة متنوعة وهي في تطور دائم مما يفرض على مختلف المشرعين مواكبة هذا التطور.

- ان موضوع الجريمة المعلوماتية موضوع حديث ويتزايد انتشاره يوما بعد يوم.

-السلوك الاجرامي لمرتكبي الجريمة المعلوماتية يختلف تماما عن السوك الاجرامي لمرتكبي الجرائم التقليدية.

وبناء على أهمية الموضوع **تهدف** دراستنا هذه الى:

-التعريف بالجريمة المعلوماتية وذكر خصائها.

-ذكر أنواع الجريمة المعلوماتية ودوافع ارتكابها وكيف تم مواجهتها في التشريع الجزائر.

-التوعية والتثقيف حول مخاطر الجريمة المعلوماتية سواء على الافراد او على المؤسسات.

-لإثراء المكتبة أكثر بمراجع حول هذا الموضوع.

اما الأسباب التي دفعتنا لاختيار هذا الموضوع فهي تنقسم الى أسباب موضوعية وأخرى ذاتية.

الأسباب الموضوعية:

-نظرا لزيادة معدل ارتكاب الجريمة المعلوماتية.

-كون هذا الموضوع من المواضيع الجديدة ذات قيمة علمية.

- الجريمة المعلوماتية يمكن ان تسبب خسائر مالية كبيرة للأفراد وكذلك الدول.

-لان هذه الجريمة تختلف عن الجرائم التقليدية من عدة جوانب.

أسباب ذاتية:

-الرغبة في التعمق أكثر في موضوع الجريمة المعلوماتية.

-لان الجريمة المعلوماتية في تطور مستمر وهذا ما يجعلها موضوعا مثيرا للاهتمام ويحفزني للبحث في هذا الموضوع الشيق.

– ان اختيار هذا الموضوع نابع من الشغف الشخصي، بحيث انه كان موضوع بحثي ولفت نظري انه يستحق الدراسة أكثر.

الدراسة السابقة: من خلال بحثنا قد اطلعنا على العديد من الدراسات نذكر منها:

–أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام بعنوان مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، لطالب بدري فيصل جامعة الجزائر 01 2018/2017.
–مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الاجرام لطالب سوبر سفيان بعنوان جرائم المعلوماتية جامعة ابو بكر تلمسان 2011/2010.

وعليه سنحاول من خلال دراستنا ان نبرز النقاط المهمة في الجريمة المعلوماتية، وذلك بطرح **الإشكالية التالية:**

ماهي الجريمة المعلوماتية؟ وكيف تم مواجهتها في التشريع الجزائري؟

لمعالجة هذه الإشكالية وضفنا المنهج الوصفي وكذلك المنهج التحليلي حيث استعملنا المنهج الوصفي من خلال وصف الجريمة المعلوماتية.

اما المنهج التحليلي بواسطته قمنا بتحليل مختلف المواد القانونية التي تتعلق بالجريمة المعلوماتية.

للإجابة عن هذه الإشكالية ارتأينا تقسيم هذه الدراسة الى فصلين حيث سنتناول في الفصل الأول ماهية الجريمة المعلوماتية وذلك من خلال مبحثين في المبحث الأول سنتعرف على مفهوم الجريمة المعلوماتية، اما المبحث الثاني فسنتطرق فيه الى الاثبات في الجريمة المعلوماتية، اما الفصل الثاني فقد خصصناه لدراسة مواجهة الجريمة المعلوماتية في التشريع الجزائري قسمناه أيضا الى مبحثين في المبحث الأول سنتطرق الى الضوابط التشريعية لمواجهة الجريمة المعلوماتية، اما المبحث الثاني فسنتناول الضوابط العملية لمواجهة الجريمة المعلوماتية.

الفصل الأول: ماهية الجريمة المعلوماتية

الفصل الأول ماهية الجريمة المعلوماتية:

تعد الجرائم المعلوماتية من الجرائم الحديثة التي ظهرت نتيجة للثورة التي شهدها العالم في مجال تقنية المعلومات والاتصالات، بحيث ان هذه الثورة بقدر ما ابهرت العالم بمزاياها والتي اصبح بفضلها العالم كقرية صغيرة الا انها خلفت عيوب الا وهي ظهور هذا النوع من الجرائم، اذ تعد الجريمة المعلوماتية من الجرائم التي لم يتوقعها المجتمع البشري وهي جريمة خطيرة لأنها قد تمس الحياة الخاصة للأفراد كما قد تمس السيادة الوطنية والامن القومي للبلاد، لذا وجب معرفة ماهية هذه الجريمة المعلوماتية هذا ما سنتناوله من خلال هذا الفصل، حيث قسمنا هذا الفصل الى مبحثين:

المبحث الأول: خصصناه لمفهوم الجريمة المعلوماتية.

اما المبحث الثاني: فسنتطرق الى الاثبات في الجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من أكثر الجرائم انتشارا في الوقت الحالي، ذلك نظرا لتطور الحاصل في تكنولوجيا الحاسب الالي وكذا ظهور شبكة الأنترنت التي بقدر ما سهلت الحياة و اختصرت الوقت و قدمت تسهيلات وخدمات و إيجابيات، الا ان لها جانب سلبي يتمثل في إساءة البعض استخدام هذه التكنولوجيا مما ساهم في انتشار الجريمة المعلوماتية، لذا من خلال هذا المبحث سنتطرق الى تعريف الجريمة المعلوماتية و كذا ذكر خصائصها في المطلب الأول اما المطلب الثاني فقد خصصناه لدراسة صور الجريمة المعلوماتية ودوافع ارتكابها، والمطلب الثالث تطرقنا فيه الى اركان الجريمة المعلوماتية.

المطلب الأول: تعريف الجريمة المعلوماتية وخصائصها

سنتطرق في الفرع الأول الى تعريف الجريمة المعلوماتية اما الفرع الثاني فسنتطرق فيه الى خصائص الجريمة المعلوماتية.

الفرع الأول تعريف الجريمة المعلوماتية:

لم يكن هناك اجماعا على تعريف الجريمة المعلوماتية، ذلك نظرا لما أحيط بها من غموض واختلاف بسبب ارتباطها بالتطور المستمر واللامتناهي لتكنولوجيا الاعلام والاتصال،[1] لهذا سنحاول التعرف على أبرز المحاولات الفقهية والتعاريف القانونية للجريمة المعلوماتية:

أولا التعاريف الفقهية للجريمة المعلوماتية:

اختلف الفقهاء حول تعريف الجريمة المعلوماتية من بين هذه التعاريف:

-تعريف الفقيه تاديمان للجريمة المعلوماتية على انها: (كل اشكال السلوك غير مشروع الذي يرتكب باستخدام الحاسب الالي).

[1] عميمر عبد القادر، التحديات القانونية لاتباث الجريمة المعلوماتية، النشر الجامعي الجديد، الجزائر، 2021، ص22.

-كما انه للفقيه تاديمان تعريف اخر للجريمة الحاسب الالكتروني حيث عرفها أيضا بانها: (كل جريمة ضد مال مرتبطة بالمعالجة الالكترونية للبيانات) وهو تعريف يختلف عن التعريف السابق.

-وعرفها دافيد تومسون بانها: (اية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسب الالي)[1].

-كما عرف الأستاذ مروي الجريمة المعلوماتية على أساس وسيلة ارتكابها بحيث قال بانها: (الفعل غير مشروع الذي يتورط في ارتكابه الحاسب الالي)[2].

-ويرى الأستاذ ماسي ان المقصود بالجريمة المعلوماتية هو: (الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح).

-وذهب الفقيه روسونبلا الى تعريفها بقوله: (هي كل نشاط غير مشروع موجه لنسخ او الوصول الى المعلومات المخزنة داخل الحاسوب او تغييرها او حذفها او الوصول او التي تحول عن طريقه)[3].

-وقد عرفها الدكتور علي القهوجي بانها:(سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها)[4].

[1] د فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، مصر الإسكندرية، 2016، ص 40.

[2] خالد ممدوح إبراهيم، امن الجريمة الالكترونية، الطبعة الأولى، الدار الجامعية، مصر، 2008، ص 42.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 48.

[4] غانم مرضي الشمري، الجرائم المعلوماتية، دار العلمية الدولية للنشر والتوزيع، الاردن، 2016، ص28.

ثانيا التعريف القانوني للجريمة المعلوماتية:

ان معظم المشرعين تفادوا تعريف الجريمة المعلوماتية واوكلوا هذه المهمة الى الفقه والقضاء الى ان بعض التشريعات أعطت تعريفا لنظام المعلومات وليس لنظام المعالجة الالية للمعلومات ومن بين التشريعات التي عرفت النظام المعلوماتي نذكر ما يلي:

-قانون المعاملات الأردني رقم 85 لسنة 2001 والذي عرف نظام معالجة المعلومات في المادة 2 الفقرة 10 على انه (النظام الالكتروني المستخدم لإنشاء رسائل المعلومات وارسالها او تسليمها او معالجتها او تخزينها او تجهيزها على أي وجه اخر).

-قانون اليونسترال النموذجي بشأن التجارة الالكترونية حيث عرف هذا القانون نظام المعلومات من خلال المادة 2 على انه (النظام الذي يستخدم لإنشاء رسائل البيانات او ارسالها او تخزينها لتجهيزها على أي وجه اخر)[1].

- لقد قامت وزارة العدل في الولايات المتحدة الامريكية بتعريف الجريمة عبر الانترنت على انها (أي جريمة لفاعلها معرفة بتقنية الحاسبات تمكنه من ارتكابها).

عرف مكتب تقييم التقنية الجريمة المعلوماتية بأنها (الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا)[2].

<u>اما المشرع الجزائري</u> قام بتعريف الجريمة المعلوماتية في المادة الثانية من القانون 09-04 والتي سماها الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بانها (جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في أي جريمة يرتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية).

[1] راضية عيمور، الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية جامعة الاغواط، الجزائر، المجلد السادس، العدد الأول،2022، ص 92-93.

[2] د عميمر عبد القادر، المرجع السابق، ص22.

يلاحظ ان المشرع الجزائري اعتمد في تعريفه للجريمة المعلوماتية على معيارين هما معيار موضوع الجريمة ومعيار وسيلة ارتكاب الجريمة.

1-معيار موضوع الجريمة:

اعتمد المشرع الجزائري في تعريفه للجريمة المعلوماتية على موضوع او محل الجريمة الا وهو المساس بأنظمة المعالجة الالية للمعطيات وهي جرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان (المساس بأنظمة المعالجة الالية للمعطيات) والتي تحكمها المواد من 394 مكرر الى المادة 394 مكرر 7.

2-معيار وسيلة ارتكاب الجريمة:

إضافة الى استناد المشرع في تحديد تعريف الجريمة المعلوماتية الي موضوع الجريمة اعتمد أيضا على معيار اخر وهو وسيلة ارتكاب الجريمة وهي المنظومة المعلوماتية، او نظام الاتصالات الالكترونية بالقول (.... واي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية) فوسيلة ارتكاب الجريمة او تسهيل ارتكابها هي محل اعتبار في تكييف الجريمة[1].

الفرع الثاني: خصائص الجريمة المعلوماتية

ان ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت اضفى عليها مجموعة من السمات التي تميز هذه الجريمة عن الجرائم العادية تتمثل هذه السمات في:

أولا الجريمة المعلوماتية متعدية للحدود او جريمة عابرة للدول:

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية او ملموسة تقف امام نقل المعلومات عبر الدول المختلفة،[2] فلا وجود لنقاط تفتيش ولا مراكز عبور في هذه البيئة الرقمية

[1] د. عميمر عبد القادر، المرجع السابق، ص 18-19.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 51.

فالجريمة المعلوماتية يمكن ان ترتكب في مكان معين من العالم وتحقق نتائجها في مكان اخر يبعد عنه بألاف الكيلومترات، كما يمكن ارتكاب الجريمة في بلد تكون فيه الشمس مشرقة لتحقق نتيجتها في نفس اللحظة في مكان تسوده ظلمات الليل.

ثانيا سهولة ارتكاب الجريمة المعلوماتية:

عند ارتكاب الجرائم التقليدية كالقتل والسرقة يتطلب الامر قوة عضلية، الا ان ارتكاب الجريمة المعلوماتية يعتمد فقط على القدرات الذهنية للجاني وتحكمه الجيد في الحاسوب ووسائل الاتصال الحديثة، فلا يحتاج الجاني لارتكابها الى القيام بجهد عضلي ولا حتى الى التنقل والاستعانة بمركبة لنقل المسروقات، بحيث يمكن للجاني ان يرتكب جريمته وهو يرتشف فنجان قهوة خلف مكتبه وفي قاعة مكيفة ودون ان يشعر به أحد حتى ولو كان في مكان مزدحم بالأشخاص.

ثالثا الجريمة المعلوماتية جريمة ناعمة:

ما يميز الجريمة المعلوماتية عن الجرائم التقليدية انها لا تترك اثار مادية كالتي تتركها الجرائم التقليدية، فلا وجود للكسر او بقع الدم، وكل ما تخلفه هي اثار رقمية ليس لها وجود مادي ملموس كما ان الوسائل التي ترتكب بها لا تحدث جروحا ولا تسيل دماء بل هي عبارة عن أجهزة الكترونية من الحواسيب والبرامج التقنية[1].

رابعا صعوبة اكتشاف الجريمة المعلوماتية واثباتها:

تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فان ذلك يكون عادة بصدفة، بحيث يبدو من الواضح ان عدد الحالات التي يتم فيها اكتشاف هذه الجريمة قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.

[1] د. عميمر عبد القادر، المرجع السابق، ص 28.

ويمكن رد السبب الذي يقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية الى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية.

كما ان قدرة الجاني على تدمير دليل الإدانة في اقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

خامسا الجريمة المعلوماتية جريمة الأذكياء:

في غالب الأحيان يكون مرتكبو الجريمة المعلوماتية يتصفون بذكاء وبقدرتهم على التحكم في الوسائل الالكترونية، وهذا الذي يجعلهم يرتكبون جرائم بدقة عالية واحترافية، ويحققون أهدافهم بهدوء دون احداث فوضى او دون لجوئهم الى العنف[1].

المطلب الثاني: صور الجريمة المعلوماتية ودوافع ارتكابها

للجريمة المعلوماتية صور عديدة سنتطرق اليها في الفرع الأول كما اننا سنتطرق في الفرع الثاني على البواعث التي قد تدفع المجرم المعلوماتي لارتكاب هذا النوع من الجرائم.

الفرع الأول صور الجريمة المعلوماتية:

لقد اختلف الفقهاء في تقسيم الجريمة المعلوماتية وذلك نتيجة لظهور جرائم جديدة من حين لأخر بحيث ان الجريمة المعلوماتية ليست محصورة، فهي متغيرة وجديدة فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الالي والانترنت ظهرت معه جريمة جديدة، ورغم ان الفقهاء لم يستقروا على معيار واحد لتصنيف الجريمة المعلوماتية، الا ان منهم من صنفها بالرجوع الى وسيلة ارتكابها او على أساس محلها. [2]

[1] د. عميمر عبد القادر، المرجع السابق، ص43.

[2] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة نحمد بوضياف المسيلة، العدد 11، 2018، ص357.

وعلى هذا الأساس يمكن تقسيم الجريمة المعلوماتية الى:

أولا الجرائم الواقعة بواسطة النظام المعلوماتي:

في هذا النوع من الجرائم يعتبر الحاسب الالي وسيلة تسهل النتيجة الاجرامية وتضاعف جسامتها، تنقسم هذه الجرائم بدورها الى:

1-الجرائم الواقعة على الأشخاص:

وهي الجرائم التي تستهدف حياة الأشخاص او شرفهم، فلحياة الأشخاص خصوصية وحرمة لا يجوز الاعتداء عليها، من بين هذه الجرائم:

أ-جرائم الذم والقدح عبر الانترنت:

تعتبر جرائم السب والقذف من أكثر الجرائم شيوعا على شبكة الانترنت، حيث أصبح في عصرنا هذا الكثير من الأشخاص يستخدمون الانترنت بطريقة تسيء الى شرف الاخرين او كرامتهم او سمعتهم، تعتبر هذه الجرائم جرائم مستحدثة من حيث وسيلة ارتكابها، اذ ظهرت بظهور الانترنت كما ان صور الذم والقدح والتحقير قد يكون وجاهيا عبر خطوط الاتصال المباشر او قد يكون كتابيا او بواسطة مطبوعات، هذه الجرائم عادة ما ترتكب عبر الانترنت من خلال المبادلات الالكترونية الكتابية او الصوتية او عن طريق الفيديو وذلك يكون اما عبر البريد الالكتروني او شبكة الويب او غرفة الدردشة[1].

[1]محمد امين شوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009، ص31.

ب-جرائم انتحال الشخصية:

مع التنامي المتزايد لشبكة الانترنت ازداد ارتكاب هذا النوع من الجرائم، حيث أصبح للمجرمين قدرة أكبر على جمع المعلومات الشخصية للأفراد والاستفادة من تلك المعلومات لانتحال شخصيتهم، كما انه يوجد جرائم انتحال شخصية مواقع، هذا يقع بكثرة في المجال التجاري ففي اغلب الأحيان يؤدي هذا الاحتيال الي الإساءة الى سمعة الضحية[1].

ج-جرائم الاستدراج:

يقوم المجرم المعلوماتي بجذب ضحاياه وفي الاغلب يكون الكثير منهم في مرحلة المراهقة وذلك من خلال تكوين صداقات معهم عبر الانترنت ثم تتحول هذه الصداقة الى لقاء واقعي، مما يسمح لذلك المجرم ارتكاب جريمته بكل سهولة.

إضافة الى هذه الجرائم يوجد كذلك جرائم التهديد والابتزاز وكذا التحريض على الانتحار وجرائم الاباحة كنشر المواد الفاحشة عبر الانترنت بوجه عام وللقصر بوجه خاص، وكذلك نشر معلومات للقصر عبر الانترنت من اجل أنشطة جنسية غير مشروعة والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية، بحيث ان كل هذه الأفعال تلحق اضرار بحياة الأشخاص وشرفهم وسمعتهم[2].

2-الجرائم الواقعة على الاموال:

في هذا النوع من الجرائم يستهدف المجرم المعلوماتي بواسطة الحاسب الالي، الكسب المالي من بين الجرائم الواقعة على الأموال نذكر ما يلي:

[1] عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية-مكتبة القانون والاقتصاد، الطبعة الأولى،2012، المملكة العربية السعودية، ص164.

[2] د. عميمر عبد القادر، المرجع السابق، ص55.

ا-جرائم تحويل الالكتروني الغير مشروع:

لقد أدت الثورة الرقمية الى إمكانية اجراء تحويلات ومبادلات للأموال من أي مكان في العالم، ففي الغالب يحصل مجرمو المعلوماتية على كلمات المرور الخاصة بالغير اما باختراقهم اثناء تواجدهم في النظام المعلوماتي او من خلال بث برامج تعقب على الأنظمة المعلوماتية التي يتجه اليها أكثر المستخدمون وسرقة كلمة المرور الخاصة بهم والحصول على البيانات الخاصة بالضحية واجراء تحويلات مالية الكترونية من حسابه وادخالها في ارصدة مجرمي المعلوماتية.

ب-جرائم السطو على ارقام البطاقات الائتمانية:

منحت الثورة الرقمية لقراصنة المعلوماتية إمكانية سرقة ارقام البطاقات الائتمانية وذلك بواسطة برامج تشغيل، او إمكانية التقاط هذه الارقام عبر قنوات الانترنت المفتوحة واستخدامها بطريقة غير مشروعة في عملية التسوق عبر الانترنت بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقة[1].

ج-تجارة المخدرات عبر الانترنت:

في عصر الانترنت انتشرت مواقع تتعلق بالترويج للمخدرات وتعليم كيفية صنعها وكذا بيعها بكافة اصنافها وأنواعها.

د-جريمة غسيل الأموال عبر الانترنت:

لقد اختلف الكثير حول تعريف غسيل الأموال الا انه يمكن تعريفه على انه (أي عملية من شانها إخفاء المصدر غير مشروع الذي اكتسبت منه الأموال) فقد ساهمت الانترنت كثيرا في عملية تسهيل غسل الأموال.

[1] محمد امين شوابكة، المرجع السابق، ص 187.

حيث انه من المميزات التي اضافتها الانترنت لغسل الأموال، هو اغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما ان عمليات الغسيل عبر الانترنت تتم بسرعة أكبر وبدون ترك أي اثار في الغالب[1].

3-الجرائم الواقعة على امن الدولة:

استخدمت العديد من الجماعات المتطرفة الانترنت لانتشار المعتقدات والأفكار بصرف النظر عن الأفعال التي تهدد امن الدولة ومن هذه الجرائم:

أ-جرائم الإرهاب:

لقد اخذت جريمة الإرهاب مسارا حديثا يتماشى مع التطور المعلوماتي بحيث اصبحت الانترنت أداة لتجنيد وتجييش أعضاء جدد عبر مختلف منصات التواصل الاجتماعي، وذلك من خلال محاولة التأثير على المعتقدات الدينية للأفراد بغرض المساس بأمن الدولة، قد تكون جرائم الإرهاب بتعاون عدة افراد من أجل الاضرار بالبلد، وأيضا يمكن ان تتم هذه الجريمة بالإشادة بالأفعال الإرهابية التي ترتكب ضد الدولة عن طريق زراعة فيروسات مخربة.

ب-التجسس الالكتروني:

مع التطور الرقمي أصبح من السهل ان تقوم الأجهزة الاستخباراتية بعمليات التجسس للحصول على اسرار ومعلومات ومن تم افشائها لدول أخرى عادة تكون معادية او استغلالها بما يضر المصلحة الوطنية للدولة[2].

[1] عبد الصبور عبد القوي علي مصري، المرجع السابق، ص148.

[2] عبد الصبور عبد القوي علي مصري، المرجع نفسه، ص157.

فيمكن ان تتم جريمة التجسس الالكتروني عن طريق قرصنة المواقع الرئاسية وكذا الحكومية او اختراقها من اجل الاطلاع على اسرار الدولة سواء العسكرية او الاقتصادية.[1]

ثانيا: الجرائم الواقعة على النظام المعلوماتي: تنقسم هذه الجرائم الى:

1-الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

ان المقصود بالمكونات المادية للنظام المعلوماتي اي المعدات والأجهزة التي تستخدم في تشغيل النظام كالأقراص المدمجة واشرطة الكاسيت والكابلات، نظرا لطبيعة هذه الأجهزة تكون الجرائم المرتكبة ضدها جرائم تقليدية والتي تؤدي الى خسائر فادحة، كالسرقة، التدمير، الاحراق او الاضرار بمفاتيح التشغيل.

ويرى بعض فقهاء القانون ان سرقة وقت الالة يدخل ضمن هذا النوع من الجرائم، فيحدث أحيانا ان العاملين بالنظام المعلوماتي يلجؤون الى استخدام النظام المعلوماتي لأداء اعمال خاصة بهم، وعليه تكون السرقة منصبة على وقت الجهاز الذي يمكن تقييمها من حيث المال وليس على المكونات المادية[2].

2-الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

لقد ذكر المشرع الجزائري هذا النوع من الجرائم في المادة 394 مكرر من قانون العقوبات التي نصت على ما يلي (يعاقب بالحبس من ثلاثة 03 أشهر الى سنة وبغرامة من 50.000دج الى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك).

[1] خالد حسن احمد لطفي، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفكر الجامعي، الإسكندرية، 2019، ص38.

[2] سوبر سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الاجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011/2010، ص 40.

من خلال هذه المادة يتبين لنا انه تكون الجرائم الواقعة على المعلومة المعالجة اليا من خلال التلاعب فيها او اتلافها:

أ-التلاعب في المعلومات:

التلاعب اما ان يكون مباشرا او غير مباشرا.

-المقصود بالتلاعب المباشر هو ان يدخل المجرم معلومات بمعرفة المسؤول عن القسم المعلوماتي، بحيث يمكن للمجرم المعلوماتي من خلال هذا التلاعب ضم مستخدمين غير موجودين بالعمل وغايته من ذلك الحصول على رواتبهم، او الإبقاء على ملفات لأشخاص تركوا العمل للحصول على مبالغ مالية شهرية.

-اما التلاعب غير المباشر فيتم بإدخال غير مباشر للمعلومات المسجلة بالنظام المعلوماتي وذلك باستخدام التلاعب عن بعد، باستعمال أدوات معينة او معرفة ارقام الحسابات او مفاتيح الشفرة او أداة ربط بالمركز المعلوماتي لأي جهة[1].

ب-اتلاف المعلومات:

يعرف الإتلاف بأنه هو ذلك الفعل الذي يجعل الشيء غير صالح للاستعمال أو يعدم صلاحيته أو يعطله سواء بصفة كلية أو جزئية، ويتم اتلاف المعلومات اما بالطرق العادية كالحريق او السرقة او عن طريق استبدال او محو المعلومات.

يعتبر استبدال المعلومات جريمة من جرائم التزوير المعلوماتي الذي يعتبر من الجرائم الخطيرة لأنه في حالة ما إذا نجح يستمر مدة طويلة لاكتشافه وينجر عنه مكاسب كبيرة بمجرد استبدال رقم برقم اخر.

[1] سوبر سفيان، المرجع السابق، ص43.

كما يعتبر من أسهل طرق اتلاف المعلومات هو محوها، ذلك لان أثر الجريمة قد اندثر فكمثال عن ذلك: قام شخصان باختلاس مبلغ مالي يقدر ب 61.000 دولار مرسلة من شركة التامين الى أحد المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل[1].

3-الجرائم الواقعة على البرامج المعلوماتية:

تكون هذه الجرائم اما على مستوى البرامج التطبيقية او على مستوى برامج التشغيل:

أ-الجرائم الواقعة على البرامج التطبيقية:

تتحقق هذه الجرائم عن طريق تحديد البرنامج أولا ثم التلاعب به أو تعديله، ومثال ذلك قيام احد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتحصيل المبالغ الزائدة في حساب خاص به اعطى له اسم zzwick.

ان التلاعب بالبرنامج قد يأخذ عدة اشكال مثلا ان يقوم أحد المبرمجين بزرع برنامج غير مسموح به في البرنامج الأصلي، يسمح له ذلك البرنامج بالدخول غير مشروع في العناصر الضرورية لأي نظام معلوماتي.

ب-الجرائم الواقعة على برامج التشغيل:

تعتبر برامج التشغيل هي المسؤولة عن عمل النظام المعلوماتي، وذلك بقيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثال ذلك: جريمة تصميم برنامج وهمي يتم بواسطته تنفيذ الجريمة، هذا ما قامت به إحدى الشركات التأمين الأمريكية في مدينة لوس أنجلوس بواسطة مبرمجها

[1] سوبر سفيان، المرجع السابق، ص 44.

إذ قامت بتصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين والهدف من ذلك حصول هذه الشركة على عمولات من شركات التامين.[1]

الفرع الثاني دوافع ارتكاب الجريمة المعلوماتية:

من أبرز الدوافع لارتكاب الجريمة المعلوماتية:

أولا اثبات التفوق وتحقيق الشهرة:

يقوم بعض الأشخاص بارتكاب الجرائم المعلوماتية لإرضاء غرورهم من اجل اثبات قدرتهم على تحقيق النتيجة، بغض النظر عن الاضرار اللاحقة بالغير من جراء هذا التصرف وهو نوع من التفاخر والتعالي الذي يدفع اليه في بعض الأحيان التحدي او الرغبة في تحقيق المتعة

كما ان الشعور بالنقص يمكن ان يكون دافعا لارتكاب الجريمة المعلوماتية ليثبت المجرم المعلوماتي ان هذا النقص النفسي او الفسيولوجي الذي يعاني منه لا يعيقه عن التفوق في مجالات أخرى[2].

ثانيا الدافع المادي (الربح والكسب):

تعتبر الرغبة في تحقيق المكاسب المادية الكبيرة وفي زمن قياسي من اهم الأسباب التي تؤدي الى اقدام مجرمي المعلوماتية الى اقتراف جرائمهم، فاذا نجح المجرم في ارتكاب الجريمة المعلوماتية فان ذلك سيحقق له ارباحا هائلة ويمكن توضيح مدى الأرباح التي يحققها المجرم المعلوماتي من خلال ما رواه أحد المجرمين المحترفين في سجن كاليفورنيا بحث قال: (لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الامريكية وبإمكاني ان اكرر ذلك في أي وقت لقد كان شيئا سهلا فانا اعرف أسلوب عمل

[1] نمديلي رحيمة، خصوصية الجريمة المعلوماتية في القانون الجزائري والقانون المقارن، المؤتمر الدولي الرابع عشر، طابلس، 24.25 مارس2017، ص104.

[2] د. عميمر عبد القادر، المرجع السابق، ص 50.

جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن ان تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني)[1].

ثالثا الحصول على معلومات جديدة:

ان الكثير من مرتكبي الجريمة المعلوماتية يكون الدافع لارتكابهم هذه الجريمة هو حب الاطلاع والحصول على المعلومة، وهذا الدافع يعتبر حالة نفسية تصاحب مرتكب الجريمة وتدفعه لارتكابها اما بصورة متعمدة او غير متعمدة اين يرضي فضوله العلمي او النفسي ويشعر بالارتياح والطمأنينة بمجرد تحقيق الهدف بالوصول الى معلومات جديدة[2].

رابعا الرغبة في قهر النظام المعلوماتي:

يميل مرتكبو هذه الجريمة الى اظهار تفوقهم على وسائل التكنولوجيا الحديثة،[3] فالمجرم المعلوماتي حين يشعر بقهر النظام المعلوماتي يحقق نوعا من الانتصار النفسي اين يشعر بالفرح والسرور نتيجة اتيانه مثل هذا الفعل، وهنا يلبي المجرم حاجياته من خلال قهر النظام المعلوماتي[4].

خامسا الانتقام:

يعد الانتقام من بين الدوافع لارتكاب الجرائم بصفة عامة سواء تقليدية او معلوماتية، ففي الجرائم التقليدية يقوم المجرمون بالترصد لضحاياهم وضربهم او خطفهم او سرقتهم انتقاما من تصرفات قام بها هؤلاء الأشخاص، نفس الشيء يمكن القيام به عن طريق وسائل الاتصال الحديثة من طرف اشخاص يملكون معلومات عن خصومهم، والتي تكون في الغالب مؤسسات

[1] نهلا عبد القادر المومني، المرجع السابق، ص 90.

[2] صابر بحري منى خرموش، اهم الدوافع السيكولوجية وراء الجريمة الالكترونية، مجلة دراسات في سيكولوجية الانحراف، العدد01، الجزائر، 2021، ص49.

[3] نهلا عبد القادر المومني، المرجع نفسه، ص 91.

[4] صابر بحري منى خرموش، المرجع نفسه، ص50.

تعامل معها مرتكب الجريمة ووقع خصام بينهما مثل ان يكون عاملا فيها وتم فصله او تم أخذ حقه ...الخ فيقوم هذا الأخير باستغلال المعلومات التي تحصل عليها بمناسبة تعامله مع هذه المؤسسة والقيام بجريمته عن طريق حذف او تغيير معلومات او عن طريق زرع برامج خبيثة بها، من اجل تعطيلها او الحصول على معلومات واعطاءها لخصوم المؤسسة او مساومتها على ذلك، كما يمكن التشهير ضد مؤسسات او اشخاص من اجل الانتقام من تصرفاتهم[1].

سادسا التعاون والتواطؤ:

هذا الدافع في الغالب يكون بين متخصصين في المنظومة المعلوماتية، اين يتكفل شخص بالجانب الفني من المشروع الاجرامي واخر يكون من محيط او خارج مؤسسة المجني عليه، يقوم بتغطية عملية التلاعب، وكذا تحويل المكاسب المادية وعادة ما يتبادلون المعلومات حول نشاطهم بصفة منتظمة.

يجدر الإشارة بان دوافع ارتكاب الجريمة المعلوماتية ليست ثابتة لأن سلوك المجرم المعلوماتي ودوافع ارتكابه للجريمة قد تتحول بسرعة، فمثلا قد يكون دافع قيامه بهذه الجريمة هو محاولة قهر والتغلب على النظام المعلوماتي فيتحول هذا الدافع الى محاول تدمير النظام المعلوماتي او الحصول على أموال.

[1] د. عميمر عبد القادر، المرجع السابق، ص 51.

المطلب الثالث: أركان الجريمة المعلوماتية

تقوم الجريمة المعلوماتية على ثلاث اركان تتمثل فيما يلي:

الفرع الأول: الركن الشرعي

والذي يقصد به وجود نص قانوني يجرم الفعل ويوضع العقاب المترتب عليه في حالة وقوع الفعل، ففي إطار الجريمة المعلوماتية نصت المادة الأولى من قانون العقوبات الجزائري على انه (لا جريمة ولا عقوبة او تدبير امن بغير قانون).

وقد اجمع فقهاء القانون الجنائي على ضرورة سن نصوص قانونية يجرم من خلالها المشرع الانتهاكات والأفعال التي تقع على الأنظمة المعلوماتية او من خلالها[1].

لذا جرم المشرع الجزائري بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان (المساس بأنظمة المعالجة الالية للمعطيات) من المادة 394 مكرر الى 394 مكرر 7 من قانون العقوبات المعدل والمتمم.

كما جاء القانون 09-04 المتعلق بقواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها للحد من وقوع الجرائم المعلوماتية.

وبلجوء المشرع الى النص على هذه الجرائم، وجعلها في نطاق مبدا الشرعية يمنع بذلك القاضي من اللجوء الى القياس، بمعنى عدم جواز لجوء القاضي الجنائي الى قياس فعل لم يرد نص على تجريمه على فعل ورد نص بتجريمه.[2]

---

[1] د. عميمر عبد القادر، المرجع السابق، ص 87.

[2] حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 06 العدد 02، الجزائر، 2020، ص 173.

الفرع الثاني الركن المادي والمعنوي

أولا: الركن المادي

ان عناصر الركن المادي تختلف من جريمة الى أخرى، أي باختلاف نوع الجريمة فالجريمة الشكلية لا يتكون ركنها المادي الا من عنصر السلوك فقط، بينما الجريمة ذات النتيجة فان ركنها المادي يتكون من تلاث عناصر الا وهي السلوك والنتيجة والعلاقة السببية.[1]

وباستقراء النصوص القانونية المنظمة للجريمة المعلوماتية في قانون العقوبات الجزائري و بعض القوانين المقارنة، نلاحظ ان الجريمة المعلوماتية من الجرائم الشكلية، ذلك لان المشرع الجزائري لم يشترط ان تترتب نتيجة معينة بل اكتفى بتوفر السلوك المادي لقيام الجريمة المعلوماتية بغض النظر عن الضرر الذي تسبب فيه هذا السلوك للضحية، و الدليل على ذلك ان القانون يعاقب على مجرد الدخول الى المنظومة المعلوماتية دون ان يشترط حصول ضرر عن هذا الدخول بل جعل تحقيق النتيجة في الدخول و البقاء عن طريق الغش في المنظومة المعلوماتية كظرف مشدد و ليس شرط للعقوبة.

كما ان القانون يعاقب على مجرد الشروع في هذه الأفعال بنفس العقوبة المقررة للجريمة التامة ولا يعدو ان يكون الضرر مجرد ظرف مشدد للعقوبة او ان يكون محل لدعوى مدنية للمطالبة بالتعويض، ويجدر الإشارة على انه يختلف النشاط او السلوك في الجريمة المعلوماتية باختلاف نوع الجريمة المرتكبة فهناك جريمة ترتكب بواسطة المنظومة المعلوماتية وأخرى ترتكب ضد هذه المنظومة[2].

[1] د. عميمر عبد القادر، المرجع السابق، ص 89.

[2] د. عميمر عبد القادر، المرجع نفسه، 90.

ثانيا: الركن المعنوي

يعتبر الركن المعنوي ضروري لقيام أي جريمة فلا يكفي مجرد توفر الركن المادي للجريمة وانما يشترط القانون ان تكون هناك رابطة نفسية تربط الجاني بالفعل المادي الذي قام بارتكابه وهو ما يعرف بالركن المعنوي للجريمة فلا وجود لجريمة بدون توفر الركن المعنوي.

يتخذ الركن المعنوي في اغلب الجرائم صورة القصد الجنائي والذي يتحقق بتوافر إرادة بعمل غير شرعي لدى الجاني مع علمه بان القانون يجرمه[1]والقصد الجنائي قد يكون عام كما قد يكون خاص، فالمقصود بالقصد الجنائي العام هو الهدف المباشر للسلوك وينحصر في حدود ارتكاب الفعل، اما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه للجريمة بل يتأكد من تحقيق النتيجة مثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من ازهاق المجني عليه[2].

وعليه فإن الجريمة المعلوماتية تعد من الجرائم العمدية التي يكفي لقيامها توفر القصد الجنائي العام المتمثل في علم الجاني بعناصر الجريمة وارادته الى الحاق الضرر بالنفس او المال او البيانات المخزنة في الحاسوب، ولكن هذا لا يمنع من القول ان هناك بعض صور الجريمة المعلوماتية التي يتطلب فيها توفر القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنت[3].

[1]حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 02، الجزائر، 2020، ص 174.

[2] بوضياف اسمهان، المرجع السابق، ص 354.

[3]د. عميمر عبد القادر، المرجع السابق، ص91.

المبحث الثاني: الإثبات في الجرائم المعلوماتية

لقد عرفت محكمة النقض الاثبات بمعناه القانوني بانه (هو إقامة الدليل امام القضاء بالطرق التي حددها القانون فهو قوام الحق الذي يتجرد من قوته مالم يقم الدليل عليه) ويعني ذلك ان الاثبات في حقيقته هو البحث عن الدليل المتعلق بواقعة معينة وتقديمها للسلطات المختصة، فقد نتج عن الطبيعة الفنية والتقنية للجريمة المعلوماتية في مجال الاثبات الجنائي نوع جديد من الأدلة يطلق عليه الدليل الرقمي او الدليل الالكتروني وهو يختلف عن الدليل التقليدي وهذا يدعونا الى التطرق لتعريف الدليل الرقمي وخصائصه وانواعه وكذا الإجراءات المتبعة لجمعه وذلك من خلال المطالب الاتية:

المطلب الأول تعريف الدليل الرقمي وخصائصه: سنتطرق الى تعريف الدليل الرقمي في الفرع الأول اما الفرع الثاني فسنتناول فيه خصائص الدليل الرقمي.

الفرع الأول تعريف الدليل الرقمي:

يعود السبب في تسمية الدليل الرقمي بهذا الاسم اي (الرقمي) الى البيانات داخل العالم الافتراضي بجميع أنواعها، سواء كانت صورا او سجلات او نصوصا تأخذ اشكال ارقام (0-1) ويتم تحويلها عند عرضها الى صور او تسجيل او نص[1].

قام البعض بتعريف الدليل الرقمي على انه (الدليل الذي يجد له أساسا في العالم الافتراضي ويقود الى الجريمة) فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات والذي يؤدي الى اقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت[2].

[1] د. عميمر عبد القادر، المرجع السابق، ص 104.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص 177.

كما تم تعريف الدليل الرقمي بانه (الدليل المأخوذ من أجهزة الكومبيوتر والذي يكون في شكل مجالات او نبضات مغناطسية او كهربائية يمكن تجميعها وتحليلها بإستخدام برامج تطبيقات وتكنولوجيا وهو مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور او الأصوات او الاشكال والرسوم وذلك من اجل اعتماده امام أجهزة انفاذ وتطبيق القانون)[1].

ومن التعريفات السابقة يمكن القول: ان الدليل الرقمي هو (أي معلومات سواء كانت من صنع الانسان او تم استخلاصها من الحاسوب وبشكل يمكن قراءته او تفسيره من اشخاص لديهم مهارات في إعادة تشكيل المعلومات بمساعدة من برامج الكومبيوتر)[2].

الفرع الثاني خصائص الدليل الرقمي:

يتسم الدليل الرقمي بعدة خصائص تميزه عن الدليل التقليدي سنتناول بعض خصائصه على النحو التالي:

أولا الدليل الرقمي دليل علمي:

ان العناصر التي تكون الدليل الرقمي أي البيانات والمعلومات سواء كانت محملة او مخزنة او منقولة في صورة رقمية تتميز بانها ذات طبيعة غير ملموسة الشيء الذي يلزم لقراءة هذا النوع من الأدلة وجود أجهزة ومعدات الكترونية من نفس الطبيعة وكذلك استخدام برامج ونظم خاصة،[3] فما ينطبق على الدليل العلمي ينطبق كذلك على الدليل الرقمي فالدليل العلمي يخضع لقاعدة في القضاء المقارن وهي قاعدة (القانون مسعاه العدالة اما العلم فمسعاه الحقيقة)

[1] د. عميمر عبد القادر، المرجع السابق، ص 103.

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 178.

[3] د. عميمر عبد القادر، المرجع نفسه، ص 107.

فان كان الدليل العلمي يجب ان لا يتعارض مع هذه القاعدة العلمية فان الدليل الالكتروني له ذات القاعدة اذ لا يجب ألا يخرج الدليل الرقمي عما توصل اليه العلم الرقمي والا فقد معناه[1].

ثانيا الدليل الرقمي دليل تقني:

يعتبر الدليل الرقمي من طبيعة تقنية بحيث يستمد هذه الطبيعة من الوسط الذي يوجد فيه، ومن الآلات والأجهزة التي يستخلص منها الحاسوب أو أية منظومة معلوماتية أخرى، ولهذه الخاصية دلالات عديدة منها أنه لا يمكن فهم او الوصول إلى هذا النوع من الأدلة إلا من طرف اشخاص لهم معرفة وخبرة تقنية، كما أنه يمكن محو هذا النوع من الأدلة بسهولة ويسر، ولكن في بعض الأحيان قد يفقد الجناة السيطرة على مثل هذه الادلة لأنها ذات طبيعة ديناميكية تمكنه من التنقل من مكان لآخر عبر شبكات الاتصال، كما أنه يمكن أن يوفر نسخة أو نسخ أخرى إلى جانب النسخة الأصلية وهو ما دفع الفقهاء الى وصفه بأنه دليل لا يمكن اتلافه او اضاعته او تغييره، كما ان الطبيعة التقنية للأدلة الرقمية تتطلب ضرورة توفر معدات خاصة تستخدم لجمعها وتحليل محتوياتها واخضاعها لإجراءات معينة لتأكد من سلامتها من أي عبث او تلاعب[2].

ثالثا الدليل الرقمي دليل متنوع ومتطور:

يعتبر الدليل الرقمي دليل متنوع ذلك لأنه يتكون من كافة اشكال وأنواع البيانات الرقمية، فالدليل الرقمي بمثابة القالب الذي يتضمن مجموعة من البيانات الرقمية، هذه البيانات تتخذ مظاهر عديدة، كأن يكون محتوى البيانات الرقمية يتضمن صور سمعيات، مرئيات ونصوصا، كما ان هذه البيانات الرقمية التي يحتويها يمكن ان تكون منفردة او مجتمعة لكي تكون دليلا للإدانة او البراءة.

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 180

[2] د. عميمر عبد القادر، المرجع السابق، ص107.

كما ان الدليل الرقمي دليل متطور وهذا راجع لوجوده في بيئة متطورة بطبيعتها وذلك التطور يكون تلقائيا، فالعالم الرقمي ليس له نهاية كما انه ليس من السهل احتواءه، لهذا يعتبر الدليل الرقمي دليلا متطورا.

رابعا الدليل الرقمي يصعب التخلص منه:

ان هذه الخاصية من أحد اهم خصائص الدليل الرقمي، بحيث ان هذه الميزة يتمتع بها الدليل الرقمي دون غيره من الأدلة التقليدية، فنجد أنه يمكن التخلص بكل سهولة من الأدلة التقليدية كالأوراق والأشرطة المسجلة إذا كانت تحتوي على اعتراف شخص بارتكابه للجريمة، وذلك بتمزيقها مثلا او حرقها، كما انه يمكن التخلص من الشهود بقتلهم او تهديدهم بعدم الادلاء بالشهادة،[1] اما الدليل الرقمي فحتى لو تم إزالته من الجهاز يمكن استرداده وذلك بطرق معينة من قبل مختصين في عالم التقنية، كما يمكن حفظه على موقع معين كقوقل درايف بحيث يمكن الوصول الي الدليل بواسطة أي جهاز، فالقاعدة المتعلقة بهذه الخاصية هي انه كلما حدث اتصال تكنولوجيا المعلومات بإدخال بيانات فانه يصعب التخلص منها حتى ولو تم استعمال وسائل متطورة[2].

خامسا الدليل الرقمي دليل قابل للنسخ:

بحيث أنه من الإمكان استخراج نسخ من الدليل الرقمي وتكون هذه النسخ مطابقة تماما للأصل ولها نفس القيمة العلمية كما ان هذه الخاصية لا تتوفر في الأنواع الأخرى من الأدلة التقليدية وهي تشكل ضمانة للحفاظ على الدليل من الفقدان والتلف والتغيير[3].

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص182.

[2] فيصل ستوف العساف، سلطان سليمان الجداني، ماهية الدليل الرقمي في النظام السعودي: راسة مقارنة، الجريدة العالمية للقانون والدراسات السياسية، تاريخ النشر 15 افريل2023، ص59.

[3] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الاسكندرية، 2006، ص66.

المطلب الثاني: انواع الدليل الرقمي وشروط قبوله:

يتخذ الدليل عدة صور سنتعرف عليها من خلال الفرع الأول كما ان لقبول هذا الدليل يجب ان يتوفر فيه شروط سنتناولها في الفرع الثاني:

الفرع الأول أنواع الادلة الرقمية:

لقد قسم بعض الفقهاء الادلة الرقمية الى نوعين رئيسيين ألا وهما: ادلة رقمية لم تعد لتكون وسيلة إثبات وادلة رقمية اعدت لتكون وسيلة إثبات:

أولا: ادلة رقمية التي لم تعد لتكون وسيلة إثبات:

وهي الأدلة التي يتم تقديمها دون إرادة الشخص، أي هي الأثر الذي يتركه المستخدم أثناء استخدامه للكمبيوتر أو الإنترنت، بما في ذلك الرسائل التي أرسلها أو الرسائل التي استقبلها. يُطلق على هذا النوع من الأدلة اسم البصمة أو التتبع الرقمي، ومثال على ذلك:

البيانات والمعلومات الموجودة في ملفات السجل التي تحتوي على معلومات متضمنة ملفات الولوج log files، والتي تتضمن تاريخ ووقت تنزيل أو إرسال ملف المستخدم أو الملف الاحتياطي للنظام الذي يستخدم في حالة تعطل النظام او بيانات الكوكيز.

تكمن أهمية هذا النوع من الأدلة في انه قد يحمل معلومات تساعد في الكشف عن الجريمة ومرتكبها، كما ان هذا النوع من الأدلة يتميز انه يمكن ضبطه حتى ولو مرت فترات زمنية طويلة ذلك باستعمال برامج وتقنيات خاصة[1].

[1]بن طالب لندا، الدليل الالكتروني ودوره في الاتباث الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2019، ص 38.

ثانيا ادلة رقمية اعدت لتكون وسيلة اثبات:

يمكن اجمالها في:

1-السجلات التي تم انشاؤها تلقائيا بواسطة الحاسب الالي:

وهي عبارة عن مخرجات آلة الحاسوب وهذه المخرجات او السجلات لا يكون الانسان قد ساهم فيها، مثل: سجلات الهاتف وفواتير جهاز الحاسوب.

2-السجلات المختلطة:

المقصود من ذلك هو الملفات التي جزء منها تم حفظه بالإدخال، وجزء اخر تم إنشاؤه بواسطة الحاسوب، ومثال على ذلك: أوراق العمل المالية المدخلة والمعالجة من برنامج Excel. [1]

يبدو ان أهمية التمييز بين النوعين تكمن في ان النوع الأول لم يعد أصلا ليكون وسيلة اثبات لبعض الحقائق، أي لم يعد ليكون اثرا لمن صدر عنه، كما ان هذا النوع من الأدلة الرقمية يتم الحصول عليها باستخدام تقنيات خاصة تكون صعبة ومعقدة، اما النوع الثاني والذي يعتبر أكثر أهمية من النوع الأول ذلك لأنه يتم اعداده مسبقا كوسيلة اثبات لذا يتعمد حفظه للاحتجاج به لاحقا[2].

[1] د. عميمر عبد القادر، المرجع السابق، ص113.

[2] بن طالب لندا، المرجع السابق، ص38.

الفرع الثاني شروط قبول الدليل الرقمي:

لقبول الدليل الرقمي في الدعوى كأساس تشيد عليه الحقيقة يجب ان يتوفر على هذه الشروط:

أولا: يجب ان يكون دليل يقيني غير قابل للشك:

المقصود باليقين عبارة عن حالة ذهنية او عقلية تؤكد وجود الحقيقة، فالقاضي يمكنه ان يصل الى يقينية الدليل المقدم عن طريق المعرفة الحسية وذلك من خلال المعاينة وفحص الادلة المقدمة، وعن طريق كذلك المعرفة العقلية أي ان يقوم القاضي باستنتاج واستقراء لكي يصل الى الحقيقة التي يسعى اليها ويصدر حكمه بناءا عليها.

ثانيا: يجب الحصول على الدليل الرقمي بطريقة مشروعة:

تعرف المشروعية بانها (التوافق والتقيد بأحكام القانون في إطار ومضمونه العام، فهي تهدف الى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة وبالتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من اجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته)، لذا فمن ضروري ان تكون إجراءات الحصول على الدليل الرقمي تتفق مع الأنظمة القانونية والأنظمة الثابتة في وجدان المجتمع. وسنتعرض لهذه الإجراءات في المبحث الموالي.

ثالثا: أن يكون الدليل الرقمي له علاقة بموضوع الجريمة المعلوماتية:

وهذا الشرط تمت الإشارة اليه في قانون الاثبات الفيدرالي الامريكي تحديدا في المادة 407، وأطلقت عليه مبدا العلاقة الكاشفة، ان ثبوت العلاقة الكاشفة في الدليل الرقمي يتطلب ان يتطابق الدليل الرقمي المستخرج من الحاسب الالي للأصل المخزن بداخله[1]، بحيث لا يكون هناك ادعاء بأن البيانات غير صحيحة بسبب عدم دقة الحاسب الالي[2].

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 178-190.

[2] غانم مرضي الشمري، المرجع السابق، ص188.

رابعا: ان يكون الدليل الرقمي قابلا للمناقشة:

المقصود بهذا الشرط إلزامية مناقشة الدليل الجنائي، أي أن القاضي لا يمكن أن يؤسس قناعته إلا على الأدلة التي طرحت للمناقشة في جلسات المحاكمة، وتم عرضها للمناقشة أيضا على أطراف الدعوى، مما يعني أن الأدلة الرقمية مهما كانت طريقة الحصول عليها فإنها تعرض للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة.

كما تجدر الإشارة إلى أن القاضي لكي تكون له الهيمنة على هذا النوع من الدعاوى الجنائية فيجب أن يكون على علم بكيفية التعامل مع تقنية المعلوماتية حتى يضمن له هذا التأهيل نجاح مهمته[1].

المطلب الثالث: إجراءات جمع الدليل الرقمي لإثبات الجرائم المعلوماتية

يمكن تقسيم إجراءات الحصول على الدليل الرقمي الى إجراءات تقليدية سنتعرف عليها من خلال الفرع الأول واخرى حديثة سنتطرق اليها في الفرع الثاني.

الفرع الأول الإجراءات التقليدية لجمع الدليل الرقمي

من خلال هذا الفرع سنقوم باختصار دراسة الإجراءات التقليدية التي يعتمد عليها للحصول على الدليل الرقمي والمتمثلة في التفتيش، المعاينة، الضبط والخبرة بالإضافة الى الشهادة.

[1] ربيعي حسين، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة 1، 2016/2015، ص268.

أولا: التفتيش

لم يعرف المشرع الجزائري التفتيش الا ان معظم التشريعات أجمعت على ان المقصود بالتفتيش هو إجراء من إجراءات التحقيق الذي يهدف الى الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم المنسوب إليه التهمة، وقد عرف المجلس الأوروبي إجراء التفتيش في الجرائم المعلوماتية بأنه الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني[1].

1-شروط التفتيش في الجريمة المعلوماتية:

لقد حدد المشرع شروط وجب توافرها لإجراء التفتيش وهذه الشروط يمكن تقسيمها الى شروط موضوعية وأخرى شكلية والتي تتمثل في:

أ-الشروط الشكلية:

-وقت اجراء التفتيش:

لقد حدد المشرع الجزائري وقت اجراء التفتيش في المادة 47 من قانون الإجراءات الجزائية والتي نصت على انه (لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة 5 صباحا، ولا بعد الساعة الثامنة 8 مساءا الا إذا طلب صاحب المنزل ذلك او وجهت نداءات من الداخل او في الأحوال الاستثنائية ...) [2]غير ان بحسب الفقرة الثالثة من نفس المادة لا ينطبق هذا القيد على الجريمة المعلوماتية وبعض الجرائم الأخرى المذكورة في نص المادة بحيث ان التفتيش في هذا النوع من الجرائم يكون في أي زمان.

[1]زروقي عاسية، طرق الاتباث في ظل قانون الإجراءات الجزائية، اطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، تخصص قانون عام، جامعة الدكتور مولاي طاهر، سعيدة 2018/2017، ص 339.

[2]المادة 47 من قانون الإجراءات الجزائية.

-حضور بعض الأشخاص أثناء إجراء تفتيش نظم الحاسب الآلي

فالأصل ان يحضر المتهم او من ينوبه (شاهدين) اثناء التفتيش، إلا أن المشرع الجزائري في المادة 45 من قانون الإجراءات الجزائية قد استثنى مجموعة من الجرائم الخطيرة ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من قاعدة الحضور هذه، وهذا راجع لطبيعة الدليل الرقمي من حيث سرعة اتلافه.

-محضر تفتيش نظم الحاسب الآلي:

يجب تحرير محضر من خلاله يثبت ما تم من إجراءات وما تم الحصول عليه من أدلة، كما انه لم يتطلب القانون شكلا خاصا في محضر التفتيش وبالتالي ينطبق عليه ما ينطبق على المحاضر عموما، والتي تقتضي أن يكون مكتوبا باللغة العربية، ووضع تاريخ تحريره وأن يوقع فيه محرره، وأن يوجد فيه كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها، أما بالنسبة لمحضر تفتيش نظم الحاسب الآلي، فإنه يلتزم بالإضافة إلى الشكليات المذكورة من المستحسن ان يكون هناك شخص مختص في الحاسب الآلي يرافق قاضي التحقيق للاستعانة به.[1]

ب-الشروط الموضوعية:

-السبب:

ألا وهو وقوع الجريمة سواء جنحة او جناية، وان يوجه اتهام الى الشخص المراد تفتيشه او تفتيش مسكنه، والغاية من ذلك هو الحصول على دليل يفيد في الكشف عن الحقيقة.

-محل التفتيش:

محل التفتيش في الجريمة المعلوماتية هو الحاسب الالي بجميع مكوناته مادية كانت او معنوية وكذا شبكات الاتصال المتمثلة في مكونات الخادم والمزود الالي والملحقات التقنية.

[1] زروقي عاسية، المرجع السابق، ص342.

-السلطة المختصة بالتفتيش:

لقد اسند المشرع الجزائري إجراء تفتيش الحاسب الآلي الى سلطة التحقيق قاضي التحقيق واستثناءا النيابة العامة، إلاَ أنه يجوز لقاضي التحقيق إذا تعذر عليه القيام بهذه العملية ان ينيب ضباط الشرطة القضائية للقيام بإجراء التفتيش[1].

ثانيا المعاينة:

المعاينة هي اجراء استدلال او تحقيق الذي يهدف الى اظهار الحقيقة في جريمة وذلك لكشف عناصرها واركانها وجمع ادلة الاثبات فيها عن طريق مناظرة مكونات المكان الثابتة وموجوداته المنقولة من أجهزة وأدوات واثار ناشئة عن وقوعها[2].

ويقصد بها أيضا:(اثبات مباشر ومادي لحالة الشخص والأشياء والأمكنة ذات صلة بالحادث).

إن الجهة المكلفة بإجراء المعاينة هي الشرطة القضائية والتي بمجرد علمها بارتكاب جناية او جنحة، تنتقل الى مسرح الجريمة، إلا ان مسرح الجريمة المعلوماتية يختلف عن المسرح الخاص بالجريمة التقليدية كالقتل، بحيث ان الجريمة المعلوماتية تتكون من مسرحين:

1-مسرح تقليدي:

والذي يتكون من المكونات المادية للحاسب الآلي، كما يمكن أن يحتوي على اثار مادية كالأوراق، البصمات....

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 105.

[2] عبد الصبور عبد القوي علي مصري، المرجع السابق، ص 364.

2-مسرح افتراضي:

يحتوي على جميع البيانات والمعلومات الرقمية المخزنة في الحاسب الالي والتي من الممكن ان تساهم في الكشف عن الحقيقة[1].

تالثا الضبط:

يقصد به الحصول على أشياء ذات صلة بجريمة وقعت، هذه الأشياء تفيد في الكشف عن الحقيقة.

إلا ان الضبط في الجريمة المعلوماتية يختلف عن الضبط في الجرائم التقليدية، وذلك لان الأدلة المتحصل عليها جراء تفتيش النظم المعلوماتية، لا تشمل فقط المكونات المادية انما مكونات ذات طبيعة معنوية الا وهي البيانات، المراسلات والاتصالات الالكترونية، فإذا كان ضبط الأدلة المادية لا يثير اشكال مثل الحاسب الالي وملحقاته، فقد أثارت الطبيعة المعنوية للبيانات جدلا فقهيا واختلافا تشريعيا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبتة عليها[2]، انقسمت هذه الاختلافات الى اتجاهين:

الإتجاه الأول:

ذهب أصحاب هذا الاتجاه الى القول انه لا يمكن إجراء الضبط على الكيانات المنطقية للحاسوب لإنتفاء الكيان المادي عنها، وبالتالي لا تصلح البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية لعدم وجود الطابع المادي في هذه البيانات وذلك في حال تجردها عن الدعامة المادية.

[1]فلاك مراد، اليات الحصول على الأدلة الرقمية كوسائل اتباث في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، 2019، ص 210.

[2]زروقي عاسية، المرجع السابق، ص343.

الإتجاه الثاني:

يرى هذا الإتجاه أن البيانات المخزنة آليا والمجردة عن الدعامة المادية لا مانع أن تكون محلا للضبط[1].

وقد أخذ المشرع الجزائري بالاتجاه الثاني حيث نصت المادة 06 من القانون 09-04 على (عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية 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.)

رابعا الخبرة:

لم يقم المشرع الجزائري بتعريف الخبرة إلا ان البعض قام بتعريفها على انها اجراء يهدف الى استعمال قدرات شخص الفنية والعلمية التي لا تتوافر لدى رجل القضاء او المحقق من أجل الحصول على دليل قد يساهم في الكشف عن الحقيقة بشأن واقعة.

فقد اولى المشرع الجزائري اهتماما بالخبرة واعتبرها اجراء من إجراءات الحصول على الدليل ونظم اعمالها من المواد 143 الى 156 من قانون الاجراءات الجزائية.

وقد اسند المشرع الجزائري مهمة تعيين خبير الى جهات التحقيق والى المحكمة سواء من تلقاء نفسها او بناء على طلب الخصوم حيث نصت المادة 143 من قانون الإجراءات الجزائية على انه (لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم.)

[1] سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص 159.

تكمن أهمية الاستعانة بالخبير في مجال الجريمة المعلوماتية عند غيابه فقد لا تستطيع الضبطية القضائية الكشف عن الغموض في الجريمة وهذا راجع لنقص الكفاءة في التعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، مما قد يترتب عن ذلك تدمير او محو الدليل بسبب الإهمال.[1]

أنواع الخبراء المعلوماتيين:

-**المبرمج:** يكون مختص في كتابة أوامر البرامج بغض النظر إذا كانت برامج النظم او برامج التطبيقات، فالمتخصص في كتابة أوامر التطبيقات يكون على دراية بموصفات النظام الإداري المطلوب من محلل النظم، ويقوم بتحويل ذلك الى برامج الكترونية رقمية، اما المتخصص في كتابة برامج النظم فهو يقوم باختيار وتصحيح وكذلك تعديل برامج نظام الحاسب الالي الداخلية، التي تسيطر على وحدات الإدخال والإخراج.

-**المحلل:** وهو الذي يقوم بتحليل خطوات العمل وكذلك يقوم بتحليل بيانات نظام معين مثل ما هو الحال في نظم المعلومات الإدارية.

-**مهندس الصيانة والاتصال:** وهو المسؤول عن صيانة وفحص التقنيات الالكترونية الرقمية وشبكاتها.

-**مشغل الحاسب الالي:** هو المكلف بتشغيل الحاسب الالي ومكوناته، كما انه يملك خبرة في كتابة البرامج واستخدام أدوات إدخال البيانات.

-**مدير النظام المعلوماتي:** وهو المكلف بالإدارة في النظم المعلوماتية.[2]

[1] سعيداني نعيم، المرجع السابق، ص166.

[2] بن طالب لندا، المرجع السابق، ص77.

خامسا الشهادة:

تعرف الشهادة بانها (تقرير الفرد لما يكون قد سمعه او رآه او أدركه بالحواس) كما يقصد بالشاهد في الجريمة المعلوماتية هو ذلك الشخص الذي يملك خبرة معلوماتية ومتخصص في تقنية الحاسب الالي وشبكاته، ويسمى هذا النوع من الشهود بالشاهد المعلوماتي وذلك لكي يمكن التمييز بينه وبين الشاهد التقليدي.

ويشمل الشاهد المعلوماتي عدة طوائف من بينها:

- **القائمون على تشغيل الحاسب الآلي:** وهم الخبراء الذين تكون لهم دراسة بتشغيل جهاز الحاسب الآلي ومعدات متصلة به.

-**المحللون:** وهم الذين يقومون بتحليل الخطوات ويقومون ايضا بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة بغية استنتاج العلاقة الوظيفية بينها.

-**المبرمجون:** هم المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين الأولى هم مخططو برامج التطبيقات والثانية هم مخططو برامج النظام.

-**مهندسو الصيانة والاتصالات:** هم مسؤولين عن أعمال الصيانة الخاصة بالحاسب الالي وبمكوناته وشبكات الاتصال المتعلقة به.

-**مديرو النظم:** هو الشخص الذي توكل له مهمة أعمال الإدارة في نظم المعلوماتي[1].

[1] فلاك مراد، المرجع السابق، ص 216.

الفرع الثاني الإجراءات الحديثة لجمع الدليل الرقمي:

نظرا للتطور المستمر ولعدم كفاية الإجراءات التقليدية للوصول الى الادلة الرقمية استحدث المشرع الجزائري إجراءات أخرى للحصول على الأدلة، المتمثلة في التسرب واعتراض المراسلات وكذا مراقبة الاتصالات الالكترونية:

أولا: التسرب

1-**تعريف التسرب:** لقد عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 من قانون الإجراءات الجزائية على انه (قيام ضابط او عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم او شريك لهم او خاف...).

شروط التسرب: اشترط المشرع لإجراء التسرب ما يلي:

-الحصول على إذن من وكيل الجمهورية أو من قاضي التحقيق وان يكون هذا الاذن مكتوبا ومسببا والا كان هذا الاجراء باطلا بحسب نص المادة 65 مكرر15 من قانون الإجراءات الجزائية.

-يجب ان لا تتجاوز عملية التسرب أربعة أشهر.

-أن يكون هذا الإجراء في جرائم محددة في المادة 65 مكرر 05 من قانون الإجراءات الجزائية والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية.[1]

بالتالي يمكن ان نقول ان اجراء التسرب في الجريمة المعلوماتية يكمن في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم

[1] سعيداني نعيم، المرجع السابق، ص176.

مستخدما في ذلك أسماء وهمية أو صفات مستعارة الهدف من ذلك الاستفادة منهم والحصول على ادلة للكشف عن الحقيقة. [1]

ثانيا اعتراض المراسلات:

لم يعرف المشرع الجزائري اجراء اعتراض المراسلات واكتفى بتنظيمه في المواد من 65 مكرر 05 الى المادة65 مكرر 10من قانون الإجراءات الجزائية، باستقراء نص المادة 65 مكرر 05 نجد انه المقصود (باعتراض المراسلات، اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج، التخزين والتوزيع، كما انها قابلة أيضا للاستقبال والعرض) وقد وسعت المادة 2 فقرة (و) من القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال من المفهوم التقليدي لاعتراض المراسلات وادخلت الاتصالات الالكترونية ذلك تماشيا مع التطور في مجال التكنولوجيا حيث نصت على (أي تراسل او ارسال او استقبال علامات او إشارات او كتابات او صور او أصوات او معلومات مختلفة بواسطة أي وسيلة الكترونية).

1-شروط اعتراض المراسلات: لقد وضع المشرع الجزائري جملة من الشروط للقيام باعتراض المراسلات وهي شروط شكلية وأخرى موضوعية:

أ-الشروط الشكلية:

-الحصول على اذن قضائي:

بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية الاذن يكون صادر من وكيل الجمهورية، وفي حالة فتح تحقيق قضائي الاذن يصدر من قاضي التحقيق، قد نص المشرع في المادة 65 مكرر 07 من قانون الإجراءات الجزائية على بعض شروط في الاذن وهي:

[1] سعيداني نعيم، المرجع السابق، ص 177.

-أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

-أن يكون مكتوبا تحت طائلة البطلان، ذلك لأن الأصل في العمل الإجرائي الكتابة.

-أن يسلم لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

-ان يكون مصدره مختصا نوعيا ومكانيا أصلا بالبحث او التحقيق في الجريمة التي صدر الاذن بشأنها.

محضر العمليات:

اشترط المشرع الجزائري في المادة 65 مكرر 9 على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص أن يحرر محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري يذكر بالمحضر أيضا تاريخ وساعة بداية هذه العملية وكذا نهايتها.

كما اوجب عليه في المادة 65 مكرر 10 نسخ او وصف الصور والمراسلات والمحادثات المسجلة والمفيدة في إظهار الحقيقة كمرفقات تودع بالملف، وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم[1].

[1]صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكاديمية للبحث القانوني، العدد1، جامعة بجاية،2010، ص 68.

القائم باعتراض المراسلات:

يقوم بعمليات الاعتراض والالتقاط والتسجيل ضابط الشرطة القضائية، كما يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية المناب أن يسخر كل عون مؤهل لدى مصلحة أو وحدة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5.

ب-الشروط الموضوعية: تتمثل هذه الشروط في:

السبب:

يعتبر التسبيب أساس العمل القضائي، فهو واجب عند إصدار الإذن بإجراء عمليات اعتراض المراسلات سواء من طرف وكيل الجمهورية أو قاضي التحقيق.

نوع الجريمة:

لقد حدد المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجرائم التي يتم فيها اجراء اعتراض والالتقاط والتسجيل، ومن هذه الجرائم، الجرائم الماسة بأنظمة المعالجة الالية للمعطيات.[1]

2-طريقة اعتراض المراسلات في الجريمة المعلوماتية:

يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني، ومن ثم فعملية الاعتراض تنصب عليه، وذلك من خلال المعلومات الموجودة في حاشية رسالة البريد الالكتروني E-mail header، حيث يحتوي على عنون IP المرسل للرسالة وهذا العنوان

[1] صالح شنين، المرجع السابق، ص 69.

يحتوي على معلومات تتمثل في الحاسوب الذي تم بواسطته ارسال الرسالة، وكذا الموقع الجغرافي الذي أرسلت منه ومعلومات مزود الخدمة الذي يتعامل معه الذي أرسل الرسالة.[1]

ثالثا: مراقبة الاتصالات الالكترونية

لقد إستحدث المشرع الجزائري إجراء المراقبة الالكترونية بموجب المادة الثالثة من القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

ولم يقم بتعريف اجراء مراقبة الاتصالات الالكترونية، الا ان الفقه قد عرفه على أنه (مراقبة شبكة الإتصالات، أو هو ذلك العمل الذي يقوم به المراقب بإستعمال التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر)[2].

1-شروط القيام بإجراء مراقبة الاتصالات الالكترونية:

الحصول على إذن:

لا يجوز مراقبة الاتصالات الالكترونية إلا بناء على إذن من جهة مختصة قانونا بإصداره، وإلا كان إجراء غير مشروع، وقد خول المشرع الجزائري اصدار الاذن الى السلطة القضائية أي قضاة النيابة العامة والتحقيق والحكم.

الجرائم التي يجوز فيها المراقبة الالكترونية:

لقد حدد المشرع الجزائري في المادة الرابعة الجرائم التي تسمح باللجوء إلى المراقبة الالكترونية ومن بينها: الوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وكذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني.

[1] سعيداني نعيم، المرجع السابق، ص182.

[2] سعيداني نعيم، المرجع نفسه، ص 183.

-وقد حددت الفقرة (ج) من المادة الرابعة من القانون السالف الذكر حالتين اذ توفرت يمكن اللجوء إلى إجراء مراقبة الاتصالات الالكترونية، وهي:

-إذا اقتضت التحريات والتحقيقات القضائية ذلك.

-حين يكون من الصعب الوصول إلى نتيجة دون اللجوء إلى المراقبة الالكترونية.

كما ان المشرع الجزائري لم يذكر الوسائل التي يتم استعمالها لإجراء المراقبة الالكترونية الا ان بعض الفقهاء ذهبوا لتحديد الوسائل المستعملة لإجراء مراقبة الاتصالات الالكترونية تتمثل في:

-استعمال ما يطلق عليه بقلم التسجيل او يسمى أيضا بالفخ والمتابعة، ومن خلال هذا القلم يتم تسجيل أسماء الذين يتراسلون مع المتهم أي مع بريده الالكتروني او مع من يقوم بالمحادثة الفورية.

-استخدام وسائل التنصت على مضمون الرسالة الالكترونية او المحادثة الفورية الالكترونية.

في الأخير يمكننا القول ان إجراءات جمع الدليل الرقمي سواء الحديثة او التقليدية، إذا تضافرت وتحققت في الدليل، وكانت طبقا للشروط القانونية، اعتبر الدليل الرقمي دليلا مشروعا لإثبات الواقعة القانونية[1].

[1] زروقي عاسية، المرجع السابق، ص351.

خلاصة الفصل الأول:

من خلال دراستنا لماهية الجريمة المعلوماتية نستخلص انها من الجرائم المستحدثة التي عرفت انتشارا كبيرا في الآونة الأخيرة، فبرغم من ان الفقهاء لم يجمعوا على تعريف واحد للجريمة المعلوماتية، الا انه يمكن تعريفها بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية، او من داخل نظام حاسوب وتشمل جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية.

كما ان الجريمة المعلوماتية لها مميزات تجعلها تختلف تماما عن الجرائم التقليدية من بين المميزات انها جريمة عابرة للحدود وهي جريمة تقنية مرتبطة بالتطور التكنولوجي، وقد لاحظنا من خلال دراستنا لصور الجريمة المعلوماتية انها ليست محصورة في نوع معين بل لها أنواع كثيرة، ولا يمكن قيام هذا النوع من الجرائم الا إذا توفرت على اركان والمتمثلة في الركن الشرعي، الركن المادي والمعنوي.

كما ان الاتباث في الجريمة المعلوماتية يختلف أيضا عن الجرائم التقليدية بحيث ان اثباتها يكون بواسطة دليل خاص بها يسمى بالدليل الرقمي او الدليل الالكتروني ويتم الحصول عليه اما بإجراءات تقليدية كالتفتيش، المعاينة، الضبط، الخبرة او إجراءات حديثة كالتسرب، اعتراض المراسلات، مراقبة الاتصالات الالكترونية.

الفصل الثاني: مواجهة الجريمة المعلوماتية في التشريع الجزائري

الفصل الثاني: مواجهة الجريمة المعلوماتية في التشريع الجزائري

لقد تزايدت معدلات ارتكاب الجريمة المعلوماتية ذلك بسبب التطورات الهائلة لتكنولوجيا المعلومات، بحيث أصبح من السهل ارتكاب هذا النوع من الجرائم، ذلك لأنها لا تترك آثار مادية، كما ان الجريمة المعلوماتية لا تستغرق وقت كبير لارتكابها وهدا الذي جعلها صعبة الاتباث كما قلنا سابقا، لذا فقد سارع اغلب مشرعي العالم لوضع هياكل وكذا قوانين لمعاقبة مجرمي المعلوماتية وكذا حماية معطيات الحاسب الآلي وقد ساير المشرع الجزائري مشرعي العالم حيث حاول احتواء هذا النوع من الجرائم بوضع ضوابط للتصدي لها، وهو ما سنتطرق اليه في هذا الفصل.

حيث سنتناول الضوابط التشريعية لمواجهة الجريمة المعلوماتية في المبحث الأول.

اما المبحث الثاني فسيتضمن الضوابط العملية لمواجهة الجريمة المعلوماتية.

المبحث الأول: الضوابط التشريعية لمواجهة الجريمة المعلوماتية

امام هذا الانتشار الواسع للجريمة المعلوماتية لم يقف المشرع الجزائري مكتوف الايدي وانما قام بمواجهة هذه الجريمة من خلال وضع نصوص قانونية المتمثلة فيما يلي:

المطلب الأول: مواجهة الجريمة المعلوماتية في ظل قانون العقوبات

لقد حاول المشرع الجزائري التصدي للجريمة المعلوماتية وذلك بتجريم المساس بأنظمة المعالجة الالية للمعطيات من خلال المواد من 394 مكرر الى 394 مكرر7 بموجب قانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 66-156 المتضمن قانون العقوبات[1]، وقد ادرج عليه تعديل سنة 2006 بموجب القانون 06-23،[2] بحيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الالية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال، في هذا المطلب سنتعرف على صور جرائم المساس بأنظمة المعالجة الالية للمعطيات في قانون العقوبات الجزائري و ذلك في الفرع الأول اما الفرع الثاني فسنتطرق الى العقوبات المقررة لهذه الجرائم[3].

[1] قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية، العدد 71.

[2] قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية، العدد 84.

[3] درار عبد الهادي، اليات التصدي للجريمة الرقمية في التشريع الجزائري، المجلة العصرية للدراسات القانونية، جامعة أبو بكر بلقايد، تلمسان، المجلد 01، العدد 02، 2023، ص 258.

الفرع الأول: صور جرائم المساس بأنظمة المعالجة الالية للمعطيات في قانون العقوبات

تتخذ جرائم الاعتداء على المنظومة المعلوماتية في قانون العقوبات الجزائري الصور الاتية: الدخول والبقاء غير مرخص في المنظومة المعلوماتية، المساس بمنظومة المعلوماتية، كما تتضمن صور أخرى سنتعرف عليهم من خلال هذا الفرع.

أولا: الدخول والبقاء غير مرخص في المنظومة المعلوماتية

1-الدخول غير مرخص في المنظومة المعلوماتية:

يقصد بالدخول غير مرخص لمنظومة المعالجة الالية للمعطيات، الولوج عن طريق الغش بهدف الوصول الى معلومات وبيانات مخزنة في هذه المنظومة، ويتحقق الدخول اليها من خلال التعدي سواء بطريقة مباشرة او غير مباشرة، ومهما كانت الوسيلة المستعملة سواء بإستعمال كلمة مرور صحيحة إذا كان الدخول غير مخول لاستخدامها، او عن طريق شفرة خاصة او برامج، سواء كان ذلك عن طريق شبكة المعلومات او باستعمال الحاسوب او الهواتف الذكية، وغيرها من وسائل الاتصال[1].

ويكون الدخول المباشر عن طريق الضغط على زر الدخول، ويمكن ان يتحقق ذلك في حالة إذا لم يقم صاحبة المنظومة المعلوماتية بإغلاقها او لم يضع كلمة السر للدخول اليها، لذا فيمكن الدخول اليها بكل سهولة للوصول الى الملفات الموجودة داخل المنظومة، إلا انه يمكن ان تكون تلك الملفات محمية بكلمة السر، في هذه الحالة نكون أمام محاولة الدخول وهي جريمة معاقب عليها.

[1] د. عميمر عبد القادر، المرجع السابق، ص64.

اما الدخول غير المباشر فيمكن أن يكون عن طريق التعرف على كلمة السر باستخدام برامج مخصصة او عن طريق تجريب عدة كلمات سر الى غاية الوصول الى كلمة السر المستعملة، وكذلك يمكن استغلال الثغرات الأمنية أي ان يخترق المنظومة المعلوماتية، كما يمكن الدخول أيضا عن طريق انتحال الهوية من خلال سرقة هوية شخص اخر والوصول الى البيانات والمزايا الخاصة به[1].

قد نص المشرع الجزائري على الدخول غير مشروع في المادة 394 مكرر من قانون العقوبات.

2-البقاء غير مرخص في المنظومة:

يقصد به بقاء الشخص داخل نظام المعالجة ملك لشخص اخر بعد دخوله اليه رغم معرفته ان بقاءه فيه غير مرخص، او بمعنى اخر استمرارية التواجد داخل نظام المعالجة دون اذن من صاحبه او من يملك السيطرة عليه[2].

قد نص المشرع الجزائري على جريمة البقاء غير المرخص كذلك في المادة 394 مكرر من قانون العقوبات ففعل البقاء يتم بعد الدخول غير المرخص أكثر من الوقت المحددة، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، ويجرم البقاء حتى ولو تم بصفة عرضية[3].

تانيا: جريمة المساس بالمنظومة المعلوماتية

تنص المادة 394 مكرر 1 بمعاقبة كل من يقوم بإدخال معطيات الى نظام المعالجة الالية، او يقوم بإزالة هذه المعطيات او تعديلها وذلك عن طريق استعمال الغش.

---

[1] د.عميمر عبد القادر، المرجع السابق، ص65.

[2] راضية عيمور، المرجع السابق، ص 100.

[3] احسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة06، دار هومة، الجزائر، 2007، ص 445.

إذا فهذا السلوك يتجسد في الصور التالية: الإدخال، المحو، التعديل، يكفي ان يصدر أحدهم من الجاني أي ان المشرع الجزائري لم يشترط ان تكون هذه الصور مجتمعة.

كما ان أفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات، وذلك اما بإضافة معطيات جديدة لا يحتويها نظام المعالجة الالية للمعطيات، او محو او تعديل معطيات موجودة من قبل.

يعتبر هذا السلوك ايضا تجسيدا لفعل افساد وتخريب المعطيات التي يحتويها نظام المعالجة الالية، مثل ادخال فيروس في برامج من اجل اتلافها.

تالثا: صور أخرى

لقد جرمت المادة 394 مكرر2 من قانون العقوبات الجزائري الأفعال التالية:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.

-كما جرم المشرع الجزائري كذلك حيازة أو إفشاء أو نشر أو استعمال المعطيات التي تم الحصول عليها من إحدى جرائم الغش المعلوماتي لأي غرض[1].

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012، ص 185.

الفرع الثاني: العقوبات المقررة لجرائم المساس بأنظمة المعالجة الألية للمعطيات

أولا: العقوبات الأصلية

لقد نص القانون 04-15 على عقوبات أصلية لجرمتي الدخول والبقاء غير مشروع في المنظومة المعلوماتية وكذلك جريمة المساس بالمنظومة المعلوماتية، كما يلي:

1-عقوبة الدخول والبقاء غير مشروع في المنظومة المعلوماتية:

تنص المادة 394 مكرر من قانون العقوبات (يعاقب بالحبس من ثلاثة 03 أشهر الى سنة وبغرامة من 50.000دج الى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك).

كما نصت الفقرة الثانية والثالثة من المادة 394 مكرر على تشديد عقوبة الدخول والبقاء غير المشروع كما يلي (تضاعف العقوبة إذا ترتب على ذلك الفعل حذف او تغيير لمعطيات المنظومة

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة 6 أشهر الى سنتين 2 والغرامة من 50.000 الى 150.000 دج)[1].

2-عقوبة المساس بمنظومة المعلوماتية:

نصت عليها المادة 394 مكرر 1 من قانون العقوبات كالتالي (يعاقب بالحبس من ستة 6 أشهر الى ثلاث 3 سنوات وبغرامة مالية من 500.000 دج الى 2.000.000 كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية او أزال او عدل بطريق الغش المعطيات التي يتضمنها).

[1] المادة 394 مكرر من قانون العقوبات الجزائري.

وكذلك نصت المادة 394 مكرر2 يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة مالية من 100.000دج إلى 500.000دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم

2-حيازة أو إفشاء أو نشر او إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[1].

ثانيا عقوبة الشخص المعنوي:

نصت المادة 394مكرر 04 عن العقوبات الواجبة التطبيق على الشخص المعنوي إذا ارتكب أي جريمة اعتداء على نظام المعالجة الألية للمعطيات والعقوبة تتمثل في: غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

تالثا: عقوبة الاشتراك والشروع في الجريمة

نصت المادة 394 مكرر5 على **عقوبة الاشتراك** في الجريمة بقولها (كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها).

[1] المادة 394 مكرر 1 و2 من قانون العقوبات الجزائري.

اما **الشروع في الجريمة** فقد نصت على عقوبته المادة 394 مكرر7 بقولها (يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها)[1].

رابعا: العقوبات التكميلية

نصت المادة 394 مكرر6 على عقوبات تكميلية والتي تتمثل في:

1-المصادرة :

تشمل الأجهزة والبرامج والوسائل المستعملة في ارتكاب جريمة من جرائم المساس بالأنظمة المعلوماتية مع مراعاة حقوق الغير وحسن النية.

2-اغلاق المواقع:

يتعلق الامر بالمواقع التي تكون محلا لجريمة من جرائم المساس بالأنظمة المعلوماتية.

3-اغلاق محل او مكان الاستغلال:

إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال عن ذلك اغلاق مقهى الكتروني الذي ترتكب في هذا النوع من الجرائم بشرط ان يكون مالكه على علم بهذه الجريمة[2].

[1]خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، 2010، ص ص101-100.

[2]د. فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، اعمال المؤتمر الدولي الرابع عشر الجرائم الالكترونية، بتاريخ 29-03-2017، ص129.

المطلب الثاني: مواجهة الجريمة المعلوماتية في ظل قانون الإجراءات الجزائية والقواعد الخاصة بحقوق المؤلف والحقوق المجاورة:

اولا سنتطرق الى مكافحة الجريمة المعلوماتية في قانون الإجراءات الجزائية وهذا في الفرع الأول، اما في الفرع الثاني فسنتعرض الى مواجهة الجريمة المعلوماتية في القواعد الخاصة بحقوق المؤلف والحقوق المجاورة.

الفرع الأول: مواجهة الجريمة المعلوماتية في قانون الإجراءات الجزائية

لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لكي يتماشى مع التطور الذي لحق بالجريمة المعلوماتية، بحيث قام ب:

أولا: تمديد الاختصاص المحلي للمحكمة

قام المشرع الجزائري بتعديل المادة 329 من قانون الإجراءات الجزائية وذلك (بجواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الالية للمعطيات...) وجاء هذا التعديل عقب المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.[1]

ثانيا: تمديد الاختصاص المحلي لوكيل الجمهورية

لقد حددت الفقرة الأولى من المادة 37 من قانون الإجراءات الجزائية المعدل والمتمم اختصاص وكيل الجمهورية في مكان وقوع الجريمة، أو في محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى

[1] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر،2011، ص174.

لو حصل هذا القبض لسبب آخر، غير ان المشرع الجزائري وفي إطار مواجهة الجريمة المعلوماتية عمل على تعديل نصوص قانون الإجراءات الجزائية، لكي تكون ملائمة مع خصوصية الجريمة المعلوماتية، حيث قام بتعديل المادة 37 من قانون الإجراءات الجزائية بموجب القانون 14-04 المؤرخ في 10 نوفمبر 2004 وأضاف اليها فقرة ثانية تنص على جواز تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى، اذا كان الامر يتعلق بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات، الإرهاب، تبييض الأموال وجرائم الصرف[1].

ثالثا: العمل بنظام المشروعية في تحريك الدعوى العمومية

يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144مكرر 1 و144 مكرر 2 من قانون العقوبات المعدل والمتمم بالقانون 09/01.

رابعا: إضافة الى ذلك فقد أدرك المشرع الجزائري انه لمواجهة للجريمة المعلوماتية لابد أيضا من **إرساء قواعد إجرائية وقائية وتحفظية**، التي من شأنها ان تتفادى وقوع الجريمة المعلوماتية او الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها منها قواعد تقليدية كالتفتيش، المعاينة، الضبط الخبرة.

[1] امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر، الجزائر،2006، ص56.

بالإضافة الى إجراءات مستحدثة تتمثل في اعتراض المراسلات وكذلك التسرب وقد تطرقنا الى هذه الإجراءات التي تعتبر إجراءات وقائية وفي نفس الوقت إجراءات لجمع الدليل الرقمي في المبحث الثاني من الفصل الأول[1].

كما اقر المشرع الجزائري **إجراء الوقف للنظر** في الجريمة المعلوماتية وذلك في المادة 51 التي نصت على (إذا رأى ضابط الشرطة القضائية لمقتضيات التحقيق، ان يوقف للنظر شخصا او أكثر ممن اشير إليهم في المادة 50، فعليه ان يطلع وكيل الجمهورية بذلك ويقدم تقريرا عن دواعي التوقيف للنظر... ويمكن تمديد اجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص مرة واحدة عندما يتعلق الامر بجرائم الاعتداء على أنظمة المعالجة الالية للمعطيات)[2].

الفرع الثاني: مواجهة الجريمة المعلوماتية في القواعد الخاصة بحقوق المؤلف والحقوق المجاورة:

اعتبر المشرع الجزائري برنامج الحاسوب الالي ضمن المصنفات الأدبية والفنية، بحيث نصت المادة الرابعة من الامر 03-05 المؤرخ في19-07-2003، المتعلق بحقوق المؤلف والحقوق المجاورة على (تعتبر على الخصوص كمصنفات أدبية او فنية محمية ما يأتي:

ا-المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات، والقصص، والقصائد الشعرية، وبرنامج الحاسوب، والمصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها.....)[3].

[1] راضية عيمور، المرجع السابق، ص 103.

[2] سميحة بلقاسم، حميد بوشوشة، الجريمة الالكترونية بعد جديد للإجرام في الجزائر واقعها واليات مجابهتها، مجلة العلوم الإنسانية لجامعة ام بواقي، المجلد 10، العدد 01، جوان 2023، ص 543.

[3] زبيحة زيدان، المرجع السابق، ص88.

وقد تضمنت المواد من 151 الى 160 من الامر 03-05 الجرائم المعلوماتية التي تمس حقوق المؤلف والحقوق المجاورة نذكر:

أولا: يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الاتية:

-الكشف غير مشروع للمصنف او المساس بسلامة مصنف او أداء لفنان مؤد او عازف.

-استنساخ مصنف او أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.

-استيراد او تصدير نسخ مقلدة من مصنف او أداء.

-بيع نسخ مقلدة لمصنف او أداء.

-تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف او أداء، هذا ما نصت عليه المادة 151 من الامر 03-05.

ثانيا: يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الامر فيبلغ المصنف او الأداء عن طريق التمثيل او الأداء العلني، او البث الإذاعي السمعي او السمعي البصري، او التوزيع بواسطة الكبل او بأية وسيلة نقل أخرى لإشارات تحمل أصواتا او صورا واصواتا او باي منظومة معالجة معلوماتية، هذا بحسب نص المادة 152[1].

ثالثا: العقوبات المقررة لجريمة التقليد:

يمكن تقسيم هذه العقوبات الى قسمين:

1-**عقوبات أصلية:** والتي تشمل عقوبات بسيطة وأخرى مشددة.

[1] الامر رقم03-05، الصادر بتاريخ 19 يوليو2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44.

أ-العقوبات البسيطة:

يعاقب مرتكب جنحة التقليد لمصنف او أداء، مثل ما ورد في المادتين 151-152 من الامر 03-05، بالحبس من ستة أشهر الى ثلاثة سنوات، وبغرامة من 500.000 الى 1.000.000 دينار جزائري، سواء كان النشر قد حصل في الجزائر او خارجها طبقا للمادة 153 من الامر نفسه.

كما نصت المادة 154 من الامر 03-05، على معاقبة الشريك في ارتكاب جريمة التقليد سواء بأعماله او بالوسائل التي يحوزها للمساس بحقوق المؤلف بنفس العقوبة المقررة في المادة 153 السابقة الذكر.

وأيضا قد نصت المادة 156 من الأمر 03 -05 على انه يعاقب بنفس العقوبة المقررة في المادة 153، كل من يمتنع عن دفع المكافأة المستحقة للمؤلف.

ب-العقوبة المشددة: شدد المشرع العقوبة في حالة العودة، الى ضعف العقوبة المنصوص عليها في المادة 153 من الامر 03-05.

2-العقوبات التكميلية: تكمن هذه العقوبات في

أ-مصادرة المبالغ:

نصت المادة 157 من الامر 03-05 على مصادرة المبالغ سواء المبالغ التي تمثل الإيرادات الناتجة عن الاستغلال غير شرعي للمصنف او أداء محمي، واتلاف العتاد الذي أنشئ لمباشرة النشاط غير المشروع وكل النسح المقلدة، [1]وقد حددت المادة 159 الجهة التي يؤول اليها الأموال والوسائل المصادرة، بحيث يتم تسليمها للمؤلف او مالك الحقوق او ذوي حقوقهما، فذلك بمثابة تعويض عن ضرر الذي لحق بهم.

[1]المادة 157 من الامر 03-05، السابق الذكر.

ب-الغلق المؤقت:

يكون الغلق لمدة لا تتجاوز ستة أشهر لمؤسسة يستغلها المقلد او شريكه، وأن يكون الغلق نهائي عند الانقضاء بالموازاة مع حجم الخسائر او الجريمة المرتكبة.

ج-نشر ملخص حكم:

أي التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، تكون هذه العقوبة بطلب من الطرف المدني طبقا لنص المادة 158 من الامر 03-05، ويتحمل المحكوم عليه نفقات ذلك على ان لا تتعدى المصاريف قيمة الغرامة المحكوم بها[1].

المطلب الثالث: مواجهة الجريمة المعلوماتية في تنظيمات وقوانين أخرى:

إضافة الى قانون العقوبات وكذا قانون الإجراءات الجزائية والقواعد الخاصة بحقوق المؤلف والحقوق المجاورة، حاول المشرع الجزائري ايضا محاربة الجريمة المعلوماتية من خلال قوانين خاصة أخرى، تتمثل في:

الفرع الأول: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها:

لمواكبة التطور الذي عرفته الجزائر في مجال التقنية والتكنولوجيا أصدر المشرع الجزائري قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، بحيث تظهر أهمية هذا القانون في انه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وكذلك بين القواعد الوقائية التي يمكن من خلالها الكشف المبكر للاعتداءات المحتملة والتدخل لتحديد مصدرها والتعرف على الشخص الذي ارتكبها[2].

---

[1] بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، جامعة الجزائر 01-بن يوسف بن خدة، 2018/2017، ص149.

[2] فاروق خلف، الأليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني، الجزائر، 2015، ص18.

حيث جاء هذا القانون بأحكام خاصة بالجريمة المعلوماتية تتمثل في:

-النص على مراقبة الاتصالات الإلكترونية في المادة 4 من القانون 09-04، اذ ان المشرع الجزائري قد تبنى هذا الإجراء برغم ان الدستور الجزائري يضمن سرية المراسلات والاتصالات بكل أشكالها في المادة 39 منه، وهذا لخطورة بعض الجرائم المعلوماتية المحددة.

لقد بينت المادة الرابعة من القانون 09-04 الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر وهذه الحالات هي:

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

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

ج-لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الالكترونية.

د-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

-تسجيل الاتصالات الإلكترونية في حينها.

-القيام بإجراءات التفتيش والحجز للمنظومة المعلوماتية.

-وقد نصت المادة 16 من القانون 09-04 على انه (في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات القضائية المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكل الكتروني)[2]

[1] المادة الرابعة من القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 05 اوت 2009، الجريدة الرسمية، العدد 7.

[2] المادة 16من القانون 09-04، السابق الذكر.

اذ يستخلص من هذه المادة ان المشرع نص على إمكانية تبادل المساعدات القضائية على المستوى الدولي لضمان نجاح عمليات التحقيق والتحريات لمواجهة الجرائم المعلوماتية.
الا ان المادة 18من القانون 09-04 ذكرت الحالات التي لا تجوز فيها عملية المساعدة القضائية الدولية تتمثل هذه الحالات في:

-إذا كانت هذه المساعدة القضائية تمس بالسيادة الوطنية.

- وإذا كان فيها مساس بالنظام العام[1].

كما الزم المشرع الجزائري في المادة 10 من قانون 09-04 على مقدمي الخدمات في مجال الانترنت بمساعدة السلطات المكلفة بالتحريات والتحقيقات القضائية.

وكذلك ألزمت المادة 11 من نفس القانون مقدمي الخدمات، بحفظ المعلومات التي يمكن بواسطتها ان يتعرف جهات التحقيق على مستعملي الخدمة، وحدد هذا القانون مدة حفظ المعطيات وهي سنة واحدة من تاريخ التسجيل.

وقد نصت المادة 12 من القانون 09-04 على التزامات خاصة بمقدمي خدمة الانترنت تتمثل في:

أ-واجب التدخل الفوري لسحب المعطيات او المحتويات التي تكون مخالفة للقانون ومنع الدخول اليها او تخزينها.

ب-وضع الترتيبات التقنية التي يتم من خلالها حصر الدخول الى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة وان يخبروا المشتركين لديهم بوجودها.

[1]المادة 18 من القانون 09-04 السابق الذكر.

وقد نصت المادة 11 المشار اليها سابقا على:

مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمة بحفظ:

أ-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج-الخصائص التقنية وكذلك مدة وتاريخ ووقت الاتصال.

د-المعطيات التي تتعلق بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

هـ-المعطيات التي تسمح بالتعرف على المرسل إليه او المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها[1].

الفرع الثاني: قانون البريد والاتصالات الالكترونية وقانون التأمينات

أولا: قانون المتعلق بالبريد والاتصالات الالكترونية:

لقد سارع المشرع الجزائري من خلال هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية والهدف من ذلك هو مسايرة التطور التكنولوجي،[2] لذا قد أصدر قانون رقم 18-04 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية، من خلال هذا القانون قد ألغى المشرع بموجبه القانون رقم 2000-3 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية.

فقد أكد المشرع من خلال هذا القانون على عدم مساس استعمال شبكات والخدمات الالكترونية بحفظ الحياة الخاصة.

[1] زبيحة زيدان، المرجع السابق، ص155-156.

[2] زبيحة زيدان، المرجع نفسه، ص76.

وفي حال مخالفة ذلك يتعرض لأحكام جزائية محددة في هذا القانون والتي تتمثل في:

1-انتهاك سرية المراسلات الالكترونية

يمكن لهذه الجريمة ان تتحقق بالاطلاع غير المشروع على الرسائل الالكترونية أو سماع المحادثات الالكترونية بطريقة غير مشروعة، بغض النظر عن محتواها وسواء كانت تتضمن اسرار أو لا، إضافة الى ذلك نشر أو إفشاء مضمونها أو استعماله بدون ترخيص[1]، اذ نصت المادة 164 من هذا القانون على انه (يعاقب بالحبس من سنة (1) الى خمس سنوات وبغرامة مالية من 500.000 الى 1.000.000 دج، كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل او المرسل إليه أو يخبر بوجودها) [2].

2-تحويل المراسلات الصادرة عن طريق البريد الالكتروني:

بالرجوع الى نص المادة 165 من قانون رقم 18-04 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية، يعاقب كل متعامل للاتصالات الالكترونية يحول بأي طريقة كانت المراسلات الصادرة او المستقبلة عن طريق الاتصالات الالكترونية، بالحبس من سنة الى ثلاث سنوات او بغرامة من 1.000.000 الى 5.000.000 دينار جزائري[3].

[1]شيخ سناء، شيخ محمد زكرياء، مكافحة الجريمة الالكترونية في القانون الجزائري، مجلة وميض الفكر للبحوث، العدد5، سبتمبر 2020، ص8.

[2]المادة 164 من قانون رقم 18-04 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية، العدد 27.

[3]شيخ سناء، شيخ محمد زكرياء، المرجع نفسه، ص8.

ثانيا: القانون المتعلق بالتأمينات

بالإضافة الى القوانين السابقة الذكر قرر المشرع الجزائري مواجهة الجريمة المعلوماتية أيضا في قانون 08-01 المعدل للقانون 83-11 المتعلق بالتأمينات الاجتماعية، اذ نص من خلال هذا القانون على ان صفة المؤمن له اجتماعيا تثبت ببطاقة إلكترونية، حيث نصت المادة 06 مكرر 1 من هذا القانون على انه تسلم البطاقة الإلكترونية مجانا للمؤمن له اجتماعيا من طرف هيئات الضمان الاجتماعي وتعتبر هذه البطاقات صالحة عبر كامل التراب الوطني وتقدم لكل مقدم علاج او خدمات متعلقة بعلاج، وبحسب نص المادة 65 مكرر يتم تزويد هذا الأخير بمفتاح إلكتروني يسمى (المفتاح الإلكتروني لهيكل العلاج).

ونظرا لأن البطاقة الإلكترونية هذه تتضمن معلومات خاصة بحياة الشخص أقر المشرع الجزائري حماية لها، إذ نص في المادة 93 مكرر 2 على ان يعاقب كل من يسلم أو يستلم هذه البطاقة الإلكترونية بهدف استعمالها بطريقة غير مشروعة، حيث جاءت كما يلي:

(دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين الى خمس سنوات وبغرامة من 100.000 دج الى 200.000دج كل من يسلم او يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا او المفتاح الالكتروني لهيكل العلاج او المفتاح الالكتروني لمهني الصحة)[1].

كما نصت المادة 93 مكرر 3 على انه تضاعف العقوبة على كل من يقوم عن طريق الغش بتعديل او حذف كلي او جزئي للمعطيات التقنية او الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا او في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة وهي نفس العقوبة التي تطبق كذلك على من يقوم بتعديل او نسخ بطريقة غير مشروعة

[1] المادة 93 مكرر 2 من القانون رقم 08-01 المؤرخ في 23 يناير 2008 المعدل للقانون رقم 83-11 المؤرخ في 02 يونيو 1983 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، العدد 04.

البرمجيات التي تسمح بالوصول او استعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا او في المفتاح الالكتروني لهيكل العلاج او لمهني الصحة.

يستنتج ان المشرع الجزائري وهو بصدد قانون خاص لم يفوت الفرصة بتشديد العقوبة على كل من يقوم بالتلاعب في البيانات او المعطيات التي تدرج في البطاقة الالكترونية سواء كانت تلك المعطيات تقنية معالجة آليا او إداريا، كما قد نص المشرع على حماية البرمجيات وذلك من خلال تشديد العقوبة على كل من قام بتعديل او نسخ فيها بطريقة غير مشروعة[1].

المبحث الثاني: الضوابط العملية لمواجهة الجريمة المعلوماتية

بما ان الجريمة المعلوماتية من الجرائم الحديثة المرتبطة بتطور تكنولوجيا الاعلام والاتصال لا تكفي الضوابط التشريعية وحدها لمواجهتها، بل يجب أيضا ان تدعم هذه الضوابط بضوابط أخرى ميدانية عملية، لذا فقد قام المشرع بإنشاء هيئات لمكافحة هذا النوع من الجرائم وهو ما سنتناوله في هذا المبحث، بحيث سنتطرق في المطلب الأول للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال اما المطلب الثاني سنتناول فيه الهيئات الخاصة بأجهزة الامن والمطلب الثالث فسنتعرض فيه الى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال:

في سبيل مكافحة الجريمة المعلوماتية او كما سماها المشرع الجزائري جرائم تكنولوجيا الاعلام والاتصال، قام المشرع بإنشاء الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال[2] سنتعرف عيها أكثر من خلال الفروع الآتية.

---

[1] زبيحة زيدان، المرجع السابق، ص77.

[2] حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03، ديسمبر 2021، ص465.

الفرع الأول: تعريف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

تم انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته بموجب المادة 13 من قانون09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المؤرخ في 2009/08/05 حيث نصت هذه المادة على: (تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.)

وقد صدر مرسوم الرئاسي رقم 15-261 تم فيه تحديد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وكذلك تنظيمها وسيرها، الا ان هذا المرسوم الغي وذلك بموجب المرسوم الرئاسي الجزائري رقم 19-172 وهذا المرسوم الرئاسي الجزائري قد الغي كذلك بموجب المرسوم الرئاسي الجزائري رقم 20-183وهو الاخر تم إلغاءه بموجب المرسوم الرئاسي الجزائري رقم21-439 وهو الذي يطبق حاليا.

يلاحظ ان المشرع الجزائري قد تذبذب تشريعيا في تحديد تشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بالرجوع الى نص المادة 02 من المرسوم الرئاسي الجزائري رقم 21-439 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المؤرخ في 07 نوفمبر 2021، التي نص على ان هذه (الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى رئيس الجمهورية)[1].

[1] المادة 2 من المرسوم الرئاسي رقم 21-439 المؤرخ في 07 نوفمبر 2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 86.

يتضح ان المشرع الجزائري قد اعترف صراحة بتمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بالشخصية المعنوية.

والمقصود بالشخص المعنوي هو عبارة عن مجموع من أموال او اشخاص تتظافر وتتعاون لمدة زمنية ذلك من اجل تحقيق اهداف أي ان هذه الأشخاص او الأموال تكون لها مصلحة جماعية مشتركة مستقلة عن المصالح الذاتية والفردية.

الا ان فكرة الشخصية المعنوية اختلف حولها الفقهاء منهم من أكدوا وجودها، وفئة أخرى من الفقهاء رفضوها ولم يقبلوها، وتبريرهم لهذا الرفض هو ان الشخصية المعنوية مفهوم ميتافيزيقي لا وجود له فهم يعترفون فقط بالشخص الطبيعي.

واكتساب الشخصية المعنوية يعني اكتساب الشخصية القانونية وهذا بنص القانون، أي يصبح الشخص المعنوي القانوني يتمتع بأهلية تسمح له باكتساب الحقوق وتحمل الالتزامات.[1]

اذ ترتب عن تمتع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بالشخصية المعنوية، آثار تتمثل فيما يلي:

-ذمة مالية مستقلة:

أي ان الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال باعتبارها شخصا معنويا، فهي تتمتع بذمة مالية مستقلة.

-الاهلية:

تمتعها بأهلية التقاضي اذ يحق للمدير العام للهيئة او ممثله اللجوء الى القضاء سواء بصفة مدعي او مدعى عليه، كما تكتسب أيضا الهيئة أهلية التعاقد هذا ما تأكده المادة 14

[1] الدكتور براهيمي سهام، الأستاذة براهيمي فائزة، الأساس القانوني للتنظيم في ظل التشريع الجزائري-الشخصية المعنوية او الاعتبارية-، مجلة القانون والعلوم السياسية، العدد السابع، الجزائر، جانفي 2018، ص30.

من القانون 09-04 ان هذه الهيئة تبادل المعلومات مع نظيرتها في الخارج بهدف جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام وتحديد أماكنهم[1].

-الموطن:

وهو مقر إقامة الهيئة والذي حدد بالجزائر، تكمن أهمية تحديد الموطن في تحديد الاختصاص الإقليمي في المنازعات التي تكون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال طرفا فيها.

-تحمل مسؤولية الاضرار الذي تسببه للغير:

بما ان الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال شخص معنوي فهي بذلك تعتبر كيانا قائما بذاته ومستقل، لهذا فهي التي تتحمل مسؤولية كل ضرر سواء مادي او معنوي تسببه للغير.[2]

[1] المادة 14 من القانون 09-04 المؤرخ في 05 اوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

[2] سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 02، الجزائر، 2022/12/30، ص565.

الفرع الثاني: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والمهام الوكلة لها:

أولا تشكيلة الهيئة: لابد للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال لكي تقوم بأعمالها ان تتكون من جهاز إداري، اذ نص المشرع في الفصل الثاني المادة 05 من المرسوم 21-439 على ان هذه الهيئة تتشكل من مجلس التوجيه، والمديرية العامة المنصوص عليها في المواد يكونان تحت وصاية رئيس الجمهورية.

1-مجلس التوجيه: نص المشرع الجزائري على مجلس التوجيه في المادة 06 و المادة 07 من المرسوم الرئاسي الجزائري 21-439 بحيث يتولى رئاسة هذا المجلس الأمين العام لرئاسة الجمهورية ، كما يتولى المدير العام للهيئة امانة مجلس التوجيه.

اما اعضاء مجلس التوجيه يتكونون من:

-الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج.

-الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية.

-الأمين العام لوزارة العدل.

-الأمين العام لوزارة الاتصالات السلكية واللاسلكية.

-قائد الدرك الوطني.

-المدير العام للأمن الوطني.

-المدير المركزي لأمن الجيش الوطني الشعبي.

-المدير العام للأمن الداخلي.

- رئيس مصلحة الدفاع السيبراني ومراقبة امن الانظمة لأركان الجيش الوطني الشعبي.

-ممثل عن رئاسة الجمهورية[1].

[1]المادة 6 من المرسوم الرئاسي رقم 21-439 المؤرخ في 07 نوفمبر 2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 86.

وقد حددت المادة 07 من المرسوم الرئاسي رقم 21-439 السابق الذكر مهام مجلس التوجيه نذكر من بين هذه المهام:

-توجيه عمل الهيئة والاشراف عليه ومراقبته.

-فيما يخص المسائل المتعلقة باختصاص الهيئة، يقوم مجلس التوجيه بدراستها والبث فيها.

-دراسة مشروع ميزانية الهيئة والموافقة عليه.

-ابداء رأيه في مسائل تتصل بمهام الهيئة وكذلك تقديم اقتراح في مجال اختصاص الهيئة[1].

2-المديرية العامة

يدير المديرية العامة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مدير يعين بموجب مرسوم رئاسي وتنهى مهامه أيضا بموجب مرسوم رئاسي، أي ان منصب هذا المدير يعتبر من الوظائف العليا في الدولة[2].

تتكون المديرية العامة من:

-مديرية المراقبة الوقائية واليقظة الإلكترونية.

-مديرية الإدارة والوسائل.

-مصلحة للدراسات والتلخيص.

-مصلحة للتعاون واليقظة التكنولوجية.

-ملحقات جهوية[3].

[1] المادة 07 من المرسوم الرئاسي رقم 21-439 السابق الذكر.

[2] المادة 09 من المرسوم الرئاسي 21-439 السابق الذكر.

[3] المادة 10 من المرسوم الرئاسي 21-439 السابق الذكر.

قد نص المشرع الجزائري على المهام الذي تقوم بها هذه المديرية في المادة 10 من المرسوم الرئاسي الجزائري 21-439 نذكر من بين هذه المهام:

-اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها وكذا السهر على تنفيذها.

-اعداد مشروع ميزانية الهيئة.

-تمثيل الهيئة لدى القضاء في جميع اعمال الحياة المدنية.

-تمثيل الهيئة لدى سلطات ومؤسسات الوطنية والدولية.

-ضمان التسيير الإداري والمالي للهيئة[1].

ثانيا: المهام الموكلة لهيئة الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

بالرجوع نص المادة 14 من القانون رقم 09-04 (تتولى الهيئة المذكورة في المادة 13أعلاه، خصوصا المهام الآتية:

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

-مساعدة مصالح الشرطة القضائية والسلطات القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات لإعلام والإتصال، من ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

[1] المادة 11 من المرسوم الرئاسي 21-439 السابق الذكر.

–تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم)[1].

من خلال هذه المادة يتضح ان الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تقوم بإجراء الحجز والتفتيش في المنظومة المعلوماتية كما تضمن هذه الهيئة مراقبة الاتصالات الإلكترونية بخصوص الجرائم الإرهابية والتخريبية التي تمس أمن الدولة ولها دور مساعد في مواجهة الجريمة المعلوماتية وذلك من خلال تلقيها لطلب المساعدة القضائية الداخلية او الأجنبية.

بالتالي يمكن القول ان هذه الهيئة تلعب دورا مهم في الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام وكذلك مكافحة هذه الجرائم.

المطلب الثاني: الهيئات التابعة للجهاز الأمني

بالإضافة الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، يوجد هيئات تابعة للجهاز الأمني هذه الهيئات مكلفة بالتدخل لمواجهة الجرائم المعلوماتية تنقسم هذه الهيئات الى صنفين سنتعرف عليهم من خلال فرعين.

[1] المادة 14 من القانون 09-04 السالف الذكر.

الفرع الأول: الهيئات التابعة للأمن الوطني

تتمثل هذه الهيئات في المصلحة المركزية لمكافحة الجريمة المعلوماتية والمخابر الجهوية للشرطة العلمية، وكذلك الخلايا الولائية المختصة في مكافحة الجريمة المعلوماتية:

أولا: المصلحة المركزية لمكافحة الجريمة المعلوماتية

في إطار مواجهة الجريمة المعلوماتية تم انشاء المصلحة المركزية لمكافحة الجريمة المعلوماتية التي أضيفت الى الهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 تقوم هذه المصلحة بالمهام الاتية:

-تشارك في حماية المنظومة المعلوماتية وكذلك الفضاء السيبراني الوطني.

-تقوم هذه المصلحة بمساعدة الشرطة القضائية في مجال التحريات التقنية.

-تساعد في التكوين المتخصص لعناصر الشرطة المتواجدين في فرق مكافحة الجريمة المعلوماتية.

-تراقب المصلحة الشبكات المفتوحة.

-كما تقوم أيضا هذه المصلحة بالتعاون والمشاركة في التحريات والتحقيقات سواء على المستوى الوطني او الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال[1].

[1] سميحة بلقاسم، حميد بوشوشة، المرجع السابق، ص 548.

ثانيا: المخابر الجهوية للشرطة العلمية

تضم المخابر الجهوية للشرطة العلمية دائرة مكلفة بالبحث والتحقيق في الجريمة المعلوماتية تسمى هذه الدائرة (دائرة الأدلة الرقمية والاثار التكنولوجية) وهذه الدائرة لم تكن في بداية إستحداثها سنة 2004 إلا قسم، لكن بسبب كثرة انتشار الجريمة المعلوماتية تم ترقيتها الى دائرة تضم هذه الدائرة ثلاث (3) اقسام:

-قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات.

-قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

-قسم تحليل الأصوات

تتكون هذه الدائرة من ثمانية أعضاء، محققين أربعة من بينهم أعوان شرطة رسميين أي يتمتعون بصفة الشرطة القضائية، وباقي الأعوان حائزون على شهادات في تخصص الإعلام الالي[1].

من مهام هذه الدائرة:

تقديم الدعم التقني لمصالح الشرطة وكذا الجهات القضائية في مجال التحري والبحث عن الجريمة المعلوماتية، ذلك بناء على الطلب الذي يصلها من أعوان الشرطة التابعين لخلايا مكافحة الجريمة المعلوماتية والذين يتبعون لمختلف مديريات الأمن الوطني، وأيضا الطلبات التي تقدم من العدالة سواء طلب مقدم من قاضي التحقيق او من طرف وكيل الجمهورية وحتى من طرف قضاة الموضوع في حالة لجوؤهم للخبرة في الجريمة المعلوماتية.

[1]عبد القادر عميمر، اليات اتباث الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، اطروحة لنيل شهادة دكتوراه علوم في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، بن يوسف بن خذة، كلية الحقوق، 2019-2020، ص 313.

يكلف أعضاء هذه الدائرة بدور مهم عند معاينة مسرح الجريمة المعلوماتية وحجز الأدلة، اذ يقومون بتحليل وفحص الأجهزة المضبوطة لإستخراج الأدلة منها.

في سنة 2007 تم انشاء أقسام مختصة في تتبع الأدلة الرقمية بمخابر الشرطة العلمية يقع مقر هذه الأقسام في الجزائر العاصمة، وهران وقسنطينة، تقوم بإستغلال الأجهزة الإلكترونية بهدف تتبع كل ما من شأنه ان يساعد في حجز الأدلة أو اكتشاف الجريمة، من بين الأجهزة المستغلة للكشف او ضبط الأدلة المتعلقة بالجريمة المعلوماتية أجهزة التصوير، الأقراص الصلبة، بطاقة الذاكرة...إلخ[1].

تالثا: الخلايا الولائية المختصة في مكافحة الجريمة المعلوماتية:

في سنة 2010 تم انشاء ما يقارب 23 خلية، لمكافحة الجريمة المعلوماتية وهي موزعة على النحو الاتي:

-ثمان خلايا على مستوى الشرق.

- ثمان خلايا على مستوى ولايات الوسط.

- ستة خلايا على مستوى ولايات الغرب.

-وخلية واحدة على مستوى ولايات الجنوب.

الا ان المديرية العامة للأمن الوطني قامت بتعميم خلايا مكافحة الجريمة المعلوماتية على مستوى كل مصالح أمن ولاية الوطن[2].

[1]عبد القادر عميمر، اليات اتباث الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، المرجع السابق، ص313.

[2]حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية، بحث مقدم الى اعمال الملتقى المنظم بكلية الحقوق، جامعة محمد خيضر، بسكرة، 2016، ص8.

الفرع الثاني: الهيئات التابعة للدرك الوطني

لمواكبة التطور الحاصل في مكافحة الجريمة المعلوماتية، قامت قيادة الدرك الوطني بإستحداث هياكل تابعة لها من اجل مواجهتها، يمكن اجمال هذه الهياكل في:

أولا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم انشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام في 26 يونيو 2004 بموجب المرسوم الرئاسي رقم 04-183 المتضمن إحداث المعهد الوطني للأدلة وعلم الإجرام، وهذا المعهد هو عبارة عن مؤسسة عمومية ذات طابع إداري موضوعة تحت وصاية وزير الدفاع الوطني وبتفويض منه يمارس قائد الدرك الوطني سلطات الوصاية، قد نصت المادة 04 من المرسوم الرئاسي 04-183 السابق الذكر، على مهام الذي يقوم بها هذا المعهد من بين هذه المهام:

- يقوم بإجراء الفحوص العلمية وكذا الخبرات في مجال التحريات الأولية والتحقيقات القضائية، بهدف إقامة الدليل الذي يمكن من خلاله التعرف على مرتكبي الجريمة.

-يقدم المساعدة العلمية من خلال القيام بالتحريات بإستعمال مناهج الشرطة العلمية والتقنية والتي تهدف الى الحصول وتحليل الأشياء والوثائق والأثار التي أخدت من مسرح الجريمة.

-المشاركة في الدراسات والتحاليل التي تتعلق بالوقاية والتقليل من كل أنواع الجرائم.

-تصميم وإنجاز بنوك المعطيات طبقا للقانون.

-المبادرة بالبحوث التي لها علاقة بالجريمة واجرائها، ذلك باللجوء الى تكنولوجيات تقنية.

-العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيد الدولي والوطني[1].

[1]المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، العدد 41، ص 20.

يتضمن المعهد الوطني للأدلة وعلم الإجرام على أقسام ومصالح، التي من خلالها يمكن للمعهد ان يقوم بالمهام المنوطة به بكل دقة، من بين هذه الأقسام والمصالح نذكر:

-مصلحة البصمات:

يتم فيها مقارنة البصمات من اجل التعرف على الجثث، يذكر ان جهاز الدرك الوطني يحتوي أنظمة التعرف الالي على البصمات.

-مصلحة الإعلام الالي:

يتم في هذه المصلحة رصد ومراقبة وتتبع عمليات الاختراق وكذا القرصنة المعلوماتية، واكتشاف المعلومات المسروقة وتفكيك البرامج.

- قسم التحليل الدقيق:

هذا القسم مجهز بأحدث الوسائل، يتم فيه إجراء عمليات المسح الإلكتروني، وكذلك تحاليل المقارنة للشعر والألياف وغيرها من الأمور التي يتم العثور عليها في مسرح الجريمة بواسطة جهاز الميكروسكوب الإلكتروني[1].

قسم الوثائق:

تعمل هذه المصلحة على التأكد من صحة الوثائق والامضاءات وكذلك تقوم بالتحقق من النفوذ بالإضافة الى التأكد من الأوراق السرية.

قسم السيارات:

يتم في هذا القسم التعرف على السيارات المسروقة وتتبع عملية تغيير او تحريف الأرقام الخاصة بها.

[1] سميحة بلقاسم، حميد بوشوشة، المرجع السابق، ص550.

بالإضافة الى هذه المصالح والاقسام هناك أيضا: قسم الحرائق والانفجارات، قسم الطب الشرعي، قسم الإدارة، قسم علم الإنسان وعلم الأسنان الشرعيين، قسم البواعث المؤدية للموت، مصلحة البيولوجيا الشرعية، مصلحة الإدمان، مصلحة الإشارة، مصلحة بصمة الاصبع، مصلحة الإلكترونيك، مصلحة الصور والصوت ....

كما يجدر الإشارة ان المعهد الوطني للأدلة الجنائية وعلم الإجرام يعد من أهم الهيئات في الجزائر التي أنشأت لمكافحة الجريمة والتي من بينها الجريمة المعلوماتية[1].

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني

تم إنشاء هذه المركز سنة 2008 يقع مقره ببئر مراد رايس، يهدف هذا المركز الى تحليل البيانات والمعطيات المتعلقة بالجريمة المعلوماتية المرتكبة وتحديد هوية مرتكبها، سواء كان شخصا واحدا او أشخاص والغاية من هذا تأمين وحماية المنظومة المعلوماتية.

يعتبر هذا المركز مركز توثيق وأيضا نقطة اتصال وطني، من بين مهام مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية:

-مساعدة باقي الأجهزة الأمنية في أداء مهامها.

-المراقبة المستمرة والدائمة على شبكة الانترنت.

-القيام بمراقبة الاتصالات الالكترونية في حدود ما يسمح به القانون لفائدة وحدات الدرك الوطني وكذا الجهات القضائية.

-المشاركة في عمليات التحري والتسرب لفائدة الدرك الوطني والجهات القضائية.

[1] سميحة بلقاسم، حميد بوشوشة، المرجع السابق، ص551.

-مساعدة وحدات الدرك الوطني في معاينة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.

-يقوم هذا المركز بالمشاركة في قمع الجريمة المعلوماتية وذلك من خلال التعاون مع مختلف مصالح الأمن والهيئات.[1]

ثالثا: مديرية الأمن العمومي والاستغلال

تعمل هذه المديرية على التنسيق بين الوحدات الإقليمية والمركز التقني العلمي في إطار البحث والتحري في الجرائم المعلوماتية.

رابعا: المصلحة المركزية للتحريات الجنائية

تعتبر هذه المصلحة هيئة ذات اختصاص وطني، وهي جهاز تابع للدرك الوطني مكلف بعدة مهام في إطار التحري والمساهمة في اجراء التحقيقات من اجل مواجهة الجرائم بجميع أنواعها ومن بينها الجريمة المعلوماتية.

المطلب الثالث: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

إن تميز الجريمة المعلوماتية بالطابع التقني وارتكابها في بيئة غير مادية، إضافة الى انتشارها بشكل كبير دفع المشرع الى التدخل سنة 2021، وإنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، بموجب الامر رقم 21-11 المؤرخ في 25 غشت 2021، المعدل والمتمم لقانون الإجراءات الجزائية[2] يتواجد هذا القطب على مستوى محكمة مقر مجلس قضاء الجزائر، كما يعتبر هذا القطب دعم لجهاز العدالة

[1] رابح سعاد، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، العدد 01، جامعة جيلالي اليابس سيدي بلعباس، الجزائر، جوان 2021، ص 281.

[2] الامر رقم 21-11 المؤرخ في 25 غشت 2021، المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65.

لتتمكن من متابعة الجريمة المعلوماتية التي أصبحت تشكل خطرا سواء على الافراد او الدولة[1] للتعرف أكثر على هذا القطب الجزائي سنتطرق في الفرع الأول الى الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، كما سنتطرق في الفرع الثاني الى اختصاصه النوعي.

الفرع الأول: الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

أولا: طبيعة الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

يتمثل الاختصاص الإقليمي طبقا لما جاءت به المادة 329 فقرة 01 التي نصت على ما يلي (تختص محليا بالنظر في الجنحة محكمة محل الجريمة او محكمة محل إقامة أحد المتهمين او شركائهم او محل القبض عليهم، ولو كان هذا القبض لسبب اخر).

الا ان المشرع قد وضع استثناء، اذ أجاز تمديد هذا الاختصاص في بعض الجرائم بحيث نصت المادة 129 الفقرة 05 من قانون الإجراءات الجزائية على (يجوز تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود، والجرائم الماسة بأنظمة المعالجة الالية للمعطيات، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف) وتطبيقا لهذه المادة مدد المشرع الاختصاص المحلي لكل من وكلاء الجمهورية، وقضاة التحقيق، محاكم المجالس القضائية في إطار الجرائم نفسها وذلك من خلال المرسوم التنفيذي رقم 06-348 والذي سبق لنا الإشارة اليه.

[1] بن عميور امينة، بوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 01، جامعة الاخوة منتوري قسنطينة1، الجزائر، 2022، ص68.

وقد نص المشرع في المادة 211 مكرر 23 من الامر رقم 21-11 المعدل والمتمم لقانون الإجراءات الجزائية (يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحيتهم في كامل التراب الوطني).

من خلال هذا النص نستنتج ان المشرع الجزائري قد منح القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال اختصاصا إقليميا وطنيا، وذلك لان الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال تعتبر من الجرائم الخطيرة.

وقد نصت المادة 211 مكرر 22 من الامر 21-11 السابق الذكر (ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والجرائم المرتبطة بها[1])، أي ان هذا القطب لا يكون تابع للمجالس القضائية بل ينشأ داخل المحكمة ويكون مستقل عن أقسامها، وتعيين القضاة في القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يكون بنفس طريقة تعيين القضاة، ويتشكل القطب الجزائي من تشكيلة جماعية مثل اقسام المحكمة.

ثانيا: تحديد الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

كما سبق وذكرنا فقد نص المشرع من خلال المادة 211 مكرر من القانون رقم 21-11 السابقة الذكر على ان الاختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يكون عبر كامل التراب الوطني.

[1] المادة 211 مكرر 22 من الامر رقم،21-11 السابق الذكر.

الا ان المشرع فصل أكثر في هذا الاختصاص كما يلي:

1-الاختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

بالرجوع الى نص المادة 211 مكرر 26 من القانون رقم 21-11 السابق الذكر، فقد اوكل المشرع للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال اختصاص حصري إذا تعلق الامر بالجرائم المنصوص عليها في المادة 211 مكرر 24 وكذلك المادة 211 مكرر25، يكون هذا الاختصاص الحصري في كافة التراب الوطني وهذا بالنظر الى خصوصية تلك الجرائم.

2-اختصاص مشترك للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

يكون هذا الاختصاص بحسب المادة 211 مكرر 27 بمناسبة قيام الجرائم الماسة بأنظمة المعالجة الالية للمعطيات التي تمد الاختصاص المحلي بها وفقا للفقرة الثانية من المادة 37 لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى[1].

نفس الامر لامتداد اختصاص قاضي التحقيق بمناسبة الجرائم الماسة بأنظمة المعالجة الالية للمعطيات طبقا للمادة 40 الفقرة 20 من قانون الإجراءات الجزائية.

[1]بن عميور امينة، بوحلايس إلهام، المرجع السابق، ص75.

3 اختصاص وجوبي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

يقوم الاختصاص المحلي الوجوبي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال طبقا لنص المادة 211 مكرر 28 من القانون رقم 21-11 السابق الذكر، في حالة تزامن مع اختصاص القطب الجزائي الوطني الاقتصادي والمالي، وهذا يعتبر اختصاص تفضيلي راجع لارتباط الجرائم المتصلة بتكنولوجيا الاعلام والاتصال مع الجرائم الاقتصادية المالية.

وقد نصت المادة 211 مكرر 29 من القانون رقم 21-11 السابق الذكر، انه في حالة تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر وفقا لنص المادة 211 مكرر 16 من القانون رقم 21-11 وجوبا باختصاص محكمة مقر مجلس الجزائر[1].

الفرع الثاني الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المقصود بالاختصاص النوعي هو ان تكون الجهة الجزائية مختصة في نوع معين من الجرائم من حيث طبيعتها او جسامتها مخالفة او جنحة او جناية[2].

وعليه فإن المشرع الجزائري قام بإنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومنح له الحق في الفصل بشكل حصري في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها.

[1] بن عمير امينة، بوحلايس إلهام، المرجع السابق، ص76

[2] نصيرة بوعزة، المحاكم ذات الاختصاص المحلي الموسع كألية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث والدراسات، المجلد 7، العدد 1، جوان 2021، ص184.

هذا من خلال نص المادة 211 مكرر 24 الذي جاء فيه (مع مراعاة احكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس القطب، حصريا بمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المذكورة ادناه وكذا الجرائم المرتبكة بها:

-الجرائم التي تمس بأمن الدولة او الدفاع الوطني.

-جرائم نشر وترويج اخبار كاذبة بين الجمهور من شأنها المساس بالأمن او السكينة او استقرار المجتمع.

-جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم او العابر للحدود الوطنية.

-جرائم المساس بأنظمة المعالجة الالية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

-جرائم الاتجار بالأشخاص او بالأعضاء البشرية او تهريب المهاجرين.

-جرائم التمييز وخطاب الكراهية)[1].

[1] المادة 211 مكرر 24 من الامر رقم 21-11 السابق الذكر.

خلاصة الفصل الثاني:

في هذا الفصل لقد تطرقنا الى الضوابط التي حاول من خلالها المشرع الجزائري حماية المنظومة المعلوماتية وكذلك التصدي للجريمة المعلوماتية علما أنها في انتشار مستمر، لذا فقد تناولنا في المبحث الاول مواجهة الجريمة المعلوماتية تشريعيا من خلال قوانين عامة كقانون العقوبات وقانون الإجراءات الجزائية كما تطرقنا الى مواجهة الجريمة المعلوماتية في قوانين خاصة كالقانون المتعلق بحقوق المؤلف والحقوق المجاورة وكذلك القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وقانون البريد والاتصالات الالكترونية وكذا قانون التأمينات.

اما المبحث الثاني فقد تطرقنا فيه الى الضوابط العملية لمواجهة الجريمة المعلوماتية، اذ توصلنا الى ان المشرع الجزائري حاول أيضا عمليا التصدي للجريمة المعلوماتية وذلك بإنشاء هيئات كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وكذا الهيئات التابعة لجهاز الامن، كما انه قام أيضا بإنشاء قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

الــخاتمة

الخاتمة:

في الأخير يمكننا القول ان الجريمة المعلوماتية جريمة مستحدثة وهي نوع من أنواع الجرائم المعاصرة التي ظهرت بظهور الثورة التكنولوجية وتطورت بتطورها، ارتباطها بهذه التكنولوجيا جعلها تتميز عن الجرائم العادية بدءا من تسميتها وصولا الى الأفعال المنسوبة اليها.

كما توصلنا الى ان الجريمة المعلوماتية من الجرائم التي يصعب مواجهتها، هذا راجع لطبيعتها الافتراضية التقنية بالإضافة الى انها سهلة الارتكاب لأنها على عكس الجرائم التقليدية كالقتل والسرقة التي تتطلب قوة عضلية، فهي تعتمد على ذكاء الجاني كما تعد الجريمة المعلوماتية من الجرائم التي يصعب اتباثها هذا لأنها لا تترك أي أثر مادي.

تعرفنا على ان الجريمة المعلوماتية ليست محصورة في نوع معين بل لها صور عديدة نذكر منها جريمة الذم والقدح عبر الأنترنت، جرائم انتحال الشخصية والاستدراج وجرائم التهديد والابتزاز.....

أصبحت هذه الجريمة تشكل هاجسا بالنسبة للأفراد وحتى الدول، باعتبارها من الجرائم العابرة للحدود، الامر الذي دفع الدول الى العمل على مكافحتها من خلال سن تشريعات، على غرار المشرع الجزائري الذي حاول التصدي لها عن طريق تجريم المساس بأنظمة المعالجة الالية في قانون العقوبات من خلال المواد من 394 مكرر الى 394 مكرر7.

كما قام المشرع الجزائري بإرساء قواعد إجرائية الهدف منها تفادي وقوع الجريمة المعلوماتية من بين هذه الإجراءات اجراء التفتيش، المعاينة واعتراض المراسلات.

قد حاول المشرع الجزائري مواجهتها أيضا عبر قوانين خاصة كقانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، اذ تم فيه النص على اجراء مراقبة الاتصالات الالكترونية وكذا التفتيش والحجز في المنظومة المعلوماتية.

إضافة الى هذا قام المشرع بإنشاء هيئات لمكافحة الجريمة المعلوماتية وتتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والهيئات الخاصة بأجهزة الامن، كما قام بإستحداث قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

من خلال دراستنا لهذا الموضوع توصلنا الى النتائج الاتية:

-ان المشرع الجزائري لم يستقر على تسمية واحدة لهذا النوع من الجرائم بحيث انه في بعض المرات قام بتسميتها الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومرات أعطاها تسمية جرائم المساس بأنظمة المعالجة الالية للمعطيات.

-لم يكن هناك اجماعا فقهيا حول تعريف الجريمة المعلوماتية.

-الجرائم المعلوماتية تختلف تماما عن الجرائم التقليدية.

-ان الجرائم المعلوماتية هي جرائم لها صور كثيرة.

-ان المشرع الجزائري أغفل العديد من النقاط التي تخص الجريمة المعلوماتية فهو قام بسن نصوص عن جرائم المساس بأنظمة المعالجة الالية للمعطيات الا انه لم يتطرق الى جريمة التزوير المعلوماتي التي هي في تزايد مستمر.

بتاء على هذه النتائج يمكن ان نقدم التوصيات التالية:

-ضرورة الاستقرار على تسمية واحدة للجريمة المعلوماتية وتكون هذه التسمية شاملة لجميع صور الجريمة المعلوماتية.

-مراجعة القوانين التي تتعلق بالجريمة المعلوماتية، ولما لا وضع قانون خاص بهذه الجريمة نظرا لأنها تشهد تطورات سريعة ومستمرة.

- الاهتمام بتكوين الخبراء والمحققين وكذا القضاة على التعامل مع الجرائم المعلوماتية

-فرض الرقابة على المواقع الالكترونية.

-ان توفر الدولة حماية لمستخدمي الانترنت من مخاطر الجريمة المعلوماتية.

-إقامة شراكات مع الجامعات ومراكز البحوث لتعزيز الابتكار في مجال مواجهة الجريمة المعلوماتية.

-ضرورة وجود تعاون دولي لمكافحة الجريمة المعلوماتية.

-إطلاق حملات توعية للتعريف بمخاطر الجريمة المعلوماتية.

-تدريس مواد خاصة بالحماية القانونية للمعلوماتية وكل ما يتعلق بالكومبيوتر والانترنت.

قائمة المراجع

أولا: الكتب

➢كتب عامة:

1-احسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة06، دار هومة، الجزائر، 2007.

➢كتب متخصصة:

1-امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر، الجزائر،2006.

2-خالد حسن احمد لطفي، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفكر الجامعي، الإسكندرية، 2019.

3-خالد ممدوح إبراهيم، امن الجريمة الالكترونية، الطبعة الأولى، الدار الجامعية، مصر، 2008.

4-خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، 2010.

5-زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر،2011.

6-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الاسكندرية، 2006.

7-عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية-مكتبة القانون والاقتصاد، الطبعة الأولى، المملكة العربية السعودية، 2012.

8-عميمر عبد القادر، التحديات القانونية لاتباث الجريمة المعلوماتية، النشر الجامعي الجديد، الجزائر، 2021.

9-غانم مرضي الشمري، الجرائم المعلوماتية، دار العلمية الدولية للنشر والتوزيع، الطبعة الأولى، الاردن،2016.

10-فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، مصر الإسكندرية، 2016.

11-محمد امين شوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.
12-نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010.

ثانيا: الاطروحات والرسائل

➢اطروحات الدكتوراه

1-بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، جامعة الجزائر 01-بن يوسف بن خدة، 2018/2017.
2-بن طالب لندا، الدليل الالكتروني ودوره في الاتباث الجنائي (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون، جامعة مولود معمري، تيزي وزو، 2019.
3-ربيعي حسين، اليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة 1، 2016/2015.
4-زروقي عاسية، طرق الاتباث في ظل قانون الإجراءات الجزائية، اطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، تخصص قانون عام، جامعة الدكتور مولاي طاهر، سعيدة 2018/2017.
5-سوبر سفيان، جرائم المعلوماتية، مذكرة لنيب شهادة ماجستير في العلوم الجنائية وعلم الاجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011/2010.
6-عبد القادر عميمر، اليات اتباث الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، اطروحة لنيل شهادة دكتوراه علوم في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة الجزائر، بن يوسف بن خذة، كلية الحقوق، 2019-2020.

➢رسائل الماجستير

1-حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012، ص185.

2-سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012.

ثالثا: المقالات

1-براهيمي سهام، الأستاذة براهيمي فائزة، الأساس القانوني للتنظيم في ظل التشريع الجزائري الشخصية المعنوية او الاعتبارية، مجلة القانون والعلوم السياسية، العدد السابع، الجزائر، جانفي 2018.

2-بن عميور امينة، بوحلايس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 01، جامعة الاخوة منتوري قسنطينة1، الجزائر، 2022.

3-بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة نحمد بوضياف المسيلة، العدد 11، 2018.

4-حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03، ديسمبر 2021،

5-حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 06 العدد 02، الجزائر، 2020، ص 173.

6-درار عبد الهادي، اليات التصدي للجريمة الرقمية في التشريع الجزائري، المجلة العصرية للدراسات القانونية، جامعة أبو بكر بلقايد، تلمسان، المجلد 01، العدد 02، 2023.

7-رابح سعاد، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، العدد 01، جامعة جيلالي اليابس سيدي بلعباس، الجزائر، جوان 2021.
8-راضية عيمور، الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، جامعة الاغواط، الجزائر، المجلد السادس، العدد الأول،2022.
9-سميحة بلقاسم، حميد بوشوشة، الجريمة الالكترونية بعد جديد للإجرام في الجزائر واقعها واليات مجابهتها، مجلة العلوم الإنسانية لجامعة ام بواقي، المجلد 10، العدد 01، جوان 2023.
10-سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 02، الجزائر،2022/12/30.
11-شيخ سناء، شيخ محمد زكرياء، مكافحة الجريمة الالكترونية في القانون الجزائري، مجلة وميض الفكر للبحوث، العدد 5، سبتمبر 2020.
12-صابر بحري منى خرموش، اهم الدوافع السيكولوجية وراء الجريمة الالكترونية، مجلة دراسات في سيكولوجية الانحراف، العدد 01، الجزائر، 2021.
13-صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكاديمية للبحث القانوني، العدد 1، جامعة بجاية،2010.
14-فاروق خلف، الأليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني، الجزائر، 2015.
15-فلاك مراد، اليات الحصول على الأدلة الرقمية كوسائل اتباث في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، 2019.
16-فيصل ستوف العساف، سلطان سليمان الجداني، ماهية الدليل الرقمي في النظام السعودي: دراسة مقارنة، الجريدة العالمية للقانون والدراسات السياسية، تاريخ النشر 15افريل2023.

17-نصيرة بوعزة، المحاكم ذات الاختصاص المحلي الموسع كألية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث والدراسات، المجلد 7، العدد 1، جوان 2021.

رابعا: ملتقيات ومؤتمرات

1-حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية، بحث مقدم الى اعمال الملتقى المنظم بكلية الحقوق، جامعة محمد خيضر، بسكرة، 2016.
2-فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، اعمال المؤتمر الدولي الرابع عشر الجرائم الالكترونية، طرابلس، بتاريخ 29-03-2017.
3-نمديلي رحيمة، خصوصية الجريمة المعلوماتية في القانون الجزائري والقانون المقارن، المؤتمر الدولي الرابع عشر، طرابلس، 24.25 مارس2017.

خامسا: النصوص القانونية

1-قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية، العدد 71.
2-قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية، العدد 84.
3-القانون رقم 08-01 المؤرخ في 23 يناير 2008 المعدل للقانون رقم 83-11 المؤرخ في 02 يونيو 1983 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، العدد 04.
4-القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 05 اوت 2009 الجريدة الرسمية العدد 47 صادرة بتاريخ 16اوت 2009
5-قانون رقم 18-04 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية الجريدة الرسمية العدد 27الصدر بتاريخ 13 ماي 2018.

6-الامر رقم03-05، الصادر بتاريخ 19 يوليو2003، المتعلق بحقوق المؤلف والحقوق المجاورة الجريدة الرسمية العدد 44.
7-الامر رقم 21-11 المؤرخ في 25 غشت 2021، المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية، العدد 65.
8-المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي الجريدة الرسمية العدد 41.
9-المرسوم الرئاسي رقم 21-439 المؤرخ في 07 نوفمبر 2021 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 86.

الفهرس

فهرس المحتويات

المحتوى	الصفحة
الاهداء	
الشكر والعرفان	
مقدمة	01
الفصل الأول: ماهية الجريمة المعلوماتية	
تمهيد الفصل	06
المبحث الأول: مفهوم الجريمة المعلوماتية	07
المطلب الأول: تعريف الجريمة المعلوماتية وخصائصها	07
الفرع الأول: تعريف الجريمة المعلوماتية	07
الفرع الثاني: خصائص الجريمة المعلوماتية	10
المطلب الثاني: صور الجريمة المعلوماتية ودوافع ارتكابها	12
الفرع الأول: صور الجريمة المعلوماتية	12
الفرع الثاني: دوافع ارتكاب الجريمة المعلوماتية	20
المطلب الثالث: اركان الجريمة المعلوماتية	23
الفرع الأول: الركن الشرعي	23
الفرع الثاني: الركن المادي والركن المعنوي	24
المبحث الثاني: الاثبات في الجريمة المعلوماتية	26
المطلب الأول: تعريف الدليل الرقمي وخصائصه	26
الفرع الأول: تعريف الدليل الرقمي	26
الفرع الثاني: خصائص الدليل الرقمي	27
المطلب الثاني: أنواع الدليل الرقمي وشروط قبوله	30
الفرع الأول: أنواع الأدلة الرقمية	30
الفرع الثاني: شروط قبول الدليل الرقمي	32

المطلب الثالث: إجراءات جمع الدليل الرقمي لاتباث الجريمة المعلوماتية	**33**
الفرع الأول: الإجراءات التقليدية لجمع الدليل الرقمي	**33**
الفرع الثاني: الإجراءات الحديثة لجمع الدليل الرقمي	**41**
خلاصة الفصل الاول	**47**
الفصل الثاني: مواجهة الجريمة المعلوماتية في التشريع الجزائري	
تمهيد الفصل	**49**
المبحث الأول: الضوابط التشريعية لمواجهة الجريمة المعلوماتية	**50**
المطلب الأول: مواجهة الجريمة المعلوماتية في ظل قانون العقوبات	**50**
الفرع الأول: صور جرائم المساس بأنظمة المعالجة الالية للمعطيات في قانون العقوبات	**51**
الفرع الثاني: العقوبات المقررة لجرائم المساس بأنظمة المعالجة الالية للمعطيات	**54**
المطلب الثاني: مواجهة الجريمة المعلوماتية في ظل قانون الإجراءات الجزائية والقواعد الخاصة بحقوق المؤلف والحقوق المجاورة	**57**
الفرع الأول: مواجهة الجريمة المعلوماتية في قانون الإجراءات الجزائية	**57**
الفرع الثاني: مواجهة الجريمة المعلوماتية في القواعد الخاصة بحقوق المؤلف والحقوق المجاورة	**59**
المطلب الثالث: مواجهة الجريمة المعلوماتية في تنظيمات وقوانين اخرى	**62**
الفرع الأول: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها	**62**
الفرع الثاني: قانون البريد والاتصالات الالكترونية وقانون التأمينات	**65**
المبحث الثاني: الضوابط العملية لمواجهة الجريمة المعلوماتية	**68**
المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	**68**
الفرع الأول: تعريف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	**69**

الفرع الثاني: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والمهام الوكلة لها	**72**
المطلب الثاني: الهيئات التابعة للجهاز الامني	**75**
الفرع الأول: الهيئات التابعة للأمن الوطني	**76**
الفرع الثاني: الهيئات التابعة للدرك الوطني	**79**
المطلب الثالث: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال	**82**
الفرع الأول: الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال	**83**
الفرع الثاني: الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال	**86**
خلاصة الفصل الثاني	**88**
خاتمة	**90**
قائمة المراجع	**94**
فهرس المحتويات	**101**
ملخص المذكرة	**104**

مـلخص مذكرة الماستر

تعتبر الجرائم المعلوماتية من الجرائم الحديثة التي جاءت نتاجا لتطور التقنيات المعلوماتية، اذ ان هذه الجريمة تختلف كليا عن الجرائم التقليدية من حيث الخصائص، الأركان والبيئة التي ترتكب فيها.

كما ان إثبات هذا النوع من الجرائم يكون عن طريق دليل يختلف عن الأدلة التقليدية الا وهو الدليل الرقمي.

ونظرا للتنامي الخطير لهذه الجريمة دفع ذلك المشرع الجزائري الى التدخل عن طريق سن قوانين تجرم وتعاقب الاعتداءات التي تحصل في المنظومة المعلوماتية على غرار قانون 09-04 القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، كما ان المشرع استحدث هيئات تعمل ميدانيا لمواجهة هذا النوع من الجرائم.

الكلمات المفتاحية:

1/الجريمة المعلوماتية **2/**المجرم المعلوماتي **3/**أنظمة المعالجة الالية للمعطيات **4/**الدليل الرقمي **5/**مواجهة الجريمة المعلوماتية **6/**المشرع الجزائري.

Abstract of Master's Thesis

Information crimes are considered one of the modern crimes that came as a result of development of information technologies, as this crime is completely different from traditional crimes in term of characteristics, element and the environment in which it is committed.

The proof of this type of crime is also done through evidence that differs from traditional evidence, namely digital evidence.
Due to the serious growth of this crime, this prompted the Algerian legislator to intervene by enacting laws that criminalize and punish attacks that occur in the information system ,such as law 09-04 concerning prevention and combating crimes related to information and communication technology, the legislator also created bodies to counteract this type of crime .

Keywords:
1/ Information crimes **2/** Information criminal **3/**Automated data processing systems **4/**Digital evidence **5/** Combating information crime **6/** Algerian legislator.