وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم الحقوق

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

جرائم تكنولوجيا الإعلام والإتصال وآليات مكافحتها في ضوء القانون رقم 04/09

ميدان الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون قضائي

من إعداد الطالبة:عامر فوزية

تحت إشراف الأستاذ: بن عوالي علي

أعضاء لجنة المناقشة

الأستاذ: بن عودة يوسف	رئيسا
الأستاذ: بن عوالي علي	مشرفا مقررا
الأستاذ: بوسحبة الجيلالي	مناقشا

السنة الجامعية: **2025/2024**

نوقشت في : 10 /2025/06

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

UNIVERSITE Abdelhamid Ibn Badis MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: عامر فوزية ...... الصفة: أنثى ......

الحامل لبطاقة التعريف الوطنية رقم: 109870058 والصادرة بتاريخ: 2019/07/17 ......

المسجل بكلية: الحقوق والعلوم السياسية ...... قسم: قانون خاص ......

والمكلف بإنجاز مذكرة ماستر بعنوان:

جرائم تكنولوجيا الإعلام والاتصال وآليات مكافحتها في ظل قانون رقم 09/04

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

التاريخ: ......

إمضاء المعني

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

إهـــداء

إلى من أوصاني بهما ربي برا وإحسانا

إلى والدي أطال الله في عمره

إلى من غيبته الموته ولم ينسى القلب

أمي رحمها الله وأسكنها الله الفردوس الأعلى

إلى أخواتي الحبيبات

وبالأخص أخي عبد الرحمن الذي دعمني ورفقني في كل خطوة على هذا الطريق

فـــوزية

شكـــر وعرفـان

الحمد لله إلى أن يبلغ الحمد منتهاه الحمد لله إلا أن ترضى حمد الله عند الرضى

الحمد والشكر لله العلي القدير الذي منى عليّ باتمام هذه المذكرة

أتوجه وأتقدم بأسمى عبارات الثناء والتقدير للأستاذ الفاضل بن عوالي علي

على إشرافه على هذه المذكرة

وعلى كل ما قدمه من دعم وتوجيه وإرشاد هادف لتفعيل هذا العمل

كما يشرفني أن أتقدم بجزيل الشكر والتقدير إلى السادة الأساتذة الكرام أعضاء الجنة

على قبولهم مناقشة هذ العمل المتواضع

أتقدم بجزيل الشكر لكل من ساعدني في إنجاز هذا العمل ولو بكلمة طيبة

قائمة المختصرات

ج.ر.ج.ج.د.ش	الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية
ق.ع	قانون العقوبات
ق.إ.ج	قانون الإجراءات الجزائية
د.ط	دون طبعة
ص	الصفحة

مقدمة

مقدمة:

جلب التطور التكنولوجي لحياة الإنسان العديد من المحاسن، إذ أن الثورة المعلوماتية التي يعرفها العالم حلياً، إنعكست صورتها بشكل كبير على جميع مجالات الحياة الإقتصادية ولإجتماعية والقانونية والأمنية للدول، حتى أصبح العصر الحالي يعرف بعصر التكنولوجيا ونقطة إنطلاق الثورة المعلوماتية كانت نتيجة لظهور الحاسب الآلي سنة 1837[1] على يد المصمم تشارلز بابيج والذي عرف بدوره تطورا كبيرا، إذ أنه أصبح معتمد من طرف جميع هيئات الدولة في ممارسة وظائفها ولم يتوقف هذا التطور عند الحاسب الآلي بل ظهرت مايسمى بالشبكة العنكبوتية سنة 1975، والتي هي الأخرى وأعطت نقلا متسرعا في نمط الحياة وتغيير الكبير فيه، حيث أصبحت نصف سكان العالم يستعملون الشبكة العنكبوتية[2].

على الرغم من الفوائد الهائلة التي تحققها والتي تم تحقيقها في مجال تكنولوجيا المعلومات على جميع المستويات، وفي مختلف مجالات الحياة المعاصرة فإن هذه الثورة التكنولوجيا المتنامية رفقتها في المقابل جملة من الإنعكسات السلبية الخطيرة جراء سوء إستخدام هذه التقنية المتطورة والإنحراف عن الأغراض المتوخاة منها، تجلت في تفشي طائفة من الظواهر الإجرامية المستحدثة ألا وهي ظاهرة الجرائم المعلوماتية أو الجرائم الالكترونية التي لم تعد تقتصر على إقليم دولة واحدة بل تجاوزت حدود الدولة ، وهي جريمة مبتكرة ومستحدثة تمثل إحدى صو الذكاء الإجرامي، مما صعب من مهمة إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية الأجنبية، وتعود بداية شيوع هذه الجريمة إلى ستنيات القرن الماضي حيث تم في هذه المرحلة ظهور أول معالج لها يسمى بجرائم الكمبيوتر، أين إقتصرت المعالجة على مقالات ومواد صحفية التي تناقش التلاعب الذي يحصل بالبيانات والتجسس، والدمار، الذي يحصل في نظام الكمبيوتر وخلال فترة السبعينيات ظهرت دراسة

أنظر الموقع الإلكتروني http://mawdoo3.com تاريخ الاطلاع :2025/05/09 على الساعة 11:43

مسحية إهتمت بالجرائم المعلوماتية وأيضا دراسات قانونية قد عالجت بعض الجرائم الواقعية فعلا.

ومع بداية الثمانينات بدأت جرائم الكمبيوتر في تضاعف وزاد إرتباطها بعمليات إقتحام نظام الكمبيوتر عن بعد وتدمير الملفات، وهذا ما أدى إلى إشاعة مصطلح الهاكزر الذي يحمل معنى مقتحم النظام ،ومع التوسع الهائل لشبكة الأنترنت في فترة التسعينات أدى ذلك إلى ظهور أشكال جديدة مثل تعطيل نظام معين وتعطيله عن القيام بعمله كما تميزت هذه المرحلة بانتشار الكبير للفيروسات عبر شبكات الأنترنت عن طريق المواقع الإلكترونية التي سهلت إنتشارها إلى ملايين المستخدمين[1].

وبما أن الجريمة الإلكترونية ظاهرة جديدة بسبب إرتباطها بتقنيات المعلومات والإتصالات سهلة الإرتكاب تنشأ في الخفاء وفي بيئة إفتراضية دون إن تخلف أي اثر محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات وخبرات تقنية عالية، لذا تعتبر من أخطر وأعقد الجرائم على الإطلاق وتأتي في مقدمة الأشكال الجديدة للجريمة المنظمة وخطورة هذه الجرائم النابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها.

ولكبح هذا النوع من الجرائم سارع المجتمع الدولي إلى إبرام إتفاقيات دولية وإقليمة تتضمن مجموعة من الآليات القانونية، كمنع تطور وإمتداد الجرائم الإلكترونية وبما أن الدولة الجزائرية جزء من المجتمع الدولي فهي الأخرى ليست بمنأى عن الجرائم الإلكترونية فسارع المشرع الجزائري إلى إحتواء هذا النوع من الجرائم بالمصادقة على الإتفاقيات الدولية والإقليمية.

والمشرع الجزائري على غرار باقي التشريعات العربية والغربية وضع القواعد الخاصة بالوقاية من الجرائم المتصلة بالجرائم المعلوماتية ومكافحتها وتجلى ذلك من خلال ما إحتواه التشريع العقابي وكذا القواعد الإجرائية التي تتبع في مجال الكشف عنها لذا إفرد المشرع

[1] سعيدي سليمة، حجاز بلال، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الاسكندرية، طبعة الأولى، 2017،صفحة57.

الجزائري فصلا كملا في قانون العقوبات الجزائري وهو الفصل السابع الموسوم بعنوان "الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات"، هذا فضلا عن إصدار المشرع الجزائري قانون 09/ 04 المؤرخ في 05/09/ 2009[1] المتضمن القواع الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها "وكذا إستحداثه بموجب المرسوم الرئاسي 261/15 المؤرخ في 2015/10/08 للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.[2]

أهمية الموضوع: تبرز أهمية الموضوع من خلال الجوانب التالية:

الأهمية العلمية: تتجلى من خلال إبراز الجانب النظري للأحكام القانونية والجزائية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما والوقوف على مدى مواكبة الآراء الفقهية المتعلقة بتكنولوجيات الإعلام ولإتصال.

الأهمية العملية: تنحصر في إبراز الجانب العملي والواقعي لأحكام القانونية الجزائرية القانونية الجزائرية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها والتحديات التي تواجه المشرع الجزائري في التصدي لهذا النوع من الجرائم والوقوف على ميكانيزمات المؤسساتية التي إستحدثها المشرع الجزائري على غرار الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والإتصال.

وأما عن دوافع اختيارنا لهذا الموضوع : تنحصر في أسباب ذاتية، وأخرى موضوعية.

الأسباب الذاتية: إن تنامي ظاهرة الإجرام المعلوماتي والإعتداءات الواقعة على الأشخاص والمؤسسات في الجزائر بالآونة الأخيرة شكلا دافعا وحافزا قويا للبحث ودراسة الموضوع، كما شكل لدينا مستوى من الوعي بالأهمية الأكاديمية للموضوع ناهيك عن الرغبة

---

[1] القانون الجزائري رقم 09-04 المؤرخ في 05أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، ج.ر.ج.ج.د.ش. العدد47المؤرخة في 16أوت 2009.

[2] أنظر المرسوم الرئاسي رقم 15-261، المؤرخ في2015/10/08، يحدد تشيكلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر.ج عدد53ن مؤرخ في 2015/10/08.

في معرفة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والتخوفات التي تختلجها وكذا الوسائل والاليات المعدة لمكافحة هذا النوع من الجرائم الخاصة.

الأسباب الموضوعية : أما من الناحية الموضوعية تتمثل في إنتشار الجرائم المعلوماتية في المجتمع بشكل ملحوظ ، مما يجب تسليط الضوء عليها فهذه الدراسة محاولة جادة منا لفهم كيفية مجابهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي أوجدها المشرع الجزائري.

وتتلخص أهداف الدراسة في أهداف علمية وأخرى عملية وقد تجلت فيما يلي:

الأهداف العلمية:

وضع دراسة قانونية جزائية متخصصة في مجال الجرائم الماسة بتكنولوجيات الإعلام والإتصال يستفيد منها من له علاقة بالموضوع ومن له إهتمام بلإجرام المعلوماتي وبالمساهمة في إثراء المكتبة القانونية الجزائرية بدراسة قانونية تتعلق بالجرائم الماسة بتكنولوجيات الإعلام والإتصال وجعل هذه الدراسة منطلقا لدراسات أخرى في هذا المجال.

الأهداف العملية: إما عن الأهداف العملية فدراسة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال من الموضوعات التي تم تناولها بشكل مجحف ومقتضب إلا أن الملاحظ هو إن هناك إهتمام متنامي من قبل الباحثين القانونين بهذا الموضوع بعد إنتشار هذه الظاهرة على مختلف إنحاء العالم عامة وعلى المستوى الوطني بشكل خاص وعليه فان الدراسة تسعى إلى:

- ✓ إعطاء مفهوم لجرائم المتصلة بتكنولوجيات الإعلام والإتصال وإلى أهم الخصائص التي تتمتع بها.
- ✓ معرفة أصناف الجرائم المتصلة بتكنولوجيات الإعلام في التشريع الجزائري .
- ✓ معرفة الإجراءات وأهم آليات مكافحة جرائم المتصلة بتكنولوجيات الإعلام والإتصال في الواقع العملي.

وفي سبيل تحقيق ذلك سنحاول الإجابة عن إشكالية جوهرية تدور حول التساؤل الرئيسي الذي مفاده إلى أي مدى ساهم القانون 09-04 في مكافحة الأنماط المستجدة في جرائم تكنولوجيا الإعلام ولإتصال؟

- وتندرج تحت هذه الإشكالية مجموعة من التساؤلات نجملها فيما يلي:
- بم تتميز الجريمة الإلكترونية عن باقي الجرائم التقليدية؟
- ماموقف المشرع الجزائري من الجريمة الإلكترونية، وما سبل التي إقرها لمكافحتها؟

وللإجابة على هذه الإشكالية تم الإعتماد على المنهج الوصفي الذي إعتماده في وصف الجزئيات المتعلقة بالجرائم الماسة بتكنولوجيات لإعلام والإتصال والوقاية منها والمنهج التحليلي إعتماده في تحليل وإستقراء النصوص القانونية المتعلقة بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

وجاءت حدود الدراسة في الإيطار التشريعي وذلك من خلال ماأقره المشرع الجزائري بشأن الجرائم الماسة بتكنولوجيات الإعلام والإتصال في كل من قانون العقوبات الجزائري وقانون الإجراءات الجزائية ، وقانون المتضمن القواعد الخاصة بالوقاية من الجرائم الماسة بتكنولوجيات الإعلام والإتصال.

وسبقنا في دراسة هذا الموضوع مجموعة درسات سابقة لها علاقة مباشرة بموضوع دراستنا والتي من بينها:

الدراسة الأولى: للباحث مصطفاوي عبد القادر الموسومة بعنوان "الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" أطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق تخصص ، قانون عام جامعة الجزائر1 كلية الحقوق السنة الجامعية2021-2022 وما يمكن قوله بخصوص هذه الدراسة إنها تناولت الآليات الجزائية الموضوعية لمواجهة الجرائم الإلكترونية ولتقينا مع هذه الدراسة في بعض الجزئيات التي تناولها الباحث من بينها الجرائم التقليدية المتعلقة بالمساس بالإنظمة المعالجة الآلية للمعطيات والإجراءات المستحدثة للجريمة المعلوماتية.

الدراسة الثانية: للباحث إبراهمي جمال الموسومة بعنوان التحقيق الجنائي في الجرائم الإلكترونية "أطروحة لنيل شهادة الدكتورة في العلوم تخصص قانون جامعة تري وزو كلية الحقوق وعلوم السياسية قسم الحقوق سنة 2018 ولقد تناول الباحث إجراءات التحقيق في الجرائم الإلكترونية ولقد التقينا مع هذه الدراسة في بعض الجزئيات المتعلقة بالتحقيق وإجراءاته فبالجرائم الماسة بتكنولوجيات الإعلام والإتصال.

الدراسة الثالثة: شنتير خضرة المسومة بعنوان "الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)"أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث (ل.م.د) تخصص قانون جنائي ،جامعة أحمد دراية أدرار، كلية الحقوق والعلوم السياسية ،سنة الجامعية 2020-2021 ومايمكن قوله بحصوص هذه الدراسة أنها تناولت الاليات القانونية والمؤسساتية لمكافحة الجريمة المعلوماتية.

وصدفتنا بصدد دراستنا هاته وجهتنا بعض الصعوبات نذكر أهمها :

كون الموضوع له علاقة بالجانب التقني والفني ،وهذا مايستدعي الإلمام أكثر بالموضوع .

إستجابة للإشكالية المطروحة تم الإعتماد على التقسيم الثنائي الذي يشمل فصلين.

الفصل الأول: الإطار الفاهمي للجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

المبحث الأول : ماهية جرائم تكنولوجيا الإعلام والإتصال.

المطلب الأول: مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

المطلب الثاني: أركان الجريمة المتصلة بتكنولوجيا الإعلام والإتصال.

المبحث الثاني: المجرم الإلكتروني وسماته .

المطلب الأول: مفهوم المجرم الإلكتروني .

المطلب الثاني: صور الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ودوافع إرتكابها .

الفصل الثاني: الآليات القانونية والإجرائية لمكافحة جرائم تكنولوجيا الإعلام والإتصال .

المبحث الأول: الآليات القانونية والمؤسساتية لمكافحة جرائم تكنولوجيا الإعلام والإتصال .

المطلب الأول: جهود المشرع الجزائري في مكافحة جرائم تكنولوجيا الإعلام والإتصال على صعيد الوطني .

المطلب الثاني: جهود المشرع الجزائري في مكافخة جرائم تكنولوجيا الإعلام والإتصال على الصعيد الدولي.

الميحث الثاني: آليات البحث وتحري في جرائم تكنولوجيا الإعلام والإتصال في التشريع الجزائري.

المطلب الأول: طرق التحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

المطلب الثاني: الدليل الإلكتروني وسلطة القاضي في تقديره.

الفصل الأول

الإطار المفاهيمي لجرائم تكنولوجيا الإعلام والإتصال

تمهيد:

يعرف العالم اليوم ثورة تكنولوجية هائلة متزايدة بشكل مستمر على جميع الأصعدة السياسية ولإقتصادية وإجتماعية وثقافية ، وإبراز ما يميز هذه الثورة التكنولوجية هي التقدم الحاصل في تقنية المعلومات والإتصالات التي غيرت هي الأخرى من بنية العالم، فأصبحت معظم الأفعال مقترنة باستعمال تكنولوجيات الإعلام والإتصال هذا الوجه الإيجابي لها أما الشق السلبي في إستعمال تكنولوجيا الإعلام والإتصال هو تمكن الفئة المجرمة من توظيف تكنولوجيا الإعلام والإتصال في المخطط الإجرامي حتى أصبح من الصعب إكتشافها والتصدي لها فصار من الضروري إيجاد آليات لمكافحة هذه الجريمة ، لكن قبل البحث عن آليات مكافحة الجريمة الإلكترونية لابد أولا من التطرق إلى الإطار المفهيمي للجريمة الإلكترونية وكذ تبيان خصائصها وأركانها وكذا مرتكبها.

ولأجل ذلك فقد تم تقسيم هذا الفصل إلى مبحثين خصص الأول لماهية جرائم تكنولوجيا الإعلام والإتصال ، بينما خصص المبحث الثاني للمجرم الإ لكتروني وسماته .

المبحث الأول: ماهية جرائم تكنولوجيا الإعلام والإتصال.

تعتبر الجريمة الإلكترونية إحدى أخطر الأوجه السلبية التي نتجت عن التقدم السريع الذي مس جميع المجالات العلمية والحياتية في عصرنا الحالي، وأدى التطور الملحوظ الذي شهدته هذه الجريمة في اللآونة الأخيرة إلى صعوبة مواجهتها وتعقد أساليب مكافحتها ، لكي نستطيع إيجاد آليات مكافحة ناجعة لابد من تحديد تعريف دقيق لهذه الظاهرة الإجرامية ، لذا فإنه لبد من تطرق لبعض المفاهيم والمصطلحات التي تعد معرفتها بمثابة مدخل لموضوع دراسة ومن أجل ذلك تم تقسيم هذا المبحث إلى مطلبين خصص المطلب الأول لتحديد مفهوم الجريمة المعلوماتية و خصص المطلب الثاني لأركان الجريمة المعلوماتية.

المطلب الأول مفهوم جرائم تكنولوجيا الإعلام والإتصال .

تعرّف الجريمة عموما في نطاق القانون الجنائي أنها فعل غير مشروع صادر عن الإرادة الجنائية يقرر له القانون عقوبة وتدابير إحترازية تقوم أساسا على عناصر الجريمة والسلوك ووصفه والنص القانوني على تجريم السلوك وإيقاع العقوبة[1] أما الجريمة الإلكترونية فقد وجد الفقه صعوبة كبيرة في إيجاد تعريف دقيق لها، بل حتى في إيراد تسمية موحدة لها فهناك عدة تسميات لها منها: الجريمة المعلوماتية، جرائم إساءة إستخدام تكنولوجيا المعلومات والإتصال جرائم الكمبيوتر والإنترنت، الجرائم المستحدثة، الجريمة الناعمة، جرائم ذوي الياقات البيضاء ولقد أطلق المشرع الجزائري تسمية "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات" في قانون الجزائري رقم 04-15[2] واستعمل تسمية "الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" في القانون الجزائري رقم 09-04.[3]

ورغم إختلاف المشرعين في تسميات الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إلا أن تسميتها تصب في منحى واحد يقضي بتبيان أفعال تدخل ضمن الجرائم يستعمل فيها وسائل تكنولوجية حديثة، سوف نتطرق في هذا الفرع إلى التعريف الفقهي لجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ثم نتطرق إلى التعريف التشريعي لجرائم تكنولوجيا الإعلام والإتصال وتعريف المشرع الجزائري .

الفرع الأول: تعريف جرائم تكنولوجيا لإعلام والإتصال.

إن من المجمع عليه من قبل الفقه هو غياب إجماع بخصوص تعريف الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ، حيث تعددت المفاهيم وتختلف بإختلاف الزاوية التي تنظر منها إلى هذه الجريمة ، فهناك جانب من الفقه عرفها من الزاوية فنية، وأخرى قانونية، وهناك جانب

---

[1] أحمد سقيعة، الوجيز في القانون الجنائي العام، دار هومه، جزائر الطبعة الخامسة، 2007، ص21.

[2]القانون رقم 04-15المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات الجريدة الرسمية الجزائرية العدد 71بتاريخ 2004/11/10.

[3] القانون رقم 09-04 مؤرخ في 14 شعبان 1430الموافق 5غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ،الجريدة الرسمية 47 بتاريخ 16 غشت سنة 2009.

آخر حاول تعريفها بالنظر إلى وسيلة إرتكابها أموضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير مختلفة .ومن أجل إعطاء مفهوم شامل للجريمة لابد من تعريفها من كل الجوانب.[1]

أولا:التعريف الفقهي لجرائم تكنولوجيا الإعلام ولإتصال .

تعددت تعريفات الجريمة المعلوماتية ولا يوجد تعريف جامع مانع لها، فهناك جانب من الفقه عرفها بناءا على الوسيلة إرتكابها، أو موضوعها أو بمدى دراية وتحكم مرتكبها بتقنية المعلومات وهذا ماسنبينه في الأتي:

أ) تعريفات تقوم على موضوع الجريمة:

تعرف الجريمة الإلكترونية في هذا الإطار على أنها: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى معلومات مخزنة داخل الحساب الآلي أو التي تحوّل عن طريقه[2] وعرفتها الدكتورة هدى قشقوش بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة لآلية للبيانات أو نقل هذه البيانات[3]، وتعرف الجريمة الإلكترونية أيضا بأنها: "نمط من أنماط الجرائم المدونة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"، ويلاحظ على هذه التعاريف تركيزها على موضوع الجريمة دون الوسيلة المعتمدة فيها وهذا أهم إنتقاد يوجه لهذه التعاريف لأن أهم مايميز هذه الجرائم أنها تتم في وسط إفتراضي وتمس بمعطيات الحاسب لآلي سواء أكانت مادية أو معنوية.

---

[1] عبد الفتاح حجازى، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، القاهرة ، مصر ، 2007 ص13.

[2] محروس نصار غايب ، الجريمة المعلوماتية ، مقال منشور على الموقع الإلكتروني، www.iasj.net/iasj?func=fulltext&ald=28397 أطلع عليه بتاريخ :12/ 01 /2025 الساعة 15:06.

[3] هدى قشقوش، جرائم الحساب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى ،1992 صفحة 22.

ب) تعريفات تقوم على محل الجريمة وسيلة إرتكابها

من هذا التصور تتحقق الجريمة الإلكترونية باستخدام الكومبيوتر ، فالأستاذ "جون فورستر" يعرفها بأنها فعل إجرامي يستخدم الكومبيوتر كأداة رئيسية في إرتكابه ، وهذا مذهب إليه أيضا الفقيه تايدمان "Tiedeman " حيث أشار إلى أنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"، ويصف هذه الجريمة مكتب تقيم التقنية في الولايات المتحدة الأمريكية بأنها: "جريمة التي تلعب فيها بيانات الكومبيوتر وبرامج المعلوماتية دورا رئيسيا " وعرفها الأستاذان" روبرت ج.ليند كوست" (j.Robert Lindquist) و"جاك بولوقنا" (jak bologna) بأنها "جريمة تستخدم فيها الحاسوب كوسيلة أو أداة لإرتكابها أويمثل إغراء بذالك أو جريمة يكون الكمبيوتر نفسه ضحيتها"[1] أما منظمة التعاون الإقتصادي والتنمية OECD" فقد عرفتها بأنها "فعل أو إمتناع من شأنه لإعتداءعلى الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، وعرفت " أيضا بأمنها الممارسات التي تقع ضد الأفرد أو المجتمع مع توفر الباعث الإجرامي بهدف التسبب في الأذى لسمعة الضحية عمدا،أو إلحاق الضررالنفسي والبدني به سواء أكان ذلك بأسلوب مباشر أوغير مباشر للإستعانة بشبكات الإتصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحداثات والهواتف المحمولة وما تتبعها كرسائل والوسائط المتعددة.[2]

ولقد لقيت هذه التعريفات عدة إنتقادات منها إتسامها بالعمومية ولإتساع لأنه يدخل كل سلوك ضار بالمجتمع يستخدم فيه الجانب لآلي في قائمة الجرائم الإلكترونية.

إن التمعن في التعريفات السابقة يرى بأنها قد وسعت من مفهوم الجريمة الإلكترونية بحيث إعتبرت أن مجرد إستعمال الكمبيوتر في الفعل المجرم يصبغ عليه تكيف الجريمة الإلكترونية

---

[1] أيمن عبد الله فكري حسين، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية ، الطبعة الأولى ، مكتبة القانون والإقتصاد، الرياض ، السعودية 2014 .

[2] شرف الدين وردة ،مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية –في التشريع الجزائري –مجلة المفكر ،كلية الحقوق ولعلوم السياسية ،جامعة محمد خيضر، بسكرة العدد الخامس عشر ،جوان 2017،ص540.

ولكن الواقع ليس كذلك في حين أن هناك جرائم رغم إستعمال جهاز الكمبيوتر إلى أنها تبقى جرائم عادية كمثال ذلك تزوير النقود باستعمال الحاسب الآلي.[1]

ج) تعريفات متنوعة لجرائم تكنولوجيا الإعلام والإتصال :

وقد ذهب الخبراء متخصصون في دول الإتحاد الأوروبي إلى القول إن الجريمة الكمبيوتر هي:" كل فعل عمدي ينشأ عن إستخدام غير مشروع لتقنية المعلوماتية ويهدف إلى الإعتداء على الأملاك المادية أوالمعنوية التي تكون من ضمنه[2] "وبرجوع الى مؤتمر الأمم المتحدة العاشر

لمنع الجريمة ومعاقبة المجرمين يتضح إنه تبنى تعريف منضبط لجريمة تقنية المعلومات بأنها:" أية جريمة يمكن إرتكابها بواسطة نظام حسابي أو شبكة حسابية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة الكترونية"[3].

أما إتفاقية بودابست لمكافحة الجرائم المعلوماتية 08 نوفمبر 2001 التي تعتبر من أهم الإتفاقيات المتعلقة بمكافحة الجريمة لإلكترونية عن طريق وضع نظام دولي يمتاز بالسرعة والفعالية في التنفيذ وكذلك إقرار سياسية جنائية في مجال التصدي للجريمة الإلكترونية ، كما أنها لم تتضمن تعريفا للجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، وتضمنت تجريم مجموعة من الأفعال منها الولوج غير المشروع للنظام المعلوماتي ،الإعتراض غير قانوني على النظام المعلوماتي،التزويروالغش المعلوماتي[4]. ونفس الأمر بالنسبة للإتفاقية العربية لمكافحة

---

[1] عادل يحي ، السياسة الجنائية في مواجهة الجريمة المعلوماتية ، الطبعة الأولى ، دار النهضة العربية ،القاهرة ،مصر 2014،ص45.

[2] عفيفي كمال عفيفي،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية دور الشرطة والقانون ،دراسة مقارنة ، منشورات الحلبي الحقوقية ، طبعة اولى ، بيروت ، 2003 ،صفحة 32.

[3] إعلان فينا بشأن الجريمة والعدالة ،مواجهة تحديات القرن الحادي والعشرون مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين ، الذي عقد في فينا في فترة الواقعة مابين 17/10 نيسان لعام 2000الفقرة 17،صفحة 37.

[4] الإطلاع على إتفاقية بودابست لمكافحة الجرائم المعلوماتية المؤرخة 08 نوفمبر 2001 ،أنظر الموقع الإلكتروني https://rm.coe.int تاريخ الاطلاع 2025/05/14 01:12 .

جرائم تقنية المعلومات لم تعرف هي الأخرى جرائم تكنولوجيا الإعلام والإتصال شأنها شأن اتفاقية برن لحماية المصنفات الأدبية والفنية .

ومن التعريفات التي لقيت إستحسنا تعريف خبراء منظمة التعاون الإقتصادي والتنمية والذين إعتبرو الجريمة الإلكترونية كل سلوك غير مشروع أوغير أخلاقي أوغير مصرح به المتعلق بالمعالجة الآلية للبيانات أونقلها.

ثانيا:التعريف التشريعي لجرائم تكنولوجيا الإعلام والإتصال .

نجد بعض التشريعات العربية أعطت تعريفا للجريمة الإلكترونية كما فعل كلا من المشرع الكويتي والسعودي فالأول عرفها في المادة (1)الأولى من القانون مكافحة جرائم تقنية المعلومات رقم:63 لسنة 2015 ،"كما يلي في تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية المعنى الموضح قرين لكل منها.....الجريمة المعلوماتية: كل فعل يرتكب من خلال إستخدام الحاسب الآلي أو الشبكة المعلوماتية أوغير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون "[1] ، أما نظام مكافحة الجرائم المعلوماتية السعودي فقد عرفها في الفقرة الثامنة المادة الاولى(8/1) بانها:" أي فعل يرتكب متضمنا إستخدام الحاسوب الالي أو الشبكة المعلوماتية بمخالفة أحكام هذا لنظام"[2].

في حين بعض تشريعات العربية لم تعطي تعريفا لجرائم تكنولوجيا الإعلام والإتصال كما هو الحال بالنسبة للمشرع والبحريني والإماراتي التونسي حيث نجد هذ الأخير إكتفى بالإشارة

---

[1]قانون مكافحة جرائم تقنية المعلومات الكويتي رقم :63 لسنة 2015، الصادر يوم الأحد12 يوليو 2015، العدد 1244 .

[2]أقر نظام مكافحة الجرائم المعلوماتية السعودي مجلس الوزراء في جلسته الأسبوعية يوم الإثنين 1428/03/07هـ الموافق2007/03/26، وصدر بموجب المرسوم الملكي رقم (م/17)بتاريخ 31428/8هـ ،القانون موجود على الموقع الإلكتروني للجريدة الرسمية للمملكة العربية السعودية: //www.uqn.gov.sa/channels/royal:http -decreesتم الإطلاع :2025/05/09.الساعة 18:16.

إلى الأفعال التي تكون الجريمة المعلوماتية ضمن مواد 16الى 25من المرسوم التونسي المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات لسنة 2022[1].

ويمكننا القول أن المشرعين الكويتي والسعودي تقدما على التشريعات العربية الأخرى عندما عرفا الجريمة الالكترونية ذلك إن تعريفها يعد نقطة إرتكاز مهمة لأتشريع محل البحث لما للجريمة الإلكترونية من أهمية كونها من الجرائم المستحدثة في العصر الحالي.

ثالثا: تعريف جرائم تكنولوجيا الإعلام والإتصال في التشريع الجزائري .

المشرع الجزائري كغيره من التشريعات المقارنة لم يعطي تعريفا معينا للجريمة الإكترونية بل لم يستعمل مصطلح الجريمةالإكترونية أو المعلوماتية أو السيبرانية في القوانين التي سنها في هذا لمجال ، إذ كانت الجرائم الإلكترونية قبل تعديل قانون العقوبات الجزائري سنة 2004 تصنف ضمن جرائم النظام العام كالسرقة وخيانة الأمانة والإختلاس وغيرها من الجرائم ، فجرائم تكنولوجيا الإعلام والإتصال رغم خصوصياتها وإختلافها عن الجرائم التقليدية [2] إلا أنها كانت في غياب النص تلبس ثوب العقوبات المقررة لنظيراتها التقليدية ، وفي سنة 2004 أطلق المشرع الجزائري تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك بمقتضى القانون رقم 15/04 المعدل والمتمم لقانون العقوبات والتي نص عليها في المواد من 394 مكرر إلى 394 مكرر 07 [3]ومن خلال هذه المواد قم المشرع الجزائري بتقسيم الجريمة الإلكترونية إلى أربعة

---

[1] أنظر المواد من 16 إلى 25 من المرسوم التونسي المؤرخ في 13سبتمبر 2022 المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات وإتصال ،الرائد الرسمي للجريدة الرسمية التونسية ،العدد 103 المؤرخة في 16 سبتمبر 2022 ، ص49 .

[2] نشناش منية ،الركن المفترض في الجريمة المعلوماتية ، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة ،المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة ، بكلية الحقوق والعلوم السياسية، بجامعة بسكرة ، يومي 16-17 نوفمبر 2015،ص12.

[3]أنظر:ج.ر.ج .ش العدد71المؤرخة في 10نوفمبر 2004 ص08 ،

طوائف فئة تتضمن جرائم الولوج إلى المعطيات المعالجة آليات عن طريق الغش والتزوير وكذا جريمة الحذف والتغير والتخريب في المعطيات ، وفئة جرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها إستعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات.

وكذا البحث أو التجميع في المعطيات مخزنة في النظام معلوماتي وفئة الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب وفئة الجرائم الإلكترونية للشخص المعنوي والتي تعادل عقوبتها خمس مرات عقوبة الشخص الطبعي وفقا للمادة 394 مكرر4 من قانون العقوبات الجزائري ، ثم أصدر المشرع الجزائري القانون رقم 06-23[1] المعدل ومتمم لقانون العقوبات المتضمن تجديد العقوبة على كل الجرائم الواردة في هذا القانون ، وهو مايؤكد إقرار المشرع الجزائري للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كجرائم جديدة ومستحدثة متميزة عن الجرائم التقليدية من حيث محلها ومرتكبها[2] ، وفي سنة 2009عاد المشرع الجزائري وسمها جرائم المتصلة بتكنولوجيا الإعلام والإتصال بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها المؤرخ في 05 غشت2009 ، إذ جاء في نص المادة الثانية(02) فقرة "أ" منه أن:" جرائم تكنو لوجيا الإعلام والإتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية"[3]، وحددت هذه المادة أيضا بعض المصطلحات بقولها :"يقصد في مفهوم هذا القانون بما يأتي :

---

[1] أنظر :القانون الجزائري رقم 06-23 المؤرخ في 20ديسمبر 2006 ،ج.ر.ج العدد84 المؤرخة في 14 ديسمبر 2006 ص11،ص29، المعدل ومتمم للأمر الجزائري رقم 66-156 ،المؤرخ في 08 جوان 1996 والمتضمن قانون العقوبات الجزائري ج.ر.ج ، ش، العدد 49 المؤرخة في 11جوان 1966، 852ص.

[2] شنتير خضرة ،الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)،أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث تخصص قانون الجنائي ،جامعة أحمد دراية كلية الحقوق والعلوم السياسية بأدرار ،2020-2021 ، ص11 .

[3] القانون رقم 09-04،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكفحتها ،المشار اليه سليقا.

الجرائم المتصلة بتكنولوجيا الإعلام والإتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أونظام للاتصالات الإلكترونية.

- منظومة معلوماتية : أي نظام منفصل أومجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذالبرنامج معين .
- معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرنامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفته.
- الإتصالات الإلكترونية : بأنها إرسال أوإستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أو وسيلة إلكترونية .[1]

من الخلال التعريف السابق يتبين إن المشرع الجزائري قد وسع من تعريف الجريمة الإلكترونية خاصة حين إعترف بأنها أية جريمة أخرى ترتكب أويسهل إرتكابها عن طريق منظومة معلومتية أو نظام الإتصالات الإلكترونية ونحن نرى أنه قد أحسن مافعل ، لكي تدخل في دائرة التجريم أنواع جديدة أخرى من الجرائم الإلكترونية والتي قد تكتشف مستقبلا .

وبناءا على ماذكرى أعلاه يتضح أن الجرائم تكنولوجيا الإعلام والإتصال لم تحظ بتعريف شمال أو متفق عليه،إذ أن وضع تعريف محدد لها أمر ليس باليسير، لذلك ذهب بعضهم إلى القول بضرورة مرعاة إعتبارات مهمة عند وضع تعريف لها أن يكون التعريف مقبولاً ومفهوماً على المستوى العالمي وأن يرعى التطور السريع و المتلاحق في تكنولوجيا المعلومات وأن يفرق في

[1] انظر :ج.ر.ج العدد 47، المؤرخة في 16 اوت 2009، ص 05 ، ص08

التعريف بين الجريمة العادية والجريمة الإلكترونية، وذلك عن طريق إيضاح الخصائص ومميزات الجريمة الإلكترونية[1].

الفرع الثاني: خصائص جرائم تكنولوجيا الإعلام والإتصال .

تعد الجريمة المعلوماتية من بين الجرائم المستحدثة التي ظهرت في ظل التطور التكنولوجي الهائل الذي عرفه مجال الإعلام والإتصال باتساع التغطية بشبكة الأنترنت والأنتشار الواسع للحواسب والوسائط الالكترونية ومختلف وسائل الإتصال الحديثة لاسيما الهواتف النقالة هذا الأمر الذي أضفى عليها مجموعة من السمات التي تميزها عن الجرائم العادية وتتمثل :

اولا : جريمة مستحدثة :

تعتبر جرائم تكنولوجيا الإعلام والإتصال من الجرائم الحديثة غير التقليدية تقوم أساسا على جهاز إلكتروني متطور، يشكل أدات الجريمة ووسيلة تنفيذها ، فبدون هذ الجهاز تنتفي الجريمة المعلوماتية ، ويطلق على مرتكبها الفاعل بوسائل تكنولوجيا الذي يختلف عن المجرم التقليدي. [2]

ثانيا: جريمة عابرة للحدود الوطنية:

تستمد الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هذه الصفة من عدم حصرها في مكان جغرافي واحد ، فهي تتصل بالشبكة العنكبوتية التي توجد في أغلب بقاع العالم والتي ساهمت في ربط عدد كبير من الحواسيب ببعضها البعض ، خاصة في ظل التطور التكنولوجي

---

[1] خالد ممدوح إبراهيم ،الجرائم المعلوماتية ، الطبعة الأولى ،دار المفكر الجامعي ،الإسكندرية ،مصر ، 2009، ص75.

[2] عبد الصديق الشيخ ،الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكمولوجيات الإعلام والإتصال ومكافحتها .مقال منشور بمجلة معالم الدرسات القانونية والسياسية ،المجلد04 العدد01،السنة 2020،ص193.

الحاصل في الآونة الأخير[1]. فالجريمة الإلكترونية لا تعترف بالحدود المكانية والزمانية فالعالم كله يمكن أن يكون مسرحا لإرتكاب الجريمة كما لا يحددها زمان معين رغم الإختلاف

في المواقيت بين الدول وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات المتابعة الجزائية وهذه الطبيعة التي تتميز بها الجريمة الإلكترونية ، كونها جريمة عابرة للحدود خلفت العديد من المشاكل حول تحديد الدولة صاحبة الإختصاص القضائي لهذه الجريمة وكذلك حول تحديد القانون الواجب التطبيق وكذلك إشكاليات تتعلق بإجراءات قضائية ، ويعد ذلك من بين الأسباب التي تستدعي ضرورة تفعيل التعاون الدولي بشأن مكافحة الجريمة الإلكترونية .[2]

ثالثا:جريمة ناعمة وسريعة التنفيذ :

إن كانت الجريمة بصورتها التقليدية كالسرقة والقتل تحتاج الى جهد عضلي فان الجريمة الإلكترونية لاتحتاج إلى العنف أو سفك الدماء فإن نقل البيانات من حاسب إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف او تبادل إطلاق نار مع رجال الأمن بل تعتمد على الذكاء وإكتساب مهارات تقنية عالية للحاسب الآلي لذلك سميت بالجرائم اللطيفة [3] فركنها المادي لايتجاوز مجرد كبسة زر فهي تستهدف المعنويات لا الماديات التي تتطالب جهدا ذهنيا وتقني، فتنصب على المعلومات والبيانات المخزنة في نظام الحاسوب ووسائط التخزين عن الطريق تغيريها أو إتلافها أو نسخها أوتلاعب بها ومحويها، وبتالي بإن العلاقة بين مدى الدراية بالجوانب الفنية و باتقنيات الحاسب الآلي وبين الجريمة الإلكترونية علاقة طردية فكلما زادت خبرة الأفراد بمعرفة تقنية الحاسوب زاد إحتمال لستخدام خبرتهم بشكل غير مشروع.

---

[1] خلفي الزوبير ،الجرائم الماسة بتكنولوجيا افعلام والإتصال في التشريع الجزائري،مذكرة ماستر ،في القانون الجنائي 2023/2022 ص14.

[2] الطاهر ياكر ،الجرائم الإلكترونية ، الأحكام الموضوعية والإجرائية ، دراسة مقارنة ، دار بلقيس للنشر ، الجزائر، 2024 ص31.

[3] نادية بوراس ، محاضرات الجريمة الإلكترونية ،جامعة محمد لمين دباغين ، سطيف (02)،كلية الحقوق والعلوم السياسية قسم حقوق السنة الجامعية 2022-2023 ، ص7

رابعا :جريمة يصعب إكتشافها .

تتصف الجريمة المعلوماتية بأنها جرائم خفية ومستترة وإكتشافها في كثير من الأحيان يكون بمحض الصدفة ، حتى الضحية لا يلاحظ وقوعها رغم إنها قد تقع أثناء تواجده على الشبكة ذلك لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة ، كإرسال فيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها ، والتجسس وتنصت على المكالمات وغيرها من الجرائم كما أن نشاط الجاني لايمكن رؤيته ، بحيث يتم بنقل معلومات على شكل نبضات غير مرئية لأنها غالبا ما تكون مرمزة ومشفرة كما له القدرة أيضا على تدمير أدلة الإدانة في وقت قياسي لايستغرق إلا بعض الثواني وهذا مايصعب إكتشاف هذه الجرائم ولأن مستعملي تكنولوجيا الإعلام والإتصال غير مجبرين على الكشف عن هويتهم عند إستعمالهم لهذه التكنولوجيات وخاصة عند تواصلهم بشبكة الإنترنت يكون من الصعب التوصل إليهم هذا ما أدى إلى فرار الكثير من مرتكبي جرائم من الجزاء[1] ، وخاصة في الدول التي لاتملك التقنية والمهارات الازمة في مؤسساتها الأمنية أوخلال التحقيق في تلك الجرائم من قبل سلطاتها القضائية، والدليل العملي في ذلك أنه لم يكتشف من هذه الجرائم إلا1% فقط وما تم الإبلاغ عنه لا يتعدى10% والقضايا المطروحة أمام القضاء لم تكن أدلتها كافية إلا في حدود الخمس .

خامسا: جريمة يصعب إثباتها .

الأصل في الجريمة إقامة الدليل وإسناده للمتهم غير أنه ما يميز الجريمة الإلكترونية عن غيرها من الجرائم بأنها صعبة الإثبات وهذا راجع إلى غياب الدليل الفيزيقي للجريمة مثل البصمة ، و الشعر والدم الذي يدين مرتكب الجريمة ، حيث يسهل محو الأدلة وتلاعب بها فالجاني لايترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه وهذا يعسر كثيرا من إجراءات إكتشاف الجريمة ومعرفة مرتكبها و لكونها تتم في فضاء إفتراضي يصعب على المحقق العادي

[1]نهلا عبد القادر المومني ، الجرائم المعلوماتية ،دار الثقافة للنشر والتوزيع ،عمان ، الاردن ،الطبعة الاولى ،2008،ص51-52.

التعامل معها، هذا نوع من الجرائم يحتاج إلى شرطي إلكتروني ومحقق إلكتروني وقاضي إلكتروني[1].

لذلك فإن التحقيق في الجريمة المعلوماتية يستلزم طرق خاصة مستحدثة للإثبات والوصول إليها وذلك بتدريب وتعليم المختصين على كل العلوم الحاسب الآلي والإلمام بتقنيات تكنولوجيا الإعلام والإتصال قد يسهل إستخلاص الدليل الإلكتروني من بيئته الإفتراضية وتحقق من سلامته و يتطلب لذلك أن تقوم سلطة التحقيق بالتدريب والتأهيل اللازمين والإستعانة بذوي الخبرة والكفاءة حتى تكون أعمالهم في التحري والتحقيق على قدر من المهنية التي يمكن من خلالها تقديم دليل إلكتروني موثوق إلى القضاء[2].

مع العلم أن الدليل الإلكتروني يترك دائما آثارا في حالة محوه أو تعديله والخبير فقط من يكتشف التلاعبات التي تحدث في النظم المعلوماتية التي يحدثها المجرمون لمحو آثار جرائمهم والآثار التي توصل إليهم، وسيكون في هذا الموضوع توضيحات أكثر عند التطرق للآليات البحث والتحري عن جرائم المتصلة بتكنولوجيا الإعلام والإتصال في الفصل الثاني من هذه الدراسة .[3]

سادسا : إمتناع المجني عليه عن التبليغ :

تتصف الجريمة الإلكترونية بتكتم وعد الإبلاغ عنها ممن وقع ضحيتها وعدم الكشف عنها يرجع إلى خوف الضحية من الفضيحة وتشهير كما هو الحال في الجرائم التي تمس خصوصية الأفراد وسمعتهم وشرفهم وحتى المؤسسات المالية و المصارف والشركات التجارية الضخمة تتفادى التبليغ عن الجرائم خوفا من الإضرار بمركزها المالي وحفاظا على شعور المساهمين

---

[1] طاهر ياكر ،مرجع سابق ،ص33.

[2] خالد ممدوح ابراهيم ، مرجع سابق ، ص73.

[3] أحمد مسعود مريم ،آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوءالقانون رقم 04/09،مذكرة ماجستر، قانون جنائي ،جامعة قاصدي مرباح كلية الحقوق والعلوم السياسية ، ورقلة ،2013/2012،ص12.

[3] عفيفي كمال عفيفي ، مرجع سابق ، ص22.

بالائتمان وعدم زعزعة ثقتهم[1]، وخوفا أيضا من أن تؤدي أعمال التحقيق التي تقوم بها الشرطة الى إحتجاز حواسيبها وتعطيل شبكتها لفترة طويلة مما قد يتسبب في زيادة خسائرها المالية ففي أحد الوقائع تعرض أحد البنوك في بريطانيا لسرقة ثمانية مليون جنيه إسترليني، من إحدى أرصدته إلى رقم في سويسرا وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته قام البنك بدفع مليون جنيه له بشرط إلتزام الفاعل بعد الإعلام عن جريمته في مقابل إعلام البنك عن الآلية التي نجح من خلالها في إختراق نظام الأمن لحاسوب البنك الرئيسي[2].

سابعا:جريمة فادحة الإضرار:

إن إزدياد إعتماد البنوك والشركات والمؤسسات على الحاسب الآلي في تسييرها أدى إلى زيادة ومضاعفة ، الأضرار والخسائر التي تخلفها الإعتداءات على المعطيات ، فبرغم من عدم وجود إحصائيات دقيقة للخسائر لناجمة عن الجرائم المعلوماتية، إلى أنه أشارت التقديرات إلى ضياع نحو1.5مليار دولار أمركي[3]، أكدت "إنتل سكيوريتي" الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات أن قطاعات الأعمال العالمية تتكبد خسائر سنوية تصل إلى400 مليار دولار أمركي ، وأوضحت الشركة أن الهجمات الإلكترونية أصبحت إقتصادا متناميا قائما بذاته إذ تبلغ قيمته مابين2 إلى3 ترليون دولار سنويا ، أوما يشكل 15إلى 20 بالمئة من القيمة الإقتصادية الناتجة عبر الأنترنت[4]، وقد تكبدت شركة بريطانية خسائر بلغت 1.3 مليار دولار بسبب هجوم إلكتروني واحد، وخسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة ، وإن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة الملكية الفكرية تتسبب بخسارة للأفراد بحوالي 160مليار دولار، وذكرت الدراسة إن الجريمة الالكترونية تعتبر صناعة

---

[2] شنتير خضرة، مرجع سابق ص17.

[3] نور الدين بن سولة ، الجرائم الإلكترونية في ضوء التشريع الجزائري ،مقال منشور في مجلة الحوار المتوسطي ، المجلد التاسع ، العدد31، 2018/3/1.ص274.

[4] إنتل سيكوروتي: خسائر قطاعات الأعمال من الهجمات الإلكترونية تصل إلى 400مليار دولار سنويا ،االبوابة العربية للأخبار التقنية ، تاريخ الإطلاع 2025/05/10 15:56.

نامية تضر بالتجارة والقدرة التنافسية والإبتكار كما أنها تبطئ وتيرة الإبتكار العالمي من خلال تقليل معدل العائد للمبدعين والمستثمرين.

المطلب الثاني :أركان جريمة تكنولوجية لإعلام ولإتصال.

إذا كانت الجريمة الإلكترونية تنفرد بمميزات خاصة بها تجعلها مختلفة عن غيرها من الجرائم التقليدية لأن ذلك لا يعني خروجها عن المبادئ العامة التي تحكم التجريم والعقاب فجرائم تكنولوجيا الإعلام والإتصال مثلها مثل غيرها من الجرائم يشترط لقيامها توافر ثلاثة أركان أساسية يحددها المشرع مسبق بنصوص قانونية واضحة طبقا لمبدأ الشرعية الجزائية.

تعتبر أركان الجريمة جزاءا لا يتجزأ من طبيعتها وتركيبتها، وتخلف أحدها يؤدي إنتفاء الجريمة بأكملها ، لذا يتطلب القانون كأصل عام ركن مادي وركن معنوي، وركن شرعي بموجبه يتم التجريم والعقابة،وهو الأمر المعمول به في كل الجرائم تقليدية كانت أم مستحدثة مع إحتفاظ هذه الأخيرة ببعض الخصوصيات المتعلقة أركانها الثلاثة كما يأتي بيانه فيما بلي:

الفرع الأول :الركن الشرعي لجرائم تكنولوجيا لإعلام والإتصال .

بعد توفر الشرط الإفتراضي والأساسي للجريمة المعلوماتية ألا وهو نظام المعالجة الآلية للمعطيات، يظهر الركن الشرعي لها والذي يمثل النموذج القانوني والصفة الغير مشروعة للفعل إذ يعد الركن الشرعي السند القانوني لتجريم الفعل وذلك تطبيقا لمبدأ الشرعية "لا جريمة و لاعقوبة إلا بنص" ومعنى ذلك حصر جميع الجرائم والعقوبات في نص القانون بحيث لا يمكن توجيه أي اتهام ضد شخص لإرتكابه فعل معين، مالم يكن منصوص على هذا الفعل في القانون[1]، كما لا يمكن توقيع العقوبة مالم يكن منصوص عنها ومحددة سلفا في القانون لايجوز القياس في التجريم وإعمالا لذلك جرم المشرع الجزائري الأفعال الماسة بتكنولوجيا الإعلام

[1] طاهر ياكر مرجع سابق، ص38.

والإتصال بموجب القانون 15/04 المؤرخ في 10نوفمبر 2004 لذي جرم بعض الصور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبها في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من الفصل الثالث المعنون بالجنيات والجنح ضد الأموال من الباب الثاني المتعلق بالجنيات والجنح ضد الأفراد وذلك في المواد من 394 مكرر الى 394 مكرر 08 من قانون العقوبات المعدل ومتمم في حين جاء القانون 04/09 المتضمن لقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بعد إجراءات وقائية وقمعية في مكافحة الجريمة المعلوماتية بمختلف صورها وأشكالها[1] .

ولم يكتفي المشرع الجزائري لذلك فرض حماية جنائية على الحياة الخاصة للأفراد من خلال قانون رقم :23/06 المؤرخ في 20 ديسمبر 2006 والذي المادة 303 وإقراره بالمادة 303 مكرر 3 وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة، فهذا يعني أن المشرع نص تجريم الفعل المرتكب لاجريمة ولا عقوبة أوتدبير أمن إلا بنص ، والمشرع الفرنسي فصل بين جرائم الإعتداء على نظام المعالجة الآلية للمعطيات وبين جريمتي تزوير المستندات المعالجة الآلية للمعطيات وإستعمالها ،كذلك تجريم كل الإعتداءات على نظام المعالجة الآلية وإستعمالها.[2]

وتجدر الإشارة أنه ثار إختلاف حول إدماج النصوص القانونية الجديدة الخاصة بالجريمة الإلكترونية في قانون العقوبات أو في قانون خاص، فظهر هناك من إدمجها في جرائم الأموال باعتبار أنه يمكن إضفاء صفة المال على كيانات المادية والمعنوية للحاسوب، والبعض الآخر يفضل إدماجه في إيطار الجزء الخاص بالجرائم ضد الملكية الفكرية باعتبار الكيان المادي للحاسوب عناصر مادية قابلة للتملك كما أن الكيان المعنوي يدخل في إطار الملكية الفكرية وهناك من يرى إضافة جزء آخر بالجرائم المعلوماتية مستقل عن الأجزاء التقليدية باعتبار أن هته الجرائم تتعلق بقيم إقتصادية جديدة لها طابع خاص ، والإتجاه الثالث يرى أنه لابد من إلحاق كل

---

[1] الطاهر ياكر مرجع نفسه ص39.

[2] إيمان بغدادي،أثرتعديل قانون العقوبات الجزائري في التصدي ، للجريمة الإلكترونية ،مجلة أفاق للبحوث والدراسات سداسية ، دولية محكمة ،المركز الجامعي ، إيليزي ص188 .

جريمة معلوماتية بما يقابلها في قانون العقوبات التقليدي مثل : وضع جريمة التزوير لمعلوماتي في باب المحررات،لإعتداء على المعطيات .....الخ[1]

الفرع الثاني:الركن المادي للجريمة الإلكترونية .

يقصد بالركن المادي للجريمة وجود فعل خارجي له طبيعة ملموسة تحركها الحواس الركن المادي يعني بصورة خاصة الواقعة الإجرامية التي يتكون منها السلوك المادي الخارجي الذي ينص القانون على تجريمه ،أي كل مايدخل في كيان الجريمة وتكون له طبيعة مادية فتلمسه الحواس وهو ضروري لقيام الجريمة إذ لايعرف القانون جرائم بدون ركن مادي لذلك سماه البعض بماديات الجريمة [2].

والجريمة الإلكترونية ليست مثل أي جريمة تستلزم وجود أعمال تحضيرية إذ أنه يصعب الفصل بين العمل التحضير والبدء في التنفيذ، حتى وإن كان القانون لايعاقب على الأعمال التحضيرية إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشئ فشراء برامج الإختراق ومعدات لفك الشفرات وكلمات المرور وحيازة صور دعارة للأطفال أو حتى بعض الفيروسات التي لم يتم إطلاقها الالكترونيا ,كل هذه الأفعال تمثل جريمة في حد ذاتها .[3]

ويتكون الركن المادي للجريمة الالكترونية من السلوك إجرامي والنتيجة والعلاقة السببية علما أنه يمكن تحقيق الركن المادي دون تحقيق النتيجة كالتبليغ عن الجريمة قبل تحقيق نتيجتها وتأسيسا على ذلك فإن الفقه القانوني إشترط لقيام الركن المادي ثلاثة عناصر أساسية المتمثلة في:

---

[1]علي عبد القادر القهوجي ،الحماية الجنائية لبرامج الحاسب الآلي،دار الجامعية للطباعة والنشر ،دون طبعة ،لبنان،سنة1999 نص35.

[2]الطاهر ياكر مرجع سابق ص39.

[3]عبد الفتاح حجاز بيومي ،جرائم الكمبيوتر والانترنت ،دار الكتب القانونية ،مصر 2004،ص113.

أولا السلوك الإجرامي : ويقصد به ذلك النشاط الذي يصدرعن إرادة الإنسان والذي يظهر في العالم الخارجي ، ويأتي في صورتين فقد يكون فعل إيجابي بمعناه الدقيق أي إتيان فعل ينهى عنه القانون وإما في شكل سلوك سلبي وهو الإمتناع عن القيام بفعل يأمر به القانون.[1] وفي الجريمة المعلوماتية يمكن أن نجده بنوعيه السلوك الإيجابي والسلبي لاننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي يتطور بتطور الوسائل التي وجدت بين يدي الفاعل وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية والتي إستطاعت أن تخرج من تقليدية السلوك الإجرامي إلى مساحات أكتر تعقيدا أو وجدت بلاشك صعوبات كثيرة[2].

ثانيا: النتيجة الإجرامية : ويقصد بها الأثر المادي الذي يحدث ، فالسلوك قد أحدث تغيرا ملموسا ومفهوم النتيجة يقوم على أساس مايعتد به المشرع وما يترتب عليه من نتائج بغض النظر عن ما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.

ثالثا العلاقة السببية : حتى يتم الركن المادي بعناصره كافة لابد من أن تكون هناك علاقة سببية بين السلوك الإجرامي الذي أتاه الجاني ونتيجة الحاصلة بحيث يمكن القول أن هذه النتيجة من ذلك السلوك فإن إنتفت العلاقة السببية فلا مجال لمسائلة الفاعل ،وبذلك فإن العلاقة السببية تلعب دورا هما في رسم حدود المسؤولية الجنائية[3].

ويختلف الركن المادي في الجرائم الماسة بتكنولوجيا الإعلام والإتصال، من جريمة لأخرى ففي جريمة الدخول غير المشروع الذي نصت عليها المادة 394 مكرر من قانون العقوبات حيث يتمثل الركن المادي في هذه الجريمة ، في النشاط الإجرامي المتمثل في فعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات أو جزء منه ، فمجرد الدخول تقوم به الجريمة حتى ولو لم يترتب على دخوله ضرر، أو يتحقق من وراء الدخول فائدة طلما أن ذلك الدخول

---

[1] محمد أمين شوابكة ،جرائم الحاسوب والانترنت (الجريمة المعلوماتية)،دار الثقافة للنشروالتوزيع،عمان الاردن ،2009،ص16.

[2] عبد الفتاح بيومي حجازى، جرائم الكمبيوتر والأنترنت ، مرجع سابق ص114.

[3] جلال محمد الزغبي ،جرائم تقنية نظام المعلومات الإلكترونية ،دار الثقافة ،عمان 2010،ص54.

غير مشروع ويتحقق فعل الدخول إلى النظام عن طريق الغش[1] أما في جريمة البقاء غير المشروع فقد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام ، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات وتعد هذه الجريمة من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة إجرامية معينة فيكفي البقاءغير الصرح به داخل النظام المعلوماتي ليقوم الركن المادي لهذه الجريمة بالإظافة إلى أنه يصعب تقديم دليل على إثباتها حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الإنفصال عن النظام المعتدي عليه[2] ويتمثل الركن المادي في جريمة الإعتداء العمدي في أن النشاط الإجرامي فيها ينحصر في أفعال الإدخال والمحو والتعديل يكفي توافر إحداها لقيام الجريمة فلا يشترط إجتماعها معا ، حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن المادي في الجريمة وهناك جرائم الإعتداء العمدية على المعطيات ، داخل النظام المعلوماتي أو خارجه نص عليها المشرع في المادة 394مكرر 1 من ق.ع وهي إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزال أوتعدل بطريق الغش المعطيات التي يتضمنها، بمعنى إدخال بيانات لم تكن موجودة في نظام المعالجة الآلية، بقصد التشويش على صحة البيانات أو محو وإزالة جزء من المعطيات المسجلة على الدعامة أوتحطيم تلك الدعامة أوتعديل المعطيات الموجودة داخل النظام وإستبدالها بمعطيات أخرى ويتحقق هذ الفعل عن طريق برامج غريبة تتلاعب في المعطيات سواء بالمحو جزئي أو كلي باستخدام قنبلة المعلوماتية الخاصة[3] بمعطيات برامج الممحاة أو برامج الفيروسات بصفة عامة، ومما سبق نجد أن هذه الأفعال(الإدخال والمحو والتعديل)جاءت على سبيل الحصر وبالتالي لا يقع تحت طائلة التجريم أي فعل آخر غيرها كانسخ المعطيات أونقلها[4].....إلخ .

---

[1] غنية باطلي ،الجريمةالإلكترونية (دراسة مقارنة)،دون طبعة ،منشورات الدار الجزائرية ،2016،ص35 .

[2] عبد القادر مصطفاوي، الأليات الجزائية والموضوعية لمواجهة الجرئم المتصلة بتكنولوجيا الإعلام والإتصال،أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة الجزائر 1،كلية الحقوق ،2021- 2022 ص93.

[3] عبد القادر مصطفاوي ،مرجع نفسه.

[4] مسعود خثير،الحماية الجنائية لبرامج الكمبيوتر ،أساليب وثغرات ،طبعة 10 ،دار الهدى ،الجزائر ،2010 ، ص124.

أما الجرائم العمدية على المعطيات الموجودة خارج النظام نصت عليها المادة 394 مكرر2 من قانون العقوبات " وهي كل من يقوم عمدا أو عن طريق الغش بتصميم أوبحث أو تجميع أوتوفير أو نشر أو الإتجار في المعطيات المخزنة المتحصل عليها من الجرائم المنصوص عليها في هذ القسم"هذه المادة تهدف الى حماية هذه المعطيات من إستعمالها في أغراض غير مشروعة كالمنسفات الغير المشروعة كالإرهاب والتحريض على الفسق ...الخ[1].

الفرع الثالث الركن المعنوي : هو السلوك الذهني أو النفسي للجاني بإعتباره محور القانون الجنائي ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية ، ويقوم الركن المعنوي للجرائم المرتكبة عبر الإنترنت على أساس مجسد في توفير الإرادة الإجرامية لدى الفاعل وتوجه هذه الإرادة للقيام بالعمل الغير مشروع الذي جرمه القانون[2]، كإنتحال شخصية المزود عبر الإنترنت وسرقة أرقام البطاقة الإئتمان ويختلف الركن المادي في الجريمة المعلوماتية من جريمة إلى أخرى فمثلا جريمة الدخول الغير الصرح به إلى نظام الحاسوب الآلي تتطلب قصدا جنائيا عام يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج ، داخل النظام المعلوماتية بشكل غير مصرح يعد جريمة، باعتبار حماية المشرع لمحل الحق وهو الجهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج وعلى النحو فدخول إلى نظام الحاسب الآلي خطأ أو سهو ينفي عنه شرط القصد الجنائي فور علمه بدخول غير الشرعي وفي الجريمة الإحتيال لإلكترونية التي بدورها جريمة عمديه ، يتطلب المشرع لقيامها القصد الجنائي لقيام مسؤولية الجاني بنوعيه الخاص والعام فالمجرم يعلم أنه يخالف القانون. وبرغم من ذالك يقوم بالفعل.

المبحث الثاني:المجرم الإلكتروني وسماته .

رغم أن الجريمة الإلكترونية تقترب من الجريمة التقليدية من حيث الأركان العامة والمجني عليه والموضوع إلى أنها تختلف عن الجريمة العادية من حيث الصفات الفاعل ومميزاته وطبيعة

[1] مريم أحمد مسعود،مرجع سابق، ص.39

[2] طاهر ياكر مرجع سابق، ص42 .

السلوك الإجرامي المنفرد نظرا لخطورة الجريمة المعلوماتية ، ومن خلال ما سبق تتضح لنا الأهمية البالغة التي يكتسبها هذا الموضوع ، سنحاول تحديد مفهوم المجرم الإلكتروني وبالأخص مجرم المعلوماتي ، بإعتباره من المجرمين المتمردين ، ودراسة سلوك الإجرامي لهذ المجرم من خلال تحديد الدوافع والسمات الإجرامية التي ينفرد بها عن غيره من المجرمين .

المطلب الأول: مفهوم المجرم الإلكتروني .

إن الجريمة المعلوماتية لاتسمح لنا بأن نكون بصدد مجرم عادي، بل أمام مجرم يتمتع بمهارات تقنية ويكون على دراية شاملة بعلم التكنيك المستخدم في نظام الحاسب الآلي والإنترنت فشخصية المجرم ألمعلوماتي سواء كان طبيعيا أو معنويا والآليات التي إستعملها لإرتكاب الجريمة تجعل منه شخصا يتسم بصفات خاصة تضاف إلى الصفات الأخرى التي تتوافر في المجرم العادي الأمر الذي يستدعي القيام بالبحث عن مفهوم المجرم المعلوماتي من خلال إعطاء تعريف دقيق له وكذلك إلى تحديد أهم الأصناف وسمات.

الفرع الأول: تعريف المجرم الإلكتروني.

يطلق فقهاء القانون الجنائي على مرتكب الجريمة المعلوماتية مصطلح المجرم المعلوماتي وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الآلي الإلكتروني، والقادر على استخدام هذا التكنيك لإختراق الكود السري لتغير المعلومات أولتقليد برامج أو تحويلها عن طريق الحاسوب نفسه[1] والقادر على تحويل ناوياه إلى لغة رقمية بإستخدام التقنية الرقمية المعلوماتية وذلك بأداء فعل أو الإمتناع عنه هذا الصنف من المجرمين لديهم تأثير خطير جدا على الأشخاص الطبعين صغار كانوا أوكبارا ، أوعلي الأشخاص المعنويين كالمؤسسات والدولة ، فالمجرم لمعلوماتي لايحتاج الى التنقل الحركي لمكان وقوع الجريمة بل يقوم بالفعل الإجرامي عن بعد من حيث الزمان والمكان بإستخدام خطوط وشبكات

[1] هدى حامد قشقوش, مرجع سابق ، ص27

الإتصال بين الجاني ومكان وقوع الجريمة ، ومثال ذالك مقام به الطالب الأمريكي حين عمد سنة1981 برفقة أصدقائه إلى إستعمال خط الهاتف للدخول إلى ملفات سرية مخزنة في حاسوب تابع للحكومة الفدرالية الأمركية[1] .

الفرع الثاني أصناف المجرم المعلوماتي :

إن سهولة التعامل مع الإنترنت قد أد إلى عدم إمكانية حصر من يرتكبون الجرائم المعلوماتية في طبقة أو فئة معينة أو جنس معين ، فقد يكون مرتكبوها من البالغين أو الأحداث أو المثقفين ومن الفقراء أو الأغنياء وسواء كانوا من الرجال أو من النساء، تبعا لإختلاف الأسباب والدوافع التي أدت إلى إرتكاب هذه الجريمة ، الأمر الذي يستلزم تحديد أصناف المجرمون المعلمتيون ثم إبراز أهم الدوافع والأسباب التي أدت بهم إلى إرتكاب هذا الفعل الإجرامي وذلك وفق التفصيل الأتي :

يعد من أفضل التصنيفات لمجرمي التنقية التصنيف الذي أورده في مؤلفهم جرائم الكمبيوتر الصادر1995 حيث تم تقسيم مجرمي التقنية إلى ثلاث طوائف المخترقون المحترفون، والحاقدون كما من بين التصنيفات الهامة التميز بين الصغار السن من مجرمي المعلوماتية وبين البالغين الذين يتجهون للعمل معا لتكوين المنظمات الإجرامية الخطيرة [2].

أولا: فئة القراصنة أو المخترقون :

يرتكبون جرائمهم بدافع التحدي الإبداعي إذ ينصبون أنفسهم أوصياء على أمن نظم المعلومات في المؤسسات المختلفة وينقسمون إلى قسمين فئة الهاكرز والكراكز:

أ) القراصنة الهاكرز (HACKERS):

---

[1] رضا عسال ،عماد عبد الرزاق ،الجريمة الالكترونية والمجرم المعلوماتي ،مقاربة مفاهمية ،مجلة ببليوفيليا ، لدراسات المكتبات والمعلومات ،العدد 05 ،2020.ص

[2] سهام. خليلي ، خصوصية المجرم الإلكتروني ،مجلة الفكر العدد 15 جوان 2017 ص406.

وهو مستخدم حاسوب متطفل ومستكشف ، غرضه التوصل إلى الدخول غير المصرح به إلى نظم الحاسوب دون قصد الإيذاء أو الإتلاف أو التخريب وذلك لشعوره الذاتي بالسلام والحرية المطلقة في العالم الإفتراضي وولعه الشديد به ، إذ نجده يستغل مداركه التقنية ليخترق كافة الشبكات ويسبح في عالم البيانات ولايقيم أهمية لحواجز كلمات المرور أو الشيفرات وعليه

فهو يقتصر دوره في التسلية ومثال ذلك ما حدث من إختراقات لنظام شركة "مايكروسوفت" سنة 2000 من قبل مجموعة مجهولة[1].

الفئة الغالبة على أفراد هذه الطائفة صغر السن وقلة الخبرة وعدم التميز بين الأنظمة محل الإختراق ومثالها حالة الإختراق أحد الصبية لايتجاوز عمره 17 سنة حيث إخترق كمبيوتر العديد من المؤسسات الإستراتجية في أروبا والولايات المتحدة الأمركية ومن بينها كمبيوتر المتصلة ببرنامج حرب النجوم الذي كان مخطط لتنفيذ من قبل الولايات المتحدة الأمركية في حقبة الحرب الباردة [2].

ب) فئة القراصنة الخبيثون الكراركز :

كلمة كراكر " cracker" كلمة كراكر مشتقة من الكلمة الإنجليزية"to crack " ومعناه الكسر أوالتكسير ، وهي عبارة عن إسم إختاره لأنفسهم مجموعة من المخربين المهرة القادرين على إختراق أي شبكة أو أي جهاز حاسب ، فهم لايقلون مهارة أو كفاءة عن الهاكرز لكنهم يستخدمون هذه المهارة في التخريب والسرقة والحصول على الأموال بطريقة غير مشروعة .[3]

ولقد برز هذا المصطلح عام 1985 ويدل على المجرم الخطير الذي يتسلل بصورة خفية إلى مواقع مختارة بعناية لإرتكاب جريمته سواء أكانت في صورة الإتلاف أو التخريب أو لإرهاب أو الإبتزاز أو العدوان على الأموال بالسرقة والنصب ومثاله ما حدث في محدثات السلام

---

[1] سهام خليلي،مرجع سابق ،ص405

[2] سعيدي سليمة ، حجاز بلال مرجع سابق ص26-27.

[3] عبد الفتاح بيومي حجازي،مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت ،دار كتب القانون ، مصر ،2007،ص30

في" كامب ديفد" الثانية من إختراق لنظام توزيع البريد الإلكتروني للصور التابع لوزارة الخارجية الأمركية[1] ويمكننا تقسيم الكراكرز الى:

1. المحترفون :

غالبا ما يحملون درجات جامعية عالية في تخصصات الكمبيوتر والمعلوماتية ويكنون على دراية ببرامج التشغيل ومعرفة عميقة بالخبايا والثغرات الموجودة .

المحترفون تعد الطائفة الأخطر في مجرمي التقنية لأنها تتميز بسعة الخبرة والإدراك الواسع للمهارات التقنية وكذلك تهدف إعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجهات التي تكلفهم لإرتكاب الجرائم الإلكترونية كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي وهم يقومون بالتسلل داخل النظام المعلوماتي وتحطيم البيانات وتجدر الإشارة إلى أن هذه الطائفة معظمها من الشباب الأكبر سنا الذي تتراوح أعمارهم بين 40/25 سنة.[2]

2. الحاقيدون :

هي أقل خطورة ويغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين السابقتين بل الدافع من أفعالها غير المشروعة هي الرغبة في الإنتقام والثأر لتصرف صاحب العمل معهم وهم ينقسمون إما إلى مستخدمين من النظام كالموضفين مشتركون أو على علاقة بمحل الجريمة ،أو إلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم [3].

---

[1]بكوش محمد الامين ،هروالة نبيلة هبة ،خصوصية المجرم الالكتروني ، مجرم الانترنت نموذجا ،مجلة البحوث في الحقوق والعلوم السياسية ،المجلد 07العدد01 السنة 2021 ص81.

[2]سهام خليلي، مرجع سابق ص408.

3. طائفة صغار السن:

يطلق عليهم البعض الأخر بصغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها....كما أنها تعتبر تلك المجموعات التي تميل إلى التحدي الفكري وهم غالبا مايكونون في فترة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على إقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية ،ومثال على ذلك حالة قيام مراهق بالغ من العمر أربعة عشر سنة بإقتحام جهاز الحاسب الآلي الخاص بالقوات الجوية الأمركية وحصل منها على معلومات عسكرية خطيرة مما أحدث إرتباكاً داخل تلك القاعدة ، أين ترتب عنها إتخاذ قرارات تكلف تنفذيها الكثير من الوقت والجهد والمال[1].

4. **فريكور Phreaker**:

وهو الشخص يخترق أنظمة الإتصالات الهاتفية عن طريق الأفعال والغش والسرقة المعلوماتية للخطوط الهاتفية بغية التقليل من الفواتير الهاتف الخاصة بهم وهو كل شخص لديه القدرة على تقنية على إستكشاف نظام الهاتف لكي يعمل على خدمة الإتصال الهاتفية مجانية ومثال على ذلك قضية كابتن كراش 1971[2].

5. طائفة مجرموا المعلومات أصحاب الأراء المتطرفة :

المتطرفون الفكريون هم من نزلت بهم عقولهم إلى مستنقع الشطط في التفكير ، متطرفون لإفكارهم وآرائهم ، ومتجاوزون بذلك كل حدود المعقولة[3]، والمقبولة لتّحاور والنقاش بخصوص قضية أو غاية ليس لها علاقة بمصالحهم الشخصية ، وهم في سبيل تحقيق ما يعتقدونه على إستعداد لإرتكاب أنشطة إجرامية مختلفة ، وتخلف أرائهم أضرار جسيمة سواء على الأفراد من

---

[1] محمد علي العريان ،الجرائم المعلوماتية ،دار الجامعة الجديدة لنشر والتوزيع ،مصر 2004،ص73.

[2] بكوش محمد الامين ،هروال نبيلة هبة مرجع سابق ص82.

[3] ياسمينة بونعارة، الجريمة الإلكترونية ،مجلة جامعة الأمير عبد القادر للعلوم الإسلامية ،قسنطينة،العدد 39،تاريخ النشر 21جوان 2016 ،ص285.

المجتمع أو على قطاعات كاملة منه هادفين من ذلك تحول المجتمع إلى الأفضل من وجهة نظرهم من دون قيد أو شرط .

الفرع الثالث : خصائص المجرم المعلوماتي .

أ) المجرم المعلوماتي شخص ذكي ومتخصص .

يتميز المجرم الإلكتروني بالذكاء وعدم الميول الإستعمال العنف والقوة ، وهذا الأمر بديهي لأن المجرم الذكي يسعى لإخفاء جريمته بإحكام وذلك بعدم ترك أدلة ضده فيفضل العمل بهدوء ولا يلجأ للعنف الذي يترك دليلا ماديا واضحا لأن الجريمة الإلكترونية توافي شروط عمله كونها تتطلب قدرة ذهنية وعقلية عميقة فهو يستخدم طرقا جديدة لا يعرفها أحد سواه فكلما قلت معرفة الأخرين بالطريقة كلما صعب إكتشافها من طرف عناصر الأمن المتخصصة [1].

يمتلك المجرم الإلكتروني المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية الإلكترونية حيث يستطيع المجرم الإلكتروني أن يُكون تصورا كاملا لجريمته حتى لايتمكن من ملاحقته وتتبع أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكمبيوتر فالمجرم الإلكتروني عادة يمهد الإرتكاب جرائمه بالتعرف على كافة الظروف المحيطة به لتجنب ما من شأنه ضبط أفعاله والكشف عنه[2] .

كما أنه يتمتع بقدرة ومهارات تقنية يستغلها في إختراق الشبكات وكسر كلمات المرور أو الشفرات بغية الحصول على البيانات والمعلومات الموجودة في أجهزة الكمبيوتر ومن خلال الشبكات، وبحسب الدراسة التي أجراها أحد الباحثين في ذلك المجال والتي لخص فيها أن المجرم المعلوماتي هو شخص يتمتع بالذكاء والمهارة في مجال إستخدام التقنيات المعلوماتية فهو:

- يتميز بالقدرة على إختراق النظم المعلوماتية والتلاعب بالأنظمة الأمنية.

---

[1] مصطفى محمد موسى ،أساليب إجرامية بالتقنية الرقمية ماهيتها نمكافحتها ، دراسة مقارنة ،دار الكتب القانونية ، مصر ،2005 ص22 .

[2] طارق ابراهيم الدسوقي عطية ،الأمن المعلوماتي (النظام القانوني لحماية المعلومات)،دار الجامعة الجديدة،القاهرة،مصر الطبعة2009،ص177.

- لديه القدرة الفائقة على المعالجة الإلكترونية للنصوص الكلمات والتعامل مع البرامج .
- يبتكر أساليب متطورة لإرتكاب أفعاله وإخفاء أثارها .

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز اليها "الأستاذ بارك" بكلمة " S K R A M " تعني المهارة المتطلبة لتنفيذ النشاط الإجرامي والتي قد يكتسبها عن طريق دراسة متخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الإجتماعي مع الأخرين[1].

ب) المجرم المعلوماتي شخص إجتماعي :

يتميز مرتكب الجريمة المعلوماتية بأنه شخص إجتماعي فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها أو بدافع الحصول على المال أو بهدف الإنتقام[2] ، إذ أنه يوظف مهاراته في كيفية عمل الحواسيب وتخزين البيانات والمعلومات والتحكم في أنظمة الشبكات وفي الدخول الغير المصرح به مرات ومرات .

ج) المجرم المعلوماتي يتمتع بالخبرة والمهارة:

يتصف مررتكب الجريمة المعلوماتية بأنه على قدرة عالية من الخبرة والمهارة في إستخدام التقنية المعلوماتية ذلك لأن مستوى الخبرة والمهارة التي يكون عليها هي التي تحدد الأسلوب

---

[1] محمد الأمين بكوش، البعد الجديد للإجرام وخصوصية المجرم الإلكتروني،مقال منشور ،المجلة الجزائرية للحقوق والعلوم السياسية ،المجلد 07،العدد02،2022

[2] خالد ابراهيم ممدوح ،مرجع سابق ،ص135.

[3] عبد الفتاح بيومي حجازي ، ،مبادئ الاجراءات الجنائية في جرائم الكمبيوتروالانترنت ،مرجع سابق ص33 .

الذي ترتكب به تلك الجرائم ، فهو يتمتع بالمهارة والمعرفة الكافيتين لإختراق المواقع الإلكترونية وكسر حواجز الشفرة بعكس المجرم العادي في الجرائم التقلدية والذي غالبا مايتميز بالقوة العضلية ونادرا مايتميز بعضهم بالذكاء[1]، بناءا على ذلك لايستطيع أي شخص أن يرتكب الجرائم المعلوماتية دون المعرفة التامة بكيفية التعامل مع جهاز الحاسوب والإنترنت والبيانات والمعلومات بشكل منهجي ودقيق ، كماأنه يُعرف عن المجرمون المعلوماتية خوفهم من إنكشاف جرائمهم وإنفضاح أفعالهم بالرغم من أن هذا الخوف يصاحب المجرمين على خلاف أنماطهم .

د) المجرم المعلوماتي مجرم عائد للإجرام :

يتميز مرتكبو الجرائم الإلكترونية بفرط في النزعة الإجرامية للميل إلى إرتكاب الجرائم وذلك فإن كثيرة من المجرمين يعدو لإرتكاب أنشطة إجرامية أخرى في مجال الكمبيوتر إنطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديهم إلى المحكمة في المرات السابقة ويؤدي ذلك إلى عودة المجرم إلى الإجرام وقد ينتهي به الأمر كذلك في المرة التالية إلى تقديمهم للمحاكمة[2]، والأمثلة على ذلك ماقام به الهاكرز ، البريطاني "جاري ميكنون" GaryMckinnon" الذي إخترق حسابات وكالة الفضاء الأمركية "نسا" بين سنتي 2001و2002، وتم القبض عليه للمرة الأولى سنة2002، ولكن السلطات أفرجت عنه لعدم كفاية الأدلة ، ثم تم القبض عليه مرة أخرى في سنة 2005، وحكم عليه بالوضع تحت المراقبة وبالحرمان من إستخدام الإنترنت[3] .

المطلب الثاني: صورالجريمة الإلكترونية ودوافع إرتكابها.

الفرع الأول :صورالجرائم المتصلة بتكنولوجيا الإعلام ولإتصال في التشريع الجزائري.

---

[2] شنتير خضرة مرجع سابق ص34

[3] غريبي بشرة ،خصوصية المجرم المعلوماتي ودوافعه،مجلة نوميروس الأكادمية ،المجلد الثاني، العدد الثاني،2021،ص 105،.

تصنف الجريمة التقليدية بحسب خطورتها إلى جنيات وهي الأخطروالجنح وهي متوسطة الخطورة ثم المخالفات، وهي أقل خطورة وتصنف بحسب خطورتها إلى جرائم عادية وسياسية وجريمة عسكرية وأخرى إرهابية على إختلاف هذه الجريمة فإن الجريمة الإلكترونية عرفت إختلاف حول تقسيماتها، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة ولبعض الأخر يستند على دوافع إرتكابها وأخرون يؤسسون تقسيماتهم على تعدد محل الإعتداء وتعدد الحق المعتدى عليه أما بالنسبة للمشرع الجزائري فقد قسم الجريمة المعلوماتية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها وبالتالي تشمل جرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على نظام المعلوماتي حددها المشرع بموجب قانون العقوبات وهذا ماسيتم بيانه.

أولا :الجرائم معلوماتية المرتكبة باستخدام النظام المعلوماتي .

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفًا لجسماتها ويهدف الجاني من ورائها إلى تحقيق ربح مادي بطريقة غير مشروعة تستخدم النظام المعلوماتي في حد ذاته أوبرامجه كوسيلة لتنفيذ الجريمة وتنقسم هذه الجرائم بدورها إلى :

جرائم واقعة على الأشخاص وجرائم واقعة على الأسرار[1].

1. جريمة الإعتداء على الأشخاص باستعمال النظام المعلوماتي .

رغم تطور الإنسان في مجال إستعمال النظام المعلوماتي خاصة الآونة الأخيرة ، لم يجعل منه في مأمن من الوقوع ضحية الإستغلال في خصوصيته أو حياته الشخصية من طرف مستعملي البرامج المعلوماتية بطريقة غير شرعية ، ويقصد بجرائم الإعتداء على الأشخاص تلك الجرائم التي تنال بالإعتداء أو تهديد أوتشهير وتمس بحقوقه الشخصية ، وتعد جرائم الشرف من أهم الجرائم التي إنتشرت باستعمال النظام المعلوماتي ومن الجرائم الواقعة على الأ شخاص نجد:

[1] الطاهر ياكر ، مرجع سابق، ص19.

أ) **جرائم السب والقذف والتشهير** : تعتبر من الجرائم التقليدية تصدت لها جميع التشريعات على إختلافها دولية وداخلية ، وهي تمس الأفراد والكينات على حد سواء فعادة ترسل عبارات السب والقذف والتشهير عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب مما يؤدي بكل من يدخل الموقع مشاهداتها أو الإستماع إليها ويتحقق بذالك الركن العلني الذي تتطلبه العديد من التشريعات في السب العلني وإذا لم يتطلع عليه أحد فيمكن تطبيق مواد السب أو القذف غير علني[1].

ب) جريمة التهديد:

عالجها المشرع الجزائري في المادة 284 من قانون العقوبات الجزائري و تصيب المجني عليه سواء كانت فعل مادي أو قول يشكل إعتداء على الحرية المجني عليه يعد تهديد ،أما التهديد الإلكتروني أي حصول فعل التهديد باستعمال وسائل إلكترونية ووسائل أخرى كالهاتف والبرقيات والفاكس وغالبا متكون المعلومات المستخدمة في التهديد ذات طابع محرج لضحية ويمكن أن تؤدي في بعض الأحيان إلى تدمير حياته الإجتماعية، نتيجة تعلقها بمعلومات سرية أو بجهة العمل مما يؤدي إلى إحجام الضحية عن رفع الدوى قضائية ضد المهدد[2].

ب) إنتحال الشخصية :

عالجها المشرع الجزائري في المادة 245من قانون العقوبات الجزائري وإنتحال الشخصية باستعمال تكنولوجيات الإعلام والإتصال عبر مواقع الإنترنت ومواقع التواصل الإجتماعي وغيرها من الموضوعات المهمة، وتصف هذا النوع من الجرائم بالخفاء حتى الضحية لا يمكنّ إن يلاحضها رغم وقوعها أثناء تواجده على الشبكة وتتميز بالسرعة والتطور في إرتكابها وذالك راجع لتطور التكنولوجي المتسارع.

---

[1] سمية مزغي ،جرائم المساس با لأنظمة المعلوماتية ،مذكرة مقدمة لنيل شهادة الماجستير ،كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر بسكرة 2014،ص26

[2] نجم محمد صبحي ،جرائم الواقعة على الاشخاص ط1،مكتبة دار الثقافة ،القاهرة ،مصر 1994نص153وبعدها ،للمزيد ،انظر في ذلك سارة محمد حنش ،مسؤولية الجزائية عن التهديد عبر الوسائل الالكترونية دراسة مقارنة مذكرة مقدمة لنيل شهادة الماجيستر في القانون العام ،جامعة الشرق الاوسط ،لبنان 2020ص20.

ت) المواقع مخلة بالحياء(الإباحة الجنسية) :

تعد من أكثر الجرائم تأثيرا على الأشخاص والمجتمع ،إذ يعمد الجاني على عرض صور أو فيديوهات على شبكة الإنترنت أو مواقع معينة تحتوي على ممارسات منافية للقيم الأخلاقية لا تستثني لا الكبير ولاالقاصر، مما يزيد في المساس بالكيان المجتمعي. ويعمل القائمون على هذه الأفعال بالترويج إلى أعمال معينة يمكن أن تكون تجارية أو غيرها بعرض صور أو مقاطع ليفيديو وهدا من قبيل الغزو الفكري للمجتمعات المحافظة[1].

2. الجرائم الإلكترونية الواقعة على الأسرار .

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة ،ويتخذ هذا النوع من الجرائم صورتين الأولى تتعلق بالجرائم الواقعة على أسرار الدولة حيث أتاح الإنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والإقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات والثانية تتعلق بالجرئم الواقعة على أسرار المهنية والهدف من إرتكاب هذه الجريمة هو سرقة المعلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الإمتناع عن القيام بعمل[2] ،وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنيات والجنح ضد الشئ العمومي في المادة 61إلى المادة 96مكرر من قانون العقوبات بالإضافة إلى المادة 394مكرر 03 التي تنص على تضاعف العقوبات المنصوص عليها في هذاالقسم إذ أستهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.

---

[1] بغداد ادهم بسام ،وسائل البحث والتحري عن الجريمة الالكترونية مذكرى مقدمة لنيل شهادة الماجستير ،جامعة النجاح الوطنية غزة ،فلسطين ن2018ص9.

[2] رحموني محمد ،خصائص الجريمة الإلكترونية ومجالات إستخدامها ،مجلة الحقيقة ،العدد41،2018،ص447.

3. جرائم معلوماتية الواقعة على الأموال :

الأموال تشمل كل ما يملكه الإنسان من عقارات منقولات سندات .. إذ وجب الحفاظ عليه وحمايته من السرقة وغيرها من الأفعال التي تؤدي به إلى الضياع ، وقد تقع هذه الأفعال على الواقع كاسرقة والإختلاس ، أوقد تقع عليه بواسطة الوسائط الإلكترونية بأفعال تمثل في مجملها التجارة الإلكترونية، و جرائم التحويل الإلكتروني للأموال وجريمة غسيل الأموال عبر الإنترنت وقد تدخل المشرع الجزائري في حماية هذه الأموال عن طريق سن مجموعة من القوانين والتدابير توفر الحماية والردع[1] نذكر منها :

أ) **السرقة الإلكترونية** :هي أحد أنواع الجرائم الإلكترونية، وتتمثل في الخداع والإستغلال غير مشروع من قبل مستخدمي شبكة الإنترنت، حيث يقوم الجاني بأساليب ووسائل منظمة ومخطط لها بإستخدام بعض المعلومات الإلكترونية أو التواصل مع بعض الأشخاص بهدف الإحتيال عليهم ، للحصول على معلومات شخصية أوسرية أويستلم الجاني أملاك وأموال مملوكة للغير بدون حق، مما يؤدي وقوع المجني عليه ، ضحية للجريمة من مصادر إلكترونية[2] وإن كل من جريمة السرقة الإلكترونية وجريمة السرقة العادية يقومان على أساس أستلاء الجاني على أموال غيره ، لذلك لم يشرع المشرع الجزائري نصوصا قانونية تجرم وتعاقب مرتكبي جريمة السرقة الإلكترونية، ويطبق القضاء الجزائي الجزائري الأحكام القانونية العامة المتعلقة بالسرقة العادية على السرقة الإلكترونية .[3]

التحويل الإلكتروني للأموال :يعتبر التحويل الإلكتروني غير المشروع للأموال كأحد أنواع الجريمة المعلوماتية باعتبارها جريمة تتسم بالحداثة نظرا لإرتباطها بتكنولوجيا المعلومات ، ونظرا لإعتماد البنوك على التحويل الإلكتروني للأموال في الوقت الراهن يتم إستخدام الأنظمة المعلوماتية في

---

[1] القانون الجزائري رقم 18-05 المؤرخ في 10ماي 2018 ،المتعلق بالتجارة الإلكترونية نج.ر.ج العدد 28 المؤرخة في 16 ماي 2018،ص04،ص10.

[2] محمد طيب عمور ،السرقة الإلكترونية تكيفها الشرعي وطرق اثباتها ،مقال منشور في مجلة الاحياء الصادرة عن جامعة الجلفة المجلد 19 العدد22 سنة 2019ص410.

[3] سمية مزغي ،المذكرة السابقة ،ص40.

الصارف والمؤسسات النقدية لعمليات التحويل بشكل يومي، والتحويل الإلكتروني للأموال أو النقل المصرفي يعني عملية يقيد البنك بمقتضاها مبلغا معينا في الجانب المدين من حساب الأمر بالنقل بناء على أمر كتابي ، منه وفي جانب الدائن من حساب آخر[1]، وقد تناول المشرع الجزائري عملية التحويل المصرفي في المادتين 543 مكرر19و543 مكرر من القانون الجاري رقم 02/05المؤرخ في 06 فيفري 2005 المعدل ومتمم للأمر الجزائري رقم 75-59.المتضمن القانون التجاري الجزائري. [2]

وتتم عملية التحويل الإلكتروني للأموال داخل بنك واحد ، وهذه العملية أيضا قد تتم بين بنكين مختلفين ، ويكون لكل بنك عمله الخاص ،وقد يكون هناك بنك ثالث ويسمى البنك الوسيط لتسوية عملية التحويل، ويأخذ التحويل الإلكتروني العديد من الصور نذكر منها الإحتيال على النظام المعلوماتي ويعد من أهم الجرائم التي ترتكب في مجال التكنولوجيا المعلوماتية ونجد أيضا الإحتيال باستخدام بطاقة الدفع الإلكتروني تعرضت هذه الأخيرة إلى عدة إستعمالات غير مشروعة من قبل حاملها والغير ،فتقع الجريمة على بيانات بطاقة الإتمان الإلكترونية أو إساءة إستخدامها وتتعدد صور التحويل الإلكتروني ، من غسيل أموال باستعمال تكنولوجيات الإعلام والإتصال ، خيانة الأمانة في النطاق المعلوماتي التي نص عليها المشرع في المادة 376 من قانون العقوبات الجزائري....الخ.

4. الجرائم المعلوماتية الماسة بأمن الدولة :

تتمثل في الإعمال الإرهابية التي نص عليها المشرع في المادة 87 من قانون العقوبات الجزائري ولا تنحصر الأعمال الإرهابية على القتل أو الإغتيالات والخروج عن القانون بل تستغل

---

[1] قدة حبيبة ، مفهوم عملية التحويل المصرفي وطبيعتها القانونية ،مقال منشور بمجلة دفاتر السياسية والقانون ، العدد 10،جامعة قاصدي مرباح ورقلة ،العدد الأول 2014،ص33.

[2] انظر المواد 543مكرر19،مكرر20،من القانون رقم 75-59المؤرخ في 26سبتمبر 1975،المتضمن القانون التجاري الجزائري،ج.ر.ج.ج.العدد101،المؤرخة في 19ديسمبر1975ص1306ص1388،والمعدل بالقانون الجزائري رقم87_20المؤرخ في 23 ديسمبر 1987المتضمن قانون المالية لسنة 1988،ج.ر.ج.جالعدد54،المؤرخ في 28ديسمبر 1987ص2112ص2177.

الجمعات الإرهابية وسائل الحديثة في تنفيذ مخططاتها الدنيئة مثل الإتصالات والتنسيق وبث بعض الأقوال المغلوطة ، وخاصة أن الإرهاب الإلكتروني ظاهرة إجرامية عابرة للحدود الوطنية وتطور بتطور التكنولوجي خاصة مع بروز الذكاء الصطناعي فبعدما كان المجرم التقليدي قبل ظهور الثورة الرقمية يعتمد على التخطيط والتنقل والقوة للقيام بالأعمال الإجرامية من بينها الأعمال الإرهابية كالقتل وتفجيرات وإستهداف الممتلكات بغرض تغير النظام السياسي وبفعل ماتقدمه التكنولوجيا أصبح يعتمد الإرهاب على وسائل إلكترونية التي تسهل القيام بالعمليات الإجرامية ،ومن بين الجرائم التي تمس بأمن الدولة نجد أيضا جريمة التجسس التي تصدى لها المشرع الجزائري في قانون رقم 09_04 وإلحاقها بجرائم الإرهاب[1].

وإن جرائم الجوسسة جرائم قديمة كانت تقتصر بعضها على الأسرار المتعلقة بالدفاع الوطني ، ليمتد ويشمل جميع المجالات الاقتصادية والصناعية التي تنال من هيبة الدولة وتساهم في اضطرابيها ومع التطور التكنلوجي طور من هذه الجريمة أين وجد الجاسوس ظالته فيها حيث اصبح ينقل المعلومة باستعمال الوسائل التقنية المتطورة .

ثانيا :الجريمة الإلكترونية الواقعة على النظام المعلوماتي :

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال جاء القانون رقم 04/ 15الصادر في 10نوفمبر 2004 المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المواد 394مكرر إلى 394مكرر 07 وتأخذ صورة الإعتداء صورتين وهما الدخول والبقاء في منظومة معلومتية كما تضمن جريمة التلاعب بمعطيات الحاسب الآلي وهذا ماسنتناولها في العنصر الموالي :

أ) **جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتبة:**

[1] بعجي عبد النور ،مالك نسيمة ،الارهاب الالكتروني بين عولمة الجريمة وضرورة المكافحة نمقال منشور بمجلة الدراسات والبحوث القانونية ،الصادرة عن جامعة محمد بوظياف ،مسيلة ،كلية الحقوق والعلوم السياسية ،مجلد السابع ،2022،02ص65.

فعل الدخول : تنص عليه المادة 394 مكرر من قانون العقوبات السابق الذكر على أنه "يعاقب بالحبس من(03) ثلاثة أشهر إلى(01) سنة وغرامة من خمسين ألف،(50.000دج) إلى مائة ألف دينار(100.000دج) كل من يدخل أو يبقى بواسطة إستعمال الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير للمعطيات المنظمة ، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من(06) ستة أشهر إلى(02) سنتين وغرامة من(50.000دج) خمسين ألف إلى (150.000دج) مائة وخمسون ألف دينار[1]". وبتالي فإن الوصف الذي أعطي لهذا الفعل هو الدخول عن طريق الغش ، فعل الدخول غير المشروع لا نعني به هنا الدخول بالمعنى المادي أي الدخول إلى مكان معين كمنزل أو غيره وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة لآلية للمعطيات وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أولايعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام، وسواء تم الدخول إلى النظام كله أو إلى جزء منه فقط أي أن الجريمة تقوم بفعل الدخول إلى النظام .

أما فعل البقاء الغير المشروع يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات والإستمرار في التواجد داخله وذلك دون إذن صاحبهه رغم علمه بأن بقاءه فيه غير مرخص إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ هنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء الغير

[1] أنظر :ج.ر.ج العدد71المؤرخة في 10نوفمبر 2004ص11وص12.

المشروع[1] ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الإطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية والتي يستطيع الجاني فيها الحصول على خدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم الدفع كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية [2].

ب) جريمة التلاعب بالمعطيات الحاسب الآلي :

جاء في المادة394 مكرر 1 من قانون العقوبات " يعاقب بالحبس من ستة (06) أشهر إلى ثلاث(03) سنوات وبغرامة من 500.5000 دج إلى 2.000.000دج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها " بمعاقبة كل شخص قام بادخال معطيات في نظام المعالجة الآلية أو أزال أو عدل هذه المعطيات وذلك عن طريق إستعمال الغش هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال أو المحو أو التعديل كما إن المشرع لم يشترط إجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي وفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الالية للمعطيات سواء باضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل كما أن هذا السلوك يجسد فعل

[1] أمال حبات ،الجريمة المعلوماتية في التشريع الجزائري بين قانون 04-15 و09-04 مجلة هيرودوت للعلوم الإنسانية والإجتماعية مجلد 7العدد2023،25.

[2] حمزة بن عقون ،السلوك الاجرامي للمجرم المعلوماتي ،بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية ،تخصص علم الاجرام وعلم العقاب ،جامعة الحاج لخضر ،باتنة ،2011-2012.ص108

التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها[1].

جرمت المادة 394 مكرر من قانون العقوبات السابق الذكر الأعمال الآتية تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في المعطيات المخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم الغش المعلوماتي السابقة الذكر ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية برامج القرصنة التي يمكن أن تستعمل في إرتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية أو المعطيات المعلوماتية في حد ذاتها كما جرم المشرع كذلك أفعال الحيازة أو الإفشاء أو نشر أو إستعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض.

الفرع الثاني: دوافع إرتكاب الجريمة المعلوماتية.

إن الدافع أو الباعث أو الغرض أو الغاية تعد تعبيرات لكل منها دلالة الإصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص في الجريمة وللجريمة المعلوماتية تتباين الدوافع المؤدية الإرتكابها تبعا لطبيعة المجرم ومدى ثقافته ومعرفته بمجال الحاسب الآلي لذلك نجد أن عدة دوافع لإرتكابها فبعضها يرجع إلى دوافع شخصية بنوعيها المالية مثل البحث عن الربح أو الذهنية كالسعي إلى إظهار التفوق وأخرى خارجية كالإنتقام مثلا وكل هذه الدوافع يكون مصدرها الرغبة الإجرامية وهذا ماسيتم توضيحه كالتالي:

1. دوافع شخصية :

يقصد بالدوافع الشخصية تلك العوامل الصيقة بشخصية المجرم المعلوماتي والتي تدفعه لإرتكاب الجريمة المعلوماتية والتي سنجملها فيما يلي:

1.أ تحقيق الربح المادي :

[1] أمال قارة الحماية الجزائية المعلوماتية في التشريع الجزائري ،دار الهومه للنشر والتوزيع ،االطبعة الثانية،الجزائر ص102.

يعتبر هذا الدافع من بين أكثر الدوافع التي تحرك الجاني لإرتكاب جرائم الإنترنت ذلك لأن من خصائص هاته الجرائم هو حجم الربح الكبير الممكن تحقيقه منها خاصة غش الكميوتر أو الإحتيال المرتبط بالكمبيوتر يتيح تعزيز هذا الدافع وتحقيق الثراء السريع عن طريق إتاحة الإطلاع على معلومات معينة وأساسية وذات أهمية خاصة لمن يطلبها ولذلك تتعدد الأساليب الازمة للوصول إلى هذا الهدف المنشود لذلك فإن هذا السبب يعد من أكثر الأسباب التي تؤدي الى إنتشار الإجرامي المعلوماتي بحيث تظهر الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة مالمشاكل المالية أو الديون ومن يعتبر السعي إلى تحقيق الربح في المرتبة الأولى من دوافع إرتكاب جرائم الحاسب الآلي[1].

وفي درسات أشار إلى الرغبة في الثراء والربح المادي عادة ما تواجهها صعوبات بالغة لتحقيقها البطرق القانونية والمقبولة إجتماعيا لذا يلجأ بعض الأفراد إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ ووفرة المردود وقلة الخطورة إضافة إلى إمكانية محو الدليل وتوفير وسائل التقنية التي تعرقل الوصول إليه مع ضمان التستر وعدم التشهير.

ووفقا لدراسات فإن قطاع المالية يعد أكثر القطاعات إستهدفا من جرائم الحاسب الآلي ويرجع ذلك أن البنوك تعتمد وبشكل أساسي على أنظمة التمويل الإلكتروني الأمر الذي زاد فرص النصب وبشكل هائل فمجرد السقوط رموز التحويل الالكتروني المستخدمة في الأيدي الخاطئة فإن ملاين الدولارات يمكن أن تنقل وبثوان معدودة دون أن يترك دليل ضده كما أن شركات التأمين تعد من القطاعات المستهدفة لعمليات النصب والإحتيال كما أنها قد تقوم بدور الجاني في بعض الأحيان كشركة تأمين بمدينة لوس أنجلس الأمركية [2].

1.ب.الرغبة في قهر النظام المعلوماتي وإثبات الذات :

---

[1] رضا عسال ،عماد عبد الرزاق،مرجع سابق، ص156.

[2] سفيان سوير،جرائم المعلوماتية ، مذكرة الماجستر في القانون الجنائي ،كلية الحقوق والعلوم السياسية ،جامعة أبوبكر بلقايد 2010-2011 ص109

يعد الرغبة في قهر النظام المعلوماتي دافعا أقوى من السعي إلى تحقيق الربح رغم أن هذا الأخير يظهر دافعا أكثر تحريكا للمجرمين المعلوماتيين إلا أن الدافع إلى قهر النظام أيضا تجسد بنسبة معتبرة من تلك الجرائم الإكترونية خاصة مايعرف بأنشطة المتطفلين وهؤلاء ليسوا على جانب كبير من الخطورة الإجرامية وإنما هم غالبا يفضلون تحقيق إنتصارات تقنية ودون أن يتوفرلديهم أية نويا سيئة كما يشكل إختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة متعة كبيرة وتسلية تغطي أوقات الفراغ مما يؤدي ذلك إلى الرغبة في تحقيق الذات ومن ثم قهر النظام المعلوماتي[1]، فهذه الطائفة يخالجهم شعور بالفخر إذا ماتمكنوا من إختراق مواقع على الشبكة الإنترنت أو وصلوا إلى قاعدة بيانات محمية إذا يعد ذلك من الأمور التي يتباهون بيها أمام أقرانهم ويشبعون بيها فضولهم ويثبتون بها قدراتهم على إختراق البرامج ويسعون من خلالها إلى تحقيق الشهرة[2].

2. الدوافع الخارجية :

في بعض المواقف يتأثر الإنسان ويستسلم للمؤثرات والدوافع الخارجية بارتكابه بعض الجرائم المعلوماتية نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات والتي سيتم توضيحها كالتلي:

2.أ.دافع الإنتقام :

يعد دافع الإنتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب جريمة لأن دافع الإنتقام غالبا مايصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها وغالبا مايكون أحد موظفيها الذي يقوم بارتكاب الجريمة المعلوماتية بدافع الإنتقام نتيجة إما لفصله أو تخطيه في الحوافز أو الترقية أو الطرد من الوظيفة[3]، فهذه الأمور تجعله يقدم على إرتكاب جريمته وتشير التقديرات إلى أن نسبة كبيرة من الجرائم المرتكبة عبر الإنترنت ترتكب من قبل موضفي الجهة نفسها وإبراز مثال على ذلك الواقائع التي حدثت في الولاية المتحدة الأمركية

---

[1] سفيان سوير،مرجع سابق، ص28.

[2] شنتير خضرة مرجع سابق ص35.

[3] محمد سامي الشوا، ثورة المعلومات وانعكساتها على قانون العقوبات ،دار النهضة العربية ،1994،ص06.

عندما حكم على الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة 150 ألف دولار لأنه أدخل فيروسا في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع 160سجلا من سجلات العملاء وذلك إنتقاما من الشركة لأنها قامت بفصله من العمل .

3. دوافع سياسية وتجارية :

إنتشرت الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت من هذه المواقع مايكون موجها ضد سياسة دولة محددة أو ضد عقيدة أو مذهب معين وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف حيث تعد الدوافع السياسية من أبرز المحاولات الدولية لإختراق شبكات حكومية في مختلف دول العالم كما أن الأفراد قد يتمكنون من إختراق الأجهزة الأمنية الحكومية[1].

كذلك أصبحت شبكة لإنترنت مجالا خصبا لنشر أفكار العديد من الأفراد والمجموعات ووسيلة للترويج الأخبار وأمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو النظام الحكم أو قدحا في رموز دولية أو سياسية و الإساءة لها ،وهي تعد عموما محرك أنشطة الإرهاب الإلكتروني فكثيرة هي المنظمات في عصرنا الحالي والتي تتبنى بعض الأراء والأفكار السياسية أو الدينية أو الإيديولوجية ومن أجل الدفاع عن هذه الأراء تقوم بأفعال إجرامية ضد معارضيها فمثلا هناك العديد من عمليات الإختراق تعود لأسباب عقائدية حيث يقوم البعض المجموعات التي تتبنى فكرة الإصلاح بعملية رقابة أخلاقية أوإجتماعية أودينية فتتجسس على المواقع التي تقدم خدمات أو معلومات تتعارض مع قناعتها وتعمل على كشف الأسرارها أو حتى تدميرها فهناك بعض المواقع أخذت على عاتقها مهمة التجسس على مواقع حكومية وكشف أسرار الدبلوماسية والعسكرية وأما عن دوافع الحصول على المعلومات التجارية بمختلف الأشكال التي

[1] رضا عسال ،عماد عبد الرزاق ،مرجع سابق ص156.

يكون عموما دوافعها المنافسة وأخيرا لايمكن حصر كل الدوافع أو ذكرها كل البواعث التي قد تدفع المجرم المعلوماتي الى إرتكاب هذا الفعل المجرم [1].

[1] عبد الرحمن المويشر تركي ،"بناء نماذج أمنية لمكافحة الجرائم المعلوماتية وقياس فعاليته"،أطروحة دكتوراه ،الرياض ،المملكة العربية السعودية ،كلية الدرسات العليا بجامعة نايف للعلوم الأمنية،2009ص39.

الفصل الثاني

الآليات القانونية والإجرائية لمكافحة جرائم تكنولوجيا الإعلام والإتصال

تمهيد:

جرائم تكنولوجيا الإعلام والإتصال فرضت جملة من التحديات القانونية من أجل مكافحتها والوقاية منها مما إستوجب دخل المشرع الجزائري من أجل إستحداث هيئات متخصصة للوقاية من هذه الجرائم وضرورة إتباع إجراءات خاصة لمكافحتها ، سنحاول من خلال هذا الفصل ، إستعراض أبرز الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم المعلوماتية ، بالإظافة إلى تبني إجراءات معينة للكشف والحد من جريمة محل الدراسة ولتوضيح أكثر سيتم تقسيم الفصل إلى مبحثين أساسيين:

المبحث الأول :اللآليات القانونية والمؤساستية لمكافحة جرائم تكنولوجيا الإعلام والإتصال

المبحث الثاني : الدليل الإلكتروني وسلطة القاضي في تقديره.

المبحث الأول: الآليات القانونية والمؤسساتية لمكافحة جرائم تكنولوجيا الإعلام والإتصال.

لقد خصصت مختلف التشريعات الوطنية والدولية مؤسسات ومصالح ووحدات من أجل مكافحة الجريمة الالكترونية، فعلى المستوى الوطني في الجزائر مثلا نجد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، والمصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمدير الأمن الوطني ومركز الوقاية من الجرائم الإعلام الآلي والجرائم المعلوماتية التابع لدرك الوطني وكذا المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع إلى الدرك الوطني كما قام المشرع الجزائري باستحداث منظومة أمن الأنظمة المعلوماتية ،حتى يتمكن من تحقيق الإستراتجية الوطنية في أمن أنظمة المعلومات ولأكثر تفصيل حول هذه الهيئات تم تقسيم هذا المبحث إلى مطلبين.

المطلب الأول: جهود مكافحة الجريمة المتصلة بتكنولوجيا الإعلام والإتصال على الصعيد الوطني

إتخذ المشرع لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال مجموعة من التدابير سواء وقائية أوعقابية وقد أنشأ المشرع هيئة إدارية تكلف بالوقاية والتحري عن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وهذا في الجرائم الخطيرة والتي تمس بأمن الدولة عموما أو توصف بالجرائم الإرهابية وفي إيطار الكشف عن مرتكبي هذه الجرائم أجاز المشرع لهذه الهيئة بالتعاون مع الشرطة القضائية وضع ترتيبات تقنية إلكترونية هدفها إما إعتراض الرسائل الإلكترونية أو تسجيل المعطيات المعلوماتية الشخصية ما يتعارض مع حرمة الحياة الخاصة وسرية المرسلات الخاصة، خصوصا أنها مضمونة دستوريا لذلك تقوم الضرورة للبحث في كيفية التوفيق بين إلتزام الهيئة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وبين حرمة الحياة الخاصة باعتبارها حقوق مكفولة دستوريا وفي إيطار قمع هذا النوع من الجرائم حذا المشرع الجزائري حذو

باقي التشريعات المقارنة وكان لازما عليه البحث عن هيئة متخصصة تقوم بمساعدة الدولة وتنتهج المنهج الوقائي ولقد لجأ المشرع الى فكرة السلطات الإدارية[1].

الفرع الأول: المكافحة للجريمة المعلوماتية في التشريع الجزائر

أولا: مكافحة الجريمة المعلوماتية بموجب القوانين العامة:

1. **مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري** : لقد كفل الدستور الجزائري لسنة 1996 وكذاالتعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية حقوق الأساسية والحريات الفردية وعلى أن تضمن الدولة عدم إنتهاك حرمة الإنسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق ومن أهم المبادئ الدستورية العامة المادة 38 التي جاء فيها أن الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

المادة44 التي نصت على أنه "الإبتكار الفكري والفني والعلمي ومضمونة للمواطن حقوق المؤلف يحميه القانون لايجوز حجز أي مطبوعة أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام الإ بمقتضى أمر قضائي الحريات الأكاديمية وحرية البحث العلمي تمارس في إطار القانون".

وعليه ما يمكن إستقرائه من نص المادة أعلاه أنه ، تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة التنمية المستدامة للأمة إذ لايجوز إنتهاك حرمة حياة المواطن الخاصة ، وحرمة شرفه كما أن القانون يحمي سرية المرسلات والإتصالات الخاصة بكل أشكالها مضمونة ،إن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوعة أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي .

[1] فضيلة عاقلي ،الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري،المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية "،طرابلس ،بتاريخ 24-25مارس2017،ص127.

2. **بموجب القانون المدني** : ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه إعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الإعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124من التقنين المدني الجزائري " كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض " وقد جاء هذا النص عاما وشاملا لأي إعتداء يقع على حق من الحقوق الملازمة للشخصية بما فيها الحق في الخياة الخاصة ، وقد أورد هذا النص مبدأ مهما هو حق من وقع إعتداء على حياته الخاصة في التعويض عما لحقه من ضرر[1]، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض "فالفعل الضار هو أساس المسؤولية "وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الإعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الإنترنت ، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات وفي تحديد هوية المعتدي وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي إقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل إعتداء قابل للإثبات وإن وقع على الشبكة[2].

3. **مكافحة الجريمة الالكترونية بموجب قانون العقوبات الجزائري:** لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10نوفمبر 2004 المتمم الأمر رقم 22-15 المتضمن

[1] حسين نوارة ،أليات تنظيم المشروع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا ،الملتقى الوطني "أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"الجزائر 29مارس2017،121.

[2] حسين نوارة ، مرجع سابق، ص122..

قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7[1].

وبغرض تدارك الفراغ القانوني فقد قام المشرع الجزائري بموجب القانون رقم 04-15[2] إستحداث جملة من النصوص والتي جرم من خلالها الفعال المتصلة بالمعالجة الآلية للمعطيات وحدد لكل فعل منها مايقابله من الجزاء إذ قام المشرع الجزائري بسن جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء وسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22[3] إذ نصت المادة 394 مكرر منها مايلي :"يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50000 إلى 100000دج كل من يدخل أو يبقى عن طريق الغش كل أو جزء من مظومة للمعالجة الآلية للمعطيات أو يحاول ذلك " وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج" ويعاقب .....كل من يقوم عمدا وعن طريق الغش بما يأتي :

- تصميم أو بحث أوتجميع أوتوفير أو نشر أو الإتجار في المعطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .
- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ".

---

[1] فضيلة عاقلي ، مرجع سابق،ص127.

[2] قانون رقم 04-15 مؤرخ في 2004/11/10 يعدل ويتمم الامر رقم 66-156،يتضمن قانون العقوبات ،جريدة رسمية عدد71،صادر بتاريخ 2004/11/10،معدل ومتمم.

[3] براهمي جمال ،مكافحة الجريمة الإلكترونية في التشريع الجزائري،المجلة النقدية للقانون والعلوم السياسية ،كلية الحقوق والعلوم السياسية جامعة ملود معمري ،تزيوزو ،العدد2،الصادرة في 2016/11/15،ص124_125.

وتضيف المادة 394 مكرر 6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالإحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية :"يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو المكان الإستغلال إذا كانت الجريمة قد وقعت بعلم مالكها "[1] .

وفي إطار قمع الجريمة الإلكترونية أورد المشرع الجزائري بموجب هذا القانون، عقوبات أصلية وأخرى تكملية تطبق على الشخص المعنوي عند إرتكابه جرائم ماسة بتكنولوجيات الإعلام والإتصال سواء بصفته فاعلا أصليا أو شريكا ، كما تطبق عليه أحكام الشروع ، وأقر له المشرع الجزائري عقوبة تقدر 05 بخمس مرات من العقوبة المالية المقررة للشخص الطبعي وإذا لم ينص المشرع الجزائري على عقوبة الغرامة بالنسبة للشخص الطبيعي فإننا نطبق أحكام المادة 18مكرر 02 من قانون العقوبات الجزائري .

4. مكافحة الجريمة بموجب قانون الإجراءات الجزائية الجزائري:

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة وإستجواب المتهم والضبط والتسرب والشهادة والخبرة

نجد أن المشرع نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية ونص على التفتيش في المادة 45 الفقرة 7من[2] نفس القانون المعدلة حيث إعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية ونص على توقيف

---

[1] حسين نوارة مرجع سابق ،ص118_119.

[2] بوضياف اسمهان ،الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر ،مقال منشور في مجلة الاستاذ الباحث للدرسات القانونية والسياسية ،العدد11،2018،ص362..

النظر في الجريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على "إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور و لقد أشار المشرع الجزئري إلى ظروف وكيفية الجوء لهذ الإجراء في المادة 65 مكرر5 من ق.إ.ج[1] على نحو " إذا إقتضت ضرورات التحري في الجريمة المتلبس بها ، أوتحقيق الإبتدائي في ....الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن : بإعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكي.

ثانيا: مكافحة الجرائم الإلكترونية بموجب القوانين الخاصة

قانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما لقد جاء في قانون 04/09 مجموعة من التدابير الوقائية التي يتم إتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أوكشف عنها وعن مرتكبها في وقت مبكر وهي كالتالي :

1. **المراقبة الإتصالات الإلكتروني** : لقد نصت المادة 04 من القانون 09-04 [2]على أربع حالات التي يجوز فيها للسلطات الأمنية القيام بمراقبة المرسلات والإتصالات الإلكترونية وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة ، وفي إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.
2. **القانون الخاص بحقوق المؤلف والحقوق المجاورة** : يرى معظم الفقه أن "المقع الإلكتروني مصنف متعدد الأغراض " يتم إستخدامه من الشركات التجارية كعلامة تجارية لتميز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الإنترنت أو كإسم تجاري أو شعار لجذب الجمهور كما يمكن أن يستغل كمصنف أدبي أوفني من المؤلفين عند عرض أفلامهم السينامئية أو لوحاتهم الزيتية أو ألعاب الفيديو ...وغيرها في كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض مايريد من خدمة ، وبمجرد تسجيل إسم الموقع يحضى بالحماية القانونية المقررة لحق الملكية

[1] فضيلة عاقلي ،مرجع سابق ص131.

[2] أنظر المادة 04 من قانون 09-04 السالف الذكر.

الفكرية الذي يتضمنه ، أي تحديد القانون الواجب التطبيق حسب الطبيعة القانوية للمواقع فعند تسجيل الموقع كمصنف أدبي أوفني "لايجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد" كإستعمال إسم كامل لشخص معين معروف دون الحصول على موافقة صاحبه[1]

3. **قانون البريد والاتصالات اللاسلكية** :بإستقراء القانون الذي يحدد القواعد العمة المتعلقة بالبريد والإتصالات لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية للتطور التكنولوجي لذلك بات من السهولة إمكانية إجراء التحويلات المالية عن الطريق الإلكتروني ذلك مانصت عليه المادة 87 منه كما نصت المادة 2/84 منه على إستعمال حولات دفع عادية أو إلكترونية أو برقية كما نصت في المادة 105منه على احترام المراسلات بينما اتت المادة 127 منه بجراء كل من تسول له نفسه وبحكم مهنته ان يفتح او يحول او يخرب البريد او ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف او الخدمات العمومية من خمس الى عشر سنوات .[2]

وضع الترتيبات التقنية دون موافقة المعنين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص او عدة اشخاص في اماكن خاصة او عمومية او التقاط صور لشخص اوعدة اشخاص يتواجدون في مكان خاص "

4. **قانون التأمين:** قد تطرق هذا القانون كذلك الى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي ،في النصوص قانونية عديدة تحص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب علاج وهي صالحة في كل التراب الوطني ،وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أوحذف كلي أوجزئي للمعطيات التقنية أ, الادارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا حسب المادة 93 مكرر2[3]

---

[1] حسين نوارة ،مرجع سابق ،ص120_121.

[2] اسمهان بوضياف مرجع سابق ،ص365.

[3] فضيلة عاقلي مرجع سابق ،ص132.

الفرع الثاني : مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة

اولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

تعود فكرة انشاء هذه الهيئة للمادة 13من القانون رقم 09/ 04 المؤرخ في 05اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتهما نصت على انه " تنشأ هيئة وطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها " تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم "أما مهامها فقد اوردتها المادة 14 من نفس القانون . ويمكن تعريفها على ان الهيئة الوطنية للوقاية هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية ، بذمة مالية مستقلة توضع تحت سلطة وزارة الدفاع بعدما كانت توضع لدى وزير العدل في المرسوم 15-261 ، كما تخضع الهيئة لمجموعة الاحكام التشريعية والتنظيمية المطبقة في وزارة الدفاع الوطني ،ويحدد مقر الهيئة بمدينة الجزائر العاصمة ويمكن نقله الى اي مكان آخر من التراب الوطني بموجب المرسوم الرئاسي [1]

1. تشكيلة الهيئة وتنظيمها :

فحسب المرسوم الرئاسي رقم 20-183 السالف الذكر في المادة 05 منه ،فإن الهيئة تتكون من مجلس توجيه ومديرية عامة يديرها مدير عام يتم تعينه بموجب مرسوم رئاسي ، وتنتهي مهامه بحسب الاشكال نفسها [2]

1.1 المدرية العامة

- مدرية للرقابة الوقائية واليقضة الالكتروني
- ومديرية للادارة والوسائل
- وصلحتين مصلحة للدرسات وتلخيص

---

[1] إن المرسوم الرئاسي رقم 15-261 ،المؤرخ في 08أكتوبر 2015،يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،الجريدة الجزائرية ،العدد53،الصادر في تاريخ 08أكتوبر 2015.

[2] المرسوم الرئاسي رقم 20-183 المؤرخ في 13يوليو2020،يتضمن الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحتها نالجريدة الرسمية الجزائرية العدد40،الصادر بتاريخ 26ذو القعدة 1441الموافق 18يوليو 2020.

- ومصلحة للتعاون واليقضة التكنولوجية

2.1 مهام المدرية العامة:

- فالسهر على السير حسن للهيئة
- واعداد مشروع الميزانية وعرضه على مجلس التوجيه للموافقة.
- إعداد وتنفيذ برنامج عمل الهيئة بعد الموافقة عليه من قبل مجلس التوجيه .
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهم.
- إعادة التقرير السنوي لنشاطات الهيئة ورفعه لمصادقة مجلس التوجيه.
- تبادل المعلومات مع مثيلاتها في الخارج بهدف تجميع كل المعطيات المتعلقة بتحديد مكان وهوية مركبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والتعرف عليهم.
- تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية .
- السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة .
- ضمان التسيير الاداري والمالي للهيئة .
- تحضير إجتماعات مجلس توجيه الهيئة [1].

3.1 مجلس التوجيه :

يضم مجلس التوجيه مجموعة من الأعضاء هم:

- الوزير مكلف بالعدل
- الوزارة المكلفة بالداخلية
- الوزير المكلف بالداخلية
- الوزارة المكلفة بالمواصلات السلكية واللاسلكية

[1] المادة 09 من المرسوم الرئاسي رقم 172/19.

- المدير العام للأمن الوطني
- قائد الدرك الوطني[1]

4.1 مهام مجلس التوجيه :

يقوم مجلس التوجيه بالإجتماع في دورة عادية مرتين في السنة باقتراح من رئيسه ،كما يمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا ،بناءا على إستدعاء من رئيسه أو بطلب من أحد اعضائه أو من المدير العام للهيئة ويرأسه رئيس الجمهورية ويمكن أن يفوض ممثليه التداول حول الإستراتجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتتمثل صلاحياته فيما يالي:

- التداول حول مسائل التطور والتعاون مع المؤسسات والهيئات الوطنية الأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال .
- القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيا الإعلام والإتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة .
- إقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته .
- الموافقة على برنامج عمل الهيئة وإعداد نظام داخلي والمصادقة علية .
- إبداء الرأي في كل مسالة تتصل بمهام الهيئة وتقديم كل إقتراح يتصل بمجال الهيئة والمصادقة علية .
- المساهمة في ضبط المعايير القانونية في مجال إختصاصه، ودراسة مشروع ميزانية الهيئة والموافقة عليه.[2]

---

[1] حسين ربيعي ،آليات البحث والتحقيق في الجرائم المعلوماتية نأطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية ،جامعة باتنة 1،سنة الجامعية 2015-2016ص33

[2] المرسوم الرئاسي رقم 19-172،المؤرخ في 26جوان 2019،يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها .

2. مهام الهيئة الوطنية في مكافحة جرائم تكنولوجيا الإعلام والإتصال : تمارس الهيئة المهام المنصوص عليها في المادة 14من القانون 04-09[1]،والمواد 12،9،11من المرسوم الرئاسي 19-172 فيمايلي :

1.2: دورها في الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

تهدف التدابير الوقائية الى توعية مستخدمي تكنولوجيا المعلومات والإتصالات بخطورة الجرائم التي قد يقعون ضحية لها أثناء تصفح أو استخدام هذه التقنيات ، ومن أهم هذه الجرائم :

- التجسس على الإتصالات والرسائل الإلكترونية .
- التلاعب بحسابات العملاء أوببطاقات إئتمانهم .
- إختراق أجهزة الشركات والمؤسسات الرئيسة أو الجهات الحكومية .....الخ .

2.2:دور الهيئة في مكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال .

- ✓ مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ، لاسيما من خلال جمع المعلومات والتزويدها بها ومن خلال الخبرات القضائية .
- ✓ تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهاعلى المستوى الوطني ضد الفاعلين والمشتركين.
- ✓ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وتحديد مكان تواجدهم .[2]

---

[1] انظر :إلى المادة 14القانون 04/09المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،ج.ر.ج العدد47المؤرخ في 2009/08/16،ص8.

[2] لمعرفة مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها أنظر :www.legifrance..gouv..fr/affich texte.de

أما من خلال أحكام المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها فإضافة إلى المهام المسندة لها بموجب أحكام القانون 04/09 المشار إليه سابقا تكلف الهيئة على الخصوص ووفقا لنص المادة 04 منه بما يأتي :

- ✓ تحديد الاستراتجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ووضعها حيز التنفيذ .
- ✓ المساهمة في تكوين المحقيقين المحتصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والإتصال .
- ✓ تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.
- ✓ تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية [1]

ثانيا: الأقطاب الجزائية المتخصصة :

إن تنامي الجريمة المعلوماتية ، والإمتداد الإقليمي الذي تجاوزته الجريمة وصعوبة التحكم فيها وضع على عاتق المجتمع الدولي التصدي له ، فكانت فكرة إبرام إتفاقية وكان على مشرع الجزائري تنفيذ أحكام الإتفاقية ضمن القوانين الداخلية ، ومسايرة التطورات التشريعية على المستوى الدولي إضافة إلى عدم تحكم المحاكم على مستوى الدرجة الأولى بمعالجة مثل هذا النوع من الجرائم ، وقلة الكفاءة لدى القضاة ، مما إستوجب على المشرع الجزائري التوجه إلى إحداث محاكم ذات إختصاص موسع أطلق عليها مصطلح الأقطاب المتخصصة .[2]

[1] المادة 04 من قانون 04/09

[2] أمينة بن عميور ، إهام بوحلاس ،القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال نمقال منشور في مجلة البحوث في العقود وقانون الاعمال ،المجلد 07،العدد 01،2022،ص67

ظهرت فكرة إنشاء محاكم جزائية ذات إختصاص محلي موسع بموجب القانون الجزائري رقم04-14 ،وتطبيقا لأحكام هذا القانون الجزائري الذي جاء على إثره المرسوم التنفيذي 06-348 [1]المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ثم صدر القانون الجزائري رقم 08-09 المتضمن قانون الاجراءات المدنية والادارية المعدل والمتمم.[2]

أولا:الإختصاص النوعي للأقطاب الجزائية المختصة في الجرائم الماسة بتكنولوجيا الإعلام والإتصال بالرجوع إلى أحكام المادة : 211مكرر22 من الأمر 21-11 فإن القطب المستحدث يختص بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها غير أنه ينبغي التميز بين المراحل التالية :

1. خلال المرحلة المتابعة الجزائية :يختص وكيل الجمهورية على المستوى القطب المستحدث، بموجب أحكتم الفقرة الاولى من المادة 211مكرر من الامر21-11 بمتابعة كافة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها سواء كانت القضية في طور البحث والتحري، أو إيداع المحاضر الخاصة بها على مستوى نيابة الجمهورية ويتصرف فيها طبقا للقانون .
2. خلال مرحلة التحقيق القضائي : يختص قاضي التحقيق على مستوى القطب المستحدث بموجب أحكام الفقرة الأولى من المادة 211مكرر من الأمر 21-11بالتحقيق في كافة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المرتبطة بها ويتصرف فيها طبقا للقانون .

[1] المرسوم التنفيذي 06-348 المؤرخ في 05-10-2006،ج.رعدد63المؤرخ في 08-10-2006

[2] الامر رقم 21-11المؤرخ في 25-08-2021 المتضمن تعديل قانون الاجراءات الجزائية ،ج..ر،عدد65 المؤرخ في 26-08-2021

3. خلال مرحلة المحاكمة :خلافا لوكيل الجمهورية وقاضي التحقيق ، فإن قاضي الحاكم لدى القطب المستحدث يختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها ،الموصوفة بالجنح ، وهو مانصت عليه صراحة الفقرة الثانية من المادة 211 مكرر22من الامر 21-11.[1]

أما الجرائم الموصوفة بالجنايات ، فلا يمكن لقضاة الحكم على مستوى القطب المستحدث معالجتها ، كونها من إختصاص محكمة الجنايات الابتدائية وتبقى الجنايات التي تم التحقيق فيها من طرف القطب المستحدث تخضع الاختصاص محكمة الجنايات لمجلس قضاء الجزائر

ثانيا :الإختصاص الإقليمي : منح المشرع الجزائري القطب المستحدث اختصاصا وطنيا بموجب المادة 211مكرر23 ليمارس بذلك كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب اختصاصهم عبر كافة الإقليم الوطني وذلك وفق نمطين :

ثالثا:الإختصاص الحصري : ويقصد به إختصاص القطب المستحدث حصريا ودون سواه بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال عبر كافة الأقليم الوطني ويكون ذلك في حالتين :

الحالة الأولى : بالنسبة الجرائم المحددة قانوناعلى سبيل الحصر في المادة 211مكرر24 هذه الجرائم هي:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الطني .
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن السكينة العامة أو استقرار المجتمع .

[1] المواد من 11مكرر الى 211مكرر22 من الامر 21-11 السالف لذكر

- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ،ذات الطابع المنظم او العابر للحدود الوطنية .
- جرائم المساس بانظمة المعالجة الآلية للمعطيات، التعلقة بالإدرات والمؤسسات العمومية
- جرائم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين .
- جرائم التمييز وخطاب الكراهية.

بالنسبة للجرائم الأكثر تعقيدا : يختص القطب المستحدث كذلك دون سواه بمعالجة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال الأكثر تعقيدا عبر كافة الإقليم الوطني ونظرا لتعدد الفاعلين أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو لطابعها المنظم العابر[1] للحدود الوطنية تتطلب إستعمال وسائل تحري خاصة أو لجوء إلى تعاون قضائي دولي مما يجعل أجهزة التحقيق التقليدية عاجزة عن البحث والتحري وضبط الدليل لذلك أعطى المشرع الإختصاص الحصري للقطب المستحدث نظرا للآليات المستحدثة التي يتمتع بها .

رابعا: **الإخصاص التفضلي** : يمارس وكيل الجمهورية لدى القطب المستحدث كذا قاضي التحقيق ورئيس القطب إختصاصا مشتركا مع الجهة القضائية المختصة محليا ، بموجب المواد 37 40 و 329 من قانون الإجراءات الجزائية ، والتي تضبط معيار الإختصاص المحلي بمكان إرتكاب الجريمة أو محل إقامة أحد مرتكبين أو محل القبض على أحدهم مع جواز تمديده لدائرة

[1] أمينة بن عميور ، إهام بوحلاس مرجع سابق ص68.

إختصاص محاكم أخرى عندما يتعلق الأمر بجرائم المخدرات جرائم تبيض الأموال والإرهاب وجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المتعلقة بالتشريع خاص بالصرف.[1]

الفرع الثالث: دور الأجهزة الامنية في مكافحة الجريمة المعلوماتية

أولا: الأمن الوطني ودوره في كافحة الجريمة المعلوماتية

في سبيل المكافحة الفعالة للجريمة الإلكترونية خصصت المدرية العامة للأمن الوطني موارد بشرية ، وهيكلية وتنظيمية لمحاربة كافة أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجريمة المعلوماتية ومن أجل ذلك بادرت المدرية العامة للشرطة القضائية باستحداث مصلحة مختصة في مكافحة الجريمة المعلوماتية سميت بالنيابة مدرية مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ،بالإضافة الى نيابة مديرية الشرطة العلمية و التقنية ، حيث تتولى هذه الأخيرة أعمال البحث والتحري والتحقيق في هذ النوع من الجرائم ، وهذه الوحدة هي المخبر المركزي للشرطة العلمية والكائن مقره بالعاصمة ، وتم إنشاء مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة و وهران بالإضافة الى ثلاث مخابر أخرى قيد الإنجاز على مستوى ورقلة ،بشار ، وتمنغرست ويوجد على مستو كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والأثار التكنولوجية التابعة لمخبر الأدلة الجنائية ،تتولى هذه المصالح عملية البحث والتحقيق في الجرائم المعلوماتية والتي تعمل على تحليل الدلائل المادية التي تم جمعها إثر معاينة المخلفات والتحريات في ميادين الدلائل الإلكترونية الناجمة عن الجرائم الإلكترونية والبصمات الصوتية ومعالجة الصورة والإشارة وإستغلال الهواتف المحمولة وإعداد تقارير الخبرة التي طلبتها منها السلطة القضائية المختصة ،كما تعمل المصلحة على ضمان تسير بنوك المعطيات في علم

[1] سالمة عبد النبي ،دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال في مواجهة الإعتداءات الواقعة على المعطيات المعلوماتية مقال منشور بمجلة الحقوق والعلوم السياسية ،جامعة خنشلة ،المجلد 11العدد02السنة 2024ص22.

التحقيق الجنائي ، بالأخص المحفوظات الآلية للبصمات الصوتية والمخلفات المرتبطة بتكنولوجيات الإعلام والإتصال .

وفي سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية تم إنشاء مايقارب 48 فرقة لمكافحة هذه الظاهرة الاجرامية ، ويتمثل دورها في تلقي شكوى والبحث والتحقيق في الجرائم المعلوماتية، فتم بذلك تقريب هذه المصالح من المواطنين [1].

ومن أجل مواكبة التطور التكنولوجي والرفع من المستوى المعرفي والمهاري و لأدائي للمحققين تم إستحداث صنفين من التكوين المتخصص .[2]

الصنف الأول محقق في الجريمة المعلوماتية « ICC » خاص بإطارات ومفتشي المصالح المحققة في مجال الجريمة المعلوماتي والصنف الثاني متدخل أول في الجريمة المعلوماتية " PICC" خاص بأعوان الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية ،كما يقوم الأمن بتأهيل وإعداد الكفاءات العلمية المؤهلة لمواجهة هذا النوع من الإجرام ،وذلك بتطوير العملية التدريبية لرفع مستوى الأداء لتلبية الإحتياجات الأمنية الحالية والمستقبلية.

و النتائج التي توصلت إليها الشرطة الجزائرية في مكافحة الجريمة الإلكترونية لا بأس بها فقد كان ذلك محط إشادة من بعض الشخصيات ،ومنها ما ورد في تصريح للسيد مانغ هانغواي "meng Hongwei [3]" رئيس منظمة الأنتربول خلال زيادة العمل التي قام بها

---

[1] براردي نعيمة ،الإتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر دراسة تحليلية استطلاعية بالجزائر العاصمة رسالة لنيل شهادة الدكتوراه في العلوم الاعلام والاتصال ،كلية العلوم السياسية والإعلام ،جامعة الجزائر 03،السنة الجامعية 2012-2013ص117

[2] المعلومة متاحة عبر الموقع الرسمي لمدرية الأمن الوطني : https://www.algeriepolice.dz والذي تم الإطلاع عليه يوم 2025/05/15 ساعة 00:49.

[3] شنتير خضرة مرجع سابق ص196.

للجزائر في شهر ماي سنة 2018 حيث أشاد بالتقدم الذي أحرزه الجهاز الشرطي الجزائري وما وصلت إليه الشرطة الجزائرية من تطور وإحترافية ، ودعا إلى تعزيز التعاون[1]وتفعيل آليات تبادل الخبرات المعلوماتية من أجل ضمان فعالية أكثر في مواجهة جميع أشكال الجرائم المستحدثة وبلأخص الجريمة الإلكترونية فالمستوى الجيد الذي وصلت إليه الكفاءات العاملة في جهاز الشرطة في هذا الخصوص سوف يسمح بتعزيز برامج التعاون بين الجزائر ودول أخرى وتجسيدا لذلك فالجزائر ممثلة في المديرية العامة للأمن الوطني والإتحاد الأروبي ، قام بتاريخ الحادي عشر 11من شهر جوان سنة 2019بالإطلاق الرسمي للتوأمة بعنوان "تعزيز الخبرة العلمية والتقنية الجزائرية " مما سيسمح بالرفع من مستوى خبرة الشرطة العلمية والتقنية الجزائرية بما يتماشى مع المعايير والممارسات الأروبية الحسنة، حيث تمكنت الشرطة الجزائرية من حل لغز عديد القضايا من الجرائم الإلكترونية ذات البعد الدولي ، ومنها قضية وقعت نهاية سنة 2009 والتي تم الإبلاغ عنها من طرف مكتب التحقيقات الفدرالية (FBI) كانت ضحيتها شركة أمركية تعرضت لعملية إختراق إلكتروني لبياناتها البنكية قامت بها منظمة إجرامية ، كان أحد أفرادها يقطن بإحدى ولايات الشرق الجزائري ، وبعد تحريات مكثفة حدد مكانه وهويته وقدم للعدالة وبعد شهر من ذلك تلقت الشرطة الجزائرية بلاغا أخر في قضية تعرض فيها بنك كندا إلى إختراق إلكتروني سحب خلاله المجرمون مبلغ مالي قدر ب: 200 دولار ، وكان من بين المتورطين في ذلك مواطن جزائري ، وبفضل كفاءة الشرطة المتخصصة تم تحديد هوية ومكان إقامة المشتبه فيه وتم تقديمه إلى العدالة[2].

---

[2]شنتير خضرة مرجع سابق ص169.

ثانيا:الدرك الوطني ودوره في مكافحة الجريمة المعلوماتية

يعد الدرك الوطني من بين قوات الأمن الفاعلة في مكافحة الإجرام عموما والجريمة الإلكترونية خصوصا ، وذلك من خلال ماله من إمكانات بشرية ومادية مخصصة لهذا الغرض فمكافحة الجريمة الإلكترونية التي أضحت من بين أولويات الدولة الجزائرية ، وذلك في إطار الإستجابة للإنشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء السيبراني الوطني ، فالبداية الفعلية لمحاربة قيادة الدرك الوطني للجريمة الإلكترونية كانت في سنة 2004[1] ليتم بعدها إنشاء مركز الوقاية من الجرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها والذي يعد اليوم العصب الذي يسير مهام المكافحة واليقضة وفرض إحترام القوانين في الوقت الذي يبحر فيه الملاين من المستخدمين عبر صفحات الإنترنت سواء من الخواص أو المؤسسات في الفضاء الإلكتروني .

لقد عمل المركز السالف الذكر منذ إنشائه سنة 2008 على تأمين منظومة المعلومات الخدمة الأمن العمومي ، حيث يهدف ضباط أعوان الشرطة القضائية المؤهليين في الدرك الوطني الى تطبيق القوانين وجمع الادلة وتحليل معطيات وبيانات الجرائم الالكترونية المرتكبة والبحث والتحري عن مرتكبي الجرائم عموما اذ استطاع المركز معالجة ازيد من 100جريمة الكترونية سنة 2014 وما يفوق 500 قضية رقمية خلال سنة 2015 منها 300جريمة تتعلق بمواقع التواصل الاجتماعي فايسبوك ، ومن 20جريمة رقمية تعلقت باختراق مواقع رسمية

[1]المرسوم الرئاسي رقم 09-143،المؤرخ في 02جامادى الاولى عام 1430 الموقف 27ابريل سنة 2009، يضمن مهام الدرك الوطني وتنظيمه ،الصادر في ج.ر.ج.العدد 26،بتاريخ 03مايو سنة 2009،ص17:جاء المادة الثانية 02 منه "الدرك الوطني قوة عسكرية منوطة بها الامن العمومي وتحكمه القوانين والتنظيمات الجاري بها العمل في وزارة الدفاع الوطني والقوانين والتنظيمات المتعلقة بهمة الامن العمومي وكذا احكام هذ المرسوم " .

لمؤسسات خاصة وعامة استهدف مجرموها انظمة المعالجة الالية للمعطيات[1] ، وفي الخمسة أشهر الاولى من سنة 2019 تم معالجة 1188 قضية بنجاح من مجموع 1515 مسجلة مع توقيف 1512 متورط ولأن الأطفال هم من أكثر الفئات العمرية تضررا من الجريمة الإلكترونية فقد قامت قيادة لدرك الوطني بمجوعة من البرامج التوعوية بالتنسيق مع وزارة التربية الوطنية من خلال دروس التوعية في المدارس التي جربت فيها تلك البرامج كخطوة أولى نحو زيادة وعي الطلاب بمخاطر الجريمة الالكترونية وحمياتهم منها[2].

ولأن عملية مواكبة التطورات والمستجدات الحاصلة في مجال التكنولوجيات الحديثة أمر لابد من السعي لتحقيقه في سبيل تقديم خدمات أمنية ترقى إلى تطلعات المواطنين عمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل متواصل، وذلك من خلال إنشاء مدارس ومعاهد لهذ الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني، والمعهد الوطني للشرطة القضائية بسحاولة والذي تم إنشاؤه سنة 1999 ليقوم بتكوين متخصصين في الشرطة القضائية وإجراء البحوث متعلقة بالظواهر الإجتماعية ذات الصلة بالجريمة[3].

---

[1] بارة سميرة ،الدفاع الوطني والسياسلت الوطنية للآمن السيبراني في الجزائر الدوور والتحديات ،ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من ملتقى الدوولي حول سياسات الدفاع الوطني بين الإلتزمات السياسية والتحديات الإقليمية كلية الحقوق والعلوم السياسية ،مخبر التحولات السياسية والإقتصادية والإجتماعية ، في التجربة الجزائرية ،جامعة قاصدي مرباح ،ورقلة يومي لإثنين والثلاء،30و31 جانفي 2017 ص ، 435-437.

[2] تقرير الصلحة الممركزية لمحاربة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، حول تشكيل عملياتي المحاربة الجريمة عبر شبكة العنكبوتية ،السالف الذكر ص70.

[3] مرسوم رئاسيرقم08_151، المؤرخ في20 جمادة الاولى 1429 الموافق26مايوسنة 2008، المتضمن استحداث مدرسة للشرطة القضائية تابعة لدرك الوطني ،المنشور بج.ر.ج ،العدد27،الصادر بتاريخ 28مايو 2008ص4 .

ومن أجل التحكم الجيد في الجرائم يضم الدرك الوطني في هياكله المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي والذي أطلق عليه إسم الشهيد بن "شيشة احمد"[1]، حيث يقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام بإجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية ، بالستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والأثار والوثائق المأخوذة من مسرح الجريمة بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجرائم بناءا على طلب من القضاة والمحققين أو السلطات المؤهلة ويقوم المعهد بالدعم التقني للوحدات أثناء التحقيقات المعقدة ، تصميم بنوك معطيات وإنجازها وفقا للقانون، المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام دورا فعالاً في مجال مكافحة الجرائم السيبرانية إذ تكلف دائرة الإعلام الآلي والإلكتروني بمعالجة وتحليل وتقديم كل دليل إلكتروني لفائدة أجهزة العدالة وتقديم مساعدة تقنية للمحققين في التحقيقات المعقدة كما تقسم دائرة الإعلام الآلي [2] ولإلكتروني إلى مخابر مخبر الإعلام الآلي مخبر الفيديو ومخبر الصوت لتحديد شرعية التسجيلات الصوتية مثلا وعلاوة على ذلك ، يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام من بين المؤسسات التي سيكون لها دور في مكافحة الجريمة الإلكترونية .

إن جميع الدول ملزمة على مواصلة جهودها الرامية إلى تطوير الهياكل المتخصصة في مكافحة الجريمة الإلكترونية داخل هيئات إنفاذ القانون وأجهزة النيابة العامة والجهاز القضائي ، بحيث تحصل على الخبرات والمعدات الازمة للتصدي للتحديات التي تفرضها الجريمة السيبرانية

[1] عبد العزيز ديلمي،دور الشرطة المجتمعية في الوقاية من الجريمة والإنحراف دراسة نظرية لبناء نموذج للشرطة الجوارية في الجزائر أطروحة مقدمة لنيل شهادة دكتوراه في العلوم الإجتماع الجريمة والإنحراف ، كلية العلوم الإنسانية والإجتماعية ،جامعة الجزائر 02،السنة الجامعية 2012-2013، ص479.

[2] شنتير خضرة مرجع سابق ص202.

ولجمع الأدلة الإلكترونية في الإجراءات الجنائية وتبادل المعلومات عنها وإستخدامها الإستخدام الأفضل حتى لا تفقد تلك الإجراءات مصداقيتها أمام الجهات القضائية المختصة.

المطلب الثاني : مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال على الصعيد الدولي والإقليمي.

المؤسسات الدولية والإقليمية لمكافحة الجريمة الإلكترونية، هي نماذج عملياتية وضعت من أجل المساعدة في عملية المكافحة بما لها من إمكانيات مادية وبشرية متخصصة في هذا النوع من الإجرام ، الذي لابد فيه من توطيد العلاقات بين كل تلك المؤسسات والهيئات ، والمصالح التي خصصت لمكافحة الجريمة الإلكترونية ، والتي سوف تقتصر الدراسة على أهمها ، فعلى المستوى الدولي نجد المنظمة الدولية للشرطة الجنائية أنتربول كمؤسسة دولية شرطية بارزة في مكافحة الجريمة الإلكترونية فرع أول ، وكذا آليات التعاون الدولي وما لها من دور بارز ومهم في مكافحة الجريمة الالكترونية فرع ثاني ، ليأتي الدور في الحديث على كل من الأفريبول واليوروبول والأوروجيست كمؤسسات إقليمية لمكافحة الجريمة الإلكترونية وهذا ماسنحاول شرحه من خلال هذ المطلب.

الفرع الأول :دور المنظمات الدولية في مكافحة الجريمة المعلوماتية

اولا :المنظمة الدولية للشرطة الجنائية الأنتربول "Enterpol"

تعد المنظمة الدولية للشرطة الجنائية الانتربول من أقدم صور التعاون الشرطي في مكافحة الجريمة ففي نهاية سنة 1923نجح الدكتور" جوهانو سويرا " مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية ، وذلك في فترة من الثالث 03 الى 07 من سبتمبر عام 1923 ضم مندوبي تسع عشرة 19 دولة ، وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية ، حدد مقرها بفينا تعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة ، والتي أطلق عليها إسم المنظمة الدولية للشرطة الجنائية لأنتربول سنة 1956

وحدد مقرها في المدينة ليون الفرنسية حيث تنقسم شبكة اتصالات الأنتربول إلى ثلاثة مستويات هرمية[1] المكاتب المركزية الوطنية المحطات الإقلمية والمحطة المركزية الموجودة في الأمانة العامة للأنتربول وتضم المنظمة الدولية للشرطة الجنائية الأنتربول حاليا حوالي 194 بلدا عضوا تستضيف كل دولة مكتبا مركزيا وطنيا الأنتربول يربط الشرطة الوطنية بشبكة الأنتربول العالمية ، وعند البحث عن علاقة بعض الدول بالمنظمة الدولية الجنائية نجد ان الجزائر إنخرطت في المنظمة مباشرة بعد الإستقلال ، أي في سنة 1963 وقد جسد المشرع الجزائري تلك العلاقة في العديد من النصوص القانونية ، كقانون الإجراءات الجزائية من خلال مفهوم إجراءات التسليم وآثاره ، سواء طبقا الإتفاقية أو بطريقة دبلوماسية ، وهذا بعد إنجاز الطلبات، الواردة في شكل إستمارات من الأنتربول أو بضمانات دولية.

أ) مهام المنظمة الدولية للشرطة الجنائية الأنتربول

كونها أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم تتمثل مهامها في مايلي:

- التعاون الدولي لمواجهة الإجرام الدولي المتزايد باستمرار.
- ومن المهام التي يقوم بها الأنتربول فيما يخص الجريمة الإلكترونية تعقب مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة .
- تعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الإتصال بحثا عن ما قد تحتويه من أدلة وبراهين تدل على إرتكاب الجريمة الإلكترونية إذ يتم تبادل المعلومات من خلال منصة الإتصالات الآمنة التي تعمل مدار الساعة ومن أجل تسهيل التحقيقات المتعلقة بالجرائم الإلكترونية التي تجريها وكالات وزارة العدل ووزارة الأمن الوطني.

[1] يوسف حسن يوسف ،الجرائم الدولية للانترنت ،الطبعة الاولى، المركزالقومي للادرات القانونية ،القاهرة ،مصر 2011ص146.

- تعزيز العلاقات بين الأنتربول ومنظمات الشرطة الإقلمية وغيرها من المنظمات الدولية لسد الثغرات وزيادة التكامل بينها ورصد الإتجاهات للكشف عن الجرائم الإنترنت والمجرمين الإلكترونيين ومجموعات الجريمة الإلكترونية[1].
- ضبط المجرمين أو توقيفهم مؤقتا إلى حين تسليمهم[2].

ب) دور الأنتربول في مكافحة الجريمة الإلكترونية

تمثل المنظمة الدولية للشرطة الجنائية أنتربول همزة وصل بين مختلف أجهزة الشرطة عبر العالم ومع المنظمات الإقليمية والدولية الأخرى من خلال موقعها الهام الذي يسمح لها بتعزيز قدرتها على منع الجريمة وتحديد هوية المجرمين واعتقالهم ، ولأن الجريمة الإلكترونية تعد إحدى أكبر التحديات التي تواجه مختلف دول العالم ، فإن منظمة أنتربول قامت ومازالت تقوم ببذل مجهودات من أجل مكافحتها والأمثلة على ذلك كثيرة نذكر منها على سبيل المثال : ماحصل في الجمهورية اللبنانية حين تلقت النيابة العامة اللبنانية برقية من الأنتربول في ألمانيا تم على إثرها توقف أحد الطلبة الجامعين.

من قبل القضاء اللبناني بتهمة إرسال صورة إباحية لقصر دون العاشرة أعوام من موقعه على شبكة الإنترنت وفي شهر مارس من العام 2008 قُدم للإنتربول[3]

الفرع الثاني: دور المؤسسات الاقليمية لمكافحة الجريمةالمعلوماتية

وضعت عدة مؤسسات إقليمية لمكافحة الجريمة كانتيجة توحيد مجهودات دول جمع بينها الموقع الجغرافي والحدود السياسية وتهديد المشترك الذي تفرضه الجرائم العابرة للحدود كما هو الحال في الجرائم الإلكترونية فنجد على سبيل المثال الأسيابول الخاصة بدول أسيا والأميربول

---

[1] حسين بن سعيد بن سيف الغافري المرجع السابق ص507،نقلا عن جميل عبد الباقي الصغير ،الجوانب الاجرائية للجرائم المتعلقة بالانترنت ،دار النهضة العربية ،القاهرة 1998،ص75.

[2] يمكن الرجوع الى الاتفاقيات التالية :الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية والحكومة الايطالية المؤرخ في 04محرم 1426الموافق 13فبراير 2005،الموقعة بالجزائر في 22جويلية سنة 2000 .

[3]أمير فرج يوسف ، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر ،المرجع السابق ص428.

الخاص بدول أمريكا واليوروبول،والأورجيست الخاص بدول أروبا والإتحاد الإفرقي للتعاون الشرطي الخاص بدول إفريقيا والموجود مقره في الجزائر العاصمة.

فهي كلها آليات مؤسساتية قوية جعلت لمكافحة هذه الظاهرة الإجرامية وتسهيل القبض على مرتكبها، ولكن نظرا لكثرة تلك المؤسسات ستقتصر الدراسة على ثلاثة منها وهي الإتحاد الإفريقي للتعاون الشرطي فرع الأول ومكتب الشرطة الأروبية اليوروبول والوكالة الأروبية للتعاون في مجال العدالة الجنائية الأورجيست الفرع الثاني

أولا:الأفريبول(Afripol) كمؤسسة إقليمية لمكافحة الجريمة الإلكترونية.

الإتحاد الإفرقي للتعاون الشرطي آفريبول هو آلية أنشئت من أجل مضاعفة رصيد التعاون الشرطي في الدول الإفريقية على المستويات الإستراتيجية وتكتيكية بين مؤسسات الشرطة في إفريقيا ولمنع الجريمة العابرة للحدود الوطنية والكشف عنها والتحقيق فيها بالتعاون مع المؤسسات الشرطة الوطنية والإقليمية والدولية ، ولقد شكلت الندوة الجهوية الإفريقية الثانية والعشرون 22 للأنتربول المنعقدة في سبتمبر 2013 بمدينة وهران بالجزائر فكانت الإنطلاقة الأساسية لإنشاء الأفريبول حيث تبنى المدراء والمفتشون العامون للشرطة من الدول الأعضاء للإتحاد الإفريقي فكرة إنشاء ألية للتعاون الشرطي الإفريقي ثم تلا ذلك عدة لقاءات ، أُعلن في القاء المنعقد في الجزائر بتاريخ الحادي العشر 11 من شهر فبراير سنة 2014 ، على إنشاء الآلية الإفرقية للتعاون الشرطي آفريبول ويعد إنعقاد الجمعية العامة الأولى الآلية للإتحاد الإفريقي للتعاون في مجال الشرطة الأفريبول بماثبة التأسيس الفعلي للأفريبول[1]، وحسب المادة 02 من النظام الأساسي الآلية الإتحاد الإفريقي للتعاون الشرطي أفريبول فإن هذه الأخيرة تعتبر مؤسسة تقنية باعتبارها آلية التعاون الشرطي بين الدول الأعضاء في الإتحاد الإفريقي وتستمد شخصيتها القانونية منه حيث تقوم الأفريبول على عدة مبادئ كما جاء في المادة الخامسة 05 من نفس

[1] براهمي جمال ،التحقيق الجنائي في الإلكترونية ،أطروحة لنيل شهادة الدكتوراه في العلوم ، تخصص القانون ،قسم الحقوق ، كلية الحقوق والعلوم الإنسانية ،جامعة ملود معمري ،تزي وزو نالجزائر نوقشت في 2018/06/27،ص308.

النظام والتي تضمنت بعض المبادئ المنصوص عليها في المادة 04 من القانون التأسيسي للإتحاد الإفريقي ومن هذه المبادئ نذك[1].

1. مهام الإتحاد الإفريقي للتعاون الشرطي آفريبول منها

- مساعدة مؤسسات الشرطة في دول الأعضاء على وضع إطار للتعاون بين المؤسسات الشرطة على المستويات الوطنية والإقليمية والقارية والدولية
- العمل على تطوير قدرات أجهزة الشرطة في الدول الأعضاء بواسطة برامج متطورة لتدريب الشرطة من خلال إنشاء مراكز إمتياز إفرقية وكذا تعزيز التنسيق مع هياكل مماثلة في منع ومكافحة الجريمة
- إعداد إستراتجية إفريقية منسقة لمكافحة مختلف أنواع الجرائم الخطيرة كالجريمة الإلكترونية ممايستدعي منها تطوير أنظمة الإتصال المناسبة وقواعد البيانات الضرورية لذلك تعتبر هذه المنظمة أداة فعالة وفاعلة لايمكن الإستغناء عنها في مجال التعاون الشرطي الذي سيضمن ردا مشتركا ومناسبا على كل التهديدات المستحدثة التي تواجهها بلدان إفريقا وتمس بالأمن والسلم العالميين.
- كما تعد منظمة الإتحاد الإفريقي للتعاون[2] الشرطي أفريبول إضافة نوعية بالنسبة للجزائر التي لها عدة مقومات تساعدها في أن يكون لها دوربارز في أمننة القارة الإفريقية خاصة وأنها إحتضنت مقرالأفريبول وتم إختيارها لرئاسة هذه المنظمة مرتين متتاليتين .

ثانيا: الأوروبول والأوروجيست

تعتبر اليوروبول والأوروجيست وكالتين مهمتين على المستوى الأروبي في مكافحة الجريمة الخطيرة بصفة عامة والجريمة الإلكترونية بصفة خاصة هذه الجريمة التي فرضت نفسها على جميع المستويات الدولية والإقليمية والوطنية مما إستوجب وضع آليات كفيلة للتصدي لخطورتها

---

[1] المواد 2-4-5 من القانون التأسيسي للإتحاد الإفرقي ،على الموقع الإلكتروني الموالي : https://au.int/sites تاريخ الإطلاع 2025/05/15.

[2] نقموش محمد ،ميلودية أحمد ،الجريمة المعلوماتية :مفهوم حتمية تطوير آليات التعاون الدولي في مجال مكافحتها ،مجلة الدراسات القانونية والسياسية ،جامعة عمارثلجي بالأغواط، الجزائر ،المجلد الرابع (04)،العدد الثاني ،جوان 2018،ص277.

ويعد جهاز الشرطة الأروبية المسمى اليوروبول أحدى تلك الآليات العملياتية التي لها دور مهم في مكافحة الجريمة الإلكترونية.

أ) اليوروبول(Eurepol) وكالة إقليمة لمكافحة الجريمة الإلكترونية

تم إقتراح إنشاء مكتب مركزي للشرطة الجنائية لدول الإتحاد الأوربي ، والمسمى حاليا اليوروبول في قمة لكسمبورج 1991ليتم إنشاؤه بشكل ملموس بموجب إتفاقية "ماستريخت" التي وقعت في السابع من شهر فبراير سنة 1999 بهولندة ودخلت حيز التنفيذ في الأول من نوفمبر سنة 1993 والأن الإتفاقية كانت تهدف الإقامة وحدة أروبية شاملة وإلى تحسين التعاون وتسير الإتصال وضمان تبادل المعلومات بشكل فعّال بين الدول الأعضاء في مجالات مختلفة خاصة مكافحة الجريمة تم تحديد مقر اليوروبول في مدينة لاهاي سنة 1994 ليحصل على الشخصية القانونية في الفاتح من الشهر أكتوبر سنة 1998 ليبدأ عمله بصفة فعلية في الأول من الشهر جويلية سنة 1999[1].

يحتل مكتب الشرطة الأوروبية يوروبول موقعا مركزيا في بنية الأمن الأروبي ويوظف أفضل محللي الجريمة المدربين في أروبا والذين يستخدمون أدوات فنية متطورة من أجل مساعدة الوكالات الوطنية في تحقيقاتها اليومية والأجل المكافحة الفعالة للجريمة الإلكترونية قام اليوروبول بإنشاء مراكز ووحدات تابعة له على غرار الفريق العامل المعني بالجريمة الإلكترونية السيبرانية التابعة للإتحاد الأروبي والذي تم إنشاؤه سنة 2010 داخل اليوروبول بهدف توفير منصة لمديري التحقيقات والملاحقات القضائية في مجال الجريمة الإلكترونية ولجعل الفضاء الإلكتروني مكانا أمنا لمواطني الإتحاد الأروبي ومؤسساته وحكوماته ويتألف من رؤساء الوحدات الوطنية لمكافحة الجرائم الإلكترونية لمختلف الدول الأعضاء بالإضافة إلى ممثلين عن المفوضية الأروبية وممثلين عن اليوروبول والأوروجيست [2].

---

[1] شنتير خضرة مرجع سابق ص 169 .

[2] نقموش محمد ، ميلودية أحمد، مرجع سابق ص277.

ولقد قدم هذا المركز إسهامات كثيرة في مكافحة الجريمة الإلكترونية من خلال عمليات الدعم العملياتي الفوري مما سهل في إعتقال المجرمين إضافة إلى قيامه بتحليل مئات الآلاف من الملفات والتي في غلبيتها تكون خبيثة أو تحتوي على فيروسات إلكترونية ، كما يهتم المركز بدراسة التهديدات التي قد يشكلها الإجرام الإلكتروني المنظم وبالأخص الإرهاب الإلكتروني وكل الجرائم الإلكترونية التي تؤثر على البنية التحتية الحيوية والمعلوماتية للإتحاد الأروبي والجرائم الإلكترونية التي تتسبب في أضرار جسيمة لضحاياهم مثل الإستغلال الجنسي للأطفال عبر الإنترنت ، وتعمل وكالة الشرطة الأروبية اليوروبول على مكافحة الجريمة الإلكترونية من خلال عدة وسائل وأدوات وبرامج وعمليات كالتي قامت بها في إطار مكافحة جريمة إستغلال الأطفال في إنتاج المواد الإباحية والمسماة عملية تحطيم الجليد والمنفذة في الرابع عشر من شهر جوان 2005 والتي تم خلالها مداهمة وتفتيش عدة دول أروبية منها النمسا بلجيكا فرنسا إيطاليا وغيرها تم خلالها توقيف أشخاص من تلك الدول.

ب) الأروجيست(Eurojust) كوكالة إقليمية لمكافحة الجريمة الإلكترونية .

بدأت الوكالة عملها رسميا في الفاتح من شهر سيبتمبر 2001 وبعد هجمات الحادي عشر من شهر من نفس الشهر 2001التي شهدتها الولايات المتحدة الأمركية إزداد التركيز على مكافحة الإرهاب ولم يعد الأمر ينصب على مجال الوطني والإقليمي فقط بل تعداه ليشمل البعد الدولي مما دفع المجلس الأوربي إلي إصدار قرار في الثامن والعشرون من شهر فبراير سنة 2002 تم من خلاله إنشاء الأوروجيست كوحدة تنسيق قضائي، مهمتها كما جاء في المادة 85 من معاهدة لشبونة دعم وتعزيز التنسيق والتعاون بين السلطات الوطنية المسؤولة عن التحقيق في الجرائم الخطيرة التي تمس دولتين أو أكثر من الدول الأعضاء أو مقاضاتها على أساس العمليات المنفذة والمعلومات المقدمة من سلطات الدول الأعضاء واليوروبول ،وبعد مفاوضات مكثفة إعتمد البرلمان والمجلس الأوروبين لائحة الأوروجيست " Eurojust "الجديدة في

نوفمبر 2018 والتي بدا تطبيقها في ديسمبر 2019 وأصبح لها شخصية قانونية تضطلع بعدة مهام[1] نذكر منها:

- بإمكان الأروجيست مكافحة مستويات متزايدة من الجرائم الخطيرة العابرة للحدود والتي تعد الجريمة الإلكترونية أحدها .
- تدعم وتعزز التنسيق والتعاون بين السلطات الوطنية المسؤولة عن التحقيقات والملاحقات القضائية المتعلقة بالجرائم الخطيرة على أساس العمليات التي نفذت والمعلومات التي قدمتها سلطات لدول الأعضاء واليوروبول والأنتربول ومكتب المدعي العام الأروبي ومؤسسات وهيئات ومكاتب ووكالات الإتحاد المسؤولة والمتخصصة خاصة إذا كانت الجريمة لها تأثير على دولتين أو أكثر من الدول الأعضاء أو يتطلب الأمر محاكمة على أسس مشتركة .
- وتقوم الأروجيست أيضا بتقديم أراء في حدود صلاحياتها إلى اليرروبول بعد دراسة التحليلات التي أجراها بمبادرة منها أوبناء على طلب مكتب المدعي العام الأروبي.

بالضافة إلى هذه المهام يمكن الوقوف على دور المهام الذي تلعبه وكالة الأوروجيست في مكافحة الجريمة المعلوماتية على الصعيد الأوروبي كونها ساعدت على تذليل العديد من الصعوبات خاصة منها الإجرائية التي تواجهها الدول الأروبية[2].

الفرع الثالث :التعاون الدولي ودوره في مكافحة الجريمة الإلكترونية.

بالضافة إلى الآليات التي تم التعرض إليها توجد آليات أخرى لاتقل أهمية عن سابقتها ألا وهي التعاون الدولي فهو التبادل العون والمساعدة وتظافر الجهود المشتركة بين دولتين أو أكثر لتحقيق نفع أو خدمة مشتركة سواء عالميا أو إقليميا كما أنه كل ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف معاقبتهم على جرائمهم وذلك من خلال تدابير وقائية تستهدف الصيغة غير الوطنية للجريمة التي تتطلب إمكانيات لا تملكها السلطات

---

[1] .eu www.eurojust.europa :// https للمزيد بخصوص هذ المسالة الرجوع إلى الموقع الإلكتروني للأوروجيست .

[2] صايش عبد الملك ، الجهزة الأروبية المكلفة بماكفحة الهجرة السرية مهمة مستحيلة بمعدات عسكرية ،المجلة الأكادمية للبحث القانوني ،كلية الحقوق والعلوم السياسية ، جامعة عبد الرحمن ميرة ،بجاية ،جزائر ،مجلد 11،العدد2015،1،ص20.

القانونية لدولة واحدة مالم تدعمها وتساندها جهود السلطات القانونية في الدولة الأخرى فهو يساعد في تنفيذ القرارات التعاونية التي من شأنها وضع حد الأنشطة غير القانونية خاصة المرتكبة عبر الإنترنت ،ويتجسد التعاون الدولي من خلال دور المنظمات والمعهدات والإتفقيات[1] الدولية في مكافحة الجريمة المعلوماتية .

أولا :الإتفاقيات ودورها في مكافحة الجريمة المعلوماتية :

تظهر أهمية الجهود الإقليمية والدولية في مواجهة الجريمة الإلكترونية من خلال العمل على مكافحة هذه الجريمة ، والتي رسخت في مساعي عقد وإبرام الإتفقيات الدولية الثنائية والمتعددة الأطراف والذي برز بدوره كعنصر فعال في مكافحة الظاهرة خصوصا المحافظة على الثقة المتبادلة بين الدول في تقديم مساعدة الفنية والتقنية والأمنية والقضائية الأمر الذي جعلها تضع توصيات وتبرم إتفقيات تدرج في تشريعات داخلية لدول الأعضاء وتعالج كل ما هو مستحدث في مجال التقدم العلمي والتكنولوجي الرقمي تعد الإتفاقيات الدولية والمعاهدات من أهم صور التعاون الدولي بصفة عامة ، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة ومن بين الإتفقيات نذكر:

1. **إتفاقية بودابست** : تم إبرام أول معاهدة دولية متعلقة بمكافحة الجريمة الإلكترونية أو جرائم الإنترت سنة2001 بالعاصمة المجرية بودابست تم صياغة المعاهدة من طرف عدد كبير من الخبراء المختصين في القانون في مجلس أروبا وبمساعدة دول أخرى لاسيما الولايات المتحدة الأمركية وبعد مشاورات عديدة بين خبراء المعلوماتية والكمبيوتر وأجهزة إنفاذ القانون على مستوى العالم أدى في النهاية إلى توقيع عليها من قبل 30 دولة بتاريخ 23نوفمبر 2001[2] في العاصمة بودابست حيث حددت أهم الإجراءات القضائية والمتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب إتفاقيات دولية .

[1] شنتير خضرة مرجع سابق ص217.

[2] الطاهر ياكر مرجع سابق ص188.

2. الإتفاقية العربية لمكافحة الجرائم الإلكترونية.

مع تطور العصر الرقمي وتنامي المساعي لبناء مجتمع مرتكز على المعلومات والمعرفة كان لابد من تحديث الأطر التنظمية والقانونية لتتلائم مع المتطلبات الحديثة الخاصة بالفضاء السيبراني وزيادة تجانسها وتعتبر التشريعات السيبرانية عنصرا أساسيا في توفير البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات والمعرفة ولبناء الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الإنترنت وبالرغم من الجهود الواعدة التي تقوم بها بعض الدول في المنطقة العربية لاتزال معضمها بعيدة عما وصلت إليه الدول المتقدمة في هذ المجال وبما أنها ليست بمنأى عن تهديدات الجريمة الإلكترونية كون هذه الأخيرة عابرة للحدود ومن أجل تظافر الجهود لمواجهتها إعتمدت الجامعة العربية مايسمى بقانون العربي الإسترشادي الذي تم إعتماده من قبل مجلس الوزراءالعدل العرب في دورته 19بالقرار رقم 495 الدورة 19بتاريخ 8اكتوبر 2003ويعد هذا القانون من أبرز الجهود العربية المبذولة في مجال مكافحة الجريمة لإلكترونية ، وفي نفس السياق نجد الإتفاقية العربية لمكافحة جرائم تقنية العلومات والتي تم التوقيع عليها في القاهرة 2010/12/21وتهدف الإتفاقية حسب المادة الأول منها إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفظا على أمن الدول العربية ومصالحها وسلامة مجتمعها وأفرادها[1].

إلاأن هذا التعاون تعيقه صعوبات فقد أدى إختلاف المفاهيم المتعلقة بتعريف الجرائم الإلكترونية بين تشريعات الدول إلى وضع قاون محدد لمكافحتها كما تواجه عملية مكافحة هاته الجريمة عدة صعوبات في التعاون الدولي ، نذكر منها على سبيل المثال لا الحصر ما يلي:

- ✓ عدم وجود نموذج موحد للنشاط الإجرامي : فالأنظمة القانونية التي وضعت من أجل مكافحة الجرائم الإلكترونية يختلف وصفها للأفعال الإجرامية التي تتم بها هذه الجرائم ، فقد نجد أنواعا من الجرائم الإلكترونية مباحة في نظم قانونية معينة ومجرمة في أخرى، فبغير التعاون الدولي في مجال التشريع العقابي سيزداد معدل إرتكاب الجرائم الإلكترونية ويطمئن ويرتكب

[1] لخضر دهيمي ،النظام القانوني لعمل الشرطة في الجزائر اطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي، جامعة البليدة 02 السنة الجامعية 2015/2014،ص244.

مرتكبوها من عدم إمكانية ملاحقتهم إذ سيكون من السهل عليهم التنقل من دولة تجرم الفعل إلى أخرى تبيح قوانينها ذلك الفعل .

- ✓ تنوع وإختلاف النظم القانونية الإجرائية : المتمثلة خاصة في طرق التحري والتحقيق والمحاكمة كما هو الحال بالنسبة لطرق جمع الأدلة الإلكترونية ، فهذه الإجراءات قد يكون لها قيمتها القانونية في دولة ما وعدمها في دولة أخرى مما ينجر عنه عدم فائدة تلك الإجراءات التي قد تكلف الدولة القائمة بها جهود بشرية وتكاليف مادية كبيرة ليحصل منها المجرم الإلكتروني في الأخير على فرصة للإ فلات من العقاب في حال عدم وجدوها والإعتداد بها أمام القضاء ، وتعد قضية الدودة الحاسوبية أحسن مثال على ذلك ، حيث تم إعداد هذا الفيروس في الفلبين سنة 2000، وعند إطلاقه أصيب على إثره الملاين من الحواسيب في جميع أنحاء العالم ولكن التحقيقات لم تجر حينها بسبب أن ذلك الفعل لم يكن مجرما أنذاك في الفلبين.
- ✓ مشكلة الإختصاص في الجرائم الإلكترونية : من أكبر المشاكل التي تواجه مكافحة الجريمة الإلكترونية إذ ينتج لنا مايسمى بتنازع الإختصاص بين الدول وإفلات المجرمين الإلكترونين بجرائمهم الإلكترونية التي تتنازعها مبادئ الإختصاص التقليدية كمبدأ الإقليمية ومبدأ الشخصية ومبدأ العينية .
- ✓ التجريم المزدوج:

يعتبر نظام تسليم المجرمين من الأنظمة التي تساهم بصورة إيجابية وفعالة في تحقيق الإستقرار العالمي ،إلا أن التجريم المزدوج الذي يفرض في تسليم المجرمين يعد عقبة كبيرة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة الإلكترونية وغيرها من الجرائم

- ✓ صعوبات خاصة بالمساعدات القضائية الدولية : تعرف المساعدة القضائية بأنها كل إجراء قضائي تقوم به دولة من شأنها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم وتتخذ المساعدة القضائية عدة[1]صور نذكر منها :

[1] يقصد به أن يكون الفعل المطلوب التسليم بشأنه معاقبا عليه في القوانين كلتا الدولتين الطالبة التسليم والمطلوب إليها ذلك و إن لم يحقق هذا الشرط بالنسبة إلى الدولة التي تتمسك به فإنه يرفض التسليم لعدم توافر الشرطه.

أ) **تبادل المعلومات** :متمثل في تقديم معلومات ووثائق والإستدلالية والمواد للجناة التي تتطلبها سلطة قضائية أجنبية حين النظر في الجريمة ما ، وجهت فيها الإتهامات لشخص لايتواجد تحت سلطتها .

ب)**نقل الاجراءات** : ويقصد به قيام دولة ما بناءا على إتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة أرتكبت في إقليم دولة أخرى ولمصلحة تلك الدولة متى توافرت شروط معينة من أهمها أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوبة منها نقل الإجراءات ، وأن تكون تلك الإجراءات مقررة في قانون الدولة المطلوب منها القيام بها عن ذات الجريمة ، وقد أقرت العديد من الإتفاقيات الدولية والإقليمية هذا النوع من المساعدة ، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية في المادة 22 منها ، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة سنة 2000 المادة 21 منها[1].

ت)**الإنابة القضائية الدولية** :ويقصد بها ذلك الطلب الذي تقدمه الدولة الطالبة إلى الدولة أخرى مطلوب منها إتخاذ إجراء قضائي من إجراءات الدعوى الجنائية لما لذلك الإجراء من أهمية في تلك الدعوى القائمة أو لتعذر القيام به نتيجة الإصطدام بالسيادة الدولية ولأجل تسهيل تلك الإجراءات الجنائية بين الدول ، جاءت الإنابة القضائية كحل يكفل إجراء التحقيقات اللازمة كاتفتيش وسماع الشهود وغيرها ولكن نظرا لتعقيد إجراءات الإنابة القضائية والفوارق الإجرائية

فيها نتيجة نقص الموظفين المدربين ،والصعوبات اللغوية التي يواجهونها ، أدى ذلك إلى تعقد الإستاجبة وبطئها وهو مالا يسجيب لطبيعة التعامل مع الجرائم الإلكترونية[2].

---

[1] شنتير خضرة مرجع سابق ص220.

[2] عبد العزيز أحمد ، خصوصية التحقيق في الجريمة المعلوماتية ،مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية ،السنة الجامعية 2022/2021. ص85

المبحث الثاني :آليات البحث والتحري للكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

أصدار المشرع للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها قد أرسى قواعد إجرائية جديدة تخضع لها السلطة القضائية وأعوانها تطبيقا لمبدأ الشرعية ، الذي يعد حجر الزاوية في الإجراءات القانونية للتحقيق في الجرائم المرتكبة ومتابعة فاعليها وتوقيع العقوبة المناسبة لهم ،هذه الإجراءات الجديدة التي يستطيع بها رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لايمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقلدية فقط التي أرسها قانون الإجراءات الجزائية ، لذلك سيكون تقسيم هذا المبحث على نحو يسمح بالتعرف على الأدلة الرقمية وأساليب إستخلاصها وفقا للمطلبين التاليين :

المطلب الأول: طرق التحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال .

المطلب الثاني: الدليل الإلكتروني وسلطة القاضي في تقديره.

المطلب الأول : طرق التحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

إن الجرائم المرتكبة عن طريق الشبكة المعلوماتية الإنترنت والشبكات الرقمية تتطور بدون توقف مرتبطة بالتطور التكنولوجي فمنذ 2006 كان من أولويات المشرع الجزائري تدعيم الإجراءات الجزائية بوسائل قانونية للتحقيق من أجل جمع الأدلة الرقمية تحت شروط تجعل منها أدلة أصلية على الصعيد القانوني نجد القانون رقم 22/06المؤرخ في 2006/12//20[1] المعدل لقانون الإجراءات الجزائية الذي إحتوى على مجموعة من الإجراءات الجديدة لمكافحة أنواع

[1]القانون رقم 22/06 المؤرخ في 2006/12/200 المعدل وتمم للقانون رقم 155/66 المتضمن قانون الاجراءات الجزائية

محددة من الجرائم ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجريمة المنظمة العابرة للحدود والقانون رقم 04/09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، يحوي هذا القانون تدابير مهمة لتدعيم فعالية وسرعة التحريات والتحقيقات الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال

وعلاوة على الأدوات المدرجة في قانون الإجراءات الجزائية الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال مثل إعتراض المرسلات، أوجد المشرع وسائل أخرى أكثر فعالية مثل : التفتيش المعلوماتي ، حجز المعلومات ، التفتيش عن بعد ، إدرجها ضمن قانون04/09 السالف ذكره وقبل التطرق لعناصر هذا المطلب الأجدر بينا تعريف التحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وهو مايعرف بالتحقيق الرقمي، وهو مجموعة الأساليب المتبعة من أجل معرفة وتقديم معطيات مخزنة في وسيلة إلكترونية ممغنطة أمام جهة قضائية.

الفرع الأول : طرق التحقيق التقليدية في الجرائم تكنولوجيا الإعلام والإتصال.

تعد مرحلة جمع الإستدلالات من المراحل المهمة في مجال الجرائم المعلوماتية والتي يقوم بها رجال الضبطية القضائية ، وهي مرحلة التي تسبق مرحلة التحقيق الإبتداء التي تقوم به النيابة العامة ، وقد إستقر الأمر في أغلب التشريعات على أهمية هذه المرحلة باعتبارها مرحلة أساسية بالنسبة للسلطات المختصة بتحريك الدعوى العمومية ، فعملية جمع الإستدلالات من إختصاص الضبطية القضائية من حيث تقصي الجرائم والبحث عن مرتكبها وبذالك تعتبر خط الدفاع الأول ضد الجرائم المرتكبة سواء كانت من الجرائم التقليدية أو من الجرائم المستحدثة الإلكترونية يتطلب كشف جرائم الحاسوب والوصول إلى مرتكبها وملاحقتهم قضائيا إجراءات خاصة تتعلق بإكسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب.

أولا : الإنتقال إلى مسرح الجريمة الإلكترونية :

معاينة مسرح الجريمة من أهم إجراءات التحري والتحقيق في كافة الجرائم التي نص عليه المشرع الجزائري في المادة 61 من ق.إ.ج ينتقل بمقتضاه المحقق أو القاضي لمكان وقوع الجريمة ليشاهد بنفسه ويجمع الأثار المتعلقة بها ويقوم بجع الأشياء التي تفيد في كشف الحقيقة ويعد مسرح الجريمة بمثابة الشاهد الصامت الذي إذا أحسن المحقق إستنطاقه حصل على معلومة مؤكدة ، أما الجريمة الإلكترونية فمسرح الجريمة فيها داخل بيئة الحاسوب[1]، والبيانات الرقمية التي تتواجد وتنتقل داخل بيئته وشبكاته ، وفي ذاكرته والأقراص الموجودة بداخله فالمقصود بمعاينة مسرح الجريمة الإلكترونية هو معاينة الأثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت والتي تشمل الرسائل المرسلة منه أو الواردة إليه وكافة الإتصالات الإلكترونية التي تمت من خلال الحاسب والشبكة العالمية فالمعاينة تتم داخل تلك الأجهزة كما تتم داخل شبكة الإنترنت نفسها عن طريق بيانات المتهم ، كالولوج إلى بريده الإلكتروني أو معاينة حسابه على مواقع تواصل الإجتماعي ، كما يمكننا من خلال معاينة الحساب الآلي للمتهم معرفة المواقع الإلكترونية التي زاراها ، أو الملفات التي حملها والحسابات التي إخترقها فالمعاينة في الجريمة الإلكترونية ليست مسألة مرتبطة بالضرورة لإنتقال عبر العالم المادي بل قد تتم عبر العالم الإفتراضي وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أو مأمور الضبط القضائي أن ينتقل من خلالها إلى العالم الإفتراضي للمعاينة من ذلك:

- من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به .
- كما يمكنه اللجوء إلى مقهى الإنترنت .

[1]ممدوح عبد الحميد عبد المطالب ،دار الكتب القانونية ،المحلة الكبرى ،مصر 2006،ص35.

- وأيضا يجوز له اللجوء إلى مقر عمل مزود خدمة الإنترنت الذي يعتبر أفضل مكان يمكن إجراء المعاينة فيه[1].

أ) ونظرا لأهمية الأدلة الإلكترونية المسقاة من مسرح الجريمة والتي تكون غالبا ذات دلالة قاطعة في الإثبات، فقد أكدت المعاينة الفنية في كثير من الأحيان فعاليتها في إظهار حقيقة الجريمة ومعرفة كيفية وأسباب وقوعها وهوية ومرتكبها ، لذلك يترتب على المحقق مراعاة الدقة والترتيب وبذل أقصى ما يمكن من العناية والإهتمام عند إجرائه للحيلولة دون فقدان مايمكن إستخلاصه من معلومات قيمة قد تفيد في تنوير التحقيق ولمعاينة مسرح الجريمة المعلوماتية لبد من تفرقة بين أمرين:

أ) معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardworde)

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من المكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة .

ب) معاينة الجرائم الواقعة على المكونات المنطقية غير مادية أو بواسطتها (software) كتلك الواقعة على برامج الحاسوب وبياناته، وهذا ما يثير العديد من الصعوبات فالمعاينة عندما تنصب على مكونات المعنوية هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات....إلخ.

ومن أجل أن تتم المعاينة بشكل صحيح ولأنجاح في الجرائم المعلوماتية وصى الخبراء بموجب إتباع ومرعاة قواعد وإرشادات فنية أبرزها مايلي :

[1] محمد زكي أبوعامر ، الإجراءات الجنائية ،الطبعة الثامنة ،دار الجامعة الجديدة 2008،ص123 ومبعها

- الإعداد الجيد قبل المعاينة بحيث يكون هناك فرق متخصصة في هذا النوع من الجرائم المتكونة من خبراء وفنيين ومحققين لهم تكوين عال في ميدان مكافحة الجريمة الإلكترونية ويتم وفق وضع مخطط تفصيلي مدروس حتى لا تضيع الإدلة ويذهب مجهودهم سدى .
- تحديد أجهزة الحواسيب الموجودة وتحديد مواقعها بأسرع وقت ممكن إضافة إلى البحث عن مزود الخدمة بالإنترنت "مودام" من أجل قطع الإتصالات الخارجية التي يمكن أن تخرب الأدلة أو تمحوها من ذاكرة الحاسوب، كما يرعى ضرورة أخذ صورة رقمية عن الأجهزة الموجودة وخاصة الأجزاء الخلفية التي تحمل الأرقام التعريفية للأجهزة المتحفظ عليها .
- ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة مع رصد الإتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث والرابع في تدمير الأدلة من خلال إتصالها بالأجهزة محل المعاينة.
- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ماتكون طويلة وذلك بين إقتراف الجريمة والكشف عنها الأمر الذي يمنح فرصة الأحداث تغييرات أو العبث بالأثر المادية أو زوال بعضها مما يؤدي إلى غموض الدليل المستقى من المعاينة .
- عدم التسرع في نقل أي مادة معلوماتية من مسرح الجريمة وذلك قبل إجراء إختبارات لازمة من عدم وجود أي مجالات مغناطسية في المحيط الخارجي لموقع الحساب الآلي والتي قد تؤدي الى إتلاف البيانات المخزنة مباشرة في حالة تعرضها لها .

- تصوير جهاز الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والملحقات والتحفظ على المستندات الخاصة بالإدخال وكذلك ملحقات الحاسب الآلي المادية والورقية التي قد تحمل آثار لإرتكاب الجريمة ، مع مرعاة تسجيل تاريخ ومكان إلتقاط كل صورة [1].
- الحرص على عدم إتلاف أي بيانات يتم إستخراجها من الجهاز والتأكد من وجود نسخة منها داخل الجهاز نفسه مع الفحص الدقيق لكل الملفات للتعرف على جميع العمليات التي قام بها مستخدم الجهاز والمواقع التي إرتادها على شبكة الإنترنت وكذا أسماء حساباته في مواقع التواصل الإجتماعي وكلمات المرور الخاصة به.
- يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات و الخيوط الكهربائية للحاسوب والتي تكون متصلة بمكونات النظام حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة .
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الإختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة .
- الملاحظة الجيدة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء .
- تحفظ على ما تحتويه سلة المهملات الإلكترونية من معلومات أو الملفات أو أوراق كربون نسخ ، أو أقراص ممغنطة سليمة أو محطمة مع فحصها ورفع البصمات عنها .[2]

ثانيا: تفتييش الأنظمة المعالجة الآلية للمعطيات وضبطها .

---

[1] عبد الكريم خالد،الردايدية ،ص11

[2] أحمد يوسف الطحطاوي ،الادلة الالكترونية ودورها في الاثبات الجنائي ، دراسة مقارنة دار النهضة العربية القاهرة مصر 2015ص134.

يقصد بالتفتيش" التقصي والبحث عن الأدلة سعيا وراء ضبطها بقصد الإستعانة القانونية بها لإدانة المتهم ، بالتالي ينبغي القيام بضبط مايترتب عليه التفتيش بطريقة علمية حتى لا يفقد قيمته القانونية .

أمام القضاء إذ تطلب الأمر ذلك ، فقد نصت المادة 05 فقرة 01 من قانون 04/09 "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي محالات المنصوص عليها في المادة 04 المذكورة أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

أ) منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
ب) منظومة تخزين معلوماتية ...

ويقصد بالمنظومة المعلوماتية حسب ما عرفها المشرع في المادة 02 فقرة ب بأنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

كما وسعت المادة 5 الفقرة الثالثة في إجراءالتفتيش بنصها:"...إذاتبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ".

في جميع الأحوال يعتبر التفتيش أو الولوج كما يفضل تسميته بعض المحقيقين الجنائين في الجريمة الإلكترونية[1]، أهم إجراءات التحقيق لأنه ينتهي في أغلب الأحيان بضبط الأدوات التي

[1]عبد الصديق الشيخ ،الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد ،ص198.

أستعملت في إرتكاب الجريمة ، أوضبط أي شيئ أخر يفيد في كشف الحقيقة والمستهدف في التفتيش بالنسبة للجريمة المعلوماتية هو الحاسوب بمكوناته المادية والمعنوية[1].

1. تفتيش مكونات المادية الحاسوب :

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة للبحث في أي شيئ يتصل بجريمة معلوماتية للكشف عنها ، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، الا أن هناك حالات خاصة للتفتيش في هذه المكونات هي: في حالة كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات ،إذا وجدت مكونات الحاسوب المادية في حالة الحاسوبات الآلية المحمولة في الأماكن العامة بطبيعتها كالمطاعم سيارات الأجرة ..إلخ فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات [2].

2. تفتيش المكونات المعنوية الحاسوب المنطقية:

عرف الفقه الجنائي إختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراءات التفتيش يرى البعض عدم جواز التفتيش المكونات المعنوية للحاسوب ، وقد عملت الدول التي تبنت هذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية ، إتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل مايشغل حيزا ماديا في فراغ معين جاز تفتيش هذا الحيز ويمكن قياسه والتحكم فيه، وبناءًا عليه فإن الكيان المنطقي للحاسوب أو

[1] أحمد موسى مريم مرجع سابق ص86 .

[2] عبد القادر فلاح ،أيت عبد المالك نادية ،التحقيق الجنائي في الجرائم الإلكترونية وإثباتها في التشريع الجزائري ،مقال منشور في مجلة الأستاذ الباحث للدراسات ،القانونية والسياسية ،المجلد04،العدد02،السنة 2019ص10.

البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ، يقاس بالبيت والكيلو بايت والميغابايت غير أن النصوص القانونية التي تنص أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء المادية.

وقد إتفقت بعض التشريعات كاتشريع الكندي في المادة 487 التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شئ يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها ونصت صراحة على إمكانية تفتيش مكونات الحاسوب المادية للكشف عن الجريمة المعلوماتية بإتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها.

رابع : شروط إجراء عملية التفتيش في الجريمة الإلكترونية في تشرع الجزائري .

لأجل مكافحة الجريمة الإلكترونية سمحت العديد من القوانين بالتفتيش عن هذه الجريمة والحصول على دليل إلكتروني يمكن من خلاله إثبات أو نفي هذه الأخيرة عن المتهم أو المتهمين بها ففي التشريع الجزائري كانت بعض المواد في قانون 04/09 مصدر مشروعية لهذا الإجراء فقد جاء في المادتين 03 و05 منه أنه[1]" في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني أو مقتضيات التحريات والتحقيقات ،وفي إيطار قانون الإجراءات الجزائية يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها أو دخول وتفتيش منظومة تخزين معلوماتية ولأن التفتيش يمس بخصوصية الأفراد ومستودع أسرارهم خص هذا الإجراء بمجموعة من الضمانات التي تسمح بايجاد توازن بين مصلحة العامة والخاصة " والمادة 44 من ق .إ.ج .ج تضمنت مجموعة من ضمانات ، إذ لايكن القيام بعملية تفتيش مساكن الأشخاص الذين يظهر أنه مساهمو في جناية أو جنحة متلبس بها أو تحقيق في الجرائم

[1] قانون 09-04 السالف الذكر.

الإلكترونية أو تفتيش مساكن أشخاص يتبين أنهم يحوزون أوراق أو أشياء لها علاقة بالأفعال الجرمية المرتكبة إلا بإذن مكتوب صادر من وكيل الجمهورية أو من قاضي التحقيق مع التأكيد على ضرورة إضهار الإذن قبل الدخول وشروع في التفتيش كما تأكد نفس المادة أن يتضمن الإذن وصفاً للجرم المرتكب وكذا عنوان الأماكن التي سيتم التفتيش فيها كل ذلك تحت طائلة البطلان .

في هذا الإطار ومن خلال إستقراء المواد القانونية ، خاصة قانون الإجراءات الجزائية يتبين أن المشرع الجزائري قصد مراعاة القواعد الإجرائية المنصوص عليها قانونا والمتعلقة بدخول المنازل وفقا للمواد 44،45،47 من ق.إ.ج.ج، وذلك حينما يتعلق الأمر بتفتيش منظومة معلوماتية لحاسب آلي موجودة في منزل أو محل له خصوصيته ، ولأن المادة 81 من ق.إ.ج.ج نصت على أن عملية التفتيش تباشر في جميع الأماكن التي يمكن العثور فيها على أشياء تكون مفيدة لإظهار الحقيقة ، وعليه فإن البحث في مجال الجريمة الإلكترونية يشمل الأشخاص الطبعية والمعنوية وأجهزة الحاسوب وملحقاته أي كل مايمكن أن يكون ذا طبيعة مادية أو معنوية كما يجوز تمديد التفتيش إلى نظم معلوماتية أخرى قد تكون داخل أو خارج الدولة بغرض تفتيش عن بعد هنا لا يكون التفتيش الإ بموجب طلب مساعدة من السلطات الأجنبية المختصة طبقا للإتفقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

خامسا: :حجز المعطيات (ضبط المعطيات)

يعتبر ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش وغايته ، ويقصد به وضع اليدعلى شئ يتصل بالجريمة ويفيد في كشف الحقيقة وعن مرتكبها وهو يرد إلاعلى الأشياء المادية، وبالتالي الصعوبة ليست في ضبط أدلة الجريمة الواقعة على مكونات المادية للكمبيوتر كالبصمات مثلا إنما تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وكذا المكونات المعنووية للحاسوب ، وفي هذا الإطار إختلفت التشريعات الإجرائية

ولإتجهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية التي لا يصلح بطبيعتها محلا لوضع اليد ،فيرى البعض أنه لا يمكن تصور إجراء ضبط على الكيانات المعنوية للحاسب الآلي لإنتفاء الكيان المادي عنها وبالتالي عدم صلاحيتها أخذ بهذ الإتجاه التشريع الألماني، في حين يرى إتجاه أخر أن معطيات المخزنة آليا تصلح أن تكون محلا للضبط المنصوص عليه في النصوص التقليدية[1].

أما المشرع الجزائري نظم ضبط أو حجز الأدلة الإلكترونية في عدة مواد قانونية منها المادة 06 قانون 04/09[2] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،التي جاء فيها :"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية ،معطيات مخزنة من ضبط أو حجز معطيات تكون مفيدة في كشف الجرائم أو مرتكبيها ، وجاء في الفقرة الرابعة من المادة 15 من المرسوم الرئاسي رقم 20-183[3] الذي يتضمن إعادة تنيظم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها على أن مدرية المراقبة الوقائية واليقظة تتولى مهمة "جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض إستعمالها في الإجراءات القضائية "، ودون أن ننسى مواد قانون الإجراءات الجزائية ، وخاصة المواد 45، 47، والمادة 84 من ذات القانون ،والتي أشارت إلى ضرورة أن لا يتعدى الضبط الأشياء والوثائق النافعة في إظهار الحقيقة، وعملا بالمادة 07 من القانون الجزائري رقم 09-04 المتضمنة الإجراءات الخاصة بالحجز عن طريق منع الوصول إلى المعطيات إذا إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 السالفة الذكر لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة

---

[1] عبد الصديق الشيخ مرجع سابق ص200.

[2] قانون 09-04

[3] المرسوم الرئاسيرقم 20-183 سالف الذكر.

لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

وفقا للمادة 08 من قانون العقوبات الجزائري رقم 09-04 المتضمنة الاجراءات الخاصة بالمعطيات المحجوزة ذات المحتوى المجرم يمكن لسلطة التي تباشر التفتيش ان تامر باتخاذ الإجراءات الازمة لمنع الإطلاع على المعطيات التي يشكل محتوها جريمة لاسيما عن طريق تكليف اي شخص مؤهل باستعمال الوسائل التقنية لذلك[1].

وطبقا للمادة 09 من قانون الجزائري رقم 09-04 المتضمنة الأحكام الخاصة بحدود إستعمال المعطيات المعلوماتية المتحصل عن طريق المراقبة الإلكترونية المنصوص عليها في المادة 04 من قانون 09-04 تحت طائلة العقوبات المنصوص عليها عن طريق إجراءات الحجز المعطيات المعلوماتية إلا في حدود الضرورة للتحريات أو التحقيقات القضائية .

الفرع الثاني طرق التحقيق المستحدثة في الجرائم الماسة بأنظمة المعالجة الآلية للبيانات

على الرغم من كل ماتمت الإشارة إليه بخصوص حرمة الحياة الخاصة للأفراد ، إلا أن طبيعة الجريمة الإلكتروني وخطورتها ، فرضت على المشرعين وضع نصوص قانونية يكون بموجبها للسلطات المختصة في البحث وتحري ومراقبة جانب من تصرفات الأفراد للوصول إلى أدلة المطلوبة والمشرع الجزائري واحد من أولئك المشرعين إذ أوجد أساليب بحث وتحري خاصة نصت عليها بعض المواد كالمادتين 03 و 04 من قانون 04/09 واللتان نصتا على إمكانية إجراء المراقبة الإلكترونية ووضع ترتيبات تقنية مراقبة الإتصالات الإكترونية وتسجيل محتواها في حينها إذا إستدعت مقتضيات حماية النظام العام ذلك ، نظرا لخطورة الجريمة الإلكترونية وصعوبة إكتشاف المجرم الإلكتروني وإيجاد الأدلة المناسبة للتحقيق.

[1]انظر ج.ر.ج العدد47 المؤرخة في 16اوت 2009 ص06.

التقليدي ، قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية وقانون 04/09 سالف الذكر وهي : إعتراض المراسلات وإلتقاط الصور و التسرب

أولا : إعتراض المراسلات

إن الإعتراض والتسجيل والإلتقاط والتسرب هي عدة تسميات يمكن إختزالها في مصطلح واحد هو المراقبة التي لا تخرج عن كونها رقابة مشروعية لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مرئية نتيجة الإشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها نظرا لطابع السرية الذي يكتنفها.

وإعتراض المراسلات هو نوع من أنواع المراقبة الإلكترونية وهو القيام بإعتراض كل المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية التي يقصد بها التنصت الهاتفي و يعرف المشرع الجزائري هذه التقنية في المادة 65 مكرر 5 من ق.إ.ج.ج،بأنها إعتراض أو تسجيل أونسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابل للإنتاج والتوزيع والتخزين والإستقبال والعرض ، كما أن نفس المادة جاءت على سبيل الحصر للجرائم التي يستوجب فيها إعتراض هذه الإتصالات السلكية واللاسلكية [1].

والمقصود بالمراسلات هي جميع الرسائل أو الرموز أو تسجيلات أو أي شئ من هذا القبيل يكون في عالم الإفتراضي أو في بيئة الإكترونية ،والمقصود بالإتصال هو أي مكالمات وتسجيلات صوتية وصور وفيديوهات وكما هو معروف فإن الدولة تعمل دائما على إقامة التوازن بين مصلحة العدالة في محاربة الجرائم وبين حماية حقوق وحريات الإنسان وحرمته

[1] فوزي عمارة ،اعتراض المرسلات وتسجيل الاصوات والتقاط الصور كاجراء تحقيق قضائي في المواد الجزائية مجلة العلوم الانسانية كلية الحقوق والعلوم السياسية جامعة المنتوري قسنطينة عدد33 جوان 2010ص236.

الخاصة المنصوص عليها في دستور 2020 في المادة[1]47 بقولها لكل شخص حق في حماية حياته الخاصة وشرفه ولكل شخص حق في سرية مراسلته ولإتصالات الخاصة في أي شكل كانت ولا مساس بهذه المراسلات إلا بأمر معلل من السلطة القضائية وكذلك عرف القانون 04/09 المؤخر في05 أوت سنة 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في المادة 02 الفقرة 02 الإتصالات الإلكترونية هي أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أوصور أو صوت معلومات مختلفة بواسطة وسيلة إلكترونية كما نص نفس القانون في المادة 03و 04 على كيفية العمل باجراء إعتراض المراسلات والإتصالات السلكية واللاسلكية وأهم الضمانات التي جاءت بها لحماية الأشخاص من المساس بحرمة مراسلاتهم.

ومن أهم المرسلات التي يقوم بيها المشتبه فيهم في البيئة الإلكترونية غالبا ماتكون عن طريق البريد الإلكتروني إلاأن هذا الأخير محاط بحماية فنية ، ولا يمكن الوصول إليه إلا عن طريق إجراءات فنية خاصة ،ومن هنا فعملية إعتراض ومراقبة البريد الإلكتروني التي تجري بغرض ضبط الدليل الرقمي ، تنصب على ثلاثة عناصر أساسية وهي :

الوارد : (IN) ويتم من خلاله مراقبة ومراجعة قائمة المراسلات الإلكترونية التي وصلت المشتبه فيه .

عن طريق الصادر : (OUT) وهو عكس الوارد يفيد في الكشف عن قائمة المراسلات التي أرسلت من طرف المشتبه فيه .

[1] أنظر المادة 47من المرسوم الرئاسي الجزائري نرقم 442/20 المتعلق باصدار التعديل الدستوري المصادق عليه في اسفتاء أول نوفمبر 2020ج.ر.ج.د.ش العدد 82 المؤرخة في 30ديسمبر 2020ص13.

أما العنصر الأخير فهو الحفاظ على سلة المهملات Trash الذي يسمح بالإطلاع على المراسلات المحفوظة داخل البريد الإلكتروني الخاص بالمشتبه فيه المحذوفة والتي تحفظ بشكل آلي في سلة المهملات .

وينبغي التنبيه في هذا الصدد إلى أن المراسلات التي تصلح لأن تكون محلا لهذ الإجراء الإعتراض أو المراقبة لابد أم تتسم بالسرية والخصوصية .

فلايسمح المشرع به إلابإذن من وكيل الجمهورية المختص وتباشر العملية تحت مراقبته وهذا مقررته المادة 04 من القانون 04/09 التي جاء فيها بأنه "لايجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة " وعند مباشرة التحريات وتحقيقات يحرر ضابط الشرطة القضائية المأذون محضر عن كل عملية إعتراض للمراسلات وتجيل الأصوات وإلتقاط الصور مع ذكر تاريخ وساعة بداية الإجراء ونهايته .... [1].

ثانيا: تسجيل الأصوات وإلتقاط الصور .

يتم تسجيل الأصوات عن طريق وضع أجهزة تنصت في أمكنة أو مركبات خاصة أو عمومية وإخفائها لتلقي أحاديث قد تفيد في التعرف على الحقيقة وتسجيلها أما إلتقاط الصور فيقصد به تثبيت صورة شخص على مادة خاصة مما يسهل الإطلاع عليها ونسخها وذلك باستخدام الوسائل المعدة لذلك .

وبفضل التطور التكنولوجي لوسائل الإتصالات وكذا التصوير لم يعد تسجيل الأصوات وإلتقاط الصور عملا صعبا فقد يتم ذلك على مسافات بعيدة ومثال ذلك تقنية التجسس على الهاتف

[1] عبد العزيز أحمد ، خصوصية التحقيق في الجريمة المعلوماتية ،مذكرة لنيل شاهدة الماستر ،تخصص قانون جنائي والعلوم الجنائية 2022/2021،ص95.

النقال التي يطلق عليها تسمية السن الازرق (Blue tooth وهي طريقة التي تسمح بالتقاط التسجيلات والمحادثات المارة من وإلى الهاتف النقال التابع للغير داخل مسافة معينة [1].

ونظرا لسهولة القيام بعملية التنصت والمراقبة الإلكترونية فرضت التشريعات مجموعة من الشروط للقيام بها ولعل أهمها صدور الإذن من قبل السلطة المختصة للقيام با إجراءأوعملية وهو شرط نصت عليه المواد الدستوورية كالمادة 47 من تعديل الدستوري الجزائري لسنة 2020 والمادة 04 من قانون 04/09 والمادة 65 مكرر 5 من ق .إ.ج.ج والأمثلة كثيرة على ذلك .

هذا إظافة إلى أن الإذن يجب أن يتضمن كل العناصر التي يمكن من خلالها التعرف على الإتصالات المراد إلتقاطها والأماكن المعنية بالمرقبة والجريمة التي تبرر اللجوء لهكذا إجراء والمدة التي يستغرقها هذا الأخير .

ثالثا :التسرب الإلكتروني أو الإختراق :

تكملة للحالات التي نصت عليها المادتان 3و4 من قانون 04/09[2] يأتي الدور للحديث عن وسيلة أخرى من وسائل الحديثة للحصول على الدليل الإكتروني ألا وهي التسرب أو ما يسمى بالإختراق والذي خصص له المشرع فصل الخامس من الباب الثاني من قانون الإجراءات الجزائية و من خلال المواد من 65 مكرر 11إلى غاية المادة65 مكرر 18 منه ومن خلال التعديل الذي جاء به قانون 06-22 المعدل والمتمم ، لقانون الإجراءات الجزائية حيث تناول

[1] إلهام بن خليفة ،القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام وافتصال مداخلة القيت بمناسبة الملتقى الوطني الموسوم بعنوان لمواجهة مكافحة المعلوماتية في مواجهة المخاطرية ، المنعقد بجامعة محمد بوضياف المسيلة 26فيفري2019،متاحة على الموقع الالكتروني http;dspqce .univ.eloued.dw، تاريخ الإطلاع 2025/02/15على الساعة 14:14.

[2] قانون 09- 04 المتضمن الوقاية من جرائم تكنولوجيا الاعلام والاتصال ومكافحتهاالسالف الذكر .

مفهومه وشروطه وحدد مقصوده في المادة السالفة الذكر على أنه" قيام ضابط أو أعوان الشرطة القضائية تحت مسؤولية ضابط مكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك " وتتمثل عملية التسرب في نطاق الجريمة الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الإفتراضي باختراق مواقع معينة ، أو الإشتراك في محادثات غرف الدردشة والظهور بمظهر كما لو كان فاعل مثلهم مستخدما أسماء أو صفات وهمية لإيقاع الجاني ويلاحظ من خلال ماسبق ذكره أن التسرب عملية معقدة ، تتطلب أن يدخل العون المكلف بالعملية معقدة تتطلب أن يدخل العون المكلف بالعملية في إتصال بالأشخاص المشتبه فيهم ويربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية ويتطلب التسرب و المشاركة في نشاط الخلية الإجرامية الإرتكاز على مبدأين:

- المبدأ العام: تقديم صورة على الوسط المراد التسرب فيه ، ويستوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات .
- المبدأ الخاص : يستند على تعميق التحري عن هذا الوسط ونشاطاته ومميزاته ووسائله وطبيعة الأشخاص المنتمين إليه ليتم بعد ذلك دراسة الوظيفة العملياتية في هذا المجال بتوفير الوسائل البشرية والتقنية اللازمة .

1. شروط التسرب :

أ) الشروط الشكلية :

تتمثل الشروط الشكلية لهذا لإجراء في الإذن وما يجب أن يتضمنه حيث يقوم وكيل الجمهورية أو قاضي التحقيق بمنح الإذن بالتسرب شرط أن يكون مكتوبا وإلا كان الإجراء باطلا وهذا ماجاء في المادة 65 مكرر5 بنصها على أنه "يجب أن يكون الإذن المسلم تطبيقا للمادة 65مكرر11 مكتوبا ومسببا وذلك تحت طائلة البطلان " كونا أن الأصل في العمل الإجرائي

الكتابة ، ويتم العملية تحت رقابة وكيل الجمهورية أو قاضي التحقيق الذي[1]أذن بها ، والذي يصدر إذنه بناءا على تقرير يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب كما يتعين ذكر المدة التي تستغرقها العملية والتي لايمكن أن تتجاوز أربعة أشهر قابلة لتجديد ضمن نفس الشروط الشكلية كما يمكن للقاضي الذي رخص بها أن يأمر بوقفها قبل إنقضاء المدة .

ب) الشروط الموضوعية : تنحصر الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري في شرطين أساسين يتمثلان في:

تحديد نوع الجريمة التي يجب أن لا تخرج عن الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 5 في سبعة أنواع وهي "جرائم المخدرات الجريمة المنظمة العابرة للحدود الوطنية جرائم تبيض الأموال ،الجرائم الإرهابية ،جرائم الفساد ، الجرائم المتعلقة بالتشريع الخاص بالصرف ، وجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ونظرا للخطورة التي يقوم بها العون المتسرب فقد أحاطه القانون بحماية عن طريق جملة من التدابير، التي تضمن الحفاظ عليه وعلى عائلته ، وتؤمن العون المتسرب من الخطر ، ومنه يمكن القول أن مشروعية أي إجراء من الإجراءات السابقة يستوجب عدم مخالفتها للقواعد القانونية المنظمة لها ،أي الشروط الشكلية والموضوعية ، اللازمة لممارستها مع مرعاة المواثيق الدولية وحقوق الإنسان ، وإلا نكون إزاء إجراء غير مشروع ينجم عنه طرح كل دليل جنائي ناجم عنه وغير معتد به وفي كثير من الأحيان يقع باطلا بطلانا مطلقا95 ويتم إستبعاده من أدلة الإثبات .

[1]خالد ابراهيم ممدوح ، فن التحقيق الجنائي في الجرائم افلكترونية ،المرجع السابق نص274.

الفرع الثالث : دور مزود الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال .

أولا : مفهوم مقدمي الخدمات

الطبقا للمادة 02 من القانون الجزائري رقم 09-04 المتضمنة التعريف التشريعي الجزائري لمقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته القادرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعملها ومن هذ التعريف يتضح لنا أن مقدمي خدمات تكنولوجيات الإعلام والإتصال قد يكون مقدم خدمة الإتصال بواسطة منظومة معلوماتية و/او نظام لاتصالات او يكون معالج او مخزن للمعطيات المعلوماتية لفائدة خدمة الإتصال أو مستعملة وأشار المشرع الجزائري إلى مقدمي خدمات الإنترت في المادة 12 من القانون الجزائري رقم 09-04.

ثانيا :إلتزمات مقدمي الخدمات

ووفقا لأحكام القانون الجزائري رقم 09-04 تتمثل إجراءات إلتزمات مقدمي خدمات تكنولوجيات الإعلام والإتصال في إجراءت تقديم مقدمي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية وإجراء حفظ مقدمي الخدمات المعطيات المتعلقة بحركة السير والإجراءات الخاصة بمقدمي خدمة الإنترنت.

أ) مساعدة السلطات

وفقا للمادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها فإن مزود الخدمات يلتزم بمايلي :

مساعدة السلطات في الإجراءات التحضيرية لجمع وتسجيل بيانات محتوى الرسالة في الوقت المناسب ، بحيث أنه لما كان مزود خدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها والمعلومات التي خزنها وكل الإتصالات التي أجرها ومن ثم فانه ملزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها وذلك بتجميعها أو تسجيلها ، ويتعين على مقدمي الخدمات كتمان السرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق .

ب) حفظ المعطيات المتعلقة بحركة السير

- نصت المادة 11من قانون 09-04 على أن يلتزم مقدمو الخدمات بحفظ .
- المعطيات المتعلقة بالتجهيزات المستعملة للإتصال.
- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالخدمات التكملية المطلوبة أو المستعملة ومقدميها .
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

وبالنسبة لنشاط الهاتف يقوم المتعامل بحفظ المعطيلت المذكورة في المادة 11 "أ"من القانون الجزائري رقم 09-04 وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه[1].

وتحدد مدة حفظ المعطيات بسنة واحدة إبتداءا من تاريخ التسجيل حسب المادة 11 من القانون الجزائري رقم 09-04 ودون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام مقدمي الخدمات لإلتزماتهم المنصوص عليها في المادة السلفة الذكر تقوم مسؤولية الجزائية للأشخاص الطبعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ويعاقب الشخص

[1] المادة 11 من قانون 09-04

الطبعي بالحبس من 06 أشهر إلى 05 سنوات وبغرامة من 50.000 دج إلى 500.000 دج ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في القانون العقوبات الجزائري[1].

1. الإجراءات الخاصة بمقدمي خدمات الإنترنت

طبقا للمادة 12 من القانون الجزائري رقم 09-04 زيادة عن الإجراءات المفروضة على مقدمي الخدمات المنصوص عليها في المادة 11 من القانون الجزائري رقم 09-04 السالفة الذكر ، يتعين على مقدمي خدمات الإنترنت القيام بالإجراءات التالية :

التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الأداب العامة وإخبار المشتركين لديهم بوجودها[2].

المطلب الثاني : الدليل الرقمي وسلطة القاضي في تقديره.

لقد أثار الدليل الإلكتروني الكثير من التساؤلات حول ما إذا كان يمثل الحقيقة أولا نظرا لقابلية التلاعب به وتزيفه وتعديله والعبث فيه ، وذلك بسبب الطبيعة الرقمية التي تميزه وهذا ماجعل المشرع يتدخل وينظم مسألة الدليل الإلكتروني ويحيطه ببعض الضمانات التي يمكن إن توفر الحماية لهذ الدليل من بين هذه الضمانات مشروعية الدليل ومشروعية الحصول عليه وكذا قيمته في الإثبات أمام القاضي ولهذا سنتطرق في هذ المطلب إلى تعريف الدليل الإلكتروني وشرعية الحصول عليه وسلطة القاضي في تقديره.

[1] انظر :ج.ر.ج العدد 47 المؤرخة في 16اوت 2009ص07.

[2] انظر ج.ر.ج العدد47 المؤرخة في 16اوت 2009ص08.

الفرع الأول: مفهوم الدليل الرقمي:

أولا تعريف الدليل الإلكتروني:

المقصود بالدليل الإلكتروني هو الوسيلة المشروعة والمتحصل عليها بالطرق المشروعة من أجل تقديمها للقاضي وذلك من أجل تحقيق حالة اليقين لديه والحكم بموجبها [1]، وهناك من يعرفه بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطسية أو كهربائية ممكن تجميعها وتحليلها ، بإستخدام برامج معلوماتية ، وهي مكون رقمي لتقديم المعلومات في أشكال متنوعة مثل النصوص المكتوبة أو الأصوات أو الاشكال أو رسوم وذلك من أجل إعتماده أمام الجهات القضائية [2]والدليل الإلكتروني هو وسيلة من وسائل الإثبات العلمية الجنائية الحديثة التي يعتمد عليها القاضي ، في تكوين قناعته فهو أي معلومة سواء من صنع الإنسان أوتم إستخلاصها من الحاسوب يتقبلها العقل والمنطق من أجل إستقرائها والوصول إلى الحقيقة وبالرجوع إلى المشرع الجزائري نجد أنه لم يعرف الدليل الإلكتروني سواء في القانون 04/09 أو حتى في المرسوم 261/15 المتعلق بتنظيم الهيئة الوطنية للوقاية من الجرائم تكنولوجيات الإعلام والإتصال ...إلخ.

ثانيا :خصائص الدليل الرقمي

يتمتع الدليل الإلكتروني بمجموعة خصائص التي تميزه عن الدليل التقليدي وتتمثل في ما يلي

1. **الدليل الرقمي دليل علمي:** يتشكل من معطيات إلكترونية غير ملموسة يتم إستخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي ،ومايسري على الدليل العلمي يسري على الدليل الإلكتروني وإذا كان الدليل الإلكتروني يخضع لقاعدة تجاوبه مع الحقيقة كاملة وفقا لقاعدة "القانون مسعاه العدالة أما العلم فمسعاه الحقيقة " إذا يستبعد تعارضه مع قاعدة العلمية

[1] نور الهدى محمود ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ،مجلة الباحث للدراسات الاكاديمية ، المجلد الرابع ، العدد 2،ص908.

[2] سمير شبلاق ، حجية الدليل الرقمي في الكشف عن الجريمة ، مذكرة ماستر تخصص قانون جنائي عام قسم حقوق ، كلية الحقوق والعلوم السياسية ، جامعة دكتور ملاي الطاهر ، سعيدة ، الجزائر 2019-2020 ص6

السليمة فإن الدليل الإلكتروني له الطبيعة ذاتها ويجب أن لا يخرج عما توصل إليه العلم الإلكتروني الرقمي وإلا فقد معناه .

2. **الدليل الإلكتروني دليل تقني** : بمعنى أنه مستوحى من البيئة التقنية التي يتواجد فيها والمتمثلة في مختلف الأجهزة التكنولوجية ومن أجهزة الحاسب والخوادم والمضيفات والهواتف والشبكات ، ولا يمكن تصور وجود الدليل رقمي خارج هذا الإطار .
3. **الدليل الرقمي متنوع ومتطور**: يأخذ عدة أشكال يمكن أن يكون في شكل بيانات مشفرة أو وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام كما يمكن أن يكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي وأن تكون مخزنة في نظام البريد الإلكتروني.
4. **صعوبة التخلص من الدليل الرقمي** يختلف الدليل الإلكتروني عن الدليل التقليدي حيث هذا الأخير يمكن تخلص منه بسهولة إذا كان مكتوب يمكن حرقه ...أما الدليل الرقمي لا يمكن التخلص منه بسهولة وذلك بسبب القدرة على إسترجاعه من الذاكرة الميتة للحاسوب أو شبكة الإتصال أو أحد دعائمه وذلك باستخدام أدوات وبرمجيات ذات طبيعة رقمية متطورة كما يمكن نسخه في عدة أجهزة [1].
5. **الدليل الإلكتروني ذو طبيعة رقمية ثنائية** : الدليل الإكتروني يتكون من تعداد غير محدود من أرقام ثنائية في هيئة الواحد والصفر 1-0 وهذا يعني أن المعلومات والبينات داخل الحاسوب الآلي سواء كانت نصوص أو صور أو فيديو ....ليس لها وجود مادي إنما هي مجموعة أرقام ترجع إلى أصل واحد هو الرقم الثنائي 1-0 فما من شيئ في العالم الرقمي إلاويتكون من معادلة ثنائية قوامها الرقمان المذكران ، وهما في تكوينهما الحقيقي عبارة عن نبضات وذبذبات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة مع العلم أن تكوين معطيات هذه المعادلة الثنائية تختلف في الحجم والموضوع وكمية أو حجم الرقمين 1-0 في ملف يمكن أن يختلف عن كميته في ملف أخر وما يمكن إستخلاصه هو أن تمتع الدليل الإلكتروني بالخصائص السالفة الذكر جعلته دليلا ذا طابع خاص يختلف عن باقي الأدلة المألوفة وأصبح على حد

[1] فاطمة العرفي الجزائري ،حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري ،مجلة صوت القانون ،المجلد 08،العدد02 ،2022.ص503.

تعبير بعض القانونيين المختصيين أنه الدليل الأحسن والأفضل للإثبات في الجرائم الإلكترونية لكونه مستمدا من طبيعة الوسط الذي وقعت فيه .

ثالثا: شروط صحة قبول الدليل الإكتروني في إثبات الجريمة المعلوماتية .

لدليل الإلكتروني أهمية بالغة في إثبات الجريمة الإلكترونية وليس هي فحسب بل تتعد تلك الأهمية إلى الجرائم التقليدية كالتجارة بالمخدرات وغسيل الأموال وجرائم القتل والإختطاف وغيرها التي تستخدم التكنولوجيا الحديثة في إرتكابها وحتى يحظى الدليل الإلكتروني بتلك الأهمية السابقة لابد من أن تتوفر فيه بعض الشروط لكي يعتد به في الإثبات ومن هذه الشروط

المشروعية وهو شرط يلزم وجوده في كل الأدلة بشتى أنواعها وخاصة الجنائية فهي الأساس القانوني الذي يرتكز عليه سواء في وجود الدليل أو في إجراءات الحصول عليه ، أي أن المشرع قد قبله ضمن أدلة الإثبات الجنائي بمعنى يجيز القانون للقاضي الإستدلال به في تكوين عقيدته وقناعته في الحكم، وأن تكون الجهة المختصة بجمع الدليل قد إلتزمت بالشروط المحددة قانونا إنطلاقا من الحصول على إذن النيابة العامة للقيام باجراءات التفتيش والضبط للحصول عليه.[1]

يجب أن تتم مناقشة الدليل الإلكتروني في جلسة المحكمة تكريسا لمبدأ المواجهة بين أطراف الدعوى ، وهو ما يعبر عنه بشرط وضعية الدليل أي أن يكون لدليل أصل ثابت في أوراق الدعوى وليس بضرورة مناقشته علنا يكفي أن يوضع تحت نظر القاضي في ملف الدعوى وأن يتاح للخصوم الإطلاع عليه ومناقشته عملا بالفقرة الأخيرة من المادة 212 من قانون إ.ج .ج "لا يسوغ للقاضي أن يبني قراره إلاعلى الأدلة المقدمة له في معرض المرفعات والتي حصلت المناقشة فيها حضوريا أمامه"،وأن يكون الدليل الإكتروني المتحصل عليه له علاقة بموضوع الجريمة الإلكترونية وهو شرط تمت الإشارة إليه في المادة 401 من قانون الإثبات الفيدرالية الأمركي والمعروف بمبدأ العلاقة الكاشفة ،حيث يتطلب هذ القانون وجود علاقة بين الدليل وبين

[1] تومي يحي، جرائم الاعتداء ضد الافراد باستخدام تكنولجيا الاعلام والاتصال اطروحة من اجل نيل شهادة الدكتوراه علوم تخصص قانون كلية الحقتق جامعة الجزائر سنة الجامعية 2017-2018ص249.

الواقعة محل الدعوى ولإثبات تلك العلاقة الكاشفة يتطلب الأمر شرطا آخر وهو مطابقة الدليل الإلكتروني المستخرج من الكمبيوتر للأصل الموجود بداخله .[1]

ان تكون الادلة الالكترونية يقينية اي بعيدة عن الظن والتخمينات ومفاد ذلك ان لايكون الدليل قابلا للشك فاذا كان كذلك فان الشك يفسر لصالح المتهم ويرجع ذلك الى السلطة التقديرية للقاضي

الفرع الثاني: موقف المشرع الجزائي الجزائري من الدليل الإلكتروني في الاثبات .

تختلف انظمة الاثبات في كل دولة ههناك من تاخذ بنظام الاثبات الحر وهناك من تاخذ بنظام الاثبات المقيد وسنشرح هذه الانظمة كما يلي :

أ) **نظام الاثبات المقيد:** أو نظام الأدلة القانونية وفيه يقوم المشرع بتحديد ادلة الاثبات وكذا قوة لاثباتية لكل دليل من الادلة بناء على قناعة المشرع بها ويكون فيه دور قاضي سلبي حيث يتقيد في حكمه سواء بالإدانة او البراءة بانواع معينة من الادلة طبقا لما يرسمه التشريع وقد اعاب الفقه الجنائي على هذا النظام انه اخرج القاضي من وظيفته الطبيعية التي تتمثل في فحص الدليل وتقديره ومن ثم تكوين اقتناعه الشخصي وأقحم المشرع في وظيفة القاضي واملاء ادلة الادانة عليه على سبيل الحصر .[2]

ب) **نظام الإثبات الحر** :والذي يقوم على اساس حرية الإثبات فلا يقوم المشرع بتحديد طرقا معينة للإثبات بل يترك ذلك للقاضي الذي يكون دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعته بها ،فلا يلزمه القانون بأدلة للاستناد اليها في تكوين قناعته فله ان يبني هذه القاعدة على اي دليل مطروح امامه .

ث) **نظام الاثبات المختلط** :وهو نظام وسط بين نظام الاثبات المقيد ونظام الاثبات الحر وفيه تم التصدي للإنتقادات الموجهة لنظام الإثبات الحر حول خشية تعسف القاضي الجزائي وخروجه

---

[1] خالد ممدوح ابراهيم مرجع سابق ص188.

[2] رمزي رياض عوض،مشروعية الدليل الجنائي في مرحلة المحاكمة وماقبلها ، دراسة تحليلة تأصيلية مقارنة ،دارالنهضة العربية القاهرة ،1997ص58. [2]

عن جادة الصواب ، كما تم تلاقي ما وجه من انتقادات لنظام الإثبات المقيد وذلك بان حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه ،لما جعل دور القاضي سلبيا في عملية الإثبات ، وذلك من خلال إعطاء القاضي الجزائي الحرية في تقدير ووزن مايعرض عليه من أدلة ثبوتية وفقا لاقتناعه الشخصي .[1]

وفي هذا الصدد فان المشرع الجزائري وكغيره من التشريعات أخذ بالنظام الحر فلا نجده قد افرد نصوص خاصة تفرض على القاضي مقدما قبول او عدم قبول اي دليل بما في ذلك الدليل الرقمي وهو امر منطقي طالما ان المشرع الجزائري يستند لمبدأحرية الاثبات حيث نصت المادة 212 من قاجج على انه يجوز اثبات الجرائم باي طريقة من طرق الاثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي ان يصدر حكمه تبعا لاقتناعه الخاص ولا يسوغ للقاضي ان يبني قراره الا على الادلة المقدمة له في معرض المرفعات والتي حصلت المناقشة حضوريا امامه "كما نصت المادة 307 من ق اج ج ايضا ان القانون لا يطلب من القضاة ان يقدمو حسابا عن الوسائل التي قد وصلوا بها الى تكوين اقتناعهم وان يبحثوا باخلاص ضمائرهم في اي تاثير قد احدثته في ادراكهم الادلة المسندة للمتهم ..."

ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الإقتناع الشخصي للقاضي الجزائي إلا إستثناء نجده أحذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين يشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر كجريمة الزنا المنصوص عليها في المادة 339 و341 من ق.ع ومنه إن الأصل في الدليل مشروعية وجوده ومشروعية الحصول عليه ومتى تفور هذا في الدليل الرقمي وطبقا لبمدأ الشرعية الإجرائية يكون الدليل مقبولا أمامه ويعتد به كوسيلة من وسائل الإثبات أمام القضاء .

وبتحليل المادة 212 من ق .إ. ج .ج نجدها تكرس قاعدتين تكمل إحدهما الأخرى، من جهة قاعدة الإقتناع الحر للقاضي الجزائي ومن جهة أخرى قاعدة حرية إختيار وسائل الإثبات

[1] نادية ضريقي،دراج عبد الوهاب ،سلطة القاضي الجنائي في تقدير الالكتروني المستمدة من التفتيش الجنائي ،مجلة الاستاذ الباحث للدراسات القانونية والسياسية ،مجلد 04،العدد02،السنة 2019ص127.

الجزائي وبتالي فان المشرع الجزائي منح للقاضي الجزائي سلطة تقدير الأدلة بمافيها الدليل الرقمي وتكوين إعتقاده من أي دليل يطمئن إليه وإن كان الدليل الرقمي ذوالأصالة العالمية والأوفر والأنسب في إثبات الجريمة المعلوماتية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الإقتناع الشخصي حيال هذا الدليل.

فرع ثالث : سلطة القاضي الجزائي في تقدير الدليل الرقمي.

تعد مرحلة الحكم بمثابة المرحلة الحاسمة في الدعوى الجنائية ، ذلك أن غاية هذه الأخيرة هي الوصول إلى حكم حاسم لها حائز لقوة إنهائها، ولهذا فإن الحكم يمثل أهم إجراءات الدعوى لأنه يمثل غايتها ، وعملية تقدير الأدلة تشكل جوهر هذا الحكم ، حيث لا يمكن الوصول إليه وإدراكه مالم يمارس القاضي سلطته التقديرية على الأدلة محل الواقعة وفي مجال جرائم الإلكترونية يخضع الدليل الرقمي شأنه شأن الدليل الجزائي لمبدأ العام في الإثبات الجنائي وهو حرية القاضي في الإقتناع، والقاضي في ظل هذا المبدأ يملك الحرية الواسعة في تقييم عناصر الإثبات ووزن الأدلة وتقديرها، بالكيفية التي تمكنه من تكوين عقيدته في الدعوى المعروضة عليه وباعتبار الدليل الرقمي تطبيقا من تطبيقات ،الدليل العلمي فلا يمكن للقاضي أن ينازع في قيمة ما يتمتع به الدليل من قوة إستدلالية قد إستقرت بالنسبة له وتأكدت من الناحية العلمية إن الأصالة العلمية للدليل الرقمي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي إذ إن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية حتى للقاضي مستنيدين في رأيهم أن لهذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين وهناك من يرى أنم مبدأ حرية القاضي في الإقتناع يجب أن يبسط سلطته على كل الأدلة دون إستثناء حتى على الدليل الرقمي معتبرين إن الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتهاوهذا مأخذ به المشرع الجزائري[1].

أما فيما يخص مسألة التشكيك في سلامة الدليل الرقمي ، بسبب قابليته للعبث والخطأ في إجراءات الحصول عليه، فهي مسألة فنية لايماك القاضي الفصل فيها،بإعتبارها مسألة فنية

[1]يكر طاهر مرجع سابق ص141.

الرأي فيها يعود للخبير ، لذلك فإذا توافرت في الدليل الرقمي الشروط المطلوبة ، بخصوص سلامته من العبث والخطأ ، فإن هذا الدليل لايمكن رده إستثناءا لسلطة القاضي التقديرية وفقا للمدتين 212 و307 من قانون الإجراءات الجزائية ، وعليه نلخص مماسبق إلى أنه رغم طبيعة الدليل الرقمي وأهميته في إثبات الجرائم المعلوماتية إلاأنه تبقى السلطة التقديرية للقاضي الجزائي في تقدير لهذا الدليل الرقمي وأي مسالة تشكيك في صحته تفسير لصالح المتهم بالإظافة إلى ذلك يلزم أن يكون الدليل الرقمي محصل عليه بطرق قانونية ومشروعة لجعل الحقيقة العلمية حقيقة قضائية[1].

[1] عياشي حفيظة، سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري ،مجلة القانون والعلوم السياسية ،المجلد 09،العدد01،2022،ص551.

خاتمة

خاتمة

خاتمة

ختاما لما سبق إستعراضه بصدد دراستنا هاته ، نجد أن موضوع جرائم تكنولوجيا الإعلام والإتصال يعد من المواضيع البالغة في الأهمية نظرا لخوطرتها ، نتيجة الأضرار التي لا يمكن حصرها وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى ، مما يتطلب دراسة عميقة حولها.

حاولنا معالجة الموضوع من خلال فصلين أساسيّن حيث تناولنا في الفصل الأول الإيطار المفاهمي لجرائم تكنولوجيا الإعلام والإتصال وذلك بالتطرق إلى مفهومها من حيث الفقه ومن حيث التشريع ومن ثم تبيان أركانها ، وكذا الدوافع المؤدية لرتكابها وتبيان خصائصها التي جعلتها تنفرد عن نظيرتها التقليدية سواء تعلقت هذه الخصائص بالجريمة ذاتها أو بالمجرم الإلكتروني، هذه الطبيعة المتميزة للجريمة الإلكترونية جعلت المشرع الجزائري يدرك مدى خطورتها على الفرد وعلى المجتمع على حد سواء وكان لابد من التصدي لها خصوصا أن الجزائر تشهد إستعمال موسع للتقنية المعلوماتية في جميع القطاعات وهذا ما تعرضت له بالتفصيل من خلال الفصل الثاني حيث تطرقنا للآليات القانونية والمؤساساتية لمكافحة الجريمة المتصلة بتكنولوجيا الإعلام والإتصال وجهود المشرع الجزائري معتمدة لمكافحتها سواء على المستوى الوطني أو الإقليمي أو الدولي فنجد المشرع سعيا منه لتدارك الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية قد قام بإدراج تعديلات خاصة على القانون العقوبات الجزائري وإستحداث قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها محاولة منه لتقليص من هذه الجرائم المستحدثة والعابرة للحدود .

وبعد ذلك تناولنا في الفصل الثاني إجراءات البحث والتحري التقلدية وكيف وسع المشرع من صلاحيتها مثل المعاينة والتفتيش والقواعد الإجرائية المستحدثة لمكافحة الجرائم تكنولوجيا

الإعلام والإتصال مثل إعتراض المراسلات والإتصلات السلكية ولاسلكية والتسرب والإختراق وكذلك تطرقنا إلى مقدم الخدمات ودوره في مكافحة الجريمة الإلكترونية ، ثم بينا مفهوم الدليل الإلكتروني ومشروعية الحصول عليه وبينا سلطة القاضي في تقديره والوسائل التي تساعد في تكوين قناعته .

من خلال هذه الدراسة توصلنا لنتائج التالية :

- ✓ جرائم تكنولوجيا الإعلام والإتصال جرائم مستحدثة عابرة للحدود .
- ✓ ومايمكننا إستنتاجه هو عدم وجود تعريف جامع مانع للجريمة الإلكترونية مما نتج عنه الإختلاف المتباين في الأفعال التي تعد من قبيل الجرائم الإلكترونية وقد يكون سبب ذلك الطبيعة المتسارعة والتطور الكبير الذي تشهده هذه الجريمة الخطيرة وعدم قدرة التشريع على مجاراتها نظرا لما يتميز به هذا الأخير من جمود وبط ء في إجراءات صدوره .
- ✓ المشرع الجزائري لم يحديد الجريمة المرتكبة بإستخدام النظام المعلوماتي وترك المجال واسع ليدخل في نطاقها كل ما تقرره التقنية الجديدة وتطوراها .
- ✓ إن الجريمة الإلكترونية لها ميزات خاصة تختلف بها عن الجرائم التقليدية الأخرى ومرد ذلك يعود للبيئة الرقمية الإلكترونية التي فيها مما أكسبها وأكسب مرتكبها المجرم الإلكتروني سمات معينة صعبت معها عملية المكافحة الإجرائية والمؤسساتية المتخذة بشأنها .
- ✓ لم يضع المشرع الجزائري نصاً خاصاً بالجرائم الإلكترونية رغم ما تسببه هذه الجرائم من أضرار على المجتمع والدولة معا خاصة وأن الجزائر تتجه نحو رقمنة الإدارة الجزائرية بما يتماشى والعصرنة الحاصلة في العالم .

✓الدليل الإلكتروني له طبيعة خاصة تستدعي التعامل معها بحذر، خاصة حين القيام بعملية التفتيش والضبط ،لأن المجرم الإلكتروني لديه خبرة جيدة في إخفاء ماينتج عنه من أدلة .

✓مقدمو الخدمات الذين تتمشى تقنياتهم مع تطور تقنيات المعلومات والإتصالات الحديثة يلعبون دورا مهما في مكافحة هذا النوع من الجرائم .

✓آليات المكافحة الحالية غير كافية لمجابهة الجريمة الإلكترونية فلا يمكن لأي دولة مهما بلغ تطورها التكنولوجي والمعلوماتي أن تتصدى لهذه الجريمة العالمية بمفردها فالمجرم الإلكتروني قد يكون في دولة ما وينفذ جريمته في دولة وتتحقق نتيجتها في دولة أخرى أو عدة دول مما يصعب عملية متابعته خاصة في حالة عدم وجود اتفاقية بين الدولة التي يتواجد على أرضها والدولة المطالبة به، وعليه فإن آليات المكافحة المخصصة من طرف بعض الدول تعد غير كافية للتصدي للجريمة الإلكترونية.

✓شكلت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها محور إهتمام العديد من السلطات ، مما أدى إلى تعاقب السلطات على ترأسها بداية من وزارة العدل سنة 2015 ثم وزارة الدفاع الوطني سنة 2019 لتوضع تحت سلطة رئيس الجمهورية سنة 2020.

ومن خلال هذه النتائج نحاول تقديم إقتراحات الأتية :

✓يتعين على القائمين على الشؤون القانونية والقضائية الإهتمام بتكوين رجال البحث والتحري في الجرائم الإلكترونية تكويناً قانونياً وتكوين رجال العدالة تكويناً تقنية حتى يكون هناك تنسيق فيما بينهم للوصول إلى أدلة إلكترونية صحيحة ومقبولة أمام الجهات المعنية .

✓نظرا لكثرة الجرائم الإلكترونية وتنوعها يستحسن إنشاء شرطة متخصصة بهذه الجرائم تكون مهمتها الوحيدة متابعة مثل هذا النوع من الجرائم .

- ✓ضرورة تكثيف الحملات التوعوية للشباب والأطفال ، من أجل وقايتهم من خطورة الإدمان على الأنترنت لأن هذ النوع من الإدمان يقتل فيهم روح الإبداع ،ويجعلهم في عزلة عن العالم الحقيقي ،كما قد يوقعهم في جرائم إلكترونية مختلفة ،والتي تصل نتائجها في بعض الأحيان إلى حصد الأرواح كما حصل لمن كانو ضحايا الألعاب الإلكترونية الخطيرة ، كلعبة الحوت الأزرق.

قائمة المصادر والمراجع

أولا: المصادر

❖ **القرآن الكريم :**

❖ **النصوص الرسمية :**

❖ **الإتفقيات والمنظمات الدولية:**

1. إتفاقية بودبست المؤرخة في 23 نوفمبر سنة 2000 بعاصمة المجر .

2. الإتفقية العربية لمكافحة الجرائم تقنية المعلوماتية المحرر بالقاهرة بتاريخ 2010/12/21 صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-258المؤرخ في 2014/9/8.

3. المنظمة الدولية لشرطة الجنائية الأنتربول ، مقرها في باريس ووضع ميثاق هذه المنظمة في فترة 1956/06/13.

4. إعلان فينا بشأن الجريمة والعدالة،مواجهة تحديات القرن الحادي والعشرون مؤتمرالأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي أنعقد في فينا في فترة الواقعة مابين 17/10 نيسان لعام2000الفقرة 17،صفحة 37.

❖ **التشريع الأساسي :**

1. التعديل الدستوري لسنة 2020المصادق عليه في إستفتاء أول نوفمبر 2020، الجريدة الرسمية ،العدد82المؤرخة في30ديسمبر 2020.

❖ **القوانين والأوامر:**

1. الأمررقم 21-11المؤرخ في 25-08-2021 المتضمن تعديل قانون الإجراءات الجزائية، الجريدة الرسمية، عدد65 المؤرخ في 26-08-2021. القانون الجزائري رقم 06-23 المؤرخة في 20ديسمبر 2006، الجريدة الرسمية العدد84 المؤرخة في 14ديسمبر.

2. 2006،المعدل والمتمم للأمر الجزائري رقم 66-156 المؤرخ في 08جوان1996 والمتضمن قانون العقوبات الجزائري الجريدة الرسمية العدد49 المؤرخة في 11جوان1966

3. الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424الموافق 19يوليو2003 متعلق بحقوق المؤلف والحقوق المجاورة .

4. القانون رقم 09-04 مؤرخ في 14شعبان 1430 الموافق 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها .الجريدة الرسمية الجزائرية ،العدد 47المؤرخة في16أوت2009.

❖ **النصوص التنضمية:**

❖ **مراسيم الرئاسية:**

1. المرسوم الرئاسي رقم 15-261،المؤرخ في 08 أكتوبر 2015،يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها الجريدة الرسمية العدد53 الصادر في تاريخ 08 أكتوبر 2015.

2. مرسوم رئاسي رقم08_151،المؤرخ في20جمادة الأولى1429الموافق26مايو سنة 2008،المتضمن احداث مدرسة للشرطة القضائية تابعة لدرك الوطني ،المنشور بج.ر.ج العدد27،الصادر بتاريخ 28مايو 2008 .

3. مرسوم رئاسي رقم 04-432 ،المؤرخ في 17 ذي العقدة عام 1425 الموافق 29ديسمبر سنة 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي المنشور في ج.ر.ج العدد84ن بتاريخ 29ديسمبر سنة 2004.

4. أنظر المرسوم الرئاسي رقم 15-261، المؤرخ في2015/10/08 ،يحدد تشيكلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية عدد53،مؤرخ في 2015/10/08.

5. مرسوم رئاسي رقم 04-432 ، المؤرخ في 17 ذي العقدة عام 1425 الموافق 29ديسمبر سنة 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي المنشور في ج.ر.ج العدد 84 بتاريخ 29ديسمبر سنة 2004.

6. المرسوم التنفيذي 20-183 ،المؤرخ في 13يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيت الإعلام والإتصال ومكافحتها ،الجريدة الرسمية الجزائرية العدد40،الصادر بتاريخ 26ذو القعدة 1441 الموافق 18يوليو2020.

❖ **مراسيم تنفيذية :**

1. المرسوم التنفيذي 06-348 المؤرخ في 05-10-2006،ج.ر ،عدد 63 المؤرخ في 08-10-2006 .

❖ **النصوص الرسمية غير الجزائرية:**

1. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم :63 لسنة 2015،الصادر يوم الأحد 12 يوليو 2015، العدد 1244 .

2. مكافحة الجرائم المعلوماتية السعودي مجلس الوزراء في جلسته الأسبوعية يوم الإثنين 1428/03/07هـ الموافق2007/03/26، وصدر بموجب المرسوم الملكي رقم (م/17) بتاريخ 31428/8هـ ،القانون موجود على الموقع الإلكتروني للجريدة الرسمية للمملكة العربية السعودية: //www.uqn.gov.sa/channels/royal:http decrees-

3. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم :63 لسنة 2015،الصادر يوم الأحد 12 يوليو 2015 ،العدد 1244.

4. المواد من 16 إلى 25 من المرسوم التونسي المؤرخ في 13سيبتمبر 2022 المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات وإتصال ،الرائد الرسمي للجريدة الرسمية التونسية ،العدد 103 المؤرخة في 16 سبتمبر 2022 .

ثانيا: المراجع

❖ **المؤلفات**

❖ **الكتب :**

1. أمال قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري ،دار هومه للنشر والتوزيع الجزائر 2008.

2. أحمد السقيعة، الوجيز في القانون الجنائي ،دار الهومه ،الجزائر ،الطبعة 05

3. أمير فرج يوسف ،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر ،الطبعة الأولى ،مكتبة الوفاء القانونية ،الإسكندرية ،مصر ،2011.

4. أحمد يوسف الطحطاوي الأدلة الإلكترونية ودورها في الإثبات الجنائي ، دراسة مقارنة دارالنهضة العربية القاهرة، مصر 2015.

5. جلال محمد الزغبي ،جرائم التقنية ،نظم المعلومات الإلكترونية، دار الثقافة ، الطبعة الأولى عمان،2010.

6. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي الإسكندري 2010.

7. رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وماقبلها ، دراسة تحليلة تأصيلية مقارنة ،دارالنهضة العربية القاهرة.

8. سعيدي سليمة ، حجازى بلال جرائم المعلومات والشبكات في العصر الرقمي ،دار الفكر الجامعي ،الطبعة الأولى،الإسكندرية ،مصر،2017.

9. طارق إبراهيم الدسوقي عطية ،الأمن المعلوماتي (النظام القانوني لحماية المعلومات)،دار الجامعة الجديدة، القاهرة، مصر، الطبعة 2009 .

10. طاهر ياكر،الجرائم الإلكترونية ،الأحكام الموضوعية والإجرائية ، دراسة مقارنة ،دار بلقيس للنشر،الجزائر 2024.

11.عبد الفتاح بيومي حجازي ،الدليل الجنائي والتزوير في الجرائم الكمبيوتر والإنترنت ، الطبعة الثالثة دارالجامعة الجديدة مصر 1999.

12.عبد الفتاح البيومي حجازي ، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دارالفكر الجامعي، الإسكندرية، 2006.

13.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار كتب القانون ، مصر،2007.

14.علي عبد القادر القهوجي الحماية الجنائية لبرامج الحاسب الآلي دار الجامعة للطباعة والنشر، دون طبعة، لبنان،1999.

15.عفيفي كمال عفيفي نجرائم الكمبيوتر وحقوق المؤلف (المصنفات الفنية ودور الشرطة والقانون)،دراسة مقارنة ،منشورات الحلبي الحقوق،طبعة أولى ،بيروت ،2003.

16.عادل يحي،السياسة الجنائية في مواجهة الجريمة المعلوماتية ،دارالنهضة ، الطبعة الأولى القاهرة ، مصر،2014.

17.غنية باطلي ،الجريمة الإلكترونية (دراسة مقارنة)، دون طبعة ، منشورات الدار الجزائرية ، الجزائر،2016.

18.محمد علي العريان ،الجرائم المعلوماتية ،دار الجامعة الجديدة لنشر والتوزيع ،مصر 2004.

19.مصطفى محمد موسى ،أساليب إجرامية بالتقنية الرقمية ماهيتها مكافحتها ، دراسة مقارنة دار الكتب القانونية ، مصر ،2005.

20.حمد حماد مرهج الهيتي ، جرائم الحاسوب ، ماهيتها ، موضوعها ، أهم صورها والصعوبات التي تواجهها ، دار المناهج للنشروالتوزيع ،2006.

21.محمد أمين شوابكة ،جرائم الحاسوب والانترنت (الجريمة المعلوماتية)،دار الثقافة للنشروالتوزيع ،عمان الأردن ،2009 .

22.مسعود خثير ،الحماية الجنائية لبرامج الكمبيوتر ،أساليب وثغرات،طبع 10، دار الهدى الجزائر 2010 .

23.نهلا عبد القادر المومني ،الجرائم المعلوماتية ،دار الثقافة لنشر والتوزيع طبعة الأولى عمان ،الأردن ، 2008.

24.نجم محمد صبحي ،جرائم الواقعة على الأشخاص طبعة01، مكتبة دارالثقافة ، القاهرة مصر 1994 نص153 وبعدها ، للمزيد ،أنظر في ذلك سارة محمد حنش ،مسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية دراسة مقارنة ، مذكرة مقدمة لنيل شهادة الماجيستر في القانون العام ، جامعة الشرق الأوسط لبنان2020.

25.هدى قشوش،جرائم الحاسب الإلكتروني التشريع المقارن ،دارالنهضة العربية، الطبعة الأولى ،القاهرة ،مصر، 1992.

26.هدى حامد قشقوش السياسة الجنائية لمواجهة الجريمة المعلوماتية ،دار النهضة العربية القاهرة، 2012.

27.يوسف حسن يوسف ،الجرائم الدولية للإنترنت، المركز القومي للإدرات القانونية ، الطبعة الأولى ،القاهرة ، مصر 2011.

❖ **المقالات :**

1. أمال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، المجلة الدولية للبحوث القانونية والسياسية ،المجلد 05،العدد 03 .

2. إيمان بغدادي أثر تعديل قانون العقوبات الجزائري في الصدي للجريمة الإلكترونية مجلة أفاق البحوث والدرسات السداسية ، مجلة دولية محكمة المركز الجامعي إليزي.

3. براهمي جمال ، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية ،كلية الحقوق والعلوم السياسية جامعة ملود معمري ،تزي وزو العدد2،الصادرة في 2016/11/15.

4. بوضياف إسمهان الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر ، مقال منشور في مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،العدد11سبتمبر2018 .

5. بن طيبي مبارك ،رحموني محمد ، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية ، مجلة القانون والعلوم السياسية ، مجلد05 العدد02، سنة 2019.

6. بكوش محمد الامين ،هروالة نبيلة هبة ،خصوصية المجرم الإلكتروني ، مجرم الإنترنت نموذجاً ، مجلة البحوث في الحقوق والعلوم السياسية ،المجلد 07العدد01 السنة 2021 .

7. بعجي عبد النور مالك نسيمة ،الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة مقال منشور بمجلة الدراسات والبحوث القانونية ،الصادرة عن جامعة محمد بوظياف ،مسيلة كلية الحقوق والعلوم السياسية ، مجلد السابع، العدد 02،2022 .

8. رحموني محمد ،خصائص الجريمة الإلكترونية ومجالات إستخدامها ،مجلة الحقيقة ،العدد 2018.

9. رضا عسال، عماد عبد الرزاق ،الجريمة الالكترونية والمجرم المعلومات ، مقاربة مفاهمية مجلة ببليوفيليا، لدراسات المكتبات والمعلومات ،العدد 05، 202-2020.

10. سهام خليلي ، خصوصية المجرم الإلكتروني ، مجلة الفكر، العدد 15، جوان2017.

11.سلمى عبد النبي ،دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في مواجهة الإعتداءات الواقعة على المعطيات المعلوماتية ،المجلد 11،العدد02،السنة 2024.

12.صايش عبد الملك ،الجهزة الأروبية المكلفة بماكفحة الهجرة السرية مهمة مستحيلة بمعدات عسكرية ،المجلة الأكادمية للبحث القانوني ،كلية الحقوق والعلوم السياسية جامعة عبد الرحمن ميرة ،بجاية ،جزائر ، مجلد 11،العدد ،2015.

13. عبد الصديق الشيخ ،الوقاية من الجرائم الإلكترونية في ظل قانون رقم 09-04 المتضمن قواعدالخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ،مقال منشور في مجلة معلم الدرسات القانونية والساسية ،المجلد 04 العدد01 ،السنة 2020.

14. عياشي حفيظة سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري مجلة القانون والعلوم السياسية المجلد 09، العدد01 ،2022.

15.غريبي بشرة ،خصوصية المجرم المعلوماتي ودوافعه،مجلة نوميروس الأكادمية المجلد الثاني، العدد الثاني،2021.

16.فوزي عمارة ،إعتراض المرسلات وتسجيل الأصوات والتقاط الصور كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية كلية الحقوق والعلوم السياسية ، جامعة المنتوري قسنطينة ،عدد33 ،جوان 2010.

17.فضيلة عاقلي ،الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري المؤتمر الدولي الرابع عشر"الجرائم الإلكترونية "طرابلس، بتاريخ 24-25 مارس2017.

18.فاطمة العرفي الجزائري ،حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري مجلة صوت القانون المجلد 08،العدد02 ،2022.

19.قدة حبيبة مفهوم عملية التحويل المصرفي وطبيعتها القانونية مقال منشور بمجلة دفاتر السياسية والقانون ، العدد 10، جامعة قاصدي مرباح ورقلة العدد الأول 2014 .

1. محمد طيب عمور السرقة الإلكترونية تكيفها الشرعي وطرق إثباتها مقال منشور في مجلة الأحياء الصادرة عن جامعة الجلفة المجلد 19 العدد22 سنة 2019 .

حمـد زكـي أبوعـامر، الإجـراءات الجنائيـة ،الطبعـة الثامنـة،دار الجامعـة الجديـدة 2008،ص123 ومبعها.

.20

21.محـروس ناصـر غايـب ،الجريمـة المعلوماتيـة ،مقـال منشـور علـى الموقـع الإلكترونـي www.iasjnet/iasj?func=fultesct&ald=28397

22.نور الهدى محمودي ،حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ،مجلة الباحث للدرسات الأكاديمية ، المجلد 04العدد 02 ،جوان 2017.

23.نور الدين بن سولة ،الجرائم الإلكترونية في ضوء التشريع الجزائري ، مقال منشور في مجلة الحوار المتوسطي المجلد التاسع العدد31 تاريخ /2018/03.

24.نقموش محمد ، ميلودية أحمد ،الجريمة المعلوماتية : مفهوم حتمية تطوير آليات التعاون الدولي في مجال مكافحتها ،مجلة الدراسات القانونية والسياسية ،جامعة عمار ثلجي بالأغواط الجزائر المجلد الرابع (04)،العدد الثاني ،جوان 2018.

25.نادية ضريفي، دراج عبد الوهاب ، سلطة القاضي الجنائي في تقدير الإلكتروني المستمدة مـن التفتـيش الجنـائي ، مجلـة الأسـتاذ الباحـث للدراسـات القانونيـة والسياسـية ، مجلـد 04،العدد02،السنة 2019.

26.ياسمينة بونعارة،الجريمة الإلكترونية ، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة ،العدد 39،تاريخ النشر21 جوان 2016.

❖ **أطروحات الدكتوراه**

1. برارديي نعيمة ،الإتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر دراسة تحليلية إستطلاعية بالجزائر العاصمة ،رسالة لنيل شهادة الدكتوراه في العلوم الإعلام والإتصال،كلية العلوم السياسية والإعلام ،جامعة الجزائر03،السنة الجامعية 2012-2013

.

2. تومي يحي،جرائم الإعتداء ضد الأفراد باستخدام تكنولجيا الإعلام والإتصال أطروحة من أجل نيل شهادة الدكتوراه علوم تخصص قانون كلية الحقوق جامعة الجزائر سنة الجامعية 2017-2018 .
3. حمزة بن عقون ،السلوك الإجرامي للمجرم المعلوماتي ، بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية ،تخصص علم الإجرام وعلم العقاب جامعة الحاج لخضر باتنة 2011-2012.
4. حسين ربيعي ،آليات البحث والتحقيق في الجرائم المعلوماتية أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية ،جامعة باتنة 01،سنة الجامعية 2015-2016.
5. شنتير خضرة ،الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)،أطروحة لنيل شهادة دكتوراه،جامعة أحمد دراية ،أدرار 2021/2020.
6. عبد القادر مصطفاوي، الأليات الجزائية والموضوعية لمواجهة الجرئم المتصلة بتكنولوجيا الإعلام والإتصال،أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة الجزائر 01،كلية الحقوق 2021- 2022.
7. لخضر دهيمي ،النظام القانوني لعمل الشرطة في الجزائر أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي،جلمعة البليدة 02السنة الجامعية 2015/2014 .
8. عبد العزيز ديلمي، دور الشرطة المجتمعية في الوقاية من الجريمة والإنحراف دراسة نظرية لبناء نموذج للشرطة الجوارية في الجزائر ،أطروحة مقدمة لنيل شهادة دكتوراه في العلوم الإجتماع الجريمة والإنحراف ، كلية العلوم الإنسانية والإجتماعية ،جامعة الجزائر 02،السنة الجامعية 2012-2013.

❖ **مذكرات :**

2. بغداد أدهم بسام ،وسائل البحث والتحري عن الجريمة الإلكترونية مذكرى مقدمة لنيل شهادة الماجستير،جامعة النجاح الوطنية ،غزة ،فلسطين.

3. سمية مزغي ،جرائم المساس با لأنظمة المعلوماتية ، مذكرة مقدمة لنيل شهادة الماجستير كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر بسكرة2014.
4. سفيان سوير ،جرائم المعلوماتية،مذكرة الماجستر ، كلية الحقوق والعلوم السياسية ، جامعة أبوبكربلقايد، تلمسان، 2010-2011.
5. عبد العزيز أحمد خصوصية التحقيق في الجريمة المعلوماتية،مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون الجنائي جامعة الطاهر ملاي كلية الحقوق والعلوم السياسية سعيدة ،2021-2022.
6. مريم أحمد مسعود ،أليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوءالقانون 09_04 ، مذكرة مقدمة لنيل شهادة الماجستير، تحصص قانون جنائي ، قسم حقوق كلية الحقوق والعلوم السياسية ،جامعة قاصدي مرباح ورقلة 2013/2012.
7. خلفي زوبير، الجرائم الماسة بتكنولوجيا الإعلام والإتصال في التشريع الجزائري ،مذكرة الماستر ،قانون جنائي ، جامعة العربي التبسي كلية الحقوق والعلوم السياسية تبسة،2023/2022.

❖ **مداخلات علمية :**

1. إلهام بن خليفة ،القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مداخلة ألقيت بمناسبة الملتقى الوطني الموسوم بعنوان " مكافحة المعلوماتية في مواجهة المخاطرية" ، المنعقد بجامعة محمد بوضياف المسيلة 26 فيفري2019، متاحة على الموقع الإلكتروني http;dspce.univ.eloued.dw تاريخ الإطلاع 2025/02/15على الساعة 14:14.
2. بارة سميرة ، الدفاع الوطني والسياسلت الوطنية للآمن السيبراني في الجزائر الدوور والتحديات ،ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من ملتقى الدوولي حول سياسات الدفاع الوطني بين الإلتزمات السياسية والتحديات الإقليمية كلية الحقوق والعلوم السياسية ،مخبر التحولات السياسية والإقتصادية والإجتماعية ، في التجربة الجزائرية جامعة قاصدي مرباح ،ورقلة يومي ،الإثنين والثلاء،30و31 جانفي 2017 .

3. حسين نوارة ،أليات تنظيم المشروع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة الإلكترونية ،الملتقى الوطني "أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"الجزائر 29 مارس.

4. سمير شبلاق ، حجية الدليل الرقمي في الكشف عن الجريمة ، مذكرة ماستر تخصص قانون جنائي عام قسم حقوق ، كلية الحقوق والعلوم السياسية ، جامعة دكتور مولاي الطاهر ،سعيدة ، الجزائر 2019-2020.

5. نشناش منية ،الركن المفترض في الجريمة المعلوماتية ورقة بحثية قدمت في ملتقى وطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة المنظم من قبل قسم الحقوق ومخبر الحقوق والحريات في الأنظمة المقارنة بكلية الحقوق والعلوم السياسية ،جامعة بسكرة المنعقد يومي 16/17نوفمبر 2015.

❖ **محاضرات:**

1. نادية بوراس محاضرات الجريمة الإلكترونية ،جامعة محمد لمين دباغين ،كلية الحقوق والعلوم السياسية ،سطيف (02)، سنة 2023/202.

❖ **المواقع الإلكترونية:**

الموقع الإلكتروني :https:// www.eurojust.europa .eu

أنظر الموقع الإلكترونيhttp://mawdoo3.com

فهرس المحتويات

فهرس المحتويات

مـلخص مذكرة الماستر

موضوع الجرائم الماسة بتكنولوجيا الإعلام والإتصال من المواضيع الحساسة جدا لما لها من تأثير على كيان الدولة سياسيا وإجتماعيا وإقتصاديا وأمنيا ، وعملية التصدي تتطلب مجهودا تشريعيا كبيرا على المستويين الدولي والوطني، فالجهود المبذولة في التصدي للجرائم الماسة بتكنولوجيات الإعلام والإتصال لم تكن بالقدر الكافي إلى بعد سنة2004 أين عدل المشرع الجزائري من قانون العقوبات وأضاف فصلا سابعا مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وأفرادها ضمن قانون خاص وهو القانون الجزائري رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والإتصال.

الكلمات المفتاحية:

1/ الجريمة المعلوماتية 2/المجرم الإلكتروني 3/ تكنولوجيا الإعلام والإتصال 4/ الدخول غير مصرح به 5/ الإختراق والتسرب 6/ معالجة آلية للمعطيات.

Abstract of Master's Thesis

The issue of crimes related to information and communication technologies is one of the very sensitive topics because of its impact on the states political, social, economic and security entity, and the response process requires a great legislative effort ,working at the international and national levels.In 2004,where did the Algerian legislator amend the penal cod and add a seventh repeated chapter to it under the title prejudice to automatic data processing systems, and its members within a special law, which is Algerian law No.09-04 containing special rules for the prevention of crimes related to information and communication technolog .

Keywords: **1/ Cybercrime 2/Cybercriminal 3/ Information and Communication Technology 4/ Unauthorized Access 5/ Hacking and Data Breach 6/ Automated Data Processing.**