وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم: قانون العام

المرجع:

مذكرة نهاية الدراسة لنيل شهادة الماستر

أساليب البحث والتحري في الجريمة الإلكترونية

الشعبة: الحقوق.

التخصص: قانون جنائي وعلوم جنائية

من إعداد الطالب(ة)

خيرات ليلى

تحت إشراف الأستاذ(ة)

بن عزوز صارة

أعضاء لجنة المناقشة

الأستاذ(ة)..... بن صابر فتيحة .....رئيسا

الأستاذ(ة)..... بن عزوز صارة .....مشرفا مقررا

الأستاذ(ة)..... مزيود صافي .....مناقشا

السنة الجامعية: 2024-2025

نوقشت يوم: 22-06-2025

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

UNIVERSITE

كلية الحقوق و العلوم السياسية
مصلحة الدراسات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: جبرات ليلى الصفة: طالبة جامعية

الحامل لبطاقة التعريف الوطنية رقم: 118017958 والصادرة بتاريخ: 07.12.2018

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون العام

والمكلف بإنجاز مذكرة ماستر بعنوان:

أساليب البحث والتحري في الجريمة الإلكترونية

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

التاريخ: 2025.06.30

إمضاء المعني

عن رئيس المجلس الشعبي البلدي
و بتفويض منه
مستشار إختصاص في الإدارة العامة

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

الإهداء

.بلي إذا أعطيتني نجاحا فلا تأخذ تواضعي، وإذا أعطيتني تواضعا فلا تأخذ اعتزازي بكر امتي

أهدي هذا العمل المتواضع

الى الصدر الدافئ، والقلب العطوف رمز الصبر و التضحية الجوهرة الثمينة" أمي" الغالية، الى من علمني أن أرسم على الوجوه المستنيرة،

.وسقاني كؤوس الكفاح، وكان القدوة في النضال وحسن مثال صاحب الشهامة " أبي" الغالي بارك الله في عمره

الى أخوتي واخواتي واولاد إخوتي

الى كل أهلي واقاربي

الى كل زملاء و أحباء

الى كل من ساهم من قريب أو بعيد في مديد العون

اليكم جميعا نتقدم بشكرنا الخالص.

خيرات ليلى

شكر و التقدير

بسم الله الرحمن الرحيم

"ربي أوزعني أن اشكر نعمتك التي أنعمت علي وعلى والدي و أن اعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين. " سورة النمل الآية 19

قال رسول الله صلى الله عليه و سلم " و من لا يشكر الناس لا يشكر الله"

نشكر الله عز و جل على أنه هدانا بالقوة لإتمام هذا العمل المتواضع.

كما أتقدم بالشكر الجزيل إلى الأستاذة " بن عزوز صارة" على نصائحها وتوجيهاتها التي أنارت دربي ، و التي لم تبخل علي بالمراجعة و المعلومات القيمة.

الشكر موصول كذلك للأساتذة الأفاضل أعضاء لجنة المناقشة.

كما نتقدم بالشكر الجزيل إلى كل من شجعنا وساندنا وقدم لنا العون والمساعدة والنصح والمشورة وساهم في إخراج هذا العمل إلى النور ونسأل الله أن يجعل ذلك في ميزان حسناتهم ويجزيهم عنا كل خير وأن يجعل هذا العمل خالص لوجهه سبحانه إنه سميع مجيب الدعاء .
وآخر دعوانا أن الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وصحبه أجمعين.

قائمة المختصرات

ق.ا .ج .ج :قانون الإجراءات الجزائية الجزائري

ص: صفحة

ط: طبعة

مج: مجلد

ب س ن: بدون سنة نشر

ع:العدد

ج: الجزء

ص ص:من صفحة إلى صفحة

مقدمة

إن التطور الهائل الذي شهده كل من محال تقنية المعلومات ومجال الإتصالات و الإندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، فبات يطلق على هذا العصر عصر المعلومات، فمنذ وقت ليس ببعيد كان كم المعلومات المتولدة عن التفاعلات البشرية محدودًا إلى حد كبير ولم يشكل حجمها أي مشكلة أمام عمليات تجميعها وتخزينها وإعادة استرجاعها ، إلا أنه ومع تقدم البشرية وتزايد معارف الإنسان وعلومه بدأ كم المعلومات يتزايد ويتكاثر وصارت الطرق التقليدية لتجميع وتنظيم هذه المعلومة العاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفعالية، وأصبح من الضروري اللجوء إلى استخدام أساليب علمية والتقنية متطورة لمواجهة هذه الطفرة ، فكان أن ظهرت الحاسبات الإلكترونية ، بالإضافة إلى ظهور مستحدثات تقنية كأقراص الفيديو الرقمية وأقراص الليزر، ووسائط الإتصال .... وذلك من أجل تسهيل التحكم في المعلومات ومعالجتها واسترجاعها، وهو مادعا بالكثير من رجال الاقتصاد و الإجتماع إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في القرنين التاسع عشر والعشرين، ففي حين كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان ، فإن هدف الثورة الثانية هو إحلال الآلة محل النشاط الذهني الانسان.[1]

إن جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة الكترونية أو بمعنى أدق رقمية يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية

[1]– عبد الجبار الحنيص، الإستخدام غير المشروع النظام الحاسوب في وجهة نظر القانون الجنائي، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، مج27، ع1 .2001.ص34

والاجتماعية والثقافية والأمنية. إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولا عربية كثيرة أضحت مهتمة بتلك الظواهر ، ومفهومها القانوني، وسمات المجرم المعلوماتي، وهو ما سوف نحاول أن تتعرض له بشئ من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة[1].

وتظهر **أهمية** دراسة هذا الموضوع في كونه يتسم بالحداثة، ولم ينل بعد حظه من الدراسة، وطبيعة الموضوع كونه محل اهتمام ودراسة على المستوى الوطني والدولي كذلك إزدياد حجم الجرائم، وما لجأ إليه المجرمون من استخدام لأحدث الأساليب العلمية الإرتكاب جرائمهم فكان لابد من التطرق للأساليب القانونية التي استحدثها المشرع للبحث والتحري على هذا النوع من الجرائم.

ينبع **الهدف** من هذه الدراسة من محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن جدة وحداثة الجرائم الإلكترونية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها و كيفية التعامل معها وأسلوب التحقيق فيها، إذ لا شك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

ولعل أهم **الاسباب** التي دفعتني للخوض في هذا الموضوع حداثة الموضوع ومحاولة جمع شتات الموضوع عبر التقصي في التشريع الداخلي عن العناصر ذات الصلة، ورغبتي الخاصة في الكتابة فيه خصوصا لما لمسته من مستجدات كثيرة واشكالات افرزها الواقع العملي.

تتمثل أسباب اختيار الموضوع في ما يلي:

[1]– هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة، الطبعة الأولى 1994،ص91

1- أسباب ذاتية: نظرا لما أحدثته الجريمة الإلكترونية من ضجة كبيرة في العالم، وما للموضوع من أهمية بالغة، اخترنا الخوض في هذا الموضوع أملا منا أن نثري المكتبة القانونية بعمل ولو بسيط.

2 -أسباب موضوعية: نظرا لتفشي ظاهرة الإجرام الإلكتروني بشكل سريع، وتطور الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية، مما أدى إلى خلق عدة صعوبات في إثبات هذا النوع من الجرائم، كان لزاما أن نتطرق إلى طرق إثبات هذه الجريمة المستحدثة ومعرفة قيمة الدليل الذي تثبت به أمام القضاء.

من هذا المنطلق نطرح الإشكالية التالية :

مامدى وجود قرار بقانون بشأن الجرائم الالكترونية فما مدى نجاعة الوسائل المتبعة في البحث التحري للكشف عن الجرائم الالكترونية؟

وإنطلاقاً من هذه الاشكالية يتفرع عنها بعض الاسئلة الفرعية وأهمها:

-مدى صلاحية الوسائل التقليدية في البحث والتحري عن الجريمة الالكترونية في ظل خصوصية هذه الجريمة؟

ماهية الجريمة الإلكترونية؟ وما هي فئات محرمي المعلوماتية ؟

-ما هي الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية؟

-ما أنواع الجرائم المعلوماتية أو الإلكترونية والوسائل المناسبة للحماية منها ؟

-ما هي الجرائم الإلكترونية المتواجدة بالمجتمع الليبي؟ وما موقف القانون الليبي منها ؟

-ماهي وسائل اساليب البحث والتحري الخاصة في المتابعة الجرائم الاكترونية؟

أما عن **المنهج العلمي** الذي اعتمدنا عليه في دراسة هذا البحث هو **المنهج التحليلي** القائم على تحليل النصوص القانونية والوقوف على المراد منها. واستيعاب الجوانب المختلفة لموضوع الدراسة.

و اعتمدنا أيضا على **المنهج الوصفي** من حيث معرفة مواصفات الدليل الإلكتروني والتي جعلته يتميز عن باقي الأدلة.

يقتضي إيفاء هذا الموضوع حقه تقسيمه هذه الموضوع الى فصلين اما عنوان **الفصل الأول الإطار النظري للجريمة الإلكترونية** وسوف نقسم الفصل إلى مبحثين، إذ سيكون عنوان المبحث الأول ماهية الجريمة الإلكترونية. وفي المبحث الثاني أساليب الكشف عن الجريمة الإلكترونية اما **عنوان الفصل الثاني جاء الإطار القانوني للتحري عن الجريمة الإلكترونية.**

ويتضمن مبحثين، سيخصص المبحث الأول الأساليب التقليدية للبحث والتحري عن الجريمة الإلكترونية. والمبحث الثاني الأساليب المستحدثة للبحث والتحري عن الجريمة الإلكترونية.

وسوف تنهي البحث بخاتمة تتضمن أهم النتائج والتوصيات

الفصل الأول :

الإطار النظري للجريمة الإلكترونية

في ظل عصر السرعة وثورة التكنولوجيا لا يستطيع أحد أن ينكر أهمية الانترنت، أحد أهم دعائم تكنولوجيا الاتصال والمعلومات. ولكن هناك على الجانب الآخر آثار سلبية من أهمها ظهور نوع جديد من الجرائم يدعى بجرائم المعلوماتية، تعتبر الجريمة المعلوماتية كظاهرة تضرب في عمق المجتمع وتدمره في وضع يتميز بالهدوء والسكينة.

الحداثة هذه الجريمة فقد كانت هناك عدة اتجاهات مختلفة في تعريفها، كما انها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى، كما أفرزت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية، والمجرم المعلوماتي ليس كأي مجرم متخصص ومحترف[1].

إن الجريمة الإلكترونية جريمة حديثة نسبيا لارتباطها بتكنولوجيا المعلومات المتطورة. فقد وجدت تعاريف مختلفة لها، كما أنها تقسم بمجموعة من الخصائص والسمات التي تميزها عن غيرها من الجرائم الأخرى، وأن هذه الجريمة ترتكب من قبل أفراد من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسب والتعامل مع شبكة الإنترنت[2].

وعليه سوف تتناول في هذا الفصل ماهية الجريمة الإلكترونية (المبحث الأول)، كما سنتطرق إلى دراسة التحري عن الجريمة الإلكترونية (المبحث الثاني).

[1]– غربي جميلة ،آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم القانون العام ،كلية الحقوق و العلوم السياسية،جامعة أكلي محند أولحاج البويرة،2021–2020، ص ص4.5

[2]– نهلا عبد القادر المومني ،الجرائم المعلوماتية ،دار الثقافة للنشر والتوزيع الأردن ،ط 2010 ،ص47

المبحث الأول : ماهية الجريمة الإلكترونية

تعددت الاجتهادات بشأن تعريف الجريمة الإلكترونية نتيجة لتباين وتنوع المعايير التي انطلقت منها تلك التعريفات، فهناك جانب من الباحثين عرفوها من زاوية تقنية، وآخرون عرفوها من زاوية قانونية، وهناك اجتهادات بتعريفها انطلقت من وسيلة ارتكابها، أو استناداً لمعايير تتعلق بمنفذيها، أو انطلاقاً من معايير خاصة متعلقة بالبيئة التي يتم فيها ارتكاب هذه الجريمة، وغيرها الكثير من المعايير الأخرى.

وغالباً ما يتم استخدام مصطلحات، كالافتراضية، والحاسوب، والبريد الإلكتروني، والإلكترونية، والرقمية والمعلوماتية، عند تعريف الجرائم الإلكترونية؛ الأمر الذي يعكس التداخل في المحتوى، أو يعكس فجوات مهمة في التعريف ، الذي عادة نراه يتأرجح بين الجرائم التي ترتكب بواسطة الحاسوب، وتلك التي ترتكب بواسطة أي نوعمن المعدات والوسائل الرقمية.

تعود البدايات الأولى لاستخدام مصطلح الجريمة الإلكترونية إلى وسائل الإعلام، التي اعتبرت الجريمة الإلكترونية ظاهرة صعبة التحديد كونها تنظم مجموعة من الأفعال والأنشطة غير المشروعة، ويكون القاسم المشترك بينها هو الإنترنت والحاسوب، أو مختلف التقنيات الحديثة للاتصال[1].

المطلب الأول : مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية جريمة مستحدثة نشأت نتاج التطور التكنولوجي الذي شهده العالم، وبالتالي وجب إثباتها والتوصل إلى مرتكبيها.

[1]– عبير مجلي ابو دية،الجرائم الإلكترونية(دراسة نظرية)،الملتقى الخامس للرابطة العربية للبحث العلمي و علوم العربي ،جامعة منوبة،تونس ،2018، ص ص4.5

ولما كان رجال القضاء يرنون إلى إيجاد طرق إثبات هذه الجريمة تتماشى وطبيعتها، وتضمن الإحاطة بجميع ملابساتها[1].

الفرع الأول : تعريف الجريمة الإلكترونية

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والإتصال، جرائم الكمبيوتر والأنترنت الجرائم المستحدثة، الجريمة الناعمة إجرام ذوي الياقات البيضاء. وتجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والإتصالات) وظهور مصطلح[2] cybercrime

أولا: الاتجاه الموسع لمفهوم الجريمة المعلوماتية.

يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم الجريمة المعلوماتية خشية حصرها في مجال ضيق فمنهم من عرفها بأنها : " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب ، كما يعرفها البعض بأنها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية أو المعنوية ، كما ترى الدكتورة نائلة

[1]– لبيض عادل ،نزلي بشرى،إثبات الجريمة الإلكترونية، مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإداري.قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة قاصدي مرباح،ورقلة،20172018،ص7

[2]– نايري عائشة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإداري،قسم الحقوق،كلية الحقوق و العلوم السياسية،احمد دراية ،2016–2017، ص ص5.6

عادل محمد فريد أن الجريمة المعلوماتية هي : كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دوراً لإتمامه، على أن يكون هذا الدور على قدر من الأهمية[1].

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات، أو بيانات أو برامج، أو محوها، أوكتابتها، أو أي تدخل آخر في محال إنجاز البيانات، أو معالجتها وتبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر[2].

ودائما حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة. أما البعض من الفقهاء يعرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسوب الآلي الرقمي و شبكة الأنثرنت بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف.

ومن خلال هذه التعريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص

الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل مجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا تكون أمام جريمة إلكترونية، كمن يقوم بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك[3].

---

[1]– عبد الحكيم ،مولاي ابراهيم ،الجريمة الإلكترونية ،مجلة الحقوق و العلوم الإنسانية ،ع23 ،جامعة زيان عاشور بالجلفة– الجزائر ،جوان2015،ص213

[2]– مليكة عطوي، المحلة السابقة الذكر، ص 09، نقلا عن الطاهر روابنية المسائلة، مقال ع 01، 1991، ص 15

[3]– نايري عائشة ،المرجع السابق،ص8

ثانيا: التعريف القانوني

تعرف الجريمة الالكترونية في القانون كونها فعل أو سلوك مادي يصدر عن إدارة جنائية عمدية يقرر لها قانون العقوبات عقوبة أو جزاء، أو هي فعل أو امتناع عن فعل يصدر عن مجرم ذكي يستخدم الوسيط الالكتروني لارتكاب أفعال غير مشروعة، وقد تطرق إليها.

المشرع الجزائري في المادة 02 من القانون 09-04 باعتبارها من قبيل الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو اتصالات الكترونية ونجد أن مختلف التعريفات تستند إما إلى موضوع الجريمة وأخرى إلى الوسيلة المستخدمة أو الصفات شخصية لدى مرتكب الفعل المجرم، أما المشرع الجزائري فحصر تعريف الجريمة الالكترونية في جانبها المعلوماتي فقط، بحيث ركز على أنظمة المعالجة الآلية للمعطيات الشخصية، دون التطرق إلى جوانب أخرى ترتبط بها، كالجانب الشخصي والجانب التقني، لذلك تختلف الجريمة الالكترونية عن الجريمة المعلوماتية في هذا التعريف.

غير أنه يتفق كل من التعريف الفقهي والقانوني في كون الجريمة الالكترونية هي فعل أو امتناع الهدف منه تحقيق الضرر وتتم عن طريق الحاسوب، هذا الأخير تتكون من مكونات مادية كأدوات ومستلزمات الكمبيوتر كالأقراص والشاشة، فهذه المكونات أو العناصر لا تتم عبر الولوج إلى شبكة الانترنت فقد يتم التعدي عليها عبر السرقة أو الكسر أو التفجير، ومن طرف شخص لا يفقه في التقنية أو استخدامها بشكل أو بآخر على خلاف العناصر التي تشكل محلا للجريمة الالكترونية كالبيانات والبرامج والمعلومات المختزنة داخله سواء بسرقتها أو تدميرها أو الاطلاع على أرقامها السرية والدخول إليها أو إرسال فيروسات عبر برامج ضارة[1].

[1]- مشري سلمى ،مفهوم الجريمة الإلكترونية،محاضرات في مقياس الجريمة الإلكترونية،جامعة تندوف،2016-2017، ص ص2.3

الفرع الثاني : أنواع (صور) الجريمة الإلكترونية

الجريمة الإلكترونية جريمة حديثة نسبيا، لارتباطها بتكنولوجيا المعلومات المتطورة، فقد وجدت تعاريف مختلفة لها، كما أنها تتسم بمجموعة من الخصائص والسمات التي تميزها عن غيرها من الجرائم الأخرى، وأن هذه الجريمة ترتكب من قبل أفراد من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسب والتعامل مع شبكة الإنترنت.

تتنوع الجرائم الإلكترونية تبعاً لتنوع مجالاتها، فيما يأتي عرضاً لبعض هذه الجرائم[1].

أولا – الجرائم التي تقع على الأشخاص:

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف.

أ- **الجريمة انتحال الشخصية** :هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت[2].

[1]– عبير مجلي أبو دية ،المرجع السابق،ص11

[2]– مدير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص ص42.43

ب – جريمة المضايقة والملاحقة: وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة، وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والصحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية[1].

ج – جرائم التغرير والاستدراج :هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمي الشبكة، وهي تقوم على عنصر الإمام حيث يوهم المجرمون ضحايا هم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية أو اجتماعية اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية[2].

د – جرائم التشهير وتشويه السمعة :مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم.

[1]– محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، ط الأولى، عمان، 2004، ص 45

[2]– عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر كلية الحقوق والعلوم السايسية، جامعة الطاهر مولاي، سعيدة، سنة 2015/2016، ص 19

وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة.

هـ- الجرائم المخلة بالأخلاق والآداب العامة : إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الالكترونية أو محاولة إغوائهم لإرتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة، وتصوير قاصرين ضمن أنشطة للجنس.

والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجا خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما حول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز[1].

ثانيا: الجرائم التي تقع على الأموال

هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية .

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فأنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن

[1]- عمار حشمان،الجريمة المعلوماتية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص إدارة التحقيقات الاقتصادية و المالية،قسم علوم التسيير ،كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير،جامعة قاصدي مرباح ،ورقلة ،2018-2019، ص ص6.7

الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي.

أ- جرائم صناعة ونشر الفيروسات: الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل.

وأما عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة. بها، وقد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشار، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي فون نيو مان على صعيد الحاسب الآلي دون الانترنت، ومن أشهرها فيروس رسائل الحب فيروس الدودة الحمراء، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في اقل من 9 ساعات عام[1] 2001.

ب- جرائم الاختراقات :الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت الحماية تلك الحاسبات أو الشبكات.

وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم المجرد الفضول والبعض الآخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

[1]- عمار حشمان،المرجع السابق، ص ص7.8

وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق.

ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع[1].

ج – جريمة تعطيل الأجهزة والشبكات: يطال التعطيل أجهزة الحاسب الآلي عبر برابحها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطلها وهو الأمر الذي يعيقها عن تأدية عملها.

د – جريمة النصب والاحتيال : أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف النصب والاحتيال ومن بينها

–خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت.

–إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات السرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم[2].

[1]– عمار حشمان،المرجع السابق،ص8.9

[2]– عمار حشمان،المرجع السابق،ص8

المطلب الثاني : الطبيعة القانونية للجريمة الإلكترونية

أصبحت الأجهزة الإلكترونية جزءاً مهماً في الحياة اليومية للإنسان: الحواسيب بأنواعها، وأجهزة الاتصالات على تنوعها التي يعدها الكثيرون إحدى أعمدة الحضارة التي نعيش والتطور الذي نشهد، ومنها كذلك أجهزة البث والاستقبال الفضائي وآلات التصوير وأجهزة التسجيل الصوتي وغيرها. ولا شك أن تلك الأجهزة تتكامل فيما بينها في الوظيفة، فضلاً عن التناسق التام في الصناعة حيث أدبحت آلات التصوير مع الحواسيب والهواتف النقالة بشكل واسع . وترافق مع هذا التطور ظهور جرائم الكمبيوتر والإنترنت وشاع مصطلح الجريمة الإلكترونية، أو جرائم التقنية العالية ، وبدأت الدول المتقدمة بسن التشريعات والقوانين التي تكفل مواجهة هذه الجرائم[1].

الفرع الأول : الخصائص الجريمة الإلكترونية

لما كانت الجريمة الإلكترونية هي نتاج التطور العلمي والتكنولوجي، وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا تجد لها مجموعة من الخصائص أو السمات تجعلها منفردة عن غيرها من الجرائم، سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة[2].

أولا : صعوبة اكتشاف الجريمة الإلكترونية .

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، وتعني الصعوبة في اكتشاف أن هناك جريمة وقعت، بغض النظر عن مرتكبيها، فقد تقع جريمة معلوماتية دون أن يشعر أحد بأن هناك جريمة وقعت إلا بعد مرور فترة من الزمن.

---

[1]– مداوي سعيد مداوي القحطاني،الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها، بحث لمسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015،وزراة الداخلية ،دولة قطر ،ص15

[2]– عبد القادر نشادي ،الجرائم المعلوماتية في وسائل الاتصال الحديثة دراسة وصفية تحليلية لمجموعة من الجرائم المرتكبة عبر الوسائط الاتصالية الحديثة في الجزائر، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والإتصال، كلية علوم الإعلام والإتصال، قسم الإتصال، جامعة الجزائر 3 2016–2017، ص ص 70–71

وغالبا لا يتم الإبلاغ عن هذه الجرائم إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، أصنف إلى ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي تم اكتشافها[1].

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى. وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة، يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

ثانيا: صعوبة اثبات الجريمة الإلكترونية

يعتبر اكتشاف الجريمة المعلوماتية – أمر كما سبق وذكرنا – ليس بالهين والسهل، ولكن حتى في حال اكتشافها والإبلاغ عنها، فإن اثباتها أمر تحيط به الكثير من الصعاب. أي الصعوبة في اثبات وقوع الجريمة بعد اكتشافها.

معظم هذه الجرائم لا تترك ورائها أثار تقليدية، مثل البصمات والآثار المادية في الجريمة العادية، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا توجد مستندات ورقية ولا شهود في القضية.

ولعل أسباب صعوبة اثبات الجريمة المعلوماتية تعود للاتي:

-إنها لا تترك أثرا بعد ارتكابها يلمس أو يرى بالعين المجردة.

-صعوبة الاحتفاظ الفني بأثارها إن وجدت.

-ضعف الخبرة الفنية لدى المحقق التقليدي مما يصعب عليه التعامل معها والتحقيق فيها.

-أنها جرائم ترتكب غالبا في الخفاء.

-سهولة محو الدليل والتخلص منه في ثوان معدودة.

[1]– نايري عائشة ،المرجع السابق،ص15

–ترتكب الجريمة في دولة ما وتتحقق النتيجة الإجرامية في دولة أخرى، أي أنها جريمة ليس لها حدود[1].

الفرع الثاني : أركان الجريمة الإلكترونية

إن للجريمة الإلكترونية أركان ثلاثة وتتمثل في الركن الشرعي وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

أما الركن المادي يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي, وأخيرا الركن المعنوي وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ[2].

أولا: الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه[3].

يترتب على إهمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي،

[1]– غربي جميلة،المرجع السابق،ص10.11

[2]– عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقاربة رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط 2014، ص ص من 26 إلى 36

[3]– أسامة أحمد المناعة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014، ص 45

إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم[1].

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين:

-مطابقة الفعل لنص التجريم.

-ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة.

ثانيا: الركن المادي

يسبق الفعل الإجرامي أعمال تحضيرية من شأنها تفعيل الركن المادي في هذه الجريمة كإمتلاك حاسب آلي واتصاله بشبكة الأنترنت، وامتلاكه برنامج للإختراق ذاو يقوم هو باستحداث هذا البرنامج، وغيرها من هذه السمات رغم أن هذه التقنيات مشروعة بحسب الأصل ما لم تستعمل في أفعال مجرمة، لذلك يشترط في الركن المادي مباشرة التصرف التقني وأن تكون لهذا الفاعل دراية كافية وتحكم في هذه الوسائل.

وهذا ما أورده المشرع في المادة الثانية من القانون رقم 09/04 السابق الذكر جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

[1]- حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، ط الأولى، منشورات الحلبي الحقوقية، بيروت 2014، ص 57

كما تناولت المادة 394 مكرر من ق.ع الأعمال المادية لهذه الجريمة كالدخول أو البقاء بطريقة غير مشروعة في كل أو جزء من المنظومة للمعالجة الآلية المعلوماتية أو يحاول ذلك. فمجرد محاولة تعتبر جريمة يعاقب عليها القانون، وتشدد العقوبة على هذا الفعل، كما تضلعف

العقوبة في حالة المساس بهذه المعطيات سواء كان ذلك بالحذف، أو تغيير، فالفعل المادي قد يتحقق بالنتيجة كدخول وتخريب، أو زيادة، أو محو أو بدون نتيجة كمحاولة واكتشاف المرتكب ومتابعته من خلال المنظومة الأمنية لأي دولة[1].

ثالثا: الركن المعنوي

يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه.

يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به بعد جريمة باعتبار حماية المشرع المحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي.

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم

[1]– غربي جميلة،المرجع السابق،ص15

يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع[1].

[1]– عمار حشمان،المرجع السابق، ص ص15.16

المبحث الثاني : أساليب الكشف عن الجريمة الإلكترونية

إذا وقعت جريمة ما ونما الى علم السلطات العامة نبأ ارتكابها فإن تلك السلطات تبدأ في التحرك وتتخذ مجموعة من الإجراءات التمهيدية بهدف تجميع أكبر قدر ممكن من المعلومات حول الجريمة وظروف ارتكباها، وتتمثل هذه الإجراءات في التحري الذي يقوم بها الضبطية القضائية ولا تبدأ إجراءات هذه المرحلة إلا بعد وقوع الجريمة، وهي تقوم على التحري عن الجرائم والبحث عن مرتكبيها وجمع الاستدلالات اللازمة للتحقيق في الدعوى.

حيث اسند المشرع الجزائري هذه العملية للضبطية القضائية وأعمال التحري تشكل مرحلة من المراحل الإجرائية التي تعقب وقوع الجريمة[1]، فإننا سنتناول في هذا المبحث مفهوم التحري وأهميته وضوابط التحري في الجريمة الإلكترونية.

المطلب الأول : مفهوم التحري

إن تحريك الدعوى العمومية يتوقف على توافر مجموعة من المعلومات التي تمكن للنيابة العامة من تحريكها، فيتم في مرحلة التحريات البحث عن الجرائم ومرتكبيها بجمع الأدلة والمعلومات من طرف الجهة القضائية المختصة والمعهود إليها هذه المهمة[2]. سوف تحاول الوقوف على تعريف التحري الفرع الأول،وأهمية التحري الفرع الثاني أما تحديد الطبيعة القانونية لإجراءات التحري الفرع الثالث.

الفرع الأول : تعريف التحري

التعريف التحري اختلف فقهاء القانون و ظهرت تعاريف مختلفة إلا أنها تصب كلها في نفس القالب سأحاول توضيحها في هذا الفرع.

---

[1]– عادل عبد العالي خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الاسكندرية. ص ص14.15

[2]– شناوي ليزا،مزاري ويزة،أساليب البحث والتحري عن الجرائم المستحدثة في قانون الإجراءات الجزائية،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون عام داخلي،قسم الحقوق ،كلية الحقوق و العلوم السياسية،جامعة مولود معمري تيزي وزو،2015–2016،ص5

أولا: التحري لغة واصطلاحا.

جاء معنى التحري في كتاب لسان العرب كما يلي:

تحرى الحرى عن | تحرى في / يتحرى ، تحر ، تحريا ، فهو متحر ، تحرى الحقيقة أي بحث عَنْهَا.

يَتَحَرَّى الأمور قبل البدء في أي مشروع بمعنى يَتَقَصَّاهَا بِالبَحْثِ وَالتَّنْقِيبِ وَالتَّفْتِيشِ.

مهنة الصحافي تدعوه إلى أن يتحرى صحة الأخبار أي أن يتأكد منها ومن مصادرها مباشرة [1].

أما اصطلاحا فلم يورد المشرع الجزائري في قانون الإجراءات الجزائية تعريفا واضحا المرحلة التحري الأولية واكتفى فقط بالإشارة إلى السلطة المكلفة بها، حيث تنص المادة 12 الفقرة 03 من نفس القانون ما يلي:

ويناط بالضبط القضائي مهمة البحث عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها تحقيق قضائي. "

إلا أن الفقهاء اجتهدوا في تعريفهم المرحلة التحري فنجد أن الدكتور احمد علي عرفها بأها مجموعة الإجراءات الأولية التي يباشرها رجال الضبطية القضائية لمجرد علمهم بارتكاب الجريمة والتي تتمثل في البحث عن الآثار والأدلة والقرائن التي تثبت ارتكاب الجريمة والبحث عن الفاعل والقبض عليه وإثبات ذلك في محاضر وتمهيد التصرف في الدعوى العمومية من طرف النيابة العامة.

[1]– أبي الفضل جمال الدين ابن منظور، لسان العرب ، مج الثاني، دار صادر ، بيروت ، ب د ن، ص 462

أما الدكتور محمد محدة فقد عرف مرحلة التحري والاستدلال بأنها إجراءات تمهيدية لإجراء الخصومة الجنائية ومستمرة بعدها وضرورة لازمة لتجميع الآثار والأدلة والمعلومات بهدف إزالة الغموض والملابسات المحيطة بالجريمة وملاحقة فاعلها.

وحسب رأي اللواء عبد الواحد إمام مرسى فهي مجموعة من الإجراءات الجوهرية غير المنظورة يتوخى فيها مأمور الضبط القضائي أو مرؤوسهم الصدق والدقة في التنقيب عن الحقائق المتعلقة الموضوع معين واستخراجها من مكمنها في إطار القانون[1].

ثانيا- التعريف القانوني.

تنص الفقرة الثانية من المادة 12 من قانون الإجراءات الجزائية على ما يلي:

ويناط بالضبط القضائي مهمة البحث عن الجريمة المقررة في قانون العقوبات وجمع الأدلة فيها والبحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي.

هذا النص يتطابق في محتواه مع نص الفقرة الأولى من المادة 14 من قانون الإجراءات الجزائية الفرنسي ونفس المنحى ملاحظة بالنسبة لأغلب التشريعات العربية.

مما سبق يمكننا أن نستخلص العناصر الأساسية للتحري والتي تتمثل في:

أ- أنها مجموعة من الإجراءات الجزائية.

ب- ينفذها أعضاء الضباط القضائي.

ج- تبدأ بعد ارتكاب الجريمة وتنتهي بتحريك الدعوى القضائية.

د- مضمونها معاينة الجرائم وجمع الأدلة عنها والبحث عن مرتكبيها.

[1]- خداوي مختار ،إجراءات البحث و التحري الخاصة في التشريع الجنائي الجزائري ،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص القانون الجنائي و العلوم الجنائية ،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة الطاهر مولاي سعيدة،2015-2016، ص ص12.13

هـ- تستهدف التمهيد لتحريك الدعوى العمومية ومباشرتها والسير في التحقيق القضائي.

وقد نهج نفس المنهج المشرع المصري في نص المادة 24 من قانون الإجراءات الجنائية، فإن المشرع قد أشار بمعنى عام وشامل بقوله في مجال تحديد اختصاصات مأمور الضبط القضائي ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على جميع الإيضاحات والتحريات وفقا لنص المادة نفس توضيح كافة الأمور المتعلقة بالجريمة أي كل من شأنه تحديد الجريمة ورسم معالمها[1].

الفرع الثاني : أهمية التحري

بمجرد وقوع الجريمة يقوم رجال الضبط القضائي بعمل التحريات والإجراءات اللازمة عنها وعن مرتكبيها وتحرير محضر بذلك فيما بعد على النيابة العامة التصرف فيه ولذلك فإن أهمية مرحلة البحث والتحري في الإجراءات الجزائية تتخذ صورا شتى تتناولها كالأتي:

أولا- أهميتها من حيث علاقتها بالخصومة الجنائية.

إن إجراءات البحث والتحري لا تخرج عن كونها إطار يعطي صورة واضحة عن وقوع الجريمة وكيفية حدوثها والظروف التي رافقتها ومحاولة الكشف عن الغموض المحيط بها وملاحقة مرتكبيها وضبطه. وهي بذلك إجراءات تمهيدية تساعد على تهيئة أدلة الدعوى إثباتا أو نفيا وتسهيل مهمة التحقيق الابتدائي والمحاكمة في كشف الحقيقة[2] وهذا ما يدل على المسؤوليات التي تقع على عاتق رجال الضبط القضائي أثناء قيامه بالبحث والتحري لكشف الحقيقة بشان الجريمة وفاعليها فيسمح ذلك بتقديم التهم للمحكمة مباشرة في اتخاذ إجراءاته وهو ما يحقق سرعة الفصل في الدعوى العمومية ويغني عن مضاعفة عدد قضاة التحقيق ولذلك نجد وكيل الجمهورية يكلف

[1]- بوديسة بجاد عبد الرؤوف،آليات التحري عن الجريمة الإلكترونية في القانون الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر ،تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة محمد البشير الإبراهيمي برج بوعريريج،2020-2021، ص ص32.33

[2]- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، ط السابعة، دار النهضة العربية، 1993 ، ص 331

رجال الضبط بجمع الاستدلالات، بل ويقومون به من تلقاء أنفسهم دون انتظار هذا التكليف أو حتى الإبلاغ بالجريمة[1].

ثانيا – أهميتها من حيث الإسهام في اختصار الإجراءات الجزائية:

إن البحث والتحري الذي يقوم به أعضاء الضبط القضائي يمكن للنيابة العامة من توجيه القضية الوجهة السليمة بعد أن يكتسب وكيل الجمهورية فكرة لا بأس بها استنادا لمحضر جمع الاستدلالات ونوعية الأدلة والقرائن التي تم جمعها والمعلومات التي تم الحصول عليها حيث بناءا على تلك المحاضر يمكن أن يقوم وكيل الجمهورية بحفظ القضية إذا رأى أنه لا محل للسير فيها وبذلك تسمح هذه المرحلة بحفظ الشكاوي والبلاغات غير المدعمة وهي بهذا النحو تساهم في سرعة الإجراءات الجنائية .

كما تعد بمثابة إعداد وتحضير للدعوى الجنائية، فالمعلومات التي يمكن جمعها من هذه المرحلة يمكن أن تنتج أدلة في الدعوى.

ثالثا: أهميتها من حيث المحافظة على أدلة الجريمة وآثارها:

إن أهمية البحث والتحري يظهر من خلال الكشف عن الأدلة المادية للجريمة والقيام بتجميعها، لأن هذه الآثار والأدلة هي التي تقود للكشف عن الغموض وهنا تظهر أهمية المحافظة عليها من الزوال ومنع الحاضرين من لمسها أو إضافة أي شيء عليها حتى تبقى في حالة سليمة لحين وصول رجال التحقيق وهذه الإجراءات ينبغي أن يقوم بها رجال الضبط القضائي بسرعة فور الإعلام بوقوع الجريمة، فقد ألزم المشرع ضباط الشرطة القضائية الانتقال إلى مكان الحادث لمعاينة مسرح الجريمة ، وهنالك بعض الجرائم يعتبر انتقال ضابط الشرطة القضائية إلى مسرح ارتكابها من أوجب الالتزامات حتى لا تطمس آثارها وهي الجرائم المتلبس بها وهذا ما نصت عليه المادة 42 من قانون الإجراءات الجزائية « يجب على ضابط الشرطة القضائية الذي بلغ

[1]– أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري، ج الأول، ديوان المطبوعات الجامعية .1998 ص166

بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة عنها[1].

الفرع الثالث : الطبيعة القانونية الإجراءات التحري

تتحدد هذه الأخيرة من خلال تحديد الطبيعة القانونية للجهة القضائية المكلفة بهذه المهمة المتمثلة في الضبطية القضائية ، بالنظر إلى الأعمال التي يقوم بها إذا كانت نفسها التحقيقات الإبتدائية أم إجراءات تسبق التحقيق الإبتدائي، وفي أي مرحلة من مراحل الخصومة الجنائية تجرى إجراءات التحري، وأساس تلك الطبيعة.

أولا: الطبيعة القانونية لمهام ضباط الشرطة القضائية.

يتسم قانون الإجراءات الجزائية بعدم الوضوح في تحديد أعمال الضبطية القضائية، إن كانت تحقيقات إبتدائية أم إجراءات أولية تسبق التحقيق الإبتدائي ؟

نستطيع القول أنها مرحلة تحري واستدلال كون الخصومة الجنائية من الأصل تمر بـ 3 مراحل (مرحلة التحري مرحلة التحقيق الإبتدائي مرحلة التحقيق النهائي "المحاكمة").

يستنتج ذلك من النصوص القانونية، فتنص المادة 13 من ق ا ج ج على ما يلي:" إذا ما افتتح التحقيق فإن على الضبط القضائي أن ينفذ تفويضات جهات التحقيق وتلبية لطلباته يتبين من المادة أن أعمال الضبطية القضائية يقف عند بداية التحقيق.

وهذا ما أكدته المادة 12 الفقرة الأخيرة " يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي بالإظافة إلى المادة 215 من قانون الإجراءات الجزائية التي تنص : " لا تعتبر

[1]– الكيال فاطمة ،ظوابط البحث و التحري على الجرائم،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم القانون العام،كلية الحقوق و العلوم السياسية،جامعة عبد الحميد بن باديس،2020–2021، ص ص8.9

المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك."

وكذلك المادة 17 من نفس القانون التي تبين وتوضح عمل عضو الشرطة القضائية التي تنص على " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و 13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الأولية ..." . هذا يعني أن المحاضر التي يحررها رجال الضبطية القضائية تسمى محاضر التحريات الأولية.

ثانيا: أساس تلك الطبيعة

أساس الطبيعة القانونية لأعمال الضبطية القضائية ووصفها بالتحريات الأولية هو استنتاج من النصوص الدستورية والقانونية وذلك بالرجوع إلى نص م 60 من دستور 2016 والمادة 215 من ق.ا.ج التي تؤكد ذلك[1].

المطلب الثاني : ضوابط التحري في الجريمة الإلكترونية

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية .[2]

حدد المشرع الجزائري في نص المادة 14 من قانون الإجراءات الجزائية صفة القائمين بالتحري والاستدلال وهم ضباط الشرطة القضائية، أعوان الضبط القضائي والموظفين والأعوان المنوط بيهم قانون بعض مهام الضبط القضائي، وأوردهم على سبيل الحصر ولم يجز لغيرهم مباشرة

[1]– شناوي ليزا،مزاري ويزة،المرجع السابق، ص ص 7.8.9

[2]– عز الدين عثماني .إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية مخبر المؤسسات الدستورية والنظم السياسية جامعة تبسة، ع 04، جانفي 2018،ص50

إجراءات التحقيق، كما حرص المشرع على ضرورة توافر صفات معينة في الشخص القائم بالتحري وذلك ضمانا لاحترام الحقوق الفردية في تلك المرحلة[1].

الفرع الأول : الأجهزة المكفلة بالتحري عن الجريمة الإلكترونية

لقد كان للتزايد المستمر للجرائم المعلوماتية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في محال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدثتتولى مهمة التحري عن جرائم العالم الافتراضي وكشف النقاب عنها، وقد حملت هذه الاجهزة تسميات مختلفة منها مثلا شرطة الانترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا، وسوف نستعرض أهم هذها لأجهزة سواء على المستوى الداخلي أو الدولي وذلك كما يلي:

أولا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي:

لقد ظهرت العديد من الأجهزة والهيئات المختصة في محال الجريمة المعلوماتية في إطار مكافحتها والبحث والتحري عنها وعن مرتكبيها سواء على المستوى الوطني أم على صعيد الدول الأجنبية.

إنه بالنظر إلى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة إلى أن تعهد بمسألة البحث والتحري عن هذا النوع من الجرائم الأجهزة متخصصة، لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا

[1]– المادة 14 من قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06/22 المؤرخ في 20/12/2006 بموجب الأمر رقم 15/02 ج ج جدش، ع 40

النوع المستحدث من الإحرام. وسوف تحاول أن تلقي الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نعرج على الوضع في بلادنا[1].

أ- **الأجهزة المختصة في الدول الأجنبية:** كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة وتذكر على سبيل المثال في هذا الصدد الدول التالية:

1-الولايات المتحدة الأمريكية: قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة المكافحة الجريمة المعلوماتية.

2 -في بريطانيا :قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المحال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001.

3 -في فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية.

4 -في الصين: قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم القوة المضادة للهكرة" وهي تختص برقابة المعلومات التي يسمح لمواطنيها. الدخول إليها عبر الأنترنات[2].

ب- الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني: أما الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الحريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلكإما على مستوى جهاز الشرطة أو الدرك الوطني.

---

[1]- سعيداني نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،مذكرة نهايةالدراسة للحصول على شهادة الماجستير،تخصص قانون جنائي،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الحاج لخضر باتنة،2012-2013، ص ص103.104

[2]- سعيداني نعيم ،المرجع السابق،ص105

فعلى مستوى جهاز الشرطة فقد أنشات المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها حلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر. أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإحرام بيوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية بالاضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها بيئر مراد رايس والتابع . المديرية الأمن العمومي للدرك الوطني وهو قيد الانشاء.

ثانيا : الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي.

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لابد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإحرام. ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن أن يحقق أهدافه لا قبل للشرطة الإقليمية بتحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد تذكر ما يلي[1]:

أ- على المستوى الدولي: بعد المنظمة الدولية للشرطة الجنائية (الأنتربول) من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة

[1]- سعيداني نعيم ،المرجع السابق،ص106.

الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية. وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين[1]:

الأولى : تجميع البيانات والمعلومات المتعلقة بالجريمة والمحرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

الثانية: التعاون في ملاحقة المحرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الحالية في مجال الجرائم المعلوماتية بوضع قائمة إسمية لضباط متخصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

ب- الأجهزة على المستوى الإقليمي.

الشرطة الأوروبية أو الأوروبول وهو جهاز على مستوى الإتحاد الأوروبي تم إنشاؤه في تكسبورغ عام 1992 ومقره في مدينة لاهاي هلندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في محال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإحراما المعلوماتي. ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة المختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية.

[1]- سعيداني نعيم ،المرجع السابق،ص107

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه إسم (Internet Crime Repporting online System) ICROS في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

الأوروجست :Eurojust وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد إختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوروبي أو دولة عضو مع دولة

أخرى من غير الاتحاد الأوروبي. وبعد الأروجيست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات و مباشرة متابعات جزائية[1].

الفرع الثاني : الوسائل المستخدمة في التحري وجمع الأدلة في الجريمة الإلكترونية.

عند القيام بالتحقيق في جريمة ما فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة وقواعد فنية تحقق الشرعية، وسهولة الوصول الى الجاني وحيث أن للجرائم الالكترونية طابعها الخاص المميز لها فإن التحري فيها يحتاج الى معرفة تامة وإدراك الرسائل وقوع الجريمة وبالتالي حل لغزها والوصول الى الجاني، وفي سبيل ذلك يعتمد المحقق على مجموعة من الوسائل المختلفة.

أولا: الوسائل المادية

وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحري المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

-عناوين IP والبريد الالكتروني وبرامج المحادثة.

[1]- سعيداني نعيم ،المرجع السابق،ص108

-البروكسي (PROXY) حيث يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة CASHE MEMORY وضمان الأمن وتوفير خدمات الذاكرة الجاهزة.

-برامج التتبع حيث تقوم هذه البرامج بالتعرف على محادثات الاختراق التي تتم مع تقديم بيان شامل بها الى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة الخدمة الأنترنت المستضيفة للمخترق. وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى ومن الأمثلة على HACKTRACER VL هذه البرامج.

-نظام كشف الاختراق (INTRASION DETECTION SYSTEM) ويرمز له اختصارا بالأحرف IDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجرى حدوثها على أجهزة الحاسبة الالكترونية أو الشبكة مع تحليلها بحثا عن أية إشارة قد تحل على وجود مشكلة قد تهدد أمن الحاسبة الالكترونية أو الشبكة.

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية أو الشبكة ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع[1].

وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

[1]- بوديسة بجاد عبد الرؤوف،المرجع السابق، ص ص42.43

-أدوات تدقيق ومراجعة العمليات الحاسوبية.

-أدوات فحص ومراقبة الشبكات، هذه الأدوات تستخدم في فحص بروتوكول ما وذلك المعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات ARPوظيفتها تحديد مكان الحاسبة الالكترونية فيزيائيا على الشبكة.

ثانيا : الرسائل الإجرامية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثانية والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

-اقتفاء الأثر : يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد الكتروني ثم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

-الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

-الاستعانة بالذكاء الاصطناعي، من خلال استنساخ النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية وفق برامج صممت خصيصا لهذا الغرض[1].

الفرع الثالث : الذكاء الاصطناعي و دوره في جريمة الإلكترونية

تعد التهديدات الأمنية الإلكترونية أكثر التحديات التي تواجهها الاقتصاديات العالمية، حيث بشكل استخدام أحدث تقنيات الحماية المعقدة وتعزيز أنظمة البنية التحتية لأمن المعلومات أزمة كبيرة على الاقتصاد لما تكلفه من مبالغ ضخمة، ويعتبر حجم الاستثمار في أمن المعلومات من أهم أولويات الحكومات والشركات في مختلف دول العالم، لذا يجب أن يكون هناك العديد من الاستراتيجيات الحماية الشركات ومختلف شبكاتها من التهديدات الحقيقية لأمن المعلومات صف لذلك أن المخاطر الإلكترونية التغير باستمرار والجرائم الالكترونية القسم الا بطابع دولي، من هنا تظهر الحاجة إلى بناء أنظمة ذكية لإدارة أمن المعلومات مبنية على تقنيات الذكاء الاصطناعي

[1]- بوديسة بجاد عبد الرؤوف،المرجع السابق،ص44

و منهاجياتها للدعم عمليات التحكم و المراقبة و اتحاد القرارات الدقيقة من قبل الخبراء وأصحاب المعرفة ودعم عمليات إدارة أمن المعلومات و اكتشاف عمليات التلاعب و التجسس[1].

كما أن تطبيقات الذكاء الاصطناعي في الكشف عن الجريمة ومواجهة الجرائم الالكترونية ومدى تطورها في المؤسسات العسكرية قد تتمثل في:

أولا: الذكاء الاصطناعي والمؤسسات العسكرية

في ظل التطور التكنولوجي والسباق نحو امتلاك تقنيات الذكاء الاصطناعي وسعيا للريادة العالمية في مختلف المجالات العسكرية منها والسلمية، ومع الصراع الشديد بين القوى الكبرى لامتلاك هذه التقنية العسكرية، أصبح من الضروري مواكبة هذه التطورات العالمية.

أ- **الذكاء الاصطناعي وموازين القوى العالمية:** يجد الذكاء الاصطناعي وتطبيقاته في المجالات المتعلقة بالمؤسسات العسكرية دعما شديدا من قبل الدول الصناعية الكبرى وخاصة أمريكا وانجلترا والصين، وقد أنشأت هذه الدول وكالات لتطوير تطبيقات الذكاء الاصطناعي في المجال العسكري حيث يمثل تطوير أسلحة بتقنيات الذكاء الاصطناعي مضمارا جديدا تتسابق فيه القوى العسكرية المؤثرة في العالم، وتمكن الباحثون في هذا المجال من تطوير العديد من الأسلحة الرئيسية والأنظمة المرتبطة بالأسلحة والتي تشكل جزءا من مبادرة استراتيجية التطبيقات الذكاء الاصطناعي، ومن هذه التطبيقات إنتاج المساعد الذكي للقبطان والذي يساعد الطيار المقاتل تحت ظروف المناورة الشديدة، ونماذج آليات الاستطلاع المستقلة التي يمكنها الدخول في أراضي العدو، وتجنب هجوم ونقل معلومات حربية إلى مراكز القيادة، أضف إلى ذلك العديد من النظم الذكية والتي تساعد القادة العسكريين على التوصل إلى قرارات صائبة في ظل الكم الهائل من المعطيات والمعلومات المعقدة والمتضاربة أحيانا والسرعة التي تميز الصراعات الحديثة في ظل التطور الحادث في العالم.

[1]- لخضر دولي ،نفيسة ناصري،دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية،على الموقع الإلكتروني: https://asjp.cerist.dz/en/article/87915التاريخ الولوج:10-05-2025على الساعة 12:20

وتشير التقارير الحديثة إلى أن عدد براءات الاختراع التي تم تسجيلها في تكنولوجيا الذكاء الصناعي في أبرز خمسة مكاتب لحقوق الملكية الفكرية سجلت زيادة بنحو 1 في المئة سنويا في المتوسط في السنوات الخمس الأخيرة، وفي ظل هذا الاتجاه ناحية تطبيق تقنيات الذكاء الاصطناعي في المجال العسكري تستطيع القول إن الغلبة في معارك المستقبل ستصبح لمن ينجح أكثر في تطبيق هذه التكنولوجيا في ساحات القتال. حيث سيسهم استخدام الذكاء الاصطناعي في تغيير أساسي لطبيعة الحروب .

وتجدر الإشارة هنا إلى أن الذكاء الاصطناعي في المجال العسكري قد يكون هو المتحكم الأول في موازين القوى العالمية حيث يرى خبراء أن الذكاء الاصطناعي مستقبل العالم كله وبطبيعة الحال فإن أية دولة تهيمن في هذا المجال ستحكم هي العالم، ومن جانب آخر يرى البعض أن التوسع في استخدام تطبيقات الذكاء الاصطناعي في المجال العسكري قد يكون له عواقب وخيمة فقد تتخذ الآلة العسكرية قرارا تلقائيا بشن هجوم استباقي ضد دولة أخرى إذا ما استشعر الذكاء الاصطناعي أن هذه الضربة قادرة على جسم المعركة المصلحة الجيش الذي يخدمه، الأمر الذي يطرحتساؤلاً هاما حول الدور البشري ومدى تدخله في عمل أنظمة الذكاء الاصطناعي العسكرية[1]، وذلك لكونهم يتمتعون بقدرات تحليل تواكب المتغيرات والمخاطر، لاتخاذ القرارات الصحيحة والتي تعد العنصر الحاسم للفوز بأي معركة، كما قد يؤدي التنافس بين الدول الكبرى من أجل امتلاك أفضل ما يمكن من الذكاء الاصطناعي العسكري هو السبب الأكثر منطقية لاندلاع حرب عالمية ثالثة في المستقبل القريب[2].

ب- تطور الأسلحة والذكاء الاصطناعي: نقل الذكاء الاصطناعي المجال من الحرب المعلوماتية إلى الحرب الذكية، لتصبح بذلك مركزية للصراعات في المستقبل إذ إن الحرب اليوم تتضمن نماذج بدائية أكثر من تكنولوجيا المعلومات. قد لا تكون العقول البشرية قادرة على مواكبة سرعة

[1]- مراد عبسي، الذكاء الاصطناعي العسكري وشرارة الحرب العالمية الثالثة،على الموقع الإلكتروني https://almustaqbal.com/article/1064951/:تاريخ9-9-2018،على الساعة 12:55

[2]- علي أحمد إبراهيم ،تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية،مجلة القانونية ،ع3 ،الأردن،ص 2821

صنع القرار التي يطلبها المقاتل المجهز بالذكاء الاصطناعي، وبالتالي يمكن للجيوش البدء في إبعاد البشر عن ساحة المعركة، وإعطائهم أدوارا إشرافية، والسماح لأنظمة غير مأهولة بالقتال للحفاظ على الأرواح البشرية، وهو ما يعني تغير استراتيجيات المعارك المستقبلية، ومن النماذج الجديرة بالدراسة والبحث في هذا المجال النموذج الصيني حيث بدأت القيادة الصينية في إعطاء الأولوية للذكاء الاصطناعي على أعلى المستويات، فقد أصدرت الصين خطة جديدة لتطوير الجيل الجديد من الذكاء الاصطناعي، واضعة جدول أعمال طموحا يهدف قيادة العالم في مجال الذكاء الاصطناعي بحلول عام 2030.وهي تدعم هذا الالتزام بتمويل عميق لأبحاث الذكاء الاصطناعي المتطورة بلغ نحو 150 مليار دولار في تطوير تقنيات الذكاء الاصطناعي في المجال العسكري، وفي هذا السياق نجحت شركة صينية مملوكة للدولة في إطلاق سرب مكون من 119طائرة دون طيار، كونت أشكالاً في السماء في إشارة إلى تقدم هذا القوة الاقتصادية العملاقة في مجال الذكاء الاصطناعي، ويعتقد أن الذكاء الاصطناعي العسكري الصيني سيدخل مجالات الحرب الإلكترونية والطائرات دون طيار التي بإمكانها ضرب أهداف الأعداء بكل سهولة[1].

ثانيا: الذكاء الاصطناعي ومواجهة الجرائم الالكترونية

تشير العديد من الدراسات إلى ظهور الاعتداءات الالكترونية والتي يطلق عليها القرصنة السيبرانية للسيطرة على الأجهزة الحكومية ووسائل النقل العالمية، وتهديد للبنية التحتية للدول، حيث تصبح الأجهزة المتصلة بالإنترنت وأنظمة الأتمتة المنزلية والأجهزة القابلة للارتداء أكثر انتشارا، مما يزيد من فرص القراصنة والمتسللين في غزو الحياة الخاصة بالإنسان والاضرار به ومن المتوقع أن تشمل مثل هذه الهجمات السيبرانية التسلل إلى الأجهزة القابلة للارتداء ورفع درجة حرارتها أو التسبب في إطلاق ومضة ضوئية للنظارات الإلكترونية تسبب العمى، أو إعطاب الأجهزة المنزلية وقطع التيار الكهربي عنها، على أن هذه الهجمات في الغالب لن تستهدف

[1]- علي أحمد إبراهيم ،المرجع السابق،ص2822

الإنسان نفسه لكنها على الأقل سوف تشعر الإنسان بأنه غير أمن في منزله إلى جانب ما سيلحق به من أضرار مادية.

أ- **الإرهاب السيبراني:** يعتبر الإرهاب السبيراني أكثر الظواهر الإجرامية مدعاة للقلق خلال السنوات القادمة، وقد ظهر مع انتشار البرامج الخبيثة والضارة الأجهزة الحاسبات، وامكانية استخدام الإرهابيين لشبكة الإنترنت في التدمير والفوضى ومن الممكن أن يكون هذا التدمير أكثر ضررا من الطرق التقليدية في العالم الحقيقي[1].

ب-**الابتزاز السيبراني:**حيث إنه ومع تطور التقنيات الحيوية والتي تقتصر حاليا على عدد قليل جدا من أجهزة المستخدمين، وبمجرد أن تصبح وسيلة أساسية لمصادقة الحسابات الخاصة بالفرد على الإنترنت سوف تصبح معرضة لخطر السرقة والاستيلاء عليها مثل أي نوع آخر من المعلومات، وهو ما سيسهل عمليات الابتزاز من خلال المطالبة بدفع فدية نظير عدم تدمير هذه الحسابات، وقد بدأت بالفعل الهجمات الإلكترونية تحت مسمى القدية في جميع أنحاء العالم، وإن كانت ليست شائعة جدا اليوم ولكن يتوقع في المستقبل القريب أن تنتشر على نطاق واسع، ثم من الممكن أن تصبح أكثر خطورة كان تتعرض المنازل والسيارات إلى هجمات الاصطياد تليها مطالب لدفع الفدية لجعلها تتوقف .

ج-**السوق السوداء للمعلومات:** انتشار أسواق المعلومات فتحت مجالاً خصبا الجرائم الحاسبات، حيث أصبح جزء كبير من اقتصاد الإنترنت يدور حول الإعلانات، وجزء كبير من هذا الإعلان يستهدف استخدام قواعد بيانات المعلومات الشخصية، وهذه المعلومات قيمة للغاية ومن الممكن أن تكون مسروقة فيما يسمى بالسوق السوداء للمعلومات والتي يمكن أن تتمثل في السجلات الطبية، ورسائل البريد الإلكتروني الشخصية، وغيرها من الشركات القائمة على المعلومات.[2]

[1]- علي أحمد إبراهيم ،المرجع السابق،ص2823

[2]- علي أحمد إبراهيم ،المرجع السابق،ص2824

خلاصة الفصل الأول:

تعد الجريمة الإلكترونية من الأنماط الإجرامية الحديثة، فجربها ثورة تقنية المعلومات والاتصالات عن بعد، مما جعلها تتميز بخصائص مختلفة، بحيث أوجدت بظهورها ويتطورها السريع إشكالات إجرائية أمام الجهات المكلفة بالبحث والتحقيق عنها وعن مقترفها، نتيجة القصور الذي اعترى النصوص الجزائية الإجرائية. الذي صيغت نصوصه لتنظيم الإجراءات المتعلقة بالجرائم التقليدية، بحيث لا توجد صعوبة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي، الذي له حرية تقدير الدليل ومن ثمة الأخذ به أو إبعاده.

الفصل الثاني :

الإطار القانوني للتحري عن الجريمة الإلكترونية

تتولى النيابة العامة القيام بإجراءات التحقيق والإشراف على الضبطية القضائية أثناء عملها في البحث الجنائي والتفتيش، فأجهزة الشرطة تقوم بدور فعال ورئيس حال وقوع الجريمة، بمعاينة مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة وذلك بهدف مساعدة أجهزة التحقيق للتوصل إلى حقيقة الواقعة ومعرفة مرتكبيها[1].

أما بالنسبة للجرائم الالكترونية فتختلف عن الجرائم الأخرى فيما تعلق بالتحري وجمع الأدلة، مما يوجب على السلطة المختصة بالتحقيق الإلمام الواسع بمعطيات الحاسوب وطبيعته وتشغيله ويتعين على المحقق معرفة بيئة الحاسوب والأنترنت والمعرفة الكافية بمسائل الضبط والتفتيش وكشف الأدلة والتحفظ عليها.

إن إجراءات التفتيش والضبط التي تقوم بها أجهزة الضبط القضائي سواء في الجرائم العادية أو الجرائم الواقعة على الحاسوب تمس حقوق الناس وحرياتهم لذا وجب أن تتم هذه الإجراءات بصورة صحيحة وقانونية، لأن اللجوء الى الطرق الغير مشروعة يؤدي الى بطلان هذه الإجراءات[2].

وعليه سوف تتناول في هذا الفصل الأساليب التقليدية للبحث و التحري عن الجريمة الإلكترونية (المبحث الأول)، كما سنتطرق إلى دراسة الأساليب المستحدثة للبحث والتحري عن الجريمة الإلكترونية (المبحث الثاني).

[1]– بوديسة بجاد عبد الرؤوف،المرجع السابق،ص48

[2]– مولاي ملياني دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان الجزائر ، 2017/2018.ص164

المبحث الأول : الأساليب التقليدية للبحث والتحري عن الجريمة الإلكترونية

يصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن تحدد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الأدلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم المعلوماتية .

ومما لا شك فيه أن المشرع لم يجز إستخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها: المعاينة، الخبرة التفتيش وضبط الأشياء ومما لاشك فيه أيضا أن هذه القواعد عامة النطاق تنظم إستخلاص الدليل في جميع الجرائم، تقليدية كانت أم مستحدثة إلا أنها في الثانية قد تكون بحاجة إلى تطوير لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها.

المطلب الأول : التفتيش

المقصود بالتفتيش في مدلوله القانونية لا يختلف سواء كان بالجرائم الإلكترونية أو في فقه الإجراءات الجزائية، فيقصد به بحث بوليسي أو قضائي لغاية ضبط ما يفيد في كشف الحقيقية فالهدف من التفتيش في الجرائم الإلكترونية هو ما يحتويه الحاسب الآلي من أشياء مادية ومعنوية تساعد في كشف الحقيقة ويمكن للقضاء نسبتها للمتهم، ويمكن أن يكون المحل الحاسب الآلي أو أنظمته أو شبكة الانترنت[1].

وفي حالة التفتيش، إذا كانت المكونات المادية في المنزل فإنها تخضع للتفتيش وفقا للقواعد العامة وفي حالة كانت هذه المكونات معزولة وموجودة في غير المكان المراد تفتيشه.

الفرع الأول : تعريف التفتيش

يعرف التفتيش على أنه البحث في مستودع السر عن أشياء تفيد في الكشف عن الجريمة وقعت ونسبتها الى مرتكبيها، وهو إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة

[1]- سعيداني نعيم،المرجع السابق،ص143

مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص. وذلك بهدف إثبات ارتكابها أو نسبتها الى المتهم وفقا لإجراءات قانونية محددة"، وعرفه البعض الآخر بأنه: " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون.

من خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة.[1]

كما يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية الجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة.

وأن ضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش والتي يتم الحصول عليها أثناءه. وعلى ذلك فإنه يتضح لنا أن هذين الإجرائين ما هما إلا وسيلة للإثبات المادي، ذلك أن التفتيش يستهدف ضبط أشياء مادية تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليه إرتكابها. كما أن رجال الضبطية القضائية قد تعودوا في الجرائم التقليدية على ضبط إلا الأشياء المادية.

من أجل هذا فإن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال إتخاذ الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية، لكون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي.[2]

[1]– مصطفى محمود محمد، الإثبات في المواد الجنائية في القانون المقارن ط 1. القاهرة مطبعة جامعة القاهرة 1987.ص214

[2]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية ما، دار الفكر الجامعي، الاسكندرية، مصر. 2009.ص182

ثانيا: أنواع التفتيش

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه الضابط الشرطة القضائية بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن بعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية بوضع اليد على الشيء وحبسه والمحافظة عليه للحصول على دليل المصلحة التحقيق عن طريق إثبات واقعة معينة [1]، وهو ما سنبرزه فيما يلي:

أ- **تفتيش نظم المعلوماتية:** عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات هي:

الحالة الأولى :في حالة ما إذا 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.

الحالة الثانية : إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في

[1]- مولاي ملياني دلال، المرجع السابق، ص 214

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الحالة الثالثة : إذا وجدت مكونات الحاسوب المادية في حالة الحاسوبات الآلية المحمولة في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة .... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات.[1]

ب- تفتيش نظم الحاسوب المنطقية أو المعنوية: يعرف الكيان المنطقي للحاسوب بأنه مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

وقد هذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذر التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن القاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك[2]".

الفرع الثاني : إجراءات التفتيش النظم الإلكترونية وضبطها

تتلخص هذه الإجراءات كما يلي:

أولا-إجراء التفتيش بحضور أشخاص معينين بالقانون :

من بين هذه الأشخاص المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية – القائم بالتفتيش ، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش

[1]- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنات، عالم الكتب الحديثة الأردن 2004 .ص 7.

[2]- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009، ص441

بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية الجزائري على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات."

ثانيا – إعداد محضر خاص بالتفتيش :

ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ثالثا – إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده :

لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه[1]، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي.

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

-تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خدمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على آثار الجريمة.

-إبعاد المتهم عن مكان النظام إن كان قريبا منه.

[1]- طارق إبراهيم الدسوقي عطية ،المرجع السابق، ص 385

-أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.

-الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.

-عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.

-يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها[1].

وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم الإلكترونية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم الإلكترونية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا السهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من ق إ ج ج[2].

المطلب الثاني : الحجز

ان ارتفاع معدل الجريمة الكترونية بسبب علاقتها بشبكة الانترنت أضطر العديد من الدول إلى سن قوانين موضوعية واجرائية لمواجهة هذه الجرائم المستحدثة والمشرع الجزائري استحدث اليات جديدة ومهمة للتصدي والكشف عنها من بينها إجراء الحجز الكتروني للبيانات المعلوماتية التي من اختصاص الضبطية القضائية بإضافة الى اجراء حفظ المعطيات المتعلقة بحركة السير

[1]- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الطلبي الحقوقية.2007.ص12

[2]- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1 .2011-2012.ص125

الذي يقوم به مزودي الخدمات الوسيطية وبالتالي تتضمن الدراسة في هذا الموضوع معطيات قانونية واخرى فنية وتقنية ذات أهمية بالغة[1].

وقد تبنى المشرع الجزائري في القانون 09/04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها المؤرخ في 05/08/2009 اجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان حجر المعطيات المعلوماتية ، وخص لها المواد التالية (06 .07. 08).

الفرع الأول: تعريف الحجز

يختلف الحجز الأشياء في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل ، ففي هذه الأخيرة يكون المحل أشياء مادية ، أما في الجريمة الإلكترونية تكن الأشياء ذات طبيعة معنوية كالبيانات ، المراسلات الإلكترونية ، وتجدر الإشارة إلى أن الحجز الأشياء قد يرد على عناصر معلوماتية منفصلة مثل الأسطوانات الممغنطة، وهنا لا يثور أي إشكال عند القيام بالضبط ، لكن الصعوبة تكون عندما يلزم ضبط النظام كله ، أو الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها . أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية : – وحدات الإدخال – لوحة المفاتيح– الفارة –نظام القلم الضوئي – وحجز وحدة الإخراج – الشاشة – الطابعة – الرسم –والمصغرات الفيلمية ، وكل ما يتم ضبطه من بيانات إلكترونية يتعين تحريزها وتأمينها فنيا .. تنص المادة 06 من القانون رقم 04-09 على أنه : " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ، أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية[2].

[1]– عفيفي كامل عفيفي، المرجع السابق، ص 65

[2]– طرشي نورة المرجع السابق، ص 126

الفرع الثاني : إجراءات الحجز المعطيات المعلوماتية.

تناوله المشرع في المادتين 6 و 7 من القانون رقم 09/04 السابق الذكر، وتتمثل شروط إجراء الحجز فيما يلي[1]:

-عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

-يجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

- إذا استحال إجراء الحجز وفقا لما هو منصوص عليه فيما سبق لأسباب تقنية، لذا يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

-على السلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

[1]- فلاح عبد القادر ،حجز و حفظ في الجريمة الإلكترونية،على الموقع الإلكتروني https://asjp.cerist.dz/en/article/169811:التاريخ الولوج:28-04-2025على الساعة11:23

-تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

كما نظم القانون رقم 09/04 السالف الذكر إجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها في المادة 10 منه، وجعله من التزامات مقدمي الخدمات في مساعدة السلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وأضافت المادة 12 من ذات القانون أنه زيادة على الالتزامات المنصوص عليها في المادة 11 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، يتعين على مقدمي خدمات "الانترنت" ما يأتي:

-التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن[1].

[1]- فلاح عبد القادر،أيت عبد المالك نادية ،التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري،العدد2،المجلد 4.2019.خميس مليانة،ص1698

المبحث الثاني : الأساليب المستحدثة للبحث والتحري عن الجريمة الإلكترونية

تطرقنا فيما سبق وبالرجوع إلى الأنظمة القانونية الإجرائية الحالية، يلحظ أن هناك قصورا بخصوص أساليب التحري التقليدية في استخلاص الدليل الإلكتروني. فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة، كما أن هذه الإجراءات تخص استخلاص الدليل من الجرائم سواء كانت تقليدية أو مستحدثة، والأكيد أن هذه الإجراءات غير كافية لاستيعاب كافة أشكال الجريمة الالكترونية، فهي تحتاج من المشرع تدعيمها أو استحداث أخرى جديدة لمواكبة التطورات التقنية في مجال مكافحة الجريمة الالكترونية، وما قام به المشرع الجزائري في التعديلات المتتالية لأحكام قانون الإجراءات الجزائية، بإدراج قواعد إجرائية جزائية جديدة وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد.

فنص المشرع الجزائري على إجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في التسرب واعتراض المراسلات وكذلك من خلال القانون 01-02 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، استحداث إجراءين آخرين هما المراقبة الإلكترونية وحفظ المعطيات.[1]

المطلب الأول : المراسلات تسجيل الأصوات التقاط الصور

مكن المشرع الجزائري ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[2].

[1]- مسعود شهيرة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي،قسم القانون العام،كلية الحقوق و العلوم السياسية،جامعة عبد الحميد بن باديس مستغانم،2020-2021،ص ص45،44

[2]- المادة 21 من المرسوم الرئاسي رقم 15/261 المؤرخ في 8 أكتوبر 2015 المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، جره العدد 53 الصادرة في 8 أكتوبر 2015

والتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات، فيتم عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية[1].

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 09/04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية المراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

بالإضافة إلى أن كل منهم بريء حتى تثبت إدانته ، لذلك هل يجوز إثبات أو نفي الاتهام عن المشتبه فيه، باللجوء إلى وسيلة التسجيل الصوتي أو اعتراض المراسلات أو التقاط الصور في الأماكن العامة والخاصة.[2]

[1]– غربي جميلة ،المرجع السابق،ص ص68،69

[2]– معتوق عبد اللطيف، الإطار القانوني المكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج الخضرة باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق، 2011–2012 ، ص106

الفرع الأول : المراسلات

لقد اتخذ المحرمين من المراسلات وسيلة لتسهيل وتنفيذ مخططاتهم الإجرامية وخصوصا الوسائل العصرية المتطورة مثل الوسائل السلكية واللاسلكية ، ومقابل ذلك أدرج المشرع الجزائري أساليب الاعتراض تلك المراسلات قصد إحباط هذه المخططات الإجرامية وكشف حيلهم.

أولا: تعريف المراسلات

الاعتراض يعني الاستيلاء بغتة واعتراض المراسلات يقصد به التتبع السري والمتواصل للمراسلات الخاصة بالمشتبه به ودون علمه، ويعرف على انه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية في مواجهة الإحرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية[1].

يقصد بالمراسلات قانونا هي جميع الخطابات المكتوبة سواء أرسلت بطريق البريد أو بواسطة رسول خاص، وكذلك المطبوعات والطرود والبرقيات التي توجد لدى مكاتب وسواء كانت داخل مظروف مغلق أو مفتوح ، كما تعد من قبيل المرسلات الخطابات التي تكون في بطاقة مكشوفة متى كان واضحا أن المراسل قصد عدم اطلاع الغير عليها دون تمييز[2].

إلا أن هناك من يرى أن المراسلات يقصد بها التخابر والاتصال بين الأفراد فيما بينهم سواء بالكتابة أو غيرها أي سواء كانت رسائل بريدية أو مكالمات هاتفية.

والمشرع الجزائري في المادة 65 مكرر 5 من قانون الاجراءات الجزائية خص بالذكر المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ، دون الرسائل والخطابات

[1]– خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة الجزائر، 2010، ص ص 72–73

[2]– حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، ط الثانية، منشأة المعارف، الإسكندرية، مصر، 1990، ص 78.

والمطبوعات والطرود لدى مكاتب البريد.وعليه فإن السؤال المطروح، هل هذه الأخيرة فعلا ليست معنية بالاعتراض؟

إلى حين إثبات العكس، فمن الملائم عدم الكلام عن الاعتراض إلا عندما يتعلق الأمر بمراقبة اتصال سلكي أو لاسلكي بين مرسل ومرسل إليه دون علمهما أو على الأقل دون علم أحدهما فقط.

ونظرا للتطور الذي عرفه مجال الاتصال فإن نص المادة 65 مكرر 5 السالفة الذكر جاء موسعا، أي لم يقتصر الاعتراض على المكالمات الهاتفية فحسب بل وسعه لمختلف أنواع الاتصال السلكية واللاسلكية ، كما أن المشرع لم يول أهمية لأداة الاعتراض فقد تكون تقليدية أو بأحدث ما تم ابتكاره في هذا المجال[1].

ثانيا : التكييف القانوني لإجراءات المراسلات

يعتبر إجراء التنصت الهاتفي من نوع خاص حيث أنه يلجأ إليها في أي مرحلة من مراحل الجريمة، وهذه العملية تخضع إلى أحكام خاصة والتي تضمن ضمانات من شأنها حماية الحياة الخاصة يتبين ذلك من حيث أنه:

لا يلجأ إلى إجراء التنصت الهاتفي باعتباره إجراء مستحدث إلا في الجرائم الخطيرة.

يتم إجراء التصنت خفية وبدون رضا المشتبه فيه، خاصة وأن المتهم لو كان يعلم بهذا التسمع ما صدر منه ذلك الحديث.

إجراء التصنت يكون بموجب الفترة المحددة في الإذن الذي تختلف من تشريع إلى آخر فضلا على أنه عند وضع الترتيبات التقنية قد أجاز القانون الدخول إلى المحلات السكنية في أي ساعة من اليوم.

[1]- عمار حشمان،المرجع السابق،ص54

يترتب على إجراء التسمع ضبط دلائل معنوية فلا تكتسب الطبيعة المادية إلا إذا سجلت ونسخت في أجهزة معدة لهذا الغرض[1].

ثالثا: الشروط و ضمانات المقررة المراسلات السلكية واللاسلكية

مما لاشك فيه أن أسلوب إعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم المعلوماتية، فهو من جانب آخر يمثل إنتهاكا لحرمة الحياة الخاصة للأفراد وإعتداء على سرية مراسلاتهم وإتصلاتهم التي كفلتها الدساتير والتشريعات العقابية .والمشرع الجزائري في هذا الصدد كما أعطى لسلطات التحقيق مكنة إعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، فمن ناحية أخرى لم يفتح الباب على مصرعيه في اللجوء إلى هذه الوسيلة بل أحاط إستخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

أ- **ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:** طبقا للمادة 05 مكرر من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء إعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء[2] .

وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الإعتراض وحديثه وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا، مع ملاحظة أنه في فرنسا ومنذ صدور القانون 2004/204 المؤرخ في

[1]- ياسر الأمير فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، جامعة القاهرة، ط1، 2009، ص 150

[2]- أحمد فتحي سرور ،الوسيط في قانون الإجراءات الجزائية ، دار النهضة العربية، القاهرة، ط3، 1981، ص 9

09/03/2004 المعدل لقانون الإجراءات الجزائية أصبح حسب المادة 706/95 الإذن بإعتراض المراسلات من إختصاص قاضي الحريات والاحتباس بمنحه بناءا على طلب من وكيل الجمهورية إذا تعلق الأمر بالتحقيق في الجرائم المحددة حصرا بالمادة 706-73، وتخضع إجراءات الإعتراض لرقابته في أجل 15 يوم قابلة للتجديد بنفس الشروط في الشكل والأجل.

وقد نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء إعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية إعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والإنتهاء منها.

ب- تحديد طبيعة المراسلة ومدة الإعتراض: وهذا ما يفهم صراحة من نص المادة 65 مكرر 7 التي نصت على أنه يجب أن يتضمن الإذن بإعتراض المراسلات كل العناصر التي تسمحبالتعرف على الإتصالات أو المراسلات المطلوب إعتراضها، كما أن المشرع قد إستوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا المقتضيات التحري والتحقيق وهي نفس المدة التي حددها المشرع الفرنسي في المادة 100 من قانون الإجراءات الجزائية الفرنسي.[1]

[1]- عمار فوزي ، مجلة علوم الانسانية ، جامعة منتوري – قسنطينة ، ع33 ، جوان 2010،ص237

الفرع الثاني : تسجيل الأصوات

تعتبر الأحاديث الشخصية أسلوب من أساليب الحياة الخاصة للأفراد، يتم من خلالها تبادل للأسرار وللأفكار الشخصية دون خشية تصنت الغير عليها أو إستراق السمع.

لكن ومع إنتشار الجرائم الخطيرة أجاز المشرع اللجوء للمراقبة السمعية لأجل كشف غموض الجريمة وضبط الجناة من خلال الاستعانة بتقنيات متطورة .نصت على أسلوب تسجيل الأصوات م 65 مكرر 5 من ق.ا.ج.

أولا: تعريف تسجيل الأصوات

يعرف بأنه النقل المباشر واللآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل بحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي، بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه والتسجيل الصوتي المتخذ كوسيلة للتحري عن الجرائم يشمل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة[1].

يتم تسجيلها بأجهزة تعمل بواسطة الإتصال السلكي الخارجي أو اللاسلكي والتي تتم عن طريق وضع مكروفونات تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة.

التسجيل الصوتي الذي يهمنا هو الذي يجريه رجال الضبطية القضائية للاستعانة به في مجال الإثبات الجنائي، وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية، نظراً لكونها لم تصدر في شأن دعوى جنائية حركتها السلطات القضائية بقصد الحصول على الحقيقة كما يخرج عن نطاق البحث تسجيل الأحاديث التي تتضمن إعتداء على حق من

[1]- حافظ بن زلاط مقال منشور على الأنترنت بعنوان التصنت الهاتفي في ظل قانون الإجراءات الجزائية، 2015 .على الموقع الإلكتروني www.droitetentreprise.org:

التاريخ الولوج:2025-05-18على الساعة 16:30

يتم تسجيل حديثه، كما في حالة تسجيل الأحاديث التليفونية أو الإذاعية أو الصحفية متى تم ذلك بموافقة المعني[1].

ثانيا : شروطها

كما رأينا سلفا، وحفاظا على الحق في سرية المراسلات بكافة أنواعها والمكفولة دستوريا، أحاط المشرع الجزائري إجراء المراقبة الالكترونية تحت طائلة البطلان بشروط قانونية، تتمثل في النقاط الآتية:

أ- وجود إذن قضائي: أوجب المشرع الجزائري وجود الإذن القضائي الصادر عن السلطة القضائية المختصة وذلك بموجب المادة 4/105 من القانون 09-04 سالف الذكر التي تنص على "... لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية، عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة سنة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

ب- وجود ضرورة: يتم اللجوء إلى إجراء مراقبة الاتصالات الالكترونية في حالة توفر معمومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو المقتضيات التحريات كالتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[2].

[1]- سعيداني نعيم،المرجع السابق،ص180

[2]- سعيداني نعيم،المرجع نفسه،ص181

الفرع الثالث : التقاط الصور

لا يجوز بأي حال من الأحوال النقاط صور لشخص ما دون رضاه أو محاكاتها أو نشرها لأن ذلك يعتبر تدخل في حياته الخاصة وهنكا لحق من حقوق الإنسان التي تحميها مواثيق حقوق الإنسان والدساتير الوطنية ، فقد نص الدستور الجزائري في المادة 39 على أنه : "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون" [1] ، إلا أن هناك استثناءا من هذا المبدأ شرعه المشرع الجزائري قصد مكافحة جرائم الفساد وحماية الصالح العام.

وقد رخص القضاء النقاط الصور كوسيلة لتحديد هوية المشتبه فيه ، وهذا ما يدل على أن القضاء الجنائي لم يستبعد استعمال هذه الوسيلة في الإثبات الجنائي، لأن حجية الصورة الفوتوغرافية مرتبطة بحالات التلبس التي يقوم ضابط الشرطة القضائية بإثباتها وهذا خلال جميع مراحل البحث والتحري ، كتصوير أفراد العصابة ومحمل الجريمة وعمليات استلام و تسليم الاشياء والوسائل المستعملة إلى غير ذلك من الأدلة الجنائية.

أولا: تعريف النقاط الصور

لم يتطرق المشرع الجزائري إلى تعريف عملية التقاط الصور وقد أشار إليها فقط بمصطلح "الالتقاط" ، إلا أن البعض عرفها بأنها تمثيل لشخص أو شيء عن طريق أحد الفنون من نقش أو تحت أو تصوير فوتوغرافي أو فيلم ، ولم تقف الصورة عند حد تجسيد المادة لشخص ما بل تعدت ذلك إلى عكس شخصيته و انفعالاته[2].

[1]– حولي فرح الدين، أساليب البحث والتحري طبقاً للقانون رقم 06–22 المعدل والمتم لقانون الإجراءات الجزائية مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء .2009.ص20

[2]– ركاب أمينة، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان 2015.ص ص 60.61

وبما أن المحرمين لم يتوانوا في استخدام أحدث الأساليب العلمية في ارتكاب الجريمة ، كان لا بد من استغلال التطور العلمي والتكنولوجي في محاربة هذه الجريمة ، فقد استمر التطور التقني في إنتاج أجهزة التصوير وزيادة كفاءة العدسات التلسكوبية وأجهزة تصوير الأفلام.

ومن بين الأجهزة المستعملة في هذا الإجراء بجد وسائل الرؤية والمشاهدة القادرة على التصوير من مسافات بعيدة ، وأجهزة التصوير بالأشعة تحت الحمراء التي تتيح التصوير في الظلام ، والمرايا ذات الازدواج المرئي الي تسمح بالتصوير داخل الأماكن المغلقة من خلال زجاج شفاف من جهة و يبدو كالمرأة من الجهة التصوير وزيادة كفاءة العدسات التلسكوبية وأجهزة تصوير الأفلام ومن بين الأجهزة المستعملة في هذا الإجراء بجد وسائل الرؤية والمشاهدة القادرة على التصوير من مسافات بعيدة ، وأجهزة التصوير بالأشعة تحت الحمراء التي تتيح التصوير في الظلام ، والمرايا ذات الازدواج المرئي الي تسمح بالتصوير داخل الأماكن المغلقة من خلال زجاج شفاف من جهة و يبدو كالمرآة من الجهة الأخرى ، وعدسات التصوير الدقيقة التي يسهل وضعها بزوايا الغرف أو بمفاتيح الإثارة أو بأماكن من الصعب التعرف عليها[1].

ثانيا : شروطها

لكي تكون عملية النقاط الصور مشروعة ووفق الإجراءات القانونية يجب أن تتوفر بعض الشروط الموضوعية والشكلية ، وهذه الشروط ليست خاصة بالتقاط الصور فقط وإنما هي خاصة كذلك بعملية اعتراض المراسلات و تسجيل الأصوات وهي كالآتي :

أ- **الشروط الموضوعية:** السلطة المختصة بإجراء العملية : وكيل الجمهورية أو قاضي التحقيق بالرغم من أنه لا يقوم بهذا الاجراء بنفسه ، إلا أنه يجري تحت إشرافه و مراقبته المباشرة.

[1]- مباركية رابح،إجراءات التحري و التحقيق في الجريمة الإلكترونية،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد البشير الإبراهيمي برج بوعريريج،2021-2022،ص ص82.83

1 –وقت و مكان إجراء العمليات : لم يضع المشرع الجزائري قيود زمنية ولا مكانية لهذه الإجراءات الخاصة حيث أجازها في أي وقت من ليل أو نهار وفي أي مكان عام أو خاص باستثناء السفارات و القنصليات الأجنبية التي لا يمكن أن تخضع لهذه العمليات.

2 –عدم مسؤولية القائم والمشرف على هذه العمليات : إن الاعتداء على الحياة الخاصة بتسجيل الأصوات و اعتراض المراسلات و التقاط الصور و دخول مساكن بغير اذن صاحبها و تسلق الجدران ليلا و فتح الأقفال وغيرها كلها أفعال محرمة ، إلا أنها لا تعتبر كذلك إذا ما تمت في إطار إجراءات البحث و التحري الخاصة وبإذن من وكيل الجمهورية أو قاضي التحقيق.

3 –ضرورة اللجوء اليها : لا بد أن توجد ضرورة ماسة تستدعي اللجوء إلى القيام بهذه الإجراءات إضافة إلى وقوع حريمة من الجرائم السبعة المذكورة بنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية وهي وجود دلائل قوية ونسبتها إلى المتهم[1].

ثانيا : الشروط الشكلية

1– إذن وكيل الجمهورية أو قاضي التحقيق قبل مباشرة العملية : حسب نص المادة 65 مكررة من قانون الإجراءات الجزائية فعند وقوع إحدى الجرائم المذكورة ضمن نفس المادة يجوز الوكيل الجمهورية أو لقاضي التحقيق أن يأذن باعتراض المراسلات وتسجيل الأصوات والنقاط الصور، بمعنى لا بد من وجود إذن مسبق قبل البدء بهذه العمليات .

2 –ضرورة أن يكون الإذن مكتوب : يجب أن يكون الإذن مكتوب ويسلم الضابط الشرطة القضائية المكلف بالعمليات وهو يعطي الحق الحاملة الاستعانة بأهل الخبرة.

3 –محاضر العمليات : يجب تحرير محضر يرسل الى قاضي التحقيق عند كل مرحلة على حدا وبشكل منفصل ولا يتم الانتظار إلى بلوغ المرحلة النهائية ، حيث يشمل كل محضر تاريخ وساعة بداية العملية ونهايتها ويرفق محضر يتضمن وصفا أو نسخة من المراسلات والصور

[1]– أحمد غاي ، ضمانات المشتبه فيه أثناء التحريات الأولية ، ط 1 ، دار هومة ، الجزائر ، 2005، ص 231

والمحادثات وإذا كانت المكالمات أو المحادثات بلغة أجنبية يتم ترجمتها من طرف مترجم يتم تسخيره لهذا الغرض[1].

المطلب الثاني : التسرب

استحدث المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات ، وذلك بسبب عجز الأساليب التقليدية ، ومن بينها إدراج المشرع لعملية التسرب بموجب القانون رقم 06-22، مؤرخ في سنة 2006 ، المتضمن قانون الإجراءات الجزائية ، حيث خص الفصل الخامس منه تحت عنوان " في التسرب " ، المواد من 65 مكرر 11 إلى المادة 65 مكرر 18 ، إذ تناول من خلالها مفهوم هذه العملية وشروط إجراءها ، و الحماية الجنائية للقائم بعملية التسرب[2].

الفرع الأول: تعريف التسرب

تعرف المادة (65) مكرر (12) من القانون الإجراءات الجزائية الجزائري التسرب على أنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك .

انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية. لذلك اعتبار لهذه الضرورة تقطن المشرع الجزائري وجرد الضابط أو

[1]- رشيد شميشم، الحق في الصورة ، مجلة العلوم الانسانية والاجتماعية، جامعة المدية ، ع03 ، 2008 ، ص 127

[2]- محمد أمين الخرشة مشروعية الصوت والصورة في الإثبات الجنائي، ط1، دار الثقافة، الأردن، 2011،ص171

العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب[1].

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة (65) مكرر (16) من قانون الإجراءات الجزائية بأنه لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء ... وما تضمنته كذلك المادة (65) مكرر (17) من القانون نفسه بأنه " إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة (65) مكرر (14) أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر .

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة (65) مكرر) وهي جرائم المخدرات الجريمة المنظمة، جرائم تبييض الأموال والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ويمكن تصور عملية التسرب في الجرائم الالكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات أو نوادي الهاكر،

[1]– خداوي مختار،إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الطاهر مولاي سعيدة.2015–2016 ،ص38

مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد استدراجهم والكشف عنهم وعن أعمالهم الإجرامية[1].

الفرع الثاني: شروط التسرب

صدور إذن من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية – أن يكون الإذن مكتوبا ومسببا يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة يحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 04 أشهر، غير أنه يمكن أن تجدد، حيث تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على : " ... يجوز الوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن.... حسب الحالة بمباشرة عملية التسرب[2].

أولا الشروط الشكلية:

نظرا لما تتطلبه عملية التسرب من سرية وحيطة وحذر نتيجة خطورة العملية على حياة المتسرب، ولحسن سير العملية استوجب شروطاً شكلية التي يمكن إجمالها في:

أ- **تحرير تقرير من طرف ضباط الشرطة القضائية** :يقوم ضباط الشرطة القضائية قبل مباشرة عملية التسرب بكتابة تقرير إلى وكيل الجمهورية، وهذا كمبدأ عام على أعمال الشرطة القضائية.

كما نصت م 65 مكر 13 من نفس القانون صراحة أن ضباط الشرطة القضائية المكلف بتنسيق عملية التسرب هو المسؤول عن تحرير التقرير الذي يتضمن العناصر التالية:

1 -طبيعة الجريمة : حددها المشرع الجزائري في نص م 65 مكرر 05 من ق.ا.ج والمتمثلة في جرائم المخدرات الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبيض الأموال، جرائم

[1]- خداوي مختار،المرجع السابق،ص39

[2]- مسعود شهيرة،المرجع نفسه،ص56

الإرهاب، الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد[1].

2 –السبب وراء العملية: على ضابط الشرطة القضائية أن يذكر مبررات ودواعي اللجوء إلى هذا الإجراء من أجل إقناع وكيل الجمهورية بمنح الإذن و هذا ما يدعو الضابط الشرطة الفضائية إعلى تأسيس طلبه على عدد من العناصر التي تبرر هذا الإجراء.

3–هوية ضابط الشرطة القضائية: يقوم ضابط الشرطة القضائية الذي يحرر التقرير بكتابة إسمه ولقبه وجميع المعلومات المتعلقة بهويته ويذكر صفته والمصلحة التابع لها.

4 –تحديد عناصر الجريمة: ذكر جميع المعلومات المتعلقة بالجريمة والعناصر المكونة لها وذلك بتحديد هوية الأشخاص المشتبه فيهم وذكر وسائل المستعملة في الجريمة[2].

ب– الحصول على الإذن: يشترط في إذن التسرب توافر عدة عناصر وهي:

1 –أن يكون الإذن مسببا صادر من وكيل الجمهورية أو قاضي التحقيق متضمنا للأسباب الداعية لإتخاذ مبنية على تحريات جدية لإجراء عملية التسرب.

2 –أن يكون الإذن مكتوبا لأن التدوين خير وسيلة الإثبات بحيث يدون وكيل الجمهورية جميع المعلومات ويتم صياغتها في ورقة رسمية وتخلف الكتابة في الإذن يعرض العملية للبطلان

3 –أن يذكر الإذن نوع الجريمة التي تبرر اللجوء إلى هذا الأسلوب.

4 –يحدد في الإذن هوية ضابط الشرطة القضائية المنسق للعملية بذكر الإسم واللقب والصفة والرتبة والمصلحة تابعة لها.

[1]– عدلي دحمان ،سعد الدين ثامر البشير ،التحقيق الجنائي في الجرائم الإلكترونية،مذكرة لنيل شهادة الماستر،تخصص قانون جنائي و علوم جنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة زيان عاشور الجلفة،2020–2021،ص62

[2]– عدلي دحمان ،سعد الدين ثامر البشير ،المرجع السابق،ص63

5- تحديد المدة الزمنية فحسب م 65 مكرر 15 أن عملية التسرب يجب أن لا تتجاوز 04 أشهر قابلة للتجديد حسب مقتضيات التحقيق والتحري ويتم تمديد عملية بنفس الشروط السالفة الذكر المتعلقة بالإذن إلا أنه يمكن لوكيل الجمهورية أو قاضي تحقيق مصدر الإذن أن يأمر بإيقاف العملية في أي وقت حتى قبل إنقضاء المدة المحددة مع مراعاة الإستثناء الذي أوردته المادة 65 مكرر 17 الذي يقضي بإمكانية تمديد الإذن بالتسرب لمدة 04 أشهر أخرى إذا لم يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه ولصحة الإجراءات تودع نسخة من الإذن في ملف الإجراءات بعد إنتهاء من عملية التسرب.

ج- **الجهات مخولة بإصدار الإذن:** إن الأشخاص المخول لهم بمنح الإذن بمباشرة عملية التسرب هم وكيل الجمهورية وقاضي التحقيق بعد إخطار وكيل الجمهورية[1].

1 -وكيل الجمهورية: وهو المسؤول الأول عن منح رخصة الإذن بصفته الممثل الأول للنيابة العامة وهذا بعد أن يقدم ضابط الشرطة القضائية طلب بمنح الإذن مرفوق بتقرير عن العملية.

2-قاضي التحقيق: يستطيع قاضي التحقيق أن يمنح رخصة الإذن بمباشرة العملية بعد إخطار النيابة العامة (وكيل الجمهورية).

ثانيا: الشروط الموضوعية العملية التسرب

شروط تتمثل في:

أ- **ضرورة اللجوء لعملية التسرب:** نظراً لخطورة عملية التسرب لا يتم اللجوء إلى هذا الإجراء إلا إذا اقتضت ضرورات التحقيق والتحري ذلك أي تحتم الأمر اللجوء إليه وذلك من خلال باعتباره الإجراء الوحيد أو الأنسب الذي بواسطته يمكن إظهار الحقيقة بعد أن أثبتت وسائل البحث العادية

[1]- نايري عائشة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون إداري،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة احمد دراية أدرار،2016-2017،ص54

عدم نجاعتها، أو أن الإستمرار فيها ونجاحها في تحقيق الغرض منها قد أضحى بعيد الإحتمال .

"

هذا ما أكدته م 65 مكرر 11 من ق.ا.ج وهدف من هذا الإجراء الوصول إلى الحقيقة والأدلة القانونية والموضوعية وعليه فإن توفر حالة الضرورة تعد من الشروط الأساسية للجوء لهذا الإجراء[1].

ب- السرية في عملية التسرب: يعتبر عامل السرية شرط أساسي لسير عملية التسرب ونجاحها، فيجب على الضابط المسؤول عن العملية أن يحيطها بالسرية التامة، حيث نصت م 65 مكرر 16 من ق.ا.ج 3 على جزاءات عقابية مشددة في حالة الكشف عن الهوية الحقيقية للشخص المتسرب، كذلك م 65 مكرر 18 من ق.ا.ج التي تنص على أنه:" يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهداً عن العملية.

وتتمثل صور السرية في:

1 -استعمال هوية مستعارة: فيقوم ضابط المسؤول عن العملية تحت علم وكيل الجمهورية بمنح عون المتسرب هوية مستعارة لأن هذا الأمر يساعد على اكتشاف الحقائق التي يتعذر إكتشافها في حالة إفصاح المندمج أو المتسرب عن صفته.

فوجب على الضابط المتسلل أن يعمل تحت هوية مزيفة و وهمية وذلك لإتمام مهمتهم دون الإصطدام بعقبات تحول دون إتمامها.

[1]- شناوي ليزا،مزاري ويزة،أساليب البحث و التحري عن الجرائم المستحدثة في قانون الإجراءات الجزائية،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون عام داخلي ،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة مولود معمري تيزي وزو،2015-2016،ص 47

2 –الجهات المتخصصة عملية التسرب: من خلال المادة 65 مكر 12 من ق.ا.ج فإن المختص بمباشرة عملية التسرب هم الضابط الشرطة القضائية وأعوان الشرطة القضائية المكلفون بتنسيق العملية وبصفتهم المسؤولون عن العملية يقوم بالتحضير والتنظيم المحكم والدقيق لهذه العملية[1].

الفرع الثالث : مجالات عملية التسرب

أجاز المشرع اللجوء إلى هذا الأسلوب ومباشرته في إطار الجرائم السبعة والمحددة على سبيل الحصر وهي الجرائم المستحدثة والخطيرة المنصوص عليها في نص المادة 65 مكرر 15 من قانون الإجراءات الجزائية المعدل والمتمم وهي:

أولا : الجريمة المنظمة العابرة للحدود الوطنية.

إن الجريمة المنظمة تكون وليدة تخطيط وليست مشكلة تتشكل عشوائيا، بحيث يظهر من السلوك الإحرامي انه بلغ درجة عالية من التعقيد والتشعب لا يمكن تفكيك الجماعة بالوسائل التقليدية ، وإنما يتأتى ذلك باستعمال وسائل حديثة ، التسرب ، تسجيل الأصوات ذلك غالبا ما تملك الجماعة المنظمة إمكانيات مادية " وسائل متنوعة – مستودعات للتخزين " وتستعمل وسائل عدة هواتف نقالة – تامين الطريق " لتمويه رجال الضبطية القضائية من جهة ولتنفيذ مبتغاها من جهة أخرى[2].

ثانيا : الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويقصد بتدمير نظم المعلومات، إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة الحاسب الآلي أنا كان شكلها أو استيلاء على نقود

[1]– شناوي ليزا،مزاري،المرجع السابق،ص50

[2]– شناوي ليزا،مزاري،المرجع السابق،ص51

أو إطلاع على المعلومات ولكن يعرف بساطة أنه إحداث ضرر بالنظام المعلوماتي وإضافته عن أداء وظيفته[1].

ثالثا : جرائم الإرهاب

عالج المشرع الجزائري الظاهرة الإرهابية في وقت متقدم عن باقي الدول التي اختلفت في تحديد وصف مقبول لهذه الجريمة وعالجتها مجموعة من النصوص التي تطورت تبعا للحالة الأمنية الداخلية وما أفرزته الاتفاقيات الدولية اللاحقة.

إن الجرائم الإرهابية نص عليها قانون العقوبات ضمن القسم الرابع تحت عنوان (الجرائم الموصوفة بأفعال إرهابية تخريبية .من الفصل الأول الباب الأول من الكتاب الثالث الجزء الثاني وذلك من المادة 87 مكرر إلى 87 مكرر 09 والتي جاءت ضمن الأمر 95/11 المؤرخ في 25/02/1995 حيث صنفها من بين الأفعال التي عدت أعمالا إرهابية كل فعل يستهدف أمن الدول الوحدة الوطنية، السلامة الترابية استقرار المؤسسات وهذا ببث الرعب خلق انعدام الأمن من خلال الاعتداءات المعنوية والجسدية على الأشخاص الاعتداء على رموز الدولة، حيازة أسلحة أو ذخيرة أو مواد متفجرة أو الاستيلاء عليها والمتاجرة فيها دون رخصة من السلطات المختصة[2].

رابعا : الجرائم المتعلقة بالصرف

جاءت هذه الجرائم ضمن الأمر رقم 96/22 المؤرخ في 09/07/1996 المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال المعدل والمتمم للأمر رقم 03/01 المؤرخ في 19/02/2003 والقانون رقم 03/08 المؤرخ في 14/06/2003 تناوها المشرع في 16 مادة وعاقب على ارتكابها وعلى المحاولة في ارتكابها حيث عرفها على أنها تعتبر مخالفة

[1]– خلوة ايهاب ،مداخلة بعنوان أهمية أساليب التحري الخاصة في مكافحة الجريمة المنظمة، بمناسبة اجتماع الضبطية القضائية بقسنطينة،يوم 30/09/2010،ص2

[2]– عبد الفتاح يومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط 01، القاهرة ، 2009، ص 478

أو محاولة مخالفة للتشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال بأية وسيلة كانت (التصريح الكاذب، عدم مراعاة الإجراءات المنصوص عليها أو الشكليات المطلوبة وعدم الحصول على تراخيص مشترطة أو عدم احترام الشروط المقترنة بها، كذلك بيع وشراء واسترداد أو تصدير أو حيازة سبائك ذهبية، قطع ذهبية، أحجار أو معادن نفيسة دون مراعاة التشريع والتنظيم المعمول بها...إلخ

خامسا : جرائم المخدرات

تعتبر جرائم المخدرات من أبرز أنواع الجرائم المنظمة وهي الأكثر انتشارا على المستوى الوطني والعالمي فقد أصبح تجار المخدرات يملكون ويسيطرون على كل شيء وفي شتى المجالات ويملكون أجهزة تنصت متطورة وفي غاية الدقة، والمكافحة هذه الجريمة أورد المشرع صور هذه الجريمة ضمن قانون 18/04 المؤرخ في 25/12/2004 تحت عنوان الوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروع لها[1].

سادسا : جرائم تبيض الأموال

تعد عملية تبيض الأموال ظاهرة قديمة النشأة منذ حاجة الإنسان إلى إخفاء مصادر الكتب التي حصل من خلالها على أموال غير مشروعة، غير أنها قد تزايدت بصورة كبيرة عندما اتسع نشاط الجريمة المنظمة والذي صاحبه في الوقت ذاته استخدام أساليب أكثر كفاءة في عمليات الإحفاء، حيث تحتاج عملية تبيض الأموال في العصر الحديث إلى مهارات خاصة واستخدام أساليب عدة للنجاح في الحصول على مستند رسمي الملكية الأموال بصورة قانونية، حيث تهدف العملية إلى إخفاء المصدر الأساسي للأموال والبحث عن تغطية قانونية لأصل أو ملكية الأموال تم الحصول عليها بصورة غير قانونية، حيث يبدو في النهاية كأنها أموال تم الحصول عليها من مصادر قانونية.

[1]– زغينة وليد، أساليب التحري الحديثة وأطر تطبيقها في الجزائر، مذكرة نهاية الدراسة النبيل إجازة المدرسة العليا للقضاة الدفعة 21 .2013.ص45

و تمر عملية تبييض الأموال بمراحل أساسية وهي:

أ- **التوظيف** : تعد عمليات التوظيف الحلقة الأولى في سلسلة عمليات غسيل الأموال وتمثل جوهر عمليات التوظيف في اجتياز المكان الذي تتم فيه عملية الغسيل إما من خلال إدخال النقود في نظام مصرفي أو في تجارة قانونية أو غير ذلك من الأساليب.

ب- الخلط : ويقصد بالخلط فصل النقود عن مصدرها غير القانوني وتمريرها غير عدة معاملات مالية معقدة تجعل تتبع اثر تلك الأموال مسألة مضيعة للوقت ، كتحويلها من وإلى عدة حسابات .

ج- الدمج : أي دمج هذه الأموال مع أموال أخرى ذات المصادر القانونية وبالتالي إيجاد مبرر معقول التفسير ملكيتها ويمكن أن يطلق عليها اسم عملية التحفيف للأموال القذرة ، وعملية الدمج للأموال تتم من خلال جعل هذه الأموال تبدو كأنها أموال تم اكتسابها بصورة قانونية[1].

سابعا : جرائم الفساد

وهي كل فعل من الأفعال الواردة في قانون الوقاية من الفساد رقم 06/01 والتي تشمل كل أفعال الرشوة ، اختلاس المال العام والخاص، احد فوائد من الصفقات العمومية ، تلقى الهدايا العجز عن تبرير الزيادة غير المبررة في الأموال ، إبرام صفقات بصورة مخالفة للقانون، عدم التصريح بالممتلكات أو عدم صحة التصريح .. وأوردها المشرع الجزائري ضمن قانون 06/01 المؤرخ في 20/02/2006 والمتعلق بالوقاية من الفساد ومكافحته، ووصفها بالجرائم الخطيرة تذكر منها : رشوة الموظفين العموميين، رشوة الموظفين العموميين الأجانب وموظفي المنظمات الدولية العمومية الرشوة في القطاع الخاص، الرشوة في قطاع الصفقات العمومية، إساءة استغلال

[1]- خداوي مختار ،المرجع السابق،ص48

الوظيفة عدم التصريح أو التصريح الكاذب للممتلكات، إخفاء وتبيض العائدات الإجرامية والمتحصل عليها من جرائم الفساد[1].

[1]– خداوي مختار ،المرجع نفسه،ص49

خلاصة الفصل الثاني:

إن عالم تقنية المعلومات الحديثة عالم واسع لا يحده حد، وان الوسائل المستعملة في ارتكاب الجريمة الالكترونية متشعبة ومتنوعة وخاصة في اتباع الجرائم المعلوماتية التي تقوم بها الجها المتخصصة في الكشف عن الجرائم ولابد من تطوير الكشف عن الجرائم والمتابعة من قبل الجهات المتخصصة.

وهذا الأمر يتطلب وقفة من قبل المشرع والقضاء لاتخاذ مجموعة من الخطوات الاصلاحية لمواجهة هذا النوع من الجرائم.

الخاتمة

تستنتج من خلال هذه الدراسة أن الجرائم الالكترونية تعتبر من أخطر الجرائم التي نتجت عن الثورة المعلوماتية وهذا راجع الى تطورها المستمر ومساسها بمختلف المجالات مما جعلها عقبة أمام جميع جوانب الحياة اليومية، ولكونها تتميز بخصائص مختلفة كثيرا عن الجريمة التقليدية في كونها جريمة عابرة للحدود الدولية و الصعوبة في إثباتها وقلة الإبلاغ عليها، ومن أجل مواكبة التشريعات الرائدة في المجال المعلوماتي ، اقدم المشرع الجزائري على تعديل قانون الإجراءات الجزائية لسنة 2006 وكذا استحداث القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

كما عمل المشرع الجزائري على إتباع طرق حديثة تعمل على تسهيل عملية التحري عن الجرائم الالكترونية نظرا للخصوصية التي تتميز بها.

والجزائر ليست بمعزل عن بقية الدول، حيث عملت على تطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال اصدار تشريعات تواكب التطور الحاصل في المجال المعلوماتي، وقد اتبع المشرع الجزائري سياسة مزدوجة للتصدي لظاهرة الاجرام المعلوماتي فمن جهة قام بتعديل الجوانب الموضوعية، بالاضافة الى النصوص الخاصة التي تبناها المشرع في تعديله الأخير للقانون 04/15 المؤرخ في 10/11/2004 المعدل والمتمم للامر 66/155 المؤرخ في 8/6/1966 المتضمن قانون العقوبات، ويشمل المواد من 394 الى 394 مكرر 7 ومن ابرز تلك التعديلات كذلك ما أورده في الأمر 03/05 الصادر في 19/7/2003 والمتعلق بحقوق المؤلف والحقوق المجاورة والتي أدرجت برنامج الحاسوب ضمن المؤلفات مضمونة الحماية، وكذلك تعديل الجوانب الاجرائية، حيث قام بتعديل قانون الاجراءات الجزائية عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقام من جهة ثانية باستحداث قوانين اخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم المعلوماتية، القانون رقم 09/04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

فتعتبر بذلك مكافحة فعالة نظرا لما تمتاز به من شمولية، بحيث جاءت لتشمل اغلب الجرائم التي قد تمس نظام المعالجة الآلية للمعطيات بصفة عامة، وكذا تضمنت اغلب الجرائم التي قد تمس البيانات والمعطيات المكونة لهذا النظام، غير انها تحتاج الى نصوص اجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية من خصوصية تختلف عن باقي الجرائم.

وبذلك يكون المشرع قد تدارك النقص الذي كان موجود في التشريع العقابي الجزائري، فهو يعد قفزة في المجال التشريعي مواكبا للتشريعات المقارنة من خلال تجريمه للافعال التي يرتكبها الشخص الطبيعي، وتحميل الشخص المعنوي المسؤولية الجزائية وتوسيع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريمه حتى الاعمال التحضيرية في إطار الاتفاق الجنائي.

و على هذا الأساس استخلاصنا من خلال هذه الدراسة إلى صياغة مجموعة من النتائج و المقترحات.

أولا – النتائج:

–إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكون بجرائم تقليدية.

–إنما أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، أنها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية فهذه الجرائم تستهدف المساس بالمعلومات الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

-يتمتع الدليل الإلكتروني بمجموعة من الخصائص التي جعلته يتميز عن باقي الأدلة الجزائية، خاصة الخاصية الفنية والتقنية فيه، وأيضا مع إمكانية إسترجاعه بعد إتلافه واعتبار عملية محاولة إتلافه دليل ضد مرتكبها.

-قصور من طرف المشرع الجزائري الذي لم ينص على الدليل الإلكتروني في قوانينه ولم يضع له تعريفا جامعا شاملا.

- إن محل الدليل الإلكتروني ونطاق العمل به هو الجريمة الإلكترونية غير أنه يصلح كذلك لإثبات الجرائم التقليدية، التي تم إرتكابها عبر تقنية الكترونية.

-الجرائم المعلوماتية من بين الجرائم المستحدثة و العابرة للحدود.

-هي من الجرائم المختلفة من حيث خصائصها عن الجريمة التقليدية، كما أنها صعبة الإثبات والاكتشاف كما يقل الإبلاغ فيها.

-الجرائم المعلوماتية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق ويتصف المجرم المعلوماتي فيها بالذكاء والسرعة كذلك يكون متميزا بالدقة والتخصص في مسائل تكنولوجيا المعلومات.

ثانيا : التوصيات

-تكثيف التعاون والتنسيق الدولي بين الدول من أجل تطوير وتوحيد التشريعات الموضوعية والإجرائية التي تعنى بمكافحة الجرائم الإلكترونية عن طريق إبرام اتفاقيات دولية وإقليمية ثنائية ومتعددة الأطراف في هذا المجال، أو الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص كالاتفاقيات الأوربية حول الجريمة الإلكترونية المبرمة في بودابيست عام 2001 مع مراعاة المصلحة الوطنية ومبدأ السيادة.

-نشر الوعي في أوساط المجتمع وتحسيسه بالمخاطر الاقتصادية والاجتماعية والنفسية وغيرها الناجمة عن الاستخدامات غير المشروعة وغير الآمنة للإنترنت وما يترتب عنها من انعكاسات سلبية على حياة الفرد والمجتمع.

-إدخال برامج تعليمية في المنظومة التكوينية خاصة منها تخصيص مادة " أخلاقيات استخدام الإنترنت " للتحسيس بمخاطر الاستعمال السيء لمواقع التواصل الاجتماعي والتعريف بالجرائم المعلوماتية.

-لا يكفي مواكبة المشرع العقابي الجزائري لنصوص التشريعات المقارنة بدون تجسيدها من الناحية التطبيقية والاستعانة بمختصين وخبراء قاديرين على تشخيص الجريمة، والعمل على تكوين فرق من الضبطية القضائية لكي تختص بهذا النوع من الجرائم وتكوين قضاة مختصين في هذا النوع من الجرائم، مع توفير كافة الوسائل المادية والتقنية اللازمة لأداء عملها ومهامها على أحسن صورة.

- ضرورة تشديد الوصف الجنائي والعقوبات المقررة للانماط الاجرامية للجريمة المعلوماتية بغية تحقيق الردع والقضاء على الاجرام المعلوماتي.

-من الضروري إلى جهات التحقيق أن يتوفر لديهم كوادر بشريه تمكنها من سلطة البحث والتحري في الجرائم الإلكترونية بواسطة الوسائل الحديثة.

- العمل على تدريب المحققين في معاهد مختصة لاكتسابهم الخبرة في مجال البحث والتحري وإعطاؤهم دورات في هذا المجال.

قائمة المراجع و المصادر

النصوص الرسمية

أ – القوانين

– قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06/22 المؤرخ في 20/12/2006 بموجب الأمر رقم 15/02 ج ج جدش، العدد 40

–ب –النصوص التنظيمية

– المرسوم الرئاسي رقم 15/261 المؤرخ في 8 أكتوبر 2015 المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، جره العدد 53 الصادرة في 8 أكتوبر 2015

المؤلفات

أ–الكتب

– أبي الفضل جمال الدين ابن منظور، لسان العرب ، المجلد الثاني، دار صادر ، بيروت ، بدون سنة نشر

– أحمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الأول، ديوان المطبوعات الجامعية .1998

– أحمد غاي ، ضمانات المشتبه فيه أثناء التحريات الأولية ، ط 1 ، دار هومة ، الجزائر ، 2005

– أحمد فتحي سرور ،الوسيط في قانون الإجراءات الجزائية ، دار النهضة العربية، القاهرة، ط3، 1981

– أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الطبعة السابعة، دار النهضة العربية، 1993

– حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990

– حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2014

– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية ما، دار الفكر الجامعي، الاسكندرية، مصر. 2009

– خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة الجزائر، 2010

– طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009

– عادل عبد العالي خراشي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الإسكندرية

– عبد الفتاح يومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط 01، القاهرة ، 2009

– عبير مجلي ابو دية،الجرائم الإلكترونية(دراسة نظرية)،الملتقى الخامس للرابطة العربية للبحث العلمي و علوم العربي ،جامعة منوبة،تونس ،2018

– عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الطلبي الحقوقية.2007

– علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنات، عالم الكتب الحديثة الأردن 2004

– عمار فوزي ، مجلة علوم الانسانية ، جامعة منتوري – قسنطينة ، العدد 33 ، جوان 2010

- محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004

- محمد أمين الخرشة مشروعية الصوت والصورة في الإثبات الجنائي، ط1، دار الثقافة، الأردن، 2011

- مدير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005

- مصطفى محمود محمد، الإثبات في المواد الجنائية في القانون المقارن ط. القاهرة مطبعة جامعة القاهرة 1987

- نهلا عبد القادر المومني ،الجرائم المعلوماتية ،دار الثقافة للنشر والتوزيع الأردن ،طبعة 2010

- هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة، الطبعة الأولى 1994

- ياسر الأمير فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، جامعة القاهرة، ط1، 2009

-أسامة أحمد المناعة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014

ب- الأطروحات والرسائل والمذكرات

1-أطروحات:

- زغينة وليد، أساليب التحري الحديثة وأطر تطبيقها في الجزائر، مذكرة نهاية الدراسة النبيل إجازة المدرسة العليا للقضاة الدفعة 21 .2013.

– حولي فرح الدين، أساليب البحث والتحري طبقاً للقانون رقم 06–22 المعدل والمتم لقانون الإجراءات الجزائية مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء .2009

– عبد القادر نشادي ،الجرائم المعلوماتية في وسائل الاتصال الحديثة دراسة وصفية تحليلية لمجموعة من الجرائم المرتكبة عبر الوسائط الاتصالية الحديثة في الجزائر، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والإتصال، كلية علوم الإعلام والإتصال، قسم الإتصال، جامعة الجزائر 3

– مولاي ملياني دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان الجزائر ، 2017/2018

2–رسائل ماجستير:

– ركاب أمينة، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان 2015

– سعيداني نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،مذكرة نهايةالدراسة للحصول على شهادة الماجستير،تخصص قانون جنائي،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الحاج لخضر باتنة،2012–2013

– طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1 .2011–2012

– عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقاربة رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط 2014

– معتوق عبد اللطيف، الإطار القانوني المكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج الخضرة باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق، 2011–2012

3–مذكرات الماستر:

– الكيال فاطمة ،ظوابط البحث و التحري على الجرائم،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم القانون العام،كلية الحقوق و العلوم السياسية،جامعة عبد الحميد بن باديس،2020–2021

– بوديسة بجاد عبد الرؤوف،آليات التحري عن الجريمة الإلكترونية في القانون الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر ،تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة محمد البشير الإبراهيمي برج بوعريريج،2020–2021

– خداوي مختار ،إجراءات البحث و التحري الخاصة في التشريع الجنائي الجزائري ،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص القانون الجنائي و العلوم الجنائية ،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة الطاهر مولاي سعيدة،2015–2016

– خداوي مختار،إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة الطاهر مولاي سعيدة.2015–2016

– شناوي ليزا،مزاري ويزة،أساليب البحث و التحري عن الجرائم المستحدثة في قانون الإجراءات الجزائية،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون عام داخلي ،قسم الحقوق،كلية الحقوق و العلوم السياسية ،جامعة مولود معمري تيزي وزو،2015–2016

– شناوي ليزا،مزاري ويزة،أساليب البحث والتحري عن الجرائم المستحدثة في قانون الإجراءات الجزائية،مذكرة نهايةالدراسة للحصول على شهادة ماستر ،تخصص قانون عام داخلي،قسم الحقوق ،كلية الحقوق و العلوم السياسية،جامعة مولود معمري تيزي وزو،2015–2016

– عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر كلية الحقوق والعلوم السايسية، جامعة الطاهر مولاي، سعيدة، سنة 2015/2016

– عدلي دحمان ،سعد الدين ثامر البشير ،التحقيق الجنائي في الجرائم الإلكترونية،مذكرة لنيل شهادة الماستر،تخصص قانون جنائي و علوم جنائية،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة زيان عاشور الجلفة،2020–2021

– عمار حشمان،الجريمة المعلوماتية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص إدارة التحقيقات الاقتصادية و المالية،قسم علوم التسيير ،كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير،جامعة قاصدي مرباح ،ورقلة ،2018–2019

– غربي جميلة ،آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي و علوم جنائية،قسم القانون العام ،كلية الحقوق و العلوم السياسية،جامعة أكلي محند أولحاج البويرة،2020–2021

– لبيض عادل ،نزلي بشرى،إثبات الجريمة الإلكترونية، مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإداري.قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة قاصدي مرباح،ورقلة،2017–2018

– مباركية رابح،إجراءات التحري و التحقيق في الجريمة الإلكترونية،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإعلام الآلي و الأنترنت،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة محمد البشير الإبراهيمي برج بوعريريج،2021–2022

– مسعود شهيرة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون جنائي،قسم القانون العام،كلية الحقوق و العلوم السياسية،جامعة عبد الحميد بن باديس مستغانم،2020-2021

– نايري عائشة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون إداري،قسم الحقوق،كلية الحقوق و العلوم السياسية،جامعة احمد دراية أدرار،2016-2017

– نايري عائشة ،الجريمة الإلكترونية في التشريع الجزائري،مذكرة نهايةالدراسة للحصول على شهادة ماستر،تخصص قانون الإداري،قسم الحقوق،كلية الحقوق و العلوم السياسية،احمد دراية ،2016-2017

ج-المحاضرات

– مشري سلمى ،مفهوم الجريمة الإلكترونية،محاضرات في مقياس الجريمة الإلكترونية،جامعة تندوف،2016-2017

د-بحوث القانونية

-مداوي سعيد مداوي القحطاني،الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها، بحث لمسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015،وزراة الداخلية ،دولة قطر

ه-الملتقيات و المقالات

– خلوة ايهاب ،مداخلة بعنوان أهمية أساليب التحري الخاصة في مكافحة الجريمة المنظمة، بمناسبة اجتماع الضبطية القضائية بقسنطينة،يوم 30/09/2010

– رشيد شميشم، الحق في الصورة ، مجلة العلوم الانسانية والاجتماعية، جامعة المدية ، العدد 03 ، 2008

– عبد الجبار الحنيص، الإستخدام غير المشروع النظام الحاسوب في وجهة نظر القانون الجنائي، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الأول: 2001

– عبد الحكيم ،مولاي ابراهيم ،الجريمة الإلكترونية ،مجلة الحقوق و العلوم الإنسانية ،العدد 23 ،جامعة زيان عاشور بالجلفة–الجزائر ،جوان2015

– عز الدين عثماني .إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية مخبر المؤسسات الدستورية والنظم السياسية جامعة تبسة، العدد 04، جائفي 2018

– علي أحمد إبراهيم ،تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية،مجلة القانونية ،العدد3،الأردن

– فلاح عبد القادر،أيت عبد المالك نادية ،التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري،العدد2،المجلد 2019.4.خميس مليانة

– مليكة عطوي، المحلة السابقة الذكر، ص 09، نقلا عن الطاهر روابنية المسائلة، مقال العدد 01، 1991

و–المواقع الإلكترونية

– حافظ بن زلاط مقال منشور على الأنترنت بعنوان التصنت الهاتفي في ظل قانون الإجراءات الجزائية، 2015 .على الموقع الإلكتروني:www.droitetentreprise.org

– فلاح عبد القادر ،حجز و حفظ في الجريمة الإلكترونية،على الموقع الإلكتروني:

- مراد عبسي، الذكاء الاصطناعي العسكري وشرارة الحرب العالمية الثالثة،على الموقع الإلكتروني :https://almustaqbal.com/article/1064951/

https://asjp.cerist.dz/en/article/169811

- لخضر دولي ،نفيسة ناصري،دور الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية،على الموقع الإلكتروني https://asjp.cerist.dz/en/article/87915 :

الفهرس والمحتويات

الفهرس	الصفحة
الإهداء	
الشكر والتقدير	
قائمة المختصرات	
مقدمة	1
الفصل الأول: الإطار النظري للجريمة الإلكترونية	6
المبحث الأول : ماهية الجريمة الإلكترونية	7
المطلب الأول: مفهوم الجريمة الإلكترونية	7
الفرع الأول: تعريف الجريمة الإلكترونية	8
الفرع الثاني: أنواع (صور) الجريمة الإلكترونية	11
المطلب الثاني: الطبيعة القانونية للجريمة الإلكترونية	16
الفرع الأول : الخصائص الجريمة الإلكترونية	16
الفرع الثاني : أركان الجريمة الإلكترونية	18
المبحث الثاني: أساليب الكشف عن الجريمة الإلكترونية	22
المطلب الأول : مفهوم التحري	22
الفرع الأول : تعريف التحري	22
الفرع الثاني : أهمية التحري	25
الفرع الثالث : الطبيعة القانونية الإجراءات التحري	27
المطلب الثاني : ضوابط التحري في الجريمة الإلكترونية	28
الفرع الأول : الأجهزة المكفلة بالتحري عن الجريمة الإلكترونية	29
الفرع الثاني : الوسائل المستخدمة في التحري وجمع الأدلة في الجريمة الإلكترونية.	33

الفرع الثالث : الذكاء الاصطناعي و دوره في جريمة الإلكترونية	35
خلاصة الفصل الأول	40
الفصل الثاني: الإطار القانوني للتحري عن الجريمة الإلكترونية	42
المبحث الأول : الأساليب التقليدية للبحث والتحري عن الجريمة الإلكترونية	43
المطلب الأول: التفتيش	43
الفرع الأول: تعريف التفتيش	43
الفرع الثاني: إجراءات التفتيش النظم الإلكترونية وضبطها	46
المطلب الثاني: الحجز	48
الفرع الأول: تعريف الحجز	49
الفرع الثاني: إجراءات الحجز المعطيات المعلوماتية	50
المبحث الثاني: الأساليب المستحدثة للبحث والتحري عن الجريمة الإلكترونية	52
المطلب الأول: المراسلات تسجيل الأصوات التقاط الصور	52
الفرع الأول: المراسلات	54
الفرع الثاني: تسجيل الأصوات	58
الفرع الثالث : التقاط الصور	60
المطلب الثاني: التسرب	63
الفرع الأول: تعريف التسرب	63
الفرع الثاني: شروط التسرب	65
الفرع الثالث : مجالات عملية التسرب	69
خلاصة الفصل الثاني:	74

الخاتمة	76
قائمة المراجع	81
الفهرس والمحتويات	91

ملخص مذكرة الماستر

أصبح العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، خاصة بعد اختراع الانترنت، أمام هذا التطور فقد ارتبطت به ما يعرف بالاجرام المعلوماتي وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتجت عنه عدة اضرار لا يمكن حصرها.

لم تكتفي التشريعات المقارنة والتشريع الجزائري بتجريم أعمال الإلكترونية وقوانين العقوبات وقانون الإجراءات والقوانين الخاصة والمتعلقة بها بل أقرت أجهزة خاصة لمتابعة ومكافحة هذه الجريمة كالمخابرات المركزية بالولايات المتحدة الأمريكية و جهاز دائرة البحوث السياسية بإسرائيل و مباحث أمن الدولة في مصر و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال بأحدث الطرق العلمية والمتطورة.

الكلمات المفتاحية

1-التفتيش 2-جريمة الكترونية 3-التحقيق الإلكتروني 4- الدليل الرقمي5 – التسرب.

Abstract of The master thesis:

The world today lives in an era of technological development, or what is known as the information revolution, especially after the invention of the internet. This development has been accompanied by what is known as cybercrime, as a result of the misuse of information technology or computers, which has resulted in countless harms.

Comparative legislation and Algerian legislation have not only criminalized electronic acts, penal codes, procedural laws, and related special laws, but have also established special agencies to monitor and combat this crime, such as the Central Intelligence Agency in the United States, the Political Research Department in Israel, the State Security Investigations in Egypt, and the National Authority for the Prevention of Crimes Related to Information and Communication Technology, using the latest scientific and advanced methods.

Reintegration of detainees :

1 -Inspection 2- Cybercrime 3- Electronic Investigation 4- Digital Evidence 5- Leakage.