وزارة التعليـم العالـي والبحـث العلمـي +6./
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

المرجع: .....

قسم : القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

القواعد الإجرائية لمكافحة الجريمة المعلوماتية

ميدان الحقوق و العلوم السياسية

الشعبة:حقوق **التخصص: القانون الجنائي والعلوم الجنائي**

من إعداد الطالبة: **تحت إشراف الأستاذ:**

بلميسوم حاجة محمد كريم نور الدين

أعضاء لجنة المناقشة

الأستاذ	**جلطي منصور**	**رئيسا**
الأستاذ	**محمد كريم**	**مشرفا مقررا**
الأستاذ	**زواين خالد**	**مناقشا**

السنة الجامعية: 2023/2022

نوقشت يوم:2023/.06./.14


بسم الله الرحمن الرحيم
١٤٣٨

إهداء

إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك ولا تطيب الجنة إلا برؤيتك

(الله جل جلاله)

إلى من كلله بالهيبة والوقار إلى من علمني العطاء بدون انتظار إلى من أحمل اسمها بكل افتخار إلى من سعى وشقى لأنعم بالراحة والهناء (والدي العزيز حفظه الله)

إلى ملاكي في الحياة إلى معنى الحب و الحنان والتفاتي إلى بسمة الحياة و سر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب (امي الحبيبة حفظها الله)

الى مصدر سعادتي أخواتي الأعزاء الذي يهم أكبر وأعتمد وبالأخص منهم أختي الغالية بلميسوم أمينة التي هي سند حياتي علمتني روح المثابرة والاصرار معنى العزة و الصبر والكفاح من اجل النجاح

شكر و عرفان

اول من نشكره و نحمده اناء الليل و اطراف النهار هو العلي العظيم الواحد القهار الذي من علينا بهذه النعمة طلب العلم واغدق علينا برزقه الذي يغني فله جزيل الحمد والثناء العظيم

وشكر موصول الى كل استاذ افادنا بعلمه ولم يبخل علينا باي معلومة طوال مشوارنا الدراسي

مع الشكر الخاص لأستاذنا المشرف الدكتور نور الدين محمد كريم

ولكل الشكر لكل شخص قريب او بعيد صديق حبيب كل من دلنا و رافقنا في مشوارنا هدا

كما اتوجه بخالص الشكر والتقدير الى اعضاء اللجنة مناقشة المذكرة المتواضعة و في الاخير نسأل الله عز وجل ان تحتسب كل ادعيتكم ومساندتكم لنا حسنة عليكم و ارجو ان تقبلو منا هذه الكلمات المتواضعة التي تعبر على شكرنا وعرفانا على كل ما قد متموه لنا

مقدمة

تعتبر الشبكة المعلوماتية الدولية (الإنترنت) أعجوبة القرن التي اعتمدت عبر كامل أنحاء المعمورة وربطت شعوبها، حيث تعد وسيلة التعامل اليومي بين أفراد مختلف المجتمعات مع اختلاف الذهنيات والمستويات العلمية لمستعملي شبكة الانترنت، ورغم هذا التطور الذي يشهده كل من مجال تقنية المعلومات ومجال الاتصال نتيجة للاندماج المذهل الذي حدث بينهما، حيث أصبحت . القطاعات المختلفة تعتمد جميع في أداء عملها بشكل أساسي على استخدام أنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تحصيل المعلومات وتجميعها وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين أفراد الدولة الواحدة أو بين عدة الدولة ونظرا للجانب الايجابي التي جاءت به تقنية المعلومات إلا أنها خلقت العديد من السلبيات والتي منبينها ظهور نوع جديد من الإجرام الذي يرتبط بهذا النوع من التقنية الوليدة التي أطلق عليها بالإجرام المعلوماتي والتي جاء النص عليها في كل من اتفاقية بودابست المتعلقة بحماية المعلوماتية وأساليب منع وقمع الإجرام المعلوماتي أو الغش المعلوماتي وكذا قانون العقوبات الجزائري[1] وتأثيرا الجريمة المعلوماتية على الاقتصاد الوطني.

شكل إستخدام التكنولوجيا حدثا هاما في تاريخ البشرية وإرتباط بشكل قوي بمختلف مجالات النشاط الإنساني حتى أصبحت أمرا ضروريا يستحيل الإستغناء عنها، ومقوما أساسيا من مقومات دفع عجلة التقدم بالأمم والحضارات ومقياسا لتقدمها، غير أنه في مجال أقترنت هذه التقنية بظهور أفعال غير مشروعة أصبحت تشكل ظاهرة إجرامية من نوع خاص تختلف عن الظواهر الإجرامية العادية والكلاسيكية إذا قبلت العديد من المفاهيم سواء على المستوى القانون الموضوعي من حيث التجريم والعقاب، أو على مستوى القانون الإجرائي بفعل تغلبها

[1] – أمر 66_ 155 المؤرخ في 8 يونيو 1966 ، يتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية رقم 48 ، مؤرخة في 10 يونيو 1966 المعدل و المتمم .

– أمر رقم 21–11، ممضي في 25 غشت 2021 الجريدة الرسمية عدد 65، المؤرخة في 26 غشت 2021، يتمم الأمر رقم 66–155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية .

على قواعد المقررة كأصل عام للبحث وملاحقة مرتكبي الجرائم العادية، مما يتعين القول معه بأن الإجرام المعلوماتي قد أحدث ثورة في فلسفة التجريم والعقاب و الإجراءات الجنائية.

وهكذا برزت الجريمة المعلوماتية وبرزت معها العديد من الخصائص أو المجموعة من الميزات جعلت منها جريمة مستحدثة لا يمكن مقارنتها مع الجرائم التقليدية، كما أن هذه الخصائص جعلت من الجريمة المعلوماتية جريمة خطيرة تتجسد أو ترتكب بقوالب و أشكال عدة والتي يمكن إرتكاب من خلالها مجموعة كبيرة من جرائم وكأنها جريمة جمعت مختلف الجرائم التقليدية منها والفنية، فخصوصية الجريمة المعلوماتية تكمن بدأ من صعوبة إعطاءها مفهوما يحتويها من كل الجوانب، حيث يمكن إعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر:

- إما تتجسد في شكل جريمة تقليدية يتم إقترافها بواسائل إليكترونية أو معلوماتية.
- أو في شكل إستهداف للوسائل المعلوماتية ذاتها.
- أو أن يتم إقتراف الجرائم العادية في بيئة إليكترونية كما هو الحال بالنسبة لجرائم الصحافة.

فقلد أثارت هذه الجريمة بعض التحديات القانونية والعملية أمام الأجهزة المعينة بسبب طبيعتها الخاصة من الناحية الموضوعية ومن الناحية الإجرائية مما أظهر ذلك مدى الحاجة إلى تطور الآليات القانونية والإجرائية بما يتلائم خصوصيات هذه الجريمة.

وعليه فإن الإشكال الذي يطرح في هذا الموضوع هو :

- فيما تكمن خصوصية الجريمة المعلوماتية من الناحية الموضوعية وكذا من الناحية الإجرائية؟

أهمية البحث :

إن الجريمة المعلوماتية من حيث تطرقنا إلى مجموعة من جرائم التي ترتكب من خلالها الجرائم المعلوماتية، بالإضافة إلى تناول الجوانب الإجرائية لهذه الجريمة والتي تعد من المقدمات الضرورية التي ستظهر مدى كفائتها في التعامل مع التكنولوجيا المعلومات، ومن طبيعة الظاهرة التي يتناولها، والذي يعد من المواضيع بالغة أهمية في الوقت الراهن، وتتجلى أهميته في النقاط الآتية:

– الطبيعة الخاصة للجرائم المعلوماتية التي ميزتها عن الجرائم التقليدية سواء من حيث فاعلها او محلها أو مسرح الجريمة.

–تعتبر الجرائم المعلوماتية من الجرائم المستحدثة التي تعتمد على التقنيات الحديثة، التي ظهرت في مطلع القرن العشرين.

– خطورة هذه الجرائم وآثارها السلبية على الأفراد والدول، في ظل قصور التشريعات الوطنية عن مواكبة هذه التطورات في عالم الجريمة مما يتطلب تعاون دولي لمكافحة هذا النوع من الجرائم المستحدثة.

– أظهرت الدراسات العلمية التي أجريت حول هذه الجرائم ازدياد عددها بشكل مطرد، واتساع مجالاتها ليشمل أمور حساسة تتعلق بأمن وسلم الدول.

– إفلات العديد من مرتكبي هذه الجرائم من العقاب نظرا للغياب تقنين خاص بهذه الجرائم، وحتى إن وجد هذا التقنين فإنه يعاني من قصور نظرا لتميز هذه الجرائم عن الجرائم التقليدية.

أهداف البحث :

يسعى هذا البحث إلى تحقيق هدفه الرئيسي المتمثل في محاولة تقديم دراسة ترصد جوانب مختلفة من ملامح الظاهرة الإجرامية المعلوماتية وذلك من الناحيتين الموضوعية والإجرائية.

– يهدف الموضوع الى التعريف بمكافحة الجرائم المعلوماتية باعتبارها إحدى وسائل القانون الدولي العام والتي تسهم في تحقيق الأمن والسلم الدوليين.

– يهدف البحث إلى إبراز الدور الهام للتعاون الدولي في حل القضايا والأزمات الدولية.

– ضمان عدم زعزعة الاستقرار والأمن الدوليين والحد من انتشار ثقافة العنف بين الشعوب.

– إبراز أهم الصعوبات والتحديات التي تواجه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية وسبل التغلب عليها.

صعوبات البحث :

تتمثل هذه الصعوبات في قلة المراجع الخاصة بالتشريع الجزائري في هذا المجال المتعلق بالجرائم المعلوماتية .

أسباب اختيار الموضوع :

لقد جاء اهتمام بهذا الموضوع لاعتبارات ذاتية وموضوعية تتمثل في :

الأسباب الذاتية هي الرغبة في الدراسة ميدان مكافحة الجرائم المعلوماتية بغية الوقوف على أهم النصوص القانونية المتعلقة بمكافحة الجريمة المعلوماتية.

أسباب الموضوعية تتمثل في:

– إزدياد متسارع للجرائم المعلوماتية في ظل الثورة التكنولوجية الهائلة في ظل قصور التشريعات الوطنية في مكافحة الجرائم المعلوماتية.

– الرغبة في التعرف على مضمون المكافحة للجرائم المعلوماتية .

– أهمية موضوع مكافحة الجرائم المعلوماتية بوصفه ضمانة لحماية الأمن المعلوماتي الدولي.

– الرغبة في الوقوف على أوجه القصور ومحاولة إيجاد حلول تحسن المكافحة الدولية للجرائم المعلوماتية.

المنهج المعتمد :

سنعالج موضوع خصوصية الجريمة المعلوماتية متبعين المنهج الوصفي والتحليلي لأن دراستنا ستعتمد على وصف أهم خصائص الجريمة المعلوماتية، وتحليل أهم القواعد الإجرائية والقانونية التي تضبط هذه الجريمة في التشريع الجزائري .

تم تقسيم الدراسة إلى فصلين :

الفصل الأول بعنوان **الإطار المفاهيمي للجريمة المعلوماتية من الناحية الموضوعية** حيث قسمنا هذا الفصل إلى مبحثين المبحث الأول بعنوان **ماهية الجريمة المعلوماتية** ، وفي المبحث الثاني إلى **أسس تصنيف صور الجريمة المعلوماتية** .

أما الفصل الثاني سنتطرق فيه **خصوصية الجريمة المعلوماتية من الناحية الإجرائية** في المبحث الأول سنتطرق **المتابعة القضائية في الجريمة المعلوماتية** ، وفي المبحث الثاني سنتطرق إلى **أساليب التحري والتحقيق و إثبات في الجريمة المعلوماتية** وفي الأخير أنهينا هذا البحث بخاتمة .

الفصل الأول
الإطار المفاهيمي للجريمة المعلوماتية من الناحية الموضوعية

تمهيد

تعد الجريمة المعلوماتية ظاهرة إجرامية مستحدثة نظرا لارتباطها بالتكنولوجيا، فقد ترتب على ذلك إحاطة هذه الظاهرة بالكثير من الغموض، لأجل ذلك فقد بدا لنا أنه؛ وقبل الخوض في مجالات التعاون الدولي لمكافحة الجريمة المعلوماتية، كان لابد من الحديث عن مفهوم الجريمة المعلوماتية، وعلى ضوء ذلك سنحاول من خلال هذا المبحث التطرق إلى مفهوم الجريمة المعلوماتية ضمن المطلب الأول، أما في المطلب الثاني سنتطرق إلى تصنيف الجريمة
المعلوماتية.

إن الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول العالم ولا سيما الجزائر، بإعتبار أن هذه الجريمة أصبحت تمس حقوق الأشخاص من خلال التعديّ عليهم بمختلف الطرق والأساليب، ومن خلال هذا الفصل سنحاول إستعراض في المبحث الأول ماهية الجريمة المعلوماتية الذي يتضمن مطلبين ، مطلب الأول تعريف الجريمة المعلوماتية و المطلب الثاني خصائص الجريمة المعلوماتية أما في المبحث الثاني فقد تطرقنا إلى أسس تصنيف صور الجريمة المعلوماتية و الذي يتضمن مطلبين المطلب الأول المعلوماتية وسيلة لإرتكاب الجرائم أما المطلب الثاني المعلوماتية هدفا من إرتكاب الجرائم .

المبحث الأول : ماهية الجريمة المعلوماتية

لأن الجريمة المعلوماتية هي من الظواهر الحديثة؛ وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها ولكن الفقة لم يجتمع علي وضع تعريف محدد لها بل أن البعض ذهب إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

وجد الفقه صعوبة كبيرة في إيجاد تعريف دقيق للجريمة الإلكترونية بسبب حداثتها وسرعة وتيرة تطور تكنولوجيا المعلوماتية ووسائل الاتصال، وتباين الدور الذي تؤديه في الجريمة، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة ووسيلة لارتكابها تارة أخرى.

كما أن حداثة الجرائم الالكترونية واختلاف الثقافات والنظم القانونية بين الدول صعب من إيجاد مصطلح موحد للدلالة عليها، وهو ما أدى إلى عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، حيث يتم استعمال العديد من المصطلحات والعبارات للتعبير أحيانا على نفس الجريمة كالجريمة المعلوماتية والجريمة المتصلة بوسائل الإعلام والاتصال[1].

وتعددت التعريفات الخاصة بالجريمة المعلوماتية وتباينت فيما بينها وتعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وسوف نحاول من خلال هذا المبحث تعريف الجريمة المعلوماتية لننتقل فيم بعد إلى خصائصها.

المطلب الأول : مفهوم جريمة المعلوماتية

إختلاف النظم القانونية والثقافية بين الدول، وإنجر عنه تعريف للجريمة المعلوماتية تارة في المجال الضيق وتارة آخرى في المجال الموسع.

[1] – عبد الصديق الشيخ ، الوقاية الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 04 العدد 01 السنة 2020 ، ص 192.

لذا سوف نتطرق إلى التعريف الفقهي الضيق لهذه الجريمة ثم التعريف الموسع.

الفرع الأول : التعريف الضيق للجريمة المعلوماتية

تعددت التعاريف بشأن الجريمة المعلوماتية، فلا يوجد مصطلح محدد للدلالة على هذه الظاهرة، يطلق عليها البعض الجريمة المعلوماتية وآخرون جرائم الحاسب الآلي، ويطلق عليها البعض الآخر الجريمة الإلكترونية، أو الجريمة الرقمية على أساس لغة الحاسب الآلي[1].

إن الوسيلة المستخدمة في الجريمة و إنما ركزوا على موضوع الجريمة، فهذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها، بل تقع على الحاسب الآلي أو في داخل نظامه. [2]

لا يوجد مصطلح قانوني موحد للدلالة على ظاهرة الإجرامية الناشئة في البيئة الكمبيوتر وفيما يعد بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات[3] فظهرت عدة محاولات لتعريفها تعريفا ضيقا من بينها:

ما ذهب إليه الفقيه (MERWE) حيث يرى أن الجريمة المعلوماتية (جريمة الحاسب) هي :

– الفعل الغير المشروع الذي يتورط في إرتكابه الحاسب الآلي وهي الفعل الإجرامي الذي يستخدم في إقترافه الحاسب الآلي كأداة رئيسة.[4]

– في أخرى ذهب (Tièdement) إلى أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة بإستخدام المعالجة الآلية للمعطيات [1].

---

[1] – حمزة خضري، حمزة عشاش : "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي، الأغواط، الجزائر، جوان ،2020، ص ص 168–176.

[2] – بثينة حبيباتي الطبيعة الخاصة للجريمة المعلوماتية ، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12 عدد 03 جويلية 2020، ص ص: 617605، ص 608 .

3 - عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق ، جامعة الإسكندرية، سنة 2009، ص 26.

4 - MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,"R.I.D.P",1993;p554.

– فيما ذهب الفقيه (Rosblat) إلى تعريفها بأنها كل نشاط غير مشروع موجه لنسخ أو تغيرات أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه.

– أو أنها كما جاء في التعريف (Dauid Tompson) هي الجرائم يكون متطلبا لإقترافها ان يتوافر لدى معرفة بتقنية الحاسب.[2]

– وعرف (Leslie dball) الجريمة المرتبطة بالحاسب بأنها فعل إجرامي يستخدم الحاسب في إرتكابه كأداة رئيسية .

– وعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا .

– والحقيقة ان هذه التعريفات كانت قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي ولذلك فقد أنتقدت كون أن هذه التعريفات ركزت على وسيلة إرتكاب الجريمة لذا فهي ليست جامعة ولا مانعة.

– ومن أفضل التعريفات التي تدور حول الوسيلة هو تعريفها بأنها : تلك الجرائم التي يكون قد وقع في مراحل إرتكابها بعض العمليات الفعلية داخل نظام الحاسب، أي أنها الجرائم التي يكون دور الحاسب فيها إيجابيا اكثر منه سلبيا.

– وإزاء هذه الإنتقادات، حول جانب من الفقه تعريف الجريمة المعلومات على النحو واسع لظاهرة الإجرام المعلوماتي.

إن تعريف للجريمة على معيار شخصي و هو مدى معرفة الجاني بتقنية المعلومات و الإلمام بها ، و حيث أنّ قصور هذه التعاريف واضحة لأن شخصية الجاني لا تكفي لوحدها

1 -Klaus Tiede man, Fraude et autres délits d’affaires commis a l’aide d’ordinateurs électroniques, Rev, drpén , crim, 1984, p 612.

2 - هشام رستم، جرائم الحاسب كصورة من صور الجرائم الإقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط ، العدد 17 ، سنة 1995 ص 107 و 108.

لتعريف الجريمة الإلكترونية حيث يمكن لأي شخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية[1].

الفرع الثاني : التعريف الموسع للجريمة المعلوماتية

وهو ما ذهب إليه الفقيهان (MICHEL & CREDO) من أسوء إستخدام الحاسب او الجريمة الحاسب تشمل: إستخدام الحاسب كأداة لإرتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج الغير المصرح به لحاسب المجني عليه أو بياناته كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذات أو المعدلات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان، وإنتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إليكترونية، وتزيف المكونات المادية والمعنوية للحاسب.

وتناول رأي من الفقه تعريف الجريمة المعلوماتية بأنها : عمل أو إمتناع يأتيه الإنسان أضرارا بمكونات الحاسب وشبكات الإتصال الخاصة به التي يحمها قانون العقوبات ويفرض له عقابا.

ويمتاز هذا التعريف بانه يحتوي على كل صور الإعتداء الإيجابية والسلبية التي تقع أضرار بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به.

أنه يتضمن الأثر الجنائي المترتب على العمل أو الإمتناع غير المشروعين ويتمثل في الجزاء الجنائي بكافة صوره وأنواعه.[2]

بعد عرضنا لتعريف الجريمة المعلوماتية نضيف : أن شبكة الإنترنيت بوصفها نتاج تطور النظم المعلوماتية كأداة للربط والإتصال بين مختلف شعوب العالم، تشكل أداة لإرتكاب الجريمة المعلوماتية أو محالا لها وذلك بإساءة إستخدامها أو إستغلالها على النحو غير

[1] – رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر : الجرائم الإلكترونية، مركز جيل البحث العلمي طرابلس ، لبنان، 24 مارس 2017، ص ص: 95– 99.

2 - طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، سنة 2009، ص 157 و 158.

المشروع، ولذلك ينبغي على الجهات التشريعية مواجهتها بتشريعات حاسمة لمكافحتها وتقديم مرتكبيها للعدالة.[1]

المطلب الثاني : خصائص الجريمة المعلوماتية

الجريمة المعلوماتية إفراز ونتاج للتقنية المعلومات، وإتساع نطاق تطبيقها في المجتمع، مما يعطيها لونا او طابعا قانونيا خاصا، ويميزها مجموعة من الخصائص يمكن تجميعها حول العناصر الآتي ذكرها.

الفرع الأول : خصوصية الجريمة المعلوماتية

تعتبر الجرائم الإلكترونية جرائم حديثة إذ أنها لم تظهر إلا بعد اتساع التغطية بشبكة الانترنيت والانتشار الواسع للحواسيب والوسائط الالكترونية ومختلف وسائل الاتصال الحديثة لا سيما الهواتف النقالة، لذلك فهي تنفرد بخصائص لا نجدها في غيرها من الجرائم وتميزها عن الجرائم التقليدية[2].

تتميز الجرائم الالكترونية عن غيرها من الجرائم بأنها تعتمد أساسا على جهاز الكتروني متطور يشكل أداة الجريمة ووسيلة تنفيذها فبدون هذا الجهاز تنتفي الجريمة الالكترونية، كما أنها تتطلب تكوين وتحكم ودراية كافية بتكنولوجيا المعلوماتية وخاصة الانترنيت حيث أن أغلب الجرائم الالكترونية تتم عبر هذه الشبكة، كما لا يتصور ارتكابها دون استخدام التقنية المعلوماتية لأن هذه الأخيرة تشكل عنصراً من عناصرها، مثل الاختراق وتدمير الشبكات وتحريف البيانات أو التلاعب بها وإساءة استخدام المعلومات المتحصل عليها[3].

1 – د– جميل عبد الباقي الصغير، الأنترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ، القاهرة، سنة 2001، ص 04.

2 – رامي متولي القاضي 2011 ، مكافحة الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى، القاهرة، ص 53.

3 – محمد الألفي المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الانترنيت المكتبة المصرية الحديثة، القاهرة 2011،ص82.

أولا : صعوبة إكتشاف لجريمة المعلوماتية

تتسم الجرائم الناشئة عن إستخدام الأنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، ولأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة .

مثلا عند إرسال الفيروسات وسرقة الأموال ولبينات الخاصة او إتلافها والتجسيس وسرقة المكالمات وغيرها من الجرائم.[1]

كما أن وسيلة تنفيذها تتميز بالطابع الفني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى عدم الإبلاغ عنها في حالة إكتشافها لخشية المجني عليهم من فقدان عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة ثانية واحدة.[2]

ثانيا : صعوبة إثبات الجريمة المعلوماتية

إن الجريمة المعلوماتية في بيئة غير تقليدية حيث تقثع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والأنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ونظرا لما تطلبه هذه الجرائم من تقنية لإرتكابها فهي تستلزم أسلوب خاص التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحسين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد قادرة القوانين التقليدية على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى ظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[3] مما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

1 – محمد عبيد الكعبي، الجرائم الناشئة عن الإستعمال الغير المشروع للشبكة الانترنت، دار النهضة العربية، القاهرة سنة2001، ص 32.

2 – نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة 2 ، دار الثقافة للنشر والتوزيع، سنة 2001، ص 54.

3 – محمد عبيد الكعبي،مرجع سابق، ص 40.

ثالثا : أسلوب إرتكاب الجريمة المعلوماتية

الجرائم الإليكترونية هي الجرائم هادئة، تحتاج إلى قدرة علمية في التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية(الأنترنت) بما في ذلك بعض تقنيات إرتكاب هذه الجرائم كالإختراق سواء عن طريق إستعمال نظام التشغيل أو إستخدام البرامج أو عن طرق تشمل كلمات السر وجمعها، كما ظهرت تقنيات السلامي(salami te chnique) ، أو حصان طراودة في إرتكاب عملية الإختلاس المالي وغيرها من الأساليب المتطورة التي أفرزتها التكنولوجيا [1].

رابعا: التعاون والتواطؤ على الإضرار

وهو أكثر تكرارا في الجرائم المعلوماتية عنه في الأنماط الأخرى للجرائم الخاصة أو الجرائم أصحاب الياقات البيضاء، وهم دوي المناصب الرفيعة المستوى في الإدارات وغالبا ما يكون متضمنا فيها متخصص في الحسابات، يقوم بالجانب الفني في المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة (المجني عليها) لتغطية عملية التلاعب وتحويل المكاسب إليه، كما أنها من عادة من يمارس التملص على الحسابات تبادل المعلومات بصفة منتظمة حول أنشطتهم.[2]

خامسا : أعراض النخبة

يعتقد بعض المختصصين في تقنية الحسابات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية، إستخدام الحسابات وبرامجها لأغراض شخصية أو ممارسة بعض الهويات الرائدة في فلك هذه التقنية وهو ما يعبر عنه بأغراض النخبة، ومن شأن ذلك تمادي بعضهم إلى إستخدام نظم الحاسب بصورة غير مشروعة تصل إلى حدّ إرتكاب الجرائم الخطيرة.[3]

1 – عائشة بن قارة مصطفى، مرجع سابق، ص 44.

2 – إبراهيم الدسوقي عطية، مرجع سابق، ص 169.

3 - Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984,p11.

سادسا : الأضرار

تقع الجرائم المعلوماتية في نطاق تقنية نتقدمة يتزايد يوما بعد يوم إستخدامها في إدارة المعاملات الإقتصادية والمالية – الوطنية والدولية – الإعتماد عليها في تسيير معظم شؤون العامة لأكثر الحكومات بمانع ذلك الأمن والدفاع، ومن شأن ذلك أن يضفي أبعادا مسبوقة على الخسائر و الأضرار التي تنجم عن هذه الجرائم.

والأدل على ذلك من أم الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية (N.C.C.C.D) في نهاية القرن الماضي حوالي 500 مليون دولار في السنة.[1]

سابعا : الصفة الدولية للجريمة المعلوماتية

يمكن القول " ويحق" أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن ثم إكتسابها طبيعة دولية أو كما ذهب البعض أنها جريمة ذات طبيعة متعدية الحدود .

فمع ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحسابات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينهما آلاف الأميال، أدت إلى أن دول مختلفة قد تتأثر بالجريمة المعلوماتية المرتكبة في أن واحد.

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك من خلال التوسع الكبير في إجراء المعاملات البنكية عبر الشبكات المعلومات الدولية ذلك أعطى بُعد دولي لجرائم الإحتيال المعلوماتي بصفة خاصة .

1 - WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom “R.I.D.P” , 1991,p19.

كما يمكن للجاني الذي يتواجد في دولة بالدخول إلى ذاكرة حاسب آلي موجود في دولة أخرى، للقيام بعمل إجرامي في نطاق المعلوماتية يضر بشخص آخر موجود في دولة ثالثة مثل جرائم النصب المعلوماتي .

ومن القضايا الهامة ذات البُعد الدولي للجرائم المعلوماتية نذكر قضية " نقص المناعة المكتسبة" (الإيدز) وتتلخص وقائعها انه عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج، الذي يهدف في ظاهرة إعطاء بعض النصائح الخاصة بالمرضى نقص المناعة المكتسبة إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (من أمثلة حصان طراودة) وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي، عند العمل ثم تظهر بعد ذلك على الشاشة عبارة يقوم الفاعل من خلالها بطلب مبلغ من المال، يرسل على العنوان بدولة (بنما)حتى يتمكن المجني عليه من الحصول على المضاد للفيروس، وفي عام 1990 تم إلقاء القبض على المتهم ويدعى (جوزيف بوب) في ولاية (أوهايو) USA وطلب بريطانيا تسليمها المتهم لمحاكمته أما القضاء الإنجليزي، وقد وافق القضاء الأمريكي على تسليم المتهم.

وتظهر أهمية هذه القضية من ناحيتين:

الأولى : أنها المرة الأولى التي يتم تسليم المتهم في جريمة معلوماتية.

الثانية : أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد فيروس.[1]

الفرع الثاني : سمات المجرم المعلوماتي

في العالم الالكتروني صغير المجرمين كالكبير منهم يوجب التعامل معهم ككل باعتبارهم مصدرا للخطر, لأنه الضمان الوحيد للحماية من مصادر بالغة الخطر، وذلك لما تتميز به شخصية المجرم الالكتروني من خصائص وصفات تختلف عن مرتكبي الجرائم التقليدية, وهذا مرجعه تميز شخصيته بالتقدم في مجال استخدام الحاسب الآلي بعكس المجرم

1 – نائلة عادل فريد قورة،، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية القاهرة،؟ سنة 2005، ص 48.

العادي الذي غالبا ما يتميز بالقوة العضلية ونادرا ما يتميز بعضهم ببعض الذكاء، فقد رأى جانب من الفقه الجنائي أن المجرم الإلكتروني يمثل بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة بذاتها، فهو من جهة مثال متفرد للمجرم الذكي وإنسان اجتماعي بطبيعته من جهة أخرى.

لكن ذلك لا يعني التقليل من شأن المجرم الإلكتروني، بل أن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توفر الشخصية الإجرامية لديه . بالإضافة إلى أن الدراسات القليلة للجوانب السيكولوجية لمجرمي الحاسب أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية و بلا مشروعية الأفعال التي يقترفونها كذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال, فحدود الشر و الخير متداخلة لدى هذه الفئة اذ تغيب في داخلهم مشاعر الإحساس بالذنب, لكن هذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم المعلومات من اكتشافهم وافتضاح أمرهم إلا أن مبرر هذه الرهبة والخشية يفسرها انتماؤهم في الأغلب إلى فئة اجتماعية متعلمة[1].

أولا : المعرفة والمهارة والذكاء

تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة الميراد تنفيذها وإمكانيات نجاحها وإحتمالات فشلها، فالجناة عادة يمهدون لإرتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتُميز المعرفة بمفهومها السابق مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يُكون تصورا كاملا لجريمته ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[2].

[1] – خليلي سهام ، خصوصية المجرم الإلكتروني ، مجلة الفكر ، العدد 15 ، جوان 2017 ، ص 406.

2 – طارق إبراهيم الدسوقي عطية، مرجع سابق ، ص 176.

ويتمتع مجرمي الأنترنت بقدر لا يستهان به من المهارات تقنيات الحاسوب والأنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين من المهارة لدى الفاعل الذي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات.[1]

ثانيا : الوسيلة

الوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، وفيما يتعلق بالمجرم المعلوماتي فإت الوسائل المتطلبة للتلاعب بالأنظمة الحاسب الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة والسهولة في الحصول عليها ، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو إبتكار الأساليب التي تقلل من الوسائل اللازمة لأتمام النشاط الإجرامي.

ثالث : السلطة

يقصد بالسلطة الحقوق أو مزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من إرتكاب جريمته، فالكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة .

وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات بفتح الملفات وقراءتها وموها أو تعديلها، وقد تكون السلطة التي يتمتع بها الجاني غير شرعية كما الحال في حالة إستخدام شيفرة الدخول الخاصة بشخص آخر.[2]

رابعا : التكيف الإجتماعي

حيث ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لاشك أنهم يتكيفون في أفكارهم فيما بينهم وتنشأ بالتالي بينهم صفات وروابط تساعدهم على إرتكاب جرائمهم تتعدى تلك الروابط والصلات النطاق المحلي بحيث ينشأ بينهم روابط دولية

1 - MASCALA Corinne , criminalité et contrat électronique, Travaux de l'association, CAPITANT Henir , journées National paris, 2000,p118.

2 – طارق إبراهيم الدسوقي عطية، مرجع سابق ، ص177.

تتفق مع أفكارهم ومنهجهم، وتزداد خطورتهم الإجرامية إذا تزايد تكيفهم الإجتماعي مع وتافر الشخصية الإجرامية لديهم.[1]

خامسا : الباعث

وأخيرا يأتي الباعث وراء إرتكاب الجريمة، ولا يختلف باعث الجاني على إرتكاب الجريمة المعلوماتية في كثير من الحيان عن الباعث لإرتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء إرتكاب الجريمة المعلوماتية، ثم يأتي بعد مجرد الرغبة في فهو نظام الحاسب وتخطي حواجز الحماية حوله، وأخيرا الإنتقام من رب العمل أو أحد الزملاء[2].

ففي دراسة قديمة لإحدى المجالات المتخصص في الأمن المعلوماتي تعرض لها الفقه (PARKER) خلصا إلى أن 43% من حالات الإعتداء عاة نظم المعالجة الآلية المعلن عنها قد بوشرت بهدف إختلاس الأموال وأن 23% من أجل سرقة المعلومات وأن 19 % افعال الإتلاف وأن 15 % سرقة وقن الآلة، أي الإستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

أما فيما يتعلق بالرغبة في تحدي وقهر النظام فمن أشهر القضايا المتعلقة بهذه الحالة كان قد تعامل معها مكتب التحقيقات الفيدرالية، أطلق عليها إسم مجموعة الجحيم العالمي(GLOBAL HELL) تتلخص وقائعها في تمكين مجموعة من الأشخاص من إختراف مواقع البيت الأبيض والشركة الفديرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة وقد ظهرت من التحقيقات أن هذه المجموعات تهدف إلى مجرد الإختراق أكثر من التدمير او إلتقاط المعلومات الحساسة.

1 – ايمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، سنة 2004، ص 17.

2 - D.B.PARKER, comibattre la criminalité informatique , edoros,1987,p142.

بالإضافة إلى الباعث آخر يدفع إرتكاب الجريمة المعلوماتية من قبيل ذلك أسباب تتعلق بالحياة المهنية، كالشعور بالحرمان من بعض الحقوق المهنية وخاصة ما يتعلق منها بالراتب ، ومن أمثلة ذلك قيام موظف فصل من الشركة التي كان يعمل بها وقبل يومين من تركه العمل قام ببرمجة كومبيوتر بالشركة زارعا نوعا من الفيروسات وبعد يومين حذفت المعلومات هامة في الشركة .[1]

الفرع الثالث : تصنيف المجرم المعلوماتي

أولا : المخترقون أو المتطفلون:

يتحد في هذا الإطار نوعين من المخترقين أو المتطفلين :

1- الهاركز (Les hackers)

يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي [2] ويقصد بهم الشباب البالغ المفتون بالمعلوماتية، والحسبات الآلية، أغلب هذه الطائفة هم من الطلبة والشباب حاصلين على المعرفة في مجال التقنية المعلوماتية والباعث الأساسي لهذهذ الطائفة عو الإستمتاع باللعب والمزاح بإستخدام هذه التقنية إثبات مهارتهم وقدراتهم بإكتشاف وإظهار مواطن الضعف غب الأنظمة المعلوماتية، دون أي إلحاق ضرر بها لديهم في المغامرة والتحري والرغبة في الإكتشاف.[3]

2- الكراكز (Les crakers) :

ويعني ذلك المقتحم وتعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنين والكراكز تتراوح أعمارهم بين 25-45 عاما ومن أبرز سمات وخصائص أفراد هذه الطائفة،

1 - رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، وفي التشريع الجزائري المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012، ص 95 و 96.

2 - أسامة سمير حسين، الإحتيال الإليكتروني (الوجه القبيح للتكنولوجيا) ، الحنادرية للنشر والتوزيع ، الأردن الطبعة الأولى ، سنة 2011، ص 134.

3 - عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الأنترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى سنة 2006، ص 46.

أنهم ذوي مكانة في المجتمع وأهنهم دائما ما يكونوا من المتخصصين في مجال التقنية الإليكترونية، أي أنهم يتمتعون بالمهارات، ومعارف فنية في مجال الأنظمة الإليكترونية أو المعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية المعلومات. [1]

ثانيا : مجرمو الكمبيوتر المحترفون:

تتميز هذه الطائفة بسعة للأنشطة التي تركب من قبل أفرادها، لذا فإن هذه الطائفة تعد الأخطر من بين مجرمي وللجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الكمبيوتر كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي.[2]

وتعتبر هذه الفئة أكثر خطورة من الصنف الأول للأضرار الكبيرة التي يُلحقوانها بضحاياهم وبإعتداءاتهم الإجرامية الخطيرة.

ثالثا: الحاقدون:

هذه الطائفة لا يغلب عليها توافر الأهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارتية وبنفس الوقت لا يسعون إلى مكاسب مادية او سياسية، إنما يحرك أنشطتهم الرغبة بالإنتقام والثأر كأثر لصاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم. [3]

1 – محمد دباس الحميد، ماركو إبراهيم نينو، حماية الأنظمة المعلومات، دار حامد للنشر والتوزيع، عمان ، الطبعة الأولى ، سنة 2007، ص 73.

2 – جعفر حسين جاسم الطائي، جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة المعلوماتية)، دار البداية ،عمان سنة 2007، ص 162.

3 – نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف للنشر والتوزيع ، الأردن، دون سنة ، ص 42.

رابعا : الجماعات الإرهابية أو المتطرفون:

والتي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار إجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويتركز نشاطهم بصفة عامة في إستخدام ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه.

ولقد بدأ إهتمام الجماعات الإرهابية، وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية .

فإعتماد المؤسسات المختلفة داخل الدول على أنظمة الحسابات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في اغلب الأحوال، قد جعل من هذه الأنظمة هدفا جذبا لتلك الجماعات، حيث لا تزال الممثلة في هذا المجال قليلة وإن كان متوقعا تزايدها مستقبلا، ومن أمثلة الشهيرة في هذا الخصوص قيان إحدى الجماعات الإرهابية المعروفة في أوروبا بإسم « The Red Brigades » يتذمر ما يزيد عن 60 مركزا للمحاسبات الآلية خلال الثمانينات لتلفت الأنظار إلى أفكارها ومعتقداتها [1].

خامسا : صغار السن:

أو كما يسمون (صغار نوابع المعلوماتية) هم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية، وقد أثارت هذه الفئة جدلا واسعا في مجال الفقهي ففي حين كثر الحديث عن مخاطر هذه الطائفة، رأى جانب من الفقه أنه من أحسن عدم تصنيف هؤلاء ضمن دائرة الإجرامهم بحساب أن لديهم ميلا للمغامرة والرغبة في البحث والإستكشاف.[2]

1 – طارق إبراهيم الدسوقي عطية ، مرجع سابق، ص 181.

2 – رشيدة بوكر، مرجع سابق، ص 97.

المبحث الثاني : أسس تصنيف صور الجريمة المعلوماتية

تعتبر الجرائم المرتكبة عبر الأنترنت من الجرائم المستحدثة، وهي تستهدف الكثير من القطاعات مما يجعل تحديدها وتصنيفها يتميز بالصعوبة على العكس الجريمة التقليدية، ولم يستقر الفقهاء على التصنيف موحدّ لصور الجريمة المعلوماتية لذ إرتأينا تقسيم وتصنيف الجريمة المعلوماتية على النحو التالي:

المطلب الأول : المعلوماتية وسيلة لإرتكاب الجرائم

صاحب ظهور شبكة الأنترنت تطورات كبيرة في شتى المجالات، ورغم الفوائد التي أتت بها إلا أنها أصبحت سلاح فتاك في يدّ المجرمين الذين يمس سلامة الأشخاص وحياتهم الخاصة، وكذا الجرائم التي تقع على الأموال والسطو عليها بل تعد الأمر إلى المساس بامن الدولة وهذا ما سنتطرق إليه في الفروع الآتية:

الفرع الأول : الجرائم الواقعة على الأشخاص

إن الطبيعة الفنية للجريمة الالكترونية, تفرض صعوبة في حصرها داخل إطار قانوني تجريمي محدد وواضح لأننا أمام ظاهرة إجرامية مستحدثة كل جريمة فيها تتميز من حيث موضوع الجريمة و وسيلة ارتكابها وسمات مرتكبيها و أنماط السلوك الإجرامي المجسد للركن المادي لكل جريمة من هذه الجرائم، بسبب التسارع الرهيب في ميدان اتقنية المعلومات, فالمزيد من الوسائل والاختراعات والأدوات التقنية يساهم في تغيير أنماط الجريمة وتطور وفعالية وسائل الاعتداء, وهذا بدوره يساهم في إحداث تغيرات على السمات التي يتصف بها مجرمي التقنية مما يستدعي ضرورة توحيد الجهود من أجل الإلمام أكثر بحقيقة هذه الجرائم نظرا لغياب اتفاق عام حول التعريف القانوني للنشاط الإجرامي المتعلق بهذا النوع من الإجرام وتحديد نطاقه)، بالرغم من البعد الدولي للجريمة الالكترونية الذي يفرض حتميته التعاون الدولي في مكافحة هذا النوع من الجرائم [1].

[1] – خليلي سهام ، المرجع السابق ، ص 408.

كما تستهدف الجريمة الالكترونية معنويات وليست ماديات ملموسة, وقد ترتكب في مكان و تتحقق النتيجة في آخر فلا تعترف بالحدود الجغرافية ولا تعترف ابتدءا بعنصر المكان, بالإضافة إلى صعوبة الإثبات فيها من حيث عدم ترك الآثار المادية وسهولة محو الدليل و نقص خبرة القائمين على مكافحة الجريمة.

أولا : جريمة القذف والسب عبر الأنترنت

تعد الجرائم القذف والسب من الجرائم التي لها الأثر البالغ سلبا على الأشخاص وهي الأكثر شيوعا وإنتشارا خاصة بعد ظهور شبكة الأنترنت، وإساءة إستخدامها لنيل من شرف الغير أو كرامته أو إعتباره.[1]

والقذف هو إسناد واقعة معينة تستوجب العقاب في حالة الصدق على من تنسب إليه وذلك بشكل علني.

أما السب هو الإسناد العمدي لواقعة غير معينة إلى المجني عليه خادشة بذلك لشرفه وإعتباره.[2]

هذا ما قد يعرض الضحية إلى بعض الناس وإحتقارهم ثم إلساله لمجني عليه، على شكل رسالة بينات ويعني بذلك المعلومات التي تم إنشائها أو إرسالها بوسائل إليكترونية وبالتالي توافر عنصر العلنية في هذه الجرائم بسبب عرضها على المواقع والرسائل الإليكترونية تتسبب في أضرار كبيرة للأشخاص. [3]

1 - خالد ممدوح إبراهيم، فن التحقيقي الجنائي في جرائم الإليكترونية، الطبعة الاولى ،دار الفكر الجامعي لنشر الإسكندرية ، سنة 2009،ص 319.

2 – فوزية عبد الستار، شرح القانون الإجراءات الجنائية ، دار النهضة العربية ،سنة 1997،ص 592.

3 - خالد ممدوح إبراهيم/ مرجع سابق، ص 333.

ثانيا : صناعة ونشر الإباحة

إذا كان لشكبة الأنترت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع الشبكة الأنترنت تحرض على ممارسة الجنس لكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور فاضحة للبالغين والأطفال [1].

حيث يضر إستخدام الأطفال المستخدمين في إنتاج هذه المواد و الإعتداء عليهم في كل مرة يتم فيها عرض هذه صور. [2]

ثالثا : إنتحال الشخصية والتغرير والإستدراج.

يقصد بإنتحال الشخصية ما يعيد المجرم من إستخدام شخصية آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو الإهتماما بخصوصية وسرية المعلومات الشخصية للمستفدين على شبكة الأنترنت، وتتخذ جريمة إنتحال الشخصية عبر الأنترنت أحد الوجهين التاليين: إنتحال شخصية الفرد وإنتحال شخصية المواقع.

أما فيما يخص التغريرو الإستدراج فغالبا ضحيا هذا النوع من الجرائم هو صغار السن من مستخدمي الشبكة، حيث يوهم المجرمين ضحاياهم برغبتهم في تكوين صداقة على الأنترنت والتي قد تتطور إلى الإلتقاء مادي بين الطرفين.

إن مجرمي التغرير و الإستدراج على شبكة النترنت يمكن لهم أن تتجاوز الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر ويكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدري الكثير من الضحايا أنهم غرر بهم. [3]

---

1 - FAUCHMOUX 6 VINCENT6 Daprery pierre, le Droit de l'internet (loi ,contra et sage) , édition , lutec , paris ,2008,p215.

2 - كريستينا سكولمان، عن جرائم الأنترنت طبيعتها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر المملكة المغربية، سنة 2007، ص 40.

3 – عمرو موسى الفقهي، الجرائم المعلوماتية، جرائم الحاسب الآلي و الأنترنت في مصرو الدول العربية، المكتب الجامعي الحديث، الإسكندرية، سنة 2006، ص 102.

الفرع الثاني : الجرائم الواقعة على الأموال

أولا : السرقة عبر الأنترنت

تعرف السرقة بانها إختلاس الشيء منقول للغير دون رضاه بنية إمتلاكه[1]، وتتم سرقته – المال المعلوماتي – إن أمكن الوصف عن طريق إختلاس البيانات والمعلومات وٱستفادة منها بإستخدام السارق للمعلومات الشخصية، مثل الإسم، العنوان، الأرقام الخاصة بالمجني عليهم والإستخدام غير شرعي لشخصية المجني عليه، ليبدأ عملية السرقة المتخفية عبر الأنترنت بحيث يؤدي بالغير إلى تقديم الأموال – الإلكترونية أو المادية– إلى الجاني عن طريق التحويل البنكي [2].

تتجسد جريمة السطو على أموال البنوك عن طريق إستخدام الحاسب الآلي للدخول إلى شبكة الأنترنت والوصل غير المشروع إلى البنوك و المصارف والمؤسسات المالية[3].

ثانيا : الجرائم التي تنجر عن إساءة إستخدام البطاقة المصرفية .

و المساهمة في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، و الذي يقف من ورائها التطور المذهل لوسائل الإعلام و الأصعدة الاتصال، على جميع و المستويات الإيجابية و السلبية، هذه الأخيرة و التي أفرزت نوع جديد من الإجرام، وبهدف الوقاية من هذه الجرائم و مكافحتها يسعى المشرع الجزائري على غرار باقي الدول، لمواجهة هذا النوع من الجرائم على المستوى الداخلي و الخارجي، وهذا عن طريق سن قوانين و إجراءات كفيلة لمواجهة هذه الجرائم[4].

1 – نايف بن محمد المرواني ، جريمة السرقة ، دراسة نفسية إجتماعية ، جامعة نايف العربية للعلوم الأمنية، الرياض الطبعة الاولى، سنة 2011،ص 59.

2 – دمحمد أمين أحمد الشوابكة ، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، سنة 2004،ص 138.

3 – عباس أبو شامةعبد المحمود، عولمة الجريمة الإقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض،سنة 2007، ص 20.

4 – عمراني مصطفى، جريمة تزوير البطاقات البنكية، مجلة الدراسات والبحوث القانونية ، العدد السابع،ص 299.

نظرا للإنتشار الواسع لهذه البطاقات الممغنطة وعلى رأسها بطاقات السحب من المصارف، فقد أدى هذا إلى إزدياد إساءة إستخدام هذه البطاقة من أجل الحصول على المنفعة المالية غير المشروعة سواء من قبل حاملها الشرعي أو من قبل الغير، وفي هذا شيء من التفصيل.

1- إساءة إستخدام البطاقة من قبل حاملها الشرعي:

ترتكب هذه الجريمة من قبل حامل البطاقة الشرعي الذي بإسمه وتتعلق بحسابه وبعمله وبعدة قروض، أما عن رصيده غير كافي لسحب المبلغ او أن الرصيد مغلق مستغلا إختراقه والتلاعب به وبعد إشعاره من قبل المصرف بإلغائها او بعد إنتهاء مدة صلاحيتها.

2- إساءة إستخدام البطاقة المصرفية من قبل الغير:

فقد يعمل على سرقتها من حاملها الشرعي، وقد يعثر عليها ومعها الرقم السري وتختلف بطاقة سحب النفوذ من الأجهزة التوزيع التابعة للمصرف عن البطاقة الإئتمان والتي باتت في إطار الإنتشار الهائل لشبكة الأنترنت وإزدياد حجم التجارة الإليكترونية هدفا منشودا من قبل المجرمين. [1]

ثالثا : جرائم غسيل الأموال عبر الأنترنت

تعد جرائم غسل الأموال من أخطر جرائم عصر الإقتصاد الرقمي، فهي التحدي الحقسيقي أمام مؤسسات المال و الأعمال وتعد الإختبار الأمثل لقدرة القواعد القانونية على تحقيق الفعالية في مواجهة الأنششطة الإجرامية ومكافحة الأنماط المستحدثة منها : فهي كغيرها من الجرائم الإقتصادية جريمة ذوي الباقات البيضاء التي ترتكب من قبل محترفي الإجرام التي لا تتلائم سماتهم مع سمات الإجرامية التي عرفتها وحددته النظريات الكلاسيكية المتعلقة بعلم الإجرام والعقاب.

1 - محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ماجيستير في القانون الجنائي المعلوماتي، الطبعة الأولى دار الثقافة للنشر والتوزيع ، عمان، الأردن سنة 2009، ص ص 43، 65.

وجريمة غسيل الموال بعد تفجر قورة الإتصالات وإزدهارها إتجه غسيلوا الأموال القذرة إلى التطوير وسائلهم وإستحداث وسائل جديدة لغسل ألأموال مستفدين في ذلك من أموال التكنولوجيا الحديثة وعلى رأسها شبكة الأنترنت، كما لجأوا إلى الأنظمة الحولات الإليكترونية بدأ من البرقيات و الإيداعات والمسحوبات التقنية،وذلك عن طريق أجهزة الصرف الآلي وغيرها من الوسائط التكنولوجيا الحديثة، ومن هنا برز ما يعرف بالغسيل الأموال الرقمي. [1]

الفرع الثالث : الجرائم الواقعة على أمن الدولة

أولا : الجرائم الماسة بالأمن الفكري

ينطوي الخوف من عواقب الثورة المعلوماتية والإتصال التي مست بثقافة وقيم ومفاهيم قواعد المجتمع المادية والتربوية بإعتبار ان الشبكة العالمية للأنترنت منحت المستخدم الكثير من الخيارات من خلال عدم خضوعها لأي رقابة وعبورها للحدود الجغرافية بين الدول، وموها السريع والمتواصل، وإمكانية مشلركة الجميع من مختلف الدول العالم .

إضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدّة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة من أهم المقومات المجتمع المعلوماتي، والتي تؤدي إلى الإنحراف الفكري من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العلمية للأنترنت، وتتهدد المن بأبعاده كافة. [2]

ثانيا : الجريمة المنظمة

الجريمة المنظمة ليست وليدة التقدم والسهولة وإذ كانت إستفادت منه فالجريمة المنظمة وبسبب تقدم وسائل الإتصال والتكنولوجيا أصبحت غير محددة لا قيود الزمان ولا قيود المكان، بل أصبح إنتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية، كما إستغلت

1 – خالد الممدوح إبراهيم، مرجع سابق، ص ص 452 – 455.

2 – ناصر محمد البقهي، أثر التحويل المجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف عبد العزيز لدراسات الأمن الفكري بجامعة الملك سعود، المملكة العربية السعودية ، سنة 2009، ص 87.

عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الأنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بسهولة.

وبذلك إكتشفت جماعات الجريمة المنظمة إستخدام التكنولوجيا بصفتها فرص للإستغلال وتحقيق الأرباح غير مشروعة، ويرجح أن الترابط بين الجريمة المنظمة وشبكة الأنترنت في تطور إلى حد بعيد في المستقبل في الجريمة. [1]

ثالثا : الإرهاب

أصبح الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعوامل إجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث[2]، حيث أصبح بث ثقافة الإرهاب عبر الأنترنت عن طريق تأسيس مواقع إفتراضية تمثل المنظمات الإرهابية، وأصبحت الجماعات الإرهابية تجند عناصر جديدة من خلال الأنترنت فتعلن عبر مواقعها على الأنترنت حاجتها إلى عناصر إنتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب ، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الإستشهاد في سبيل الفور بالجنة. [3]

أضحت المواقع الإليكترونية تتيح للجماعات الإرهابية قدرا كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها لفئات مختلفة من الجمهور ورسم صورة ذهنية عن جماعة عن أعدائها أيضا. [4]

رابعا : الجريمة التجسس الإليكتروني

عمليات التجسس والتنصت هي عملية قديمة قدم البشرية وبقدر النزعات، فمنذ قدم العصور كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم وخططهم ، إلا أنه وبظهور عصر

---

1 – سامي علي عياد، الجريمة المعلوماتية و الأنترنت (الجرائم الإليكترونية)، الطبعة 1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007،ص 83.

2 – عبد الله بن عبد العزيز يوسفي، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية، الرياض ، الطبعة الأولى ، سنة 2004، ص 25.

3 – محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإليكترونية، دار ناشري للنشر والتوزيع الإليكتروني، 2004،ص 13.

4 – Debray Stephan, internet face aux substances illicites, université de paris, 2002-2003,p13.

المعلومات والإتصالات وإزدهاره تحولت وسائل التجسس والتنصت من الطرق التقليدية إلى الطرق الإليكترونية لا سيما مع إستخدام شبكة الأنترنت وإنتشارها الواسع على مستوى العالم.

ويمكن الخطر الحقيقي في عمليات التجسس التي تقوم بها الأجهزة الإستخبارتية للحصول على أسرار أو معلومات الدولة، ومن ثم إفشائها لدول أخرى تكون عادة معادية لها، أو إستغلالها بما يضر بالمصلحة الوطنية للدولة [1].

وتستهدف عملية التجسس في عصر المعلومات ثلاثة أهداف رئيسية، وهي التجسس العسكري، التجسس السياسي ، التجسس الإقتصادي. [2]

المطلب الثاني : المعلوماتية هدفا من إرتكاب الجرائم

بعدما رأينا الجرائم التي تكون المعلوماتية وسيلة لإرتكاب الجرائم فيها، لابد من نعلم ان هناك نوع آخر من الجرائم تكون فيه المعلوماتية هدفا من إرتكاب الجرائم، وقد تجسد ذلك نوعين من الجرائم ، وهي الجرائم الواقعة على نظم المعالجة الآلية للمعطيات وكذلك الجرائم الواقعة على المعلومات داخل الأنظمة المعالجة للمعلومات وذلك ما سنتطرق إليه عبر الفرعين الآتيين:

الفرع الأول : الجرائم الواقعة على نظم المعالجة الآلية للمعطيات

أولا : الجريمة الدخول أو البقاء غير المشروع في المنظومة المعلوماتية

1- جريمة الدخول غير المشروع:

إن المشرع الجزائري جرّم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية وإعتبر هذا التصرف في حد ذاته يشكل جريمة، إذ يستخلص لأول وهلة أن مجرّد إختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو مجرّد التسلية يعد إنتهاكا لنظام المعلوماتي بطريقة غير مشروعة [3].

1 - خالد ممدوح إبراهيم، مرجع سابق، ص ص 338 ، 339.

2 – علي عدنان الفيل، الإجرام الإليكتروني، الطبعة الأولى ، منشورات زين الحقوقية ، دمشق، 2011،ص ص 96 ، 97.

3 – هدى حامد قشوش، جرائم الحاسب الإليكتروني في التشريع المقارن، الطبعة الأولى ، دار النهضة العربية ، سنة 1992 ،ص 62.

والجريمة هنا تتحقق بالصور التالية :

– بمجرد الوصول إلى نظام معلوماتي لكن بطريق الغش، أي أنها جريمة عمدية تقوم بتوافر القصد الجنائي العام.

– أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه ويتوضح معنا من نص المادة 394 ق.ع. أن الجريمة الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك أي أضرار بالمعلومات ودون تحديد للزمن، وذلك أنها جريمة وقتية. [1]

حيث نصت المادة 394 ق.ع. على ما يلي : " يعاقب بالحبس 03 أشهر إلى سنة وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية المعطيات أو يحاول ذلك"[2].

2– جريمة البقاء في منظومة المعلوماتية :

لاحظنا نص المادة 394 ق.ع. يجرم الدخول وكذلك البقاء في المنظومة المعلوماتية ومما يتعين الوقوف عنه هنا هو أن المشرع فرق بين فعل الدخول غير المشروع وبين البقاء دون وجه قانوني أو مصلحة قانونية .

ويمكننا إبعاد ذلك إلى سبب بسيط يبرر هذه التفرقة وهو أنه إن كان الدخول عن طريق الخطأ يتنفى معه الجرم، فإن البقاء عن قصد يشكل جرما قائما بذاته يوحي عن إرادة الجاني غي الإضرار بالغير.

وهذا ما يؤكده توافر القصد الجنائي لديه ولم ننجد في القانون المقارن رأيا يحدد بدقة زمن إنتهاء جريمة الدخول.

وبداية جريمة البقاء في المنظومة أو في جزء منها.

1 – زبيجة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع عين مليلة، الجزائر، سنة 2011،ص 49.

2 – المادة 394 من قانون العقوبات الجزائري المعدل والمتمم بموجب القانون رقم 15/04 المؤرخ في 2004/11/10.

غير أن البعض إعتبر بأن بدايتها تكون منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام المعلوماتي ويستهدف إعتدائه على المعطيات المخزنة او بستهدف المعدات إعتدائه على المعطيات المخزنة أو يستهدف المعدات المتصلة به، مما قد يترتب عليه حذف البيانات أو المعطيات أو تغييرها ، او تخريبها وتخريب نظام إشتغال المنظومة. [1]

ثانيا: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الآلية

وهي جريمة يقوم من خلالها الجاني بإدخال معطيات أو برامج جديدة أو معلومات وهمية أو مزيفة ومَعْلُومٌ أن أي تدخل في نطاق البيانات يعد تدخلا في الكيان المنطقي للحاسوب الآلي والذي يكون بغرض الوصول إلى نتيجة معينة هي بمثابة هدف الجاني لذلك فإن البرامج الجديد إما أن يكون برنامجا وهميا يهدف إلى التمويه والتظليل في إرتكاب الجريمة وتغيير في الحقيقة وتعتبر مرحلة إدخال البيانات أو البرامج أو المعطيات الجديدة كما سماها المشرع الجزائري أهم المراحل في الجريمة الإليكترونية فهي التي تمهد لمرحلة أخطر وهي مرحلة إستغلال البيانات ، حيث نص المشرع الجزائري على هذه الجريمة في نص المادة 394 مكرر1 ق.ع. والذي قام من خلالها بمضاعفة العقوبات المنصوص عليها في المادة 394 ق.ع آنفة الذكر.[2]

ثالثا : جريمة التعامل في معلومات غير مشروعة .

حرص المشرع الجزائري تبني سياسية جزائية تكفل الحماية لنظم المعالجة الآلية فأول ما قام به هو تجريمه لمجموعة من الفعال تصب كلها في التعامل في المعلومات صالحة لأن ترتكب بها إحدى الجرائم التي تمس سرية المعلومات أو سلامتها [3]وهذا ما جاء في المادة 394 مكرر 2 حيث أخذت هذه الجريمة صورتين بحيث تتضمن كل صورة منها مجموعة من الأفعال

1 – زبيجة زيدان، مرجع سابق، ص ص 50 ، 51.

2 – زبيجة زيدان، مرجع نفسه، ص 54 .

3 – رشيدة بوكر ، مرجع سابق، ص 274.

المكونة للركن المادي للجريمة التعامل في المعلومات غير مشروعة بمكن توضيحها بشكل مختصر كالأتي[1] :

1- الصورة الأولى : جاءت المادة 394 مكرر2 في الفقرة (1) وهي كالأتي :

أ- **التصميم** : وهو عملية تتمثل في إعداد معلومات صالحة للإرتكاب الجريمة، وهذا العمل يقوم به عادة المختصون في هذا المجال كالمبرمجين ومصممين البرامج مثل: تصميم برامج الفيروسية أو البرامج الإختراق.[2]

ب - البحث : وهو البحث عن المعلومات لمعرفة كيفية تصميم المعلومات وإعدادها لكي ترتكب بها الجرائم.

ج - الجرائم : هو القيام بجمع قدر كبير من المعلومات التي تشكل خطرا كبيرا والتي من الممكن أن ترتكب بها إحدى جرائم الإعتداء على نظم المعالجة الآلية.[3]

د - التوفير : وهو عرض المعلومات وإتاحها وجعلها في متناول الغير وتحت تصرفه وحيازته، وترتكب بها جريمة الدخول أو البقاء أو جريمة التلاعب في الأنظمة.

هـ - النشر : وهو إذاعة المعلومات محل الجريمة وتمكين الغير من الإطلاع عليها، إذ من شأنه نقل هذه الأخيرة إلى عدد كبير من الأشخاص[4]وهذا ما يزيد من خطورة هذا الفعل.

و - الإتجار: وهو الإتجار بالمعلومات وتقديمها للغير بمقابل سواء كان بمقابل نقديا أو عينيا أو خدمة أو غيرها [5].

2- **الصورة الثانية** : وقد جاءت في المادة 394 مكرر 2 الفقرة 2 وهي كالاتي :

---

1 - نصت المادة 394 مكرر 2 على الأتي : " يعاقب بالحبس من شهرين إلى 03 سنوات وبغرامة من 100.000دج إلى 500.000دج كل من يقوم عمدا وعن طريق الغش للأفعال المكونة للركن المادي هذه الجريمة

2 - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الألي في القانون الجزائري والمقارن، دار الجامعية الجديدة الإسكندرية سنة 2007، ص 200.

3 - رشيدة بوكر ، مرجع سابق،ص 281.

4 - رشيدة بوكر ، مرجع سابق،ص282 - 283.

5 - محمد خليفة ، مرجع سابق، ص 204.

أ – **الحيازة** : وهي السيطرة الحائز على المعلومات بنية إحتباسها لكي يعدل فيها، أو ينتفع به، أو يستعملها، بطريقة غير مشروعة.

ب – الإفشاء : وهو الإفشاء الغير المشروع للمعلومات التي يحصل عليها بطريقة غير مشروعة عبر الوسائل التقنية الجديدة، وإنتقال المعلومات من الحيازة الجاني غلى غيره من الأشخاص .

ج – **النشر** :أصبحت نظم المعالجة الآلية ذاتها وسيلة فعالة في نشر المعلومات المتحصل عليها من جريمة من جرائم التي ذكرناها سابقا ، حيث يتم ذلك بسرعة وكفاءة عالتين ومثال ذلك قضية الفتى البالغ من العمر 21 سنة التي عرضت على مجلس قضاء باتنة والتي سبق وأن سردنا وقائعها.

د – **الإستعمال** : وهو الإستعمال الغير المشروع للمعلومات مهما كان الهدف منه في هذا الإستعمال، ومهمت كان نوعه أو الوسائل المستخدمة في ذلك، وحتى لو تم هذا الإستعمال لمرة واحدة .[1]

الفرع الثاني : الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية لمعلومات

أولا : سرقة المال المعلوماتي

وهي عملية الإستلاء على المعلومات المخزنة داخل الجهاز دون وجه الحقأو نسخ هذه المعلومات، وهو ما يعبر عنه حاليا بالقرصنة، عرفها بأنها :" سرقة المعلومات من برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية غير شؤعيةبعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أو بواسطة إلتقاط الموجات الكهرومغناطسية الصادرة عن الحاسب الآلي أثناء تشغيله وبإستخدام هوائيات موصلة بحاسبة خاصة "[2].

1 – رشيدة بوكر ، مرجع سابق، ص ص285– 286 – 290.

2 – إنتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية ، بيروت، سنة 1994،ص 57.

ونظرا لما تمثله القرصنة في وقتنا الحاضر من تهديد لمستقبل التقنية وصناعة المعلومات فأصبحت هذه الأخيرة تثير إشكالا يتعلق بطبيعة المعلومات الخاصة ذلك أن ليس لها كيان مادي محسوس وتبقى في حيازة مالكه وبالتالي يثور تساؤل حول ما إذا كانت المعلومات تصلح محلا لجريمة السرقة أم لا ؟

وممّا لا شك فيه أن المعلومات وإذا كانت تثير إشكالا في مدى إعتبارها من الأموال التي يمكن سرقتها، إلاّ أنه من المسلم بيه أن هذه المعومات إبتداءا يمكن أن تترجم إلى قيم مالية نظرا لقابليتها للإستغلال، مقارنة بالبرامج التي هي نوع من الإبداع الذهني والفكري، وبما أن البرامج عبارة عن أسلوب يظم العمل والمعالجة فإن إستخدام هذا الأسلوب بصورة غير مصرح بها من قبل مالكها أو حائزها الشرعي يشكل إعتداء على حقوق الإستغلال المالي.

وكذلك فإن المعلومة بما تمثله من صفة السرية يمكن الإعتداء عليها بمجرد الإطلاع عليها دون إذن صاحبها لأن هذا يمثل إنتهاكا لسرية المعلومة .

وبتحليل عناصر جريمة السرقة كون المال فيها يكون منقولا ومملوكا للغير ونقل حيازته من حائزه الشرعي إلى سارق فإننا نرى وجوب عدم قياس نصوص السرقة التقليدية على السرقة المعلومات بإعتبار أن معظم التشريعات لا تعترف بسرقة المعلومات بل الوصول غير المصرح لها وإختراقها وتقليدها والإستلاء عليها ونسخها نسخا غير مشروعا [1] .

وفي ظل الخلاف الفقهي الوارد بشأن قابلية هذه البرامج لتطبيق الأفعال المكونة لجريمة السرقة عليها عن عدمه وممّا يدعو بالتالي لإقتراح أن يتدخل المشرع بنصوص صريحة لمواجهة هذه الظاهرة الجديدة للإجرام التي تعيش على هامش القانون مستغلة بذلك النقص والثغرات التي توجد بالتشريع القائم [2].

1 – محمود أحمد عبابنة، مرجع سابق، ص ص 94– 95.

2 – خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر 2010، ص ص 55– 56.

ثانيا : إتلاف معلومات وبرامج الحاسب الآلي

وبقصد بإتلاف برامج الحاسب الآلي ومعلوماته إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات sabotage informatique وعادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه بل مجرد إعاقة نظام المعلومات عن الإداء بوظائفه وإحداث الضرر.

والمقصود من الإتلاف في هذا المقام ليس الإتلاف المادي، وإنمّا ذلك الذي يوجه إلى جانب المنطقي والمعنوي في الحاسب الآلي الذي بات يشكل قيمة إقتصادية عالية فإتلاف برامج ومعلومات الحاسب الآلي إفقاد لمنفعة هذه البرامج والمعلومات .

وترتكب جرائم إتلاف البرامج والمعلومات عن طريق قنابل منطقية[1]، أو عن طريق برامج الدودة والفيروس « virus » ، الذي يقصد به " برنامج ثم إعداده من قبل شخص أو أكثر على درجة متقدمة من العلم بالبرمجة بإستخدام تقنيات متطورة، بحيث يكون من خصائص هذا البرامج الإنتقالإلى أجهزة الحاسب الآلي والتكاثر والإنتشار فيها وهي برامج غير مرئية بالطرق العادية وتحتاج إلى أسلوب علمي للكشف عنها".[2]

وبسبب الفيروسات التي تنتشر في أجهزة الحاسب المتصلة بالشبكات العامة والخاصة المتعلقة بإتصال بين الحواسيب تدمر البرامج والمعلومات المخزنة داخل الجهاز، بحيث يتعطل عن العمل والقيام وبوظائفه وتضليل مستخدميه وضياع بياناته وتحويله إلى آلة صماء لا فائدة منها. [3]

1 – القنابل المنطقية أو الزمنية : تعرف بانها برامج أو جزء من برنامج ينفذ في لحظة محددة، أو كل فترة زمنية منتظمة، يوضع على شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع. عن الدكتور محمد سامي الشاوا، ثورة المعلومات وإنعكساتها على القانون العقوبات، دار النهضة العربية، القاهرة، سنة 1994، ص 194.

2 – أسامة محمد محي الدين عوض، جرائم الكمبيوتر، بحث مقدم إلى مؤتمر السادس للجمعية العربية للقانون الجنائي ، ص 425.

3 – محمد أحمد عبابنة، مرجع سابق ، ص 101.

لذلك يستوجب الأمر توفير حماية للمكونات المعنوية عن طريق نصوص تشريعية خاصة تراعي خصوصيتها لأن العقوبات البسيطة التي وضحت في ق.ع. لا يتحقق قمع وردع جريمة إتلاف المعلومات لأنها بإتلاف الأموال المادية الملموسة ليس معنوية. [1]

ثالثا : التزوير المعلوماتي

هو أي تزوير يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم بطريقة الطابعة أو كانت مرسومة عن طريق الراسم، ولذلك فالتزوير المعلوماتي قد يرد في محرر مكتوب لغة سواء باللغة العربية أو بأنه لغة أخرى مفهومة ولها دلالتها، وكذلك قد يتم في مخرجات ورقية غير مكتوبة أي مصورة طلما كانت الصورة محل إعتبار في محرر أو مستند ويترتب عليها إثبات الحق أو أثر قانوني معين. [2]

كما عرفت المادة الرابعة جريمة التزوير المعلوماتي من القانون على أنه :" كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسوب، أو على شريط أسطوانة ممغنطة أو غيرها من الوسائط يعاقب ب .... وتترك العقوبة وفقا لكل دولة".

كما نصت الفقرة الثانية من المادة الرابعة من نفس القانون على أنه:" كل من إستخدم المستندات المزورة آليا مع علمه بتزويرها يعاقب بنفس عقوبة التزوير، فإذا كان المستخدم هو نفسه مرتكب فعل التزوير يعاقب وفقا للقواعد العامة المعمول بها في هذا الشأن".[3]

فالتزوير في صورته التقليدية هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون، تغييرا من شأنه أن يترب ضررا للغير وبينه إستعمال هذا المحرر فيما أعد له.

1 – رشيدة بوكر، مرجع سابق، ص 114.

2 – خيرت عليّ محرز، التحقيق في الجرائم الحاسب الآلي، القاهرة، سنة 2012، ص ص 170 – 171.

3 – المادة 2 و 4 من القانون النموذجي العربي الموحد لمكافحة الجرائم المعلوماتية وما في حكمها، الدورة 19 بقرار رقم 495 في 2003/10/08.

أما التزوير المعلوماتي فهو تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية إستعمالها. [1]

وما يمكن ملاحظته في جريمة التزوير المعلوماتي أنها أثارات جدلا واسعا وتساؤلات كثيرة في الجانب الفقهي وكذا القضائي، وأبرزها كان القضاء الفرنسي وكانت تلك التساؤلات تدور حول مدى كفاية نصوص القوانين التقليدية للإنطباق على التزوير المعلومات؟.

وعلى هذا الأساس وبعد صدور القانون الفرنسي الجديد في 1992/12/16قرر المشرع لفرنسي عدم ضرورة إلا بقاء على التجريم الخاص بتزوير المستندات المعالجة آليا وإستعمالها، والإكتفاء بإضافة إلى جريمة التزوير العادية، ولعّل من أهم الأسباب التي أدت بالمشرع الفرنسي إلى إدراج هذه الجريمة ضمن جرائم التزوير العادية للمحررات هو أنه بصدور هذا القانون خرجت جريمتا تزوير المستندات المعالجة آليا وإستعمالها من بين جرائم الإعتداء على نظام المعالجة الآلية للمعطيات، وهو أمر منطقي يجد مبرر في إختلاف المصلحة المحمية بالقانون والتي تقف وراء تجريم كل منهما، فالمصلحة المحمية من تجريم الإعتداء على نظام المعالجة الآلية للمعطيات هي مصلحة فردية تخص صاحب هذا النظام المعلوماتي، في حين أن المصلحة التي يحميها القانون بصدد جريمة التزوير في المستندات والمحررات المعلوماتية فهي حماية الثقة العامة المقترحة في هذه المستندات أيّا كان شكلها، ومن خلال هذا المنطلق يمكن القول أن المشرع الفرنسي قد عاقب على جريمتي تزوير المستندات المعلوماتية من جهة، وإستعمالها من جهة أخرى [2].

ونلخص أن المشرع الجزائري رغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الإعتداءات الواردة على الأنظمة المعلوماتية بإستحداث نصوص خاصة إلا انه أغفل تجريم الإعتداءات الواردة على

1 – فوزية عبد الستار، قانون العقوبات (القسم الخاص) ، دار النهضة العربية، بدون بلد النشر، سنة 1988، ص ص 244.

2 – خثير مسعود ، مرجع سابق، ص ص 132 – 133.

المنتوجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى ٱتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث، رغم أنها تعتبر من أخطر صور الغش المعلوماتية .[1]

1 - آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007.، ص 140.

الفصل الثاني
خصوصية الجريمة المعلوماتية من الناحية الإجرائية

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركةالجريمة و تطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الإستعانة بالأساليب العلمية و استخدام شبكة الإنترنت هي الصفة المميزة و الغالبة، ومرد ذلك هو حدوث طفرة علمية في مجال تكنولوجيا المعلومات والإتصالات و استخدام الوسائط الإلكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئا حديثا وجد الإكتشاف طريقه إلى مجال الإثبات الجنائي و التدليل، وقد اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وعرفها بموجب القانون 09-04 المؤرخ في 05 غشت 2009 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات[1] و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

إن الجريمة المعلوماتية ترتكب بإستخدام التقنية المعلوماتية مما يعني انها ترتكب في فضاء إفتراضي مفرغ، يختلف كليا عن مسرح التقليدي الذي ترتكب فيه الجريمة حيث يتم الإستدلال عليها وضبطها وإثباتها بوسائل تقليدية، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات الجريمة المعلوماتية التي أرتكبت في عالم إفتراضي غير ملموس. فمن ناحية المنطلق سوف نحاول إبراز خصوصية الجريمة المعلوماتية من الناحية الإجرائية، وهو سنتطرق إليه في المتابعة القضائية في الجريمة المعلوماتية في المبحث الأول وأيضا أساليب التحري والتحقيق وإثبات في جريمة المعلوماتية في المبحث الثاني .

[1] – القانون رقم 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها. جريدة رسمية عدد 47. الصادرة بتاريخ: 16 غشت 2009.

المبحث الأول : المتابعة القضائية في جريمة المعلوماتية.

نظرا لطبيعة الخاصة للجريمة المعلوماتية وما نتج عنها من تساؤلات وتناقضات حول إستجابة هذه الجريمة للقواعد الإجرائية التقليدية وبالأخص ما يثار حول قواعد الإختصاص القضائي في الجريمة المعلوماتية، وكذا المساعدة القضائية الدولية في مجال المعلوماتية وهذا ما سنتطرق اليه في مطلبين كالآتي :

المطلب الأول : الإختصاص القضائي في جريمة المعلوماتية

حظي الإختصاص القضائي المتعلق بالجرائم المعلوماتية بالكثير من الإهتمام والجدل لذلك سوف نحاول طرح أهم الإختصاصات في موضوع عبر الفروع الآتية:

الفرع الأول : إختصاص النيابة العامة في تحريك الدعوى العمومية في مجال جرائم المعلوماتية في التشريع الجزائري

يتعين التأكيد هنا بأن الأمر لا يخرج عن نطاق المادة الأولى من قانون الإجراءات الجزائية وفق إستثناءات حددها هذا القانون نفسه، كما سوف نرى ومن الواضح أيضا إن دور النيابة العامة كما رسمته المادة 29 من ق.إ.ج.ج[1] وكذا المادة 36 يكون قد توسع في ظل المستحدثات والتطور الحاصل في مجال الجرائم المنظمة والجرائم عابرة الحدود والجرائم المعلوماتية على الأخص.

ومما يتعين الإشارة إليه أن تحريك الدعوى العمومية في جرائم الأنترنت وتقديم الشكاوى بشانها من قبل المتضررين، بات محل إهتمام الهيئات الدولية، فبالإضافة إلى القرارات الصادرة عن الأمم المتحدة بخصوص الجرائم المتصلة بالكمبيوتر في توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد سنة 1994 بالبرازيل بشأن جرائم الكمبيوتر، والذي أبرز الوجود المركز العالمي للشكاوي الخاصة بجرائم الأنترنت، حيث يعتبر هذا المركز من أهم المؤسسات التي ظهرت إلى الوجود في مجال مجابهة جرائم الأنترنت الذي تأسس في الولايات المتحدة الأمريكية سنة 1999.

[1] – المادة 29 من ق.إ.ج.ج.

وهو الموقع الذي يتلقى شكاوي أي شخص في أية بقعة من العالم ، ويعمل هذا المركز على التعاون مع مختلف المنظمات الدولية والوكالات المتخصصة في محاربة جرائم الأنترنت.

ومن هنا يتضح أن إختصاص النيابة العامة توسع مجاله ليمتد ويغطي نطاقات أخرى لم تكن مرخصة لها من قبل، إذ أن المادة 37 من ق.إ.ج.ج. بعد تعديله بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004وبعد أن كان إختصاص المحلي لوكيل الجمهورية محصورا في المجالات التالية:

- بمكان وقوع الجريمة .
- بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة بالمكان الذي تم في دائرته القبض على أحد الأشخاص المشار لهم ولو لسبب آخر.
- فإنه نص على تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى في إطار جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بقوانين الصرف وذلك عن طريق التنظيم. [1]

كما جاء في نص المادة 37 ق.إ.ج.ج وبصدور المرسوم التنفيذي رقم 348/06 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[2] ليكون بذلك قد شمل الإختصاص المحلي للنيابة العامة كل ربوع الوطني في ما يخص الجرائم المعلوماتية، علما أن المحاكم التي تم تمديد إختصاصها أصطلح على تسميتها في التشريع الجزائري بالأقطاب أو محكمة القطب.

والنيابة مجال إختصاص واسع جدا في إطار البحث والتحري عن الجرائم المعلوماتية ومنح الإذن بالتفتيش والقيام بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور كما هو

[1] - زيبحة زيدان، مرجع سابق،ص 109إلى 111.

[2] - المرسوم التنفيذي رقم 06-348 مؤرخ في 05 أكتوبر سنة 2006 ،المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة رسمية عدد 63 ،ص .29

منصوص عليه في المادة 65 مكرر 5 من ق.إ.ج.ج وسوف يأتي شرحه، وهذا بالإضافة إلى إستعمال التقنيات المخزنة وكذا حجز هذه المعطيات هذا فضلا عن إتخاذ التدابير الملائمة والتحفظية في إطار المساعدات الدولية المتبادلة في مجال الجريمة المعلوماتية.

الفرع الثاني : الإختصاص المحلي لقاضي التحقيق في جرائم المعلوماتية

من المعلوم أن المشرع الجزائري سار بوتيرة متسارعة على خطى التشريعات العالمية ، في إطار مواكبة التطور الحاصل في مضمار القانون لمجابهة التطور الحاصل في مجال الإجرام بصوره الحديثة لا سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1] ،وفي هدا الاتجاه جاء تعديل قانون الإجراءات الجزائية بموجب القانون رقم 014/04 المؤرخ في 10 /2004/11 ومس التعديل المادة 40 من قانون إ .ج.ج لتصبح كما يلي :

"يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر" [2] .

يجوز تمديد الإختصاص المحلي لقاضي التحقيق إلى دائرة إختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

ومن الملاحظ أن تمديد إختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة للنيابة العامة بأحكام المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 وقد حددت المادة الأولى من المرسوم المشار له مجال الإختصاص المحلي الممدد في النطاق

[1] – زيبحة زيدان، مرجع سابق، ص 113 و 114.

[2] – المادة 40من ق.إ.ج.ج.

الأقطاب القضائية المحددة في المواد 2، 3، 4، 5 من نفس المرسوم في الجرائم المذكورة سابقا وما يهمنا في الموضوع هو ما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الثالث ، الصلاحيات المكانية للضبطية القضائية في الجرائم المعلوماتية

من الواضح أن المشرع الجزائري يكون قد سارع إلى تدارك النقص وسد الفراغ القائم بخصوص مجلات التحقيق الإبتدائي إثر التطور الذي عرفته الجريمة لاسيما بأشكالها الحديثة كما هو الحال في الجرائم المعلوماتية لذلك جاءت تعديلات قانون الإجراءات الجزائية المتعاقبة لاسيما التعديل الذي جاء به القانون 22/06 المؤرخ في 2006/12/20 والذي مدد من صلاحيات الضبطية القضائية ووسع دائرة إختصاصها ودعمه في ذلك القانون رقم 04/09 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والإتصال ومكافحتها كما سوف نرى[1].

أناط القانون الجزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات تماشيا مع المبدأ الدستوري المتعارف عليه:" لا جريمة ولا عقوبة إلا بنص " [2]، وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي، ويتضح من نص المادة 12 قانون إ.ج.ج. أن مناط البحث عن الجرائم بالنسبة للضبطية القضائية ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم فإذا ما إبتدأ التحقيق القضائي تقلص دورها، لينحصر في تنفيذ

[1] – زيبحة زيدان، مرجع سابق، ص 155.

[2] – المادة 46 من الدستور الجزائري لسنة 1996 (منشور بموجب المرسوم الرئاسي رقم 96–436 مؤرخ في 07 ديسمبر 1996، يتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء شعبي يوم 28 نوفمبر 1996، جريدة رسمية عدد 76 مؤرخ في 28 نوفمبر 1996، معدل ومتمم بالقانون رقم 02–03 مؤرخ في 10 أفريل 2002، يتضمن نص تعديل الدستور، جريدة رسمية عدد 25 مؤرخ في 04 أفريل 2002، معدل ومتمم بالقانون رقم 08–19 مؤرخ في 15 نوفمبر 2008، يتضمن نص تعديل الدستور، جريدة رسمية عدد 63 مؤرخ في 16 نوفمبر 2008، معدل ومتمم بالقانون رقم 16–01 مؤرخ في 06 مارس 2016، يتضمن نص تعديل الدستور، جريدة رسمية عدد 14 مؤرخ في 07 مارس 2016) .

– الدستور الجزائري الصادر في 1 نوفمبر 2020 ،بموجب المرسوم الرئاسي رقم 20 . 442 المؤرخ في 30 ديسمبر 1 2020 ،المتعلق بإصدار التعديل الدستوري والمصادق عليه في الاستفتاء.

طلبات جهات التحقيق القضائي وإنجاز ما توجه إليهم من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي.

كما نصت عليه المدة ة18 مكرر من قانون إ.ج.ج في إطار الصلاحيات المحددة بنص المادة 36 من قانون إ.ج.ج.وكل ذلك تحت إشراف النائب العام وتحت رقابة غرفة الإتهام بدائرة إختصاص المجلس التابعين له، وفقا لأحكام المادة 206 من قانون الإجراءات الجزائية.

والمعلوم أن ضباط الشرطة القضائية نوعان : ويتمثل النوع الأول في هم الذين يتمتعون بإختصاص عام ويختصون بإجراءات الإستدلال بشأن للجرائم المنصوص عليها في قانون العقوبات، أما النوع الثاني فهم ذو الإختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر.

أما ما يهمنا في الموضوع هو دور الضبطية ومجال إختصاصها فيما يتعلق بالجرائم المعلوماتية، وعليه فإن الإختصاص الإقليمي لضباط الشرطة القضائية في مجال الجرائم المعلوماتية[1]، حسب ما نصت عليه المادة 16 ق.إ.ج.ج. بالقول :" يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة" [2].

إلا أنه يجوز لهم – في حالة الإستعجال –أن يباشروا مهمتهم في كافة دائرة إختصاص المجلس القضائي الملحقين به، وكذلك في كافة الإقليم الوطني إذا طلب منهم ذلك من القاضي المختصين قانونا.

غير أنه يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد إختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني .

[1] – زيبحة زيدان، مرجع سابق، ص 116 و 177.

[2] – المادة 16 من القانون الإجراءات الجزائية الجزائري .

ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات[1] مع العلم أنه يدخل من ضمن إختصاصات ومهام ضباط الشرطة القضائية الإنابة القضائية المرخص بها من طرف السلطة القضائية المختصة في سبيل ملاحقة الجرائم المعلوماتية .

المطلب الثاني :المساعدة القضائية الدولية في مجال الجرائم المعلوماتية

لقد اثبت الواقع العملي أن إي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية خاصة مع التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات .واتصافها بالعالمية على أساس أنها لم تعد تتمركز في دولة معينة ولا توجه للدولة بعينها بل أصبحت عابرة للحدود وتمس أضرارها سيادة العديد من الدول مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات.

ويستوجب على أعضاء المجتمع الدولي من الإيفاء بالالتزامات المترتبة على هده العضوية ومن ضمها الارتباط بعلاقات دولية ثنائية متعلقة بالمساعدة القضائية المتبادلة ودلك لتعزيز التعاون بينها واتخاذ تدابير فعالة للحد منها والقضاء عليها لمعاقبة مرتكبيها .فأجهزة أنفاد القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين من حدودها إلى أقاليم دول أخرى ذات سيادة ولذلك كان لابد من التعاون بين الدول لاتحاد الإجراءات القضائية فوق أقاليمها. فالدول بمفردها لا تستطيع القضاء على هذا النوع من الجرائم لتمييزها بمجموعة من الخصائص فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت غالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة، و أتاح التطور في العلوم وانتشار تقنيات تكنولوجيا المعلومات مجالا

[1] – زيبحة زيدان ، مرجع سابق، ص 118.

واسعا لتنفيذ العديد من الجرائم بعيدا عن أعين الجهات الأمنية هذا ما جعل الجريمة تتغير من صورتها التقليدية المادية إلى أخرى معنوية تتجاوز حدود الدول[1].

نظرا للطبيعة الخاصة التي تتميز بها الجريمة المعلوماتية بإعتبارها جريمة عابرة للحدود ، فإن ذلك دفع بعض الدول إلى ضرورة اللجوء إلى المساعدة القضائية المتبادلة من أجل ضبط هذه الجريمة وملاحقة مرتكبيها وتسلط العقاب عليهم، ولكن هذه المساعدة القضائية الدولية لا تخلو من المعيقات والقيود التي تقف أمام تطبيقها وهذا ما سنتناوله في الفروع الآتية.

الفرع الأول : التعاون القضائي الدولي وتبادل المعلومات لملاحقة الجرائم المعلوماتية.

لما كانت جرائم المعلوماتية ذات طابع عالمي وبالتالي يمكن أن تتعدى أثارها عدة دول ، فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم، يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث أرتكبت الجريمة أو جزء منها، مثل معاينة مواقع الأنترنت في الخارج، أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة أو صور إباحية، أو تفتيش الوحدات الطرفية في حالة الإتصال عن بعد أو القبض على المتهمين، أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي يمكن أن تساهم في التحقيق في هذه الجرائم، وكل ذلك لا يتحقق بدون مساعدة الدول الأخرى، ولذلك تتضمن معظم الإتفاقيات الخاصة بالجرائم التقليدية نصوصا تقضي بضرورة اللجوء إلى المساعدة المتبادلة بهدف تحقيق السرعة والفعالية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم. [2]

ويمكن تعريف المساعدة القضائية الدولية بأنها :" كل إجراء قضائي تقوم به دولة من شأن تسهيل مهمة المحاكمة في دولة أخرى، بصدد جريمة من الجرائم"[3] وتتخذ المساعدة

[1] – برقوق يوسف، ، المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01 ، العدد ، 01، 2021، ص94.

[2] – جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، سنة 2001 ص 79.

[3] – سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية ، دراسة مقارنة)، رسالة دكتوراه ، كلية الحقوق ، جامعة عين الشمس، سنة 1997، ص 425.

القضائية في المجال الجنائي صور عديدة منها: تبادل المعلومات : وهو يشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما، عن الإتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي إتخذت ضدهم وبالإضافة الى نقل الإجراءات ويقصد بها قيام دولة بناءا على إتفاقية، إتخاذ إجراءات جنائية بصدد جريمة إرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك إذا توافرت شروط معينة .

1- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها.

2- أن يكون الإجراء المطلوب إتخاذه مقرر في قانون الدولة المطلوب إليها عن ذات الجريمة.

3- أن يكون إجراء المطلوب إتخاذه يؤدي إلى الوصول إلى الحقيقة .

وقد أقر المجلس الأوروبي إتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنظمة إمكانية محاكمة الجاني طبقا لقوانينها، بناءا على طلب دولة أخرى طرف من هذه الإتفاقية بشرط أن يكون الفعل معاقبا عليه في الدولتين. [1]

أما بالنسبة للجزائر وبمناسبة صدور القانون رقم 04/09 المؤرخ في 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والإتصال ومكافحتها فقد أكدت في المادة 16 منه على أنه في إطار التحقيقات والتحريات القضائية التي تمت مباشرتها، وتتبع الجرائم المنصوص عليها في هذا القانون 04/09 والكشف عن مرتكبيها فإن السلطات الجزائية المختصة بإمكانها تبادل المساعدات القضائية في المستوى الدولي.

وفي النقطة المتعلقة بجمع الأدلة الخاصة بالجريمة المعلوماتية وجمع الأدلة يعد من إجراءات التحقيق القضائي، ويمكن أن يكون بواسطة الدخول إلى المنظومة المعلوماتية المشكوك في تخزينها للمعلومات المبحوث عنها كما أشير لها في المادة05 من القانون المذكور أعلاه، وأنه ونظرا للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة،

[1] – طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 598و 599.

فإن المشرع أجاز في حالة الإستعجال قبول طلبات المساعدة القضائية الدولية حتى وإن ورد عن طريق وسائل الإتصال السريعة مثل : الفاكس أو البريد الإليكتروني ، شريطة التأكد من صحتها. [1]

وبهذا الصدد أوجبت المادة 36 من القانون رقم 06/05 لصادر في 08/23/ 2005 والمتعلق بمكافحة التهريب المعدل بالأمر رقم 09/06 في 2006/07/15 :" على أنه وفي حالة توجيه الطلب إلكترونيا من طرف السلطات الأجنبية يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا "[2].

كما نصت المادة 17 من قانون 04/09 على أنه :" تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة و الإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل ".[3]

الفرع الثاني : القيود الواردة على طلبات المساعدة القضائية الدولية

نادت بعض الدول بضرورة إنشاء وحدات خاصة بمكافحة الجريمة المعلوماتية بواسطة الحاسب الآلي والأنترنت أُسْوَةً بجهات البحث الجنائي، الوطنية والدولية والتي هي الأنتربول لإثبات الجريمة عند وقوعها وتحديدا أدلتها وفاعلها، وهو كذلك ما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الإعتداء على المعلومات الخاصة في الأنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها[4]

– ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك عوائق تحول دون ذلك، تجعل هذا التعاون صعبا لما يلي :

---

[1] – زيبحة زيدان ، مرجع سابق، ص 145.

[2] – المادة 36 من القانون رقم 06/05 الصادر في 2005/08/23 المتعلق بمكافحة التهريب المعدل بالأمر رقم 09/06 في 2006/07/15.

[3] – المادة 17 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

[4] – إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، جامعة الإمارات، في سنة 2000، ص 228.

أولا : عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك أن الانظمة القانونية في بلدان العالم قاطبة لم تتفق على صورة محددة يندرج في إطارها ما يسمى " بإساءة إستخدام نظم المعلومات الواجب إتباعها"، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي، ومن ثم الجريمة المعلوماتية [1] والخلاف المتمثل في أن يره البعض مباحا نظرا للطبيعة الخاصة للمعلوماتية عبر الأنترنت يراه الآخر غير مباح، ومن ثم يجرم الإعتداء عليه بالنقل أو النسخ، مرد ذلك إلى طبيعة النظام القانوني السائد في كل بلد من البلدان، صحيح ان بعض الدول مثل فرنسا والولايات المتحدة الأمريكية وكندا أصدرت تشريعات تتعلق بالجريمة المعلوماتية إلا أن هذه التشريعات لازالت في مهدها ولعل عدم الإتفاق بين الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على إرتكاب الجرائم المعلوماتية .

ثانيا : عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة المعلوماتية بين الدول المختلفة، خاصة ما تعلق منها بأعمال الإستدلال أو التحقيق، لاسيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في النظام معلوماتي معين هو أمر غاية في صعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته[2].

ثالثا : عدم وجود معاهدات ثنائية أو جماعية بين الدول على النحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الأنترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على النحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول ومن

[1] – مؤتمر القانون والكمبيوتر و الأنترنت، جامعة الإمارت، كلية الشريعة والقانون عام 2000،

[2] – عبد الفتاح بيومي حجازي ، الإثبات الجنائي في الجرائم الكمبيوتر والأنترنت، طبعة خاصة ، بهجات للطباعة والتجليد، مصر ، سنة 2009،ص 188.

ثم يظهر الأثر السلبي في التعاون الدولي، وهو ما حاولت الأمم المتحدة الإهتماما به، وكذلك بلدان أوروبا. [1]

رابعا: مشكلة الإختصاص في الجرائم الحاسب الآلي: وهي من المشكلات التي تعرقل الحصول على الدليل في الجريمة المعلوماتية ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الإختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع الجريمة الحاسب الآلي في مكان معين، وينتج أثارها في مقاطعة أخرى داخل الدولة أو خارجها، ومن هنا تنشا مشكلة البحث عن الأدلة الجنائية على شبكة الأنترنت وسبق لها أن أخترقت مواقع عديدة في دول مثل الصين والكويت وجورجيا والفتنام، بل هاجمت وكالة الفضاء الأمريكية – ناسا نقلا عن الإتحاد الإماراتية – العدد 9345 يوم 2001/02/04 خارج دائرة الإختصاص التي قدم فيها البلاغ، أو تم تحريك الدعوى الجنائية فيها، وكذلك تظهر مشكلات تتعلق بفحص لبيانات في مراكز معلومات دولا أخرى، وهو ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدولة. [2]

ونرى في هذا الخصوص أن مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس المعيار الذي سبق لمحكمة النقض وان أرسته، وإعتمده المشرع وهو مكان القبض على المتهم او محل إقامة المتهم أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة ينعقد الإختصاص القضائي لسلطات التحقيق والمحاكمة فيه بالجريمة المعلوماتية، لكن على المستوى الدولي فإن الأمر في حاجة إلى الإتفاقيات الدولية ثنائية أو الجماعية . [3]

[1] – عبد الفتاح البيومي حجازي، مرجع سابق، ص 189 و 190.

[2] – محمد الأمين البشري، بحث بعنوان التحقيق في جرائم الحاسب الآلي، مقدم إلى المؤتمر القانون والكمبيوتر والأنترنت، المنفعة في الفترة من 1–3 مايو 2000بكلية الشريعة والقانون بدولة الإمارات، ص 58.

[3] – عبد الفتاح بيومي الحجازي، مرجع سابق، ص 192.

أما بخصوص المشرع الجزائري فإن اللجوء إلى الأنابة القضائية أو المساعدات القضائية فإنها مقيدة بشروط منها:

1- إنها تتم وفقا للإتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات وإتخاذ الإجراءات التحفظية أو تسليم المجرمين في ما هو مرتبط بالجريمة الإليكترونية.

2- تخضع لمبدأ المعاملة بالمثل وهو المبدأ الذي أكدته أيضا المادة 29 من القانون رقم 01/05 صادر في 2005/02/06 والمتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحته .

اما لقيود الواردة عليها فقد حصرتهاالمادة 18 من القانون 04/09 فيما يلي :

- أنها لا تنفذ ولا يمكن الإستجابة لها في الحالات التالية :

1- إذا كان فيها مساس بالسيادة الوطنية.

2- إذا كانت ماسة بالنظام العام.

- ويمكن الإستجابة لها بشروط منها :

1- شرط المحافظة على السرية المعلومة المبلغة لتلك الدولة .

1- شرط عدم إستعمالها في غير الحالة المحددة والموضحة حصريا في طلب المساعدة القضائية وقد ألزمت الإتفاقية الدولية الموضوعة للتوقيع بمقر الأمم المتحدة في نيويورك في 2005/09/14 والخاصة بقمع الأعمال الإرهاب النووي ألزمت الدول الأطراف بإتخاذ التدابير لحماية سرية المعلومات التي يحصل عليها سرا بموجب هذه الإتفاقية من دولة أخرى .مما لاشك فيه أن السلطات الجزائرية باشرت العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية وإتخذت حيال ذلك تدابير منها إحالة بعض المتهمين على العدالة[1] فعلى سبيل المثال تم فتح تحقيق قضائي في 800 قضية متعلقة بالجريمة المعلوماتية منذ دخول القانون رقم 04/09 الصادر في 2009/08/05 حيز التنفيذ وهي القضايا التي تورطت فيها جزائريون وأجانب إستهدفت شبكات وقواعد البيانات لمؤسسات الجزائرية وأجنبية وأمثلتها كثيرة ففي إطار

[1] - زيبحة زيدان، مرجع سابق، 145 وما بعدها.

تنفيذ المساعدة القضائية الدولية والإنابة القضائية تمت متابعة شاب جزائري وإحالته على العدالة بمحكمة الجنح بباتنة وهو شاب عمره 21 سنة تقني سامي في الإعلام ، قام بإختراق موقع شركة أمريكية متخصص في حماية المعلومات والبرامج الإليكترونية لعديد من الشركات الأمريكية ثم عمل على إستغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية .

وإثر إيداع شكوى من قبل الشركة المتضررة لدى الشرطة الأمريكية قدمت هذه الأخيرة المعلومات الكافية بشأن المتهم المشار له إلى مصالح امن الجزائري .

وهناك حالة أخرى أيضا تتعلق بمتابعة ومحاكمة شاب جزائري وهو طالب جامعي بقسم الإعلام الآلي بعنابة من طرف سلطات الأمن الجزائري وهذا الشاب تمكن من قرصنة عدد كبير من البطاقات البنكية عقب إختراقه لمواقع إليكترونية لمؤسسات أجنبية في أوروبا والولايات المتحدة الأمريكية وفي كندا وتمكن من سحب أموال معتبرة وإثر المعلومات المتبادلة مع الأمن الجزائري في إطار المساعدة القضائية الدولية تمت متابعة البريد الإليكتروني الذي كان يستعمله " الهاركز" المتهم المشار له والذي أدين حكم من طرف محكمة الجنح بعنابة ثم إستفاد بتدابير المنفعة العامة وفقا لما ورد في الفصل الأول مكرر بالمادة 05 مكرر1 إلى المادة 05 مكرر06 من القانون العقوبات الجزائري، وهناك العديد من الأمثلة حتى بالمقابل بالنسبة لما تعرضت له مؤسسات جزائرية من أعمال قرصنة وإختراق ومن أمثلة ذلك إختراق موقع الشروق أونلاين ومحاولة تخريبه من طرف هاكرز مصرين[1]وبالرغم من نجاح السلطات في إثبات الجرائم المعلوماتية والقبض على المجرمين المعلوماتيين في إطار المساعدة القضائية الدولية نسبيا إلا أن القيود الواردة عليها تحول بينها وبين النجاح في مواضيع عدة أخرى.

لذلك يلاحظ أن التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية، وهو ذات ما سبق التنويه إليه من أن التشريعات الجنائية لا تتقدم بذات السرعة التي تتقدم بها وتنمو حركة الإتصالات والمعلوماتية التي عمت العالم كله، لذلك لا مناص من

[1] – زيبحة زيدان، مرجع سابق،ص 147 وما بعدها.

الإتفاقيات الثنائية أو الجماعية بين الدول لتسهيل التحقيق في الجرائم المعلوماتية وبالرغم من إبرام بعض هذه الإتفاقيات فأن دلك لم يفي بالمطلوب في حل مشكلات الإختصاص وتبادل الأدلة الجنائية وتسليم المجرمين، لذلك فالحاجة ماسة إلى التشريعات جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في كل المجالات . [1]

[1] – Johannes F.NIJIbaer , challenges for the low of Evidence, leiden ,INREP,1999,p16.

المبحث الثاني : أساليب التحري والتحقيق والإثبات في الجريمة المعلوماتية

الجريمة المعلوماتية تمتاز بخصائص وعناصر تميزها عن الجرائم التقليدية المنصوص عليها في القوانين، فأن قواعد هذه القوانين تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية وهذا ما يبرز كأمر واقع مسألة صعوبة جمع الإستدلالات و الأدلة في جريمة المعلوماتية، وأيضا تطبيق الإجراءات الجنائية التقليدية، وعلى هذا الأساس فقد قسمنا هذا المبحث إلى مطلبين، يتضمن الأول : أساليب التحري والتحقيق في الجريمة المعلوماتية والثاني أساليب الإثبات في الجريمة المعلوماتية .

المطلب الأول : أساليب التحري والتحقيق في الجريمة المعلوماتية

كما نص المشرع الجزائري ضمن القانون رقم 09-04 المؤرخ في 05 أوت سنة 2009، على قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتتمثل هذه القواعد في مراقبة الاتصالات الالكترونية ، هي إجراءات التحري الخاصة التي منحها المشرع الجزائري للضبطية القضائية في كل من قانون الإجراءات الجزائية وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

لم يشد المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل الجريمة المعلوماتية لظاهرة حديثة وبهذا الصدد جاء القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ومنها ما نصت عليه المادة 03 منه مما تتطلبه مستلزمات التحريات والتحقيقات القضائية كما سيأتي ذكره.

[1] – شرف الدين وردة ، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية – في التشريع الجزائري–، مجلة المفكر ، العدد الخامس عشر،ص 541.

الفرع الأول : مراقبة الإتصالات الإليكترونية

نص القانون رقم 04/09 المؤرخ في 2009/08/05 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولجيات الإعلام و الإتصال ومكافحتها في المادة 03 منه على ما يلي:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفها للقواعد المنصوص عليها في قانون الإجراءات الجزائية في هذا القانون وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة المعلوماتية ".

ومن الواضح أو المراقبة الإتصالات حددها القانون على سبيل الإستثناء وفي حالات محددة حصرها في المادة 04 من القانون المشار له وهي :

1- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو االجرائم الماسة بأمن الدولة.

2- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني او المؤسسات الدولة أو الإقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث جارية ويكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإليكترونية .

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

والملاحظ أن المشرع ونظرا لما يترتب عن تطبيق هذه التدابير ميدانيا من مساس بحرية الحياة الخاصة وخصوصيتها وهي مقدسة ومحمية دستوريا، كما أشير لها سابقا فإنه ربط القيام بها بشرط الحصول على إذن مكتوب من السلطة القضائية المختصة .

ومن المعلوم أن الرسالة الإلكترونية ذات طابع خاص لكنها لا تختلف عن الرسالة الورقية من حيث حفظها أو الإستغناء عنها وإهمالها ، ولكن ما يتميز الرسالة الإلكترونية انه

[1] – المادة 04 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحتها .

يمكن الوصول إليها عن طريق صناديق البريد الخاصة أو الملفات المحفوظة أو الرجوع إلى سلة المهملات، ومن أجل التحقيق الذي يجري بغرض ضبط المرسلات الإلكترونية فإنه يستلزم الولوج إلى البريد الإلكتروني (E- mail) [1]، وبعد تحديد صندوق البريد للمتهم المشكو منه يتمحور العمل حول ثلاث (3) عناصر وهي : الوارد (IN)، الصادر (OUT)، الحفظ وسلة المهملات(TRASH).

فبذلك يمكن مراجعة قائمة الرسائل التي وصلت إلى المشكو منه في الوارد والعكس بالنسبة للمراسلة منه على القائمة الصادرة وكذا الشأن بالنسبة للرسائل المحفوظة أو المهملة غير أن ما يجب تأكيده هنا هو أن المشرع ونظرا لحساسية الموضوع والذي يعد مرتبطا بقدر كبير بذاتية الأشخاص فقد جعل تدابير وإجراءات التحقيق تحت طائلة المسؤولية الجزائية عندما نص في المادة 04 من القانون 04/09 فقرة (د)والأخيرة على أن الترتيبات التقنية الموضوعية للأعراض المنصوص عليها في الفقرة(أ) من نفس المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها في القانون العقوبات بالنسبة للمساس بالحرية الخاصة للغير[2] وهذا ما نص عليه الدستور الجزائري في المادة 39 من بالقول:" بسرية المراسلات و الإتصالات الخاصة بكل إشكالها مضمونة ".[3]

وكذلك قد تم ضمان هذا المبدأ في الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة الأمم المتحدة في 1948/12/10 في المادة 12 منه على :" أنه لا يجوز أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو مراسلاته ولكل شخص الحق في الحماية القانونية ضد هذا التدخل. [4]

---

[1] – **البريد الإليكتروني:** وهو إرسال وإستقبال للرسائل الإليكترونية عن طريق شبكة الأنترنت، عن الأستاذ زيبحة زيدان ، مرجع سابق، ص 128.

[2] – زيبحة زيدان ، مرجع سابق ، ص 128 و 129.

[3] – المادة 39 من الدستور الجزائري لسنة 1996.

[4] – المادة 12 من الإعلان العالمي لحقوق الإنسان صادر عن الجمعية العامة للأمم المتحدة بتاريخ 1948/12/10.

الفرع الثاني : إجراءات التفتيش للمنظومة المعلوماتية

أولا : تعريف التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش وبقدر ما إعتبره إجراء من إجراءات التحقيق وإحاطة بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم ومما يؤكد ذلك إهتمام الدستور الجزائري بهذه النقطة إذ نص في المادة 40 منه بالقول :" فلا تفتيش إلا بمقتضى القانون وفي إطار إحترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"[1].

وكما هو الشأن في مختلف التشريعات العربية فإن التعريفات تجمع على أن التفتيش هو إجراء من إجراءات التحقيق " يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة ونسبتها إلى المتهم ، تحقق وقوعها في محل يتمتع بحرمة وذلك وفقا للضمانات والقيود القانونية المقررة "[2]، ويعرف كذلك التفتيش بأنه إجراء من إجراءات التحقيق " غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شأنها"[3].

وإذا كان التفتيش المتعارف عليه في القواعد الإجرائية العامة نوعان: تفتيش المساكن وتفتيش الأشخاص، كما نص على ذلك قانون إ.ج.ج. في المواد 44 و 64 منه فإن التفتيش المنصب على المنظومة المعلوماتية يختلف عنه كلية من حيث الشروط الشكلية والموضوعية،.

ويثور السؤال عن إمكانية التفتيش وفقا لضوابط المتعارف عليها في الجرائم التقليدية والغاية منه في مجال الجرائم المعلوماتية؟

والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة بينما البيانات الإليكترونية ليس لها حسب جوهرها مظهر ملموس في العالم الخارجي ، ومع ذلك فيمكن أن يرد، التفتيش على هذه

[1] – زيبحة زيدان ، مرجع سابق، ص 130.

[2] – رشيدة بوكر، مرجع سابق، ص 394.

[3] – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانا المتهم المعلوماتي ، ط1 دار النهضة العربية القاهرة، سنة 1997، ص 45.

البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسبة الإلكترونية[1].

ولهذا أجاز لفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة إلكترونيا، والمخزنة بالحاسبة الإلكترونية ثم ضبطها والتحفظ عليها ، او ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات ، والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام. [2]

ثانيا : تفتيش المنظومة المعلوماتية

نص القانون 04/09 في المادة 05 منه على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى :

1- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

2- منظومة المعلوماتية .

يلاحظ إذن بأن التفتيش في الوضعيات المشار لها يأخذ منحنين فهو إما أن يكون عملا من أعمال التحقيق تقوم به السلطات القضائية المختصة وإما يكون من أعمال الإستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة في كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر (الحاسوب) بمكوناته المادية والمعنوية فالحاسوب كما هو معروف يتكون من مكونات مادية، وهي مجموعة وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها إستقبال البيانات المعلوماتية والغير المعالجة ولها مهام أيضا داخل جهاز الحاسوب فهي تمر إلى الوحدات الذاكرة للمعالجة أو التخزين ووحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما تحتويه من ذاكرة رئيسته وعشوائية وذاكرة القراءة ثم وحدة الحاسب والمنطق، أما وحدة الإخراج فتحتوي على

---

[1] - M. Moherenschloger ,computer crimes and others crimes against information technology in the Germany,Rev ,int,dr, pen ,1993p319,spec349.

[2] - علي عدنان الفيل إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011، ص 39.

أجهزة الشاشة والطابعة ومشغلات الأقراص، أما المكونات المعنوية للجهاز الكمبيوتر والتي تسمى أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

ومما سبق يمكن القول بأن التفتيش وعند ما يستهدف الكيانات المادية للحاسوب لا يشكل أي عائق إذ أنه من السهولة بمكان ضبط الأجهزة وحجزها أو إتلافها وإنما الإشكال يثور عند ما ينصب التفتيش على المكونات الكمبيوتر المعنوية أو المنطقية كالبرامج وقواعد البيانات ذلك أن التفتيش عن هذه البيانات يتطلب الكشف عن لرقم السري (CODE) لمرور إلى الملفات وكذا الكلمات السر أو الشفرات أو ترميز البيانات.[1]

ثالثا : شروط تفتيش المنظومة المعلوماتية

يمكن تقسيم شروط التفتيش للمنظومة المعلوماتية إلى نوعين موضوعية والأخرى شكلية.

1- الشروط الموضوعية لتفتيش المنظومة المعلوماتية

وتنحصر هذه الشروط في

أ - وقوع جريمة المعلوماتية :

والجريمة المعلوماتية هي كل فعل غير مشروع بإستخدام الحاسبة الإليكترونية لتحقيق أغراض غير مشروعة [2]، وحتى يكون التفتيش صحيحا متفقا وصحيح قانونيا فإننا لابد وأن يكون بصدد جريمة معلوماتية مما يعتبر القانون جناية أو جنحة. [3]

[1] - زيبحة زيدان ، مرجع سابق، ص 131.

[2] - هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، سنة 1992،ص 30.

[3] -خالد ممدوح إبراهيم، مرجع سابق، ص 210.

ب – تورط شخص أو أشخاص معينين في إرتكاب الجريمة المعلوماتية أو الإشتراك فيها:

ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الإعتقاد بأنه قد ساهم في إرتكاب الجريمة المعلوماتية سوء وصفه فاعلا لها أو شريكا فيها وفي مجال الحاسبة الإلكترونية .

ج – توافر إمارات قوية أو أدلة تفيد في الكشف عن الجريمة المعلوماتية :

لا يوجد التفتيش إلا إذا توافرت لدى المحق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات إستخدمت في جريمة المعلوماتية أو أشياء متحصلة منها.

د – محل التفتيش الخاص بنظام الحاسبة الإلكترونية:

وهي كل مكونات الحاسبة سواء كانت مادية أو معنوية أو شبكات الإتصال الخاصة بها بالإضافة إلى الأشخاص الذين يستخدمون الحاسبة الإلكترونية محل التفتيش.[1]

2– الشروط الشكلية لتفتيش المنظومة المعلوماتية :

يستخلص من نص المادة 05 من القانون 04/09 المشار سابقا بأن التفتيش في مجال الجرائم المعلوماتية والذي يختلف كلية عن التفتيش العادي يتوقف أساسا على طبيعة المكان الذي يحتوي أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أم عاما هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أن أجنبيا .[2]

ويمكن تحديد أهم عناصر التفتيش فما يلي من خلال القواعد العامة للقانون الإجراءات الجزائية كالتالي: وفقا للأحكام المادة 44 من ق.إ.ج.ج لاسيما بعد التعديل بموجب القانون 22/06 في 2006/09/20 وهي :

أ – وجود إذن مكتوب صادر من وكيل الجمهورية او قاضي التحقيق .

ب – الإستظهار بالإذن قبل الدخول المنزل المراد تفتيشه.

[1] – على عدنان الفيل، مرجع سابق، ص 50.

[2] – زيبحة زيدان، مرجع يابق،ص 133.

ج – أن يتضمن الإذن وصف الجريمة البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

د – حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

هـ – في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين لسلطته. [1]

أما التفتيش في الأماكن العامة وهي التي يرتدوها العامة في كل وقت ولا يتمتع بحرمة المنزل فيمكن دخولها خلاف الأماكان الخاصة وتفتيشها إذا ما تم غلقها إنتهاء فترة العمل وإنصراف العامة.

رابعا : تفتيش المنظومة المعلوماتية عن بعد

أجاز القانون الجزائري 4/09 المشار له سابقا القيام بتفتيش المنظومة المعلوماتية عن بعد ويقتضي ذلك الدخول إليها دون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب فالتفتيش هما يستهدف أشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات ، ولأن هذه قد تكون وسيلة لإرتكاب الجريمة .

فقد أجاز المشرع الجزائري من إفراغ أو نسخ تلك المعلومات المشكوك فيها والتي من شأنها الإفادة في الكشف عن الجريمة أو مرتكبيها أو حجز المعطيات وضبطها كدليل إثبات ضد المتهم يقدم أمام المحكمة .

إلا أنه برنامج الحاسوب وقاعدة البيانات تتمتع بالحماية القانونية في القانون الداخلي وفي إتفاقيات الدولية كما هو الشأن في التشريع الجزائري إذ إعتبر برنامج الحاسوب وقاعدة البيانات مصنفات محمية بموجب القانون رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة.

[1] – المادة 44 من القانون الإجراءات الجزائية المعدل بموجب القانون رقم 22/06 في 2006/09/20.

لكن رغم ذلك فقد أجيز التفتيش عن بعد وفق ما تقتضيه الحاجة القانونية [1]

خامسا : تمديد التفتيش إلى منظومة معلوماتية أخرى او جزء منها

نصت المادة 05 من القانون رقم 04/09 على ما يلي:

في الحالة المنصوص عليها في الفقرة – أ– من هذه المادة:" إذا كانت هناك أساب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك" [2] ، والملاحظ هنا أن التفتيش في هذه الحالة يكتسي طابع خاص فهو يجري عن بعد وثانيا يتم بشكل سريع وتماشيا مع سرعة الفائقة الذي يجري عليه نقل المعلومات وذلك طبقا تحت طائلة القانون في إطار حماية الحياة الخاصة للأفراد.

سادسا : الجهة القضائية المختصة بالإشراف على المعطيات التفتيش

حسب القانون 04/09 في المادة 04 منه وهي المتعلقة :" بمباشرة المراقبة بغية الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة"، ففي هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من نفس القانون وهي الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات.

إذن الإختصاص يؤول في هذه الحالة الى منح الإذن للنائب العام على ان تكون مدة الإذن ستة(06) أشهر قابلة للتجديد.

أما فيما عدا حالة المنحصرة في الفقرة – أ–من المادة04 من القانون 04/09 فإنه يتعين الرجوع إلى التدابير التي رسمها قانون إ.ج.ج في مجال التحري والتفتيش بالنسبة للجرائم الإليكترونية وبالضرورة يعود الإختصاص لوكيل الجمهورية وكذا قاضي التحقيق بإعتبارهما

[1] – زبيحة زيدان، مرجع سابق، ص 135.

[2] – المادة 05 من القانون رقم 05/09 المتعلق بالجرائم الماسة بتكنولوجيات الإعلام والإتصال ومكافحتها.

الجهة المؤهلة بمنح الإذن بالتفتيش ويحدد ذلك المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 والمتضمن تمدد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق. [1]

الفرع الثالث: إجراء الحجز داخل المنظومة المعلوماتية

تجدر الإشارة إلى القول بأن حجز الأشياء المادية كالمعدات والأوراق والمستندات يعد شيئا سهلا وغير مثير لأية إشكاليات في نظر القانون، غير أنه ليس من السهل أبدا توقيع الحجز داخل منظومة معلوماتية ذلك أن المعلمات هي في الأصل شيء معنوي.

وقد إختلفت التشريعات العالمية حول إمكانية حجز الكيانات الغير المادية المخزنة في برامج وذاكرة الحاسوب .

و عليه فقد إعتبر البعض أنه لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي كطباعتها أو تصورها ، في حين إعتبرها البعض الأخر بأن برامج الحاسوب كيانا ماديا ملموس إذ هو عبارة عن نبضات إليكترونية ممغنطة، ورأى إتجاه أخر أن المعلومات في حالتها لا تقبل التملك ولا يمكن أم يكون محلا للإعتداء ولا محلا للملكية الفكرية .[2]

غير أن المشرع الجزائري وقبل صدور القانون 04/09 كان قد أضفى حماية قانونية لقواعد البيانات بموجب الأمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة له، وإعتبر قواعد البيانات من المصنفات المحمية .

وفي إطار الحماية البيئة الجنائية لحقوق المؤلف وطبقا الأحكام المواد 146/145 من الامر 05/03 ، يتولى ضباط الشرطة القضائية أو الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة له ، معاينة المساس بحقوق المؤلف كما يتولون بصفة

[1] – زيبحة زيدان، مرجع سابق،ص 140.

[2] – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 596،وأيضا : د – هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 256.

تحفظية حجز دعائم المصنفات ووضعها تحت حراسة الديوان، وتفصل الجهة القضائية في طلب الحجز التحفظي خلال 03 أيام من تاريخ إخطارها.

وعلى الوجه العموم فأن المشرع الجزائري إنحاز إلى الإتجاه القائل بإمكانية حجز المعلومة طبقا للأحكام المادة 06 من القانون 04/09 حيث يمكن حجز المنظومة المعلوماتية برمتها إذا كان ضروريا ولمصلحة التحقيق وذلك بعد نسخها على دعامة مادية كطبعها على الورق أو ضبطها على الشاشة.

وضبط الإدلة عن طريق الحجز المعطيات أو البيانات يجري وفقا لمقتضيات قانون الإجراءات الجزائية ، بالإضافة إلى التدابير أخرى منها المصادر للأجهزة والبرامج والوسائل المستخدمة مع إغلاق الموقع الجريمة قد نص عليها القانون العقوبات في مادته 394مكرر6.

وقد نصت المادة 84 من إ.ج.ج على ضوابط المتعلقة بالأدلة منها ما يلي :

– الإطلاع على المستندات المبحوث عنها وذلك مخول لقاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه فقط.

– الإحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان سر المهنة وحقوق الدفاع.

– وعلى الفور يتم فرز الأشياء المضبوطة ووضعها في أحراز مختومة حيث لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه حسب المادة 84 ف.إ.ج.ج.[1]

الفرع الرابع : إلتزامات مقدمي الخدمات في مساعدة السلطات

بموجب المادة 10 من القانون 04/09 ألزمت مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش، كما ألزمتهم أيضا بكتمان السر بخصوص العمليات التي ينجزونها بطلب المحققين وما تحصل عن ذلك من المعلومات، وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحيق، ويطلق على مقدمي الخدمات في مجال الانترنت تسمية الوسائط في خدمة الأنترنت ويمكن دورهم في تمكين

[1] – زيبحة زيدان، مرجع سابق، ص 148.

مستخدم الأنترنت من الدخول إلى الشبكة والإطلاع عليها عما يبحث عنه، وقد عرفت المادة الأولى الفقرة الثالثة من الإتفاقية الأوروبية لمكافحة جرائم المعلوماتية التي تم إقرارها في بودابست لسنة 2001 :" عرفت مزودي الخدمات بأنهم كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الإتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة المعطيات المخزنة نيابة عن المزود الخدمة ".[1]

لعل هذه هي أهم إجراءات البحث والتحري في الجريمة المعلوماتية التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها وذلك لتعددها ، علما أن ما قدمناه في هذا المطلب كانت عبارة عن الإجراءات جاءت في القانون 04/09 سابق الذكر.

يضاف إلى ذلك ما نصت عليه المادة 65 مكرر 5 من قانون الإجراءات الجزائية المتمثلة في مايلي:

1 –إعتراض المراسلات التي يتم عن طريق وسائل الإتصال السلكية واللاسلكية:

والتي يتم عن طريق وسائل الإتصال السلكية واللاسلكية وذلك بواسطة ترتيبات تقنية يتم وضعها دون موافقة المعينين، ومن أجل التصنت والتقاط ويتبث بث وتسجيل الكلام المتفوه به بصفة سرية من أجل تحصيل الدليل.

2– إعتراض البريد الإلكتروني:

بإعتباره نظام للتراسل بإستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا، حيث يتم إعتراضه إلا بإذن من وكيل الجمهورية في إطار التحري و التحقيق الإبتدائي.

3– إلتقاط الصور :

ويندرج ذلك تحت طائفة الترتيبات التقنية التي تهدف إلى إلتقاط الصور لشخص او لعدة أشخاص يتواجدون في مكان خاص ودون الأماكن العامة حسب المادة 65 من ق.إ.ج.ج.

[1] – زيبحة زيدان، مرجع نفسه،ص 153.

4- إجراءات التسرب:

يعتبر هذا الإجراء مستحدثا في مجال التحريات والتحقيقات وقد نص عليه المشرع في المادة 65 مكرر5 من ق.إ.ج.، وكذلك في المادة 65 مكرر 11 بموجب التعديل بالقانون رقم 22/06 المؤرخ في 2006/12/20، ويقصد به قيام ضباط أو عون الشرطة القضائية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإهامهم أنه فاعل معهم أو شريك لهم.[1]

المطلب الثاني : أساليب الإثبات في الجريمة المعلوماتية

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حددها المشرع وإعترف لها بالقيمة القانونية، وتتمثل وسائل الإثبات الرئيسية في الجريمة المعلوماتية في المعاينة والخبرة وهذا ما أخذت به معظم التشريعات الدول، أما التفتيش فقد أدرجه المشرع الجزائري بموجب القانون 04/09 كأسلوب التحري والتحقيق اكثر منه كأسلوب الإثبات، أما الأساليب الأخرى المتمثلة في إجراءات الإستجواب والمواجهة وسماع الشهود فلم نتطرق إليها على أساسها أنها إجراءات خاصة بالأفراد وتتم في مواجهة البشر وليست فنية كما هو الحال بالنسبة للأسلوب المعاينة والخبرة، بالإضافة إلى تطرقنا إلى دليل آخر مستحدث يتناسب مع الطبيعة الخاصة للجريمة المعلوماتية وهو إعتماد الدليل التقني أو الإلكتروني في إثبات، وهذا ما سوف نتطرق في الفروع الأتية :

[1] – زيبحة زيدان ، مرجع سابق ، ص ص 157 ، 169.

الفرع الأول : إعتماد المعاينة في الإثبات

أولا : تعريف المعاينة:

للمعانية أهمية قصوى في إثبات الواقعة، وهي إثبات مادي ومباشرة لحالة الأشخاص والأشياء والأمكنة ذات الصلة بالحادث وتتم بواسطة عضو النيابة العامة أو من يندبه من ضباط الشرطة القضائية، وتتمتع المعاينة في الكشف عن الغموض وإظهار الحقيقة في الجريمة المعلوماتية بنفس درجة من الأهمية في الجرائم التقليدية[1].

ثانيا : أهمية المعاينة في الجرائم المعلوماتية

للمعاينة أهمية بالغة في أدلة المعاينة وفي إقتناع المحكمة في كثير من القضايا، إلا أنه يمكن القول أن السلطات المختصة التي تقوم بإجراءات المعاينة أو التي تتكفل بها تواجهها صعوبات في بعض الأحيان، كون أن الجرائم المعلوماتية لا تختلف أثارها مادية

وقد تطول الفترة الزمنية بين وقوع الجريمة وإكتشافها مما يعرض الأثار الناجمة عنها إلى المحور أو التلف أو العبث بها [2].

وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الأنترنت فائدة في كشف الحقيقة عنها وعن مرتكبيها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما لي :

1- تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة .

2- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام .

3- التحفظ على المحتويات سلة المهملات.

4- التحفظ على المستندات الإدخال والمخرجات الورقية لكمبيوتر ذات صلة بالجريمة لرفع البصمات والتي قد توجد بها. [3]

[1] – خالد ممدوح إبراهيم، مرجع سابق، ص 147 وما بعدها.

[2] – هشام رستم ، الجواني الإجرائية للجرائم المعلوماتية ، مرجع سابق، ص 59

[3] – هشام رستم، قانون العقوبات والمخاطر تقنية معلومات، مرجع سابق، ص 126-127.

5 – قصر مباشرة المعاينة على فئة معنية من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الكمبيوتر والشبكات والنظم المعلوماتية. [1]

وما هو جدير بالذكر أن المعاينة قد تكون الحل في بعض أنواع الجرائم المعلوماتية ولتحقق المعاينة لابد من وجود مسرح جريمة وهذا ما يصعب تحديده وصعوبة الحفاظ على الأثار المادية إن وجدت، وتكون عقبة الأساسية أمام المعاينة في الجريمة المعلوماتية عندما ترتكب داخل الفضاء المعلوماتي، فالمحقق يتعامل مع نبضات إلكترومغناطسية وبيانات مخزنة في نظام المعلوماتي .

ولذلك تقتضي المعاينة جهات قضائية مختصة بها مؤهلة وتتمع بالخبرة في مجال هذه التقنية، حيث يقوم المحققين بالإطلاع على مختلف الوثائق المحفوظة والمراسلات الإلكترونية المرتكبة في الجريمة وفك الشفرات وإقتفاء آثر الإتصلات الإليكترونية من جهاز الحاسب الخاص بالجاني وكذا الخاص بالضحية، حيث تستخدم كل من الإجراءات كدليل وكإثبات للجريمة المعلوماتية، ومن أمثلة فائدة المعاينة التي أتت بنتيجة ، وهو ما قامت به الشرطة الفرنسية في مداهمة منزل شخص كان يستغل الأطفال عن طريق الأنترنت ونشر صور إباحية فتمت المعاينة وثم القبض على الجاني وحجز مختلف الأجهزة المتصلة بالإنترنت الخاصة بجهازه، ما يمكن قوله ان المعاينة تحتاج إلى الضبطية قضائية مؤهلة لهذه التقنية مع التوصية في إعادة النظر في التشريع الذي ينظمها وهذا الأمر أضحى ضرورة لابد منها من أجل فتح المجال العمل الإستدلالي. [2]

[1] – Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc.5 edition,1992,p450.

[2] – محمد أمين الرومي، جرائم الكمبيوتر و أنترنت، دار المطبوعات الجامعية ، الإسكندرية، سنة 2003،ص 139.

الفرع الثاني : إعتماد الخبرة في الإثبات

أولا : تعريف الخبرة

يقصد بالخبرة – بصفة عامة– المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الإثنين معا أي العمل والدراسة ، ومن هنا يطلق على ذوي هذه المهارات "بالخبراء".[1]

والخبرة هي الوسيلة من الوسائل الإثبات التي تهدف إلى الكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالإستعانة بالمعلومات العلمية والتي لا تتوفر سواء لدى المحقق أو القاضي، فهي بحث مسائل مادية أو فنية يصعب على المحقق أن يثبت طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، وتكمن أهمية الخبرة في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية لتحقيق العدالة في المجال الجزائي، لذا فقد إهتم المشرع الجزائري بالإستعانة بالخبراء لجهات التحقيق، وأجاز للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم[2].

ثانيا : تعريف الخبير

الخبير هو شخص مختص فنيا في مجالات مختلفة ومتنوعة سواء كانت فنية أو علمية أو غيرها من المجالات الأخرى.

ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى الخبرة فنية. [3]

[1] – خالد الممدوح إبراهيم، مرجع سابق، ص 283.

[2] – رشيدة بوكر،، مرجع سابق، ص 424، وأنظر أيضا في ذات الموضوع، أ عائشة بن قارة مصطفى، مرجع سابق، ص 88 و 89.

[3] – خالد ممدوح إبراهيم، مرجع سابق، ص 285 و 286.

وتجدر الإشارة في هذا الإطار، أن بعض الفقه يرى أنه لا يشترط في الخبير المنتدب أن يكون متخرجا من معاهد أو الجامعات المتخصصة في دراسات الحاسوب والأنترنت بل يكفي إكتسابه مهارة موهبة إستعمال الحاسوب والأنترنت و التعامل مع تقنية المعلومات. [1]

ثالثا : أهمية الخبرة في مجال الجريمة المعلوماتية .

تكتسب الخبرة الفنية في جريمة المعلوماتية أهمية بالغة نظرا لأن الحاسبات وشبكات الإتصال بينها على أنواع ونماذج متعددة كذلك فأن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يعصب معها على المتخصص تتبعها وإستعابها [2] والإستعانة بخبير فني في المسائل الفنية البحثة خاصة في مجال الجرائم المعلوماتية فهو أمر وجوبي، لأن الأمر يتعلق بمسائل معقدة ومحل الجريمة فيها غير مادي ولا يكشف عن غموضها إلا متخصص وعلى درجة كبيرة من التميز .

فالإجرام للذكاء والفن ولا يكشفه إلا ذكاء ولا يقابله الا دكاء وفن متماثلين[3].

وبدا من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية، وأن نجاح الإستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، وهذا ما يدعو إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم المعلوماتية لنجاح تحقيق في مثل هذه الجرائم، ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فإن الخبير المعلوماتي قد يكون من أولئك الجناة الذين سبق لهم إرتكاب مثل هذه الجرائم وتم تكوينهم وإعادة تأهيلهم كأفراد موطنين صالحين في المجتمع [4] .

---

[1] – رشيدة بوكر ، مرجع سابق، ص ص 426 ، 427.

[2] – علي عدنان الفيل، المرجع السابق ، ص ص 26 ، 27.

[3] – Taylor Robert ,op.cit ,p01.

[4] – خيرت محرز، مرجع سابق، ص ص 96 ، 97.

رابعا ، مدى حجية تقرير الخبير التقني

يحرر الخبير لدى إنتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قام به من أعمال ونتائجها، وطبقا للمادة 215 من قانون إ.ج.ج تكون هذه التقارير مجرد إستدلالات لإنارة القاضي، ولذلك يكون رأي الخبير يعطي دائما بصفة إستشارية ولا يقيده فهو ليس بحكم وليس له قيمة قضائية أكثر من شهادة شهود، فيجوز للقاضي أن يأخذ بالخبرة أو يطرحها و أن يفاضل بين تقارير الخبراء ويأخذ بما يرتاح إليه، حيث أن كل ما يتعلق بالدعوى يجب أن ينتهي عند قاضي الموضوع لكي يتولى الفصل فيه والكلمة الأخيرة ترجع لمحكمة الموضوع وهذا الأمريسري على الناتج من الخبرة في إطار تكنولوجيا المعلومات، حيث يظل القاضي هو الخبير الأعلى.[1]

الفرع الثالث : إعتماد الدليل التقني في الإثبات

أولا : تعريف الدليل التقني

تعددت التعريف التي قبلت بشأن الدليل التقني وتباينت لذا سنعرض أهم هذه التعريفات فيما يلي :

هناك من يعرفه بأنه:" معلومات يقبلها المنطق والعقل ويعتمد العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الإتصال ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة او جاني او مجني عليه"، أو أنه يشمل "جميع البيانات الرقمية التي يمكن أن تثبت إن هناك جريمة قد أرتكبت ".

والدليل الرقمي أو الإليكتروني أو الرقمي هو عبارة عن :" كل البيانات التي يمكن أن إعدادها أو تخزينها في شكل رقمي في الحاسوب"، ويمكن تعريف البيانات الرقمية بأنها مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت والصورة، أو, أنه الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل

[1] – رشيدة بوكر ، مرجع سابق،ص 429.

نبضات كهرومغناطسية، ممكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال من أجل تقديمه أمام أجهزة تطبيق القانون .[1]

وما هو جدير بالذكر أن هناك فرق بين الدليل التقني وبرامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في القيام بمختلف العمليات التي يحتويها النظام المعلوماتي عند إعطاء الأوامر بالقيام بذلك، أما الدليل التقني فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبيها. [2]

ثانيا : تقدير القاضي الجزائي للدليل التقني

إذا توافرت في الدليل التقني الشروط العامة لما يمكن أن يتمثل أساسا لإنبعاث الثقة فيه، فإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل ودلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، وبالتالي فلا حرية للقاضي في مناقشة الحقائق العلمية الثابتة.

رغم أن هنالك إمكانية التشكيك في سلامة الدليل التقني بسبب قابلية للعبث إلا أن تلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم خاصة إذا توافرت في الدليل التقني الشروط الخاصة بسلامته من العبث والخطأ، ورغم ذلك تبقى مسألة الأدلة العلمية والفنية في الإثبات راجعة الى السلطة التقديرية للقاضي لأنه يبقى المسيطر حقيقة وبإستطاعتة تفسير الشك لصالح المتهم. [3]

[1] – رشيدة بوكر ، مرجع سابق،ص ص 382 ،383.

[2] –عائشة بن قارة مصطفى، مرجع سابق، ص 31.

[3] – رشيدة بوكر ، مرجع سابق، 507.

ثالثا : حجية الدليل الإليكتروني في الإثبات

إن الخصوصية الجريمة المعلوماتية والتي تتميز بالطابع الفني، دفع المشرع الجزائري بأن يبادر في مواكبة التطور القانوني على المستوى الدولي وتماشيا مع التطور التكنولوجي، بتمهيد للطريق أمام إستخلاص الدليل الإليكتروني في القانون رقم 04/09 في المادة 06 منه[1]، مراعيا بذلك الإعمال بالقواعد العامة التي من الضروري توافرها في الدليل الإليكتروني وهي مبدأ المشروعية، بمعنى أنه لا يكون مستخلصا بطريقة مخالفة لأحكام القانون ولا مبادئ دستورية خاصة ما تعلق منها بحماية الحريات الأساسية .

ومما هو مستقر عليه فإن القاضي الجزائري ملزم بفحص الدليل الإليكتروني لكي يتواصل إلى تشكيل قناعة إنطلاقا من عرض هذا الدليل على مناقشة الأطراف، وهو ما نصت عليه المواد 212و 234 من قانون إ .ج.ج. [2]

وبذلك يتضح لنا الدليل التقني له حجية في الإثبات وذلك بما يتميز به من موضوعية وكفاءة، ومحكم وفق قواعد علمية عملية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي من التقليل من الأخطاء القضائية و الإقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة . [3]

والإستدلال على ذلك نلاحظ إن الفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشة عن الآدلة الناشئة عن الآلة أو الأدلة العلمية مثل: الردارات، الأجهزة السنمائية، أجهزة التصوير ، أشرطة التسجيل، أجهزة التنصت. [4]

---

[1] – المادة 06 من القانون رقم 04/09 والتي تنص :" على حجز المعطيات المعلوماتية وذلك بإفراغها أو نسخها على دعامة تخزين إليكترونية قابلة للحجز الوضع في أحراز".

[2] – زيبجة ، زيدان، مرجع سابق، ص 173.

[3] – بوكر رشيدة ، مرجع سابق، ص 497.

[4] – هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجزائية ، الطببعة الثانية ، دار النهضة العربية، القاهرة، سنة 2008.، ص ص 42 ، 43.

وبظهور الدليل التقني فقد زاد من دور الإثبات العلمي وإستتبعه تعاظم دور الخبراء في القيام بدور فعال في إبداء خبرتهم الفنية، كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في وضع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة عملية قد يصعب إثبات عكسها، مما يدفع هذا الأمر بالإعتقاد بأنه بمقدار إتساع مساحة الأدلة العلمية بمقدار ما يكون انكماش وتضاؤل دور القاضي الجزائي في التقدير خاصة أمام غياب الثقافة المعلوماتية للقاضي. [1]، ولكن هذا لا ينفي حقيقة الضرورة الماسة للدليل لتقني لأنه يتماشى مع طبيعة الجريمة المعلوماتية ومع التطور التكنولوجي الحاصل مما يستدعي الامر عدم التوقف عند مضمون الدليل الإليكتروني فقط بل يجب التركيز والإهتمام بتطوير الإجراءات التي يترتب عليها الحصول على هذا الدليل مع إشتراط ضرورة مشروعيتها وخلوها من العبث والخطأ .بإعتبار أن الدليل الإليكتروني أو التقني له حجية في الإثبات خاصة في التشريعات التي تأخذ بمبدأ حرية الإثبات وسلطة القاضي التقديرية كما في التشريع الجزائري.

[1] – رشيدة بوكر ، مرجع سابق، ص498.

خاتمة

تعتبر الجرائم المعلوماتية من اخطر الجرائم وأعقدها، والتي ظهرت نتيجة تطور التقنيات والأساليب التكنولوجية، بحيث ساهمت الثورة المعلوماتية في بروز جرائم جديدة تستهدف برامج الحواسيب وتضر بأنظمتها المعلوماتية .

وعلى هذا الاساس وجب العمل على سن قوانين تقر الحماية الجنائية للمعلومات المدخلة والمرتبطة بالحواسيب . إذ ان الجرائم المعلوماتية فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الاجرام الذي بات يهدد امن المجتمعات، كونه يتميز بامتداده وانه عابر للأوطان ولا يقتصر على مكان ارتكابه فقط، والجزائر بدورها ركزت على الجريمة المعلوماتية وحاولت وضع مجموعة من الآليات الموضوعية والإجرائية لمواجهة هذا النوع من الإجرام.

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

فقد لاحظنا أن خصوصية الجريمة المعلوماتية تكمن في أنها جريمة مستحدثة إختلف الفقه والقضاء في وضع لها تعريف أو وصف جامع ومانع، وكذلك تميزها بمجموعة من الخصائص أبرزها أنها جريمة عابرة للحدود وكذا السمات التي إنفرد بها المجرم المعلوماتي،

وأهم خاصية في رأينا أنها جريمة تعددت صورها وأنماطها وإختلفت طرق وأساليب إرتكابها، بحيث يمكن أن ترتكب من خلالها تقريبا جميع الجرائم منها التقليدية التي ترتكب بواسطة أجهزة الكمبيوتر وشبكة الأنترنيت، وكذا الجرائم لفنية ،مثل الجرائم الماسة بأنظمة المعالجة الآلية مثلما لاحظنا، أما أهم خصوصية لهذه الجريمة فيتمكن في طابع الإجرائي الذي تجسد في المقام الأوّل في بعض الصعوبات، والتي تكتنف بالدرجة الأولى في مشكلة الإختصاص القضائي وكذا العقبات التي تواجه السلطات و الأجهزة الأمنية في سبيل مباشرة إجراءات البحث والتحري والتحقيق بالإضافة إلى خاصية الإثبات في هذه الجريمة ومشكلة قبول الدليل التقني بشأنها.

النتائج :

وبناءا على ما تقدمنا به فإننا سنحاول طرح بعض النتائج المتمثلة في :

1- الجريمة المعلوماتية من الجرائم المستحدثة التي ترتكب في العالم الإفتراضي غير ملموس ماديا لكن له وجودا حقيقيا.

2- الجريمة المعلوماتية هي جريمة تتجاوز الحدود الزمنية والمكانية والتي تتسم بكونها من أكثر الجرائم خطورة وذاك بسبب الإختلاف الجوهري بينها وبين الجرائم التقليدية.

3- طرق وأساليب متابعة وإثبات الجريمة المعلوماتية لا تنطبق عليها الوسائل التقليدية، بحيث ينبغي ان تكون هنالك اساليب فنية وتقنية تتماشى والبيئة الإفتراضية التي ترتكب فيها الجريمة المعلوماتية .

4- سمات المجرم المعلوماتي وما يتميز به من ذكاء ومهارة معرفة للتقنية المتطورة جعل من الجريمة المعلوماتية جريمة هادئة وأقل عنفا لأنها لا تعتمد على مجهود عضلي وإنمّا على دراسة ذهنية بالنسبة لمرتكبيها.

5- أدت خطورة الجريمة المعلوماتية بالدوّل والهيئات الدوّلية إلى محاولة وضع أطر قانونية لمكافحتها أبرزها إتفاقية بودابست 2001، أمّا بالنسبة للمشرع الجزائري فقد واكب ذلك من خلال تعديل قانون العقوبات بقانون رقم 15/04، بالإضافة غلى قانون رقم 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام الآلي والإتصال ومكافحتها.

رغم ذلك يبقى المشرع الجزائري لم يتدارك لكل الثغرات والنقائص بعد في نصوصه القانونية لذا فإننا سنقترح بعض التوصيات التالي:

التوصيات:

1- ضرورة سن القوانين المانعة للحد من هذه الجريمة وتشديد الرقابة على الأجهزة والبرامج.

2- إعادة النظر في القوالب الإجرائية الحالية بما يتماشى مع طبيعة الجريمة المعلوماتية من خلال تعديلها او إستحداث إجراءات أخرى .

3- ضرورة وضع نص يجرم سرقة المال المعلوماتي المعنوي (برامج وملومات) في التشريع الجزائري.

4- ضرورة نص صراحة على الدليل التقني أو الإليكتروني كدليل إثبات جنائي في هذا النوع من الجرائم وتعديل القواعد الإجرائية لتسهيل الحصول عليه.

5- الحث على تعزيز التعاون الدوّلي فيما بين الدول للحد من هذه الظاهرة الإجرامية من خلال إبرام الإتفاقيات العربية الجماعية والثنائية الأطراف خاصة فيما يخص التعاون القضائي و الامني.

6- ضرورة الإهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية والضبطية القضائية المتخصصة في مجال الجرائم المعلوماتية .

قائمة المراجع

أولا :المراجع باللغة العربية

أ - الكتب

*** المؤلفات العامة :**

1- عباس أبو شامة عبد المحمود، عولمة الجريمة الإقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض،سنة 2007.

2- عبد الله بن عبد العزيز يوسفي، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية، الرياض ، الطبعة الأولى ، سنة 2004.

3- فوزية عبد الستار، شرح القانون الإجراءات الجزائية ، دار النهضة العربية ، بدون بلد النشر، سنة 1979.

4- فوزية عبد الستار، قانون العقوبات (القسم الخاص) ، دار النهضة العربية، بدون بلد النشر، سنة 1989.

*** المؤلفات المتخصصة:**

1- آمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية ، دار هومه للطباعة والنشر والتوزيع، الجزائر ، سنة 2007.

2- إنتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية ، بيروت، سنة 1994.

3- جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، سنة 2002.

4- جميل عبد الباقي الصغير، الأنترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ، القاهرة، سنة 2001.

5- خالد ممدوح إبراهيم، فن التحقيقي الجنائي في جرائم الإليكترونية، الطبعة الأولى دار الفكر الجامعي للنشر ، الإسكندرية ، 2009 .

6- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر(أساليب وتغرات)، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2010.

7- خيرت عليّ محرز، التحقيق في الجرائم الحاسب الآلي، دار الكتاب الحديث للطباعة و التوزيع ، القاهرة، سنة 2012.

8- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، وفي التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012.

9- زبيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2011.

10- طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، سنة 2009.

11- عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر والأنترنت، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، سنة 2006.

12- عبد الفتاح البيومي الحجازي ،الإثبات الجنائي في جرائم الكمبيوتر و الأنترنت طبعة خاصة ، بهجات للطباعة والتجليد، جمهورية مصر العربية، 2009.

13- علي عدنان الفيل، الإجرام الإليكتروني، الطبعة الأولى ، منشورات زين الحقوقية دمشق، 2011.

14- علي عدنان الفيل إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011.

15- محمد أمين أحمد الشوابكة ، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان، سنة 2004.

16- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ماجيستير في القانون الجنائي المعلوماتي، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان، الأردن سنة 2009.

17- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الألي في القانون الجزائري والمقارن، دار الجامعية الجديدة، الإسكندرية سنة 2007.

18- محمد سامي الشوا، ثورة المعلومات وإنعكساتها على القانون العقوبات، دار النهضة العربية ،القاهرة ،1994.

19- نائلة عادل فريد قورة،، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية، القاهرة، سنة 2005.

20- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، سنة 1992.

21- هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة آلات الحديثة ،أسيوط، 1994.

22- هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانا المتهم المعلوماتي ، ط1 دار النهضة العربية ، القاهرة، سنة 1997.

23- هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، الطببعة الثانية ، دار النهضة العربية، القاهرة، سنة 2008.

24 - رامي متولي القاضي ، مكافحة الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى، القاهرة، 2011.

25 - محمد الألفي المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الانترنيت المكتبة المصرية الحديثة، القاهرة ،2011.

ب - الرسائل علمية

- حمزة خضري، حمزة عشاش : "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي، الأغواط، الجزائر، جوان ،2020،

- بثينة حبيباتي الطبيعة الخاصة للجريمة المعلوماتية ، دراسات مجلة وأبحاث، مجلد جامعة زيان عاشور، الجلفة، الجزائر، مجلد 12 عدد 03 جويلية 2020،

– رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر : الجرائم الإلكترونية، مركز جيل البحث العلمي طرابلس ، لبنان، 24 مارس 2017

– خليلي سهام ، خصوصية المجرم الإلكتروني ، مجلة الفكر ، العدد 15 ، جوان 2017

برقوق يوسف، ، المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01 ، العدد ، 01، 2021

– عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير، كلية الحقوق ، جامعة الإسكندرية، سنة 2009.

– سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية ، 'دراسة مقارنة)، رسالة دكتوراه ، كلية الحقوق ، جامعة عين الشمس، سنة 1997.

ج – المقالات و الأبحاث والندوات

1 – أسامة محي الدين عوض، جرائم الكمبيوتر، بحث مقدم إلى المؤتمر السادس للجمعية العربية للقانون الجنائي، القاهرة 25–28 أكتوبر 1993.

2– إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الأنترنت، جامعة الإمارات، في سنة 2000.

3– محمد الأمين البشري،بحث بعنوان التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون و الانترنت، المنعقد في الفترة من 1–3 مايو 2000 بكلية الشريعة والقانون،بدولة الامارات ، 2000 .

4– كريستينا سكولمان، عن جرائم الأنترنت طبيعتها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، سنة 2007.

5– هشام رستم، جرائم الحاسب كصورة من صور الجرائم الإقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة المعلوماتية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط ، العدد 17 ، سنة 1995.

د – القوانين

*** القوانين الدولية**

1– الإتفاقية الدولية الخاصة بقمع أعمال النووي الموقعة بمقر الأمم المتحدة " نيويورك"في 2005/09/16 ، وصادقت عليها الجزائر بتحفظ بموجب مرسوم رئاسي رقم 270/10 مؤرخ في 03 /11/ 2010 .

2– إتفاقية مكافحة إستعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 55/63 الصادرة عن هيئة الأمم المتحدة الجلسة العامة 31 / 2000/12.

3– القانون العربي النموذجي الموحد لمكافحة الجرائم المعلوماتية ومافي حكمها،أعتمد مجلس الوزراء العدل العرب في دورته 19 بقرار رقم 495 في 2003/10/08.

*** النصوص القانونية**

الدستور

- من الدستور الجزائري لسنة 1996 (منشور بموجب المرسوم الرئاسي رقم 96–436 مؤرخ في 07 ديسمبر 1996، يتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء شعبي يوم 28 نوفمبر 1996، جريدة رسمية عدد 76 مؤرخ في 28 نوفمبر 1996، معدل ومتمم بالقانون رقم 02–03 مؤرخ في 10 أفريل 2002، يتضمن نص تعديل الدستور، جريدة رسمية عدد 25 مؤرخ في 04 أفريل 2002، معدل ومتمم بالقانون رقم 08–19 مؤرخ في 15 نوفمبر 2008، يتضمن نص تعديل الدستور، جريدة رسمية عدد 63 مؤرخ في 16 نوفمبر 2008، معدل ومتمم بالقانون رقم 16–01 مؤرخ في 06 مارس 2016، يتضمن نص تعديل الدستور، جريدة رسمية عدد 14 مؤرخ في 07 مارس 2016) .

– الدستور الجزائري الصادر في 1 نوفمبر 2020 ،بموجب المرسوم الرئاسي رقم 20 . 442 المؤرخ في 30 ديسمبر 1 2020 ،المتعلق بإصدار التعديل الدستوري والمصادق عليه في الاستفتاء.

القانون

- القانون رقم 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها. جريدة رسمية عدد 47. الصادرة بتاريخ: 16 غشت

- قانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم الأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات -ج-ر 71 في 2004/11/10.

الأوامر

- أمر 66_ 155 المؤرخ في 8 يونيو 1966 ، يتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية رقم 48 ، مؤرخة في 10 يونيو 1966 المعدل و المتمم .

- أمر رقم 21-11، ممضي في 25 غشت 2021 الجريدة الرسمية عدد 65، المؤرخة في 26 غشت 2021، يتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية .

المراسيم

- المرسوم التنفيذي رقم 06-348 مؤرخ في 05 أكتوبر سنة 2006 ،المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة رسمية عدد 63 ،ص .29

ثانيا المراجع باللغة الأجنبية

أ - باللغة الفرنسية

1- D.B.PARKER, comibattre la criminalité informatique , edoros ,1987.

2 -Debray Stephan, internet face aux substances illicites, université de paris, 2002-2003.

3 -Klaus Tiede man, Fraude et autres délits d'affaires commis a l'aide d'ordinateurs électroniques, Rev, drpén , crim, 1984.

4- MASCALA Corinne , criminalité et contrat électronique, Travaux de l'association, CAPITANT Henir , journées National paris, 2000.

5 -FAUCHMOUX 6 VINCENT6 Daprery pierre, le Droit de l'internet (loi ,contra et sage) , édition , lutec , paris ,2008.

ب – باللغة الإنجليزية

1- Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984.

2-Johannes F.NIJIbaer , challenges for the low of Evidence, leiden ,INREP,1999.

3- MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,"R.I.D.P",1993.

4 - Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc. edition,1992.

5-M. Moherenschloger ,computer crimes and others crimes against information technology in the Germany,Rev ,int,dr, pen ,1993.

6- WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom "R.I.D.P" , 1991,p19.

الفهرس

مـلخص مذكرة الماستر

بالرغم من المزايا الهائلة التي تتحققها تقنية المعلومات في شتّى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل ظهور الجرائم المعلوماتية التي تمتاز بسمات متميزة عن الجرائم التقليدية، الأمر الذي أثار مشكلة عدم إمكانية تطبيق النصوص الموضوعية التقليدية لقانون العقوبات، فتبلورت لدى الدول فكرة وضع نصوص قانونية خاصة إلا أنها اختلفت في أسلوب المعالجة التشريعية لذلك. كما تثير الجريمة المعلوماتية من جهة أخرى نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها، مما أدى إلى ضرورة التطوير في هذه الإجراءات من خلال التطوير في الأحكام العامة للإجراءات التقليدية، وعن طريق خلق إجراءات حديثة مختلفة عن تلك المتبعة في سبيل مكافحة الجرائم العادية

الكلمات المفتاحية:

1/ الجريمة المعلوماتية 2/ المتابعة القضائية 3/ أساليب التحري 4/ إجرءات التفتيش 5/. الإختصاص المحلي 6/ الإختصاص القضائي

Abstract of The master thesis

Despite the enormous advantages achieved by information technology in various fields of contemporary life, this growing technological revolution was accompanied by the emergence of information crimes that have distinct features from traditional crimes, which raised the problem of the inability to apply the traditional substantive texts of the Penal Code. Developing special legal texts, but they differed in the method of legislative treatment of this. Information crime, on the other hand, due to its specificity, raises the problem of insufficient traditional investigation and investigation procedures in obtaining digital evidence resulting from its commission, which led to the need for development in these procedures through development in the general provisions of traditional procedures, and by creating modern procedures different from those used for
Fighting ordinary crimes

key words:

./1Information crime 2/ Judicial follow-up 3/ Investigation methods 4/. inspection procedures. 5/. Local jurisdiction 6/. Jurisdiction