وزارة التعليم العالي و البحث العلمي

Min4istry of High Education and Science Research

جامعة محمد البشير الإبراهيمي – برج بوعريريج –

University of Mohamed el Bachir el Ibrahimi - Bba -

كلية الحقوق و العلوم السياسية

Faculty of Law and Political Science

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص : قانون الإعلام الآلي و الأنترنت

الموسومة بـــ :

الإجراءات المستحدثة للتحقيق في الجرائم الإلكترونية

إعداد الطلبة:

- بوعجاجة زينب جيهان
- درابلي دنيا زاد

تحت إشراف:

الأستاذ: خنتاش عبد الحق

لجنة المناقشة

الاسم و اللقب	الرتبة	الصفة
الاستاذ خلفة سمير	أستاذ محاضر - ب-	**رئيسا**
الأستاذ خنتاش عبد الحق	أستاذ محاضر- ب-	**مشرفا و مقررا**
الأستاذ سي حمدي عبد المؤمن	أستاذ محاضر- ب-	**ممتحنا**

السنة الجامعية 2023/2022


بسم الله الرحمن الرحيم

شـــكر و عـــرفان

الحمد لله و الشكر لله الذي وفقنا لإتمام هذا العمل أتوجه بجزيل الشكر الى كل اسرة جامعة محمد البشير الابراهيمي لكلية الحقوق- برج بوعريريج- على ما قدموه لنا، من أساتذة و عمال ، كما نتقدم بجزيل الشكر لأعضاء لجنة المناقشة الموقرة الذين تكرموا بقبول قراءة هذه المذكرة ، و أخص

بالذكر من امتدت يداه في احتضان ما أنجزناه تصحيحا و إشرافا كل الشكر و التقدير للأستاذ

" خنتاش عبد الحق"

إهـــداء

الحمد لله و كفى و الصلاة و السلام على الحبيب المصطفى أما بعد :

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه ثمرة الجهد و التعب لسنين طويلة أهدي تخرجي "لأبي الحبيب " الذي وافته المنية الذي طالما أراد أن يرى هذا اليوم " رحمه الله " ، "لأمي " صاحبة العطاء إلى المرأة العظيمة التي تقف كلماتي عاجزة عن التعبير عنها أطال الله عمرها ، إلى أخي

" نبيل " سندي الوحيد بعد أبي رحمه الله ، إخوتي" ريان" و" بلال" .

إلى من تخطيت العثرات برفقتها، من كانت عونا لي في هذه الرحلة صديقتي و أختي " دنيا زاد "

زينب جيهان

أشكر الله العلي القدير الذي أنعم علي بنعمة العقل و الدين، القائل في كتابه الكريم " وفوق كل ذي علم عليم "

إلى من أدين له بسعادتي ، و كان شمعة تخترق لتضيء طريقي ، إلى من أكن له كل مشاعر التقدير و الاحترام " أبي الموقر " أطال الله عمره، إلى من وضعت الجنة تحت أقدامها، إلى التي أنحني لها بكل إجلال و تقدير إلى التي أرجو أن أكون قد نلت رضاها " أمي ".

إلى سندي و مسندي و أعز ما أملك في هذا الوجود إخوتي " ايمان " ، " ولاء ".

إلى وحيدي و ضلعي الثابت الذي لا يميل أخي " خير الدين " وفقك الله لما تحي و ترضى .

إلى من شاركني ليلي و نهاري إلى أختي التي لم تلدها أمي صديقتي " جيهان " أدامك الله صديقة و أختا .

إلى صغاري حفظهم الله " بهاء الدين " و " بلسم أزهار ".

دنيا زاد

إلى كل من شارك في هذا العمل من قريب أو من بعيد

مـقـدمــة

ظهرت الجريمة مع بداية البشرية وقد حاربها الإنسان منذ الوهلة الأولى التي أحس فيها بأنها خطر يهدد كيانه و استقراره و يهدد حياته ، و تعتبر الجريمة مظهر من مظاهر المجتمع، لأنها نتيجة للسلوكيات الإنسانية في العلاقات المتداخلة لعنصر الخير و الشر المتصارعين على مر السنين .

وعليه نجد أن المجتمع هو صاحب الحق في توقيع العقاب على الأفراد بمجرد ارتكابهم الأفعال المجرّمة بنصوص قانونية تنظمها السلطة التشريعية لكل دولة، فلا يمكن معاقبة الشخص إلا إذا سبق ارتكابه لفعل يجرّمه القانون ، هذا ما جاء في المادة الأولى من قانون العقوبات الجزائري حيث نصّ بأنه : " لا جريمة و لا عقوبة أو تدابير أمن بغير قانون " ، كما أنه لا يمكن تنفيذ العقوبة إلا بعد صدور الحكم لأن المتهم برئ حتى تثبت إدانته هذا ما بيّنته المادة 38 من الدستور .

و قد شهد العقد الأخير من القرن العشرين غزوا تكنولوجيا أدّى إلى بروز عصر جديد أحدث تحولا جذريا في كافة ميادين الحياة ، و سهّل الانفتاح على العالم بلا حدود ، و مكّن من التواصل بين الأشخاص والمؤسسات ربحا للوقت و تسريعا لتبادل و تداول المعلومات على نطاق واسع دون جهد التّنقل ، فأصبح العالم كقرية صغيرة يسهل فيها التعامل و التواصل باستمرار .

مع تسارع الاستخدام الإيجابي للتقنيات الرقمية الحديثة في أغراض ساهمت في تقديم خدمات للأفراد

والمجتمعات ، إلا أن الواقع أظهر إمكانية إساءة استخدام هذا التطور في مجالات غير مشروعة ، مما يؤدي إلى الضرر المباشر أو غير المباشر بالمصالح المادية و المعنوية للأفراد ، و التأثير السلبي على متطلبات حياتهم المعتادة ناهيك عن إمكانية تشكيل خطر على سيادة الدول و كيانات المؤسسات الوطنية و الدولية .

نتيجة لتوسّع العصر الرقمي إلى مختلف المجالات ، لم تبق الجرائم منحصرة في نمطها التقليدي القائم في وسط مادي ملموس، بل أصبحت تستعمل تقنيات جديدة في وسط افتراضي غير ملموس .

ومن هنا ظهر ما يُعرف بالجرائم المعلوماتية، لتشكّل بذلك انتهاكات خطيرة على الحياة الخاصة للأفراد

وتمسّ حرياتهم و آرائهم الخاصة .

ولعلّ أي تشريع في العالم يحاول ضمان مواكبة التطورات السريعة التي تتماشى مع التكنولوجيا الحديثة مع عدم إهمال موضوع حماية حقوق الإنسان و كذا المحافظة على أمن و استقرار الدول .

بسبب الطبيعة الخاصة لهذا النمط الإجرامي المستجد، كان واجبا على الأنظمة الجزائية أن تتدخل للوقاية من حدوث هذه الجرائم و البحث عن سبل للحد من تطورها مستقبلا ، ذلك من خلال التوجه نحو استخدام الوسائل والأساليب المتطورة في مجال التحقيق بتلك الجرائم و ضبط مرتكبيها و جمع الأدلة القائمة حولها .

وقد مرّت هذه الجريمة بتطور تاريخي مصاحبا لتطور التقنية و استخداماتها حيث ظهر هذا النوع من الجرائم في بداية الستينات بأول معالجة لما يسمى بالجريمة الإلكترونية على المقالات و المواد الصحافية ، و قد ثار جدل حول ما إذا مانت هذه الأفعال مجرد سلوكيات غير أخلاقية في بيئة الحوسبة، أم أنها تكتسب الصفة الإجرامية، و بالتالي تعتبر أفعال يعاقب عليها القانون، و مع بداية السّبعينات اكتسبت الصّفة الإجرامية و ذلك بعد إجراء عدة دراسات مسحية و قانونية اهتمت بالجرائم الإلكترونية و عالجت عددا من القضايا الفعلية .

أهمية الموضوع :

تكمن أهمية الموضوع في أن الجريمة الإلكترونية من الجرائم المستحدثة التي توجب الدراسة و التحليل أكثر، و التحقيق فيها يتطلب مهارات فنية و تقنية كما يتطلب خبرة في مجال الحاسب الآلي و الانترنت اللذان اعتبرا وسيلتين أساسيتين لارتكاب الجريمة الإلكترونية، و ما يزيد الموضوع أهمية هو خطورة هذه الجريمة

وانتشارها بسرعة رهيبة و عجز القوانين التقليدية على مواكبة هذه السرعة .

الدراسات السابقة :

ومن الدراسات السابقة التي تناولت موضوع إجراءات التحقيق في الجريمة الإلكترونية :

- كتاب فن التحقيق الجنائي في الجرائم الإلكترونية للدكتور خالد إبراهيم، حيث تناول هذا الموضوع بشكل موسع موضوع الجريمة الإلكترونية و أخص بالذكر الجريمة الإلكترونية الواقعة على الأموال و الأشخاص ، و عالج بعض صور الجريمة الإلكترونية كالقذف ، السب و الشتم عبر الانترنت .

- كتاب مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي للدكتور عبد الفتاح بيومي حجازي ، الطبعة الأولى، سنة 2006، الذي أخص بالذكر المجرم الإلكتروني و خصائصه .

- وأيضا كتاب مبادئ الإجراءات الجنائية لجرائم الكمبيوتر و الانترنت للدكتور عبد الفتاح بيومي حجازي، الطبعة الأولى، و تناول هو الآخر موضوع إجراءات التحقيق في الجريمة الإلكترونية تحليلا وتفصيلا .

صعوبات الدراسة:

واجهنا عدة صعوبات في إعداد الدراسة، ولعل من أهمها ما يلي

- ندرة المراجع المتخصصة بمكافحة الجرائم المعلوماتية الى هذا موضوع على المستوى الوطني وعلى مستوى مكتبات الجامعة .

الإشكالية :

إلى أي حد يمكن القول بأن القواعد الإجرائية التقليدية غير كافية لضبط الجريمة الإلكترونية و هل الإجراءات المستحدثة كافية للتحقيق في هذه الجرائم ؟

وقد اعتمدت على المنهج التحليلي في دراستي هذه، وذلك لتبيان مفهوم كل من الجريمة التقليدية و الجريمة المعلوماتية و التحقيق في كل منهما، مع مناقشة الاجراءات المتخذة للتصدي لهاته الجريمة المستحدثة .

ماهية الجريمة الإلكترونية والإجراءات المستحدث

الفصل الأول

ماهية الجريمة الإلكترونية و الإجراءات المستحدثة .

تعتبر الجريمة ظاهرة قديمة ارتبطت بوجود الإنسان البدائي على الأرض، فلا يمكن تصور وقوع جريمة بغير إنسان، فقد تطورت وازداد انتشارها بتطور الإنسان و اعتماده على التقنيات الحديثة، وقد شهد عصرنا الحالي تطورا كبيرا في كافة مجالات الحياة، بما فيها من أنشطة مختلفة سواء كانت اقتصادية، علمية، تجارية عسكرية، أو اجتماعية...إلخ، وذلك على المستوى الفردي والمؤسسي والمجتمعي والدولي .وعلى الرغم مما تحمله هذه التقنيات الحديثة من تسهيلات وإمكانات هائلة، يسرت على الإنسان الوقت والجهد والمال، فإن البعض قد أساء استخدامها، وهذا ما أدى إلى ظهور نمط جديد من الجرائم، وهي ما تسمي بالجرائم المعلوماتية، والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي. ويستمد هذا النوع المستحدث من الإجرام نشاطه من الإمكانات الهائلة للحاسوب والبرامج، وتطور شبكة الأنترنت، والتطور الثقافي والعلمي في التعامل مع التكنولوجيا الحديثة بمختلف أنواعها.

و هذا النوع من الاجرام يختص فيه لصوص أو مخترقين لغاية كسب أموال أو إلحاق ضرر بأجهزة الكمبيوتر لأسباب اخرى غير الربح ، قد تكون سياسية أو شخصية

المبحث الأول

ماهية الجريمة الإلكترونية.

تعد الجرائم الإلكترونية من الجرائم الحديثة التي ظهرت نتيجة لظهور أنظمة المعلوماتية ، ويعتبر ذلك أمر طبيعي نتيجة لتطور مجالات الحياة بشكل عام، باعتبار أنه كلما تطور المجتمع تكنولوجيا كلما ظهرت جرائم حديثة لم تكن موجودة في السابق، وقد تم ظهور هذه الجريمة لأول مرة في الدول المتقدمة التي اكتسبت التكنولوجيا العالية لمعالجة المعطيات ثم انتشرت إلى باقي الدول الأخرى[1] ، لهذا سنتطرق في هذا المبحث إلى دراسة الجريمة الإلكترونية لتحديد مفهومها و إبراز خصائصها و أركانها في التشريع الجزائري .

[1] بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق، جامعة عبد الحميد بن باديس، مستغانم، 2019.ص 8.

المطلب الأول

مفهوم الجريمة الإلكترونية.

قبل تعريف الجريمة الإلكترونية ،لا بدّ من التطرق إلى بعض المصطلحات المتعلقة بهذه الجريمة أولا، ثم تعريف الجريمة الإلكترونية تعريفا فقهيا و قانونيا، و سنقسم هذا المطلب إلى ثلاثة فروع، حيث نتطرق في الفرع الأول إلى تعريف الجريمة الإلكترونية و الفرع الثاني إلى خصائص الجريمة الإلكترونية ،أما بالنسبة للفرع الثالث فندرس تقسيمات و نتائج الجريمة الإلكترونية.

الفرع الأول

تعريف الجريمة الإلكترونية

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للاختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع حيث تهدف الجرائم الالكترونية عادة لإتلاف معلومات ما أو استخدامها من أجل التسبب بأذى نفسي أو مادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة، أو بيانات و حسابات خاصة بالبنوك او الأشخاص .

1- مصطلحات الجريمة الإلكترونية:

- الحاسب الآلي: هو عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها و توجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، و ذلك بتنفيذ ثلاث عمليات أساسية : استقبال البيانات المدخلة للحصول على حقائق مجردة، معالجة البيانات إلى معلومات و إجراء الحسابات والمقارنات و معالجة المدخلات، و إظهار المعلومات المستخرجة للحصول على نتائج.[1]

- ويمكن تعريفه أيضا: " أنه مجموعة من الأجهزة المترابطة و التي تعمل معا من خلال الأوامر والبيانات لتحقيق حل مسألة معينة ".[2]

- المعلومات: عرفت في فرنسا وفقا للقانون رقم **82-652** الصادر في **26 يوليو 1982** بأنها "صوت وصورة او مستند او معطيات او خطايا أيّا كانت طبيعتها " .[3]

[1] بن نعوم خالد أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، كلية الحقوق ، جامعة عبد الحميد بن باديس ، مستغانم ، 2019. ص09

[2] نفس المرجع ، ص 10

[3] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ماجستير في القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع ، 1924 2008 م ، الطبعة الأولى ، الإصدار الأول 2008 ، ص20.

- وعرفها المشرع الأمريكي في قانون المعاملات التجارية الإلكترونية لسنة **1999** في المادة **2** من الفقرة **10**: "بأنها تشمل البيانات و الكلمات و الصور و الأصوات و الرسائل و برامج الكمبيوتر الموضوعة على الأقراص المرنة و قواعد البيانات **".**[1]

- ومن القوانين التي عرفت المعلومات **القانون الأردني** للمعاملات الإلكترونية رقم **85** لسنة **2001** في **المادة 2"** هي البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات التي أنشئت أو أرسلت أو استلمت أو خزنت بوسائل إلكترونية ". [2]

- المجرم المعلوماتي **:** هو الشخص الذي يتمتع بالمهارة و المعرفة و الذكاء عند ارتكابه الجريمة الإلكترونية، و من الدوافع التي تدفعه لارتكاب هذه الجريمة هي الرغبة في التعلم و قهر النظام المعلوماتي ، كما توجد دوافع مادية تتمثل في تحقيق الربح و كسب المال **.**[3]

أولا: التعريف اللغوي: لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم او التسمية الدقيقة لهذا المصطلح ، حيث يعد مصطلح الجريمة الإلكترونية أوسع كن الجريمة المعلوماتية و هذا ما أكدته **اتفاقية بودابست** أو الاتفاقية المتعلقة بالجريمة الإلكترونية التي صادق عليها المجلس الأوربي في **23نوفمبر2001.**[4]

- ويقصد بالمعلوماتية المعالجة الآلية للمعلومات و هي ترجمة للمصطلح الفرنسي informatique وتعني تكنولوجيا التجميع ، و معالجة و إرسال المعلومات بواسطة الكمبيوتر.

ثانيا :التعريف الاصطلاحي: نجد بعض الفقهاء وضعوا تعريف الجريمة المعلوماتية في مجالين : مجال واسع و مجال ضيق.

- التعريف الواسع: هناك عدة تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرّفوها كالآتي :" كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية".[5]

[1] نهلا عبد القادر مومنيي، مرجع سابق، ص 21.
[2] .نفس المرجع، ص 21
[3] نفس المرجع السابق، ص 24.
[4] بن طالب ليندا، الدليل الإلكتروني و دوره في الإثبات الجنائي ، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وز، 2019 ص 19.
[5] جميل عبد الباقي الصغير، الأنترنت و القانون الجنائي، دار النهضة العربية، القاهرة، 2002. ص 31.

- يعرف الأستاذ **vivante** الجريمة المعلوماتية بأنها :" مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".

➢ التعريف الضيق: تعرف الجريمة المعلوماتية على أنها :"كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكاب الجريمة من ناحية و لملاحقته و التحقيق معه من ناحية أخرى".[1]

- يرى الأستاذ **mass** أن المقصود بالجريمة المعلوماتية هو: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".

ثالثا : التعريف الفقهي :انقسم الفقه إلى عدة آراء منهم من ضيّق مفهوم الجريمة ومنهم من وسّع من مفهومها.

1. الاتجاه الضيق: ومن أنصار هذا الرأي **مارو merwe** الذي عرف الجريمة الإلكترونية على أنها: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي".[2]

2. الاتجاه الواسع: ومن أصحاب هذا الرأي **ميشال michel وكريدو credo** حيث عرف الجريمة الإلكترونية بأنها " سوء استخدام الحاسب أو أنها جريمة تسهّل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرّح به لحاسب المجني عليه أو بياناته ، كما تمتد الجريمة الإلكترونية لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به [3]، و كذلك الاستخدام غير المشروع لبطاقات الائتمان و انتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية و تزييف المكونات المادية و المعنوية للحاسب الآلي بل و سرقة جهاز الحاسب في حد ذاته أو أيّا من مكوناته".

رابعا: التعريف القانوني :تطرقت معظم التشريعات الوطنية لتعريف الجريمة الإلكترونية و فيما يلي ذكر لبعض التعريفات:

1. التعريف الفرنسي :عرف **القانون الفرنسي** رقم **19** لسنة **1988** أنماط الجريمة الإلكترونية و ميّز بين الاعتداء على برامج و معلومات الحاسب الآلي ، و بين الاعتداء على أدواته و آلاته و لم ينص على تجريم سرقة البرامج و المعلومات و اعتبرها مالا معلوماتيا حين حدّد في جريمتي :
   - جريمة التوصل بطريقة التحايل لنظام المعالجة الآلية للبيانات .

[1] جميل عبد الباقي الصغير،مرجع سابق ، ص 32.
[2] بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة ماستر، كلية الحقوق، جامعة المسيلة، 2014. ص 10.
[3] نفس المرجع، ص 10.

- جريمة إتلاف برامج و معلومات الحاسب الآلي الرقمي و بذلك تكون هذه الجرائم متعلقة بمحتوى الأسطوانة الممغنطة أو الشريط الممغنط ، كما أصدر المشرع الجنائي الفرنسي قانون العقوبات الجديد **1992** المعمول به منذ **مارس 1994** الذي جرم فيه صور الاعتداء الناجمة عن المعالجة الآلية للبيانات مما يسمح بانطباقه على الأفعال التي تقع على الأنترنيت كمحل للاعتداء أو بواسطته كوسيلة للاعتداء .[1]

2. التعريف الأمريكي:

- العبث بالحاسب الآلي: حيث يرتكب الشخص جريمة العبث بالحاسب الآلي إذا قام عن علم و بدون إذن من مالك الحاسوب الآلي بما يلي :

يدخل أو يسبب الدخول إلى حاسوب أو أي جزء منه و يتلف و يحطم الحاسوب الآلي ، وقد أصدر المشرع الأمريكي عدة قوانين في مواجهة الجريمة الإلكترونية من بينها قانون آداب اتصالات حيث يجرّم فيه القذف والسب عبر شبكة الأنترنت.[2]

3. التعريف الجزائري: ظهر اختلاف حول تعريف الجريمة الإلكترونية في التشريع الجزائري، هذا ما جعل المشرع الجزائري يتبنى تعريف **المؤتمر العاشر للأمم المتحدة** إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب.[3]

الفرع الثاني
خصائص الجريمة الإلكترونية

اولا : الخصائص: تتميز بعدة خصائص تميزها عن الجريمة التقليدية من أهمها:

- جريمة عابرة للحدود: تتسم عادة بالطابع الدولي، وذلك لتخطيها للحدود الجغرافية و من ثمة اكتسابها طبعة دولية فهي تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم اذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم[4] مثل :التزوير ، إتلاف المستندات الإلكترونية ، و القرصنة و الاحتيال المعلوماتي .

- صعوبة الاثبات : لأنها جرائم تتسم بالغموض و تتصف بالخفاء و لا تترك أي أثر فهي تمحى تماما من السجلات المخزنة في ذاكرة الحاسبات الآلية .[5]

[1] ابتسام بقو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة ماستر، كلية الحقوق، جامعة العربي بن مهيدي، أم البواقي، 2016. ص 14.
[2] نفس المرجع السابق، ص 14
[3] نفس المرجع السابق، ص 15.
[4] أو مدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021.ص 27.
[5] نفس المرجع، ص 27 .

- عدم كفاية أدلة الإدانة في الجرائم الإلكترونية : وذلك لعدم وجود أي أثر كتابي و سهولة إخفاء معالم الجريمة الإلكترونية و صعوبة تتبع مرتكبيها .

ثانيا : خصائص المجرم الإلكتروني :

- الذكاء intelligence: يعتبر الذكاء من أهم صفات مرتكب الجرائم الإلكترونية ، لأن ذلك يتطلب المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي، و القدرة على التعديل و التغيير في البرامج و ارتكاب جرائم السرقة و النصب و غيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكي يتمكن من ارتكاب تلك الجرائم، و لذا دائما ما يقال عن الإجرام الإلكتروني أنه إجرام الأذكياء .[1]

- المهارة و الاحتراف: و تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم الإلكتروني ، فتنفيذ الجريمة الإلكترونية يتطلب قدرا من المهارة يتمتع بها الفاعل و التي يكتسبها عن طريق الخبرة في مجال تكنولوجيا المعلومات.[2]

- المعرفة : وتتمثل في معرفة كافة الظروف التي تحيط بالجريمة المراد ارتكابها أو تنفيذها، و كذا إمكانية نجاحها أو فشلها فالجناة عادة يمهدون لارتكاب جرائم بالتعرف على المحيط الذي تدور فيه.[3]

- المجرم الإلكتروني مجرم غير عنيف : يتسم المجرم الإلكتروني بأنه مجرم غير عنيف ، ذلك أنه ينتمي إلى إجرام الحيلة ، فهو لا يلجأ إلى العنف في ارتكاب جرائمه.

ثالثا: المجني عليه في الجريمة الإلكترونية:

- المعتدي عليه في الجريمة الإلكترونية هو من يكون ضحية غير المشروعة على مكونات الحاسوب، و قد يكون شخصا طبيعيا أو شركة، أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، الاقتصادية أو السياسية ، التي ينبغي أن تستعمل الحاسوب في إدارة أعمالها. [4]

- و حسب تقديرات بعض خبراء الصندوق الدولي للبنوك فإنه من المستحيل ان تحدد على نحو دقيق نطاق الجريمة الإلكترونية التي لا يعلم ضحاياها عنها شيء، إلا عندما تكون النظم المعلوماتية المملوكة لهم هدفا للجريمة الإلكترونية .

- و الجدير بالذكر أن سلبية المجني عليهم، و خوفهم من الإبلاغ حفاظا على سمعتهم التجارية خير دليل على التمادي في ارتكاب مثل هذه الجرائم .

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي 30 شارع سوتير ، الإسكندرية بمصر، 2006. ص 44.

[2] نفس المرجع، ص 45.

[3] نفس المرجع، ص45.

[4] خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت، دار الثقافة، الأردن، ط1 ، 2011، ص 38 .

الـــفــرع الثالث
تقسيمات الجريمة الإلكترونية و نتائجها

أولا : تقسيمات الجريمة الإلكترونية: نظرا لصعوبة حصر أنواع الجريمة الإلكترونية ، و نظرا للتباين في رؤية دور الكمبيوتر و محاولات وصف الأفعال الإجرامية بوسائل ارتكابها، فإنه يصعب وضع تقسيم يشمل كل أنواع الجريمة الإلكترونية .

- الإجرام المعلوماتي على شبكة الإنترنت : هناك العديد من الجرائم التي يكون ارتكابها لهدف ما و يتعلق بالمعلومات و يتمثل هذا الهدف إما بالحصول على المعلومات أو تغييرها و يشتمل هذا النوع على الجرائم التالية :[1]

- الاعتداءات المنطقية: و تشمل جرائم مهاجمة الشبكة بالفيروسات أو البريد الإلكتروني، و تعتبر من أخطر الجرائم التي تهدد الحواسيب و شبكة الإنترنت. و من بينها :
- القناة المخفية : canal caché: و هو نوع خطير من الاعتداءات يقوم على مبدأ تهريب المعلومات عر خرق سياسة الأمن و الحماية المعتمدة و الأنظمة المعلوماتية و هي في ذلك تتطلب ذكاء فائقا من المعتدي.[2]

- الاعتداءات المادية: و من أبرزها:

- الاعتراض المعتمد للبيانات : و يقصد به رصد إشارات الكتر ومغناطيسية في الأنظمة المعلوماتية و تحليلها بهدف استرجاع المعلومات المقروءة منها.
- الاكتساح و التفخيخ: الأول يقصد به إرسال حزمة من المعلومات إلى الشبكة للتوصل إلى تحديد أيّ من هذه المعلومات هي الصحيحة، أما الاعتداء الثاني فهو إدخال وظائف خفية في مرحلة تصميم ، تصنيع ، نقل أو صيانة النظام المعلوماتي. [3]

- الإجرام غير المعلوماتي في شبكة الإنترنت: و يحدث عندما تستخدم الإنترنت كوسيلة لارتكابها و يشمل العديد من الجرائم

- جرائم تستهدف الأشخاص : حيث نجد أن معظم الجرائم التي ترتكب عبر شبكة الانترنت تستهدف إما أشخاص أو جهات بعينها ، و غالبا ما تكون تلك الجرائم مباشرة، ترتكب في صورة تهديد أو تشهير ، أو تكون غير مباشرة في إطار الحصول على بيانات و معلومات خاصة.
- الجرائم المالية : تستهدف غسيل الأموال ، جرائم السرقة و النصب و الاحتيال عبر الانترنت.

[1] خالد عياد الحلبي، مرجع سابق، ص 38
[2] بخي فاطمة الزهراء، نفس المرجع السابق، ص 22 .
[3] نفس المرجع السابق، ص 23 .

- جرائم التزوير : و هي من أخطر طرق الغش التي تقع في مجال المعالجة للبيانات نظرا لأن الحاسب الآلي و الانترنت أصبحا يحلان محل الأوراق في معظم المجالات.[1]

ثانيا : نتائج الجريمة الإلكترونية :

- آثار مادية : و هي جملة الآثار المحسوسة التي تؤثر على الضحية مثل سرقة الأموال و سرقة بعض البيانات و المعلومات الخاصة بالضحية و الذي يكون له أثر كبير إذا كانت الضحية مؤسسات كبيرة و مهمة [2]، حيث قدرت الخسائر المادية للجرائم الإلكترونية بما يزيد عن مليارات الدولارات سنويا على مستوى الأفراد و الدولة .

- آثار مالية : تؤثر الجرائم الإلكترونية بشكل كبير فيما يخص الأموال خاصة إذا كان الهدف أو الضحية هي شركة أو مؤسسة كبيرة و في الغالب تكون عالمية، مما يجعل الخسائر المالية لهذه الشركات كبيرة جدا مثل الهجوم الإلكتروني الكبير الذي حدث لشركة التأمينات الأمريكية **anthem**

- **أندم** عام **2015** [3]، حيث بلغت الخسائر المالية التي وقعت بها الشركة حوالي 100 مليون دولار أمريكي.

- آثار أمنية : ففي ظل الانتشار الكبير للجرائم الإلكترونية على جميع الفئات أو المؤسسات سوآءا كانت كبيرة أو صغيرة ، حيث أصبحت الشركات تقوم بتوظيف موظفون متخصصين في مجال أمن المعلومات و الأمن السيبيراني [4]، من أجل حماية أنظمتها من خلال تنزيل برمجيات ترفع من الحماية لهذه الشركات ضد العابثين و المجرمين، الذين يخترقون انظمة الشركات و يدمروها.

المطلب الثاني
أركان الجريمة الإلكترونية

سنتطرق في هذا المطلب إلى أركان الجريمة الإلكترونية الأساسية المقسمة على ثلاث فروع . الفرع الأول : الركن الشرعي أما الفرع الثاني : الركن المادي ، و الفرع الثالث يتضمن الركن المعنوي.

[1] بن طالب ليندا، مرجع سابق، ص 26.
[2] أحمد شوقي الشلقان، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 51.
[3] احمد شوقي الشلقان، مرجع سابق، ص 51.
[4] أحمد شوقي الشلقان، مرجع سابق، ص 53 .

الفرع الأول
الركن الشرعي

كون الجريمة حاصل تحصيل مجموعة من السلوكيات و الأفعال المادية الصادرة عن الإنسان ، هذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة و بموجب نص قانوني يحدد فيه الفعل الضار و العقوبة المقررة لارتكابه.

واجه المشرع عدة عراقيل عند تنظيمه لمجال الحماية الجنائية من مخاطر جرائم المعلوماتية و كان أول العراقيل هو إمكانية تطبيق النصوص التقليدية على هذا النوع الجديد من الجرائم هذا ما أدى به إلى التدخل في سن قوانين جديدة تطبيقا لمبدأ الشرعية ، و فيما يلي نماذج عن بعض التشريعات :

أولا: على المستوى الدولي :

هناك العديد من الهيئات و المنظمات التي تؤدي دورا ملحوظا في إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجريمة الإلكترونية و على سبيل المثال :

- مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو "إيطاليا" عام **1985** حيث كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات و الاعتداء على الحاسب الآلي حيث أقرت مجموعة من المقترحات و التوصيات لمكافحة الجريمة الإلكترونية، و قد أكد هذا المؤتمر على وجوب التطبيقات الجديدة في مجال العلم و التكنولوجيا في كل مكان لصالح الجمهور [1]، و اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال المخلة لهذه التكنولوجيا ، كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم و تتناول الجريمة الإلكترونية باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال و الاحتيال المنظم ، حيث تضمن خطة عما لبرنامج عالمي لمنع الجريمة المنظمة عبر الوطن والإرهاب مشددة على ضرورة إجراء بحوث ذات توجه عملي و تقديم المساعدة التقنية للبلدان النامية .

- الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية " **بودابست 22 نوفمبر 2001** " تناولت كل ما يتعلق بالجريمة الإلكترونية ، سواء ما يقع ضد الشبكات أو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات المعلوماتية . فقد جاء في الفصل الاول منها تعريف بعض المصطلحات المتعلقة بالحاسوب و الأنترنت ، أما الفصل الثاني فتناول الإجراءات الواجب اتخاذها على المستوى المحلي ، وقد وردت بعض من صور الجريمة الإلكترونية وذلك من خلال المواد **02-10** ، والفصل الثالث احتوى المواد **23-31** التي أوجبت التعاون الدولي لمكافحة الجريمة و القبض على المجرمين[2] .

[1] إلهام بن خليفة، القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، كلية الحقوق، جامعة الشهيد حمة لخضر، الوادي، ص 14 .

[2] اتفاقية بودابست، المؤرخة في 23 نوفمبر2001، التي تنص على مكافحة الجرائم الالكترونية .

ثانيا: على المستوى الوطني :

- في التشريع الجزائري : نظرا لأن المعلوماتية أصبحت من وسائل ارتكاب الجرائم ، تدخل المشرع الجزائري و أورد قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيات و هو القسم السابع مكرر لمحتوى **المادة 394** مكرر إلى 394 مكرر07 ، بمقتضى القانون **04-10 المؤرخ في 2004/11/15**.[1]
- و لم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون **06-23 المؤرخ في 2006/12/20** ، و الذي مسّ المادة **303** و إقراره بالمادة **303مكرر** إلى المادة **303 مكرر 03** وهذا تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة[2]

الـــــفـــــرع الـــثـــانـــــي

الـركـــن الـــمـــادي

يتكون الركن المادي للجريمة الإلكترونية من السلوك، النتيجة و العلاقة السببية و نظرا للاختلاف الفقهي القائم حول تعريف الجريمة الإلكترونية، فإنه يصعب تحديد صورة السلوك و على سبيل المثال صورة الجريمة الإلكترونية في التشريع الجزائري ، الذي حصر الركن المادي للجريمة الإلكترونية حسب نص المواد **394** إلى **394 مكرر 7** و التي نستخلص من مضمونها الصور التالية :

أولا: الدخول أو البقاء غير المشروع داخل نظام المعلوماتية، حيث نصت المادة **394** مكرر" يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50.000 دج إلى 100.000 كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات".[3]

ثانيا: الاعتداء على سير نظام المعلوماتية ، حيث نصت **الفقرة 03** من نفس المادة على أنه " و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و غرامة من 50.000 دج إلى 150.000 دج".[4]

ثالثا: حذف أو تغيير لمعطيات المنظومة.[5]

رابعا: القيام بإدخال عن طريق الغش معطيات في نظام المعالجة الآلية أو إزال أو عدل بطريق الغش للمعطيات التي يتضمنها و هذا ما نصت عليه المادة **394 مكرر 1.**[6]

خامسا: التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية.[7]

---

[1] ابتسام بقو، مرجع سابق، ص 22
[2] القانون 06-23 من قانون العقوبات ،المؤرخ في 2006/12/20 .
[3] بن طالب ليندا، مرجع سابق،32.
[4] بن طالب ليندا، مرجع سابق، ص 32
[5] نهلا عبد القادر المومني، مرجع سابق ص 42
[6] نفس المرجع السابق، ص 42
[7] نفس المرجع، ص 43

سادسا: حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان من المعطيات المتحصل عليها.[1]

الفـــــــــــــرع الثـالـث

الركن المعنوي

الركن المعنوي هو الحالة النفسية للجاني، و العلاقة التي تربط ماديات الجريمة و شخصية الجاني و لقيام الركن المعنوي للجريمة الإلكترونية يكفي توافر القصد العام أي توافر العلم و الإرادة، و خاصة أن الجريمة الإلكترونية كما سبق القول من الجرائم العمدية ،فمتى تطابق السلوك مع الصور التي تصلح لأن تشكل جريمة إلكترونية .

المبحث الثاني

معالجة الجريمة الإلكترونية في التشريع الجزائري

إن التطور السريع لتكنولوجيا المعلومات و شبكات المعلومات أدى إلى ظهور نمط جديد، و هو الجريمة الإلكترونية بفضل توافر الوسائل التقنية، حيث ساهمت شبكات الاتصال المعتمدة في عولمة الجريمة الإلكترونية و تنوعت الأنشطة الإجرامية فيها، مما أدى بالمشرع الجزائري لوضع و سن قوانين للحد من الجرائم الإلكترونية، ووضع هيئات مختصة للوقاية من هذه الجرائم.

المطلب الأول

تجريم الأعمال الإلكترونية

سنتناول في هذا المطلب تجريم الأعمال الإلكترونية حيث أن المشرع الجزائري كغيره من التشريعات تدخّل عن طريق سن نصوص و آليات قانونية عملية لاحتواء هذه الظاهرة و التصدي لها لذا سنقسم المطلب إلى فرعين، الفرع الأول بعنوان : الجريمة الإلكترونية في قانون العقوبات الجزائري. و الفرع الثاني بعنوان : الجريمة الإلكترونية في قانون الإجراءات الجزائية.

[1] نهلا عبد القادر المومني، مرجع سابق، ص 43

الفــرع الأول
قانون العقوبات الجزائري

تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي و ذلك لما شهدته الشبكة المعلوماتية من جرائم ، و هذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون **15-04** المؤرخ في **2004/11/10** ، المتمم للأمر رقم **66-156** و المتضمن قانون العقوبات تحت عنوان" المساس بأنظمة المعالجة الألية للمعطيات" حيث يتضمن هذا القسم ثمانية مواد، من المادة **394 مكرر** إلى **394 مكرر 7** و من هذه المواد ما يلي :

- المادة **394 مكرر** : " يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة مالية تقدر ب 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ".[1]

"تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة " .
" وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و غرامة مالية 50.000 دج إلى 150.000 دج ".

- المادة **394 مكرر1**: " يعاقب بالحبس من ستة إلى ثلاث سنوات و بغرامة مالية تقدر ب 500.000 دج إلى 2.000.000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنها" .[2]

- **المادة 394 مكرر 7**: " يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها ".[3]

- وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم 06-23 المؤرخ في **2006/12/20** حيث مسّ ذلك التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و قد تم تجديد العقوبات المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم **04-15.**
- ونجد المشرع الجزائري أخذ بنفس منوال المشرع الفرنسي ، حيث يكمن الفرق في أن المشرع الجزائري لم يتطرق إلى جريمة استعمال المستندات المعلوماتية المزورة بخلاف المشرع الفرنسي الذي نص على الجريمة في المادة **462/6** من قانون العقوبات الفرنسي.

[1] القانون 04-15 المؤرخ في 2004/11/10 المتمم لأمر رقم 66-155 و المتضمن قانون العقوبات "المساس بأنظمة المعالجة الآلية "، الجريدة الرسمية رقم 71/2004
[2] قانون 04-15المؤرخ في 2004/11/10 ، مرجع سابق
[3] نفس المرجع السابق

الفرع الثاني
قانون الإجراءات الجزائية

إن الإجراءات الإلكترونية تخضع لنفس الإجراءات التي خضعت لها الجريمة التقليدية كالتفتيش و المعاينة، و استجواب المتهم و الضبط و التسرب و الشهادة و الخبرة.

المطلب الثاني
الأجهزة المختصة في متابعة الجرائم الإلكترونية

سنقسم هذا المطلب إلى أربعة فروع ، الفرع الأول بعنوان: الهيئة الوطنية للوقاية من الجرائم تكنولوجيات الإعلام و الاتصال و الفرع الثاني تحت عنوان الهيئات القضائية الجزائية المختصة و الفرع الثالث بعنوان : المعهد الوطني للأدلة الجنائية وعلم الإجرام و الفرع الرابع بعنوان : المديرية العامة للأمن الوطني .

الفرع الأول
الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

لقد نص القانون **09-04** في المادة **13** منه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و لقد صدر المرسوم الرئاسي رقم **15-261** المؤرخ في **2015/10/08** الذي يحدد تشكيلة و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، كما صدر المرسوم الرئاسي رقم **19-172** المؤرخ في **2021/11/07** المتضمن إعادة تنظيم الهيئة .

- التعريف بالهيئة : حسب المادة الثانية والثالثة من المرسوم الرئاسي رقم **21-439** فإن الهيئة تعد سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع لدى رئيس الجمهورية ، و يحدد مقرها بمدينة الجزائر، و تجدر الإشارة إلى أنه في ظل المرسوم الرئاسي رقم **15-261** كانت سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي ، توضع لدى وزير العدل، أما في ظل المرسوم الرئاسي رقم **19-172** فكانت الهيئة تعد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني . [1]

- الاختصاصات : إن الهيئة تمارس العديد من الاختصاصات في سبيل الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، و من بين المهام التي تقوم بها :

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.[2]

[1] القانون 09-04 المؤرخ في 14 شعبان عام 1430الموافق ل 5 أوت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الصادر في 16 أوت 2009، الجريدة الرسمية رقم 47

[2] القانون 09-04 المؤرخ في 14 شعبان عام 1430الموافق ل 5 أوت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الصادر في 16 أوت 2009، الجريدة الرسمية رقم 47

- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم من خلال القيام بجمع المعلومات و التزويد بها.

- تطوير التعاون مع المؤسسات و الهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.
- تجميع و تسجيل و حفظ المعطيات الرقمية للأنظمة المعلوماتية.

- تنظيم و تشكيلة الهيئة: حسب نص المادة 5 من المرسوم الرئاسي **21-439** تتكون الهيئة من مجلس توجيه و مديرية عامة ، يوضعان تحت سلطة رئيس الجمهورية و يقدمان له عرضا عن نشاطاتهما. كما أن المديرية العامة التي تضم المراقبة الوقائية و اليقظة الإلكترونية هي التي تكلف بعمليات الوقاية.[1]

الفرع الثاني
الهيئات القضائية الجزائية المتخصصة في الجرائم الماسة بأنظمة المعالجة الآلية

➢ إنشائها:

نشأت بموجب القانون **04-14** المؤرخ في **2004/11/10** المعدل لقانون الإجراءات الجزائية .تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد **37-329-40** من قانون الإجراءات الجزائية. اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم **348/06** المؤرخ في **2006/1/5**.

إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال المرتكبة في الخارج حتى لو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة **15** من القانون رقم **04**.

➢ توسيع صلاحية الضبطية القضائية:

عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني حسب المادة **16** من قانون الإجراءات الجزائية

كما يمكن تفتيش المحلات السكنية و غير السكنية في أي ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية حسب المادة **47** من قانون الإجراءات الجزائية . [2]

[1] القانون 09-04،المؤرخ في 14 شعبان عام 1430الموافق ل 5 أوت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الصادر في 16 أوت 2009، الجريدة الرسمية رقم 47

[2] القانون 15-04 المؤرخ في 2004/11/10 المتضمن قنون العقوبات ، الجريدة الرسمية ، رقم 71/200

- أساليب التحري الخاصة :

اعتراض المراسلات الإلكترونية حسب المادة **65** مكرر **5** من قانون الإجراءات الجزائية المدرجة بموجب القانون **06-22** المؤرخ في **2006/12/20** .[1]

الفرع الثالث
المعهد الوطني للأدلة الجنائية و علم الإجرام

يتكون المعهد الوطني للأدلة الجنائية و علم الجرائم من إحدى عشرة دائرة متخصصة في مجالات مختلفة تضمن إنجاز الخبرة، التكوين و التعليم، تقديم المساعدات التقنية، البحوث، الدراسات و التحاليل في علم الجريمة

- دائرة الإعلام الآلي و التكنولوجي مكلفة بمعالجة و تحليل و تقديم كل دليل رقمي و تماثلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

- أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف ، التقنيات و الطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها، تنقسم الدائرة إلى ثلاث مخابر و ذلك حسب نوع المعلومات (سمعية ، بصرية و إعلام آلي) كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات و ضمان نزاهة و شرعية الدليل و هذه المخابر هي :مخبر الإعلام الآلي ، مخبر الفيديو ، مخبر الصوت.[2]

- مخبر الإعلام الآلي **:**

من مهامه :

تحليل و معالجة حوامل المعطيات الرقمية (الهاتف ، الشريحة ، القرص الصلب ، ذاكرة الفلاش) بالإضافة إلى تحديد التزوير الرقمي للبطاقة البنكية .[3]

من تجهيزاته :

- محطة ترميم و تصليح الأجهزة و الحوامل المعطلة .

- الشبكات الإعلامية (خبرات الإعلام الآلي و التجهيزات البيانية).

- محطة ثابتة و محمولة لإجراء خبرات الإعلام الآلي.

- جهاز اقتناء معلومات الهواتف و الحاسوب .[4]

- مخبر الفيديو : يختص بإعادة بناء مسرح الجريمة بتشكيل ثلاثي الأبعاد ، كما يعمل على تحسين نوعية الصورة (فيديو ، صورة) بمختلف التقنيات و مقارنة الأوجه و شرعية الصور و الفيديو .
- مخبر الصوت **:** يختص بمعرفة و تحديد المتكلم ، و تحديد شرعية التسجيلات الصوتية و يعمل على تحسين نوعية إشارة الصوت بنزع التشويش و تعديل السرعة .

[1] احمد حسام طه تمام، مرجع سابق، ص 55
[2] نفس المرجع السابق، ص 56.
[3] جميل عبد الباقي الصغير، الانترنت و القانون الجنائي، دار النهضة الغربية، القاهرة 2002، ص 52
[4] نفس المرجع السابق، ص 53

من أجهزته :

أجهزة الازدواجية ، معالجة و تحسين التسجيلات الصوتية ، نسخ الأقراص المضغوطة و أجهزة التصليح و التعبير ، أما بالنسبة للقاعات فإنه يحتوي مخبر الصوت على خمس قاعات (3 قاعات تحليل ، قاعة تخزين و قاعة موزع) .[1]

الفرع الرابع
المديرية العامة للأمن الوطني

تصدت هذه المديرية للجريمة الإلكترونية من مختلف الجوانب :

الجانب القانوني : و المتمثل في النصوص القانونية الآتية و قانون **22-06** المؤرخ في **2006/12/10** و القانون **03-05** من القانون المدني – القانون **04-09** المؤرخ في **2009/08/05** و قانون العقوبات المواد من **394** مكرر إلى **394** مكرر**7** .[2]

الجانب الوقائي : يتجلى دورها الوقائي من خلال عقد دورات افتراضية على مستوى شبكات المعلومات عامة و مواقع التواصل الاجتماعي خاصة .[3]

الجانب الردعي : يعتبر امتداد لدورها الوقائي في حالة الإخلال بالنظام العام ، أو في حالة منشورات هدامة تمس النظام العام كعرض أجهزة حساسة أو ممنوعات للبيع عبر مواقع التواصل الاجتماعي، حيث يتم التدخل و تحديد هوية صاحب الحساب و اتخاذ الإجراءات القانونية في هذا الشأن مع إنجاز ملف قضائي ضده .

الجانب التحسيسي : يتمثل في التنقل لمختلف المؤسسات التربوية و تنظيم نشاطات، و التحسيس حول سوء استعمال شبكات التواصل الاجتماعي أو سوء استخدام الانترنت و حماية الأطفال القصر من مخاطر الانترنت .

كما تعمل المديرية العامة على تلقي الشكاوي التي قد تكون مباشرة أو غير مباشرة عن طريق إرسال النيابة العامة للقضية للتحقيق فيها .

على المستوى الدولي : لم تغفل مديرية الأمن الوطني استغلال عضويتها الفعالة في الانتربول الذي يتيح لها مجالات للتبادل المعلوماتي و تسهيل الإجراءات القضائية المتعلقة بتسليم المجرمين، و كذا مباشرة الإنابة القضائية الدولية و نشر أوامر القبض للمبحوث عنهم دوليا .[4]

و من خلال الهيكل التنظيمي للمكتب المركزي الوطني- انتربول الجزائر- يوجد مكتب الربط الانتربول 48 ولاية، و استخدام قاعدة المعطيات **124/7** ، حيث يعمل جهاز **124/7** على تحديد المعلومات اللازمة حول الأشخاص و المركبات .[5]

---

[1] جميل عبد الباقي الصغير، مرجع سابق، ص 54.

[2] القانون 06-22 المؤرخ في 2006/12/20. المعدل والمتمم للأمر رقم 66-155 ، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية ، رقم 84/2006

[3] أحمد شوقي الشلقان، مبادئ الإجراءات الجزائية في التشريع الجزائري، ص 56

[4] نفس المرجع السابق، ص 57

[5] نفس المرجع السابق، ص 57

ملخص الفصل الأول

مما لا شك فيه أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة السابق و نحن لا نزال في بداية عصر الانفجار المعلوماتي ، و التطور التكنولوجي ما زال دائما في تطور و هذا ما أوجب تحديث الأنظمة و تعليمات و قوانين مواكبة لكل عصر حسب نوع الجرائم المستحدثة .

في ظل عصر السرعة و الثورة المعلوماتية لا نستطيع أن ننكر أهمية الأنترنت لأنها من دعائم تكنولوجيا الاتصال و المعلومات هذا من الجانب الإيجابي، و لكن الجانب السلبي المخفي هو الذي أدى إلى ظهور نمط جديد من الجرائم المعلوماتية و حداثة هذه الجرائم أدت إلى ظهور تشريعات جديدة للتصدي لها .

في الفصل حاولنا قدر المستطاع التطرق لمفهوم الجريمة الإلكترونية من تعريف اصطلاحي ، لغوي، فقهي و قانوني، كما خصصنا شطر خاص بتعريف المشرع الجزائري لهذه الآفة و خصائصها، تقسيماتها و خصائص المجرم الإلكتروني أيضا .

أما الشطر الثالث خصصناه للركن الشرعي و الركن المادي للجريمة و معالجتها ، بالإضافة إلى الإجراءات التقليدية التي كانت تتخذ للتحقيق في الجريمة.

تدابير التحقيق

في الجريمة

الإلكترونية

الفصل الثاني
تدابير التحقيق في الجريمة الإلكترونية

إن تطور التكنولوجيا في جميع نواحي الحياة أدى إلى إثارة ثورة صناعية في القرن التاسع عشر حيث غزت التكنولوجيا العالم من خلال الوسائل الحديثة، كما أن النمو الاقتصادي ساهم بشكل كبير في نمو هذه الظاهرة خاصة من قبل الطبقة المتعلمة التي تتعامل مباشرة مع هذه الوسائل كالحاسب الآلي الذي أصبح وسيلة أساسية لمختلف مجالات الحياة، حيث أنه سهل الحصول على المعلومات و الكشف عن الجرائم الإلكترونية و هو ما استدعى مواكبة التشريعات الداخلية و الدولية لهذه التطورات لتجنب الجرائم المعاصرة و من بينها الجرائم المرتبطة بتكنولوجيات الإعلام و الاتصال، حيث أصبح على كل دولة الاتخاذ التدابير التشريعية و الإجراءات الضرورية لغرض التحقيق في الجرائم المعلوماتية، مع إقامة توازن بين المصالح المختصة بالكشف عن الجرائم المعلوماتية من جهة، و احترام حقوق الإنسان و الحريات من جهة أخرى .

و في سبيل نجاعة التحقيق في مواجهة الجرائم المعلوماتية تدخلت القوانين الداخلية للدول من خلال سن قواعد إجرائية تمكن الجهات المختصة من اعتمادها في سبيل الوصول إلى الجريمة المعلوماتية و الدليل المناسب لإثباتها .

و هو ما استدعى التساؤل حول ما يتماشى مع طبيعة العالم الافتراضي خاصة و أن استخلاص الأدلة يحكمها قواعد إجرائية معينة كالتحقيق و التفتيش و المعاينة و الخبرة و التي تعد قواعد ذات نطاق عام صالحة لكل الجرائم .

ولهذا سنقسم هذا الفصل إلى مبحثين حيث سنتناول في المبحث الأول تدابير التحقيق في الجريمة الإلكترونية أما المبحث الثاني سيكون بعنوان الإجراءات المستحدثة للتحقيق في الجرائم الإلكترونية .

المبحث الأول
الإجراءات التقليدية للتحقيق في الجريمة الإلكترونية

لم يكن لدى الدول خيار آخر للتصدي لظاهرة الإجرام الإلكتروني في بداية ظهورها إلا الاعتماد على النصوص الجزائية القائمة بمختلف فروعها الموضوعية و الإجرائية ، و ذلك تفاديا لإفلات الجناة من العقاب من جهة، وعدم وجود قواعد قانونية تتلاءم مع طبيعة هذه الجرائم المستحدثة من جهة أخرى، و لكن بعد التطورات التي شهدها العالم في مجال المعلوماتية و ما صاحبه من انعكاسات على الجرائم في الوسائل المستعملة لارتكابها و المحل الذي تقع عليه و نوع الجناة الذين يرتكبونها ، جعل هذه القوانين غير مواكبة لها . و بالتالي اصبح لا بد على المشرع توسيع نطاق إجراءات التحقيق التقليدية لمتابعة الجرائم الإلكترونية، التي يقصد بها تلك الإجراءات التي تثير إشكالات و عقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش و الضبط و المعاينة و الخبرة والتي هي في حاجة تطوير و تحسين لكي تتناسب مع هذه الجرائم و طبيعة الدليل الذي يصلح لإثباتها، أما غيرها من الإجراءات كسماع المتهم أو الشهود، الاستجواب و المواجهة، فإنها مستبعدة نظرا لعدم وجود أية صعوبات في اتخاذها، لذا نركز على دراسة الفئة الأولى من إجراءات التحقيق .

المطلب الأول
الإجراءات المادية

تحتاج الدعوى قبل دخولها إلى المحكمة إلى جمع المعلومات عنها من حيث نوع الفعل المرتكب و من الذي ارتكبه و الأدلة التي تثبت نسبة الفعل إلى مرتكبه، و هذا ما يعرف بالتحقيق كما أن التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية من حيث الإجراءات و ذلك لحداثة هذه الجريمة و مهارة مرتكبيها في الإجرام و محو الأدلة ، مما استدعى التساؤل حول ما يتماشى مع طبيعة العالم الافتراضي خاصة و أن استخلاص الأدلة قواعد إجرائية معينة كالتفتيش و الضبط و المعاينة و التي تعد قواعد ذات نطاق عام صالحة لكل الجرائم إلا أن تنظيمها للجرائم المعلوماتية لا بد أن يتناسب مع طبيعتها و خصوصيتها و مع طبيعة الدليل أيضا . ولهذا تم تقسيم المطلب على النحو التالي : الفرع الأول تحت عنوان التفتيش و ضبط الأدلة ، أما الفرع الثاني تحت عنوان المعاينة .

الفرع الأول
التفتيش و ضبط الأدلة في الجريمة الإلكترونية

أولا : تعريف التفتيش :

يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة.
تعريف التفتيش لغة : من مصدر فتّش أي بحث و سأل .
تعريف التفتيش قانونا : هو البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها.[1]

تعريف التفتيش فقها : عرّفه الفقه الفرنسي بأنه : "بحث بوليسي أو قضائي عن عناصر الدليل في جريمة ما". [2]
كما عرّفه جانب من الفقه بأنه : "إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون".[3]
و يمكن تعريفه أيضا : "بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي و الغرض منه البحث عن أدلة الجريمة المرتكبة ، و كل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه فيه بأنه مرتكب الجريمة ".

ثانيا : القواعد العامة للتفتيش :

الغرض من التفتيش هو البحث عن الأدلة المتعلقة بالجريمة ، التي تساعد في كشفها . و التفتيش في الجريمة الإلكترونية يخضع إلى قواعد شكلية و قواعد موضوعية :

أ- القواعد الشكلية لتفتيش نظم الحاسوب و الانترنت : الأصل أن التفتيش لا تقوم به إلا سلطة التحقيق ، فيخضع التفتيش في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق المتمثلة في وجوب التدوين بمعرفة كاتب و السرية عن الجمهور و حضور الخصوم و وكلائهم كل ما أمكن ذلك .[4]

وهناك شروط للتفتيش تختص بها الجريمة الإلكترونية دون غيرها من بينها توافر الخبرة الفنية لدى القائم بالتفتيش من خلال أن يتلقى المحقق في الجريمة الإلكترونية تدريبات أمنية خاصة ، تعرّفه كيفية التعامل مع التقنية الحديثة و كيفية ضبط الأدلة و الحفاظ عليها في هذا المجال ، كذلك يجب أن يتم التفتيش بصورة صحيحة من الناحيتين الشكلية و الموضوعية .

كذلك من القواعد الشكلية التي تحكم التفتيش عدم التجاوز في التفتيش، و ذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عم معلومات تفيد في كشف الحقيقة مع وجوب أن يكون التفتيش في حدود الإذن المكتوب ، المؤرخ و الموقع من الجهة التي أصدرته و إلا كان التفتيش باطلا .

---

[1] عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي ، ص 61 .
[2] نفس المرجع، ص 61 .
[3] نفس المرجع السابق، ص 61.
[4] بخي فاطمة الزهراء ، إجراءات التحقيق في الجريمة الإلكترونية ، مذكرة ماستر ، كلية الحقوق ، جامعة المسيلة ، 2014 ، ص 73

ويجب أن يكون إذن التفتيش محدد المدة التي تحتسب من يوم الإذن إلى الجهة المأذون لها إجراء التفتيش [1]، وأضافت الجمعية الدولية لقانون العقوبات ضرورة وجود خبير معالجة بيانات يساعد في صياغة مسودة إذن التفتيش .

وأخيرا بما أن التفتيش عن الملفات الموجودة في جهاز الكمبيوتر من الأمور المعقدة لأنها تحوي عمليات إلكترونية غامضة يمكن تخزينها حتى على رأس إبرة و تحريكها حول العالم في أي وقت ، إذا فتفتيش و ضبط نظم الحاسب الآلي يعتبر فن بقدر ما هو علم مما ينبغي على رجال الضبط القضائي و رجال النيابة العامة إتباع الخطوات التالية :

- تجميع فريق عمل يتكون من رجل الضبط القضائي المكلف بالمهمة ، وكيل الجمهورية ، خبير فني .

- التعرف قدر الإمكان على نظم الكمبيوتر قبل إجراء التفتيش .

- وضع خطة لتنفيذ التفتيش .

- العناية بمسودة إذن التفتيش ، اشتمالها على وصف محل التفتيش ، و شرح استراتيجية التفتيش الممكنة

ب- القواعد الموضوعية لتفتيش نظم الحاسوب و الأنترنت : يجب على المحقق مراعاة القواعد التالية عند القيام بعملية التفتيش :

وجود سبب للتفتيش :لا يصح إصدار الإذن بالتفتيش إلا لضبط ماديات الجريمة الواقعة بالفعل و اتهام شخص أو عدة أشخاص بارتكابها، و المساهمة فيها مع توافر إشارات قوية على وجود أشياء تفيد المحقق فيكشف الحقيقة . و يمكن حصر الشروط الموضوعية للتفتيش[2] فيما يلي :

- أن يكون التفتيش بصدد جريمة إلكترونية واقعة بالفعل سوآءا كانت جناية أو جنحة .

- لا بد من إتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة الإلكترونية أو المشاركة في ارتكابه

- لا بد من توافر الدلالات و إشارات قوية أو قرائن على وجود أجهزة و أدلة معلوماتية تفيد في كشف الحقيقة .

و تفتيش نظم الحاسب الآلي وفق الأسلوب الأمريكي يلخص فيما يلي :

-اقتحام قوة الشرطة للمكان بصورة سريعة و من كافة منافذه في وقت واحد[3] .

- إبعاد سائر المشتبه فيهم عن كافة أنظمة و معدات الكمبيوتر الموجودة في المكان على الفور كي لا يتمكنوا من تدمير أي دليل ، و توضع أجهزة الكمبيوتر الموجودة بالمكان في عهدة فريق يضم اثنين من العملاء أولهما مكتشف تم تدريبه تدريبا متقدما على نظم المعلومات و هو الذي يقوم بعملية الضبط و يتولى نزع مقبس

[1] بخي فاطمة الزهراء، مرجع سابق ص 74
[2] نفس المرجع، ص 75
[3] نفس المرجع السابق، ص 76

الكهرباء الخاص بسائر الأجهزة كما يقوم بالبحث عن الأقراص المرنة و الصلبة و الملفات و حاويات الأسطوانات .

والثاني مسجل يقوم بتصوير كافة الأجهزة و المعدات بالكيفية التي تم ضبطها عليها كما يقوم بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدّعي المجرم أن الشركة قد سرقت منزله أثناء التفتيش .

ثالثا : تحديد محل التفتيش : قد يقع التفتيش على شخص و قد يقع على مكان ، و المقصود بالشخص من مستغلي أو مستخدمي الكمبيوتر و من خبراء البرامج ، و قد يكون من المحللين و من مهندسي الصيانة و الاتصالات أو من مديري النظم المعلوماتية[1] ، أو قد يكون من أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة .

ومحل التفتيش هو المستودع الذي يحفظ فيه المرء الأشياء المادية التي تضمن سره ،و هذا الأخير في جرائم الأنترنت هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الأنترنت كما يقصد به المكان الذي يحتفظ فيه الجاني أو المجرم بجميع الوسائل التي ارتكب بها الجريمة [2].

أما إذن التفتيش طبقا للتشريع الجزائري لا بد أن يكون مكتوب من طرف إما وكيل الجمهورية أو قاضي التحقيق المختص .

الفـــــــرع الثـــــــاني

المعاينة

قبل التطرق إلى المعاينة في الجريمة الإلكترونية يجب تحديد تعريف المعاينة لغة و اصطلاحا و قانونا .

أولا: تعريفها في الجريمة الإلكترونية .

أ- تعريف المعاينة لغة : المعاينة هي المشاهدة بالعين .

ب- تعريف المعاينة اصطلاحا : هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه و يجمع الآثار المتعلقة بالجريمة و كيفية وقوعها كذلك يجمع الأشياء الأخرى التي تفيد في كشف الحقيقة ، و اتخاذ ما يلزم من إجراءات كضبط بعض الأشياء ، فالهدف من المعاينة هو : جمع الأدلة الناتجة عن الجريمة (الآثار) ، و إتاحة الفرصة للمحقق كي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها و لا غموض عن كيفية وقوع الجريمة[3] .

[1] بن طالب ليندا، الدليل الإلكتروني و دوره في الإثبات الجنائي ص 74
[2] نفس المرجع السابق، ص 74
[3] نهلا عبد القادر مومني، مرجع السابق ، ص 28 . 29

ج- تعريف المعاينة قانونا : هي إثبات حالة الأماكن و الأشياء و الأشخاص و كل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد بها آثار يرى المحقق أن لها صلة بالجريمة و الأصل أن إجراء المعاينة متروك لتقدير المحقق و لا يقوم بها إلا إذا كان هناك فائدة من ورائها كما ان هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة[1] .

ثانيا : مسرح المعاينة : إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة فإن الجريمة المعلوماتية تتم المعاينة فيها على مستويين :

أ- المسرح التقليدي (الجرائم الواقعة على المكونات المادية) : هو المسرح الذي يقع عادة خارج بيئة الحاسوب و يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة و هو قريب من مسرح الجريمة التقليدية ، و من أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب و الكابلات الخاصة و شاشة العرض الملحق به و مفاتيح التشغيل و الأقراص و غيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس[2] (الملموس) .

و ليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية و التحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة و نسبها إلى شخص معين ، و كذلك وضع الأختام في الأماكن التي تمت المعاينة فيها ، و ضبط كل الأدوات و الوسائل التي استخدمت في ارتكاب الجريمة مع وجوب إخطار النيابة العامة بذلك .

و في هذه الحالة تتميز المعاينة بالسهولة . باعتبارها أنها تتم على عناصر ملموسة كانت محلا للجريمة و تخلفت عنها .

ب- المسرح الافتراضي (الجرائم الواقعة على المكونات غبر المادية أو بواسطتها) : و المسرح الافتراضي يقع عادة داخل البيئة الإلكترونية و يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله و في مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم عن طريق الانترنت و منها جرائم التزوير المعلوماتي و التخريب[3].

و تتميز المعاينة في العالم الافتراضي بما يلي :

- ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على الأدوات المعلوماتية .

- وللمعاينة في جرائم الانترنت و الحاسوب (المعلوماتية) أشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة كما أن هناك طرقا عامة تتوافق مع طبيعة الاتصال بالأنترنت أو الوسيلة التي تستخدم مثلا : وسلة تصوير شاشة الحاسوب impression de captures d ’écran و التي تكون بواسطة آلة تصوير تقليدية أو عن طريق

[1] نهلا عبد القادر مومني، مرجع سابق ص 29
[2] نفس المرجع السابق، ص 29
[3] عبد الفتاح بيومي حجازي ،مرجع سابق، ص 100

استخدام برمجة حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة و هذا ما يصطلح عليه تجميد مخرجات الشاشة sorties d 'écran و غيرها .[1]

شروط صحة معاينة مسرح الجريمة : حتى تعطى المعاينة ثمارها للكشف عن الغموض و التوصل إلى الجاني لابد أن يراعي قاضي التحقيق ما يلي :

1- سرعة الانتقال إلى مكان الجريمة : فور تلقي المحقق أو قاضي التحقيق بلاغ عن وقوع الجريمة من الجرائم المعلوماتية و التأكد من صحة الواقعة ، عليه أن ينتقل إلى مكانها ، و ذلك ضمانا لعدم تغيير شكل مسرح الجريمة عن الوضع و الحالة التي تركها الجاني عليها[2] ، و الحصول على شهادة الشهود .

2- السيطرة على مكان وقوع الجريمة : بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة من أجل معاينتها لا بد من أن يتّبع مجموعة من الإجراءات التالية :

منع تواجد أي شخص بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار و الأدلة التي تم العثور عليها في المسرح .

- التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة .[3]

- التحفظ على كل ما له علاقة بالحادث من أشياء و أشخاص .

- إخطار الخبراء لرفع الآثار و البصمات .

ثالثا : إجراءات المعاينة التقنية .

لا بد على ضابط الشرطة القضائية اتباع بعض القواعد و الإرشادات الفنية عند معاينة مسرح الجريمة المعلوماتية ، و تتمثل هذه الإجراءات في :

عند العثور على حاسبات آلية و أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها ، و تدوين الحالة التي هي عليها إذا كانت غير شغالة أو في حالة تشغيل أو موصولة بالكهرباء أو بجهاز لاحق آخر، كما ينبغي ترقيم لواحقها بشكل متسلسل .[4]

يجب تحرير الأوراق المطبوعة على الحاسب الآلي و التي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالاتها ، و يمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل و تحرير الأوراق التي تمت

طباعتها . بالإضافة إلى تفقد الجهاز و تسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة .[5]

---

[1] عبد الفتاح بيومي حجازي، ص 101
[2] نفس المرجع، ص 101
[3] نفس المرجع السابق، ص 102
[4] بن نعوم خالد أمين، اجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، ص 98
[5] نفس المرجع السابق، ص99

عند العثور على دعائم التخزين (أسطوانات ، أقراص ، حوامل مغناطيسية) يجب ترقيمها و تسجيل الحالة التي هي عليها و المكان الذي وجدت فيها (داخل الحاسب الآلي أو خارجه).

عند الانتهاء من الترقيم يجب تصوير و دمج الأجهزة و ملحقاتها في الحالة التي هي عليها .

يجب تحرير جميع العينات التي عثر عليها من أجهزة و دعائم داخل أكياس خاصة (بلاستيكية أو ورقية) كما ينبغي حمايتها من الكسر و تأثير العوامل الجوية و إبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات و إرسالها إلى المخبر لإجراء الخبرة .

المطلب الثاني

الإجراءات الشخصية

يقصد بالإجراءات الشخصية تلك الإجراءات التقليدية حتى و إن كان بعضها مستحدث في الآونة الأخيرة التي يتدخل فيها بعض الأشخاص بحكم صفتهم ، و بواسطتهم يتم الحصول على الدليل . و التحقيق فيها يتطلب مهارات فنية و تقنية كما يتطلب خبرة في مجال الحاسب الآلي و الأنترنت وكذا خلق جهات أمنية متخصصة للتحقيق وعلى هذا سنقسم المطلب إلى فرعين . الفرع الأول بعنوان الشهادة و أنواعها أما الفرع الثاني بعنوان الخبرة .

الفـــــــــــرع الأول

الشهـــــــادة

تختلف الشهادة في الجريمة الإلكترونية عن الجرائم الأخرى و ذلك لاشتراط صفات خاصة بالشاهد في الجريمة الإلكترونية كما أن سماع الشهود هو إجراء من إجراءات التحقيق ، يهدف لجمع الأدلة المتعلقة بالجريمة بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة إلا أن وجودهم ضروري للكشف عن الجرائم و القبض عن مرتكبيها و تخلف الشاهد عن الحضور للإدلاء بأقواله يعرضه للمسائلة الجنائية.

أولا : تعريف الشهادة و أنواعها .

أ- تعريف الشهادة : هناك من عرف الشهادة بأنها الأقوال التي يدلي بها الخصوم أمام سلطة التحقيق في شأن جريمة وقعت سواء تتعلق بإثبات الجريمة و ظروف ارتكابها أو إسنادها إلى المتهم أو براءته منها ، و عرفها الدكتور عاطف النقيب : " هي تقرير الشخص لحقيقة أمر كان قد رآه أو سمعه " ، كما عرفها الدكتور أحمد فتحي السرور بأنها : " إثبات واقعة معينة من خلال أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة "[1].

كما عرفها أبو العلاء النمر : " بأنها التعبير الصادق الذي يصدر في مجلس القضاء من شخص يقبل قوله بعد أداء اليمين في شأن واقعة عاينها بحاسة من حواسه "

[1] بخي فاطمة الزهراء ، اجراءات التحقيق في الجريمة الالكترونية ، ص 66

وتخضع الشهادة إلى عدة قواعد من بينها :

تكليف الشاهد بالحضور بواسطة القوة العمومية ، كما يجب أن تسلم نسخة من طلب الاستدعاء إلى الشخص المطلوب حضوره ، كذلك يجب ذكر هوية الشاهد قبل سماع شهادته و ذكر قرابته للخصوم و من أهم واجبات الشاهد حلف اليمين[1] ، و تجدر الإشارة إلى أنه يجوز سماع شهادة القصر و ذوي العاهات و ذلك وفقا لإجراءات خاصة بكل حالة و تؤدى الشهادات بانفراد و تدوّن بمحاضر خصصت لذلك و يصادق على المحضر كل من المحقق و الكاتب و الشاهد .

ب - أنواع الشهادة : تنقسم شهادة الشهود إلى ثلاثة أنواع :

1- الشهادة المباشرة : هي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه .[2]

2- الشهادة السماعية : بمعنى من علم بالأمر من الغير شهادة سماعية بحيث لا يشهد الشخص بما رآه أو سمعه مباشرة ، بل يشهد بما سمعه رواية عن الغير فيشهد مثلا أنه سمع شخصا يروي واقعة معينة ، و هي أقل شأنا من الشهادة الأصلية المباشرة .[3]

3- الشهادة بالتسمع : و هذه الشهادة تختلف عن الشهادة السماعية حيث تتعلق هذه الأخيرة بأمر معين نقلا عن شخص معين قد شاهد هذا الأمر بنفسه ، أما الشهادة بالتسمع فتتعلق بواقعة معينة لكنها ليست نقلا عن شخص معين بالذات شاهد الأمر بنفسه كأن يقول الشاهد سمعت كذا ، و أن الناس يقولون كذا و كذا عن هذه الواقعة أو هذا الأمر .[4]

ثانيا : تعريف الشاهد المعلوماتي .

يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله و خبرته في مجال المعلوماتية و قد عرف الشاهد الإلكتروني بأنه: "الشخص الفني صاحب الخبرة و التخصص في تقنية و علوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات[5] " .

[1] بخي فاطمة الزهراء، مرجع سابق ، ص 68
[2] نفس المرجع السابق، ص 69
[3] نفس المرجع السابق، ص 70
[4] نفس المرجع السابق، ص 71
[5] إلهام بن خليفة، القواعد الاجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ، كلية الحقوق ، جامعة الشهيد حمة لخضر، الوادي، ص56

و يمكن القول أن الشاهد الإلكتروني هو كل من :

- مشغلو الجهاز الآلي : هو ذلك الشخص المسؤول عن تشغيل الجهاز و المعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات و استخراجها كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح[1].

- خبراء البرمجة : هم الاشخاص المتخصصون في كتابة أوامر البرامج و ينقسمون إلى فئتين ، الأولى هم مخططو برامج التطبيقات و الثانية هم مخططو برامج النظم .

- المحللون : هم الأشخاص الذين يحللون الخطوات ، و يقومون بتجميع البيانات الخاصة بنظام معين ، و دراسة هذه البيانات ثم تحليل النظام ، و تقسيمه إلى وحدات منفصلة و استنتاج العلاقة الوظيفية بين هذه الوحدات ، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات ، و استنتاج الأماكن التي يمكن معالجتها بواسطة الحاسوب .[2]

- مهندسي الصيانة و الاتصالات : هم المسؤولون عن أعمال الصيانة الخاصة بتقنية الحاسب و مكوناته و شبكات الاتصال المتعلقة به .

- مديري النظم : هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية .

ثالثا : التزامات الشاهد المعلوماتي .

تعد التزامات الشاهد المعلوماتي نفسها التزامات الشاهد في الجرائم التقليدية ، و من أهم هذه الالتزامات يذكر:

حضور الشاهد : تملك سلطة التحقيق كامل الحرية في أن تسمع الشهود عن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة و ظروفها و إسنادها إلى المتهم أو براءته منها ، و لها كذلك أن تسمع شهادة الشهود الذين يطالب الخصم سماعهم ما لم يرى عدم الفائدة من سماعهم [3].

نص المشرع الجزائري في المادة **223** من قانون الإجراءات الجزائية الجزائري صراحة على عقاب الشاهد المتخلف عن الحضور أو رفض حلف اليمين أو أداء الشهادة .

حلف اليمين : تنص المادة **227** من قانون الإجراءات الجزائية الجزائري على إلزام أن يؤدي الشاهد اليمين القانونية حسب الصيغة القانونية المنصوص عليها في المادة **93** من القانون نفسه و يترتب على مخالفة هذا الإجراء بطلان شهادته [4].

[1] إلهام بن خليفة، مرجع سابق، ص 56
[2] نفس المرجع السابق، ص 58
[3] نهلا عبد القادر المومني، مرجع سابق، ص 82
[4] نفس المرجع السابق، ص 83

أداء الشهادة : يلتزم الشاهد بالإدلاء بشهادته و الالتزام بقول الحقيقة ، حيث الشهادة كذبا من أجل تضليل الحقيقة تعد شهادة زور و هي منصوص عليها في المادة **332** من قانون العقوبات الجزائري ، بالتالي يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في الحاسبات و المواقع التي تحتوي على المعلومات التي تشكل جريمة بحث عن أدلة تثبتها [1].

هناك بعض القوانين الأوربية مثل القانون الإنجليزي الصادر في **1984** بشأن البوليس و الأدلة الجزائية التي أوجبت على الشاهد أن يقوم بإجراء إنعاش الذاكرة ، و ذلك لفحص الأماكن و المستندات التي توجد تحت سيطرتهم إذ لم تترتب على ذلك أضرار خطيرة ، لأن الالتزام بالتعاون ليس فقط بمجرد إصدار الأمر بإحضار الشهود و لكن إلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة للوصول إليها ، كما تسمح هذه التشريعات بالاستفادة بالشهود كخبراء .

لذلك فإن الشاهد يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها ، لكن لا يجوز إكراهه على ذلك .

الفرع الثاني

الخبرة في مجال الجرائم المعلوماتية

الخبرة هي عبارة عن إجراء من إجراءات التحقيق التي تستوجب الإلمام بمجموعة من المعلومات الفنية التي تساعد في استخلاص الأدلة اللازمة للتوصل إلى الحقيقة القضائية .

أولا : تعريف الخبرة في الجرائم المعلوماتية .

الخبرة هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية أو الإدارية التي لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله و ثقافته[2] .

كما اهتم المشرع الجزائري بتنظيم أعمال الخبرة ، حيث أجاز قانون الإجراءات الجزائية الجزائري للنيابة العامة و لقاضي التحقيق و للمحاكم كذلك الاستعانة بخبير واحد أو أكثر. كما أن الخبرة في المجال المعلوماتي تساعد على :

- الكشف عن الدليل الإلكتروني .
- تحديد الخصائص الفريدة للدليل الإلكتروني .
- إصلاح الدليل الإلكتروني و إعادة تجميعه من المكونات المادية للكمبيوتر .
- جمع الآثار المعلوماتية الإلكترونية التي تكون قد تبدلت خلال الشبكة المعلوماتية[3] .

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 83
[2] نفس المرجع، ص 321
[3] نفس المرجع السابق ص 322

ثانيا : الخبير في الجريمة المعلوماتية .

يمكن تعريف الخبير أنه كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء على مستوى المحاكم ام لا .

كما عرف بأنه كل شخص له دراية بمسألة من المسائل ، و قد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا[1] .

و من هنا سنتطرق إلى النقاط التالية :

-تعيين الخبراء : قد تعترض المحقق أثناء سيران التحقيق ، بعض المسائل الفنية الهامة التي يحتاج كشفها إلى خبرة علمية دقيقة ، حيث حدد المشرع الجزائري طرق اختبار الخبراء في المادة **144** من قانون الإجراءات الجزائية الجزائري ، و يشترط في الخبير حقيقة الجمع بين العلم ذي الاختصاص و الخبرة العلمية ، فلا يكفي

فقط كفاءة علمية عالية في مجال التخصص ، بل يضاف إليها سنوات من أعمال الخبرة في المجال فيجوز للقاضي ندب خبير من خارج الجدول [2].

أ- أنواع الخبراء :

1: المبرمج : هو المتخصص في كتابة أوامر البرامج سواء كانت برامج النظم أو برامج التطبيقات ، فالمتخصص في كتابة أوامر التطبيقات يعرف مواصفات النظام الإداري المطلوب من محلل النظم ، ثم يقوم بتحويل ذلك إلى البرامج الإلكترونية الرقمية[3] ، أما المتخصص ببرامج النظم فيقوم باختيار و تعديل و تصحيح برامج نظام الحاسب الداخلية التي تتحكم في وسائط التخزين إضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

2: المحلل : هو الشخص الذي يحلل خطوات العمل و يقوم بتجميع بيانات نظام معين كما هو الحال في نظم المعلومات الإدارية و غيرها .

3: مشغل الحاسب الآلي و شبكاته : هو المختص بتشغيل الحاسب الآلي و مكوناته ، و لديه خبرة في قواعد كتابة البرامج و تشغيل الجهاز و استخدام أدوات إدخال البيانات[4] .

4: مهندس الصيانة و الاتصال : هو المسؤول عن صيانة التقنيات الإلكترونية الرقمية و شبكاتها و فحصها .

5: مدير النظام المعلوماتي : هو المختص بالإدارة في النظم المعلوماتية[5] .

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 330
[2] نفس المرجع، ص 332
[3] نفس المرجع السابق، ص 332
[4] نفس المرجع السابق، ص 333
[5] نفس المرجع السابق، ص 333

ثالثا : أساليب عمل الخبير في الجريمة المعلوماتية :

هناك أسلوبان لعمل الخبير هما :

أ- القيام بتجميع و تحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كجريمة التهديد أو النصب ، جرائم النسخ ... الخ ، ثم يقوم الخبير بعملية تحليل رقمي لها و ذلك لمعرفة كيفية إعداده البرمجي و نسبتها إلى مسارها الذي أعدت فيه ، و تحديد عناصر حركتها ، و كيف تم التوصل إلى معرفتها ، و أخيرا التوصل لمعرفة بروتوكول الانترنت **"IP"** الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع[1] .

ب- القيام بتجميع و تحصيل لمجموعة المواقع التي لا تشكل موضوعها جريمة في ذاته ، و لكن الجرائم تقع من جرّاء تتبع موضوعات هاته المواقع مثلما هو الحال في المواقع التي تساعد الغير على معرفة جرعة المخدرات و المؤثرات العقلية حسب وزن الإنسان ، بإيهامه أنه إذا تم تتبع التعليمات الواردة فيها لن يصل الشخص إلى حالة إدمان ، كذلك الشأن بالنسبة لكيفية إعداد القنابل و تخزينها أو كيفية التعامل مع القنابل الزمنية[2] ... الخ .

رابعا : دور الخبير التقني في حفظ الأدلة الإلكترونية :

إن التحفظ على الأدلة الإلكترونية من العمليات المعقدة حيث تحتاج أولا إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، و كذلك صحة حركة الكمبيوتر فلو كان هناك فيروس في الجهاز لتم التشكيك في صحة الأدلة المستفاد منها ، و يحفظ الدليل في العالم الافتراضي برصد موقع الانترنت أو المعلومات التي تشير إلى الجريمة ، و التي تكون في مظاهر مختلفة الأشكال و نأخذ على سبيل المثال جريمة القذف في غرف الدردشة ، هنا يتم اللجوء إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي للتوصل إلى تحديد موضوع القذف و تاريخه ، و لقد لجأت العديد من المحاكم إلى مكينة إدارتها رقميا ، بحيث يتم تسليم الأدلة إلى أدارة متخصصة تتولى حفظ الأدلة الرقمية .

و يتعين على الخبير تضمين المسائل التالية في مهمته :

- تركيب الحاسب الآلي ، طرازه ، نوعه ، نظام تشغيله و الأنظمة الفرعية التي يستخدمها .

- بيئة الحاسب أو الشبكة من حيث طبيعتها ، تركيزها أو توزيعها و كذلك نمط و وسائط الاتصالات[3] .

- المكان المحتمل لأدلة الإثبات و شكلها و هيئتها .

- الآثار الاقتصادية و المالية المترتبة على التحقيق في الجريمة الإلكترونية .

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

---

[1] أحمد شوقي الشلقان، مبادئ الاجراءات الجزائية في التشريع الجزائري، مرجع سابق، ص 252

[2] نفس المرجع السابق، ص 252

[3] بخي فاطمة الزهراء ، مرجع سابق ، ص 91

- إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون تلف .

- إمكانية نقل أدلة الإثبات لأوعية مادية كالأوراق على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة [1].

و ينصرف رأي الخبير إلى الوقائع اللازم إصدار رأيه الفني بشأنها ، كما يجب أن يتوقف رأيه عند المسائل الفنية دون أن يتعدى إلى المسائل الأخرى كالمسائل القانونية .

المبحث الثاني
الإجراءات المستحدثة للتحقيق في الجرائم الإلكترونية

تبين من الإجراءات التقليدية أنها صعبة الإتباع للحصول على الدليل الإلكتروني فكان من الضروري على التشريعات المختلفة خلق إجراءات قانونية حديثة لمواجهة هذا الإجرام غير التقليدي و ذلك حتى لا يفلت المجرمون من العقاب .

في إطار إصلاح المنظومة التشريعية و القضائية ، و ضمانا لفعالية و سرعة التحقيق في القضائية المتعلقة في الجرائم المستحدثة ، استحدث المشرع الجزائري في قانون الإجراءات الجزائية إجراءات جديدة تتمثل في التسرب و اعتراض المراسلات و ذلك بموجب القانون **06-22** المعدل لقانون الإجراءات الجزائية .

المطلـــب الأول
التسرب الإلكتروني

أمام التطور المذهل الذي يعرفه مجتمعنا في ميدان الإجرام وتطور طرقه وأساليبه، كان لزاما على المشرع ابتكار طرق فعالة وجديدة لمواجهة خطر تزايد وتفاقم هذه الظاهرة، وهذا ما نلمسه في آخر تعديل لقانون الإجراءات الجزائية، فمن الأساليب المبتكرة في هذا المجال نجد استحداث أسلوب التسرب بمعية أساليب أخرى لتفعيل دور البحث والتحري وجمع الأدلة عن الجرائم، وعليه سنحاول من خلال هذا المبحث الإحاطة بمفهوم التسرب وكذا بيان الشروط والإجراءات التي وضعها المشرع الجزائري في هذا المجال حيث يعتبر التسرب الإلكتروني من أحدث الطرق لمواجهة الجرائم الإلكترونية و التي اعتمدها المشرع الجزائري و نص عليها في المواد من **65** مكرر**11** إلى **65** مكرر **18** و عليه سنعرج عن تعريفه ، شروط صحة عمليته ، و الحماية القانونية للعون المتسرب و معوقات عملية التسرب .

[1] بخي فاطمة الزهراء، مرجع سابق، ص 92

الفرع الأول
تعريف عملية التسرب الإلكتروني

عرف المشرع الجزائري التسرب في المادة **65** مكرر **12** كما يلي : " يقصد بالتسرب قيام عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم[1] " .

و عرفه الفقه بأنه تقنية من تقنيات التحري و التحقيق الخاصة تسمح لعون الشرطة القضائية بالتوغل داخل جماعة إجرامية و ذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه بهم ، و كشف أنظمتهم الإجرامية و ذلك بإخفاء الهوية الحقيقة و بتقديم المتسرب على أنه فاعل أو شريك .

و يرى البعض أن هذه العملية عملية معقدة نظرا لكونها تنطوي على أن القائم بها يربط علاقات ضيقة مع المجرمين مع حفاظه على السر المهني من أجل تحقيق الغرض النهائي من العملية ، و أنها تتطلب الاضطرار للمشاركة المباشرة في نشاط المجموعات الإجرامية من أجل قبوله بينهم [2]

الفرع الثاني
شروط صحة عملية التسرب الإلكتروني

ينطوي إجراء التسرب على المساس بالحريات الفردية و حقوق الإنسان لذا نجد ان المشرع الجزائري وضع له ضوابط أو شروط تكون بمثابة ضمانات يتعين مراعاتها عندما يقتضي ضرورة التحقيق للقيام بمثل هذا الإجراء و تتمثل هذه الشروط في :

1-أن تتم هذه العملية بإذن من وكيل الجمهورية المختص إقليميا أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية ، وهو ما جاء في المادة **65** مكرر **11** [3].

2-يجب أن يكون الإذن مكتوبا مسببا ، و إذا خلا من هذا الشرط فإن التسرب قد يقع تحت طائلة البطلان و يجب أن يتضمن التسبيب العناصر التي يستند إليها القاضي الآمر بيه و مع ذكر الجريمة موضوع التسرب و هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته ، و هو ما ورد في الفقرات الأولى و الثانية من المادة **65** مكرر **15**[4].

3-يجب أن لا تتجاوز المدة المطلوبة لعملية التسرب أربعة أشهر و التي يمكن تجديدها حسب مقتضيات التحري و التحقيق ، و التجديد يكون بإذن مكتوب و يكون بنفس المدة و هي أن لا تتجاوز أربعة أشهر ، كما يجوز

[1] الهام بن خليفة، القواعد الاجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، مرجع سابق، ص 02
[2] نفس المرجع السابق، ص 03
[3] إلهام بن خليفة ،مرجع سابق، ص 03
[4] نفس المرجع السابق، ص 04

للقاضي الذي امر بالتجديد أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة ، و هو ما حدده المشرع في الفقرات الثالثة والرابعة والخامسة من المادة **65** مكرر **15** .

4-يشترط المشرع كذلك في المادة **65** مكرر **13** وجود تقرير مسبق يحرره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب و يتضمن العناصر الضرورية لمعاينة الجرائم[1] غير تلك التي تعرض المتسرب للخطر و ذلك من أجل أن بطّلع القاضي بشكل مفصل عن ظروف القضية و متطلباتها.

5-و حسب المشرع الجزائري و طبقا للمادة **65** مكرر فإن إجراء التسرب ، يتخذ في حالة التحقيق أو التحري في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم الفساد .

الفرع الثالث
الحماية القانونية للعون المتسرب

نتيجة لخطورة عملية التسرب على القائم بها ، كفل القانون حماية خاصة و اولاه الرعاية للحفاظ على أمن و سلامة روحه و سرية مهمته ، إذ جعل المتسرب بمنأى عن تحمل المسؤولية الجزائية عن الجرائم التي يكون قد ارتكبها عرضا أثناء تسربه تنفيذا للمهام الموكلة إليه ، و منع الكشف عن هويته الحقيقية و سمح له بأخذ هوية مستعارة ، و رتب على مخالفة هذه الإجراءات عقوبات جزائية تتضاعف إذا أفضى هذا الكشف للهوية عن تعرض المتسرب أو أحد أفراد عائلته للضرب أو الجرح او عرّض حياته للخطر و هذا ما ذكر في المادة **65** مكرر **16** ، و قد تتضاعف إذا حدثت وفاة [2].

تعد من الحماية الخاصة للمتسرب عدم جواز سماعه كشاهد على العملية مع جواز ذلك بالنسبة للضابط المسؤول و المنسق ، و إذا حدث وقع توقيف العملية أو انقضى أجلها دون تجديد فإن ضروريات حماية المتسرب تجيز له مواصلة نشاطه من دون تحمله لأي مسؤولية بشرط إخبار الجهة المختصة مصدرة الإذن ، على أن لا تتجاوز فترة تأمين سلامة المتسرب مدة أربعة أشهر قابلة للتجديد مرة واحدة[3] .

لقد أجاز المشرع في المادة **65** مكرر **14** من قانون الإجراءات الجزائية اقتناء او حيازة أو نقل أو تسليم أو إعطاء مواد أو اموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها ... . و بالتالي يمكن للعون المتسرب استعمال الأموال المتحصل عليها من ارتكاب الجرائم المذكورة بنص المادة **65** مكرر **5** من قانون الإجراءات الجزائية الجزائري و من هنا نستنتج أن هناك استثناء لأحكام نص المادة **02** من القانون رقم **05-01** المتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب و مكافحتها الذي يعتبر من العائدات الإجرامية عند عمله بها سواء بالتحويل أو النقل أو الاكتساب أو الحيازة تبييضا للأموال .

[1] عز الدين عثماني، اجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية، مجلة دائرة البحوث و الدراسات القانونية و السياسية، مخبر المؤسسات الدستورية و النظم السياسية ، العدد الرابع، 2018.ص 56

[2] إلهام بن خليفة، مرجع سابق، ص 08

[3] نفس المرجع السابق، ص 10

الفـرع الرابـع
عراقيل عملية التسـرب

يصطدم المتسرب أثناء اداء مهامه بعدة عراقيل نذكر منها :

-لا يزال التسرب الإلكتروني في الجزائر في مراحله الأولى من الناحية التطبيقية و ذلك لقلة الأحكام القضائية التي تثبت اللجوء اليه في شبكة المعلومات ، مقارنة بتشريعات أخرى ، و لربما سيكون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال دور في تفعيل هذا الإجراء[1] .

-إغفال المشرع الجزائري النص على كيفية تمويل المتسرب ، لأن المتسرب يضطر أحيانا لسد بعض المصاريف الخاصة بعملية التسرب الإلكتروني من حسابه الخاص ، و هو ما يستدعي إلى إنشاء حساب أو صندوق على مستوى الخزينة لتمويل العملية و مواجهة هذه الإشكالية[2] .

-ضرورة حماية المتسرب الذي ممكن أن يقع في إشكالية القبض عليه ، و هذا ما يتطلب توفير الحماية الكافية له عن طريق وضع نصوص قانونية تنظم هذه المسألة ومنح ضمانات أكبر له .

-يتعذر سماع المتسرب كشاهد حيث يمكن مع عصرنة العدالة استحداث تقنية جديدة للإدلاء بالتصريحات عن بعد عن طريق الشاشة الإلكترونية مع إمكانية تغيير الصوت و الصورة . [3]

المطلب الثاني
اعتراض المراسلات و المراقبة الإلكترونية

نص المشرع الجزائري على إجراء الاعتراض في المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية فنصت المادة 65 مكرر 5 على أنه إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في بعض الجرائم من بينها جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية، يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية أو اللاسلكية لذا نتساءل ماذا يقصد بالاعتراض و ما هي أحكامه ؟

الفرع الأول
مفهـــوم اعتراض المراسلات

لقد أضحت الأساليب التقليدية في البحث والتحري عديمة الجدوى بسبب استغلال منفذي الإجرام التقنيات العلمية الحديثة في تنفيذ أغراضهم الإجرامية. لذلك بات من الضروري الاستعانة بالوسائل الحديثة لكشف الجريمة والبحث عن مرتكبيها أهمها اعتراض المراسلات ، وهو وإجراء أخذ به المشرّع الجزائري و أخضعه لمجموعة من الضوابط لضمان عدم المساس بحرمة الحياة الخاصة. حيث أجاز المشرع الجزائي الجزائري لأعضاء الضبطية القضائية في إطار التحري في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، جرائم غسيل الأموال أو الإرهاب، الجرائم المتعلقة بقوانين الصرف وجرائم الفساد، بسلطة اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وهذا بموجب إذن صادر عن وكيل الجمهورية.

[1] او مدور رجاء، مرجع سابق، ص 180
[2] نفس المرجع، ص 181
[3] نفس المرجع السابق، ص 182

أولا : تعريف اعتراض المراسلات .

يعرف البعض الاعتراض بأنه عملية مراقبة سرية للمراسلات السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدلة و المعلومات حول الأشخاص المشتبه في ارتكابهم او مشاركتهم في ارتكاب الجريمة .

إذ تتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات و التي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض .
أما تسجيل الأصوات و التقاط الصور فيقصد بها تسجيل المحادثات الشفوية القائمة بين الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص ، و كذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص .

يتبين أن إجراءات اعتراض المراسلات و تسجيل الأصوات و التقاط الصور هي عبارة عن إجراءات تتخذ دون علم أصحابها في أي مكان من الأماكن العامة أو الخاصة ، و هي إجراءات تنطوي على المساس بسرية المراسلات و الاتصالات و حرمة الحياة الخاصة ، و هي من ضمن حقوق الإنسان التي كفلتها الدساتير و التشريعات العقابية و يقصد من ذلك ان السلطات القضائية يجوز لها أن تعترض و تسجل و تلتقط كل المراسلات المرسلة عبر الاتصالات إن كانت ضرورة التحقيقات تستدعي ذلك ، و على حد قول الفقه القانوني الحديث يمكن

تغليب مصلحة المجتمع في التصدي للجريمة عن المصلحة الفردية في الخصوصية و السرية لغاية تحقيق الأمن و العدالة و السلامة لهذا الفرد .[1]

و تكمن أهمية إجراء الاعتراض في كون أن التكنولوجيات المعلوماتية قادرة على نقل كميات ضخمة من البيانات في شكل نصوص أو صور أو أصوات ، فإنها في المقابل تقدم إمكانيات واسعة لارتكاب الجرائم و التي تأخذ شكل بث محتوى غير قانوني كمستند يحتوي على بيانات مزورة ، إذ أنّ مثل هذه الجرائم تفرض النقل و الاتصال ، و عليه فمن غير الممكن تحديد الوقت الفعلي لهذه البيانات غير المشروعة إلاّ من خلال اعتراض محتوى المستند ، و إن لم يتم تدارك هذه البيانات بالاعتراض سوف تقع الجريمة تامة ، و بذلك يعد الاعتراض من أهم الإجراءات التقنية اللازمة لتعقب الدليل في الجريمة المتصلة بتكنولوجيات الإعلام و الاتصال و المحافظة عليه[2]

[1] بن نعوم خالد أمين، اجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مرجع سابق، ص 100
[2] نفس المرجع السابق، ص 102

ثانيا : أحكام اعتراض المراسلات و تسجيل الأصوات و التقاط الصور .

أورد المشرع الجزائري عدّة قيود حال القيام بهذا الإجراء تتمثل في :
-يجب أن تتخذ هذه الإجراءات حيال جرائم محددة على سبيل الحصر ، و هي التي ذكرناها سابقا في التسرب و هو ما أورده المشرع الجزائري في المادة 65 مكرر 5.

-ضرورة ان تتم هذه الإجراءات بناء على إذن مكتوب من وكيل الجمهورية المختص إقليميا أو من قاضي التحقيق و تحت مراقبته المباشرة في حالة فتح تحقيق قضائي ، و هذا وفقا للمادة 65 مكرر5 ، و حسب المادة 65 مكرر 7 فإنه يجب ان يتضمن الإذن المكتوب كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها و الأماكن المقصودة ، و الجريمة التي تبرر اللجوء إلى هذه التدابير و مدتها[1].
-يجب أن يكون الإذن لمدة أقصاه أربعة أشهر قابلة للتجديد، حسب مقتضيات التحري و التحقيق ، حيث أن الإذن يكون و متضمن العناصر السابقة و مدة التجديد و هو ما جاء في الفقرة الأخيرة من المادة 65 مكرر 7.
-إمكانية الدخول إلى الأماكن العامة و الخاصة من دون علم اصحابها و موافقتهم و في كل وقت و هو ما أشار إليه المشرع في المادة 65 مكرر 5.
-حسب المواد 65 مكرر 9 ، و 65 مكرر 10 فإن القائم بالاعتراض يحرر محضرا بعد الانتهاء من هذه العملية يضمن فيه محتوى العملية و الترتيبات التقنية المتخذة ، و يذكر فيه تاريخ و ساعة بداية و نهاية العملية ، و يقوم بنسخ المراسلات أو المحادثات أو الصور المسجلة و المفيدة في إظهار الحقيقة في محضر يودع بالملف و تنسخ و تترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض[2] .

الفرع الثاني
مفهوم إجراء المراقبة الإلكترونية

من بين الإجراءات الحديثة التي نصت عليها الاتفاقيات و التشريعات الداخلية ، إجراء المراقبة الإلكترونية، و التزامات مقدمي الخدمات ، و فيما يلي سنتطرق لمفهوم إجراءات المراقبة و أحكام كل إجراء وفقا لقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها كما يلي :

أولا: تعريف إجراء المراقبة الإلكترونية.

لم يتعرض المشرع الجزائري المراقبة الإلكترونية ،ولقد تصدى الفقه لذلك وعرفها بأنها مراقبة شبكة الاتصالات ،وهو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات أو معلومات عن المشتبه

فيه، سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ ، الوقت) لتحقيق غرض أمني أو لأي غرض آخر[3].

[1] عبد الفتاح بيومي، مرجع سابق، ص102
[2] نفس المرجع السابق، ص 103
[3] جميل عبد الباقي مرجع سابق، ص 104

يتبين من التعريفين أن إجراء المراقبة الإلكترونية هو من إجراءات جمع الدليل في الشكل الإلكتروني عن المشتبه فيه ، ويقوم به مراقب ذي كفاءة عالية في المجال الإلكتروني، ويستخدم في هذه المراقبة التقنية الإلكترونية عبر شبكة الانترنيت.

والشيء المراقب هو شبكة الانترنيت ، حيث يراقب من حلالها الاتصالات الإلكترونية للمشتبه فيه التي تتم عن طريق الانترنيت ، كمراسلاته مثلا عبر البريد الإلكتروني ، والجدير بالذكر أن شرطة أمريكا الشمالية تعد قائمة بالأشخاص المشتبه بهم المبحوث عنهم توضع في ملف مركزي وترسل إلى مئات المواقع ، حيث تسمح هذه التقنية بالوضع اليومي للصور في الواجهة[1]، مما تساعد جهات البحث في عملية المراقبة، كما أن هذه الطريقة تستلهم رجال التحريات الأولية لأنها بكل بساطة تنشر عبر الأنترنيت آراء للبحث ، كما يراقب القائم بإجراء المراقبة الإلكترونية البيانات غير المشروعة.

ويتطلب مصطلح "يراقب" في المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية أن يكوم مطبقا فقط على الاتصالات التي يتم التقاطها أثناء بثها وليس الحصول على اتصالات سلكية أو الكترونية مخزنة ، أي أن المراقبة هي اكتساب معطيات في الزمن الفعلي أثناء البث بين أطراف الاتصال ، فالذي يطلع لاحقا على نسخة من اتصال مخزن لا يعد مراقبا للاتصال[2].
وتعني التقنية الإلكترونية المستخدمة في المراقبة مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وتفتيشهم وجمع

الأدلة قبلهم لإثبات إدانتهم وتقديمهم للمحاكمة ، وهناك العديد من هذه التقنيات أكدت التجارب في الولايات المتحدة الأمريكية أثرها الفعال في الرصد المبكر للاعتداءات المحتملة[3] ، كما أنها تستخدم على المستوى الدولي لمكافحة الجرائم عبر الوطنية.

يحمي المشرع الجزائري على غرار التشريعات الأخرى الحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة وذلك عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة في المادة **303** مكرر من قانون العقوبات[4] والتي جاء فيها أنه : (يعاقب بالحبس 06أشهرالى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري، كل من تعتمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.....).

[1] جميل عبد الباقي الصغير، مرجع سابق ، ص 125
[2] نفس المرجع، ص 127
[3] نفس المرجع السابق، ص 128
[4] المادة 303 مكرر من قانون العقوبات المؤرخ في 2006/12/20

ويشمل مصطلح المراسلات، الاتصالات السلكية واللاسلكية مثل المحادثات التلفونية سواء التي تتم في الهاتف الثابت أو الهاتف المحمول ، وكذا الاتصالات الالكترونية التي تشمل معظم اتصالات الانترنيت بما في ذلك مراسلات البريد الإلكتروني.

غير أن المشروع الجزائري أباح الاعتداء على هذه الحرمة بسبب وقاية أفراد المجتمع من خطورة بعض الجرائم ، وذلك في المادتين **3** و**4** من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، ومن خلال استقراء هذه المواد نجد أن المشرع أحاط هذه الإباحة ببعض الضمانات القانونية الفعالة لحماية الحرية الفردية، وحماية حق الانسان في سرية اتصالاته بمختلف أنواعها وتتمثل هذه الضمانات في :

1-إباحة المراقبة بإذن القانون :

نصت المادة **03** من القانون السابق الذكر[1] على إباحة المراقبة الإلكترونية كما يلي : (مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات ، يمكن لمقتضيات حماية النظام العام او لمستلزمات التحريات و التحقيقات القضائية الجارية ، ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية ، و في هذا القانون ، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها ...) .

2-الضرورة الملحة المرخصة لإجراء المراقبة الإلكترونية :

بالرجوع إلى نص المادة **04** [2]السابقة الذكر ووفقا للمناقشات التي دارت خلال الأعمال التحضيرية لهذا القانون يتضح أنّ ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي المبرر للمراقبة ، و من قبيل ذلك أن تكون هناك معلومات كافية تنذر باحتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع

الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ، و هناك معلومات تنتقل فضائيا تنذر بوقوع اعتداء على أمن الدولة ، و في هذه الحالة يتم الترخيص بالمراقبة الإلكترونية .

3-حصر القيام بالإجراء في جرائم إلكترونية معينة :

تنص المادة **04** من الفقرة الأولى الحالات التي تتيح اللجوء إلى عملية مراقبة الاتصالات الإلكترونية، و هي كالتالي : (يمكن القيام بعمليات المراقبة المنصوص عليها في المادة **03** أعلاه في الحالات التالية:

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

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

ج-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة...).

4-لا يتم إجراء المراقبة إلا بإذن السلطة القضائية :

[1]المادة 03 من قانون العقوبات المؤرخ في 18 صفر 1386

[2]المادة 04 من قانون العقوبات المؤرخ في 1969/09/16

حتى يكون إجراء المراقبة الإلكترونية مشروعا أو مباحا يجب أن تكون عن طريق إذن مكتوب من السلطة القضائية ، و هو ما ورد في الفقرة الثانية من المادة **4** السابقة الذكر .

و جاء في الفقرة الثالثة و الرابعة من نفس المادة على أن الحالة المنصوص عليها في البند **"أ"** من الفقرة الأولى من هذه المادة فإن النائب العام لدى مجلس قضاء الجزائر هو من يمنح الإذن بالمراقبة لمدة 06 أشهر قابلة للتجديد لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و يمنح هذا الإذن على أساس تقرير مكتوب يبين فيه طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها ، و تحصر هذه الأغراض في تجميع و تسجيل معطيات ذات صلة بالجرائم الإرهابية و الاعتداءات على أمن الدولة ، فإن لم تكن المراقبة لهذا الغرض فإنّ القائم بالمراقبة يقع تحت طائلة العقوبات المنصوص عليها في المادة **303** مكرر من قانون العقوبات السابقة الذكر[1] .

[1] بن طالب ليندا، مرجع سابق، ص 130

ملخص الفصل الثاني

بعد ما تناولنا في هذا الفصل الآليات التقليدية و البسيطة إن صحّ التعبير ، تطرقنا أيضا إلى آليات التحقيق في الجريمة المعلوماتية المستحدثة و المسايرة لهذا النمط المستجد و الأكثر خطورة ، حيث أدرجنا فيه إجراءات مادية (العامة و المألوفة) التي تقتصر فقط على المعاينة التقنية ، التفتيش و ضبط الأدلة في العالم الافتراضي و كذا الخبرة التي تخضع أحيانا لأحكام قانون الإجراءات الجزائية و أحيانا لقانون 09-04.

أما بالنسبة للإجراءات المستحدثة من طرف المشرع الجزائري فكان أولها التسرب الذي يعتبر من بين الإجراءات الخاصة التي جاء بها تعديل قانون الإجراءات الجزائية ، أيضا إجراء الاعتراض و المراقبة الإلكترونية و كذلك كل ما يتعلق بحفظ و تجميع و تسجيل الأصوات و التقاط الصور التي تكون عادة بإذن مصرح من السلطة القضائية .

خـــاتمـة

أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يسمى بالثروة المعلوماتية و هذا التطور ارتبط بظهور ما يعرف بالإجرام المعلوماتي و ذلك نتيجة الاستخدام السيء لهذه الثروة المعلوماتية الذي أصبح يهدد أمن المعطيات من جهة و حرية الأفراد و المؤسسات من جهة أخرى .

هذا ما دفع المشرع الجزائري لإنشاء قواعد قانونية تحمي حريات الأفراد و مكاسبهم المدرجة في شكل معطيات كون هذه الجرائم تتميز بصعوبة الإثبات و قبول الدليل بشأنها باعتبارها لا تترك أثرا ماديا و ملموسا كما هو الحال في الجرائم التقليدية .

و رغم المجهودات التي بُذلت و لا تزال تُبذل ، فإن هذه الإجراءات تبقى عصيبة على الحل في كثير من الأحيان في غياب استراتيجية واضحة للتعامل مع هذه الجرائم و مرتكبيها ، لأن العالم و التكنولوجيا تبقى دائما في تطور .

و مما حاولنا الوقوف عليه من خلال فصلين كاملين على جل الأحكام الإجرائية الخاصة بمتابعة مرتكبي الجرائم المعلوماتية و القواسم المشتركة بين الجريمة التقليدية و الجريمة المعلوماتية (كالمعاينة و التفتيش...).

في الأخير توصلنا إلى بعض التوصيات التي نراها قد تساهم في حل بعض الإشكاليات المتعلقة بالجريم:

- ضرورة تطوير القوانين في مجال التحقيق ; التفتيش .
- الاهتمام بالتأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم باحترافية واقتدار .
- سن قوانين صارمة تتناسب مع كل جريمة معلوماتية .
- تكثيف الجهود الدولية و الإقليمية لمكافحة هذا النوع من الإجرام .
- عدم وجود إجماع فقهي على تعريف واحد لهذه الجريمة فقد تباينت التعريفات بين المفهوم الواسع و المفهوم الضيق ، كما أن هذه الجريمة يطلق عليها عدّة تسميات من بينها : الجريمة المعلوماتية ، الجريمة السيبرانية ، جريمة الغش المعلوماتي ، الاختلاس المعلوماتي ... .
-التعاون الدولي في مجال مكافحة هذه الجريمة و تفعيله .

تلخيص المذكرة :

تعرضنا في هذه المذكرة إلى الإجراءات المستحدثة للتحقيق في الجريمة الالكترونية من خلال فصلين :

حيث تناولنا في الفصل الأول ماهية الجريمة الالكترونية التي تختلف عن الجريمة التقليدية مع ذكر تقسيماتها و خصائصها ، فالجريمة الالكترونية تتطلب مهارة و خبرة كبيرة للتعامل مع حثيثات أي واقعة و اكتشاف المجرم الالكتروني ، كما تطرقنا أيضا لتعريف هذا الأخير و كيف عالج المشرع الجزائري الجريمة الالكترونية في التشريع الجزائري .

أما الفصل الثاني تحدثنا فيه عن الآليات المستحدثة التي خصصها المشرع الجزائري لكشف خيوط و ملابسات القضية(التسرب و اعتراض المراسلات) و تقديم الفاعلين للعدالة و مكافحة هذه الظاهرة .

Dans cette note, nous avons présenté les procédures développées pour l'investigation de la criminalité électronique à travers deux chapitres :

Là où nous avons traité dans le premier chapitre de la nature de la criminalité électronique, qui diffère de la criminalité traditionnelle, en mentionnant ses divisions et ses caractéristiques, la criminalité électronique nécessite une grande compétence et expérience pour faire face aux pulsions de tout incident et à la découverte du cybercriminel. Législation algérienne.

Quant au deuxième chapitre, nous avons évoqué les nouveaux mécanismes alloués par le législateur algérien pour découvrir les fils et les circonstances de l'affaire (fuites et interceptions de correspondance) et traduire les auteurs en justice et lutter contre ce phénomène.

قائمة المراجع :

الاتفاقيات :

- اتفاقية بودابست المؤرخة في 23 نوفمبر 2001 .

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

القوانين :

- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الصادر في 16 أوت 2009.

-قانون رقم 15-03 المؤرخ في 01 فيفري 2015 ، يتعلق بعصرنة العدالة ، ج . ر ، عدد 06 ، الصادرة بتاريخ 10 فيفري 2015.

-القانون 23-06 المؤرخ في 2006/12/20.

-القانون 15-04 المؤرخ في 2004/11/10 المتمم للأمر رقم 66-155 و المتضمن قانون العقوبات " المساس بأنظمة المعالجة "

الأوامر :

-أمر رقم 66-156 المؤرخ في 08 جوان 1966 ، المتضمن قانون العقوبات ، المعدل و المتمم .

-أمر رقم 66-155 الموافق ل 08 يونيو 1966 ، المتضمن قانون الإجراءات الجزائية ، المعدل و المتمم .

الكتب و المصادر :

-أحمد حسام طه تمام ، الحماية الجنائية لتكنولوجيا الاتصالات ، دراسة مقارنة ، دار النهضة ، العربية ، القاهرة، 2002 .

-أحمد شوقي الشلقان ، مبادئ الإجراءات الجزائية في التشريع الجزائري ، ديوان المطبوعات الجامعية ، الجزائر 1999 .

-جميل عبد الباقي الصغير ، الانترنيت و القانون الجنائي ، دار النهضة العربية ، القاهرة ، 2002 .

قـــــائـــمـة المـــــــراجـــــع

-عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر و الانترنيت في القانون العربي النموذجي ، دار الفكر الجامعي 30 شارع سوتير ، الاسكندرية ، 2006 .

-نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ماجيستير في القانون الجنائي المعلوماتي ، دار الثقافة للنشر و التوزيع ، 1924ه ، 2008 م ، الطبعة الاولى ، الاصدار الاول 2008

الأطروحات و المذكرات :

-بن طالب ليندا ، الدليل الإلكتروني و دوره في الإثبات الجنائي ، دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق، جامعة مولود معمري ، تيزي وزو ، 2019 .

-أو مدور رجاء ، خصوصية التحقيق في مواجهة الجرائم المعلوماتية ، رسالة دكتوراه ، كلية الحقوق ، جامعة محمد البشير الابراهيمي ، برج بوعريريج ، 2021 .

-بخي فاطمة الزهراء ، إجراءات التحقيق في الجريمة الإلكترونية ، مذكرة ماستر ، كلية الحقوق ، جامعة المسيلة ، 2014 .

-ابتسام بقو ، إجراءات المتابعة الجزائية في الجريمة المعلوماتية ، مذكرة ماستر ، كلية الحقوق ، جامعة العربي بن مهيدي ، ام البواقي ، 2016 .

-بن نعوم خالد أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، كلية الحقوق ، جامعة عبد الحميد بن باديس ، مستغانم ، 2019 .

المداخلات :

-إلهام بن خليفة ، القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ، كلية الحقوق ، جامعة الشهيد حمة لخضر ، الوادي .

-عز الدين عثماني ، إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية ، مجلة دائرة البحوث و الدراسات القانونية و السياسية ، مخبر المؤسسات الدستورية و النظم السياسية ، العدد الرابع 01 / 2018 .

المحاضرات :

-عمارة زينب، الوقاية من الجرائم الالكترونية ، محاضرات ملقاة على طلبة سنة ثانية ماستر 02 ، كلية الحقوق، تخصص قانون اعلام آلي و انترنيت، جامعة برج بوعريريج، 2022.

الفـــــــهـــرس

الفهرس:

الفـــــــهـــرس