وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي

في الحقوق

تخصص : قانون جنائي و العلوم الجنائية

بعنوان :

قواعد الاختصاص في الجريمة المعلوماتية

في التشريع الجزائري

إعداد الطالبتين خرفي نوال /قريشي هاجر:

نوقشت و أجيزت بتاريخ : .../..../2021 تحت اشراف اللجنة المكونة من السادة :

– أ . بن عمر ياسين..... جامعة ورقلة .....مشرفا

– أ . شنين صالح ..... جامعة ورقلة .....رئيسا

– أ. الداوي نجاة ..... جامعة ورقلة .....مناقشا

السنة الجامعية : 2020– 2021

وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي

في الحقوق

تخصص : قانون جنائي و العلوم الجنائية

بعنوان :

قواعد الاختصاص في الجريمة المعلوماتية

في التشريع الجزائري

إعداد الطالبتين خرفي نوال /قريشي هاجر:

نوقشت و أجيزت بتاريخ : .../..../2021 تحت اشراف اللجنة المكونة من السادة :

– أ . بن عمر ياسين.....أستاذ مساعد أ بجامعة ورقلة .....مشرفا

– د. شنين صالح .....أستاذ محاضر أ بجامعة ورقلة .....رئيسا

– د. الداوي نجاة .....أستاذ محاضر ب بجامعة ورقلة .....مناقشا

السنة الجامعية : 2020– 2021

الإهداء

إلى من وضع المولى – سبحانه وتعالى – الجنة تحت قدميها، ووقَّرها في كتابه العزيز...

(أمي الحبيبة).

إلى خير مثال لرب الأسرة، والذي لم يتهاون يوم في توفير سبيل الخير والسعادة لي..

(أبي العزيز).

إلى إخوتي وأخواتي .... إلى أصدقائي ومعارفي

إلى أساتذتي في كلية الحقوق والعلوم السياسية

إلى كل طالب علم ....إلى زملائي في قسم الحقوق

أُهدي لكم عملنا المتواضع

نوال

الإهداء

إلى من فيهما قال ذا الجلال والإكرام "ولا تقل لهما اف ولا تنهرهما وقل لهما قولا كريما"

الى الصدر الدافئ والقلب العطوف رمز الصبر والتضحية الجوهرة الثمينة " أمي" الغالية

الى من علمني النجاح والصبر وسقاني كؤوس الكفاح الى من زرع البسمة في نفسي طوال حياتي ابي الغالي بارك الله في عمره

الى مصدر همتي وفخري اخوتي وأخواتي الأعزاء الى اصدقائي وصديقاتي وبالأخص نوال التي شاركتني هذا العمل الى اساتذتي في كلية الحقوق والعلوم السياسية الى جميع طلبة السنة الثانية ماستر قانون جنائي وكل شخص عزيز على قلبي اهدي هذا العمل المتواضع

هاجر

شكر و عرفان

نشكر الله عز وجل الذي بتوفيق وفضل منه تمكنا من انجاز هذه

المذكرة نتقدم بالشكر الجزيل إلى الأستاذ المشرف على كل توجيهاته والمساعدة

التي قدمها لنا طيلة انجاز هذا العمل كما نشكر كل أساتذة قسم الحقوق

على كل ما قدموه لنا طيلة سنوات الدراسة والشكر موصول إلى كل من ساعدنا

ودعمنا في انجاز هذه الدارسة

الباحثتان

الملخص :

تتميز الجريمة المعلوماتية عن الجريمة التقليدية من حيث تعريفها وخصائصها و أركانها و كذا القانون الواجب التطبيق عليها، حيث أوجد الفقه الجنائي عدة معايير لتحديد ماهيتها منها معيار وسيلة ارتكاب الجريمة و معيار محل الجريمة ومعيار الجمع بين عدة معايير.

و ترتيبا على ذلك، اتسمت الجريمة المعلوماتية بخصائص عديدة أهمها أنها جريمة عابرة للحدود تمارس داخل أو بواسطة النظام المعلوماتي ،وترتكب من طرف مجرم معلوماتي يوصف بالسرعة و الذكاء و المهارة ، كما أنها صعبة الإثبات مقارنة بالجريمة العادية لأنها سريعة التنفيذ ومتطورة بتطور الوسائل التكنولوجية . مما أدى إلى ظهور أنواع كثيرة منها قسمها الفقه و التشريع الجنائي إلى جرائم واقعة على النظام المعلوماتي و جرائم واقعة بواسطة النظام المعلوماتي.

كل هذه الخصائص للجريمة المعلوماتية ، أوجدت صعوبة في تحديد القانون الواجب التطبيق عليها و القضاء المختص بمنازعاتها مما أدى بالقوانين المقارنة و القانون الجزائري إلى تبني التعاون و المساعدة القضائية لمكافحة هذه الجرائم عن طريق إبرام الاتفاقيات الدولية و الإقليمية و عقد المؤتمرات و الندوات لاكتساب الخبرة الكافية لمواجهة هذه الجرائم ذات البعد العالمي.

Abstract:

Cybercrime is distinguished from conventional crime in its definition، characteristics، elements and the law applicable to it، given that the jurisprudence has developed several norms in order to define cybercrime such as the norm of the means by which the crime is committed and the norm of the place of the crime as well as that of meeting several norms.

On the basis of this principle، cybercrime has been distinguished by several characteristics، in particular that it is a transnational crime and is committed within or by means of a computer system. It is a crime whose perpetrator is supposed to be a fast، intelligent and skilled person. It is also a difficult crime to prove، contrary to conventional crimes، because it is committed quickly، in a developed way by use of technological means، which has led to the appearance of several types of cybercrimes that jurisprudence and criminal legislation have classified as crimes occurring on the computer system and crimes committed using the computer system.

All these characteristics of the cybercrime have resulted in the difficulty of defining the law applicable to this crime and the competent justice، which has led the comparative laws and the Algerian law to adopt mutual assistance and legal assistance in order to combat these crimes through the conclusion of international and territorial conventions and the holding of seminars and conferences in order to gain sufficient experience to combat these crimes on a global scale.

مقدمة

مقدمة

لعل مقولة مؤسس شركة مايكروسوفت "إن أجهزة الحاسوب وجدت لتحل المشاكل التي لم تكن موجودة سابقا" تلخص كل ما تعانيه حياتنا المعاصرة من مشاكل بسبب التكنولوجيا الحديثة وحقيقة هـذا القول أن التكنولوجيـا الحديثة حلت العديد من المشاكل و المعوقات على الصعيد المهني و الشخصي لكنها في نفس الوقت أوجدت العديد من المشاكل لحياة الإنسان.

فقد شهدت الحياة اليومية تطوراً متسارعاً ومذهلا في مجال تقنية المعلومات وتعمم استعمالها فلم يعد الحديث اليوم عن الحاسوب وقدراته في تخزين المعلومات وانجاز العمليات المعقدة و إنما عن تكنولوجيا الإعلام و الاتصال Technologies de L'information et de La communication.

لينطلق عصر جديد يسمى بعصر المعلوماتية نظراً للكم الهائل من المعلومات فائقة الأهمية التي لها تأثير على الأفراد و الحكومات فأصبحت المعلومة قوة لا يستهان بها في يد الفرد أو في يد الدولة بل وحتى أصبحت المعلومات سلاحا في يد المجرمين.

ومن هنا نشأ ما يسمى بجرائم المعلوماتية ومن المعروف أن لهذه البيئة الالكترونية رواد عديدون فقد وجد المجرمون في هذه البيئة مجالا خصبا لارتكاب صور متعددة ومتباينة للجريمة المعلومـاتية فمنها مـا يتصل بالاعتداء على النظام الالكتروني وجرائم الاعتداء على الحق في الخصوصية وجرائم الاعتداء على التحويلات المالية الالكترونية و أشكالا أخرى يصعب حصرها .

فأصبحت الجريمة المعلوماتية ظاهرة عالمية و نوع مختلف و مغاير تماما عن أشكال الجرائم الأخرى التي تهدد العالم بصفة عامة و المجتمع الجزائري بصفة خاصة و الجزائر باعتبارها واحدة من الدول التي تعرضت إلى مثل هذا التطور التكنولوجي سواء كان ايجابيا أو سلبيا فكان لابد من إيجاد إطار قانوني مناسبا ، فما كان على المشرع الجزائري إلا أن يضع مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجريمة التقليدية و الجريمة المعلوماتية وذلك عن طريق تعديل قانون العقوبات وقانون الإجراءات الجزائية لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام و الاتصال. وقام باستحداث قوانين أخرى خاصة وإجراءات تتماشى وطبيعة الجرائم المستحدثة كالتي تطبق على الجريمة المعلوماتية فقط، والتي نص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته 09-04 المؤرخ في 05 أوت 2009.

فموضوع هذه الدراسة مهم بسبب استغلال وسال الاتصال الحديثة من قبل مرتكبي الجرائم المعلوماتية وهي ظاهرة جديدة مرتبطة بتكنولوجيا الحاسبات الآلية مما ميزها بمجموعة من الخصائص تختلف عن الجرائم التقليدية مما يستدعي التعامل معها بما يتلاءم مع هذه الخصوصية.

ولهذه الدراسة أهمية نظرية وعملية حيث نتطرق إلى الإجراءات التي تطبق على الأنماط المستجدة للجريمة المعلوماتية، ومع ازدياد معدل هذه الجرائم كان لزاما أن يواكب هذا فهماً كاملا لهذا النوع من الجرائم وكيفية مواجهتها سواء من الناحية التقنية أو من الناحية القانونية.

وتهدف هذه الدراسة إلى :

- الوقوف على إجراءات متابعة جرائم الفضاء الافتراضي ومكان وقوع الجريمة
- المشكلات الإجرائية التي تثيرها الجريمة المعلوماتية
- محاولة إجراء مقارنة بين التشريع الجزائري وبعض التشريعات الأخرى في مجال الجريمة الالكترونية، وإبراز جوانب التوفيق و القصور.
- البحث في مدى ملائمة الإجراءات الموجودة لمواجهة خصوصية هذه الجرائم.

يرجع السبب في اختيارنا لهذا الموضوع إلى العديد من الأسباب منها:

الشخصي و الموضوعي ، بالنسبة لسبب الشخصي هو أن الموضوع يعتبر من المواضيع الحديثة و المتطورة مع تطور التكنولوجيا ويختلف من حيث الإجراءات عن الجرائم التقليدية وراجع لرغبتنا الشديدة في الوقوف على هذه الجرائم التي ترتكب في عالم افتراضي وحقيقة التعامل معها ، فالموضوع حيوي رغم تشابك أبعاده وأحيانا الغموض و اللامنطقية الذي يميز هذه الجرائم من حيث زمان ومكان وقوعها.

والسبب الموضوعي يكمن في ما يطرحه الموضوع من قواعد إجرائية خاصة للجريمة المعلوماتية التي جاء بها القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها وكذا تعديل قانون الإجراءات الجزائية ومن جهة أخرى أن هذه الجرائم لا يتقيد مرتكبوها بالحدود الجغرافية ولا يحترمون الاختصاص القانوني للدول .

واتبعنا لمعالجة هذا الموضوع المنهج التحليلي والمنهج الوصفي وكذا منهج المقارن كمنهج مساعد كلما اقتضت الضرورة ذلك وهي الأنسب لهذه الدراسة من خلال تحليل مختلف المواد القانونية .

وقد تطرقت عدة دراسات إلى الجريمة المعلوماتية لكن أغلبها كانت تدرس من الناحية الموضوعية ولم تفصل في الناحية الإجرائية وتركزت أغلب الدراسات الموجودة على الدراسات التقنية أما الدراسات ذات البعد القانوني في مختلف جزئياته فهي متفرقة واهتم بعضها فقط على المقارنة بين التشريعات، نذكر منها:

- معاشي سميرة ، الجريمة المعلوماتية(دراسة تحليلية لمفهوم الجريمة المعلوماتية)،جامعة محمد خيضر، بسكرة ،2018.

- ابتسام يغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر، جامعة العربي بن مهيدي ، أم البواقي، 2016.

– وردي الطيب، الاختصاص القضائي في جرائم الأنترنت، جامعة الطاهر مولاي، سعيدة ،2015.

– لعقال فريال، الجريمة المعلوماتية في ظل التشريع الجزائري،جامعة أكلي محند اولحاج، البويرة، 2015.

ومن بعض الصعوبات التي واجهتنا خلال انجاز الموضوع لا نقول قلة المراجع وإنما المراجع المتخصصة خاصة التي تتناول الموضوع في التشريع الجزائري

ومن خلال كل ما تقدم فالموضوع يطرح الإشكالية التالية :

ما مدى ملائمة قواعد الاختصاص التقليدية في التشريع الجزائري في معالجة خصوصية الجريمة المعلوماتية ؟

ومن أجل معالجة الإشكالية التي يطرحها موضوعنا قمنا بتقسيم الدراسة وفقا لخطة تتكون من فصلين ، الفصل الأول: الأحكام العامة للجريمة المعلوماتية و الفصل الثاني : قواعد الاختصاص في الجريمة لمعلوماتية .

الخطة :

الفصل الأول: الأحكام العامة للجريمة المعلوماتية

المبحث الأول : مفهوم الجريمة المعلوماتية

المطلب الأول : تعريف الجريمة المعلوماتية

الفرع الأول : التعريفات الفقهية للجريمة المعلوماتية

الفرع الثاني : تعريف المشرع الجزائري للجريمة المعلوماتية

المطلب الثاني : خصائص وتقسيمات الجريمة المعلوماتية

الفرع الأول : خصائص الجرائم المعلوماتية

الفرع الثاني : تقسيمات الجريمة المعلوماتية

المبحث الثاني : الإطار القانوني المنظم للجريمة المعلوماتية

المطلب الأول : الإطار القانوني المنظم للجريمة المعلوماتية في التشريعات العربية

الفرع الأول : القانون المنظم للجريمة المعلوماتية في التشريع المغربي

الفرع الثاني: القانون المنظم للجريمة المعلوماتية في قانون الاتحاد الإماراتي

المطلب الثاني : الإطار القانوني المنظم للجريمة المعلوماتية في التشريعات الأجنبية

الفرع الأول : القانون المنظم للجريمة المعلوماتية في التشريع الفرنسي

الفرع الثاني : الاتفاقية الأوروبية الخاصة بجرائم تقنية المعلومات بودابيست

الفصل الثاني : قواعد الاختصاص في الجريمة المعلوماتية

المبحث الأول : القواعد الإجرائية للمتابعة في الجريمة المعلوماتية

المطلب الأول : إشكالات المتابعة و التحري و في الجريمة المعلوماتية

الفرع الأول: الإجراءات الكلاسيكية في الجريمة المعلوماتية

الفرع الثاني : إجراءات خاصة في التحقيق المعلوماتي

المطلب الثاني :إشكاليات الاختصاص في الجريمة المعلوماتية

الفرع الأول : القانون الواجب التطبيق على الجرائم المعلوماتية

الفرع الثاني : تنازع الاختصاص في الجريمة المعلوماتية

المبحث الثاني : الجهات و الهيئات المختصة بمتابعة الجريمة المعلوماتية

المطلب الأول : اختصاص الاقطاب الجزائية المتخصصة في الجريمة المعلوماتية

الفرع الأول : سير وتنظيم الأقطاب الجزائية المتخصصة

الفرع الثاني: طرق اتصال القطب الجزائي المتخصص بالجريمة المعلوماتية

المطلب الثاني : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

الفرع الأول : اختصاص الهيئة

الفرع الثاني : مهام الهيئة

الفصل الأول :

الأحكام العامة للجريمة المعلوماتية

تمهيد

إن بيان المشكلات القانونية و العملية التي تثيرها الجريمة المعلوماتية تتطلب منا أن نقوم ببحث في مسألة أولية وهي البحث عن تعريف لهذه الجريمة بتبيان معناها و خصائصها وكذلك طبيعتها القانونية ، ولقد استخدمت عدة مصطلحات لدلالة على هذه الظاهرة الإجرامية ، فمنهم من أطلق عليها اسم الغش المعلوماتي ، و البعض الآخر اسماها جرائم الحاسب الآلي ، أو جرائم الكمبيوتر و الانترنت ، والجريمة المعلوماتية في الدول الأوروبية يطلق عليها اسم cybercriminalité.

أما المشرع الجزائري اصطلح على تسميتها الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال [1].

المبحث الأول: مفهوم الجريمة المعلوماتية

ونظرا لحداثة هذه الجرائم فإن الإحاطة بمفهوم دقيق لا يزال محل خلاف فقهي بين فقهاء القانون الجنائي في القانون المقارن على الوصف القانوني السليم لهذا المصطلح أو التسمية وتختلف عن الجريمة التقليدية من حيث المفهوم لدى قسمنا هذا المبحث إلى مطلبين الأول نعرض فيه تعريفات الفقهية لهذه الجرائم والمطلب الثاني خصائص وتقسيمات الجريمة المعلوماتية .

. 1- لعقال فريال ،الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر ، قانون جنائي ، جامعة اكلي محند اولحاج، البويرة ،2015،ص7

المطلب الأول: تعريف الجريمة المعلوماتية

لقد ذكرنا أنه ظهر اختلاف في تعريف الجريمة المعلوماتية في العديد من التشريعات رغم وجود بعض الجهود الفقهية المختلفة التي نتج عنها عدة تعريفات متفاوتة فيما بينها منها الضيق و الواسع ، سنحاول الوصول إلى تعريف يتلاءم وطبيعة هذه الجريمة المرتكبة عبر الانترنت .

الفرع الأول: التعريفات الفقهية للجريمة المعلوماتية

– تعريفات ركزت حول وسيلة ارتكاب الجريمة

نجد الفقيهين الألمانيين LAUS.Tiedeman و CARLE.Benson عرفا الجريمة المعلوماتية على أنها: " كل أشكال السلوك غير المشروع – أو الضار بالمجتمع– الذي يرتكب باستخدام الحاسوب " و "أنها فعل إجرامي يستخدم الحاسوب في ارتكابها كأداة رئيسية"[2]

– تعريفات ركزت حول موضوع الجريمة :

أنصار هذا الاتجاه الفقيه Rosanblati الذي عرفها " أنه نشـــاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلـى المعلومـات المخزنة داخل الحـاسب أو التي تحول عن طريقه"[2]

كما عرفت الدكتورة هدى قشقوش الجريمة الالكترونية بأنها :" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات".

– التعريف المسند إلى وجوب إلمام الفاعل بتقنية المعلومات :

2– معاشي سميرة ، مفهوم الجريمة المعلوماتية (دراسة تحليلية) ، جامعة محمد خيضر بسكرة، مجلة المفكر العدد 17، 2018، ص 402 .

عرفها "David Thompson" بأنها: "أية جريمة يكون متطلبًا لاقترافها،أن تتوفر لدى فاعلها معرفة تقنية للحاسب" إذ يرى أن تعريف هذه الجريمة يجب أن يسند الى معيار شخصي إذ على الفاعل أن يكون ملما بتقنية المعلومات[3] .

– التعريف المسند إلى معايير مختلفة :

لقد اختلف هـذا الاتجـاه في المعـايير المتبنـــاة فـي تعريفه للجريمة المعلومـــاتية بعيدا عن المعايير السابقة ، إذ عرف الفقيه الفرنسي الأستاذ Massa أن الجريمة المعلوماتية هي : " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" ،وتعريف آخر للخبير الأمريكي Parker.D الذي قال " أنها فعل إجرامي أيا كانت صلته بتقنية المعلومات فيه يتكبد المجني عليه ونتيجة له خسارة ويحقق الفاعل ربحاً عمديا ". [4]

ويرى الأستاذ يونس عرب أن جرائم الكمبيوتر تعرف أنها " الأفعال غير المشروعة المرتبطة بنظم الحواسيب " و أنها سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محلها معطيات الكمبيوتر.

أما الأستاذ عبد الفتاح بيومي الحجازي فيرى أن الجريمة المعلوماتية " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ الفعل الإجرامي المقصود"[5]

---

3 – د. رضا فولي عثمان، المشكلات العلمية و القانونية للجريمة المعلوماتية في العصر الرقمي، http://www.al-fadjr.com/ar/realite/352178.html ، 20 نوفمبر 2020 ، 11:25 .

4 – معاشي سميرة ، مرجع سابق، ص 403

5 – المرجع نفسه ، ص 405

الفرع الثاني : تعريف المشرع الجزائري للجريمة المعلوماتية:

المشرع الجزائري كما المشرع الفرنسي الذي لم يعط تعريفا للجريمة المعلوماتية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب المادة الثانية من القانون 09 – 04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية [6]"

ويلاحظ على هذا التعريف ما يلي:

أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية، كونه أقر أن الجريمة المعلوماتية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم المعلوماتية في القانون الجزائري[7].

6 – القانون رقم 09-04 المؤرخ في 5غشت 2009 ،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها ، الجريدة الرسمية ، العدد 47 ، ص 5.

7– أ .نمديلي رحمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف 2 الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية ، طرابلس/ لبنان، يومي 24-25|03|2017، ص 95 .

حاول المشرع الجزائري ، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم المعلوماتية، ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام أدى إلى اتساع نطاق الجريمة المعلوماتية فهي أصبحت لا تقتصر على جريمة واحدة وإنما اتسعت إلـــى عدة جرائم ، ومن جهة أخــرى كون القانون الجنائي التقليدي غير قــادر على استيعاب الجرائم المعلوماتية الحديثة إضافة إلى ذلك المحافظة على مبدأ الشرعية الجنائية متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها[8].

المطلب الثاني: خصائص وتقسيمات الجريمة المعلوماتية

الجريمة المعلوماتية ذات طبيعة خاصة وخصائص منفردة لا تتوفر في الجريمة التقليدية سواء من حيث أسلوب وطرق ارتكابها ، مما أدى إلى ظهور أنواع كثيرة منها قسمها الفقه و التشريع الجنائي ، سنتطرق في هذا المطلب إلى السمات الخاصة بالجريمة المعلوماتية والتقسيمات لهذه الجرائم.

الفرع الأول : خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن الجريمة التقليدية ، سواء تعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي ، لدى سنتطرق لبعض خصائص هذه الجريمة[9] .

[8]- نمديلي رحمة، مرجع سابق، ص95 .
[9] - لعقال فريال مرجع سابق ، ص 15- 16

أولا :الجريمة المعلوماتية جريمة عالمية عابرة الحدود:

إن البيئة الافتراضية لا تعترف بالقيود ولا الحدود فالجريمة المعلوماتية جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت وتقنية المعلومات، فغالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه وهي جرائم لا يتواجد الفاعل على مسرح الجريمة بل يرتكبها عن بعد ، أي عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة .

ويثير الطابع الدولي لهذه الجريمة عدة إشكاليات وصعوبات قانونية لاسيما مشكلة تحديد المحكمة صاحبة الاختصاص القضائي ، أدلة الإثبات و قبولها أمام قضاء دولة أخرى وكذا تحديد القانون الواجب التطبيق بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية ،لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام اتفاقيات دولية خاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم[10].

ثانيا : صعوبة اكتشاف واثبات الجريمة المعلوماتية

تتسم هذه الجرائم بالخفاء إذ هناك صعوبة في اكتشافها و الاستدلال على مرتكبيها ويرجع ذلك إلى عدة أسباب من بينها وسيلة تنفيذها تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد وعدم تركها أثراً خارجيا ، فتنصب على البيانات

10 – سوير سفيان: الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010، ص 12.

و المعلومات المخزنة في نظم الحواسيب ، زيادة على إمكانية تدمير المعلومات التي يمكن استخدامها كدليل في الإثبات في وقت قياسي[11] .

ومن الصعوبات أيضا التي تعترض اكتشاف الجريمة المعلوماتية ضعف رقابة نظم الحواسيب فـــي اكتشاف الجرائم وهو ما يسميه البعض بالدور غير المباشر للمجني عليه في ارتكاب الجريمة، بالإضافة إلى خشية المجني عليه من الإبلاغ.

ثالثا: أسلوب ارتكاب الجريمة

إن الطبيعة الخاصة لهذه الجريمة تبرز بصورة واضحة في أسلوب ارتكابها فالجريمة المعلوماتية جريمة هادئة تقع بمجرد الدوس على أزرار لوحة المفاتيح و قيام الجاني بهتك سرية المعلومة ،محوها ، تشويهها أو تعطيلها ، فكل ما يحتاجه الجاني في هذه الجريمة قوة علمية وقدرة من الذكاء و المهارة أي أن الإجرام المعلوماتي هو إجرام الأذكياء مقارنة مع الإجرام التقليدي الذي يميل إلى العنف فالمجرم المعلوماتي عادة ما يكون ذو مهارات عالية وملم بتكنولوجيا المعلوماتية [12].

رابعا: الخبرة الفنية في التعامل مع الجريمة المعلوماتية

تتطلب الجريمة المعلوماتية الالمام بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو ملاحقتها قضائيا.

11 – لعقال فريال ، الجريمة المعلوماتية في ظل التشريع الجزائري، ص16

12–معاشي سميرة ، مرجع سابق ، ص 414.

لذلك يجد رجال الضبطية القضائية أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فضلا عن صعوبة اجراء التحريات السرية وتتبع مسار العمليات الالكترونية العابرة للحدود.

كما أن رجال الشرطة قد لا يتعاملون مع ساحة الجريمة خلال المعاينة و الدليل الالكتروني بمهارة و احترافية ، فقد يتسبب المحقق بدون قصد أو بطريق الخطأ في اتلاف الدليل الالكتروني أو تدميره[13] .

الفرع الثاني : تقسيمات الجريمة المعلوماتية

لقد تعددت الجرائم المعلوماتية بتعدد وسائلها وأنماطها في مختلف التشريعات المقارنة خاصة في أوروبا، حيث كانت الدول الأوروبية الأكثر نضجا في العالم في التعامل مع هذه الظاهرة الإجرامية، وفي مقدمتها فرنسا وبريطانيا حيث سن المشرع الفرنسي القانون رقم 19 -88 الصادر في 05 كانون الثاني 1988 الخاص بالولوج في الجرائم المعلوماتية كما تضمن قانون العقوبات الفرنسي في المادة 462 فقرة 4 منه جريمة الولوج إلى نظام المعالجة الآلية أو النفاذ غير المشروع، وشدد العقوبة في حالة إذا انجر عن هذا الولوج محو أو تعديل المعطيات المعالجة آليا، كما نص على تجريم إتلاف المعطيات أو تزوير المستندات المعالجة آليا أو استعمالها وعاقب عليها بعقوبة الحبس أو الغرامة. بينما في بريطانيا صدر

13 – غنية باطلي ، الجريمة الالكترونية (دراسة مقارنة) ، منشورات دار الجزائرية ، الجزائر 2015 ، ص 46

قانون إساءة استخدام الحاسوب لسنة 1990 وبدأ سريانه بتاريخ 29 أوت 1990، وقسم الجرائم الالكترونية إلى:

أ- الدخول غير المصرح به لنظام الحاسوب.

ب- نفس الفعل السابق لكن بنية ارتكاب أو تسهيل ارتكاب فعل آخر.

ج - التعديل أو التحويل غير المصرح به لنظام الحاسوب بقصد إضعافّ أو تعطيل النظام.

وأهم تصنيف للجرائم المعلوماتية جاءت به الاتفاقية الأوروبية بشأن الجرائم المعلوماتية وهي اتفاقية بودابست لسنة2001، حيث قسمت الاتفاقية هذه الجرائم إلى[14]:

الطائفة الأولى : الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات، أي الجرائم التي تستهدف معطيات الكمبيوتر سواء بالاطلاع عليها أو إفشائها أو تصويرها، أو إتلافها.

الطائفة الثانية : وهــي الجرائم المرتبطة بالكمبيوتر أي الجرائم التي يلعب فيهـا الكمبيوتر أو الحاسب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الالكتروني.

الطائفة الثالثة :الجرائم المرتبطة بالمحتوى، أي يلعب فيها الكمبيوتر دور البيئة الجرمية كجرائم المواد اللاخلاقية للأطفال، وجرائم القمار وغسيل الأموال والمخدرات.

الطائفة الرابعة :وهي الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف وهو نص مكمل لما جاءت به قوانين الملكية الفكرية المقررة وطنيا ودوليا[15].

---

[14] - غنية باطلي ،مرجع سابق ، ص47

15- يونس عرب، تطور التشريعات في مجال مكافحة الجرائم، الالكترونية، هيئة تنظيم الاتصالات، سلطنة عمان، مسقط، 2 و4 أفريل 2006، ص 21- 23.

ولقد أحدث المشرع الجزائري قسم في قانون العقوبات في القسم السابع مكرر من القانون 15/04 المؤرخ في 2004/11/10 المعدل و المتمم لقانون العقوبات الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

في المواد من 394 مكرر إلى غاية المادة 394 مكرر 7، وباستقرائنا لهذه المواد يتضح أن المشرع الجزائري قد قسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو الجرائم الالكترونية إلى الطوائف التالية[16]:

الطائفة الأولى : طبقا للمادة 394 مكرر من قانون العقوبات وهي جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

ويعاقب الجاني بعقوبة 3 أشهر إلى سنة وبغرامة من 50.000 د ج إلى 200.000 دج وتشدد العقوبة إذا ترتب عن الفعل الإجرامي حذف أو تغيير المعطيات ، كما يعاقب الجاني بـ 6 أشهر إلى سنتين وغرامة من 50.000دج إلى300.000دج وفي حالة التخريب النظام المعلوماتي.

16 – انظر القانون رقم 04 –15المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ، الجريدة الرسمية رقم 44 .

الطائفة الثانية : الجرائم الالكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الالكتروني والسطو والنصب والاحتيال والسلب وغيرها، وهذا ما نصت عليه المادة 394 مكرر 2، وعقوبتها من شهرين إلى 3 سنوات وبغرامة 1000.000دج إلى 10.000.000دج.

الطائفة الثالثة : الجرائم الالكترونية المتعلقة بأمن الدولة و مؤسساتها كجرائم التجسس و الإرهاب و عقوبتها تضاعف عقوبة الطائفة الثانية لخطورتها طبقا للمادة 394 مكرر3.

الطائفة الرابعة : الجرائم الالكترونيـــة للشخص المعنـــوي، حيث نص المشرع الجزائري على خلاف التشريعات المقارنة الأشخاص المعنوية بنص خاص وعقوبتها تعادل خمس مرات الجرائم المرتكبة من طرف الشخص الطبيعي طبقا للمادة 394 مكرر4 من قانون العقوبات الجزائري[17].

كمـا عـــاقب المشرع الجزائري على الشروع فـي الجريمة المعلوماتية كما هو الحال في الجريمة العادية أو التقليدية بنفس العقوبة للجريمة الكاملة مع تكييفها جنحة وفقا لقانون العقوبات .

17 – القانون رقم 14-01 المؤرخ في 04 فبراير 2014 المعدل للأمر رقم 66-156 المؤرخ في 8يونيو1966 المتضمن قانون العقوبات الجزائري.

كما نص كذلك على الاشتراك في الجريمة المعلوماتية كما هو الحال في الجريمة العادية ويأخذ الشريك في الجريمة المعلوماتية نفس العقوبة المقررة للشريك في الجريمة العادية أو التقليدية طبقا لقانون العقوبات الجزائري.

كما نص كذلك على جريمة الاتفاق الجنائي المعلوماتي للوقاية من ارتكاب الجريمة المعلوماتية، طبقا للمادة 394 مكرر 5 من نفس القانون، إلا أن المشرع الجزائري لم يستحدث نصا على جريمة التزوير المعلوماتي الذي يعتبر من أخطر صور الغش المعلوماتي الذي جرمته أغلب التشريعات الحديثة والتي انتهجها المشرع الفرنسي بتعديل قانون العقوبات لسنة 1988 بصدور قانون 1994 عدل المادة 1/441 لكي تستوعب بجانب التزوير العادي جريمة التزوير المعلوماتي[18] .

ويلاحظ أن المشرع الجزائري قد توسع في نطاق الجرائم المعلوماتية سواء وقعت على النظام المعلوماتي أو بواسطته، وسواء وقعت على الأشخاص أو الأموال أو على أمن الدولة ومؤسساتها، كما أقر جريمة جديدة الكترونية وهي جريمة الاتفاق الجنائي الكترونيا رغم أنها من الأعمال التحضيرية لارتكاب الجريمة وشدد عقوبتها وذلك خشية استعمال النظام المعلوماتي كوسيلة لارتكاب الجريمة وتسهيلها.

18 – لعقال فريال ، مرجع سابق، ص 47

و ما يعاب على المشرع الجزائري عدم إفراد معيار واضح وواحد في تقسيم الجرائم المعلوماتية و تحديد عقوبتها، وكان من الأحسن إتباع المنهاج المتبع من طرف الفقه و هو تقسيمها إلى جرائم واقعة على النظام المعلوماتي و جرائم واقعة بواسطة النظام المعلوماتي ، بعد تحديد المصطلحات الخاصة بها لتسهيل فهم ماهيتها[19].

19 – نميلي رحمة ، مرجع سابق ، ص 105

المبحث الثاني : الإطار القانوني المنظم للجريمة المعلوماتية في التشريعات المقارنة

رغم صعوبة ضبط و مكافحة جرائم الانترنت على الصعيد العالمي إلا أن هناك جهود معتبرة قامت بها جل الدول العربية و الغربية التي وضعت قوانين لمكافحة جريمة الانترنت فعلى امتداد الوطن العربي من المحيط إلى الخليج، نجد ترسانة قانونية تنظم جرائم الانترنت وبدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة، حيث حرصت أغلب الدول على تعديل النصوص التجريمية التقليدية بصورة تلاءم هذه النوعية الحديثة من الجرائم.

المطلب الأول : الإطار القانوني المنظم في التشريعات العربية

من بين البلدان العربية التي عرفت تطورا في مجال المعلوماتية واستخدام شبكة الانترنت نجد المملكة المغربية وكذا الإمارات العربية المتحدة ، فكان لزاما عليها كذلك مواكبة هذا التطور من خلال سن قوانين جديدة وتعديل تشريعاتها بما يتواكب مع هذه التطورات.

الفرع الأول: الإطار القانوني المنظم للجريمة المعلوماتية في التشريع المغربي

إن وعي المشرع المغربي بخصوص الإجرام المعلوماتي وانعكاساته على المجتمع بدأ مع صدور القانون المتعلق بالإرهاب الذي أورد إمكانية ارتكاب أفعال إجرامية إرهابية عن طريق نظم المعالجة الآلية للمعطيات ، علما أن القانون الجنائي المغربي لا يحتوي على نصوص تخص الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات مما جعل المشرع يتبنى قانون خاص بهذه الجرائم[20] .

[20]– زعيطي أمينة، مكافحة الجرائم الإلكترونية في ضوء ق ع ج دراسة مقارنة، مجلة حقوق الانسان و الحريات ، جامعة مستغانم، العدد 7 ، 2019.، ص 232 .

أمام الصعوبات التي يشكلها تطبيق النصوص التقليدية على الجريمة المعلوماتية المستحدثة اضطر المشرع المغربي إلى سن تشريع يتلاءم و خصوصية الجريمة المعلوماتية انسجاما مع مبدأ الشرعية الجنائية بعد أن أظهر الواقع الأزمة الواضحة في تكييف الأفعال المستجدة طبقا لقواعد التقليدية للقانون الجنائي ، وقد أطلق عليها تسمية " المس بنظم المعالجة الآلية للمعطيات" Atteintes aux systèmes de traitement automatisés de données (STAD).

القانون رقم 03-07 المتعلق بالمساس بنظم المعالجة الآلية للمعطيات الصادر في 16 رمضان 1424 الموافق لـ11 نوفمبر 2003[21] .

ونشير إلى أن هذا القانون يمثل الإطار الأساسي الرائد لمحاربة الجريمة المعلوماتية في المغرب ، وكذا القانون المغربي رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية ، كما جاء القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي وهو يشكل أداة هامة لحماية الحياة الخاصة والبيانات الشخصية والخصوصيات التي تطبع الجرائم المعلوماتية سواء من حيث طبيعة مرتكبيها أو من حيث المضمون أو من حيث التطبيق القضائي تطرح تساؤلات أساسية حول الكيفية التي تعامل بها المشرع المغربي من أجل احتواء هذا النوع من الجرائم سواء من خلال تبني النصوص المجرمة الكفيلة بتحقيق استراتيجيات موازية ترمي إلى خلق تنسيق بين مختلف

[21]– مصطفى الفوركي ، الجرائم الماسة بالنظم المعلوماتية في القانون المغربي،مجلة البحوث القانونية و الاقتصادية ، جامعة الحسن الأول، المغرب ،العدد1،2020 ، ص 556.

الأجهزة المعنية من أجل مواجهة هذه الجرائم، كما يمكن التساؤل عن الخصوصيات التي تميز هذا النوع من الإجرام على المستوى التطبيق العملي[22].

تدخل المشرع المغربي ليتمم مجموعة القانون الجنائي بمقتضيات مجرمة لمختلف الأفعال المجرمة الماسة بنظم المعالجة الآلية للمعطيات وذلك بمقتضى القانون رقم 07.03 لسنة 2003، على ثلاثة أسباب رئيسية وهي:

أولا : مواءمة مجموعة القانون الجنائي مع المقتضيات التي أتى بها القانون المتعلق بمكافحة الإرهاب، بحيث تم تضمين اللائحة المنصوص عليها بالفصل 218-1 الذي أضيف لمجموعة القانون الجنائي بمقتضى قانون مكافحة الإرهاب، الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات باعتبارها أفعالا إرهابية إذا كانت لها علاقة عمدا بمشروع فردي أو جماعي بهدف المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف، والحال أن مقتضيات المجموعة الجنائية لم تكن تتضمن آنذاك فصولا خاصة بالجرائم الماسة بنظم المعالجة الآلية للمعطيات وبالتالي كان المشرع ملزما إلى حد ما بإصدار قانون رقم 07.03 من أجل المواءمة والتناسق في مقتضيات مجموعة القانون الجنائي[23].

ثانيا :ملئ الفراغ الذي كان يعرفه القانون الجنائي في هذا الإطار، والذي خلق عدة إشكالات عملية بالنسبة للقضاء المغربي الذي وجد نفسه عاجزا على إيجاد أساس قانوني للمتابعة وتطبيق العقاب الملائم على مرتكبي الأفعال الإجرامية المشكلة لبعض صور الجريمة

[22]– زعيطي أمينة ، مرجع سابق ، ص233

[23]– مسامح زكرياء ، خصوصيات الجريمة الالكترونية على ضوء التشريع و القضاء المغربي ،مجلة العلوم القانونية و الاقتصادية، 21 يوليو 2020،ص550.

المعلوماتية بحيث تم في حالات عدة تبرئة مرتكبي بعض هذه الأفعال استنادا لمبدأ الشرعية القانونية الذي يفرض عدم عقاب أحد على فعل لا يعد جريمة بصريح القانون ولا معاقبته بعقوبات لم يقررها القانون.

ثالثا : مواءمة التشريع الجنائي المغربي مع الاتفاقيات الدولية والإقليمية ومع مواقف التشريعات الأوروبية وخاصة التشريع الفرنسي، بحيث استفاد المشرع المغربي كثيرا من التطور التشريعي والقضائي الذي عرفته فرنسا في هذا الصدد. ولهذا جاء الباب العاشر من الجزء الأول من الكتاب الثالث من مجموعة القانون الجنائي المغربي والمتعلق بالمس ينظم المعالجة الآلية للمعطيات شبيها إلى حد كبير مع الباب الثالث من القسم الثاني من الكتاب الثالث من المدونة الجنائية الفرنسية والمتعلقة بالمساس بنظم المعالجة الآلية للمعطيات والمتضمن للمواد من 323-1 إلى 323-7[24].

وقد صادق مجلس الحكومة المغربية في 20 ديسمبر 2012 على مشروع القانون رقم 12-136 الذي وافق بموجبه على اتفاقية "بودابيست" المتعلقة بالجريمة الإلكترونية وكذا على برتوكولها الإضافي الموقع بستراسبورغ في 28 يناير 2003 بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، وبهذا تعتبر المغرب أول دولة عربية تتبنى هذه الاتفاقية و بروتوكولها[25].

[24] – علال فالي: خصوصية الجريمة المعلوماتية" مقال بمجلة القضاء التجاري الثاني السنة 2013، ص .125

[25] - مسامح زكرياء ، مرجع سابق ، ص 550

وعموما لا تخرج صور الجريمة المعلوماتية التي تم تجريمها بمقتضى قانون 07.03 عن أربعة صور رئيسية يمكن أن تأتي مترابطة فيما بينها أو مستقلة عن بعضها البعض بحيث يكفي لتوقيع العقوبات المقررة لها ارتكاب إحدى هذه الصور فقط أو فعل من الأفعال المكونة لها، وهذه الصور هي:

- الدخول أو البقاء بشكل غير قانوني في نظام المعالجة الآلية للمعطيات .
- عرقلة سير النظام أو إحداث خلل فيه .
- الاحتيال أو الغش المعلوماتي .
- تزوير الوثائق المعلوماتية أو استعمالها .

الفرع الثاني : الإطار القانوني المنظم للجريمة المعلوماتية في قانون الاتحاد الإماراتي

قامت الدول العربية على غرار الدول الغربية بتطوير بنيتها التشريعية لمواكبة تطور الجريمة المعلوماتية، ومن بين الدول العربية الإمارات العربية المتحدة في قانون الاتحاد رقم 02 لسنة 2006 الذي ورد في شأن مكافحة الجرائم المعلوماتية جملة من المصطلحات ذات الدلالة القانونية نذكر منها:[26]

المعلومات الإلكترونية: وهي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وتشمل الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.

البرنامج المعلوماتي: هو مجموعة من البيانات والتعليمات والأوامر، قابلة لتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما.

[26] – بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر ، قانون جنائي ،جامعة محمد خيضر بسكرة ، 2016 ، ص24

النظام المعلوماتي الإلكتروني: هو مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك.

الشبكة المعلوماتية : هو ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها.

المستند الإلكتروني: عبارة عن سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية على وسيط ملموس أو على أي وسيط الكتروني آخر ويكون قابل للاسترجاع بشكل يمكن فهمه.

الموقع: هو مكان إتاحة المعلومات على الشبكة المعلوماتية .

وسيلة تقنية المعلومات:أي أداة الكترونية مغناطيسية ،بصرية، كهر وكيميائية ، أو أي أداة أخرى تستخدم لمعالجة البيانات وأداة المنطق الحاسب أو الوظائف التخزينية ويشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة.

نص القانون السابق الذكر على مجموعة من الجرائم المعلوماتية كجريمة اختراق المواقع والأنظمة الالكترونية.[27]

نصت المادة الرابعة من القانون السابق على عقوبة تزوير المستندات معترف بها معلوماتيا وكذلك على استعمال المستند المزور مع العلم بذلك ، وجرم القانون كذلك الأفعال التالية:

– العبث بالفحوص الطبية باستخدام الانترنت وكذلك القيام بالتصنت او الاعتراض المرسل عن طريق الشبكة المعلوماتية واستخدام الانترنت في الابتزاز و التهديد وعاقب على هذه

[27]– بعرة سعيدة ، مرجع سابق، ص 25

الافعال بعقوبة السجن مدة عشرة سنوات اذا كان التهديد بارتكاب جناية أو إسناد أمور خادشة للشرف والاعتبار.

– نص القانون كذلك على بعض الافعال الاخرى وجرمها كالسرقة والاحتيال والاستيلاء على سندات والحصول دون وجه حق على بيانات البطاقات الإلكترونية ونصت المادة 15 على التحريض على الدعارة والمساس بالأديان ، والمادة 16 انتهاك حرمة الحياة الخاصة وذلك بنصها على :"كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر أخبار أو صور تتصل بحرمة الحياة الخاصة أو العقلية للأفراد ، ولو كانت صحيحة عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن خمسين الف درهم ،او بإحدى العقوبتين 28.

– وتطرق كذلك قانون الاتحاد الى تجريم الاتجار بالبشر والمخدرات عبر الانترنت وكذا غسيل الأموال والترويج للأعمال الإرهابية وكذا التجسس على المؤسسات الحكومية ونصت المادة 20 على تجريم انشاء مواقع او نشر معلومات على الشبكة المعلوماتية او احدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شانها الإخلال بالنظام العام ، كما أضيفت تعديلات في قانون الإتحاد نجد منها :

– المرسوم بقانون اتحادي رقم 2 لسنة 2018 بتعديل أحكام المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات [29].

[28]– بعرة سعيدة ، مرجع سابق ، ص 26

[29] – القوانين والقرارات الحكومية المتعلقة بالأنشطة المنفذة على شبكة الانترنت، u.a.e/ar.AE/resouces/Laws ، البوابة الرسمية بتاريخ 2021/05/23 ، 21:27 .

المطلب الثاني : الإطار القانوني المنظم للجريمة المعلوماتية في التشريعات الأجنبية

تصدت للجريمة المعلوماتية مختلف التشريعات الغربية ونستدل على بعض هذه الدول بالمشرع الفرنسي وأغلب الدول الأوروبية السباقة إلى عقد العديد من المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية ومن تلك المعاهدات معاهدة بودابيست لمكافحة جرائم الانترنت[30].

الفرع الأول : القانون المنظم للجريمة المعلوماتية في التشريع الفرنسي

نص القانون رقم 78-17 الصادر بفرنسا المؤرخ في 6 جانفي 1978 الخاص بالمعلوماتية على إنشاء اللجنة الوطنية المعلوماتية و الحريات مهمتها مراقبة حسن تطبيق القانون الذي نص في المادة 14 منه على حماية البيانات الخاصة سواء كانت ملك للدولة أو الأشخاص، ويعتبر هذا القانون أول قانون ينظم الجوانب القانونية المتصلة بالمعلوماتية وأثرها على الخصوصية.

نص قانون العقوبات الفرنسي من خلال تعديلاته بنصوص خاصة بالمعالجة الآلية للبيانات، حيث أصدر قانون رقم 19-88 سنة 1988 ويعد هذا الأخير أول تشريع فرنسي لتجريم بعض جرائم الحاسب الآلي وهو ما عرف بقانون Godfrain [31]، نصت المادة 462 منه على "تجريم القيام بالدخول أو البقاء كلية أو جزئية داخل منظومة لمعالجة المعلومات وعاقبت على ذلك بالحبس لمدة شهرين إلى سنة وغرامة مالية التي تتراوح بين عشرة ألاف فرنك إلى مئة ألف فرنك" .

[30]– جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات، دار البداية للنشر ، ط1 ، عمان، 2007 ، ص 227 .

[31]- القانون رقم 19-18 لسنة1988 المتضمن قانون العقوبات الفرنسي المعدل و المتمم للقانون 78-17 المؤرخ في 06 جانفي 1970

وبصدور القانون الجديد سنة 1994 تم تعديل المادة السابقة بالمادة 323 حيث نصت على تجريم المساس بأنظمة المعالجة الآلية للمعطيات بمختلف أشكال الاعتداء التي ذكرتها المواد 1/323 و 2/323 3/323 "[32].

أدخل المشرع الفرنسي تعديلات مهمة في هذا الإطار على المدونة الجنائية الفرنسية بمقتضى القانون رقم 2012.410 المؤرخ في 27 مارس 2012 والتي قررت حماية جنائية مشددة للمعطيات الشخصية بحيث تمت إضافة فقرات جديدة لمقتضيات المواد 323-2 و323-3 وتم بمقتضاها تقرير عقوبات مشددة تصل إلى 7 سنوات حبسا وغرامة قدرها 75.000 أورو، متى ارتكب فعل الدخول أو البقاء غير القانوني أو فعل العرقلة العمدية أو فعل الغش والاحتيال في مواجهة نظام للمعالجة الآلية للمعطيات الشخصية الذي تسيره أو تنفذه الدولة.

فرنسا قامت بإنشاء عدة وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة هذا الإجرام المستحدث بجميع صوره ومن ذلك المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات، بالإضافة إلى قسم الانترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصاراً بـ (STRTD) ، والقسم الالكتروني التابع لمعهد البحوث الجزائية التابع للدرك الوطني المعروف اختصارا بـ (IRCGN)وكذا وحدات أقسام الاستعلامات والتحقيقات القضائية المعروف اختصارا بـ (BDRIJ)[33].

[32]- بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر ، قانون جنائي ،جامعة محمد خيضر بسكرة ، 2016، ص 18.

[33] - Myriam QUEMENER et joel FERRY, cybercriminalité défi mondial, 2 édition, 2009, p214.

الفرع الثاني : الاتفاقية الأوروبية الخاصة بجرائم تقنية المعلومات بودابست

تحقيقا للتعاون الدولي في مجال مكافحة الجريمة المعلوماتية تم اعتماد الاتفاقية المتعلقة بالجريمة الالكترونية من طرف مجلس الوزراء بالمجلس الأوروبي ببودابست "**The BuDAPEst convention on Cyber crimes** " بتاريخ 8 نوفمبر 2001 ، وقد جاءت هذه الاتفاقية لتوحيد السياسة الواجب إتباعها في مكافحة الجرائم الالكترونية ، ذلك بالتنسيق بين التشريعات الوطنية وتطبيق إجراءات تحقيق وملاحقة تتلاءم مع البيئة الافتراضية فجاءت الاتفاقية بـ 22 مادة من أصل 48 مادة تبين القواعد الإجرائية الخاصة بالبحث و التحري في الجريمة المعلوماتية[34] .

كما نصت الاتفاقية على قواعد الاختصاص القضائي وضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية لإقرار الاختصاص القضائي على الجرائم الواردة في الاتفاقية وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها أو على إحدى الطائرات المسجلة بموجب قوانينها وكذا على كل جريمة مرتكبة من أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي لمكان ارتكابها.

[34] – راجع الاتفاقية الأوروبية الخاصة بجرائم تقنيات المعلومات، صادقت الجزائر على الاتفاقية بموجب المرسوم الرئاسي 14–252 المؤرخ في 8 سبتمبر 2014 ،ج ر العدد 57 المؤرخة في 28 سبتمبر 2014 .

وقد تمت تكملة الاتفاقية ببروتوكول إضافي يتعلق بتجريم الافعال ذات الطابع العنصري والمعادي للأجانب المرتكبة على الأنظمة المعلوماتية والمبرمة في سترسبورغ بتاريخ 2003/09/28 ، كما تم إعداد مشروع بروتوكول يتعلق بتجريم الرسائل الارهابية وفك ترميزها.[35]

وتعتبر الاتفاقية من اهم مصادر التشريع الجزائري لاسيما بالنسبة للمصطلحات التقنية والقواعد الوقائية وهو الامر الذي جعل التشريع الجزائري اكثر انسجاما مع المعايير الدولية.[36]

[35]– امال فكيري، اشكالات الاثبات و الاختصاص في جرائم تكنولوجيا الاعلام و الاتصال العابرة للحدود ، مجلة العلوم القانونية ، عدد17 ، 2018 ، ص 642– 643

[36]–بوخبزة عائشة, الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماجستير ، جامعة وهران، 2013 ، ص 149

الفصل الثاني :

قواعد اختصاص الجريمة المعلوماتية

تمهيد

إضـافة إلى الجوانب الموضوعية التي تحكم الجريمة المعلوماتية هناك جوانب إجرائية في نصوص الجريمة المعلوماتية والتي سنتطرق إليها خلال مبحثين الأول يخص قواعد إجرائية لمتابعة الجريمة المعلوماتية و الثاني الهيئات و الجهات المختصة بمتابعة الجريمة المعلوماتية .

المبحث الأول : قواعد إجرائية لمتابعة الجريمة المعلوماتية

إن الطبيعة الخاصة للجرائم المعلوماتية انعكست على مجال قانون الإجراءات الجزائية فلزم إنشاء قواعد إجرائية حديثة إلـى جـانب القواعد الموضوعية ، كمـا أثار التعامل مع خصوصيـة هذه الجـرائم العديد من المشكـلات التي جعلت القواعد التقليديـة قـاصرة في مواجهتها فاتجه المشرع الجزائري إلى تعديل بعض القواعد والإجراءات المتعلقة بالاختصاص و التحري في هذه الجرائم.

المطلب الأول : إشكاليات المتابعة و التحري في الجريمة المعلوماتية

وضع المشرع الجزائري كغيره من التشريعات بعض القواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الآلي خاصة في مرحلة جمع الاستدلالات، حيث ان اجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة لمعاينة

مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة [37] وذلك بعد مساعدة أجهزة التحقيق للتوصل الى حقيقة الواقعة ومعرفة مرتكبيها.

الفرع الأول : إجراءات التحقيق في الجريمة المعلوماتية

يهدف التحقيق إلى الكشف عن الحقيقة وللوصول لهذا الغرض تقوم الجهات المعنية بعدة إجراءات بعضها يهدف للحصول على الدليل ، كالتفتيش والمعاينة و الخبرة ، أي هي إجراءات لجمع الأدلة المادية والتي تتميز بنوع من الخصوصية في الجرائم المعلوماتية

أولا : التفتيش في مجال الجرائم المعلوماتية

التفتيش هو عبارة عن إجراء من إجراءات التحقيق وقد أحاط القانون التفتيش بضوابط عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة، فلا تفتيش إلا بإذن مكتوب صادر عن الجهات القضائية المختصة،وهي إجراءات تضمن صحة هذا التفتيش الذي أوجب المشرع للقيام به حضور المشتبه به أثناء تفتيش مسكنه ، إلا أنه استثنى هذا الشرط عندما يتعلق الأمر بالجرائم المعلوماتية وكان ذلك لبسط نوع من السرية أثناء جمع الدليل الرقمي و الإسراع لاستخلاصه قبل فقدانه.[38]

غير أنه في الجرائم المعلوماتية يثور تساؤل حول تطبيق القواعد العامة للتفتيش على صور تفتيش نظم الحاسوب، وعندما يكون التفتيش في المكونات المادية للحاسوب هذا لا

37- ابتسام بغو, اجراءات المتابعة الجزائية في الجريمة المعلوماتبة مذكرة تكميلية لنيل شهادة الماستر في القانون تخصص قانون جنائي للأعمال,جامعة العربي بن مهيدي ,سنة 2016 ص 02

38- أمال فكيري، إشكالات الإثبات و الاختصاص في الجرائم المعلوماتية ، مجلة العلوم القانونية والسياسية ، العدد 17 ، جانفي 2018 ، ص 637

يثير إشكالية، أما خضوع المكونات غير المادية للحاسوب للتفتيش هي التي تثير إشكالية ضوابط تفتيش النظم المعلوماتية و القابلية لذلك، وقد أجاز المشرع صراحة التفتيش في المنظومة المعلوماتية من خلال نص المادة 5 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها .

إن إجراء التفتيش في الجريمة المعلوماتية يحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش العادية لأنه في إطار هذه الجرائم يقع التفتيش على مكونات الحاسوب وتفتيش الشبكة المعلوماتية المتصلة به[39].

ومن الاستثناءات أيضا الخروج عن الحدود الزمنية لإجراء التفتيش من 5 صباحا إلى 8 مساءاً فإن المادة 47 فقرة 3 من قانون الإجراءات الجزائية تنص على أنه يجوز لضابط الشرطة القضائية إجراء التفتيش في كل ساعة من ساعات الليل و النهار إذا تعلق الأمر بالتحقيق في جرائم مذكورة على سبيل الحصر ومنها جرائم المتصلة بتكنولوجيا الإعلام و الاتصال .

ونص على تفتيش المنظومة المعلوماتية القانون 09-04 في المادة 5 كما يلي : " يجوز لسلطات القضائية المختصة وكذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول ، بغرض التفتيش،ولو عن بعد إلى:

[39] – ابتسام يغو ، مرجع سابق ، ص 14.

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

ب- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة اذا كانت هناك أسباب تدعو لاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها ، انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة المختصة مسبقا بذلك.

اذا تبين مسبقا بان المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني ، فان الحصول عليها يكون بمساعدة السلطات الاجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".[40]

ثانيا : الخبرة

يجب أن تكون الخبرة في هذا المجال من نوع خاص يتماشى و خصوصية الجريمة الإلكترونية ،و قد تعمل بعض الدول على إعادة تأهيل بعض القراصنة من أجل الاستفادة من خبراتهم في الاختراق.وفي هذا الصدد يجب أن يتحلى الخبير بمؤهلات و مقدرة فنية

[40] القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجريدة الرسمية العدد 47.

عالية ،معرف تركيب الكمبيوتر،معرفة شاملة لشبكة الانترنت، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.

والخبرة هو إجراء يستهدف استخدام قدرات شخص الفنية و العلمية التي لا تتوفر لدى رجال القضاء من أجل الكشف عن دليل لمعرفة الحقيقة بشأن وقوع الجريمة ولهذا فان للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة فان التعامل مع هذه الجريمة يكون من طرف شخص ذو خبرة في مجال الشبكات ومن أهم هؤلاء الخبراء في الجزائر هو المعهد الوطني لعلم الأدلة الجنائية وعلم الإجرام بالجزائر العاصمة، وكذا الفرق المتخصصة من الشرطة عبر 48 ولاية التابعة للمديرية العامة للأمن الوطني [41].

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فإن الخبير المعلوماتي لابد أن تتوفر لديه المقدرة الفنية و الإمكانيات العلمية في المسألة موضوع الخبرة ومساعدة المحقق في إيجاد جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق وتدخل ضمن مهام الخبير معرفة :

- تركيب الحاسب الآلي و طرازه ونوعه ونظام تشغيله و الأنظمة الفرعية التي يستخدمها.
- بيئة الحاسوب أو الشبكة من حيث طبيعتها ، تركيزها أو توزيعها ، نمط ووسائل الاتصال.
- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها .
- الآثار الاقتصادية و المالية المترتبة على التحقيق في الجريمة .

[41] – ابتسام يغو ، مرجع سابق ، ص 21

– كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

– إمكانية نقل الأدلة إلى أوعية دون أخرى والأوعية المادية كالأوراق على أن تكون مطابقة لما هو مسجل على الحاسب الآلي أو النظام أو الشبكة .

أما عن الضوابط التي تحكم الخبرة نجد الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية التي يلتزم بها الخبير (أداء اليمين وخضوعه للرقابة القضائية) ، وكذا القيام بمهامه بنفسه استجابة لطلبات الخصوم وتسليم التقارير خلال المدة المحددة .

أما عن الضوابط الفنية التي تحكم الخبرة في مجال الجرائم المعلوماتية تتمثل في :

– جمع مجموعة من الأدلة الرقمية و تحصيلها من خوادم المواقع ومن جهاز المعتدي .

– تحليل رقمي لمعرفة كيفية إعداد الأدلة الرقمية و نسبتها وتحديد عناصر حركتها ثم التوصل إلى معرفة بروتوكول الانترنت (IP) للحاسوب الذي صدرت منه الرسائل و الهجمات الالكترونية [42].

ثالثا : التسرب

وهو من الإجراءات الشخصية والجريمة المعلوماتية من بين الجرائم التي تسمح بهذا الإجراء ، وقد حدد المشرع الجزائري نطاق هذا الإجراء في جرائم مذكورة على سبيل الحصر منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ونظمه في القسم الخامس من قانون الإجراءات الجزائية بموجب المادة 65 مكرر12 على أنه : " قيام ضابط الشرطة القضائية

[42] – خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، ط1، دار الفكر الجامعي ، الاسكندرية ،2009، ص 280–300

أو عون تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، بمراقبة أشخاص مشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك " [43] .

ومن أجل أن تتم عملية التسرب وتسهيل المتابعة الجريمة المعلوماتية و المجرمين ومهام المتسرب فقد أحاط المشرع هذا الإجراء بمجموعة من الشروط الشكلية والموضوعية .

أ- الشروط الشكلية :

أن يكون صادر بإذن قضائي إما وكيل الجمهورية أو قاضي التحقيق المختص ، ويكون مكتوب و إلا وقع تحت طائلة البطلان مع ذكر اسم الضابط الذي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة القضائية باعتباره مساعدا له ، و المدة المطلوبة لعملية التسرب 4 أشهر محددة قانونا قابلة لتجديد.

ب- الشروط الموضوعية :

تسبيب الإذن بالتسرب خاصة إذا ثبت أن الاعتداء على الوسائط الفعلية العادية غير كاف للتوصل إلى الحقيقة ومن تم لابد من وكيل الجمهورية أو قاضي التحقيق أن يقدم تبريرا أو الأساس الذي تم الاعتماد عليه من أجل السماح بالقيام بعملية التسرب .

يمكن تصور عملية التسرب في الجريمة المعلوماتية أو ما يسمى بالتسرب الرقمي في دخول ضابط الشرطة القضائية إلى العالم الافتراضي (شبكة الانترنت) واشتراكه في اتصال

[43] – القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المتضمن تعديل قانون الإجراءات الجزائية الجزائري 66-155 المؤرخ في 8يونيو 1966 .

مباشر لرفع ومعاينة الجرائم أو ربط الاتصال مع المشتبه فيهم والظهور كأنه فاعلا مثله وذلك باستخدام اسم مستعارا ووهميا سعيا منه لتعرف عليهم و تحديد أماكنهم[44].

الفرع الثاني : إجراءات خاصة في التحقيق المعلوماتي

إن السرعة في ارتكاب الجريمة المعلوماتية وسهولة محو آثارها من طرف الجاني جعلها من أصعب الجرائم للاكتشاف ولهذا استحدثت التشريعات الحديثة منها المشرع الجزائري إجراءات خاصة من أجل ضبطها وتسهيل اكتشافها وتقسم هذه الإجراءات إلى :

- مراقبة الاتصالات الالكترونية
- حفظ المعطيات المتعلقة بحركة السير

أولا: مراقبة الاتصالات الالكترونية

تعتبر المراقبة من أهم مصادر التحري التي يستعان بها في البحث سواء في الجرائم التقليدية أو المستحدثة كجرائم الانترنت وقد نص المشرع الجزائري في المواد 65 مكرر إلى 65 مكرر10 من قانون الإجراءات الجزائية وهي اعتراض المراسلات وتسجيل الأصوات و التقاط الصور إذا اقتضت ضرورة التحقيق ذلك بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد، وهي إجراءات تحري خاصة لما فيها من مساس بحرمة الحياة الخاصة للأشخاص[45].

[44] – ابتسام يغو ، مرجع سابق ، ص 33

[45] - المرجع نفسه ،ص 34

كما بين القانون 04/09 في مادته الرابعة الحالات التي تسمح بتطبيق الإجراءات الجديدة المتمثل في مراقبة الاتصالات الالكترونية وذلك على سبيل الحصر :

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

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

ج- لمقتضيات التحريات و التحقيقـــات القضائية عندمـــا يكـــون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة [46].

والضوابط التي تحكم هذا الإجراء بالنسبة للجرائم المذكورة في الفقرة " أ" أن النائب العام لدى مجلس قضاء العاصمة هو المختص بمنح الإذن لضابط الشرطة القضائية المنتمين للهيئة المذكورة في المادة 13 من هذا القانون إذنا مدته 6 أشهر قابلة لتجديد.

ثانيا : حفظ المعطيات المتعلقة بحركة السير

قررت التشريعات الحديثة ومنها المشرع الجزائري إلزام مقدمي الخدمات حفظ المعطيات المتعلقة بحركة السير لضمان الوصول إلى آثار الجريمة مهما كانت، ويقصد بالمعطيات المتعلقة بحركة السير هي تلك المتعلقة بالاتصال عن طريق منظومة معلوماتية باعتبارها جزء من حلقة الاتصال توضح مصدر الاتصال و الوجهة المرسل إليها .

[46] - القانون 04/09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الجريدة الرسمية ، العدد 47 .

وقد حدد المشـرع الجزائري المعطيـات الواجب حفظهـا من طرف مقدمـي الخدمات في مايلي:

- المعطيات التي تسمح بالتعرف على مستخدمي الخدمة .

- المعطيات التي تسمح بالتعرف على المرسل و المرسل إليهم وكذا عناوين المواقع .

- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال وتكون مدة الحفظ لا تتجاوز سنة واحدة ، وإلا تعرض مقدمي الخدمة للعقوبات المقررة في المادة 11من القانون 04/09 [47].

المطلب الثاني : إشكاليات الاختصاص في الجريمة المعلوماتية

كما هو معلوم ، فإن شبكة الانترنت لا تستأثر بها دولة بعينها ، ويتسنى استخدامهـا من أية بقعة في العالم تقريباً من خلال جهاز حاسوب يكون متصلاً بها . فهي بطبيعتها لا تحدّها حدود ، و تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة ، وهذا يستتبع عدم إمكان خضوعها لسلطان قانون جنائي معين .

وعملاً بمبدأ الإقليمية ، فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها ، بصرف النظر عن جنسية مرتكب الجريمة ، الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة ، والذي يستتبع بالضرورة تنازع الاختصاص ، وبالذات فيما يتصل بالجرائم التي ترتكب عبر شبكة الإنترنت . فجريمة السبّ مثلاً عبر الرسائل الإلكترونية تقع أحياناً في بلد ويتلقّاها الضحية في بلد آخر، ناهيك أن بعض الأفعال التي تُبث من خلال الإنترنت تعد أحياناً جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة.

[47] – ابتسام يغو ، مرجع سابق ، ص 39

ومما يزيد من حدة المشكلة غياب قانون محدد يجري إعماله على مثل هذه الأفعال ، ما من شأنه أن يبعث على التساؤل عن القانون الواجب التطبيق على المواقع الإلكترونية على شبكة الإنترنت وتطبيقاً للقواعد التي تحكم الاختصاص المكاني ، فإن جرائم الإنترنت العابرة للحدود Transnational Crimes تخضع في كثير من الأحيان لأكثر من قانون .

الفرع الأول : القانون الواجب التطبيق على الجرائم المعلوماتية

لقد طرحت هذه المشاكل القانونية على القضاء المقارن، حيث نجد أن الو م أ ،اعتبرت أن القانون الواجب هو القانون الأمريكي إذا تحققت آثار الجريمة في الولايات المتحدة، كما أنه يكفي لامتداد ولاية القضاء الأمريكي إلى جريمة وقعت في الخارج، إذا كانت آثارها مست مصالح أمريكية أو عرضتها للخطر.

كما تبنى القضاء الانجليزي هذا الطرح من خلال الدعاوى الناشئة عن إساءة استخدام الانترنت عملا بقانون إساءة الكمبيوتر في بريطانيا الصادر سنة 1990، ولكي يختص القضاء الانجليزي بنظر في الواقعة يجب أن تمتد آثارها إلى بريطانيا بصرف النظر عن مكان إقامة الجاني طالما أن نيته انصرفت إلى تعديل محظور في الحاسوب موجود في بريطانيا . أما في فرنسا فيمتد اختصاص القضاء هناك إلى جرائم الانترنت التي وقعت بالخارج عملا بقانون العقوبات مهما كانت الظروف الواقعة التي تبرر مصلحة فرنسا في إعمال قانونها عليه .

كما أكدت المنظمة الدولية للشرطة الجنائية الإنتربول على تعزيز وتشجيع التعاون بين أجهزة الشرطة بين الدول الأعضاء لمكافحة الجريمة خاصة جرائم الانترنيت[48].

وأهم الجهود الدولية في هذا المجال، جهود الاتحاد الأوروبي الذي قام بإنشاء قوة خاصة للجرائم المعلوماتية في دول الاتحاد ، كما أن عملها يمتد إلى كل من كندا و استراليا وألمانيا وفرنسا والولايات المتحدة الأمريكية والمملكة البريطانية.

أما في إفريقيا فلقد اجتمع مجموعة من قادة الاتحاد الإفريقي مكون من 54 حكومة افريقية ووافقوا على اتفاقية الاتحاد الإفريقي فيما يتعلق بمجال الأمن المعلوماتي وحملة البيانات الشخصية، كما وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهم بالقاهرة في 2010 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ويتطرق في الفصل السابع منها للتعاون القانوني والقضائي في مجال مكافحة هذه الجرائم.

كل هذه الوسائل القانونية والقضائية لمكافحة الجريمة المعلوماتية قد أقرتها الجزائر سواء في القانون 15/04 المعدل والمتمم لقانون العقوبات أو القانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث أقر المشرع الجزائري موضوع التعاون والمساعدة القضائية في مجال مكافحة الجريمة المعلوماتية وذلك في الفصل السابع من هذا القانون.

[48] – نمدلي رحمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال مؤتمر الجرائم الالكترونية المنعقد في طرابلس، لبنان، يومي 24-2017/03/25، ص105 ،

كما أقر القانون الجزائري الحماية القانونية لنظم المعلومات في قوانين خاصة منها قانون التأمينات الاجتماعية 01/08 المؤرخ في 2008/01/23، وقانون الملكية الأدبية والفكرية 05/03 المؤرخ في 2003/07/23 والقانون 03/15 المتعلق بعصرنة العدالة ،والقانون المتعلق بالمواصلات السلكية واللاسلكية 03/2000.

الفرع الثاني : تنازع الاختصاص في الجرائم المعلوماتية

إن الجهات القضائية من خلال الصلاحيات التي أقرها لها المشرع في متابعة الجرائم بصفة عامة و الجريمة المعلوماتية بصفة خاصة تمارس هذه المهام مقيدة في ذلك بنطاق إقليمي محدد يسمى الاختصاص المحلي وبنوع معين من الجرائم وهو الاختصاص النوعي .

أولا : قواعد الاختصاص المحلي

عالج المشرع الجزائري الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه ،وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية ، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه ، لكن لما كانت الجريمة المعلوماتية عابرة للإقليم ، فإن المشرع الجزائري أولى بعض الخصوصية في تحديد الاختصاص المحلي وأجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة المعلوماتية بموجب القانون 22/06 المؤرخ في : 20 ديسمبر 2006 المعدل و المتمم للأمر 155/66 في 08 يونيو 1966 و المتضمن قانون الإجراءات الجزائية [49].

[49] لعقال فريال ، مكافحة الجريمة المعلوماتية في ظل التشريع الجزائري، مرجع سابق ، ص 60.

لما كانت الجريمة المعلوماتية تتعدى مكان الاختصاص أجاز المشرع الجزائري تمديد الاختصاص المحلي لوكيل الجمهورية بموجب المادة 37 فقرة 2 من قانون الإجراءات الجزائية إلى دائرة اختصاص محاكم أخرى ، والاختصاص المحلي للنيابة العامة الذي يتحدد وفقا للمادة 37 قانون الإجراءات الجزائية بمكان وقوع الجريمة ومحل إقامة احد الأشخاص المشتبه في مساهمتهم في الجريمة او المكان الذي تم في دائرته القبض على هؤلاء الاشخاص حتى ولو تم القبض لسبب اخر[50]

كما أجاز تمديد اختصاص قاضي التحقيق بموجب المادة 2/40 التي تجيز لقاضي التحقيق تمديد الاختصاص إلى دائرة محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [51].

وكذلك يمتد الاختصاص المحلي لمحاكم الجنح في حالة الجرائم الماسة بأنظمة معالجة المعطيات ، كما قرر في المادة 40 مكرر2 أيضا تطبيق القواعد المتعلقة بالدعوى العمومية و التحقيق والمحاكمة أمام الجهات القضائية التي توسع اختصاصها المحلي طبقا للمواد 37 –40 من قانون الإجراءات الجزائية و الحقيقة أن مشكلة الاختصاص القضائي في الجريمة المعلوماتية تعد من المشكلات التي تعرقل الحصول على الدليل ذلك أن هذه الجريمة قد ترتكب في مكان معين وينتج آثارها في مكان آخر داخل الدولة أو خارجها .

[50] – لعقال فريال ، مرجع سابق، ص 61.

[51] – المرجع نفسه، ص 62.

ثانيا : قواعد الاختصاص النوعي

يتحدد الاختصاص النوعي للمحكمة للفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي ينظر فيها حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة أفعال إرهابية أو تخريبية المحالة اليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية كما تختص المحاكم بالنظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 328 من قانون الإجراءات الجزائية .

ولأن الطبيعة التقنية المعقدة للجرائم المعلوماتية تفرض على رجال القضاء تكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع بإجراءات خاصة إذ جعل الاختصاص ينعقد بدائرة اختصاص محاكم أخرى وهذا ما نصت عليه المواد37، 40 والمادة 329 من قانون الإجراءات الجزائية ، والتعديل الذي جاء به القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 الذي حددت أحكامه في المرسوم التنفيذي رقم 348/06 المتعلق بالتنظيم القضائي الذي نص على الاقطاب الجزائية المتخصصة ذات اختصاص إقليمي موسع لدى المحاكم بكل من الجزائر العاصمة ، قسنطينة، وهران ، ورقلة[52]

[52] – بعرة سعيدة ، مرجع سابق ، ص 94.

المبحث الثاني : الجهات و الهيئات المختصة بمتابعة الجريمة المعلوماتية

التخصص في مجال القضاء له أهمية كبيرة ودور فعال في رفع مستوى العمل القضائي ولنظام التخصص جانبين هما تخصص القضاء وتخصيص الجهات القضائية وهو من التوجهات الحديثة البارزة للتنظيم القضائي الجزائري ، وهو الأمر الذي استحدثه المشرع الجزائري بما يسمى الأقطاب الجزائية المتخصصة ، إضافة إلى إنشاء هيئة إدارية لها دور مساعد لهذه الجهات القضائية في متابعة الجريمة المعلوماتية ودور وقائي يسبق وقوع الجريمة وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

المطلب الأول : اختصاص الاقطاب الجزائية المتخصصة في الجريمة المعلوماتية

إنّ البداية الحقيقية لظهور الأقطاب القضائية المتخصصة، كانت في صورة اختصاص إقليمي موسع في المادة الجزائية، ظهرت رسميا في سنة 2004، مع صدور القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، عندما تناول في المواد 37 ، 40 و 329 إمكانية تمديد الاختصاص الإقليمي لكل من وكيل الجمهورية، قاضي التحقيق والمحكمة عندما يتعلق الأمر بالبحث والتحرّي في جرائم معينة على سبيل الحصر، وهذا يخص بعض المحاكم تتحدد عن طريق التنظيم[53] .

[53] - القانون رقم 04-14 المؤرخ في 2004/11/10 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966 .

الفرع الأول: سير وتنظيم الأقطاب الجزائية المتخصصة

أصبحت الأقطاب الجزائية المتخصصة أمرا مهما لابد منه وهذا ما جعل المشرع الجزائري يهتم بالجانب البشري في تكوين وهيكلة هذه الأقطاب الجزائية .

أ- الجانب البشري : ويعني هذا إبراز دور العنصر البشري الذي يتكون منه القطب وبالتالي الحديث يكون عن قضاة الحكم و قضاة التحقيق وأمناء الضبط [54]

وباعتبار أن الأقطاب الجزائية هي أقطاب أو أجهزة تنتمي إلى القضاء الجزائي فهو يتكون من :

- وكيل الجمهورية .
- وكيل جمهورية مساعد .
- قاضيان للتحقيق على الأقل يشرفان على غرفة التحقيق .
- قاضي حكم يشرف على قسم تابع للقضاء الجزائي المتخصص .
- أمناء ضبط مكلفون بأعمال تنظيم الملفات و مساعدة القضاة .[55]

ب – الجانب التقني : ويقصد به خضوع القضـــاة و الأمناء العاملين في القطب الجزائي إلى تأهيل خـــاص بهم من أجل التخصص و التعمق أكثر في مجـــال البحث و التحقيق في الجرائم و القضايا المعروضة عليها خاصة و أنها جرائم محدد على سبيل الحصر نظرا لخطورتها ولذلك فهي تتطلب تكوين خاص .

[54] – انظر المادة 25 – 26 من رأي المجلس رقم 01 المؤرخ في 10 جمادى الأولى 1426 الموافق لـ17 يونيو 2005 المتعلق بمراقبة القانون العضوي المتعلق بالتنظيم القضائي ، الجريدة الرسمية ، العدد 51 .

[55] – محمد أمقرن ، التنظيم القضائي الجزائري ، دار هومة للنشر و التوزيع ، الجزائر ،2009 ، ص 25 .

فمنذ إنشـاء و تأسيس هذه الأقطاب و النص عليها في القانون الجزائري فهي تعـاني من عدم وجود تخصص فعلي في القضاة لا وجود لقضاة متخصصين في هذا المجال . لذلك نجد أن الدولة تسعى دائما إلى جعل القضاة متخصصين من خلال الدورات التكوينية في إطار سياسة التكوين المستمر للقضاة في مجال الأقطاب الجزائية المتخصصة .[56]

وبالنظر إلى أن هذه الأقطاب ذات اختصاص إقليمي ونوعي موسع في هذه الجرائم بما فيها الجريمة المعلوماتية، تم صدور المرسوم التنفيذي رقم 06- 348 الذي بموجبه تم تنصيب 4 أقطاب جزائية متخصصة سنة 2008 وتحديد المحاكم التابعة لها كما يلي :

- القطب الجزائي سيدي محمد بالجزائر العاصمة بتاريخ 26 فيفري 2008 ويمتد اختصاصه الإقليمي إلى المجالس القضائية التالية : الجزائر ، الشلف ، الأغواط ، البليدة البويرة ، تيزي وزو، الجلفة، المدية ، المسيلة ، بومرداس .
- قطب جزائي بقسنطينة المنصب بتـاريخ 2008/03/03 ويمتد اختصـاصه الإقليمـي إلى المجالس القضائية التالية : قسنطينة ، أم البواقي ، بسكرة ، تبسة ، جيجل ، سطيف سكيكدة ، عنابة ، قالمة ، برج بوعريريج .
- قطب جزائي بوهران بتاريخ 2008/03/05 ويمتد اختصاصه الإقليمي إلى المجالس القضائية التالية : وهران ، بشار ، تلمسان ، سعيدة ، سيدي بلعباس ، مستغانم ، معسكر غليزان .
- القطب الجزائي المتخصص بورقلة بتـاريخ 2008/03/19 ويمتد اختصاصه الإقليمي إلى المجالس القضائية التالية : ورقلة ، أدرار ، تمنراست ، إليزي ، غرداية.[57]

[56] – كور طارق ، آليات مكافحة جريمة الصرف ، دار هومة للنشر و التوزيع ، الجزائر ، 2014 ، ص 155 .

[57]– المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 المتعلق بتمديد الاختصاص المحلي لبعض المحاكم أو وكلاء الجمهورية وقضاة التحقيق ، الجريدة الرسمية العدد 63 .

ويتضح مما سبق أن الاختصاص الإقليمي الموسع للقطب الجزائي المتخصص يشمل جميع مراحل الدعوى العمومية ابتداء من جمع الاستدلالات إلى المحاكمة .

وحـــدد الاختصـــاص النوعـــي لهذه الأقطـــاب بمقتضى القـــانون 04- 14 المؤرخ في 2004/11/10 المتضمن تعديل قانون الإجراءات الجزائية و المادة 01 من المرسوم التنفيذي رقم 06-348 المتعلق بتحديد وتعيين المحاكم ذات الاختصاص النوعي في جرائم محددة وهي جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية ، جرائم تبيض الأموال ، جرائم الإرهاب ، جريمة مخالفة التشريع و التنظيم الخاصين الصرف وحركة رؤوس الأموال من وإلى الخارج ، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .[58]

الفرع الثاني: طرق اتصال القطب الجزائي المتخصص بالجريمة المعلوماتية

إن المحاكم الجزائية ذات الاختصاص المحلي الموسع أو الأقطاب الجزائية تخضع لمقتضيات ولقواعد متميزة ، وبالتالي إجراءات مختلفة عن تلك المتعلقة بالجهات القضائية الكلاسيكية ، وهذا يتطلب توافـــر هذه الجهـــات القضـــائية المتخصصـــة على نوع جديد من القواعد والاتصال بالقضايا متى اتضحت معالم الجريمة من حيث التكييف القانوني للوقائع والطابع المميز للجريمة ولذلك لابد من اللجوء الى الجهات القضائية المتخصصة .

وتفادي إحالة الملفات البسيطة والعادية على الجهات القضائية المتخصصة ، وهو الشيء الذي يتميز به فهي تنظر فقط في الجـرائم الخطيرة ،ومن خـــلال ذلك لابد أولا من التطرق إلى كيفية إخطار واتصال القطب الجزائي .

[58] – ابتسام يغو ، مرجع سابق ، ص 74- 75 .

بعدما تصل القضية الى أروقة المحكمة فهي تسلك أحد الطرفين إما التمسك بها وإما يتم التخلي عنها ، إذ أن النيابة العامة لها من يمكن لها التصرف في ملف الدعوى بالحفظ، إذ يصبح وحده صاحب الحق في الحكم وليس للنيابة العامة الحق في إعطاء طلبات شفوية أو الكتابة حيث أن النيابة العامة لا يجوز لها التخلي عن حق المطالبة الذي خوله القانون لها وفقا لقانون الاجراءات الجزائية خاصة المادة 37 منه كما انه على وكيل الجمهورية ابلاغ النائب العام لدى المجلس القضائي التابعة له القطب الجزائي المتخصص بنسخة من اجراء التحقيق.

وهو أمر ضروري حتى يتمكن النائب العام لدى القضائي التابع له القطب الجزائي من تفعيل اجراء المطالبة بالملف فكما قلنا سابقا اذا كان وكيل الجمهورية يتبع النائب العام التابع للمجلس القضائي التابع له القطب الجزائي الذي يمارس فيه النائب العام صلاحيته.

غير أن الإشكال الذي يطرح في هذا الصدد في حالة ارتكـــاب أو وقوع جريمة تقع في محكمة تابعة لمجلس قضائي آخر وتدخل ضمن الاختصاص الموسع للقطب الجزائي فيكون الإبلاغ من طرف النائب العام التابع له القطب الجزائي المتخصص من طرف النائب العـــام لدى المجلس القضائي الذي وقعت الجريمة في دائرة اختصاصه وبالتالي على وكيل الجمهورية التخلي عن القضية لصالح النائب العام لدى القطب الجزائي المتخصص عن طريق إبلاغه للنائب العام بالمجلس الذي بدوره يجب عليه إبلاغ القطب .[59]

[59] – ابتسام يغو ، مرجع سابق ، ص 78– 79

المطلب الثاني : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

جاءت هذه الهيئة بموجب التعديلات الأخيرة تنظم في مجلس توجيه ومديرية عامة تابعة لوزارة الدفاع الوطني بعدما كانت تسييرها سلطة إدارية لدى وزارة العدل.

الفرع الأول : اختصاص الهيئة الوطنية

أنشئت بموجب المادة 13 من القانون رقم 04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية، في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[60].

وحدد المرسوم الرئاسي رقم 19- 173 المؤرخ في 6 يونيو 2019 ، الصادر في العدد الأخير من الجريدة الرسمية تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها و كيفيات سيرها. ويلغي هذا المرسوم التشكيلة السابقة للهيئة التي صدرت في الجريدة الرسمية رقم 15- 261 في 8 أكتوبر 2015.

وبموجب هذا المرسوم توضع الهيئة التي هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، تحت سلطة وزارة الدفاع الوطني كما حدد مقرها

[60] – :القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

بمدينة الجزائر مع إمكانية نقله إلى مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني ، وتضم الهيئة إلى جانب المديرية العامة، مجلس توجيه يرأسه وزير الدفاع الوطني أو ممثله ويتشكل من ممثلي الوزارات التالية :

- وزارة الدفاع الوطني .
- وزارة الداخلية.
- وزارة العدل.
- الوزارة المكلفة بالمواصلات السلكية واللاسلكية .

يكلف بالتداول حول الإستراتيجية الوطنية للوقاية من الجرائم المحددة في المرسوم وكذا التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية ، كما يقوم مجلس التوجيه دوريا بتقييم حالة التهديد في مجال هذه الجرائم للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، إعداد نظامه الداخلي والمصادقة عليه إضافة إلى دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه[61].

الفرع الثاني : مهام الهيئة

يجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه ويمكنه أن يجتمع فـــي دورة غير عادية كلما كان ضروريا بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أومن المدير العام للهيئة.

[61] –المرسوم الرئاسي رقم 19– 173 المؤرخ في 6 يونيو 2019 يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، جريدة رسمية العدد الأخير.

أما المديرية العامة للهيئة فتتولى السهر على حسن سيرها و إعداد مشروع ميزانيتها وإعداد وتنفيذ برنامج عملها كما تعمل على تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.

وتضم المديرية العامة مديرية تقنية تتكفل على وجه الخصوص بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة إضافة إلى مساعدة السلطات القضائية ومصالح الشرطة بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتلك التي تتطلب اللجوء إلى أساليب التحري للهيئة[62]

و تنص المادة 14 من القانون 09-04 على مهام هذه الهيئة كما يلي : " تتولى الهيئة المذكورة في المادة 13 أعلاه ، خصوصا المهام الآتية:

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

ب– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية .

[62]– مقال وكالة الأنباء الجزائرية ، 26 جوان 2019 ، تاريخ التصفح 25 ماي 2021 ، 20:50.

ج – تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وتحديد مكان تواجدهم".[63]

ويتضح مما سبق أن إرادة المشرع الجزائري في إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتمكينها بالنظر للمهام المسندة لها أن تكون واحدة من أهم الأجهزة المتخصصة والمتعاونة مع باقي اجهزة العدالة الجنائية الوطنية والدولية لمكافحة الجريمة المعلوماتية ،وذلك بعد أن تأكد لها بان خطر الاجرام المعلوماتي لا تكفي جهود مختلف الجهات الوطنية لمكافحته وضرورة عمل هذا الجهاز المستحدث بالتنسيق مع غيره من الأجهزة المتخصصة في ذات المجال .[64]

[63] – القانون 09-04، المؤرخ في 5 أوت 2009 ،الجريدة الرسمية ،العدد 47.

[64] بوخبزة عائشة مرجع سابق, ص255

خاتمة

خاتمـة

إن تنامي ظاهرة الجرائم المعلوماتية ، وتخطي آثارها حدود الدول ، أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموساً ، كما هو الحال في الجرائم التقليدية .

فضلاً عما يثيره ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض الإجراءات كالمعاينة والخبرة والتفتيش في نطاق البيئة الافتراضية . يضاف إلى هذا وذاك مشكلة تنازع الاختصاص بصدد هذه الجرائم باعتبار أن آثارها تتجاوز حدود الاختصاص الإقليمي ، الأمر الذي يجعل القواعد التقليدية غير مجدية في بعض الأحيان ، وتظل مشوبة بالقصور .

ورغم الجهود التي بُذِلت ولا تزال تُبذل ، فإن هذه التحديات تبقى منقوصة في كثير من الأحيان في غياب استراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها.

– تعتبر الجريمة الالكترونية من الجرائم المستحدثة لذلك فإن المعالجة القانونية يجب أن تتم في إطار شمولي ذلك أن اعتماد المحاور الرئيسية للحماية الجزائية فيما بينها لا يخلو من التكاملية حيث أن خصوصية التجريم يلزمها خصوصية في الاثبات وكذلك خصوصية في الملاحقة.

– أما خصوصية التجريم فهي نابعة من وقوع غالبية هذه الجرائم على العالم الافتراضي دون المادي، وذلك حتى مع ملامسة بعضها للعالم المادي، فإنها تبقى من الخصوصية بما يجعلها متمايزة عن غيرها من الجرائم .

– ومن ناحية خصوصية الإثبات في هذا النوع من الجرائم فإنها لا تخلو من الصعاب الجمة والتي تكتنف رصد واحتواء الدليل المتحصل من مسرح الجريمة سواء المادي أو الافتراضي .

وبناءً على ما تقدم ، فإننا نتبنى بعض التوصيات التي نراها قد تساهم في حل بعض الإشكاليات التي ألمحنا إليها في ثنايا هذه الدراسة، ومنها :

1 . دعوة المشرع الجزائري إلى المبادرة بسن تشريع يجرّم إساءة استخدام الإنترنت أسوة بالدول التي سبقتنا في هذا المجال .

2 . إعادة النظر في القوالب الإجرائية الحالية بما يتماشى مع طبيعة الجرائم المعلوماتية .

3 . حث الدول العربية على إبرام اتفاقية فيما بينها على غرار الاتفاقية الأوروبية بغية تعزيز التعاون القضائي والأمني بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم المعلوماتية عبر الوطنية .

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

5– العمل على استحداث ضبطية قضائية وكذلك نيابة متخصصة في مجال الجرائم المعلوماتية مقارنة بالدول المتقدمة .

ونختم دراستنا للموضوع بكلمة وزير الاتصال التي ألقاها بمناسبة اليوم البرلماني حول الجريمة المعلوماتية وتداعياتها على الوطن والمواطن" بالنادي الوطني للجيش أن "الجريمة الالكترونية بالنظر إلى أضرارها الجسيمة تتطلب منا جميعا تكثيف الجهود في إطار رؤية مندمجة تقوم على التكامل والتنسيق بين مختلف الفاعلين على غرار مؤسسات التربية، وسائل الإعلام والحركة الجمعوية وذلك إسهاما في المحافظة على أمن وطننا وسلامة مواطنينا ".

والحديث كان عن ارتفاع معدل الجريمة المعلوماتية في السنة الاخيرة بنسبة 22.63 بالمائة مقارنة بسنة 2019 ما يتطلب " تنظيم و تأطير مجال الرقمنة واعتماد برامج توعوية للتحسيس بمخاطر الجريمة المعلوماتية .".

إن العالم أدرك خطورة هذه الجريمة التي أصبحت "واقعا مخيفا" لما يفرضه التطور التكنولوجي والرقمي المذهل، بل هو من النتائج المؤسفة لانحراف الإنسان وسوء استعماله للعلوم والاختراعات و أن هذا النوع من الجرائم " أخطر من الحروب التقليدية التي تكون فيها ملامح العــدو مكشوفة لأن الخصم في هذه الحالة يستخدم برمجيات فتاكة يتعدى بهــا على خصوصيات الناس ويشوه صورهم ويسبب أضرارا لمركزهم الاجتماعي ومسارهم المهني".

وفي ذات السياق تبرز أهمية أدوات تأمين مواقع "الويب" التي تتعدد بتعدد أساليب الجريمة المعلوماتية ومن أبرزها شهادة "SSL " أو شهادة المفتاح العمومي التي تعتبر بطاقة

هوية رقمية للتحقق من هوية الأشخاص أو المنظمة أو الموقع وكذا بتشفير المعلومات والمبادلات التي يحتويها جهاز الخاتم.

ولكن رغم أهمية هذه الشهادة ، إلا أن 85 % من المواقع الجزائرية المشمولة بالدراسة المذكورة لا تتوفر على هذه الشهادة بحيث أن النقص المسجل في مواكبة سرعة تطور العالم الافتراضي شجع الشبكة التي تعمل خارج إطار القانون والأخلاق على ابتزاز المستهلكين وقرصنة معلوماتهم لاسيما خلال فترة الحجر الصحي.

قائمة المصادر و المراجع

Les références

قائمة المصادر و المراجع

أولا: القوانين و المراسيم

- المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، ج ر عدد 53 المحدد لتشكيلة و تنظيم الهيئة الوطنية للوقاية ممن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- المرسوم الرئاسي رقم 19- 173 المؤرخ في 6 يونيو 2019 يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، جريدة رسمية العدد الأخير.

- القانون 04/09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال الجريدة الرسمية ، العدد 47 .

- القانون رقم 04 -15المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ، الجريدة الرسمية رقم 44 .

- القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المتضمن تعديل قانون الإجراءات الجزائية الجزائري 66-155المؤرخ في 8 يونيو 1966.

- القانون رقم 19-18 لسنة1988 المتضمن قانون العقوبات الفرنسي المعدل و المتمم للقانون 78-17 المؤرخ في 06 جانفي 1970

ثانيا:الكتب القانونية

- جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات، دار البداية للنشر،عمان ، ط1 ، 2007.

- خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، ط1، دار الفكر الجامعي ، الاسكندرية ،2009.

- غنية باطلي ، الجريمة الالكترونية (دراسة مقارنة) ، منشورات دار الجزائرية ، الجزائر 2015.

- محمد أمقرن ، التنظيم القضائي الجزائري ، دار هومة للنشر و التوزيع ، الجزائر ،2009 .

- كور طارق ، آليات مكافحة جريمة الصرف ، دار هومة للنشر و التوزيع ، الجزائر ، 2014 .

ثالثا : المذكرات

- ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتبة مذكرة تكميلية لنيل شهادة الماستر في القانون تخصص قانون جنائي للأعمال،جامعة العربي بن مهيدي ، سنة 2016.

- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماجستير ، جامعة وهران، 2013 .

– سوير سفيان،الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010 .

– لعقال فريال الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر ، قانون جنائي ، جامعة اكلي محند اولحاج، البويرة ،2015 .

رابعا: المقالات والمداخلات و المجلات

– أمال فكيري، إشكالات الإثبات و الاختصاص في جرائم تكنولوجيا الإعلام و الاتصال العابرة للحدود ، مجلة العلوم القانونية ، عدد17 ، 2018 .

– رضا فولي عثمان، المشكلات العلمية و القانونية للجريمة المعلوماتية في العصر الرقمي، http://www.al-fadjr.com/ar/realite/352178.html ، 20 نوفمبر 2020 ، 11:25 .

– زعيطي أمينة، مكافحة الجرائم الالكترنية في ضوء ق ع ج دراسة مقارنة، مجلة حقوق الإنسان و الحريات ، جامعة مستغانم، العدد 7 ، 2019.

– علال فالي، خصوصية الجريمة المعلوماتية" مقال بمجلة القضاء التجاري الثاني السنة 2013.

– فضيلة عاقلي ،الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري ، أ/محاضرة "أ" جامعة باتنة-1- الجزائر. كتاب أعمـال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017.

– معاشي سميرة ، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية) ،جامعة محمد خيضر ، بسكرة ،2018 ،مجلة المفكر ، العدد17 .

– مصطفى الفوركي ، الجرائم الماسة بالنظم المعلوماتية في القانون المغربي،مجلة البحوث القانونية و الاقتصادية ، جامعة الحسن الأول، المغرب، العدد 1،2020.

– مسامح زكرياء ، خصوصيات الجريمة الالكترونية على ضوء التشريع و القضاء المغربي، المغرب، 21 يوليو 2020.

– نمدلي رحيمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال مؤتمر الجرائم الالكترونية المنعقد في طرابلس، لبنان، يومي 24–2017/03/25

– يونس عرب، تطور التشريعات في مجال مكافحة الجرائم، الالكترونية، هيئة تنظيم الاتصالات، سلطنة عمان، مسقط، 2 و4 أفريل 2006 .

– مقال وكالة الأنباء الجزائرية ، 26 جوان 2019 ، تاريخ التصفح 25 ماي 2021 ، 20:50.

– القوانين والقرارات الحكومية المتعلقة بالأنشطة المنفذة على شبكة الانترنت، u.a.e/ar.AE/resouces/Laws ، البوابة الرسمية بتاريخ 2021/05/23 ، 21:27 .

المراجع الأجنبية :

- Myriam QUEMENER et joel FERRY ، cybercriminalité défi mondial، 2 édition، 2009، p214.

- la loi 88-19 de 05 Janvier 1988 portant sur la fraude informatique.journal officiel du 06 janvier 1988 France.

الفهرس

الفهرس:

العنوان	رقم الصفحة
مقدمة	أ
الفصل الأول: الأحكام العامة للجريمة المعلوماتية	
تمهيد	9
المبحث الأول : مفهوم الجريمة المعلوماتية	9
المطلب الأول : تعريف الجريمة المعلوماتية	10
الفرع الأول : التعريفات الفقهية للجريمة المعلوماتية	10
الفرع الثاني : تعريف المشرع الجزائري للجريمة المعلوماتية	12
المطلب الثاني : خصائص وتقسيمات الجريمة المعلوماتية	13
الفرع الأول : خصائص الجرائم المعلوماتية	13
الفرع الثاني : تقسيمات الجريمة المعلوماتية	16
المبحث الثاني : الإطار القانوني المنظم للجريمة المعلوماتية	22
المطلب الأول : الاطار القانوني المنظم للجريمة المعلوماتية في التشريعات العربية	22
الفرع الأول : الاطار القانوني المنظم للجريمة المعلوماتية في القانون المغربي	22
الفرع الثاني : الاطار القانوني المنظم للجريمة المعلوماتية في قانون الاتحاد الإماراتي	26
المطلب الثاني : الاطار القانوني المنظم للجريمة المعلوماتية في التشريعات الأجنبية	29

الفرع الأول : القانون المنظم للجريمة المعلوماتية في التشريع الفرنسي	29
الفرع الثاني : الاتفاقية الأوروبية الخاصة بجرائم تقنية المعلومات بودابيست	31
الفصل الثاني : قواعد الاختصاص في الجريمة المعلوماتية	
تمهيد	34
المبحث الأول : قواعد إجرائية لمتابعة الجريمة المعلوماتية	34
المطلب الأول : إشكالات المتابعة و التحري و في الجريمة المعلوماتية	34
الفرع الاول : إجراءات التحقيق في الجريمة المعلوماتية	35
الفرع الثاني : إجراءات خاصة في التحقيق المعلوماتي	41
المطلب الثاني : إشكاليات الاختصاص في الجريمة المعلوماتية	43
الفرع الأول : القانون الواجب التطبيق على الجرائم المعلوماتية	44
الفرع الثاني : تنازع الاختصاص في الجريمة المعلوماتية	46
المبحث الثاني : الجهات و الهيئات المختصة بمتابعة الجريمة المعلوماتية	48
المطلب الأول : اختصاص الاقطاب الجزائية المتخصصة في الجريمة المعلوماتية	49
الفرع الأول : تنظيم وسير الاقطاب الجزائية المتخصصة	49
الفرع الثاني : طرق اتصال القطب الجزائي المتخصص بالجريمة المعلوماتية	52
المطلب الثاني : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال	54
الفرع الأول : اختصاص الهيئة	54
الفرع الثاني : مهام الهيئة	55
الخاتمة	59
قائمة المصادر و المراجع	63
الفهرس	68