جامعة مولود معمري – تيزيوزو -

كلية الحقوق والعلوم السياسية

قسم الحقوق

التحقيـق الجنائــي في الجرائم الإلكترونية

مذكرة لنيل شهادة الماستر في القانون

تخصص القانون الجنائي والعلوم الجنائية

إعداد الطالبة **تحت إشراف**

بن عنطر سيهام **د/ علي أحمد رشيدة**

لجنة المناقشة

أ.د/ داودي ستيتي أونيسة، أستاذة، جامعة مولود معمري، تيزي وزو.....رئيسة.

د/علي أحمد رشيدة،أستاذة محاضرة "أ" جامعة مولود معمري، تيزي وزو..مشرفة ومقررة.

د/ تاجر كورابا كريمة، أستاذة محاضرة "ب"، جامعة مولود معمري تيزي وزو.....ممتحنة.

تــاريخ المنـــاقشــة:2023/10/12.

بسم الله الرحمن الرحيم

كلمة شكر

عن أبي هريرة رضي الله عنه أنّ النبيّ صلى الله عليه وسلّم قال: «لا يشكر الله من لا يشكر النّاس»، فالحمد لله الذي أنار لنا الطريق إلى العلم وأعطانا الصبر والقوّة لإتمام هذا العمل المتواضع.

وعليه أتوجه بجزيل الشكر والامتنان إلى الأستاذة الكريمة "علي أحمد رشيدة" لقبولها الإشراف على هذه المذكرة والتي لم تبخل علي بإرشاداتها القيمة وتوجيهاتها لإثراء هذا العمل.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه المذكرة.

ولا أنسى بالشكر كل من قدّم لي يد العون من قريب أو من بعيد في إنجاز هذا العمل.

سيهـــام

إهـــداء

الحمد لله الذي أنار لنا طريقنا وكان لنا خير عون، إلى من فضلهما الله عن باقي النّاس مرتبة فأمر بعد عبادته وحده طاعتهما و الإحسان إليهما.

إلى حيث لا تخلو الحياة إلاّ بجوارهما، إلى من لا أقدر على رد جميلهما ولو عملت لهما طول الحياة.

أهدي ثمرة جهدي وعملي إلى من أخفضه جناح الذل من الرحمة، إلى والدي الكريمين وألتمس منهما الرضا والعفو.

إلى إخوتي وأخواتي وإلى جميع الأصدقاء.

سيهـــام

مقدمـــة

مقـــــدمة

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من النمو الفكري والمعرفي وهذا بفضل التطوّر الهائل الذي شهدته كل من مجال تقنية المعلومات ومجال الاتصالات والاندماج المذهل الذي وقع بينهما شيئًا فشيئًا، بحيث أصبحت مختلف القطاعات تعتمد في أداء عملها بشكل أساسي على اِستخدام الأنظمة المعلوماتية لما تتميّز به من عنصري الدقة والسّرعة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدّة دول.

ولكن على الرغم من المزايا الهائلة التي تحققت وما زالت تتحقق يوما بعد يوم على جميع الأصعدة وفي شتى الميادين، إلاّ أنّ الاستخدام المتنامي لهذه التقنيات انطوى في الوقت ذاته على جملة من الانعكاسات السلبية جراء الاستخدام السيّئ والمفرط والغير مشروع مما ألحق الضرر بمصالح الفرد والجماعة، حيث أصبحت محلا لارتكاب الجرائم الشيء الذي أدى إلى ظهور ظاهرة إجرامية حديثة سميت بجرائم تقنية المعلومات أو الجرائم الإلكترونية التي تعد من أخطر وأعقد الجرائم على الإطلاق، فهي جريمة سرية تقنية سهلة الارتكاب وصعبة الإثبات تنشأ في الخفاء وفي بيئة إلكترونية افتراضية ترتكب باستخدام الحاسب الآلي وشبكات الإنترنت، ويقترفها أشخاص يتمتعون بالذكاء وبمهارات وخبرات تقنية عالية يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات، فضلا على أنها جريمة عابرة للحدود عبر شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم، وبالتّالي إنّ التحقيق في مثل هده الجرائم وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة والتي تتطلب أسلوب تحقيق مختلف عن الجرائم التقليدية، فبعد أن كان الطابع الإجرائي التقليدي القائم على العنف والتعذيب الطريقة الوحيدة للكشف عن الجريمة واستنباط الدليل، ظهر طابع إجرائي حديث قائم على الاستعانة

بالتكنولوجيا واستخدام شبكة الإنترنتوهوالطابع المميّز لأساليبالتحقيق حيثتطورتوسائلالبحث والتحري في عصر المعلوماتية تطورا ملحوظا يواكب حركة الجريمة وتطور أساليب ارتكابها.

أهمية الدّراسة:

تنبع أهميةالدراسة من خطورة الجريمة الالكترونية في حد ذاتها والخصائص التي تتميز بها عن باقي الجرائم التقليدية وفي صعوبة التعامل معها وإثباتها، وكذا من الطرق والأساليب الإجرائية ذات الطبيعة التقنية التي تلائمها سواءً الوطنية منها أوالدولية.

أهداف الدراسة:

تهدف دراستنا إلى تحديد ماهية التحقيق الجنائي في الجريمة الإلكترونية وكذا بيان الجهود الوطنية والدولية في مواجهة هذا النّوع من الإجرام ما دفعناإلى البحث عن نجاعة الأساليب والطرق المستعملة في التحقيق الالكتروني من طرف الهيئات المختصة والأجهزة المكلفة بالعملية في مكافحة الإجرامالمعلوماتيمن خلال الإشكالية التالية: "ما مدى فعالية إجراءات التحقيق الوطنية والدولية في الكشف عن الجرائم الالكترونية؟".

نظرًا لخصوصية الموضوع وطبيعته القانونية التي تفرض المنهج المتبع فقد اخترنا أن نتبع منهجا يلم إلى حد ما بدراسة هذا الموضوع من مختلف جوانبه ألا وهو المنهج الوصفي التحليلي الذي يقوم على وصف هذه الظاهرة الإجرامية المستحدثة، وتحليل المواد التي تناولتها.

ولنتمكن من معالجة الموضوع والإجابة على الإشكالية المطروحة ارتأينا إلى تقسيم الخطة إلى التقسيم الثنائيحيث تناولنا في الفصل الأولالأحكام الموضوعية للتحقيق في الجريمة الالكترونيةاذ تطرقنا من خلاله إلى الجريمة الالكترونيةوالتحقيق فيها فيالمبحث الأول، وفي المبحث الثانيالهيئات المختصة بالتحقيق في الجريمة الإلكترونية، فيما خصصنا الفصل الثاني للإطارالإجرائي من خلال دراسة الأساليب الوطنية للتحقيق في الجريمة

الالكترونية في المبحث الأولوالأساليب الدولية للتحقيق في الجريمة الالكترونية المبحث الثاني.

الفصل الأوّل

الأحكام الموضوعية للتحقيق فيالجريمة الالكترونية

تعدّ الثورة التكنولوجية من أهم التطوّرات التي يعيشها العالم اليوم لاسيما ثورة الاتصالات، حيث ساعدت هذه التكنولوجيا على تطوّر العديد من الميادين، إلا أنّها في المقابل عرفت العديد من الانعكاسات السلبية ممّا أدى إلى انتشار ظاهرة خطيرة على المجتمعات وعلى أمنها واستقرارها تعرف بالجريمة الإلكترونية، حيث صنفت هذه الأخيرة على أنها من أخطر الجرائم المعاصرة، وذلك من منطلق الخصائص التي تمتاز بها عن الجرائم التقليدية من حيث الدقة والتقنية العالية في ارتكابها وكذا صعوبة اكتشافها وبالتالي التحقيق فيها.وعلى ضوء ذلك قسمنا هذا الفصل إلى مبحثين نتناول في أولهما الجريمة الالكترونية والتحقيق فيها فيما خصصنا الثاني للأجهزة المكلفة بالبحث والتحري في هذه الجريمة.

المبحث الأوّل

ماهية التحقيق الجنائي في الجريمة الالكترونية

للتحقيق أهمية في إثبات الجرائم وإقامة الدليل على مرتكبيها على اختلاف أنواعها، وهو كما يدل عليه اسمه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم، ولكي نتعرّف على التحقيق الجنائي في الجريمة الالكترونية سنتطرق الى تحديد مفهومها من خلالا لمطلب الأول ثم سنتناول التحقيق الجنائي في الجريمة الإلكترونية في المطلب الثاني.

المطلب الأوّل

مفهوم الجريمة الإلكترونية

ظهرت عدّة تعريفات حول الجريمة الإلكترونية منها المضيق ومنها الموسع، كما تعدّدت المصطلحات المستخدمة للدلالة عليها، فالبعض استخدم مصطلح جرائم الحاسب الآلي أو جرائم المعالجة الآلية للمعطيات، والبعض الآخر استخدم مصطلح الإجرام المعلوماتي أو الإجرام السيبيراني، في حين هناك من فضل تسمية جرائم المعلوماتية، وهناك من وجد تسمية جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال أكثر دلالة ومواكبة للتطوّر الذي يشهده عالم الإعلام والاتصال، وهذا المسمى استخدم في مشروع القانون العربي النموذجي الموحد الصادر عن جامعة الدول العربية سنة 2004، والذي اعتمد عليه مجلس وزراء الدول العربية في الدورة التاسعة عشر بموجب القرار رقم 495-19 المؤرخ في 2003/10/08.[1]

[1]- د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007، ص 38.

- نظر أيضًا مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، القاهرة، 2008 ص 112.

الفرع الأوّل

تعريف الجريمة الإلكترونية

تعدّ الجرائم الإلكترونية من الجرائم المستحدثة التي ظهرت في عصرنا الحالي، وسميّت بالجرائم الإلكترونية نظرًا لكونها ترتكب باستخدام الحاسب الآلي والتقنية الإلكترونية، كما أنّ الفعل الإجرامي يرتكب في بيئة معلوماتية رقمية أو إحدى شبكات المعلومات.

وعليه فقد تم تعريف الجريمة الالكترونية على أساس عدة معايير بالاستناد إمّا على وسيلة ارتكابها، أو موضوعها، أو على أساس المعرفة الفنية باستخدام الحاسوب، وقد يستند البعض الآخر على أكثر من معيار لتعريفها وهذا ما سوف نراه في النقاط التالية:

أولا: تعريف الجريمة الإلكترونية

1- التعريف الفقهي:

لقد اختلف الفقهاء حول تعريفهم للجريمة الإلكترونية، حيث اعتمد كلّ اتجاه على معيار معيّن في ذلك:

أ- تعريف الجريمة الإلكترونية بالاستناد إلى معيار وسيلة ارتكابها:

يستند أنصار هذا الاتجاه في تعريفهم للجريمة الإلكترونية على وسيلة ارتكابها، فيشترطون وقوعها بواسطة الكمبيوتر، فعرّفوها بأنّها: «كل أشكال السلوك الغير مشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي».

كما عرّفها (رودن أدريان) على أنّها «كل جريمة تتم في محيط الحاسبات الآلية»[1].

ب- تعريف الجريمة الإلكترونية بالاستناد إلى المعرفة الفنية باستخدام الحاسوب:

لم يستند أنصار هدا الاتجاه في تعريفه للجريمة الالكترونية على الوسيلة أو موضوع الجريمة الإلكترونية، وإنّما استندوا على المعرفة الفنية أو التقنية باستخدام الحاسب الآلي

[1]- Rodin Adrian. Computer crime and the law.CLT. 1991? Vole 15, p 399.
"Every crime takes place around computers"

بمعنى آخر أنّ أنصار هذا الاتجاه يستندون إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنيات المعلومات واستخدام الحاسب الآلي حيث عرّفوا هذا النوع من الجرائم بأنّها «أيّة جريمة يكون متطلبًا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب».

ويؤخذ على هذا الاتجاه أنه يضيق من نطاق الجريمة الإلكترونية لأنّه وبحسب رأي المنتقدين له فإنه يحصر الجريمة في نطاق المعرفة الفنية لمرتكبها وهذا يمكن وقوعه في حالات معينة وليس في جميع الحالات، إذ يرتكب الجاني الجريمة الإلكترونية دون الحاجة إلى قدر كبير من المعرفة والخبرة الفنية، كعملية إتلاف البيانات المخزنة مثلا فتعتبر من الأفعال الغير مشروعة التي لا تتطلب مهارة وقدر كبير من العلم والمعرفة لارتكابها.

كما يلاحظ أن هذه الجرائم في بعض الأحيان ترتكب من قبل مجموعات تتوزع أدوارهم بين التخطيط والتنفيذ والتجهيز والمساهمة، وقد لا تتوفر في بعضهم المعرفة بتقنية المعلومات والتي يطرح بشأنها تساؤل حول معايير تحديد المعرفة التقنية للقول بارتكاب الجريمة؟[1].

ج- تعريف الجريمة الإلكترونية بالاستناد إلى موضوعها:

يستند أصحاب هذا الاتجاه في تعريفهم للجريمة الإلكترونية إلى وجوب أن يكون الكمبيوتر محلاً للجريمة، فيجب أن يتم الاعتداء على الحاسب الآلي أو على نظامه، كأن يتم سرقة أو تقليد أو إتلاف أو تعطيل برنامج الحاسوب أو إفشاء محتويات أو حذف أو تغيير أو تزوير أو نسخ المعلومات المعالجة،حيثعرفوا الجريمة الالكترونية بأنّها «نشاط غير مشروع موجّه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوّل عن طريقه[2].

[1]- نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في العلوم القانونية، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2022، ص 18.

[2]- المرجع نفسه، ص 18.

فبالنظر إلى الموضوع محل الاعتداء نجد: الجرائم الإلكترونية الواقعة على الأشخاص، و الجرائم الإلكترونية الواقعة على الأموال:

1- **الجرائم على الأشخاص:** عادة ما تحصى ثلاث (03) أنواع منها وهي:

- جرائم القذف والسّب عبر الانترنت.
- جرائم الاعتداء على حرمة الحياة الخاصة.
- جرائم المخلة بالآداب العامة مثلا: الاستغلال الجنسي للأطفال عبر الانترنت.

2-الجرائم الواقعة على الأموال:

أما بالنسبة للجرائم الواردة على الأموال فهناك مثلا:

- جرائم التجارة الإلكترونية.
- سرقة المال المعلوماتي المعنوي عبد الانترنت.
- جرائم التحويل الإلكتروني غير المشروع للأموال عبر الانترنت.
- الجرائم المتكلفة بانتهاك حق المؤلف والحقوق المجاورة.
- جريمة الاعتداء على النظم المعلوماتية، أو جرائم إتلاف المعلومات الإلكترونية أو جرائم إتلاف النظم المعلوماتية عبر الإنترنت[1].

2- التعريف القانوني:

لا يوجد في التشريع الجزائري تعريف مباشر للجرائم الإلكترونية بهذه التسمية، لكن عرّفها القانون المتعلّق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

1 سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر 2011، ص20.

2 نادية حسان، محاضرات مادة الحماية الجنائية للنظم المعلوماتية، لطلبة ماستر القانون الجنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2021- 2022، ص 13.

والاتصال ومكافحتها[1] تحت تسمية -**الجرائم المتصلة بتكنولوجيات الإعلام والاتصال**: Les crimes liées aux technologies de l'information et de la communicationو ذلك بموجب المادة 02 منه التي تنص على أنّها: «**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات، أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية**».

مع العلم أنّه طبقا للمادة نفسها يقصد بالمنظومة المعلوماتية: «**... أي نظام منفصل أو مجموعة من الأنظمة الم.... ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين**". أماالاتصالات الإلكترونية Les communications électroniquesفهيطبقا لنفس المادة«**أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة إلكترونية**»[2].

يلاحظ من خلال هذا التعريف:

- أنّ المشرع قد اعتمد على معيار الجمع بين عدّة معايير لتعريف الجريمة الإلكترونية أوّلها هو معيار وسيلة ارتكاب الجريمة، وثانيها معيار موضوع الجريمة، وثالثها معيار القانون الواجب التطبيق والركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.
- كما حدّد نطاق الجريمة الإلكترونية وذلك من خلال إقراره بأنّ الجريمة الإلكترونية ترتكب في نظام معلوماتي، وهذا ما يوّسع من مجال الجرائم الإلكترونية في **القانون الجزائري**[3].

3 القانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، عدد 47 الصادر في 16 أوت 2009.

[2]- نادية حسان، المرجع السابق، ص 06.

[3] - نادية حسان، مرجع سابق، ص7 .

ثانيا أطراف الجريمة الإلكترونية:

لقيام أية جريمة بصفة عامة يتطلب من جهة وجود الشخص أو الطرف القائم بالنشاط الإجرامي المسمى بالمجرم، ومن جهة أخر بالطرف المستهدف من خلال النشاط الإجرامي والمسمى بالضحية، والأمر نفسه ينطبق على الجريمة الإلكترونية، حيث نجد ما يسمى بالمجرم الإلكتروني وكذا الضحية في الجريمة الإلكترونية.

1/- المجرم الإلكتروني.

اِنطلاقًا من فكرة أنّ الجريمة في تطوّر مستمر وأنّ الإجرام ليس له حدود، فإنّ التطوّر التكنولوجي في مجال الاتصالات والمعلوماتية أفرز لنا صنفا جديدًا من المجرمين والّذي يسمى ب "المجرم الإلكتروني" والذي يتميّز عن المجرم التقليدي أو المجرم في الجرائم بصورتها التقليدية من حيث صفاته وخصائصه وكذا من حيث دوافعه.

فالمجرم الإلكتروني يتمتع بعدّة ميزات يستخدمها من أجل ارتكاب الجريمة الإلكترونية، هذه الميزات تتنوع وتتعدد باختلاف درجة ومستوى المجرم الإلكتروني إذ كان مبتدئًا أو محترفًا للإجرام الإلكتروني ومن أبرز هذه السمات نذكر منها:

1- تمتع المجرم الإلكتروني بالذكاء المعلوماتي.

2- تخصص المجرم الإلكتروني في ميدان الإجرام المعلوماتي.

ودوافع المجرم الإلكتروني تختلف كما قلنا سابقًا حسب مستوى ووعي المجرم الإلكتروني وأنواعه[1].

فمن بين أنواع المجرمين الإلكترونيين نجد:

- **الهاكرس** Les Hackers: وهم أشخاص مولعين بالمجال المعلوماتي، يرتكبون الجرائم الإلكترونية من باب اللّعب أو بهدف الحصول على الشهرة.

[1]- إسماعيل بن يحي، التحقيق الجنائي الإلكتروني، أطروحة دكتوراه علوم في القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، 2021، ص 231.

- **الكيدس** Les Kids: هؤلاء ليسوا بعباقرة في المجال المعلوماتي، فغالبا ما يكونون أطفال أو مراهقين يحسنون استعمال المعلوماتية فيرتكبون جرائم إلكترونية دون الانتباه إلى خطورة أفعالهم، فهدفهم التسلية أكثر مما هو إجرامي.

- **المافيا** La mafias.

- **جماعات المجرمين** Les groupes criminels:فهؤلاء المجرمين الإلكترونيين تتعدد الأسباب التي تدفعهم إلى ارتكاب الجريمة الإلكترونية، فمنها الرغبة في الحصول على المعلومات، أو مكاسب مالية وذلك بسرقة معلومات وإعادة بيعها، ومنها الرغبة في الإحساس بالقوّة من باب النرجسية أي إثبات التمتع بالذكاء الخارق، ومنها بدافع الابتزاز والإساءة لدولة ما، وإلى غير ذلك من الدوافع التي تشكل باعثا للمجرم الإلكتروني[1].

كما يظهر من خلال المادة 394 مكرر4 من قانون العقوبات المجرم في هذه الجريمة قد يكون شخص طبيعي كما قد سبق وأن ذكرنا، كما قد يكون شخص معنوي حيث تنص على أنه: «**يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم....**» وهذا الأخير يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

2/- الضحية الإلكترونية.

بعد أن تعرفنا على المجرم الإلكتروني كأحد طرفي الجريمة الإلكترونية، سنتعرض الى الطرف الثاني في الجريمة الالكترونية والذي يسمى بالضحية، وما سينبغي التوقف عنده، هو أنّ الضحية في هذه الجريمة لا تقتصر فقط على المجني عليه وإنّما تمتد لتشمل كل متضرر من الجريمة الإلكترونية.

[1]- أ. نادية حسان، المرجع السابق، ص 10.

فقد يقع ضحية لجريمة إلكترونية أشخاصًا طبيعية أو أشخاصا معنوية[1]، وذلك في صورة مؤسسات وشركات، سواء أكانت عامة أو خاصة، وعلى هذا الأساس سوف نتطرق إلى التعرّف على هاتين الفئتين من ضحايا الجريمة الإلكترونية في نقطتين

أ/ -الشخص الطبيعي كضحية في الجريمة الإلكترونية:

لقد أدت كثرة استخدام الأفراد للحاسب الآلي والهواتف الذكية إلى ارتفاع حالات الاعتداءات على النظام المعلوماتي، خصوصًا في ظل الإقبال المتزايد على الخدمات التي توفرها شبكة الانترنت والذي يبلغ أحيانًا إلى حد ما من الإدمان، حيث أصبح سهلا على المجرم الإلكتروني اِصطياد ضحاياه، إذ يستهدفهم مباشرة من خلال قرصنة حواسبهم أو هواتفهم أو من خلال اختراق برديهم الإلكتروني وتلك الحسابات التي ينشئها الأفراد داخل العالم الافتراضي لاسيما بمناسبة إقبالهم على شبكات التواصل الاجتماعي والتي أضحت ملاذًا للقرصنة والتشهير بالأفراد من خلال نشر صورهم وإتاحتها للجمهور، أو من خلال الابتزاز بالضحايا عن طريق التهديد بنشرها مقابل الحصول على فوائد معينة قد تكون في أغلب الحالات مالية[2].

والملاحظ أنّه في كثير من الحالات لا يبادر الضحايا إلى الإبلاغ عن هذه الجرائم خشية على سمعتهم داخل الأسرة والمجتمع، الأمر الذي لا يساعد على مكافحة الجريمة الإلكترونية ويجعل الجناة يفلتون من العقاب، بل أن عزوف الضحايا عن التبليغ يشجع الجناة على مواصلة تخاطبهم الإجرامي واصطياد ضحايا آخرين.

كما أنّه في بعض الأحيان وبعد تردّده قد يبادر بعض الأفراد إلى التبليغ عن هذه الجرائم لكن بشكل متأخر، الأمر الذي يعيق جهات التحقيق من تتبع الجاني خاصة وأنّ

[1]-القانون رقم 15/04 المؤرخ في 25 ديسمبر 2004، المعدل والمتمم للأمر رقم 66/ 156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات، جريدة رسمية العدد 71، صادر بتاريخ 2004/11/10 معدل ومتمم.

[2]- إسماعيل بن يحيى، المرجع سابق، صص 34-35.

الجرائم الإلكترونية تتطلب سرعة اتخاذ الإجراءات نظرًا لطبيعتها ولما تتميّز به من خاصيات تشكل عقبات أمام جهات التحري والتحقيق.

ب/ -الشخص المعنوي كضحية في الجريمة الإلكترونية:

تشكل الجرائم الإلكترونية خطرا كبيرا على الأشخاص المعنوية، سواء تعلق الأمر بالأشخاص المعنوية الحكومية أو الخاصة، ذلك أنّها تستهدف عددا من الضحايا دفعة واحدة أو تمس بمصلحة من المصالح الحيوية للدولة، إذ ما تعلّق الأمر بمنشآت حساسة كتلك المتعلقة بالدفاع والأمن الوطنيين.

إنّ ما ذكرناه سابقًا عن إحجام الأفراد أو الأشخاص الطبيعية عن التبليغ عند وقوعهم ضحايا للجريمة الإلكترونية، ينطبق كذلك على تلك الحالات التي يكون فيها الضحايا من الأشخاص المعنوية والتي تكون فيها المؤسسات المالية والبنوك أكثرالأشخاص المعنوية عزوفًا عن التبليغ وذلك خشية فقدان ثقة العملاء والزبائن بها، فتفقد بالتالي سمعتها وقيمتها بين المنافسين، لذلك تعمدت الكثير من البنوك إلى التستر على تلك العمليات التي تتعرّض لها أنظمتها المعلوماتية من قرصنة وإتلاف وتجسس وغيرها من الجرائم الإلكترونية[1].

الفرع الثاني

أركان الجريمة الالكترونية

لقيام الجريمة الالكترونية لابد أن تقوم على ثلاثة أركان كغيرها من الجرائم التقليدية والمتمثلة في **أولا/ -الركن الشرعي**

يتمثل الركن الشرعي في النصوص القانونية التي تجرم الفعل،حيث أورد المشرع الجزائري قسما خاصا لجرائم المساس بأنظمة المعالجة الآلية للمعطيات،وهو القسم السابع مكرر من قانون العقوبات[2].

[1]- إسماعيل بن يحيى، المرجع السابق، صص 35-36.

[2]- الأمر رقم 66-156 يتضمن قانون العقوبات ،مرجع سابق

ثانيا/ -الركن المادي

يتمثل الركن المادي للجريمة الالكترونية في:

-الاعتداء على نظام المعالجة الآلية للمعطيات:ويكون بصورتين.

أ-الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات: تتضمن جريمتي الدخول والبقاء غير المرخص بهما في النظام.

أ-1 الدخول غير المرخص: يقصد بفعل الدخول هنا ذلك الدخول الالكتروني باستعمال الوسائل الفنية و التقنية إلى النظام المعلوماتي،ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص وهو ما نصت عليه المادة 394 مكرر من قانون العقوبات الجزائري التي تنص على أنه يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة(1) و بغرامة من 50.000 دج إلى 200.000دج كل من يدخل أو يبقى عن طريق الغش في كل،أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك[1].

يلاحظ من هذه المادة أن المشرع الجزائري اعتبر جريمة الدخول غير المرخص به جريمة شكلية لا تشترط لقيام ركنها المادي تحقق النتيجة الإجرامية، أي أنه اكتفى بفعل الدخول إلى نظام المعالجة الآلية للمعطيات بكامله أو إلى جزء منه فقط.

أ-2 البقاء غير المرخص: يقصد بالبقاء غير المرخص به في نظام المعالجة الآلية للمعطيات استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السلطة عليه، حيث اعتبر المشرع الجزائري حسب المادة 394 مكرر أعلاه هذا الفعل جريمة مثلها مثل جريمة الدخول غير المرخص به وحدد لها نفس عقوبة هذه الأخيرة.

ب-الصورة المشددة للاعتداء على المعطيات الداخلية للنظام:وتتخذ أحد الشكلين التاليين:

1-جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري، مجلة نقدية للقانون و العلوم السياسية، العدد 2، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو ،2016 ،ص-ص126-135.

ب-1 الاعتداء على المعطيات الداخلية للنظام: لقد حدد المشرع شكل الاعتداء على معطيات النظام الداخلية على سبيل الحصر من خلال المادة 394 مكرر 1 التي تنص على أنه يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 50.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

يتضح من خلال هذه المادة أنه لا يشترط اجتماع هذه الأفعال الثلاثة لقيام الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة بل يكفي أن يصدر عن الجاني إحداها فقط.

ب-2 الاعتداء على المعطيات الخارجية للنظام: ويقصدبها تلك المعطيات التي لها دور في تحقق نتيجة معينة، حيث نص عليها المشرع في المادة 394 مكرر 2.[1]

أما الاعتداء هنا فيقصد به ذلك الاعتداء الذي يهدف إلى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو بسلامة محتوياتها بكاملها أو بتعطيل قدرة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم، ويتحقق عندما يترتب عن فعل الدخول أو البقاء نتائج غير مشروعة ضد النظام مثل الحذف أو التخريب أو التغيير.

ثالثا /-الركن المعنوي

تعتبر الجريمة الالكترونية جريمة عمديه تقوم على القصد الجنائي ولتوفر هذا الأخير لابد أن يكون الجاني على دراية بكافة عناصر الجريمة وله علم بأن الفعل الذي يقوم به ينصب على هذا النظام بما يتضمنه من معطيات وبرامج.

الفرع الثالث

خصائص الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة التي ظهرت جراء التطوّر في مجال الاتصالات والإعلام،وهي تتميز عن الجرائم التقليدية بمجموعة من الخصائص التي أثرت

[1]-راجع نص المادة 394 مكرر2من الأمر رقم 66-156 المعدل والمتمم، مرجع سابق.

بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة. وأمام صعوبة إيجاد تعريف دقيق لها، فقد تساعد خصائصها على تحديد معالمها لفهمها جيدًا، وعليه سوف نحاول أن نبرز أهم هذه الخصائص فيما يلي: **أولا : الجريمة الإلكترونية مرتبطة بالحاسب الآلي و شبكته.**

يلعب الحاسب الآلي دورًا مهمًا ومحوريا في الجريمة الإلكترونية، فقد يكون هدفا للجريمة (مثلا في قرصنة البرامج أو وضع فيروس...الخ)، وقد يكون أداة لارتكاب الجريمة أو البيئة التي ترتكب فيها، فقد تكون المعلوماتية هي وسيلة للغش والتحايل أو تكون محل للاعتداء.

ومن ثم من الضروري التعريف بالحاسب الآلي أو الحاسب الإلكتروني باللغة العربية أو Ordinateur باللغة الفرنسية أو Computer باللغة الإنجليزية، وتستعمل هذه الكلمة في اللغتين السابقتين أيضا.

فالكمبيوتر «هو جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية طبقا للتعليمات المعطاة له بسرعة كبيرة تحل عشرات الملايين من العمليات الحسابية»[1].

أمّا شبكات الحاسب الآلي باللّغة العربية، وباللّغة الفرنسية les réseaux informatiques وComputer net Works باللغة الإنجليزية. فيقصد بها «...اِتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيًا أو لا سلكيًا، أو هي حزمة من أجهزة الحاسب المتصلة معا، وقد تكون الأجهزة موجودة في نفس الموقع، فتسمى شبكة محليةLocal ... net work أو قد تكون موزعة في أماكن متفرقة ويتم ربطها عن طريق خطوط التليفون، وتسمى في هذه الحالة بالشبكة واسعة النطاق أو الممتدة Wilde area net Word ومنها شبكة الانترنت التي تلزم للدخول إليها جهاز حاسوب ومودع modem بالإضافة إلى خط تليفوني...».

[1]- أ. نادية حسان، المرجع السابق، ص 09.

يجب أن يقع الاعتداء على الحاسب الآلي وشبكات أو بواسطتها (أي أن الحاسب الآلي وشبكاته يعتبران وسيلة للاعتداء) أما بخصوص الشبكة فأكثرها استعمالا هي الإنترنت وهي كلمة انجليزية متكونة من كلمتين: internationalأي دوليNet Works أي شبكة[1].

ثانيًا: الجريمة الإلكترونية جريمة عابرة للحدود.

من أهم الخصائص التي تميّز الجريمة الإلكترونية أنّها جريمة تتخطى الحدود الجغرافية، حيث وسعت شبكات المعلومات عملية الاتصال وتبادل المعلومات بين الدولة والأنظمة التي يفصل بينها آلاف الأميال.

ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية ارتكاب الجريمة الإلكترونية في أماكن متعدّدة من العالم وفي الوقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقع فيها الجاني[2].

فمن خلال هذه الخاصية الدولية يثار إشكال حول الاختصاص القضائي في محاكمة الجاني، بمعنى آخر ما هي الدولة المختصة بمحاكمة هذا الأخير؟ حيث أنّ هذه الجريمة لا تقع في دولة واحدة ولا تعترف بالحدود الجغرافية للدول فقد يكون الجاني والمجني عليه والضرر في بلدان مختلفة.

ومن أهم القضايا التي أكدت هذه الخاصية، قضية عرّفت باسم مرض نقص المناعة المكتسبة "الإيدز" وتتلخص وقائعها في انه عام 1989، حيث قام أحد الأشخاص المدعو "جوزيف" بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح لمرض نقص المناعة المكتسبة، إلاّ أنّها كانت في الحقيقة تحتوي على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يطلب الفاعل من خلالها مبلغ مالي يرسل إلى عنوان معيّن حتى يتمكن

[1]- أ. نادية حسان، المرجع السابق، ص 09.

[2]- د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، مصر،2008،ص 20.

المجني عليه أو الضحية إن صح التعبير من الحصول على مضاد الفيروس، وفي 03 فيفري 1990 تم إلقاء القبض عليه، وهنا تثير هذه الخاصية أي خاصية عالمية الجريمة الإلكترونية كما قلنا سابقًا عدّة أثار قانونية أهمها القانون الواجب التطبيق عليها والقضاء المختص بها[1].

ثالثًا: الجريمة الإلكترونية صعبة الإثبات.

إنّ الجرائم الإلكترونية جرائم فنية، تتم عن طريق نقل معلومات مخزنة، أو حتى تدميرها، بحيث تمتاز هذه الجرائم بصعوبة الاكتشاف والإثبات وذلك نظرًا لعدم ترك الجاني آثار تدل على إجرامه، ممّا يجعل التحقيق فيها صعب جدًا، وتتطلب من الشرطة التي تقوم بالتحقيق التحكم في مجال الحاسب الآلي وشبكته، وفي القانون الوطني والدولي[2]. فلكون هذه الجرائم تتم بواسطة إدخال أرقام ورموز دقيقة يصعب اكتشافها وإثباتها [3]، ذلك أنّ هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام وإنّما هي معلومات وبيانات تغيّر أو تعدّل أو تمحى كليًا وجزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي فلا تترك أثرًا خارجيًا مرئيًا أو ملموسًا فهي كما وصفها بعض الفقهاء بأنّها جريمة هادئة بطبيعتها لا تتطلّب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سيرتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها.

فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودًا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها أو إدانة مرتكب الجريمة بها، وإنّما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية، ولكون أنّ

[1]- عادل يوسف عبد النبي الشكري، الجريمة الإلكترونية وأزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، عمان، 2008، ص ص112- 113.

[2]- أ. نادية حسان، المرجع السابق، ص 11.

[3]- عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماستر تخصص علوم جنائية كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة،2012 ن2، ص 88.

أمر طمس الدليل ومحوه كليا من قبل الفاعل في غاية السهولة وفي زمن قصير جدًا، ومن يتعذّر عليه إن لم يكن مستحيلا ملاحقة وكشف شخصية الجاني خاصة في حالة تفتيش الشبكات، كما قد تكون البيانات المراد البحث عنها مشفرة ولا يعرف شفرة دخوله إلاّ أحد العاملين على الشبكة[1].

فالبعض ذهب للقول بأنّ صعوبة اِكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضًا إلى عدّة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنّها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التكامل معها، إذ أنها تتطلب إلمامًا خاصًا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحظة مرتكبيها، فأحيانًا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم.

المطلب الثاني

مفهوم التحقيق الجنائي في الجريمة الإلكترونية

أصبحالتحقيق عنصر مهم لدى جميع الشركات والدوائر الحكومية في الوقت الحاضر، فكثير من الدول المتقدمة تبذل قصارى جهدها في دعم هذا المجال من ناحية الأبحاث والدراسات مما يعكس أهميته وتعتمد عليه في عملية التحقيق والإثبات بالأدلة والبراهين على ارتكاب الجريمة الإلكترونية، كما أصبح التحقيق الجنائي الرقمي الآن مطلب أساسي لأية جهة لتدريب موظفيها المختصين لأساليب التحقيق الجنائي خاصة مع ارتفاع هذا النوع من الجرائم وسوف نتعرّف أكثر على التحقيق الجنائي والمحقق الجنائي من خلال الفرع الأول، ثم استخلاص خصائصه في الفرع الثاني.

[1] -إبتسام بوعباية، التحقيق في الجريمة الإلكترونية، مذكرة ماستر في الحقوق، قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريرج، 2022، ص 17.

الفرع الأوّل

تعريف التحقيق الجنائي والمحقق فيه

أولا/- تعريف التحقيق الجنائي

تتعدّد وتتنوّع تعاريف التحقيق الجنائي إلاّ أنّ مضامينها واحدة، وهو البحث والتنقيب عن الأدلة التي تفيد في الكشف عن الحقيقة سواء بالنفي أو الإثبات[1].

أ/-التعريف اللّغوي والاصطلاحي للتحقيق الجنائي:

1-التحقيق لغة:

هو التصديق والتأكيد أو التثبيت، يقال في اللغة حققت الأمر أي أثبته وصدقه، ويقال حقق الظن وحقق القول والقضية وحقق الثوب، أي أحكم نسجه وصنع الثوب صنعا تحقيقا متبعًا، وحقق فلان في قضية أي أخذ أقواله فيها وأجنى جناية أي أذنب، أي أنّ التعريف اللغوي للتحقيق هو إثبات التهمة على الجاني بإحكام[2].

2-التحقيق اِصطلاحًا:

يعرّف بأنّه مجموعة من الإجراءات التي يباشرها الجهاز القضائي المكلف بالتحقيق قصد التثبت من الوقائع المعروضة عليه ومعرفة كل من يساهم في اقترافها ثم إحالة هذا الأخير إلى جهة الحكم لتوقيع الجزاء المناسب لهم.

كما عرّف أيضًا بأنّه: «مجموعة من الإجراءات والوسائل المشروعة قانونًا والتي يقوم بها المحقق لاستجلاء غموض الحوادث الجنائية بصفة عامة والجريمة الإلكترونية خاصة والتوصل إلى الفاعل أو الفاعلين وتوجيه الاتهام ضدهم»[3].

---

[1]- أعمر قادري، أطر التحقيق، دار هومة للطباعة والنشر، والتوزيع، الجزائر، 2013.ص33

[2]- د. عبد الواحد إمام مرسي، التحقيق الجنائي على وقت، بين النظرية والتطبيق، بدون بلد نشر، 2007، ص 11.

[3]- د. عبد الواحد إمام مرسي، المرجع نفسه، ص 12.

والتحقيق الجنائي أيضًا هو العلم الذي يضع مجموعة من الإجراءات النظرية والعلمية التي يقوم بها محققي هيئة التحقيق والاتهام، بما يوصلهم إلى الكشف عن الجريمة الإلكترونية وتوفير الأدلة الرقمية ضد مرتكبيها وتقديمهم للعدالة[1].

ب-تعريف التحقيق الجنائي في الجرائم الإلكترونية:

التحقيق الجنائي في الجرائم الإلكترونية عبارة عن فحص جهاز المستعمل من طرف الجاني أو المشتبه به من قبل المحققين، فمثلا إذا تمت جريمة عن طريق الحاسوب أو الأجهزة الذكية المختلفة يأتي المحقق المتخصص ليفحص حاسبه وذلك باستخدام أدوات خاصة ودراسات سابقة وكل ما هو ممكن والهدف منها جمع الأدلة المطلوبة.

يشكل التحقيق الجنائي المعلوماتي في البيئة المعلوماتية تحديًا كبيرًا للدول بالنظر إلى طبيعة هذا التحقيق وطبيعة هذه الجرائم المعلوماتية، ففي الولايات المتحدة الأمريكية تم إنشاء شرطةweb policeكمركز لتلقي الشكاوي في جرائم الانترنت، أما على المستوى الوطني فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة، إذ يحتوي على مخبر خلية الإعلام بالإضافة إلى مخبرين جهويين بكل من وهران وقسنطينة، كما توجد على مستوى المركز فرق متخصصة في التحقيق في الجريمة المعلوماتية بالتنسيق مع المخابر السابق ذكرها، كما يوجد بالمعهد الوطني للأدلة الجنائية وعلى علم الإجرام ببوشاوي قسم الإعلام والإلكترونات يختص في هذا النوع من الجرائم[2].

ونظرا لكون التحقيق باعتباره يهدف إلى التنقيب عن الأدلة وكشف الحقيقة، كان لزامًا أن تحاط إجراءاته بسياج من الضمانات تكفل له السّير الحسن، هذه الضمانات يمكن إيجازها فيما يلي:

[1]- د. عبد الله بن الحسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي والإدعاء العام، مذكرة ماستر، كلية الدراسات العليا، الرياض، 2014، ص 13.

[2]-إبتسام بوبعاية، المرجع السابق، ص 19.

1-سرية التحقيق:

يقصد بها عدم السماح للجمهور بالدخول للأمانة التي يجري فيها التحقيق فلا يجوز لهم الحضور أثناء التحقيق، كما لا يحق لهم الاطلاع على محاضر التحقيق، فيحضر على وسائل الإعلام نشر وإذاعة مضمون محاضر التحقيق وهذا ما نصت عليه المادة 11 من قانون الإجراءان الجزائية، حيث نصت على أنّ: «**تكون إجراءات التحري والتحقيق سرية، ما لم يمنعه القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع**»[1].

غير أنّ هذه السرية ليست مطلقة وإنّما نسبية، ذلك أنّها لا تشمل أطرافًا في الدعوى لا محاميهم أو وكلائهم، وإنّما السّرية تعتبر موجهة لبعض الناس فقط.

فالتحقيق تلازمه السرية عكس المحاكمة التي تكون علنية حيث يمكن للجمهور حضورها إلاّ فيما يخص محاكمة الأحداث وبعض الجلسات السرية لاعتبارات معينة.

2-تدوين التحقيق:

يقصد بالتدوين قيام الجهة المكلفة بالتحقيق بإثبات كل الإجراءات المتخذة خلال التحقيق، وذلك بكتابتها في محاضر وفق الشكل الذي حدّد القانون وللتدوين أهمية بالغة من خلال مساهمته في الحفاظ على كل تلك الإجراءات التي قام بها قاضي التحقيق مع كافة الأطراف سواء أكانوا متهمين أو ضحايا أو شهود، فالتدوين حجة لكل الأطراف لهم وعليهم.

فالمحاضر المكتوبة تمكن لاحقًا قاضي الموضوع من تقدير قيمة وصحة الأدلة المستمدّة من محاضر التحقيق الابتدائي والتي بإمكانه الاستناد والاعتماد عليها في تكوين حكمه.

وعلاوة على شرط الكتابة، نجد أن مختلف التشريعات أوجبت أن يتم التدوين بواسطة كاتب مختص وذلك تحت طائلة البطلان[2].

[1]- أمر رقم 66-155، مؤرخ في 08 يونيو 1966، يتضمن قانون الإجراءات الجزائية، معدّل ومتمم لاسيما بالقانون رقم 07/ 17 المؤرخ في 27 مارس سنة 2017.

[2]- إسماعيل بني يحي، المرجع السابق، ص ص55-56.

3-وضع خطة التحقيق:

تبدأ مهمة المحقق بجمع الاستدلالات وفي الجريمة الإلكترونية يساعد المحقق في أعمال التحقيق فريق تقني مختص ومؤهل في الإعلام والاتصالات.

ثانيًا/-تعريف المحقق الجنائي.

ذهب جانب من الفقه إلى تعريف المحقق بأنّه: «كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، والتحقيق فيها ويساهم بدوره في كشف غموضها وصولاً إلى معرفة حقيقة الحادث وكشف مرتكبه.

كما عرّف البعض المحقق أو الباحث الجنائي بأنّه المكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدّد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها».

عرف أيضًا المحقق بأنّه «ذلك الشخص الذي عهدإليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة بهدف الكشف عن الجرائم وضبط فاعلها»[1].

الفرع الثاني

خصائص التحقيق في الجريمة الإلكترونية وشروطه

تعدّ مرحلة التحقيق الأولي أو ما يطلق عليها مرحلة جمع الاستدلالات مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية لأنّها تعد حجر الزاوية الذي سيتم على أساس بناء الدعوى برمتها فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحًا بعد مرور وقت قصير على ارتكابها، والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.[2]

[1]- د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، القاهرة، 2009، ص 40.

[2]-إسماعيل بن يحيى، المرجع السابق ، ص ص 60 66.

كما أن التحقيق في الجرائم الإلكترونية وحتى التقليدية منها يتطلب توفر شروط أساسية، وهذا ما سوف نتطرق اليه فيما يلي:

أولاً/- خصائص التحقيق في الجريمة الإلكترونية.

التحقيق الجنائي عمومًا هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليمتع التحقيق بهذه الصفة، حيث تعتبر مرحلة التحقيق أصعب مرحلة يجتازها المحقق الجنائي خاصة الإلكترونية منها.

وتكون القواعد التي يخضع لها التحقيق إمّا قانونية وإمّا فنية تقنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزائها شيئًا سوى الخضوع والامتثال.

أمّا الثانية فتتميّز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[1] فتتمثل خصائصه في الجوانب التالية:

1-أسلوبالتحقيق في الجريمة الإلكترونية:

التحقيق عمومًا هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدًا لتقديمهم للمحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة الجهات أو برمجيات كتحديد الدخول إلى المعطيات المخزنة في النظام المعلوماتي والهدف من التحقيق هو التأكد أولاً من وقوع الجريمة والتي يعاقب عليها القانون، ومن ثم معرفة نوع هذه الجريمة ومن هو الجاني والمجني عليه، وكذا معرفة كيفية وقوعها وما هي الوسائل التي استعملت في ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى[2].

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 56.

[2]- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجنائي، رسالة ماستر، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص 111.

أ-وضع خطة عمل التحقيق:

يبدأ المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللاّزمة على أساس المعلومات الموجودة والحاضرة لديه، وتعيين الفريق اللازم للقيام بمساعدته في أعمال التحقيق، وذلك على النحو الآتي:

- وضع الخطة المناسبة والتي لا تبدأ إلاّ بعد معاينة مسرح الجريمة والتعرّف على أنظمة الحماية وتحديد مصدر الخطر ووضع التخطيط الكفيل للتصدي للجريمة.
- التخطيط الفني وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذا النوع من الجرائم بالتفصيل والوضوح.
- عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم توضيحها ومناقشتها من طرف العاملون في فريق التحقيق.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيّدة من التقييد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية.
- ويجب أن ترتكز خطة العمل على مجموعة البنود الأساسية التي تيم الارتكاز عليها أثناء تنفيذ الخطة، وهي: أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب اتضاحها معهم وتقدير مدى الحاجة إلى الاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق[1]، بالإضافة إلى مراعاة الملابسات المحيطة بالوقائع ذلك أنّ من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها:
  - مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة.
  - مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.
  - مستوى الاختراق الأمني التي تسبّب فيها الجاني.

[1] نعيم سعيداني، المرجع السابق، ص112.

- ثم بعد ذلك وضع الأسلوب الأمثل للتفتيش.

ب -تشكيل فريق التحقيق:

إنّ التحقيق في الجرائم المعلوماتية يكون غالبًا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرّد حاسب شخصي واحد، ولذلك فإنّه يفضل أن يتعاون عدّة محققين في إنجاز مهمة التحقيق والعثور على الأدلة، ويجب أن يتشكل فريق التحقيق من فنيين أخصائيين ذوي خبرة في مجال الحاسوب والانترنت،ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الإعلام الآلي والاتصالات ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.[1]

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلاّ أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تطلبه من مهارات وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريًا ومن الناحية العملية غالبًا ما يتكوّن فريف التحقيق من:

- خبراء الحاسوب وشبكات الانترنت الذين يعرفون ظروف الحادثة وكيفية التعامل معها.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي.

وفي هذا الإطار نجد أنّ المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممّن لهم دراية بالتدابير المتخذة لحماية

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص118.

المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية كذلك[1].

2-العناصر الأساسية للتحقيق في مجال البرمجة الإلكترونية:

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحدّدة التي تثبت وقوع الجريمة وتحدّد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعيّن على الضبطية القضائية مراعاتها، قبل البدء في عملية التحقيق والتي تتمثل في:

أ-الإجراءات التي يجب مراعاتها قبل البدء في التحقيق:

يمكن أن نسرد الأهم منها كالآتي:

- تحديد نظام المعالجة الآلية للمعطيات، وهل بكمبيوتر معزول أو متصل بشبكة معلوماتية.
- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفعيلي عن المسئولين بها ودور كل منهم، فإذا وقعت الجريمة على الشبكة فإنّ يجب حصر ضرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه، وهل هناك حواسب آلة خارج هذه الشبكة ولها إمكانية الاتصال بهم
- مراعاة صعوبات بقاء الدليل فترة طويلة في الجريمة المعلوماتية.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.

[1]- أنظر المادة 05، الفقرة الأخيرة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنّهم قد يسيئون استخدامها لطمس البيانات.
- التأكد من أنّ خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنّ من الخدع التي يستعملها الجاني عند الاختراق: أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.
- إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر وكذا الشفرات في حالة وجودها.
- تصوير الأجهزة المستهدفة من الأمام والخلف لإثبات بأنّها كان تعمل[1].

ب-الإجراءات التي يجب مراعاتها أثناء التحقيق:

عند البدء في عملية التحقيق ولا سيما عن القيام بعملية تفتيش جهاز الحاسوب يجب على الجهات المخصّصة مراعاة ما يلي:

- عمل نسخة احتياطية من الأقراص الصلبة قبل اِستخدامها والتأكد فنيًا من دقة النسخ عن طريق (Discompte)معنزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية، وأن يكون الهدف من نسخ محتوى الأسطوانة والأقراص هو: تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة والتي يمكن استعادتها من سلّة المهملات (Corbeille)، مع أنّ هناك بعض الملفات التي إن مسحت وضعت على أزرار معيّنة مثل (Shift délite).
- العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلّق بدخول المعلومات وخروجها.
- حفظ المعدّات والأجهزة التي تضبط بطريقة فنية وسليمة.

[1]- نعيم سعيداني، المرجع السابق، ص 113.

ثانيًا/ -شروط التحقيق في الجريمة الإلكترونية.

1- **أن يكون التحقيق بصدد جريمة (جناية أو جنحة)**:[1]يقصد بذلك أن تكون الجريمة معاقبة عليها في القانون، فبمجرّد وقوع الجريمة يبدأ عمل الجهات المكلفة بالتحقيق للتأكّد من وقوعها ومعرفة من ارتكابها وما نوع هذه الجريمة وما هو النصّ القانوني الذي ينطبق على الجريمة المرتكبة فلايجب إصدار أمر بأنّ لا وجه للمتابعة أو يصدر أمر بحفظ الأوراق لعدم وجود جريمة، وذلك بناءً على أمر صادر من السلطة المختصة، ويعتبر هذا الشرط تطبيقا لمبدأ (لاجريمة ولا عقوبة إلاّ بنص)، وبناءً عليه فلا يمكن توجيه اتهام ضد أي شخص ما لم يكن منصوصًا عليه قانونيًا.

فالمبدأ العام في القضايا الجنائية أنّ التحقيق فيها وجوبيًا، وهذا ما نصت عليه المادة 66 من قانون الإجراءات الجزائية[2]. فلا يجوز إحالة المتهم بجناية إلى جهات الحكم دون المرور عبر التحقيق، وذلك لخطورة هذا النّوع من الجرائم والعقوبات المترتبة عليها من جانب وكون التحقيق فيها وسيلة دفاع المتهم، ووسيلة مساعدة قضاة الحكم في تقدير العقوبة أو التدبير الملائم للمتهم من جانب آخر.

وأما التحقيق في مواد الجنح يكون مطلوبًا وضروريًا، كلما كانت القضية معقدة وخطيرة، وكلما تطلب الأمر اتخاذ إجراء من إجراءات التحقيق، ويكون اختياریاما لم يكن ثمة نصوص خاصة طبقا المادة 66 فـ2، ق.إ.ج.ج.2

كما أنّ فتح التحقيق يعد ضروريًا إذا ما بقي مرتكب الجريمة مجهولاً أو فارا أو أنه لجأ إلى خارج الوطن.

أما فيما يخص مواد المخالفات والتي تعدّ أقلّ الجرائم خطورة فإنّ التحقيق فيها يكون دائمًا جوازي بحيث يجوز إجراء التحقيق فيها بشرط طلبه من وكيل الجمهورية طبقا المادة 66 فقرة 2 من ق ا ج.

[1]-نصيرة بوحزمة ، مرجع سابق،ص99.

[2]- أمر رقم 66-155، مرجع سابق.

وبالتالي يفهم من نص هذه المادة أنّه من كان ضحية مخالفة لا يمكن التأسيس كطرف مدني بغرض تحريك الدعوى العمومية، وبالتالي فتح التحقيق غير أنّه لا يوجد أيمانع يحول دون تأسيسه كطرف مدني إذا ما فتح التحقيق بناءً على طلب وكيل الجمهورية.

وعليه يكفي أن يتوافر في الجريمة محل التحقيق**ركنها المادي**[1]، ومن القواعد العامة للركن المادي في الجريمة أن يحدد المشرع الجزائري السلوك الإجرامي في كل جريمة على نحو يمكن القاضي من تكييف هذا السلوك أو الفعل الإجرامي ورده إلى القاعدة القانونية أو النص التجريمي الذي يحكمه ويتضمنه.

وفي الجرائم الإلكترونية يتطلب لقيام السلوك الإجرامي وجود حاسب آلي وأحيانًا تتطلب الجريمة أن يكون متصلاً بشبكة الانترنت.ويختلف السلوك الإجرامي في الجرائم الإلكترونية حسب نوع الجريمة، فقد يكون وقتيا أي يبدأ وينتهي بمجرد ارتكابها مثل جريمة السرقة المعلوماتية، وقد يكون مستمرًا مثل إنشاء مواقع تحريض القصر على العنف والدعارة أو مواقع معادية بغرض الترويج للإرهاب.

أما **الركن المعنوي** في الجريمة الإلكترونية يمكن القول بأنّها جرائم عمدية، يستوجب المشرّع فيها توفر القصد الجنائي بركنيه العلم والإرادة.ويختلف الركن المعنوي في الجريمة الإلكترونية من جريمة لأخرى.

2-أن تكون الجريمة قد وقعت فعلاً أو ترجح وقوعها:

العبرة في اتخاذ الإجراءات في شأن الجرائم الإلكترونية أن تكون الجريمة محل التحقيق قد وقعت فعلا أو ترجع وقوعها، فلا يجري التحقيق بشأن جريمة محتملة، وإلا كان الإجراء باطلاً وفي هذا الصدد يثور التساؤل حول أمرين:

- **الأوّل:** الإجراءات السابقة على مباشرة التحقيق الابتدائي والتي تجري لكشف الجريمة.

[1]- فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009-2010، ص 39.

- **والثّاني:** إجراءات الضبط الإداري التي تتخذ للعمل على منع وقوع الجريمة[1].

وممّا لا شك فيه أنّ لضابط الشرطة القضائية أن يباشروا إجراءات جمع الاستدلالات وجمع التحرّيات بشأن وجود دلائل كافية على وجود الجريمة.

وأما عن مدى تحقق صور الجريمة المشهودة في نطاق المعلوماتية، فيرى البعض أن بالإمكان تحققها، في حال أن يكتشف ضابط الشرطة القضائية أو المجني عليه أثناء قيام الجاني باختراق شبكة، أو نظام معلوماتي أو قاعدة بيانات تابعة عليه، ويكون لديهم الإمكانية الفنية لمطاردة الجاني وتتبعه بقصد معرفته.

ومثال ذلك قيام شركة خدمات الانترنت (ISP) بالولايات المتحدة الأمريكية باكتشاف أنشطة دعارة وترتيب لقاءات جنسية مع الأطفال أثناء قيامها بمراقبة أنشطة المشتركين لديها، وعلى الفور قدمت أسماء المشتبه فيهم للشرطة الفيدرالية الأمريكية التي تمكنت من القبض على العشرات منهم بعد مراقبة أنشطتهم[2].

وأيضا يمكن مشاهدة الجريمة حال حدوثها من خلال الانترنت إذا شاهد ضابط الشرطة القضائية أو الغير الجريمة حال ارتكابها، ففي مثل هذه الحالة تتحقق صورة الجريمة المتلبس بها بالمشاهدة عن بعد وعبر موجات كهرومغناطيسية، مثلها مثل المشاهدة المادية الملموسة التي نصت عليها القوانين التقليدية.

ومثال ذلك ملاحظة صاحب مقهى الأنترنت(Cyber café) لشخص يقوم ببث صورًا إباحية لفتاة عبر الانترنت مستخدمًا حاسب آلي في المقهى، فيقوم على الفور بإخطار السلطات المعنية بوجود جريمة ترتكب داخل مقهى الانترنت المملوك له.

غير أنّ قيام حالة الجريمة المتلبس بها تعترضها بعض المشكلات منها لزوم كشف حالة التلبس بالمشروعية، بمعنى أن الإجراء اللازم لكشف حالة التلبس يجب أن يكون

[1]- نصيرة بوحزمة، المرجع السابق، ص 102.

[2]- فايز محمد رجب غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، كلية الحقوق، فرع القانون الجنائي والعلوم الجنائية، جامعة الجزائر1، 2010-2011، ص 288.

مشروعًا، وهذا يكون محل صعوبة في مجال الجريمة الإلكترونية نظرًا لحداثتها وعدم وجود نصوص قانونية لتنظيمها، أضف إلى ذلك تداخل القيام بالإجراء مع موضوع الحرّية الشّخصية التي يجب أن تكون مصانة بالقدر اللازم والضروري للحفاظ على حقوق الأفراد وحرياتهم، وبالتالي يجب أن يكون الإجراء منصوصا عليه في القانون[1].

وفي هذه المسألة تثار مشكلة مشروعية التخفي عبر الانترنيت من قبل القائم بعمل التحريات، سواء بهدف الكشف عن جريمة محدّدة حدثت، أم بغرض التوصل إلى البحث عن الجرائم ومرتكبيها بشكل عام، فغالبًا ما يقوم عناصر التحريات في بلد ما بالتخفي واتخاذ أسماء وهمية ومن ثم الولوج إلى الانترنت، والدخول إلى غرف المحادثات وحلقات النقاش وتبادل الحديث مع الغير بقصد التوصّل إلى نتائج غير محدّدة تتمثل في التوصّل إلى مرتكبي جرائم معيّنة.

كما توجد مشكلة أخرى في حال حساب الزمن اللاّزم لقيام حالة التلبّس والتي غالبًا ما يترك أمر تحديدها لضابط الشرطة القضائية شريطة عدم تجاوزها مدّة محدّدة، حيث أن هذه الأخيرة بالنسبة للجريمة التقليدية قد قدّرها البعض بساعات وفي الغالب يوم أو يومين المهم ألا يكون في تقدير الزمن إسراف، بخلاف مدّة التلبس في الجريمة الإلكترونية والتي يصعب تحديدها إذا كان في الأمر مطاردة.

غير أنّ لتوضيح كيفية قيام المطاردة عبر الانترنت، يتم اللجوء لبرمجيات دقيقة لتعقب المكرة ومجرمي المعلوماتية عبر الانترنت، ويمكن لهذه البرمجيات تعقب المجرم بجدارة، ذلك أن الجاني يترك وراءه بصمة تسمى البصمة الإلكترونية.

لقد تم تطوير تقنية المطاردة والتتبع عبر الانترنت، بحيث أمكن التوصل إلى برمجيات يمكنها تتبع أولى محاولات المجرم المعلوماتي، مثل: برمجية أتسيد ATICD التي يمكنها التوصل إلى أوّل بصمة إلكترونية للمجرم عبر الانترنت.

[1]- فايز محمد راجب غلاّب، المرجع السابق، ص 290.

وبعد تحديد الجهاز المستخدم في ارتكاب الجريمة الإلكترونية، يمكن الوصول إلى مكان ومحل إقامة مستخدمه عن طريق (IP Adresse)[1].

حيث يوجد في البريد الإلكتروني رقم (IP) الخاصة بكل جهاز متصل بالانترنت في خانة (Header)، ثم يقوم رجال الضبط القضائي بالذهاب إلى (Mail option)، ثم (General préférence)، ثم إضافة (Header)، ثم يقوم باختيار (Show all Header on inconning message)، ثم يذهب إلى الرسالة المرسلة، فيجد الـ (IP)المرسل المكوّن من أربعة (04) أرقام يفصل بينهما نقطة في: X-originating-IP وبعد التوصّل إلى (IP) الخاص بالجهاز المستخدم الذي يمكننا من تحديد الموقع الجغرافي، ومزود الخدمة وخط التليفون الأرضي أو شبكة (ADSL)لمستخدم الجهاز الذي تم التوصل إلى (IP) الخاص بالجهاز، يمكننا من تحديد محل إقامة مالكه[*]2.

3-أن يجري التحقيق في مواجهة المتهم بارتكاب الجريمة للبحث عنه:

يتطلّب ذلك معرفة من هو المتهم بارتكاب الجريمة سواء أكانت إلكترونية أو تقليدية وينصرف اصطلاح المتهم إلى الشخص الذي يوجه إليه الاتهام بارتكاب إحدى الجرائم المنصوص عليها في قانون العقوبات أو في إحدى التشريعات الجنائية الخاصة كقانون مكافحة جرائم تقنية المعلومات، سواء بوصفه فاعلا أو شريكا.

[1]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية.مصر2012.ص45

2-خط الاشتراك الرقمي غير المماثل (ADSL) هو عبارة عن تقنية الشبكة التي تنقل البيانات بسرعة على خطوط الهواتف الحاسبة التناظرية ANALOGE وبشكل غير مماثل، حيث تتحرّك البيانات في اتجاه واحد وبسرعة أكبر من الاتجاهات الأخرى.

الفرع الثالث

وسائل التحقيق في الجرائم الإلكترونية

عند القيام بالتحقيق في جريمة ما، فإنه يتعيّن على المحقق الالتزام بقوانين وتشريعات ولوائح مفسّرة، وقواعد فنية تحقّق الشرعية، لسهولة الوصول إلى الجاني، حيث أن الجرائم الإلكترونية لها طابعها الخاص المميّز لها، فإنّ التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة، وبالتالي حل لغتها والوصول إلى الجاني، وتوجد هناك وسائل تساعد على ذلك وهي الوسائل المادية (أوّلاً) والوسائل الإجرائية (ثانيًا).

أوّلاً/ -الوسائل المادية.

وهي الأدوات التي غالبًا ما ستخدم في بيئة نضم المعلومات والتي نثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:[1]

1- عنوان (IP) والبريد الإلكتروني، وبرامج المحادثة:

عنوان الانترنت هو المسئول عن تراسل حزمة من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجات والشبكات المعنية نقل الرسالة وهو يوجد في كل جهاز مرتبط بالانترنت، ويتكوّن من أربعة أجزاء كل جزء يتكوّن من أربع خانات، فيكون المجموع اثنتا عشر خانة كحد أقصى، حيث يشير الجزء الأوّل من اليسار إلى المنطقة الجغرافية والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية، والرابع للجهاز الحاسب وفي حالة وجود أية مشكلة أو أية أعمال تخريبية، فإنّ أوّل ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال الغير قانونية، ويمكن لمزوّد خدمة الانترنت أن يراقب

[1]- عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم المحاسبة بأنظمة الاتصال والمعلوماتية، مجلة دائرةالبحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية، والنظم السياسية، العدد الرابع، جامعة تبسه،جانفي 2018، ص 54.

المشترك، كما يمكن للشبكة التي تقدّم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسبة الإلكترونية في حالة الاتصال المباشر. منها على سبيل المثال ما يستخدم في حالة العمل على نظام التشغيل (Windows) حيث يتم كتابة (Wim, pc FG) في أمر التشغيل يظهر مربع حوار يبيّن في عنوان (IP)، مع الملاحظ أنّ عنوان الانترنت قد يتغير مع كل اتصال بشبكة [1].

أما في حالة استخدام أحد البرامج التواصلية كأداة للجريمة، فإنه يتطلّب تحديد هوية المتصل، كما يحدّد رسالة البريد الإلكتروني و عنوان مرسلها حتى ولو لم يدوّن معلوماته في خانة المرسل.

والسؤال الذي يطرح نفسه في هذا الصدد يكمن في ماذا يكشف رقم (IP) وهل يمكن الاستفادة منه في التحقيق الجنائي؟

يمكن القول هنا أنه عندما يزور شخص ما موقع معيّن على الشبكة يسجل الموقع (IP) العائد للكمبيوتر الذي اتّصل به، وعند إرسال رسالة إلكترونية يمكن لمستلم الرّسالة معرفة عنوان (IP) للكمبيوتر المرسل أيضًا، فإذا كان يستخدم ذلك الشخص برنامج الأوتلوك مثلا، فيكفي أن ينقر على أبشن (Option) بعد أن يفتح الرسالة يطلع على عنوان (IP)[2]. لكن هل يحدّد هذا العنوان الكمبيوتر المتصل بدّقة؟

إذا كان الكمبيوتر المتصل ينتمي إلى شبكة مرتبطة بخط خاص كما هو الحال بالنسبة للعديد من شبكات المؤسسات المتوسطة والكبيرة، فانه سوف يحدد الكمبيوتر المتّصل والجهة المستخدمة.

---

[1]- عز الدين عثماني، المرجع السابق، ص 55.

[2]- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 71.

أمّا إذا كان الكمبيوتر يتصل عن طريق رقم هاتف عادي فلا يكفي رقم (IP)، لتحديد الجهة المتصلة بالموقع أو التي بعثت بالرسالة، وعليه سيقوم القسمان الأوّل والثاني من الموقع، بدءًا من اليسار، بكشف اسم مزوّد خدمات الانترنت الذي يشترك لديه المتصل، فيما يحدد القسمان الثالث والرابع رقم مجموعة الكمبيوترات، ولكن ما هو الحل إذا كان الكمبيوتر المتصل لدى مزود خدمة واحدة لديه عناوين متطابقة؟ إذا جرى الاتصال في أوقات مختلفة فكيف يمكن اكتشاف المتصل أو مرسل الرسالة في هذه الحالة إن ارتكب مخالفة قانونية؟

يمكن ذلك عن طريق مزوّد خدمة(ISP)الذيي حتفظ بسجلات كافة الاتصالات، حيث يظم حقلا للرقم وحقلين لكل من تاريخ وزمن الاتصال وحقلا لاسم المشترك[1].

تستخدم معظم المواقع نظام أو بروتوكول الكوكيز (Cookies) والفائدة منه هو في الحقيقة تسريع الدخول إلى المواقع خاصة فيما يتعلق بالمسائل التجارية، فبهذا النظام تستطيع المواقع أخذ بعض البيانات الخاصة.

كما يلاحظ وجود عدة مواقع على شبكة الانترنيت تؤمن السّرية لتحركات المستخدم، كموقع www.anonymizer.comمثلا حيث يوفر للمستخدم إمكانية إخفاء رقم (IP) عن المواقع التي يرغب في زيارتها ويوصله إليه بدون تسجيل أية معلومات حقيقية عنه.

ولكن هل يضمن الاشتراك بالخدمات المذكورة إخفاء الهوية بشكل كامل أثناء استخدام الانترنت؟ بطبيعة الحال لا، فالجهة الوسيطة التي تقدم هذه الخدمات تحتفظ بسجل عن كافة التحركات، لكنها لا تكتشفه إلاّ في حال وقع اعتداء معيّن مصدره الكمبيوتر[2].

2- البروكسي (Proxy):

البروكسي عبارة عن حلقة وصل بين الشخص وبين الانترنت على الرغم من أن بعض الناس ترى مشاكل في استعمال البروكسي، إلا أنّ فوائدها تفوق مشاكلها بكثير.

1-ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص72.

2- نصير بوحزمة، المرجع السابق، ص 140.

حيث يعمل البروكسي كوسيط بين الشبكة ومستخدمها كما ذكرنا آنفًا حيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة هذه الأخيرة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (Cache mémoire) وتقوم فكرة البروكسي على تلقي مزوّد هذا الأخير لطلبات المستخدمين للبحث عن صفحة ما ضمن فكرة (Cache) المحلية المتوفرة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلىإرسال الطلب إلى الشبكة العالمية،ومن أهم مزايا مزود البروكسي أن ذاكرة (Cache) المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها.كما يمنع من الوصول إلى بعض المواقع مما يجعل دوره قوي في جمع الاستدلالات وذلك عن طريق فحص تلك العمليات المحفوظة فيها والتي تخص المتهم والموجودة عند مزوّد الخدمة[1].

3-برامج التتبّع:

يقوم هذا البرنامج بالتعرّف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه ويحتوي على: اسم الحدث، وتاريخ حدوثه، وعنوان (IP) الذي تحدث من خلاله الاختراق، واسم الشركة المزوّدة لخدمة الانترنت المستضيفة للمخترق، وأرقام دواخلها وخوارجها على شبكة الانترنت ومعلومات أخرى.

ومن أمثلة عن هذا البرنامج: برنامج (Hack Tracer VI2) وهو يتكوّن من شاشة رئيسية تقدم للمستخدم بيان شامل عن عملية الاختراق التي تعرّض لها جهازه.

4-نظام كشف الاختراق (Intrusion détection système):

يرمز له بالاختصار بالأحرف (IDS) وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أيّة إشارة قد تدل على وجود مشكلة تهدّد أمن الحاسوب أو الشبكة.

[1]-حسين بن سعيد الغافري،السياسة الجنائية لجرائم الانترنيت ،،دراسة مقارنة،دار النهضة العربية،القاهرة ،2006،ص513.

يتم ذلك من خلال تحليل رزم البيانات أثناء اِنتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية. والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشاف النظام وجود أحد هذه التوقيعات يقوم بإنذار مدير النظام بشكل فوري وبطرق عدّة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربّما مصدرها[1].

5-نظام جرّة العسل (Horney pot).

هو نظام حاسوبي مصمم خصيصًا لكي يتعرّض لأنواع مختلفة من الهجمات عبر الشبكة، دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئًا بسهولة الاعتداء على أيّ جهاز آخر في الشبكة في الوقت الذي يتم فيه جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء وتحليلها وبالتالي اتخاذ إجراء وقائي فعّال.

6-أدوات توقيف ومراجعة العمليات الحاسوبية (Auditing Tools).

هي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معيّن وتسجيلها في ملفات خاصة ويطلق عليها (Logs)والكثير من هذه الأدوات تأتي في أنظمة التشغيل بعد إعدادها للعمل، وكلّ ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها أو إعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى

-علي عدنان الفيل،إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث،الإسكندرية، مصر،2012، ص ص71- 72

يتمكن من تسجيل المعلومات التي قد تكون لها علاقة بالحادثة وربّما تساعد في الكشف عن أسلوب الجريمة وشخصية مرتكبها[1].

7-أدوات الضبط.

تعتبر أدوات الضبط من الوسائل المادية التي تساعد في ضبط الجريمة الإلكترونية منها على سبيل المثال: برامج الحماية، وأدوات المراجعة، أدوات مراقبة المستخدمين للشبكة، برامج النسخ الاحتياطي التي تستخدم لعمل نسخة مطابقة تماما للأقراص الصلبة الموجودة في الحسابات الإلكترونية محل التحقيق وعلى مستوى (Bit Stream Bac Kop)، بعرض الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغيير.

8-الوسائل المساعدة للتحقيق.

من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية، وبرامج تشغيل الحاسبة، برامج نسخ البيانات، أيضا في الأدوات المهمة والتي تساعد في عملية التحقيق برامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة، وهناك أيضا برامج تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني ومن أشهرها (Extractor) و (Gets free) وغيرها[2].

9-أدوات فحص ومراقبة الشبكات.

هذه الأدوات تستخدم في فحص بروتوكول الانترنت ,Protocol internet)(TCP/ IP) (Protocol transmission والتي تتعرض لها ومن تلك الأدوات التي يمكن استخدمها على النّحو التالي:

[1]- محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنيت،مذكرة ماستر، جامعة نايف العربية للعلوم الأمنية، الرياض،2004، ص35.

[2]- نبيلة هبة هروال، الجوانب الإجرائية في جرائم الانترنت في مرحلة جمع الاستدلالات، ط1، دار الفكر الجامعي، الإسكندرية، 2007، ص 45.

أ-أداة ARP:وظيفتها تحديد مكان الحاسب الآلي .

ب-برنامج (Visual Route): هو عبارة عن برنامج يلتقط أية عملية فحص عملت ضد الشبكة، .

ج-أداة (Tracer):تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي قام الجاني بزيارتها والوقت والفترات التي قضاها.

د-أداة (Net stat): هي أداة لفحص الاتصال الحالي بالبروتوكول (TCP/ IP) ولها عدد من المهام أهمها: عرض جميع الاتصالات المالية، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية، وعرض كامل لجدول التوجه[1].

ثانيًا/-الوسائل الإجرائية.

يقصد بها تلك الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددّة والمتغيّرة والتي تثبت وقوع الجريمة ومعرفة الجاني ومنها:

1-اقتفاء الأثر.

من أخطر ما يخشاه المجرم الإلكتروني تقصي أثره أثناء ارتكابه الجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصّة بالمخترقين تحمل بين ثناياها العديد من النصائح، أوّلها: قم بمسح آثارك (Coveryourtracks) فلو لم يقم المخترق بمسح أثاره، فمن المؤكد أنه سيتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدّة سواء عن طريق البريد الإلكتروني أوعن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[2].

[1]- نبيلة هبة هروال، المرجع نفسه، ص 50.

[2]-حسين بن سعيد لغافري ، مرجع سابق ،ص519.

2-الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

ينبغي على المحقق الاطلاع على النظام المعلوماتي ومكوّناته من شبكات وتطبيقات وخدمات تقدّم للعملاء، كما ينبغي عليه الاطلاع على عمليات النظام والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات أمن الكامن وأسلوب النسخ الاحتياطي، بالاستعانة ببرامج الحماية كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع في حالات فشل الدخول إلى النظام، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها، والاستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية.

وفي هذا الصدد يجب على قائد فريق التحقيق التأكد من حرص جميع فريق التحقيق على هذه الأمور أثناء تعاملهم مع الأدلة الرقمية على وجه الخصوص.

3-الاستعانة بالذكاء الاصطناعي.

أثبتت تقنية الحاسبة الإلكترونية نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة وفق برامج صمّمت خصيصًا لهذا الغرض[1].

[1]- عز الدين عثماني، المرجع السابق، ص 55.

المبحث الثاني

الهيئات المختصة بالتحقيق الجنائي في الجرائم الالكترونية

نظرًا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه ولأنّ أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النّوع من الجرائم أنشأت أجهزة خاصة بالتحقيق فيها والتي سوف نحاول التطرّق إليها من خلال هذا المبحث الثاني بحيث سوف ندرس الهيئات المكلفة بالتحقيق في الجرائم الإلكترونية في المطلب الأول والهيئات الفنية المختصة بالتحرّي عن الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول

الهيئات المكلفة بالتحقيق في الجرائم الإلكترونية

نظرا لخصوصية الجرائم المستحدثة خاصة الالكترونية منها خرج المشرع الجزائري عن القواعد العامة للتحقيق القضائي كما عمل على إنشاء هيئة وطنية مختصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

الفرع الأوّل

الهيئات القضائية

أولا/- قاضي التحقيق

1- مفهوم قاضي التحقيق

يعتبر قاضي التحقيق أحد قضاة الهيئة القضائية، يتم تعيينه بموجب مرسوم رئاسي بناءا على اقتراح من وزير العدل.

أ- تعريف قاضي التحقيق

سوف نبرز من خلال هذا الجزء كل من التعريف التشريعي لقاضي التحقيق أولا ثم التعريف القضائي .

- التعريف التشريعي لقاضي التحقيق

هو القاضي المكلف على مستوى المحكمة بالبحث والتحري عن الجرائم، واتخاذ كل ما يراه لازما للتحقيق وجمع الادلة لكشف الحقيقة.وقد نظم قانون الاجراءات الجزائية ومهامه في الفصل الثالث من الباب الاول في المواد من 38 الى 175.[1]

- التعريف القضائي لقاضي التحقيق

قاضي التحقيق هو أحد قضاة المحكمة الابتدائية، ويعين من بين قضاة المحكمة بمقتضى قرار من وزير العدل لمدة ثلاث سنوات قابلة للتجديد.

2-تعيين قاضي التحقيق

ان القضاء باعتباره وظيفة عامة تتولاها الدولة عن طريق المحاكم،فيكون من الطبيعي أن تتولى السلطة التنفيذية تعيين من يتولى الوظائف العامة،ومنها الوظيفة القضائية التي تمثل مرفق من مرافق الدولة.

واذا وجد بالمحاكم عدة قضاة تحقيق فان وكيل الجمهورية يعين لكل تحقيق القاضي الذي يكلف بالتحقيق حيث تنص المادة 70 من قانون الاجراءات الجزائية على أنه يجوز لوكيل الجمهورية اذا تطلبت خطورة القضية وتشبعها أن يلحق بالقاضي المكلف بالتحقيق قاض أو عدة قضاة تحقيق أخرين سواء عند فتح التحقيق أو بناء على طلب من القاضي المكلف بالتحقيق أثناء سير الاجراءات وينسق القاضي المكلف بالتحقيق سير اجراءات التحقيق وله الصفة للفصل في مسائل الحبس المؤقت والرقابة القضائية واتخاذ أوامر التصرف في القضية.[2]ويتم التعيين في الوظائف القضائية النوعية بموجب مرسوم رئاسي بعد رأي مطابق للمجلس الأعلى للقضاء أي أن تعيين القضاة يكون من طرف المجلس الأعلى للقضاء طبقا لشروط القانون العضوي.

---

[1] فريد روابح، محاضرات في قانون الاجراءات الجزائية، السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف (2)، 2020، ص 98.

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، الجزء الأول، الطبعة الأولى، دار هومة، 2014،ص12

3-نطاق اختصاص قاضي التحقيق

يقصد بها الحدود التي حددها المشرع لقاضي التحقيق ليباشر فيها ولاية التحقيق في كل الدعاوى المعروضة عليه وقد حدد بثلاثة معايير والمتمثلة في الاختصاص المحلي أو الاقليمي (مكان وقوع الجريمة، مكان اقامة مرتكبها،مكان القبض على المتهم)، الاختصاص النوعي المتعلق بنوع الجريمة المرتكبة، فهو يختص في جميع الجرائم المحالة اليه، أما الاختصاص الشخصي فهو المتعلق بالشخص مرتكب الجريمة.

-الاختصاص الشخصي لقاضي التحقيق

الأصل أن قاضي التحقيق يحقق مع جميع الأشخاص المتمين بأي جريمة من الجرائم التي تقدم بشأنها النيابة طلباتها،الذين وردت أسمائهم في تلك الطلبات طبقا للمادتين 1/35 و1/67 من قانون الاجراءات الجزائية وكذلك الأشخاص الذين يرى قاضي التحقيق وجها لاتهامهم بالوقائع المعروضة عليه طبقا للمادة 3/67 من نفس القانون، الا أن هذه القاعدة ليست مطلقة، لأن القانون أحيانا يقيد القاضي من حيث الأشخاص الذين يجوز التحقيق معهم.[1]كمثل اذا كان مرتكب الجريمة عسكريا طبقا للمادة 25 من قانون القضاء العسكري أو اذا كانت الواقعة جنحة مرتكبة من متهم بجناية أو حدث عندما لا يكون هو القاضي المعين والمكلف بالتحقيق بجنايات الأحداث مثلما تنص عليه المادة 62 من قانون حماية الطفل رقم 12/15.[2]

- الاختصاص المحلي لقاضي التحقيق

لقد حدد المشرع قواعده بالمادة 40 من ق.ا.جويتبين من خلالها أن الاختصاص المحلي لقاضي التحقيق يتحدد بمكان ارتكاب الجريمة أو المكان الذي يقيم فيه المتهم أو المكان الذي ألقي فيه القبض عليه ولو حصل هذا القبض لسبب اخر.

[1] عبد الله أوهايبية، شرح قانون الاجراءات الجزائية الجزائري، التحري و التحقيق، دار هومة، الجزائر، 2003، ص 325.
[2] أ/ حسين العيساوي، محاضرات في مقياس التحقيق القضائي، السنة الأولى ماستر، كلية الحقوق ، مسيلة ، 2016، ص30.

كما أن مكان ارتكاب الجريمة يختلف بالنسبة للجرائم الوقتية عنها بالنسبة للجرائم المستمرة، ففي الجرائم الوقتية يكون مكانا لارتكاب الجريمة المحل الذي يقع فيه فعل التنفيذ، وفي الجرائم الوقتية يكون مكانا لارتكاب الجريمة كلمكان تقوم فيه حالة الاستمرار، و في الجرائم التي تتكون من عدة أفعال و تكون قد ارتكبت في أكثر من مكان، كان جميع قضاة التحقيق التي وقعت في دائرتهم أفعال التنفيذ مختصين محليا بنظر الدعوى، أما بالنسبة لمحل اقامة المتهم فالعبرة بوقت اتخاذ الاجراءات ضده و لو قام بتغيير اقامته بعد ذلك.

تمديد الاختصاص المحلي لقاضي التحقيق

بموجب التعديل الجديد لقانون الاجراءات الجزائية المتضمن بالقانون رقم 04-14 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الاجراءات الجزائية قام المشرع بتوسيع الاختصاص المحلي لعدد من المحاكم ومعه بالتالي لقضاة التحقيق وذلك في نوع معين من الجرائم التي حددها المشرع على سبيل الحصر في الجرائم المستحدثة والتي من بينها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات أو الجرائم الالكترونية.[1]

- **الاختصاص النوعي لقاضي التحقيق**

ان قاضي التحقيق مختص بالتحقيق في كل جريمة معاقب عليها طبقا لقانون العقوبات أو القوانين المكملة له، وان التحقيق في الجرائم الموصوفة جناية يكون الزاما ولا يجوز احالة الشخص فيها مباشرة للمحاكمة قبل اجراء تحقيق قضائي معه، أما في مواد الجنح والمخالفات فهو اختياري يخضع لتقدير النيابة في طلب فتح تحقيق أو احالة القضية مباشرة الى المحاكمة ما لم يكن مرتكب الجنحة حدثا حينئذ يكون قاضي الأحداث هو المختص الا اذا كان معه متهمين بالغين فيكون قاضي التحقيق مختصا كذلك.

[1] ذ/أحسن بوسقيعة، التحقيق القضائي، الطبعة السابعة، دار هومة، كلية الحقوق و العلوم السياسية، جامعة مولود معمري،تيزيوزو، 2008، ص 46.

الاختصاص النوعي لقضاة التحقيق بالأقطاب الجزائية المتخصصة

لقد عرف المجتمع الجزائري في الفترة الأخيرة عدة تحولات، ظهرت معها عدة أشكال من الجرائم السابقة الذكر، مما كان على المشرع التفكير في ايجاد تدابير جديدة لمواجهتها باستحداث جهات قضائية متخصصة لمعالجتها يعهد بها لفئة من قضاة التحقيق من ذوي الكفاءات المتميزة والتكوين المتخصص في المسائل المتعلقة بهذه الأنواع الخاصة من الجرائم. حيث عهد التحقيق القضائي فيها الى قضاة تحقيق تلك الجهات القضائية المتخصصة، المتمثلة في أربع جهات بمحاكم سيدي أمحمد وقسنطينة ووهران وورقلة.[1]

4- تمديد اختصاص قاضي التحقيق

لقد منحت التعديلات الجديدة لقانون الاجراءات الجزائية المتضمنة رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الاجراءات الجزائية لقاضي التحقيق صلاحيات جديدة لم يكن يتمتع بها من قبل والمتمثلة في:

أ/ اعتراضالمراسلات، تسجيل الأصوات، التقاط الصور، فاذا تعلقت الوقائع المعروضة أمام قاضي التحقيق بإحدى الجرائم المستحدثة، فيجوز له أن يعهد لضباط الشرطة القضائية بترخيص مكتوب وتحت مراقبته المباشرة للقيام بهذه الصلاحيات الجديدة المسخرة له.

ب/ الاذنبإجراء عملية التسرب لأجل مراقبة الأشخاص وذلك متى كانت الوقائع المحقق فيها متعلقة بالجرائم المستحدثة المعاقب عليها بالقانون رقم 01-06 المؤرخ في 20 فيفري 2006 المتعلق بالوقاية ومكافحة الفساد، فان قرار قاضي التحقيق بمباشرة هذا الاجراء وجب عليه أولا اخطار وكيل الجمهورية بذلك ثم يقوم بمنح اذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته على أن يتم ذكر هويته والاسباب التي دعت الى اللجوء

[1] د/أحسن بوسقيعة، المرجع السابق، ص47.

الى هذا الاجراء وتحديد مدة عملية التسرب التي لا يمكن أن تتجاوز (4) أشهرقابلة للتجديد.[1]

ثانيا: النيابة العامة

1 : مفهوم النيابة العامة الالكترونية

لتعريف النيابة العامة الالكترونية يستوجب علينا تعريف النيابة العامة بشكلها التقليدي.

أ/تعريف النيابة العامة

يطلق مصطلح النيابة العامة في ظل قانون الإجراءات الجزائية الجزائري على القاضي الذي يتولى مهمة تمثيل المجتمع أمام القضاء، وذلك بتوجيه الاتهام من أجل اقتضاء حق الدولة في العقاب.

ب- طبيعة النيابة العامة اختلف الفقه حول طبيعة النيابة العامة فيما إذا هي جزء من السلطة التنفيذية أم فرع منفروع الجهاز القضائي؟فهناك جانب من الفقه اعتبر النيابة العامة جزء من السلطة التنفيذية، أما الاتجاه الثاني فيرى أنها فرع من فروع الجهاز القضائي لأن قضاة النيابة العامة يتم تكوينهم بالمدرسة العليا للقضاة مثله مثل باقي قضاة الحكم والتحقيق، الا أنه هناك اتجاه ثالث يجمع بين الأول والثاني حيث يكسب النيابة العامة الطابع القضائي، ومن هذا المنطلق تعرف النيابة العامة أنها جهاز قضائي جزائي يتولى تحريك ومباشرة الدعوى العمومية.

ت- ممثلو النيابة العامة

***النائب العام**

هو ممثل النيابة العامة أمام المجلس القضائي وكافة المحاكم التابعة لدائرة اختصاص المجلس الذي يباشر فيه مهامه وذلك بتحريكومباشرة الدعوى العمومية بكافة دائرة اختصاصه اما شخصيا أو بواسطة مساعديه العاملين تحت اشرافه.

[1] أحسن بوسقيعة، المرجع السابق، ص115-116.

يساعده في أداء مهامه، النائب العام المساعد الأول، ونائب أو نواب عاملون مساعدون، وكلاء الجمهورية ومساعديهم الأولين ومساعديهم.

* النائب العام المساعد الأول

يساعد النائب العام في تمثيل النيابة العامة أمام المجلس القضائي بتنفيذ ما يعهد به اليه، ويساعده في ذلك واحد أو أكثر من النواب العاملين المساعدين ووكلاء الجمهوريةومساعديهم.

* النائب العام المساعديساعد النائب العام المساعد الأول والنائب العام.

* وكيل الجمهورية

يمثل النيابة العامة في تحريك ومباشرة الدعوى العمومية بدائرة اختصاص المحكمة التي بها مقر عمله، يعاونه في ذلك وكيل الجمهورية المساعد الأول ووكيل الجمهورية المساعد يتحدد اختصاصه محليا بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشبوه فيهم فيها أو في المكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص.

ج-اختصاصاتالنيابة العامة

يباشر ممثلو النيابة العامة بمختلف درجاتهم اختصاصاتهم في دائرة المحكمة التي يقع بها مقر عمله، عدا النائب العام أو من ينوبه، فان له كما قدمنا الحق في مباشرتها في سائر دائرة اختصاص المجلس، حيث تتمثل هذه الاختصاصات في:[1]

* تلقي المحاضر والشكاوى والبلاغات وتقرير ما تراه بشأنها.

* تحريك ومباشرة الدعوى العمومية

* مباشرة كافة الإجراءات اللازمة للبحث والتحري عن الجرائم المتعلقة بقانون العقوبات وابلاغ الجهات القضائية المختصة بالتحقيق والمحاكمة لكي تنظر فيها، كما لها أن تأمر بحفظها بقرار يكون دائما قابلا للإلغاء.

[1] إسماعيل طواهري، محاضرات شرح النيابة العامة طبقا للقانون الجنائي الجزائر، سنة أولى ماستر، 2022/2021، ص7.

*حضور جلسات المحاكمة والمرافعة أمام الجهات القضائية المختصة بالحكم وإبداء ما تراه لازما من طلبات والملاحظات الشفوية اللازمة لصالح العدالة وتقديم طلبات كتابية طبقا للتعليمات التي ترد اليها بالطريق التدرجي.

* السعي لتنفيذ أحكام القضاء وأوامر وقرارات التحقيقوجهات الحكم بكل الوسائل بما فيها القوة العمومية والاستعانة بالضبط القضائي.

2/ تعريف النيابة العامة الالكترونية هي نظام قضائي معلوماتي جديد يتيح للشخص طبيعي كان أو معنوي أو لوكيله إيداع شكوى على مستوى مصالح وكيل الجمهورية المختص أو النائب العام عبر الأنترنت وهذا الأخير ملزم قانونا بالرد عبر الأنترنت على تلك الشكوى أو العريضة.

يظهر جليا من خلال ما سبق بأن هذا النظام يحقق فوائد كبيرة لما فيه من اختصار للوقت والجهد والمال ولاسيما بالنسبة لأفراد الجالية الوطنية بالمهجر.[1]

أ- خصائص النيابة العامة الالكترونية

تتميز النيابة العامة الالكترونية بمجموعة من الخصائص تجعلها تختلف عن النيابة العامة التقليدية اذ تتميز بسرعة الاتصالات وسهولتها وإمكانية إيداع الشكوى الكترونيا مما تؤدي الى توفير الجهد والوقت والكلفة، ويعد جهاز الحاسوب الوسيط الالكتروني بين أطراف الخصومة.

يمكن أن نحدد أهم الخصائص الرئيسية التي يتميز بها هذا النظام فيما يلي:

- **مغادرة النظام الورقي**

أهم ما يميز النيابة العامة الالكترونية هو عدم استعمال الوثائق الورقية في كافة الإجراءات، اذ تتم بينهم الكترونيا دون استعمال الأوراق وبالتالي التخلص من الكميات

1- نجاة زعزوعة /ليلى بن قلة،مجلة الدراسات القانونية و الاقتصادية،مخبر القانون المقارن،جامعة تلمسان،الجزائر، 2021،ص296

الهائلة من الملفات الورقية التخلص من عملية التخزين العشوائي للملفات مع سهولة الاطلاع على الوثائق الالكترونية بسهولة.

- **الاعتماد على الوسيط الالكتروني**

عموما النيابة العامة الالكترونية لا تخلف من حيث الموضوع والأطراف عن النيابة العامة التقليدية، ولكنها تختلف من حيث طريقة تقديم الشكوى التي تتم باستخدام وسائط الكترونية المتمثلة في الحاسب الالي المتصل بشبكة الاتصالات الدولية.

- **سرعة التنفيذ**

تتم عملية إيداع الشكوى والوثائق الكترونيا عبر شبكة الانترنت بطريقة سريعة جدا دون الحاجة الى انتقال طرفي الخصومة القضائية، وفي هذا اختصار للوقت وتوفير الجهد.

- **جودة الخدمة للمتقاضين**

تحقق النيابة الالكترونية للمتقاضين عملا يتميز بالجودة اذ يمكنهم الاطلاع ومتابعة عرائضهم، وكذا الشكاوى المقدمة من طرفهم وكل الإجراءات المتخذة بشأنهم دون اللجوء الى المحاكم.

لكن بالرغم من اثبات فعاليتها في بعض الدول الا أنها لا تزال تعاني من بعض الصعوبات.

ب/ الصعوبات التي تواجه النيابة العامة الالكترونية

ان استخدام تكنولوجيا الحاسوب والأنترنت لتنفيذ إجراءات إيداع الشكوى الكترونيا ومتابعتها لا يخلو من بعض الصعوبات سواء كانت من الناحية التقنية وهو عملذوي الاختصاص في مجال تكنولوجيا المعلومات أو حتى من الناحية القانونية والإدارية وهو من عمل رجال الفقه والقانون.

على هذا الأساس قبل أن نتناول الصعوبات القانونية والإدارية وجب علينا أن نتحدث عن الصعوبات التقنية أولا.

*** الصعوبات التقنية**

تواجه النيابة العامة الالكترونية مجموعة من الصعوبات التقنية التي تعترض مسيرة تطور إجراءات إيداع شكوى الكترونيا ويمكن اجمالهافيما يلي:

ث- ضعف انتشار الانترنت في بعض المناطق مما يشكل سببا رئيسيا في عدم إيداع أو تسجيل الشكوى الكترونيا.

-انتشار الفيروسات على الوسائل الالكترونية مما يؤدي الى تدمير محتويات برامج الحاسوب.

-ضعف الثقة والأمان بشبكة الانترنت للتأكد من مصداقية تسجيل الشكوى وايداعها عبر الوسائل الالكترونية.

*** الصعوبات القانونية والإدارية**

من أهم الصعوبات القانونية والإدارية التي تعترض النيابة الالكترونية نذكر ما يلي:

-نقص الوعي القانوني لغالبية دول العالم الثالث، تجهل ماهية الوسائل الالكترونية وآلية استخدامها.

-ان تسجيل الشكوى الكترونيا يتطلب ميزانية ضخمة لإنشاء البنى التحتية بكافة مستلزماتها من أجهزة ومعدات وشبكات، ضف الى تطوير الموارد البشرية كتدريب وتأهيل موظفي المحكمة في التعامل مع هذا النظام الجديد.

-أما الصعوبات التشريعية تتمثل في عدم وجود تشريعات كافية سواء كانت وطنية أو معاهدات دولية تنظم أحكام النيابة الالكترونية وإجراءاتها وان كان البعض يواكب هذه

المستجدات الا أن البعض الاخر يحتاج الى تدخل تشريعي مع استحداث نصوص قانونية لمعالجتها.

الفرع الثاني

الهيئات غير القضائيةتتمثل الهيئات غير القضائية المكلفة بالتحقيق في الجرائم المعلوماتي في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إضافة إلى السلطة الوطنية لمكافحة المعطيات ذات الطابع الشخصي ووكالة أمن الأنظمة المعلوماتية.

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

أنشئت هذه الهيئة بموجب المادة 13من القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها باعتبارها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل. تمارس مهامها تحت رقابة السلطة القضائية،يقع مقرها بالجزائر العاصمة، وترك أمر تشكيل الهيئة وتنظيمها وكيفية سيرها للتنظيم الصادر بموجب المرسوم الرئاسي رقم 15-261[1]،لكن في شهر جوان تم إلغاء هذا المرسوم وألحقت الهيئة بوزارة الدفاع الوطني حسب المرسوم الرئاسي رقم 19-172 المؤرخ في 06-06-2019.

وما يلاحظ التعديل مس فقط الجهة الوصية حيث أصبحت الهيئة توضع تحت سلطة رئيس الجمهورية بعدما كانت توضع تحت وصاية وزارة العدل سنة 2015 ولدى وزارة الدفاع الوطني سنة 2019[2].

[1]- المرسوم الرئاسي رقم15-261 مؤرخ في 08 أكتوبر 2015 يحدّد تشكيلة وتنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسميةعدد 53 صادر بتاريخ 08 أكتوبر 2015.

[2]- عدلي دحمان، سعد الدين تامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة زيان عاشور، الجلفة، 2020، ص 221.

تضم الهيئة مجلس توجيه يرأسه وزير الدفاع الوطني يكلّف بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المحدّدة في المرسوم أعلاه وكذا التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية. كما يقوم مجلس التوجيه دوريا بتقييم حالة التهديد في مجال هذه الجرائم للتمكن من تحديد مضامين عملية المراقبة الواجب القيام بها والأهداف المنشودة بدقة، وإعداد نظامه الداخلي والمصادقة عليه إضافة إلى دراسة التقرير السنوي لنشاطات الهيئة المصادق عليها، بحيث يجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناءً على استدعاء من رئيسه ويمكنه أن يجتمع في دورة غير عادية كلّما كان ذلك ضروريا بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

أما المديرية العامة للهيئة، فتتولى السّهر على حسن سير هذه الأخيرة، إعدادًا لمشروع ميزانيتها، وإعداد وتنفيذ برنامج عملها، كما تعمل على تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرّف عليه،ويصدر المدير العام الأمر بصرف ميزانية الهيئة وكذا مستخدموها طبقًا للتنظيم المعمول به في وزارة الدفاع الوطني كما يعاد إدماج القضاة والمستخدمين التابعين للدوائر الوزارية الأخرى العاملين بالهيئة في هياكلهم الأصلية، وتضم المديرية العامة مديرية تقنية تتكفّل على وجه الخصوص بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداءعلى أمن الدولة، إضافة إلى مساعدة السلطات القضائية ومصالح الشرطة بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتلك التي تتطلب اللجوء إلى أساليب التحري للهيئة[1].

[1]-إبتسام بو عباية، المرجع السابق، ص 30-31.

مهام الهيئة:

تنص المادة 14 من القانون رقم 09-04 على أنه تتولى الهيئة مجموعة من المهام نذكر منها:

1-الوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال:

تكون إجراءات الوقاية بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم التجسّس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء.... الخ[1].

2-مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

حسب المادة 14 أعلاه هناك نوعان من المكافحة تقوم بها هذه الهيئة:

أ- مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم؛

ب- تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال؛

ت- تقديم المساعدة لمصالح الأمن والدرك الوطنيين ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة).

3-تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم:

تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) المماثلة على مستوى الدول بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنّها تدرس الروابط العملياتية مع الهيئات

[1]-إبتسام بو عباية، نفس المرجع، ص 33.

والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية، وكذا التعرف على الفاعلين وأماكن تواجدهم.

ثانيا/-الوحدات التابعة لسلك الأمن والدرك الوطني

لقد أصبحت مكافحة الجريمة الإلكترونية من أولويات الدولة الجزائرية، إذ لابد من الاستجابة للانشغالات الأمنية المتزايدة والمحافظة على الطمأنينة والأمن العمومي في الفضاء الإلكتروني، أو كما يسمى الفضاء الأزرق، ولأجل ذلك فقد خصّصت الدولة الجزائرية عدّة وحدات متخصصة لمكافحة هذه الجريمة، فمنها التابعة لوحدة الأمن الوطني ومنها الوحدات التابعة لسلك الدرك الوطني، وهذا ما سوف ندرسه في مطلبنا هذا.[1]

1-الوحدات التابعة لسلك الأمن الوطني

لقد أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران تحتوي على فروع تقنية، من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الانترنت بالإضافة لإنشائها ثلاث مخابر على مستوى بشار، ورقلة وتمنراست، قيد الإنجاز لأجل تعميم هذا النشاط على كافة ربوع الوطني بالإضافة إلىالمخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران الذي يحتوي على مخبر خاصً يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية"، والتي تضم ثلاث أقسام وهي:

ج-قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات.

ح-قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

1- موقع المديرية العامة للأمن الوطني https // www.algeriepolice.dz

خ-قسم تحليل الأصوات، وذلك بالاستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية[1].

2-الوحدات التابعة لسلك الدرك الوطني

تسهر مؤسسة الدرك الوطني على مكافحة الجريمة بكل أنواعها خاصة الإلكترونية منها، حيث تعمل على مكافحة هذه الأخيرة في المعهد الوطني للأدلة الجنائية وعلوم الإجرام،يقع مقره ببوشاوي حيث يختص بالتحقيق والكشف عن الجرائم الإلكترونية[2]،و التصدي لها، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها، بالإضافة إلى مراكز الرقابة على جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس التابعة للقيادة العامة للدرك الوطني[3].

وعليه يسخر الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها وحدات متنوعة وعديدة على مستوى القيادة العامة أو على مستوى القيادات الجهوية والمحلية ونذكر منها:

د - المصالح والمراكز العلمية والتقنية.

ذ - هياكل التكوين.

ر - المصلحة المركزية للتحرّيات الجنائية.

ز - المعهد الوطني لعلم الإجرام.

[1]- سليمة نواوي، دور الدرك الوطني في محاربة الجريمة الالكترونية، مذكرة ماستر جامعة ميلة ،2019، ص60.

[2]-سعيد علي نعيمي، المرجع نفسه، ص 109-115.

[3]-إبتسام بو عباية، المرجع السابق، ص 37.

المطلب الثالث

مسألة إثبات الجرائم الإلكترونية في التشريع الجزائري

إنّ الإثبات في الجرائم المعلوماتية من الأمور الصعبة التي تواجهها السلطات المختصة بالتحقيق وجمع الاستدلالات نظرا لمحلها الافتراضي الذي ترتكب فيه، عكس الجرائم التقليدية التي ترتكب في العالم المادي الذي يترك أثار مادية. نص المشرع الجزائري على مسألة إثبات الجرائم بصفة عامة في المادة 212من قانون الإجراءات الجزائية، غير أن في الجرائم الالكترونية أمر صعب لذلك اعتبر الدليل الرقمي الوسيلة الفعالة والمهمة للإثبات.[1]

وعليه سنتطرّق للقيمة القانونية للدليل الرقمي **(الفرع الأوّل)**، ثم دور الدليل الرقمي في مجال الإثبات وضبط الجرائم الإلكترونية في الجزائر **(الفرع الثّاني)**.

الفرع الأول

القيمة القانونية للدليل الرقمي (الإلكتروني)

تظهر قيمة الدليل الرقمي من خلال إبراز ميزاته التي تميّزه عن غيره من الأدلة

أولا-تعريف الدليل الرقمي:تعدد تتعاريف الدليل الرقمي بين من اعتمد في تعريفه على الجانب التقني، ومن اعتمد على الجانب القانوني، فعرّف الدليل الإلكتروني بأنّه: «كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي ».

فهو جميع البيانات الرقمية التي يمكن أن تثبت بأنّ هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو بين الجاني والضحيّة، والبيانات الرقمية هي مجموعة

[1]- سعيد علي نعيمي ،اليات التحقيق و التحري في الجرائم المعلوماتية في القانون الجزائري ،مذكرة ماستر ،كلية الحقوق و العلوم السياسية ،قسم الحقوق ،جامعة لحاج لخضر ،باتنة ن2012 ،ص105.

الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، خرائط، أصوات أو الصوّر»[1].

أمّا المشرع الجزائري نجد أنه لم يعرف الدليل الالكتروني بل ركز على الجانب الإجرائي.

ثانيًا -مميزات الدليل الإلكتروني.

يتصف الدليل الرقمي بعدّة خصائص تميزه عن الدليل العادي وهي:

س- الدليل الرقمي دليل علمي يتشكل من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات.

ش- إمكانية نسخ الدليل الرقمي، بحيث يمكن نسخ نسخة مطابقة للأصل وهي الميزة التي لا تتوفر في الأدلة التقليدية.

ص- الدليل الرقمي متنوع ومتطوّر ويمكن أن يكون وثيقة معدة بنظام المعالجة الآلية للكلمات، كما يمكن أن يكون صورة ثابتة أو متحركة أو معدّة بنظام التسجيل السمعي أو أن تكون مخزنة في نظام البريد الإلكتروني.

ض- صعوبة التخلص من الدليل التقني والرقمي: وهي أهم خصائص الدليل الرقمي، حيث مكن استرجاعها بعد محوها وإصلاحها، وذلك باستخدام أدوات وبرمجيات ذات طبيعة رقمية متطوّرة.

الفرع الثاني

دور الدليل الرقمي في مجال الإثبات

يعتبر الدليل الإلكتروني أهم دليل في إثبات وضبط جرائم الكمبيوتر والانترنت، كما له دور مهم وحجيّة في الكشف عنها[2].

[1] -حسام فاضل حشيش، الدليل الالكتروني ودوره في الاثبات الجنائي معلقا عليه بأحكام القضاء الاماراتي مع شرح للجرائم المعلوماتية قسم القانون الجنائي، دار مصر للنشر والتوزيع،القاهرة ،2019،ص136.

[2] - جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجي، دار النهضة العربية، القاهرة، مصر، 2002، ص63.

أولا-حجيّة الدليل الإلكتروني:

يقصد بحجيّة الدليل الإلكتروني قوتهاالاستدلالية في إبراز الحقيقة وصدق نسب الفعل الإجرامي إلى شخص معيّن أو كذبه، وتتوقف القيمة القانونية التي يتمتع بها الدليل التقني على مسألتين مهمتين هما: مشروعية هذا الدليل ومصداقيته.

يتسع ويضيق قبول الدليل الرقمي تبعًا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة وفي هذا الصدد نجد المشرع الجزائري وكغيره من المشرعين أفرد نصوص تساعد القاضي على قبول أو عدم قبول أي دليل بما في ذلك الدليل التقني.

كما أنّ حريّة الإثبات في المسائل الجزائية من المبادئ المستقرّة في نظرية الإثبات وبذلك أقرّ المشرع الجزائري مبدأ حرية الإثبات في المادة 212 من قانون الإجراءات الجزائية حيث نصّت على أنّه: «**يجوز إثبات الجرائم بأية طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمًا تبعًا لاقتناعه الشخصي**»[1].

ثانيا-شروط اكتساب الدليل الالكتروني كحجية للإثبات: اذا كان الدليل الالكتروني بحكم طبيعته العلمية وموضوعتيه وحياده يمثل حجة صادقة عن الواقعة.إلا انه لا يستبعد أن يكون موضوع شك في سلامته،ولذلك من أجل الأخذ به كحجة إثبات لابد يقوم على الشروط العناصر التالية:

1-يقينية الدليل الالكتروني

معناه أن الأدلة الالكترونية يجب ان تكون غير قابلة للشك أو الترجيح حتى يشيد عليها الحكم بالإدانة لأنهلا مجال لدحض قرينة البراءة او افتراض عكسها الا عند بلوغ اقتناع القاضي حد الجزم واليقين[2]

[1]- القانون رقم 66-155 المعدل والمتمم، المرجع السابق.

2-جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسيةجامعة مولود معمري. تيزي وزو .2018، ص152.

3-علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002، ص 463.

ويعتمد القاضي الجزائي عادة لبلوغ اليقين والجزم في اقتناعه بالأدلة على نوعين من المعرفة والتي هي المعرفة الحسية التي تستنبط من الحواس بعد معاينته لهذه المخرجات وفحصها. والمعرفة الفنيةالتي يدركها القاضي عن طريق التحليلات والاستقراءات والاستنتاجات الي يجريها على المخرجات الالكترونية وربطها بالملابسات التي أحاطت بها.

ثانيا: وجوب مناقشة الدليل الالكتروني

إن سلامة الدليل الالكتروني من العبث والخطأ في الاستنباط لا يكفي لاكتسابه حجية دامغة في الإثبات بل لا بد أيضامن مناقشة هذا الدليل بصفة علانية في جلسة المحاكمة وفقا لمبدأ أساسي في الإجراءات الجزائية هو مبدأ الشفوية والمواجهة بالتالي لايجوز للقاضي أن يبدي اقتناعه من معلومات شخصية حصل عليها خرج الجلسة أو في غير نطاق المرافعات والمناقشات التي جرت فيها. كما لايجوز له أن يبدي اقتناعه على رأي الغير إلاإذا كان من الخبراء والفنيين الذين استشارهم وفقا للقانون.

الفرع الثالث

موقف المشرع الجزائري من الدليل الإلكتروني

لقد نص المشرع الجزائري على الإثبات الجنائي في المادتين 212 و307 من قانون الإجراءات الجزائية حيث حسم موقفه بالنسبة لطرق الإثبات من خلال هاتين الأخيرتين وذلك حين نص في المادة 212 على أنه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك.وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي[1].

ونص في المادة 307 بأن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما.

[1] جمال براهيمي، المرجع السابق، ص157

فالنظر الى هاتين المادتين يتضح أن المشرع الجزائري تبنى كأصل عام نظام الإثبات الحر أو الاقتناع الشخصي للقاضي الجزائي .

الفصل الثاني

الإطار الإجرائي للتحقيق في الجريمة الالكترونية

لقد أثارت ظاهرة الإجرام الإلكتروني بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي،بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية. تزداد المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها غالبا ببيانات المعالجة الآلية وكيانات منطقية غير مادية، ناهيك عن إمكانية محوها وتمويه أثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية. كما امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي من القانون الجزائي بشكل أوسع مع مرور الوقت، لأن نصوص هذا القانون وضعت لتحكم الإجراءات المتعلقة بالجرائم التقليدية الي ترتكب في عالم مادي ملموس، على خلاف الجرائم الإلكترونية التي ترتكب في عالم افتراضي غير مادي.

غير أن باعتبار الجريمة الإلكترونية جريمة عابرة للحدود الوطنية فإن مواجهتها من طرف دولة واحدة تقلل من فرصة مكافحته إلا إذا كان من الضروري مواجهتها من طرف جهات تختص بأساليب البحث والتحري عن الأدلة في المجال الرقمي التي تعتمد أساسا على الكفاءة في مجال تكنولوجيا الإعلام والاتصال وذلك على الصعيدين الوطني والدولي،إلى جانب تعزيز التعاون الدولي في المجال الإجرائي للتصدي لمثل هذا النوع من الإجرام،لذلك وأمام هذا الوضع أثير التساؤل حول الأساليب المعتمدة لقمع الإجرام المعلوماتي على الصعيد الوطني والدولي وعن مدى نجاعة التعاون القائم بين الدول في مكافحة الإجرام السيبيراني.

هذا ما سنحاول الإجابة عنه من خلال المبحث الأول تحت عنوان الأساليب الوطنية للتحقيق في الجريمة الالكترونية والمبحث الثاني المعنون بالأساليب الدولية للتحقيق في الجريمة الالكترونية.

المبحث الأوّل

الأساليب الوطنية للتحقيق في الجريمة الإلكترونية

إنّ التطوّر الحالي الذي لحق بثورة المعلومات والاتصالات وما أفرزته من وسائل إلكترونية متقدمة ومتعدّدة قد انعكس سلبًا على الحياة البشرية وذلك بالجرائم التي نتجت عن ذلك، والتي يصعب مواجهتها جنائيًا.

بحيث انعكس أثر هذا التطوّر على قانون العقوبات وكذا على قانون الإجراءات الجزائية، بشكل جعل بعض أحكام هذه القوانين لا تطبق بسبب عجز قانون العقوبات عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم منهج بعض الإجراءات التقليدية وهذا ما سوف نتطرق إليه في هذا المبحث حيث سنعالج الأساليب التقليدية للتحقيق في الجريمة الإلكترونية **(المطلب الأول)**، ثم الأساليب المستحدثة لمواجهة هذا النوع من الإجرام**(المطلب الثاني)**.

المطلب الأول

الأساليب التقليدية للتحقيق في الجريمة الإلكترونية

ممّا لا شك فيه أنّ المشرّع لم يجزم على استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معيّنة والتي سوف نراها من خلال الفرع الأوّل والفرع الثاني.

الفرع الأول

التفتيش في البيئة الإلكترونية

لم يورد المشرع الجزائري تعريفا خاصًا ودقيقًا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وأحاطه بضوابط صارمة نظرًا لأهميته في كشف الأدلة من جهة، وخطورته فيها يترتب عنه من مساسه لحرية الأشخاص وبكرامتهم من جهة أخرى، وخير

دليل على ذلك اهتمام الدستور الجزائري[1] بأهمية هذا الإجراء من خلال نص المادة 47 منه والتي تنص على أنه: «**لا تفتيش إلاّ بمقتضى القانون وفي إطار احترامه ولا تفتيش إلاّ بأمر مكتوب صادر عن السلطة القضائية المختصة**»

فقد يتطلّب التحقيق تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق هو في الأصل من اختصاص سلطة التحقيق، المتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات إلاّ أنّه يخوّل استثناء لرجال الضبطية القضائية في حالات محددة قانونًا[2].

وقد أجمع الفقه الجنائي على أنّ التفتيش باعتباره إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة.يتبيّن من هذا أن التفتيش ما هو إلاّ وسيلة للإثبات المادي غايته ضبط الأدلة الخاصة بالجريمة، خاصة التقليدية منها.

غير أنّ التفتيش بالرّغم من أنه إجراء مهم لضبط الأدلة إلاّ أنه يتم تحت شروط حيث يقتضي المبدأ العام في تفتيش المساكن أن يتم في ساعات محددة. فطبقا للمادة 47 من قانون الإجراءات الجزائية فإنّه: «**لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة 05 صباحًا، ولا يجوز بعد الساعة الثامنة 20 مساءا إلاّ إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونًا**»[3]،لكن استثناءً وفيما يخص بعض الجرائم المستحدثة بما فيها الجرائم الماسة بأنظمة

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية رقم 76 المؤرخة في 8 ديسمبر 1996 المعدل والمتمم.

2 -القانونرقم 06-22 المؤرخ في 20ديسمبر سنة 2006 يعدل و يتمم الامر رقم 66-155 يتضمن قانون الاجراءات الجزائية، جريدة رسمية العدد84، صادر بتاريخ 2006/12/24.معدل ومتمم.

المعالجة الآلية للمعطيات فإنّ ما نصت عليه الفقرة الأولى من المادة 47 يتنافى مع الطبيعة غير المادية لهذه الجرائم.

كما نصّت الفقرة الثالثة من المادة 47 على أنّه: «**وعندما يتعلّق الأمر بجرائم المخدّرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم المالية بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنّه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو اللّيل وذلك بناءً على إذن مسبق من وكيل الجمهورية المختص**».

كما يمكن أن يتم التفتيش حتى إذا لم يحضر صاحب المسكن مهما كان سبب ذلك، فتطبق المادة 47 مكرر التي تضع أحكاما خاصة، إذ جاء فيها أنّ «**إذا حدث أثناء التحري في جريمة متلبس بها أو تحقيق متعلق بإحدى الجرائم المذكورة في المادة 47 فقرة 3 من هذا القانون ان كان الشخص الذي يتم تفتيش مسكنه موقوفًا للنظر أو محبوسا في مكان آخر وأن المال يقتضي عدم نقله إلى المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو الاحتمال فراره، أو اختفاء الأدلة خلال المدة اللازمة لنقله، يمكن أن يجرى التفتيش بعد الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق وبحضور شاهدين مسخرين طبقا لأحكام المادة 45 من هذا القانون**[1] **أو بحضور ممثل يعيّنه صاحب المسكن محل التفتيش**»[2].

كما نصت المادة 5 فقرة 1 من القانون رقم 09-04 المتضمن لقواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السالف الذكر على أنه: «**يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها الدخول بغرض التفتيش ولو عن بعد**

[1]- القانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006، المرجع السابق.

[2]- أ. نادية حسان، المرجع السابق، ص 28.

إلى: منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها ومنظومة التخزين المعلوماتية».

وهنا يثار التساؤل عن فعالية تفتيش المكونات المعنوية؟

وللإجابة على ذلك يقتضي الأمر الوقوف عند الضمانات والضوابط التي يجب على المحقق احترامها والتقيد بها قبل وأثناء قيامه بعملية التفتيش فمنها ما يتعلّق بمحل التفتيش وما منها ما هو إجرائي.

أولاً: محل التفتيش الإلكتروني.

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته، والسّر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد الأماكن المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة.

فلما كان المستودع في الجرائم الإلكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية (Hard wear) كوحدات المعالجة المركزية (Processeur)، ووحدات الإدخال والإخراج، ووحدات التخزين أو ما يسمى بوحدة التحكم (Unité de control) ومكونات أخرى منطقية (Soft ware) كبرامج النظام الأساسية، البرامج التطبيقية والبيانات المعالجة آليا، كما أنه له شبكات اِتصالات بعدية سلكية ولا سلكية متواجدة على المستوى المحلي والدولي، فإنه يستلزم البحث عن مدى قابلية جميع هذه المكونات للتفتيش[1].

[1]- جمال براهيمي، المرجع السابق، ص 15.

1- تفتيش المكونات المادية للحساب:

ليس هناك خلاف على أن الدخول إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها يخضع لإجراءات التفتيش المألوفة، لأنّ حكم تفتيش هذه الماديات يتوقف أساسًا على طبيعة المكان الذي تتواجد فيه.[1]

كما نص المشرع الجزائري في المواد من 44 إلى 47 من قانون الإجراءات الجزائية على أنه للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها، يجب الحصول على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن ومباشرة التفتيش.

فبناءً على ما سبق، يتضح أنّ تفتيش المكونات المادية لجهاز الحاسب وملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أيّة مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، كمراعاة وقت التفتيش الذي يخض لإجراءات التفتيش في الجرائم التقليدية، لأنّ حكم تفتيش هذه الكيانات المادية يتوقف أساسًا على طبيعة المكان الذي تتواجد فيه ما إذا كان عامًا أو خاصًا.

فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكم بحيث لا يجوز تفتيشها إلاّ في الحالات التي يسمح فيها تفتيش المساكن وملحقاته وبالإجراءات والضمانات المقررة قانونًا[2]،ففي القانون الجزائري مثلا قد اشترط في المواد من 44 إلى 47 من قانون الإجراءات الجزائية للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها، الحصول مسبقًا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن ومباشرة التفتيش.

[1]- خالد ممدوح إبراهيم، المرجع السابق، ص 195.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص 195.

أما إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواءً أكانت عامة كالمقاهي أو الحدائق العامة أو الطرق العامة أو أماكن عامة بالتخصيص كمقاهي الانترنتCybercaféومحلاّت بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقًا للأصول الخاصة بتلك الأماكن، ويستوي الأمر بالنسبة للمكونات الموجودة بحوزة شخص ما وبغض النظر عن صفة هذا الشخص، فإنّ التفتيش يخضع لأحكام تفتيش الأشخاص وبالشروط والضمانات القانونية المحددة لذلك.

2- مدى صلاحية مكونات الحاسب المنطقية للتفتيش:

تعتبر الكيانات المنطقية للحاسب مجموعة من البرامج والأساليب والقواعد الأوامر المتعلقة بتشغيل وحدة معالجة البيانات[1]. وبالتالي إذا كان محل التفتيش قد انته بعند صلاحية تفتيش مكونات الحاسب المادية فحسب، فإنّ امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول درجة صلاحيتها لأن تكون محلاً للتفتيش تمهيدًا لضبط الأدلة.

حيث أنّ الخلاف الحاصل يكمن في مسألة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور التساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الإلكترونية أو البرامج في حدّ ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، ويستشعر الفقه صعوبة المسألة بالنظر إلى غياب الطبيعة المادية للمعلومات والبيانات، بما يجعلها تتنافى مع الهدف الذي يصبو إليه التفتيش ألا وهو البحث عن الأدلة المادية.

لذلك سعى جانب من الفقه إلى تعريف التفتيش بمعناه التقليدي، وذلك بالبحث والتنقيب في نظم وبرامج الحاسوب عن أدلة الجريمة الإلكترونية، وحجتهم في ذلك أنه وإن كانت هذه النظم والبرامج عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية

[1]- عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة القضائية، الطبعة الثانية، دراسة مقارنة، منشورات الحلي القانونية، دمشق، 2007، ص 61.

إلاّ أنها قابلة للتسجيل والتخزين والتحميل على وسائط ودعائم مادية معيّنة، ولها كيان مادي محسوس من خلال استشعارها وقياسها لذلك فإنه من الممكن جدًا إخضاعها لقواعد التفتيش التقليدية.

أمّا جانب أخر من الفقه فيرى بأنه لا يمكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لأنّ هذه القواعد وضعت في وقت لم تكن فيه نظم المعالجة الآلية والحواسيب موجودة كما أنّ تطبيقاتها لم تكن معروفة[1].

بالتالي فطبيعة هذه المكونات تتطلّب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعل أحكامها تتلاءم مع متطلبات هذه التقنية. ويبدو أن أغلب تشريعات الدول المتقدمة كالمشرع الفرنسي تميل إلى هذا الاتجاه إلى جانب المشرع الجزائري الذي لم يبق مكتوف الأيدي اتجاه المتغيرات التي تحدث في عالم التكنولوجيات الحديثة، بل قام بدوره باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب ومن بين هذه النصوص المادة 05 من القانون رقم 09- 04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تسمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها [2].

3- ضمانات التفتيش الإلكترونية:

إنا عتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق جعل معظم القوانين الإجرائية تحرص على إحاطته بجملة من الضمانات القانونية والتي تنقسم إلى ضمانات موضوعية وضمانات شكلية أو إجرائية التي سوف نستعرضها على النحو التالي:

[1]- عفيفي كمال عفيفي، المرجع السابق، ص 63.

[2]- أنظر المادة 05 من القانون 09-04، السالف الذكر.

أ- الضمانات الموضوعية للتفتيش الإلكتروني:

تتمثل هذه الضمانات في مجموعة من الشروط وهي:

- سبب التفتيش:

يعتبر عنصر التسبيب ضمانة قانونية لصحة ومشروعية إجراء التفتيش حيث يتحقق بوقوع جريمة ما يتم بموجبها توجيه الاتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن قوية تفيد تورطهم في هذه الجريمة.

- **وقوع جريمة إلكترونية تحمل وصف جناية أو جنحة**

اتفقت معظم تشريعات الدول على أنه لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي للجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت الدلائل والتحريات على أنها ستقع بالفعل يعد إجراء غير مشروع.

ولا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة، بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة، حيث تستثنى من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاته موحرمة منازلهم من أجلها.[1]

هذا هو النهج الذي سار عليه المترع الجزائري حيث أدرج في الفصل السابع من القانون رقم 04-15[2]، وكذا في القانون رقم 09 04 جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.

[1]- جمال براهيمي، مرجع سابق، ص 32.

[2]- القانون 09-04، المرجع السابق.

- **اتهام شخص أو عدة أشخاص معنيين بارتكاب جريمة إلكترونية:**

إنّ مجرد وقوع جريمة إلكترونية لا يكفي لقيام السبب لتفتيش شخص ما أو تفتيش مسكنه، بل يجب أن يوجّه إليه الاتهام بصفة فاعلاً أصليًا أو شريكًا ساهم في ارتكاب واقتراف تلك الجريمة التي وقعت ويجب أن تكون هناك دلائل قوية على ذلك.

ويقصد بالدلائل الكافية في الجريمة الإلكترونية مجموعة من المظاهر المعنية التي تقوم على السياق العقلي والمنطقي لملابسات الواقعة وكذلك خبرة وحرفة القائم بالتفتيش.

- **توافر قرائن قوية على وجود بيانات أو معدّات معلوماتية لدى المتهم بالجريمة الإلكترونية أو غيره:**

إنّ توجيه الاتهام إلى شخص أو أشخاص معنيين بمساهمتهم في ارتكاب جريمة من نوع جناية أو جنحة منصوص عليها في القانون لا يكفي لقيام سبب التفتيش في الجرائم الإلكترونية، إنّما يجب أن تتوافر لدى المحقق أدلة أخرى تكون قوية وقرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أية معلومات أو مستندات إلكترونية تفيد في استجلاء الحقيقة.

حيث يتم الحصول عادة على هذه القرائن من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعد ما يتم إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش.

لكن بخلاف ما هو عليه في الجرائم التقليدية من سهولة هذه الضمانة، فإنّ التوصل إلى قرائن ودلائل قوية كسبب لقيام التفتيش في جريمة إلكترونية ليس بالأمر الهين والسهل، نظرًا للصعوبات والعقوبات التي تواجه سلطات التحرّي والاستدلال في ذلك[1].

[1]- د. جمال براهيمي، المرجع السابق، ص 35.

- محل التفتيش:

لمشروعية التفتيش في الجرائم الإلكترونية وصحته يشترط أن ينصب على محل، ويقصد هنا كل المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الإلكترونية.

حيث أنّ المحل في الجرائم الإلكترونية لا يكون قائمًا بذاته بل يكون إما مقترنا بمكان معيّن كمسكن المتهم أو بشخص معيّن (مالك أو حائز) كما هو الشأن في الحاسب المحمول أو الهاتف النّقال.

لذلك قبل البدء في التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الإلكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لأنّ حكم تفتيش هذه الوسائل يتوقّف غالبًا على طبيعة المكان الذي تتواجد فيه. ويشترط في المحل الذي يقع عليه التفتيش أن يكون معينا نافيا للجهالة ويكون مما يجوز تفتيشه.

كذلك بالنسبة للتفتيش عن بعد عبر شبكة الاتصال او التفتيش الالكتروني الذي لا يستلزم الاعتداء المادي لحرمة المكان أو الشخص المراد تفتيشه[1].

- السلطة المختصة بالتفتيش:

لكي يكون التفتيش في الجرائم الإلكترونية أو غيرها من الجرائم صحيحًا ومنتجًا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية، باختلاف تشريعات الدول، ومع مراعاة الاختصاص المحليّ الذي يتحدّد عادة إمّا بمكان وقوع الجريمة أو بمكان إقامة المتهم، أو بمكان القبض عليه طبقا المادة 40 ق.إ.ج.ج.

إلاّ انه استثناء، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وذلك وفقا للشروط والإجراءات المنصوص عليها في القانون، ولصحة إجراء التفتيش الذي يقوم به رجال الضبطية يجب أن يكون بناءً على إذن صريح صادر من هيئة مختصة.

[1]-جمال براهيمي، نفس المرجع ، ص 36.

لكن السؤال الذي يطرح نفسه هل يجوز لضباط الشرطة القضائية بمقتضى الإذن بتفتيش مسكن المتهم الولوج إلى الأجهزة الإلكترونية والتغلغل في منظومتها المعلوماتية للبحث عن أدلة الإثبات يمكن أن تكون محل ضبط؟

إن الإجابة هي أن معظم التشريعات استقرّت على أنّه يكفي الحصول على الإذن بتفتيش مسكن المتهم حتى يكون لضباط الشرطة القضائية الحق في تفتيش كل الأجهزة الإلكترونية وحجتهم في ذلك أنّ هذه الأخيرة بمختف أنواعها تمثل مجالاً حيويًا ضخمًا لتخزين مئات بل ملايين المعلومات والبيانات، لذلك فلا يعقل مع هذه الصورة التخزينية الهائلة تصور إصدار إذن بالتفتيش فيها[1].

أما موقف المشرع الجزائري إزاء هذه المسألة فهو غير واضح وحاسم اذّ بالرجوع إلى القواعد الخاصة بالتفتيش المذكورة في قانون الإجراءات الجزائية نجد أنها تتعلّق بالتفتيش التقليدي الذي ينص عادة على المكونات المادية، أما في القواعد المتعلقة بالتفتيش الإلكتروني فالمشرع لم يحسم أمره، وإنما اكتفى فقط بالإشارة إلى ضرورة قيام جهات التحقيق بإعلام السلطة القضائية المختصة مسبقًا قبل تمديد التفتيش إلى منظومة معلوماتية أخرى مرتبطة بالجهاز المأذون بتفتيشه.

لكن وطبقا لمبدأ حرمة الخصوصية التي يحميها المشرّع، فإنّ هذا الأخير يميل إلى عدم جواز الولوج إلى النظام المعلوماتي وما يمكن أن يحتوي من معلومات وبيانات سرية وخصوصية الأشخاص دون إذن خاص من السلطة القضائية المؤهلة ومؤدى ذلك أن ضابط الشرطة القضائية يحتاج في الغالب لتفتيش منظومة معلوماتية إلى إذنين بالتفتيش الأوّل يخص السكن الذي يتواجد فيه الجهاز والثاني يتعلّق بتفتيش مكونات الجهاز أو المنظومة المعلوماتية في حدّ ذاتها.

1- المادة 40 من قانون الإجراءات الجزائية، مرجع سابق.

2- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، ط2، دار الفكر الجامعي، مصر، 2011. ص55.

ب - الضمانات الشكلية للتفتيش الإلكتروني:

إنّ الهدف من وضع ضمانات شكلية للتفتيش إلى جانب الضمانات الموضوعية لا يكمن فقط في تحقيق مصلحة القضاء في ضمان صحة الإجراءات التي تتخذ في جمع الأدلة وضمان مشروعيها، وإنّما يكمن كذلك في حماية الحقوق والحريات العامة الفردية وذلك بوضع سياج أمني والذي يتمثل في الضمانات الشكلية التالية:

***احترام الميقات الزمني:**

إنّ فرض قيود زمنية لإجراء التفتيش يعدّ ضمانة إجرائية مهمة جدًا لحماية الحقوق والحريات العامة للأفراد من أي اعتداء، حيث حدّد المشرّع الجزائري أوقات التفتيش من الساعة الخامسة (05 h00) صباحًا إلى غاية الساعة الثامنة (08h00) مساءًا، ونص في قانون الإجراءات الجزائية على أنّ: «**لا يجوز البدء في التفتيش المسألة أو معاينتها قبل الساعة الخامسة صباحًا ولا يعد الساعة الثامنة مساءًا**».

إلاّ أنّه وفي حالات استثنائية يجوز الخروج عن تلك القاعدة[1]، فعندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة للمعطيات وجرائم الأموال والإرهاب وكذلك الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز التفتيش في أية ساعة من ساعات النهار والليل حيث استغنى المشرع الجزائري عن شرط الميقات الزمني وسمح لرجال الضبطية القضائية التفتيش في أي وقت لكن بناءً على إذن مسبق من وكيل الجمهورية[2] كما سبق ذكره.

***** حضور الأشخاص المعنيين أثناء التفتيش:**

يسهر المشرع الجزائري إلى جانب معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يقوم مقامه معتبرين ذلك من القواعد الأساسية التي يترتب عن مخالفتها البطلان.

[1]-د/عزالزين عثماني، مرجع سابق، ص57.
[2]- د/عزالدين عثماني،مرجع سابق، ص57.

أما فيما يخص التفتيش في الجرائم الالكترونية، فالمشرع وإقرارا منه بخصوصية جرائم الاعتداء على نظم المعالجة الآلية للمعطيات وما يتطلبه الأمر من بسط نوع من السرية أثناء جمع الدليل التقني فيها، عاد بموجب الفقرة الأخيرة من المادة 45 من ق. إ. ج واستثنى هذه الجرائم من تطبيق إحكام المادة السابقة، وأصبح بإمكان الضبطية القضائية إجراء التفتيش في جرائم المعالجة الآلية دون التقيد بشرط حضور المتهم أو من ينوب عنه أو حتى الشهود[1].

أما فيما يخص الجرائم الإلكترونية فإنّ المشرع خرج عن هذا الشرط وهذا إقرارًا منه بخصوصية هذه الجرائم والتي تمس بنمط المعالجة الآلية للمعطيات وما يتطلبه الأمر من بسط نوع من السّرية أثناء جمع الدليل التقني، واستثنى تطبيق أحكام المادة السابقة وأصبح بإمكان الضبطية القضائية إجراء التفتيش في جرائم المعالجة الآلية للمعطيات حتى وإن لم يحضر المتهم أو من ينيب عنه أو حتى الشهود.

وفي رأينا أنّ ما قام به المشرع الجزائري كان صائبًا وذلك بعدم تطبيقه لأحكام المادة 45 من ق.إ.ج على الجرائم الإلكترونية وهذا نظرًا لطبيعة هذه الجرائم وما تتميّز به من سرعة فائقة في محور آثارها وفقدان الدليل الذي تتطلبه لإثباتها.

*** تحرير محضر تفتيش:**

تعرف محاضر الشرطة القضائية بأنها «الوثائق المكتوبة التي يحررها ضابط الشرطة القضائية أثناء ممارسته لمهامه ويضمنها ما عاينه أو تلقاه من صلاحيات أو قام به بحسن عمليات تدخل في اختصاصه»[2]، وتسمى أيضًا محاضر الشرطة القضائية بمحاضر التحقيق الأولي وتكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة، فإضافة إلى الضمانات المتعلقة بالميقات الزمني للتفتيش والأشخاص المطلوب حضورهم، اشترط كذلك المشرّع أن يحرّر محضر التفتيش تدوّن فيه كل الخطوات والإجراءات المتخذة

2 بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت،2012،ص414.

[2]- د. عز الدين عثماني، المرجع السابق، ص 58.

أثناء عملية التفتيش ولا يستوجب القانون شكلاً أو شروطا خاصة في التفتيش، بل يكفي أن يتوفّر فيه ما تستوجبه القواعد العامة في المحاضر عمومًا كالكتابة باللّغة الرسمية، تاريخ تحريره، توقيع محرره....الخ.

ومن الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش، وجوب استعانة المحقق بكاتب يقوم باصطحابه لتحرير المحضر وتدوين ما تم من إجراءات وهو ما نصت عليه المادة 79* من قانون الإجراءات الجزائية[1].

فلا يختلف محضر التفتيش في مجال الجرائم الإلكترونية عن غيره في الجرائم التقليدية سوى أن بالإضافة إلى الشكليات السابقة لا بد من إحاطة القائم بالتفتيش في هذا النّوع من الجرائم بتقنية المعلوماتية الرقمية أو الاستعانة بأهل الخبرة التقنية والاختصاص في هذا المجال ليساعده في صياغة وتحرير محضر يغطي كل الجوانب الفنية للتفتيش.

ثانيا -ضبط الأدلة من البيئة الإلكترونية:

يعتبر الضبط من إجراءات جمع الأدلة الهدف الرئيسي من التفتيش والأثر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجدية وقعت والتي تفيد مثلا في كشف الحقيقة عنها وعن مرتكبيها، ووضعها في إحراز مختومة لتقدم إلى الجهة القضائية المختصة كدليل إثبات.

وتحصيل الأدلة في الجرائم الإلكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته من الأقراص الصلبة، الأقراص والأشرطة الممغنطة، الطباعة، البرامج اللينة وغيرها من الملحقات، وفي هذه الحالة لا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحري التقليدية[2].

2-تنص المادة 79 على أنّه: «**يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائمًا بكتاب التحقيق ويحرّر مضطرا بها يقوم به من إجراءات**».

[2]- حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017، ص80.

كما قد يرتبط الدليل الإلكتروني بالمكوّنات المعنوية للحاسب، لمختلف البرامج والبيانات المعالجة آليات والمراسلات والاتصالات الإلكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الإلكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات إشكالا حول مدى إمكانية ضبطها وفقًا لقواعد الضبط المألوفة مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلاّ على الأشياء المادية؟

لكن اتفاقيةبودابست لعام 2001 حسمت هذه المسألة، وذلك بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الإلكترونية لأن تكون محلاً للضبط وذلك من خلال الفقرة 03 من المادة 19 منها التي نصت على «... **يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئاتها المختصة سلطة ضبط الدليل أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين** 01 و02».

فبالرجوع إلى هذه الفقرة، نجدها تخوّل سلطات البحث والتحرّي طريقتين لضبط البيانات المعلوماتية والأدلة الرقمية التي كانت موضوع التفتيش أو الولوج بطريقة مشعبة عملا بالفقرتين 01 و02 من المادة 19.

حيث تتحقق الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث عن دعامة تخزينية مادية (كالأقراص الممغنطة، بطاقات الذاكرة، فلاش ديسك) وتلف هذه الأخيرة قابل للضبط والوضع في أحراز مختومة حسبما هو مؤثر في قواعد تحري الدليل التقليدية المنصوص عليها في قوانين الإجراءات الجزائية وهي الطريقة المقصودة في المادة 19 بمصطلح "**الضبط** saisie".

أما الطريقة الثانية فتتضمن تدابير جديدة مستخدمة خصيصا لضبط الأدلة الجنائية الرقمية، وهي المعبّر عنها في هذه المادة بمصطلح "الحصول بطريقة مشابهة على البيانات المعلوماتية" والتي تكون باستعمال تقنيات وتدابير الحماية الفنية كتقنيات التشفير والترميز برامج منع الكتابة، واستخدام خوارزميات "تجزئة" للملفات المشفرة من أجل منع الأشخاص

المرخص لهم باستخدام المنظومة المعلوماتية والوصول إلى المعطيات والبيانات الأصلية التي تحتويها هذه المنظومة أو القيام بنسخها[1].

وبالتالي فإن المشرع الجزائري أدرك خطورة الجرائم الإلكترونية من خلال النصوص السابقة وأن الجزائر ليس بمأمن عنها، فقام بتلافي القصور الموجود في قانون الإجراءات الجزائية فيما يخص ضبط الكيانات المنطقية للحاسب الآلي. لكن الواقع أثبت وجود صعوبات كثيرة ما زالت تواجه عملية ضبط هذه الأدلة ولعل أهمها الأحزمة الأمنية المفروضة من طرف مستخدم النظام للحد من الدخول والاطلاع على البيانات التي يحتويها هذا القطاع، وما يزيد من الأمر تأزمًا هو عدم معرفة المحقق الإلكتروني الجنائي لكلمات السّر أو ثغرات المرور أو ثغرات ترميز البيانات.

الفرع الثاني

المعاينة والخبرة في الجريمة الإلكترونية

تعتبر المعاينة من أهم أساليب التحقيق نظرا لما يمكن أن توفره من أدلة إثبات خاصة في الجريمة التقليدية نظرا لسهولة إجرائها في هذه الأخيرة، غير أن الأمر يختلف في الجرائم الإلكترونية وذلك راجع إلى الطبيعة الخاصة للسلوك الإجرامي فيها بالإضافة إلى اعتبارها من الجرائم المستحدثة التي تخلف مسرح مادي، ممّا استوجب ابتكار أساليب خاصة بالمعاينة والخبرة لاستجلاء الحقيقة في هذا النوع من الإجرام.

لذلك سنتناول مفهوم المعاينة في الجرائم الإلكترونية كنقطة أولى ثم مفهوم الخبرة في الجرائم الإلكترونية كنقطة ثانية.

[1]- د. هلال عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، 2011، ص 251.

أولا-المعاينة في الجريمة الإلكترونية

1/-تعريف المعاينة في الجريمة الإلكترونية وشروطها.

أ- تعريف المعاينة في الجريمة الإلكترونية

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة للكشف عن الحقيقة وعن مرتكبيها، بحيث يجب على السلطات المختصة الانتقال إلى مسرح الجريمة فور وقوعها، وذلك حتى لا يغيّر الجاني الآثار المادية للجريمة أو إزالتها[1].

ويقصد بالمعاينة في القانون الجنائي بأنّها: «إثبات مباشر ومادي لحالة شيء أو شخص معين ويكون ذلك خلال الرؤية أو الفحص المباشر للشيء بواسطة الإجراءات».

أمّا المعاينة في الجريمة الإلكترونية فيقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العلمية. وعليه عند تلقي بلاغ عن وقوع الجريمة الإلكترونية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، غير أن هذا الانتقال لا يكون في العالم المادي وإنّما في الفضاء الإلكتروني (العالم الافتراضي)، وبالتالي يتم معاينة هذا النوع من الجرائم إمّا من قبل قاضي التحقيق أو ضابط الشرطة القضائية وذلك من خلال:

- مكتبه بالمحكمة أو المركز من خلال الحاسوب الخاص به.

ط- اللجوء إلى مقهى الانترنتCyber café.

ظ- اللجوء إلى مكان عمل مزوّد بخدمة الانترنت.

كما يجوز الانتقال من خلال مقرّ مكتب الخبير التقني المختص إذا سمح له القانون بذلك، ولهذا يجب الانتقال إلى العالم الافتراضي بسرعة من أجل منع زوال آثار الجريمة[2].

---

[1]- نصيرة بوحزمة، المرجع السابق، ص 350.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص ص156-157.

ب: شروط صحة معاينة الجريمة الإلكترونية.

حتى تحقق المعاينة الهدف المرجو منها في كشف غموض الجريمة والتوصل إلى الفاعل لابدّ من مراعاة عدّة شروط أهمها:

*** سرعة الانتقال إلى مكان وقوع الجريمة الإلكترونية:**

على السلطة المختصة بالتحقيق الانتقال فور وصل خبر وقوع الجريمة إلى علمها إلى مكان الواقعة، ضمانًا لعدم تغيير شكل مشرح الجريمة عن الوضع والحالة التي تركها الجاني عليه والحصول على شهود عيان للواقعة[1].

*** السيطرة والتحكم على مكان وقوع الجريمة الإلكترونية:**

عند وصول سلطة التحقيق لمكان الحادث للمعاينة لابد من إتباع ما يلي:

ع- منع أي شخص من مبارحة مكان الواقعة حتى تنتهي الضبطية القضائية من تحرياتها.

غ- منع تواجد أي شخص داخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة سواءً بقصد أو بخطأ.

ف- حماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص.

ق- قيام الخبراء كل حسب اختصاصه برفع الآثار من مسرح الجريمة، وأوّل خبير يقوم بعمله هو خير التصوير.

*** التسلسل في معاينة الجريمة الإلكترونية:**

لضمان إجراء المعاينة بصورة مرتبة ومتسلسلة يجب على السلطة المختصة بالتحقيق الالتزام بنقطتين أساسيتين: الأولى هي تحديد نقاط البدء في المعاينة، أما الثانية هي عدم الانتقال من مكان لآخر إلاّ بعد التأكد تمامًا من معاينته وعدم ترك أيّة أشياء به.

1-**سرحان** حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرقي، المجلد عشرون، العدد الرابع، الشارقة الإمارات العربية المتحدة ،2011، ص 42

*** الدقة والعناية الفائقة في معاينة مسرح الجريمة الإلكترونية:**

وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، فإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات بما هو مرتبط بالجريمة كأجهزة الكمبيوتر والماسح الضوئي، الطابعة، الأسطوانات المدمجة، وغيرها من الوسائل المستخدمة في اقتراف الجريمة الإلكترونية[1].

*** التحفظ على مسرح الجريمة الإلكترونية بعد المعاينة:**

والعلّة في ذلك واضحة وهي إمكانية العودة إليه كلّما أراد المحقق كشف غموض أو التأكد من آثار معيّنة.

*** تدوين المعاينة في الجريمة الإلكترونية:**

يكون ذلك كتابيًا ورسميًا وتصويريًا كتصوير أجهزة الحاسب الآلي المضبطة بمحل ارتكاب الجريمة والأجهزة الطرفية المتصلة بها، مع التركيز بصفة خاصة على الأجهزة الخلفية للحاسب الآلي وملحقاته، مع مراعاة تسجيل تاريخ ووقت ومكان اِلتقاط كل صورة.

2/ مجال المعاينة في الجريمة الإلكترونية.

يعتمد المحقق لإجراء المعاينة في الجرائم الإلكترونية بحثا عن الأدلة الإلكترونية على فحص مكونات الحاسب الآلي الخاصة بالجاني والمجني عليه وكذا أنظمة الاتصال بالأنترنت.

أ- المعاينة الواقعة على مكونات الحاسب الآلي:

تعتبر الحواسيب مصدرًا غنيًا بالأدلة الإلكترونية خاصة الحواسب الشخصية التي تعدّ بمثابة أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم، لذلك فإنّ عملية فحص هذه الحواسيب

[1]- سرحان حسن المعيني، المرجع السابق، ص 353.

تمثل نقطة البداية في الكشف عن خطايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها[1].

أمّا فيما يخص المعاينة الواقعة في الجرائم الإلكترونية يجب التمييز بين حالتين أساسيتين:

ك- الحالة الأولى: هي المعانة الواقعة على المكونات المادية للحاسب الآلي.

ل- الحالة الثانية: فتخص المعاينة الواقعة على المكونات المعنوية أو المنطقية للحاسب.

أ-1 معاينة المكونات المادية للحسب الآلي:

كمعاينة أشرطة الحاسب، مفاتيح التشغيل، والأقراص وشاشة العرض وغيرها، فلا توجد أيّة صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضع هذه المكونات لمعاينتها من طرف ضابط الشرطة القضائية وكذا وضع الأختام في الأماكن التي تمت معاينتها وضبط كل ما استعمل في ارتكاب الجريمة والتحفّظ عليها مع إخطار وكيل الجمهورية بذلك.

أ-2 معاينة المكونات المعنوية أو المنطقية للحاسب الآلي:

يفترض في القائمين بهذه المعاينة الإلمام الجيّد بأجهزة الحاسب الآلي وبرامجه نظرًا لأنّ التفتيش يتم داخل جهاز الحاسب نفسه وما يحتويه من برامج، وبالتالي ضبط كل ما يفيد في كشف الحقيقة، غير أنّ الجرائم الواقعة على برامج الحاسب الآلي وبياناته تثير عدّة صعوبات تحول دون فاعلية المعاينة أو فائدتها. ذلك لأنّ برامج الحاسب الآلي مثلا غالبًا ما يشوبها عيب أو قصور ولو جزئي في أداء وظيفتها، وهذا من شأنه أن يؤثر في الحاسب فيجعله محل شك تهتز معه قيمة الدليل.

[1]- جمال براهيمي، المرجع السابق، ص 59.

ب- معاينة أنظمة الاتصال بشبكة الانترنت:

لا يكفي أحيانًا معاينة مكونات الحاسب الآلي وحدها لاستخلاص الدليل الإلكتروني إنّما يتطلب من المحقق أيضًا فحص أنظمة اتصال الحاسب بشبكة الانترنت.ويقصد بها من الناحية الإجرائية تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالأنترنت[1]، وعملية معاينة هذه الأنظمة تشمل أساليب فحص مسار الانترنت، والنظام الأمني، وكذا فحص الخادم،بحيث يتم التفتيش في شبكة الانترنت عن طريق بيانات المتهم على الشبكة.

ونظرًا لخطورة المعاينة ونتائجها التي تترتب عليها الكثير من التحقيقات يجب مراعاة عدّة نقاط قبل المباشرة فيها في الجرائم الإلكترونية والتي من بينها:

م- الإعداد الجيّد قبل المعاينة لعدم تغيير الأدلة أو إتلافها؛

ن- اِصطحاب الخبراء المتخصصين لمرافقة فريق التحقيقات؛

هـ- تصوير الجهاز وملحقات ووضعه في المكان الذي يوجد فيه؛

و- الحرص على المستندات الخاصة بالإدخال وكذلك ملحقات الحاسب الآلي المادية والورقية والمرتبطة بالجريمة وما قد يوجد عليها من آثار؛

ي- الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز....

3/ المعالجة الإجرائية للمعاينة في الجريمة الإلكترونية.

يجب التمييز في هذا الصدد بين ثلاثة حالات:[2]

[1]- جمال براهيم، المرجع السابق، ص 64.

[2]- عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، ط1، دار الحامد للنشر والتوزيع، عمان، الأردن، 2011.

أ - الانتقال للمعاينة في الجرائم المتلبس بها:

نصت الفقرة الأولى من المادة 42* من ق.إ.ج.ج على أنّ «يجب على ضابط الشرطة القضائية الذي بلّغ بجناية في حالة تلبس أن يخطر وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللاّزمة».

حرصًا من المشرع الجزائري على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأوّلية للتحقيق الجنائي، نصّ من خلال المادة 43 من ق.إ.ج.ج على أنّه«يحظر، في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأوّلية للتحقيق القضائي، وإلاّ عوقب بغرامة من 200 إلى 1000 دج. ونص في الفقرة 03 على: أما إذا كان الفاعل يهدف من وراء طمس الآثار أو نزع الأشياء عرقلة سير العدالة يعاقب بالحبس من 03 أشهر إلى 03 سنوات وبغرامة من 1.000 إلى 10.000 دج».

ب -الانتقال للمعاينة في حالة التحقيق الأولي:

يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الأولية بمجرّد أن يعلموا بوقوع الجريمة إمّا بناءً على تعليمات وكيل الجمهورية وإمّا من تلقاء أنفسهم (المادة 63 ق. إ.ج).

أما فيما يخص حالة تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة فيها فلابد من مراعاة شرطين أساسيين نصت عليها المادة 64 من ق.إ.ج.ج كما يلي:[1]

أأ - الشرط الأول: رضا صريح من الشخص الذي تتخذ لديه هذه الإجراءات.

* - الأمر رقم 66-155، المرجع السابق.

[1] - مريم أحمد مسعود، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة ماستر في القانون الجنائي، جامعة ورقلة، 2013، ص 43-44.

ب-ب - الشرط الثاني: أن يكون هذا الرضا بتصريح مكتوب بخط يده صاحب الشأن وإذ كان لا يعرف الكتابة استعان بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة لرضاه.

أمّا إذا تعلّق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة (37 فـ3) ق.إ.ج.ج فتطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر من نفس القانون.

ج- الانتقال للمعاينة في حالة التحقيق الابتدائي:

يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، كما يستعين قاضي التحقيق كالعادة بكاتب التحقيق يحرّر ما يقوم به من إجراءات وهو ما نصت عليه المادة 79 ق. إ.ج.

ثانيا -الخبرة في الجريمة الإلكترونية:

تعدّ الخبرة من أهم الوسائل إلي يلجأ إليها القاضي أو المحقق لاستجلاء حقيقة الجريمة المرتكبة وإسنادها إلى المتهم وتحديد شخص الفاعل مهما كان نوع الجريمة إلكترونية كانت أو تقليدية[1].

1- تعريف الخبرة والخبير في الجريمة الإلكترونية:

يقصد بالخبرة بصفة عامة: «الاستثارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه ". كما تعتبر الخبرة وسيلة من وسائل الإثبات التي تهدف إلى كشف الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر لا لدى المحقق ولا لدى

[1]- أنيس حسين السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، الإسكندرية، 2016، ص

القاضي.كما تقدم الخبرة عونا ثمينا لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى في أداء رسالتها غير أنّ الخبرة تقتضي شرط التخصّص والتعمّق من قبل المتّصف بها، والذي يتمثّل في الشّخص الذي لديه دراية ومعرفة بعلوم التكنولوجيا والتي تكون عن طريق التكوين والتمهين، حيث يعتبر هذا الأخير أهم صعوبة تواجه نظام الخبرة،بحيث يجب تكوين الخبير المناسب الذي سيتم الاستعانة به،باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط المألوفة بالنسبة لتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة على مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية، وبالتالي فإن الشخص لكي يكون خبيرا قضائيا في مجال الجريمة الالكترونية بشكل خاص يجب أن يكون ملما بالجوانب التقنية التالية:

- المعرفة بتركيب الحاسب وصناعته ونظام تشغيله الرئيسي والفرعي؛

- طبيعة بيئة الحاسوب والشبكة من حيث تنظيم وتوزيع عمل المعالجة الآلية وتحديد أماكن التخزين ووسائل الاتصالات؛

- المواضع الرقمية التي يمكن أن تتواجد فيها أدلة الإثبات؛

- كيفية عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة؛

- التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة؛

- المحافظة على الأدلة المستخرجة بشكل يمكن القاضي من فهمها واستيعابها.[1]

2-أنواع الخبرة في المجال المعلوماتي:

الخبرة في المجال المعلوماتي قد تكون خاصة وقد تكون عن طريق المؤسسات التعليمية، وقد تتم عن طريق جهات الضبط القضائي،وهكذا يمكن للقاضي الجزائي اختيار الخبير المعلوماتي من إحدى الفئات التالية:

[1]- فايز محمد راجب غلاب، مرجع سابق، ص362.

أ-الجهات الخاصة:

والتي تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السّعي إلى خلق منافسة حقيقة بين المنظمات الخاصّة وتظم الخبرة الفردية التي تعدّ أهم مظاهر الخبرة في مجال تكنولوجيا المعلومات، حيث أنّ المؤسسات الكبرى المتخصصة في مجال تكنولوجيا المعلوماتية والانترنت تعمل جاهدة على الاستعانة بأشخاص تثبت كفاءتهم في مجال الحاسب الآلي، حيث ثبت علميًا أنّ هناك أشخاص يتمتعون بمهارات فائقة وبموهبة في هذا المجال، مثليبل كيتس (Bill Gates)والذي يعتبر أمهر مبرمجي نظم التشغيل.[1]

ب-المؤسسات التعليمية:

لما كانت الانترنت تعدّ أحد منتجات العلم في حركته، فإنه يمكن القول وبحق أن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة الإلكترونية، أن تكون من خلال المؤسسات التعليمية، وهذه الأخيرة تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية.

ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أتم الاستعداد لمواجهة الجريمة الإلكترونية، ومثل ذلك دراسات الحاسب الآلي التي تتطوّر بشكل فائق في جامعة "ستانفورد" كذلك معهد التكنولوجيا في "ماسا شوكستن" الذي قدّم للبشرية خبراء عل درجة عالية من التفوّق[2].

جـ- جهات الضبط القضائي:

قامت بعض الدوّل وعلى رأسها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصة للخبرة في الإجرام عبر الانترنت، فقد أسّس فرعا تابعًا لمكتب التحقيقات الفيديو (FBI)أطلق عليه "المخبر أليمي الشرعي للحاسوب" مقرّه (سان ديجو) San Diego والذي تم افتتاحه في

[1]- سليمان أحمد فغل، الخبرة في مجال التحقيق الإلكتروني، دراسة مقارنة، ط2، القاهرة، مصر، 2006، ص 130.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص ص298-299.

نوفمبر سنة 2000 لكي يكون بيت خبرة عام تعدّد النواحي القضائية، غرضه مكافحة التصعيد الخطير في الجريمة الإلكترونية من خلال التصنيف والتحليل للدليل الرقمي.

3/ -يقصد **بالخبير الإلكتروني** الشخص الذي تعمق في دراسة عمل من الأعمال الإلكترونية وتخصّص في أدائه مدّة زمنية طويلة، ممّا أكسبه خبرة علمية، بحيث أصبح ملّما بتفاصيل، وعليه فإنّ أهم صعوبة تواجه نظم الخبرة تكمن في تكوين الخبير المناسب الذي سيتّم الاستعانة به باعتبار أنّ الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصّة بتعيين الخبير، بل يتطلّب الأمر شروط تتلاءم مع التطوّرات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنّية والعلمية، وبالتالي فإنّ اختيار الخبير في مجال الجرائم الإلكترونية يتحدّد بنوعية الجريمة وأنواع الحاسبات والشبكات والبرامج المستخدمة فيها، وقد حصر قانون الدليل الخاص بولاية كاليفورنيا في الولايات المتحدة الأمريكية الخبراء الإلكترونيين في كلّ من:[1]

- المبرمج الذي قام بتحرير البرنامج واختياره؛
- محلّل النظم الذي صمّم وحدّد برنامج الحاسب الآلي الذي أنتج الدليل؛
- المشغّل الذي يقوم بتشغيل البرنامج؛
- مهندس الصيانة الإلكتروني الذي يقوم على ضمانة الجهاز الأصلي؛
- مبرمجي صيانة النظام والمسئولين عن سرية عمل الحاسب الآلي المستخدم في تنفيذ برامجه؛
- طاقم عمليات البيانات الذي يعدّ البيانات بالصورة التي يستطيع الحاسب قراءتها؛

[1]- أدهم باسم نمر البغدادي، وسائل البحث والتحري عن الجرائم الإلكترونية، رسالة دكتوراه، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص ص 77، 79.

- أمناء مكتبة الأشرطة المسئولين عن معالجة المدخلات والمخرجات يدويا قبل وبعد أداء العمل[1].

4- آلية عمل الخبير الإلكتروني:

يقوم الخبير الإلكتروني بفحص الأجهزة الإلكترونية المتعلقة بالجريمة سواءً كانت حواسيب شخصية أم متواجدة لدى مزوّد خدمة الانترنت، وعليه يجب على الخبير الإلكتروني أن يكون قادرًا على القيام بالمهام التالية:

أ-حجز البيانات:

يقصد به أنّ كل شخص يدخل إلى مسرح الجريمة يجب أن يأخذ منه شيئًا، ويترك خلفه شيئًا ما، فمثلا إذا أرسل شخص رسالة إلكترونية تحمل مضمونًا احتياليا إلى أحد الأشخاص، فإنّ هذه الرسالة سوف تخزّن على الخدمات الموجودة لدى مزوّد خدمة الانترنت مع التاريخ والوقت، إضافة إلى مسار الرسالة وعنوان رقم النفاذ.

كذلك يجب على الخبير الإلكتروني أن يقوم في بادئ الأمر بعملية حجز للبيانات المتعلقة بالجريمة الموجودة لدى مزوّد الخدمة إضافة إلى حجز الأجهزة التي تحتوي هذه البيانات، والتي تكون بحيازة المشتبه به.[2]

ب-حفظ البيانات:

يقوم الخبير الإلكتروني في هذه المرحلة بنسخ البيانات التي تم حجزها، بحيث يصبح لديه نسختان منها:

- الأولى: يتم تخزينها في الأجهزة الرقمية التي تم حجزها، بحيث تبقى محفوظة بشكل جيّد.

[1]- إسماعيل أحمدفضل، مرجع سابق، ص 134.

[2]- أدهم باسم نمر بغدادي. المرجع السابق ص ص81- 84

- أما الثانية: فهي عبارة عن نسخة طبق الأصل، يتم إجراء عملية الاختبار أو الفحص عليها.

جـ-استعادة البيانات:

يجب على الخبير الإلكتروني أن يستعيد البيانات المحذوفة، وذلك باستخدام أحد برامج استعادة البيانات، وهو أمر ضروري من أجل إعادة بناء القضية، فمثلا: يمكن للخبير أن يستعيد جميع الرسائل التي قام الجاني بحذفها عن طريق تتبع الأثر الذي تتركه هذه على جهاز التخزين.

د-تحليل البيانات:

في هذه المرحلة، يقوم الخبير الإلكتروني بعملية تقويم محتوى البيانات الإلكترونية، بحيث يفحصها بدقة من أجل تحديد وسائل الجريمة ودوافعها.

هـ-إعادة بناء القضية:

هي العملية التي يقوم بها الخبير بعد تجميع وتحليل البيانات والمعلومات التي تم الحصول عليها نتيجة البحث من أجل توضيح ما حصل بين المجرم والضحية أثناء ارتكاب الجريمة، فالدليل الإلكتروني الذي تم الحصول عليه يحتوي على آثار سلوكية مثل الكلمات التي استخدمها المجرم في تصفّح الانترنت، المواقع التي قام بتصفيحها، فالربط بين السلوكيات يؤدي إلى معرفة وقت ومكان ارتكاب الجريمة، والطريقة التي تمت بها، وكيفية وصول الجاني إلى الضحية[1].

و-كتابة التقرير:

يتضمن تقرير الخبرة، النتائج التي توصّل إليها الخبير من خلال عملية البحث ومن النتائج التي يجب أن يتضمنها التقرير ما يلي:

- مواصفات مسرح الجريمة الافتراضي؛

[1]- سليمان أحمد فضل، المرجع السابق، ص ص335-336.

- ملخص عن عملية الجريمة التي تمّ القيام بها؛
- إعادة رواية أحداث القضية؛
- ملخص النتائج؛
- اقتراحات الخبير الإلكتروني؛
- وينصح أن يكون التقرير متسلسلاً من حيث بناء الأحداث وأن يكون مختصرًا من الناحية النفسية ومكتوبًا بأسلوب بسيط.

5-المعالجة الإجرائية للخبرة في الجريمة الإلكترونية:

من بين التشريعات التي أخضعت الخبرة في الجريمة الإلكترونية للأحكام العامة للخبرة في الجرائم التقليدية وهذا لعدم وجود نصوص خاصة نجد المشرّع الجزائري الذي نص على الخبرة في المواد من 143 إلى 156 من ق إ ج.

حيث نص في المادة 143 على أن لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير وذلك إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم.

وإذا رأى قاضي التحقيق أنه لا موجب للاستجابة لطلب الخبرة فعليه أن يصدر في ذلك أمرا مسببا في أجل 30 يوما من تاريخ استلامه الطلب.

كما بين المشرع إجراءات الاحتكام للخبراء من خلال الفقرة الرابعة من المادة 143 الى المادة 156 (السابقة الذكر).

ورغم عدم تضمين المشرّع الجزائري لنصوص خاصة تتعلّق بالجريمة الإلكترونية، وكذلك نقص الخبرة في مجال تكنولوجيا المعلومات، إلاّ أنّ هناك إمكانية تطبيق الأحكام المتعلّقة بالخبرة في الأحكام العامة على الجرائم الإلكترونية وفي هذا الصدد نصت المادة

143[1]على أنّ: «لجهات التحقيق أو الحكم عندما تعرف لها مسألة ذات طابع فنّي أن تأمر بندب خبير، إمّا بناءً على طلب النيابة العامة وإمّا من تلقاء نفسها أو من الخصوم.

فإذا رأى قاضي التحقيق أنّه لا موجب للاستجابة لطلب الخبرة فعليه أن يصور في ذلك أمرًا مسبّبًا في أجل (03) ثلاثين يومًا منه تاريخ استلامه الطلب.

وإذا لم يبث قاضي التحقيق في الأجل المذكور يمكن الطرف المعني إخطار غرفة الاتهام مباشرة خلال (10) عشرة أيام، ولهذه الأخيرة أجل (30) يومًا للفصل في الطلب، تسري من تاريخ إخطارها، ويكون قرارها غير قابل لأي طعن.

ويقوم الخبراء بأداء مهمتهم تحت مراقبة قاضي التحقيق أو القاضي الذي تعيّنه الجهة القضائية التي أمرت بإجراء الخبرة».

كما قد يعين خبراء غير مقيدون في جدول الجهات القضائية وذلك بقرار مسبب من هذه الأخيرة، وهذا ما نصت عليه الفقرة 3 من المادة 144 من نفس القانون[2].

أمّا فيما يخص اليمين فيقوم الخبير المقيّد في الجدول بأدائهامرّة واحدة، بينما يقوم الخبير المعيّن من خارج الجدول بتأدية اليمين لكل مهمّة محدّدة بذاتها أمام قاضي التحقيق أو القاضي المعيّن من الجهة القضائية وهذا طبقا لنص المادة 145 من نفس القانون والتي حدّدت صيغة اليمين كالتالي: «أحلف باللّه العظيم بأن قوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال».

كما أنّ للخبير الاستماع لكل شخص يرى ضرورة سماعه، ويجب تحديد المدّة التي يجب عليه إنجاز المهام المناطة به خلالها، غير أنّه يمكن تمديد هذه المدّة بقرار مسبّب من قاضي التحقيق، بهم خلالها، غير أنّه يمكن تمديد هذه المدّة بقرار مسبّب من قاضي التحقيق، بناء على طلب من الخبير أو الخبراء، وعليهم إيداع تقاريرهم في الميعاد المحدّد.

[1]- القانون رقم 06-22، المؤرخ في 20 ديسمبر سنة 2006، المرجع السابق.

[2]- انظر المادة 144، الفقرة الثالثة، قانون الإجراءاتالجزائية.

كما نص أيضا على حماية الخبراء من أي تهديد خطير ولاسيما في قضايا الجرائم المستحدثة وذلك من خلال المواد 65 مكرر 19 إلى 65 مكرر28.[1]

المطلب الثاني

الأساليب المستحدثة للتحقيق في الجريمة الإلكترونية

أجاز المشرّع لقاضي التحقيق، منذ تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المؤرخ في 20-12-2006 إذا اقتضت ضرورات التحقيق في جرائم معيّنة كالجرائم السيبيرانية اللجوء إلى أساليب تحرّي خاصة والتي سوف نراها من خلال الفروع التالية:

الفرع الأوّل

التسرب الإلكتروني

يعدّ التسرّب إجراء من إجراءات البحث والتحقيق المستحدثة والتي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الإلكترونية ومن بينها المشرّع الجزائري الذي تبنى بدوره هذا الإجراء مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة لمكافحة جرائم الحاسوب بموجب المرسوم الرئاسي رقم 02-05 المؤرخ في 2002/02/02 واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19.[2]

أوّلا: تعريف التسرّب الإلكتروني.

لقد تطّرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية على أنه «قيام ضابط أو عون الشرطة القضائية، تحتمسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أوشريك لهم أو خاف».

[1]- أمر رقم 02-15 مؤرخ في 23 يوليو سنة 2015 المعدل والمتمم للأمر رقم 66-155، مرجع سابق.

[2]- جمال براهيمي، المرجع السابق، ص ص 82-83.

وعليه يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال الآتي بيانها:

-حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات يتحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها؛

- اِستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم كافة الوسائل[1].

أما في مجال الجريمة الإلكترونية فتتم بدخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك ب:

- اختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها؛
- اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان مثلهم،مستخدما أسماء أو صفة هيئات مستعارة ووهمية وذلك سعيا منه للاستفادة منهم حول كيفية اقتحام الهكرة لموقع ما مثلا.

يلاحظ ممّا سبق أن عملية التسرب عملية معقدة، حيث تتطلّب أن يدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ويربط علاقات من أجل تحقيق الهدف النهائي من العملية.

كما تستلزم هذه العملية ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه، وكذلك معرفة عناصر الجماعة وكيفية نشأتها واِختصاصات كل فرد منها، بالإضافة إلى الوسائل التي تعمل بها، وبعد أن يتم دراسة الوسط المستهدف يتم اختيار الأشخاص المناسبين للقيام بمهمة التسرب.[2]

[1]- د. أحسن بوسقيعة، التحقيق القضائي، ط7، دار هومةللطباعة والنشر والتوزيع، الجزائر، 2008، ص 114.

[2]- هدى زوزو، "التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري"، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقة، العدد 11، جوان 2014، ص 118.

ثانيًا: شروط صحة التسرب.

باعتبار عملية التسرّب إجراء غير عادي لجمع البيانات والمعطيات الخاصة التي تشير إلى كافة الأعمال الإجرائية، وتمكين المصالح الأمنية من معرفة الإمكانيات والأساليب المستعملة لارتكاب الأفعال المجرّمة، فقد تمت إحاطته بجملة من الشروط التي يجب مراعاتها عندما تقتضي ضرورات التحري أو التحقيق اللجوء إليه، وعليه فتتمثل هذه الشروط في:

1-الشروط الموضوعية:

يشترط للقيام بعملية التسرّب مراعاة مجموعة من الشروط الموضوعية من قبل السلطة المختصة بإجراء التسرّب، خاصّة وقت ومكان إجراء عملية التسرّب، نوع الجريمة، التسبيب أن يكون المتسرّب فاعلا أو شريكًا.

أ-السّلطة المختصّة بمنح إذن بإجراء التسرّب:

تتمثل الجهة المختصة بإصدار أو منح الإذن بالتسرّب إمّاوكيل الجمهورية أو قاضي التحقيق.

- ففي مرحلة التحرّي فإنّ وكيل الجمهورية هو من يقوم بمتابعة والرقابة على تلك العملية، أي أنه هو من يأذن بالعملية وهو من يتولى متابعة سيره من خلال ما له من مكانة في إدارة نشاط ضابط وأعوان الشرطة القضائية.
- أمّا في مرحلة التحقيق، فإنّ قاضي التحقيق بعد إخطار وكيل الجمهورية هو الذي يأذن بالتسرّب وهو من يقوم بمراقبته[1]، حيث يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.

[1]- زيدان زبيخة، المرجع السابق، ص 169.

ب -وقت ومكان إجراء عملية التسرّب:

باعتبار التسرّب إجراء من إجراءات التحقيق يجعل من المتسرّب غير مقيّد بحيّز زمني يتحرك فيه، فضرورة التحقيق تبرّر عملياته طول ساعات اللّيل والنّهار، وله أن يدخل كل الأماكن التي يمكن أن يكشف فيها الحقيقة دون قيد أو شرط لأنّه لا يتحرك بصفة ضابط أو عون الشرطة القضائية بل هوية مستعارة.

جـ-نوع الجريمة:

يجب أن يتم التسرب بمناسبة الجرائم السّبعة التي حددتها على سبيل الحصر المادة 56 مكرر 5 والتي تتمثل في:

- جرائم المخدرات؛
- الجريمة المنظمة العابرة للحدود الوطنية؛
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛
- جرائم تبييض الأموال؛
- جرائم الإرهاب؛
- الجرائم المتعلّقة بالتشريع الخاص بالصّرف؛
- جرائم الفساد.

د -التسبيب:

يعتبر التسبيب أساس العمل القضائي، فمن خلاله تثبيت العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن، وكذا الحجج والمبررات التي أقنعتها لمنح الإذن بإجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية ليلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبة الإذن.[1]

[1]- هوام علاوة، "التسرب كآلية للكشف عن جرائم في القانون الجزائري"، مجلّة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص 03.

2-الشّروط الشّكلية:

نظرًا لما تتطلبه عملية التسرّب من سرية وحيطة وحذر نتيجة خطورة العملية على حياة المتسرّب حرص المشرّع على حسن سير العملية حيث استوجب شروط شكلية يمكن إجمالها فيما يلي:

أ-صدور إجراء التسرب بإذن قضائي:

إذ لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة حسب أحكام المادة (65 مكرر 11 ق.إ.ج) والتي أشرنا إليها سابقًا، على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتلافي حدوث تجاوزات وتعسّف في استعمال الحق.

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبًا وإلاّ كان هذا الإجراء باطلاً، لأنّ الأصل في العمل الإجرائي هو الكتابة كما نصّت ليه المادة (65 مكرر 15).

ب-مدّة تنفيذ عملية التسرب:

يجب أن يحدد في الإذن مدة عملية التسرب التي أقصاها 4 أشهر قابلة للتجديد إذا اقتضت ضرورات التحري والتحقيق ذلك مع إصدار إذن آخر وفق الشروط الزّمنية نفسها التي صدر فيها الإذن الأوّل.

غير أنّه في حالة ما إذا وجد المتسرّب صعوبة في الانسحاب من الشبكة له أن يبقى لمدّة قد تصل إلى ضعف المدة القانونية، ولا يمكنه في هذه الحالة الانسحاب بنفسه فجأة من التنظيم الإجرامي دون التحضير كذلك وإلاّ سيكون محلاً للشك.[1]

[1]- نصيرة بوحزمة، المرجع السابق، ص 398.

الفرع الثاني

اعتراض المراسلات وتسجيل الأصوات والتقاط الصوّر والمراقبة الإلكترونية

للمكالمات الهاتفية والرسائل الإلكترونية والأحاديث الشخصية حرمة تستمد من حرمة الحياة الخاصة لصاحبها والتي يجب حمايتها ضد جميع وسائل التصنت والاستماع والنشر أو مراقبتها والذي سوف نراه في النقاط التالية:[1]

أولا-مفهوماعتراض المراسلات والمراقبة الإلكترونية:

لم يعرّف المشرع الجزائري والفقه اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بل ركّز على الجانب الإجرائي من حيث نصّه على بعض الأساليب التي يمكن اللجوء إليها في التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في المادة 65 مكرر 5 التي تنص على أنّه «**إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو** التحقيق الابتدائي 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.*، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:

تت- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

ثث- وضع الترتيبات التقنية، دون موافقة المعنيين من أجل الالتقاطوتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في مكان خاص».[2]

غير أنّ القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 02 الفقرة "و" حيث عرّفت

---

[1]- زيدان زيبخة، المرجع السابق، ص 153.

*-المادة65 مكرر 5 ق.إ.ج.ج.

[2]-نادية حسان، المرجع السابق، ص31.

***الاتصالات الإلكترونية** على أنّها: «تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بأيّة وسيلة كانت».

وتجدر الإشارة في هذا الصدد إلى أنّ المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية، ولكي تكون كذلك يلزم أن يتوفر لديها عنصران أساسيان هما:

ج ج- عنصر موضوعي يتعلّق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري أو خاص فيما تخبر به.

ح ح- عنصر شخصي ويراد بهإرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة.

فالتصنت وبث تسجيل عنصر الكلام المتفوّه بصفة خاصة أو سرية منه طرف شخص أو عدة أشخاص في أماكن خاصة وعمومية يعتبر من العمليات التي وضعت بشكل محكم ومرتب يهدف في النهاية إلى رصد الدليل الذي سوف يثق كاهل المجرم الإلكتروني.

ويبدوا أنّ المراقبة المسلطة على التواصل بين الأشخاص عن طريق الهاتف من خلال تسجيل المحاكاة تعدّ الأخطر من اعتراض المراسلات.

فالاعتراف يتم استخدام وسائل فنية Des moyens techniques تتعلق بالتصنت L'écoute أو التحكم Le contrôle أو مراقبة محتوى الاتصالات La surveillance du contenu des communications والحصول على المحتوى بطريقة مباشرة من خلال طريقة الولوج إلى داخل النظام المعلوماتي واستخدامه، أو بشكل غير مباشر عن طريق استخدام أجهزة التصنتL'emploi de dispositifs d'écoutesويمكن أن تشتمل وسائل الاعتراض على تسجيل البيانات un enregistrement des douanes ولكل من أهم المراسلات الإلكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراف والمراقبة، هي المراسلات عبر البريد الإلكتروني.

***ويقصد بتسجيل الأصوات والتقاط الصور** تسجيل المحادثات الشفوية التي تحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص وكذلك التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص[1]، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والأماكن الخاصة.

وعليه يمكن القول في هذا الصدد أنّ بالرّغم ومن أنّ هذه التقنيات تساعد في الكشف عن الحقيقة وإثبات الكثير من الجرائم الغامضة إلاّ أنّها تحتل انتهاكا صارخا لجريمة الحياة الخاصة للأفراد.

* كما نضّم القانون رقم 09-04 كيفية إجراء **مراقبة الاتصالات الإلكترونية** في المادة 04 منه وفيها حدّد الحالات التي يتم فيها اللّجوء إلى هذا الإجراء على سبيل الحصر فجاء فيها أنّه: «يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 في الحالات التالية:

أ-للوقاية من الأفعال المخصوصة بجرائم الإرهاب أو التخريب أو الجرائم الحاسة بأمن الدولة.

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

جـ-لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوءإلى المراقبة الإلكترونية.

د-في إطار تنفيذ طلبات المساعدة القضائية المختصة...».

وتتم المراقبة بإذن مكتوب من السلطة القضائية المختصة طبقًا للفقرة 02 من المادة 04 المذكورة سابقًا. ونظرًا لكون المعطيات محميّة قانونًا فإنّ المشرّع يؤكد أنّه وفي إطار المراقبة لا يمكن للشخص الذي رخّص له بالاطلاع على هذه المعطيات استعمالها خارج

[1]- نادية حسان، المرجع السابق، ص ص30-31.

القانون بصريح نص المادة 09 من القانون رقم 09-04 التي جاء فيها: «تحت طائلةالعقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلاّ في الحدود الضرورية للتحرّيات أو التحقيقات القضائية».[1]

ثانيا/-القيود الواردة على عملية اعتراض ومراقبة المراسلات:

لتحقيق التوازن بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسّف السلطات العامة وتضمن الحرّية الفردية، والتي سوف نلخصها فيما يلي:[2]

1/-الحصول على إذن السلطة القضائية المختصّة.

يعني أنّه قبل اللجوء إلى عملية الاعتراض والمراقبة يجب الحصول أوّلاً على الإذن مسبقًا ويكون هذا الأخير مكتوبًا ومسببًا من الجهات القضائية المختصة، وإلاّ كان هذا الإجراء باطلاً.

وحتى يكون الإذن صحيحًا ومنتجًا لأثاره يجب أن يتضمّن جملة من العناصر الأساسية والمتمثلة في:

أ-طبيعة الجريمة التي تبرّر الإجراء:

والتي ينبغي أن تكون من ضمن الجرائم المذكورة في المادة 56 مكرر 05السابق الذكر.

[1]- ياسر أمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2009.ص 55

[2]- جمال براهيمي، المرجع السابق، ص 94.

ب-التعريف بالعملية:

بمعنى تحديد المراسلات والاتصالات المطلوبة اعترافها وتسجيلها، تحديد الأماكن المقصودة، تحديد المدّة التي تستغرقها التدابير التقنية في عملية الاعتراض والتي يجب أن لا تتجاوز أربعة أشهر قابلة للتجديد ضمن الشروط نفسها حسب تقدير السلطة مصدرة الإذن لمقتضيات التحرّي والتحقيق.

2/-تسبيب اللجوء إلى الاعتراض أو مراقبة المراسلات.

يقصد به المبرر الشرعي والضرورة الملحة التي تستدعي القيام بعملية اعتراض أو مراقبة المراسلات.

حيث يشترط وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة، تقدير جودها وجدّية دواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة والجناة مسبقًا[1].

3/-تحديد الجرائم محل الاعتراض والمراقبة.

إنّ الاستعانة بعملية اعتراض أو مراقبة المراسلات الإلكترونية لغرض التحقيق غير مسموح في كافة الجرائم إنّما مجال تطبيقها يتوقف عند نوع محدد فقط وهي:

خ خ- الجرائم المذكورة على سبيل الحصر في نص المادة 65 مكرر 05 من ق.إ.ج.

دد - الجرائم المنصوص عليها في الفقرات أ.بوج من المادة 04 من ق 09-04.

4/-سرية الإجراءات وكتمان السر المهني:

يعني أنه ينبغي أن تنفذ عملية الاعتراض والمراقبة في سرية تامة ودون علم أو رضا المشتبه فيه وأصحاب الأماكن، لكن مع مراعاة عدم المساس بالسّر المهني المقرر بنص المادة 45 فقرة 04 منق.إ.ج.

[1]- نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص105.

وعليه يمكن القول بأنّ رغم الصعوبات والمخاوف الكثيرة حيال هذه الإجراءات المستحدثة إلاّ أنّ الواقع يثبت أنّ من الضروري والملّح اللّجوء إلى الاستعانة بمثل هذا النوع من الإجراءات.

المبحث الثاني

الأساليب الدولية للتحقيق في الجرائم الإلكترونية

تلعب أساليب التحقيق المدني دورًا هامًا في التوصل إلى إثبات أو نفي الجريمة الإلكترونية واكتشاف غموضها وحلّ لغزها والتوصّل الى إثبات أو نفي الجريمة الإلكترونية والتوصّل للجاني وذلك من أجل تحقيق العدالة والأمن، بحيث تعزّزت بموجبها آمال القضاء والعدالة إذ حقّقت نتائج باهرة في مجال علوم الأدلة الجنائية ولكنها في الوقت ذاته اصطدمت بعائق الاختصاص خاصة عندما تكون الجريمة ذات بعد دولي، وعليه فلا يمكن التحدث عن مثل هذه الجريمة دون التطرّق إلى التعاون والتبادل بين الدول لمكافحة هذه الجرائم.

لذا ندرس التعاون الأمني في الجريمة الإلكترونية في المطلب الأوّل ثم التعاون القضائيفي المطلب الثاني.

المطلب الأوّل

التعاون الأمني الدولي في الجرائم الإلكترونية

إنّ مع تميّز الجرائم الإلكترونية على غيرها من الجرائم التقليدية ومع كونها عابرة للحدود، فإنّ مكافحتها لا تتحقّق إلاّ بوجود تعاون دولي على المستوى الإجرائي والقضائي.[1]

[1]- نادية دردار، الجهود الدولية لمكافحة الجريمة، ط1، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017.ص

الفرع الأول

التعاون الأمني تعريفه وأهميته

أولت الدوّل فيما بينها إتمامًا خاصًا بالجريمة الإلكترونية، نظرًا لخطورتها على الأمن والسلم الدوليين والوطنيين[1].

أولاً/ -تعريف التعاون الأمني الدولي:

يعتبر التعاون الأمني الدولي من بين المفاهيم التي يصعب وضع تعريف جامع مانع لها، والسّبب يرجع لعدّة اِعتبارات ولعلّ أهمها يظهر من خلال مدى اِتساع المجال والصور والأشكال التي قد يتخذها.

حيث لم يتم الاتفاق على وضع تعريف موحد له عالميًا رغم أهميّته، لأنّ الظاهرة الأمنية قد عرفت تطوّرات كثيرة نظرًا لتطوّر التحوّلات الدولية[2].

ثانيًا/ -أهمية التعاون الأمني الدولي.

يكتسب التعاون الأمني الدوّلي أهمية بالغة في مكافحة الجريمة الإلكترونية نظرًا لطبيعتها وخصوصيتها، حيث يشكل التعاون الأمني الدوّلي أحد المحاور الأساسية التي تبنى عليها المواجهة الفعالة للجريمة الإلكترونية، فلا شك أن التعاون يحكم السيطرة على الجناة أيًّا كان موقعهم أو جنسياتهم.

ويمثّل التعاون الدولي بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم الإلكترونية في الدول أحد الوسائل الهامة التي يمكن من خلالها صنع هذه الأخيرة أو الإقلال منها، وتؤكد التحقيقات في الجرائم عامة وخاصة الإلكترونية منها على أهمية

[1]- حسين بن سعيد النافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص 636.

[2]- خديجة بتقة، السياسة الأمنية الأوروبية في مواجهة الهجرة غير الشرعية، مذكرة الماستر، كلية الحقوق والعلوم السياسية، قيم العلوم السياسية والعلاقات الدولية، جامعة محمد خيضر، بسكرة، 2013، ص 10.

التعاون الأمني الدولي، بحيث يستحيل على دولة واحدة القضاء على الجرائم الدولية العابرة للحدود بمفردها.

كما أنّ التعاون الأمني الدولي لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين للعدالة وحسب، بل يتعدى الأمر ذلك ليشمل مكافحة الجريمة بشقيها الوقائي والقمعي، بما يشمل العناية بحقوق المتهمين والضحايا ومراعاة حقوق الدول وسيادتها.

وعليه من خلال أهمية التعاون الأمني الدولي يمكن تعريفه بأنه: «تبادل الكون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام وما يرتبط به من مجالات أخرى مثل مجال العدالة الجنائية، ومجال الأمن، أو لتخطي مشكلات الحدود والسيادة».

فمتى فر المجرم خارج حدود الدولة يقف الجهاز الأمني عاجزًا، لذا أصبحت الحاجة ماسة إلى وجود تعاون دولي يأخذ على عاتقه القيام بهذه المهمة.[1]

فممّا سبق يتضح أنّ التعاون الأمني الدولي يساهم مساهمة كبيرة في حصر الجريمة الإلكترونية والقضاء عليها، وهو ما يتطلب ضرورة تفاعل الدول فيما بينها وزيادة الجهود في سبيل تشجيع وتفعيل هذا التعاون.

الفرع الثاني

أسس التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية.

بالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية فإنّ التعاون الأمني الدولي في مجال المكافحة والوقاية من هذه الجرائم يجب أن يقوم على الأسس التالية[2]:

أولا/-التناول العلمي لبحث ظاهرة الجرائم الإلكترونية، وتوفير المعلومات الإحصائية والبيانات اللاّزمة، سواءً ما يتعلّق بالجريمة ذاتها أو ما تعلّق بمرتكبيها، أو ما يتعلّق

[1]- حسين بن سعيد النافري، المرجع السابق، ص 637.

[2]- عادل يحي، الأحكام العامة للتعاون الدولي لمكافحة الجريمة، ماهيته، صوره، أسسه، أهميته، ط1، دار النهضة العربية، القاهرة، مصر، 2013. ص 150

بسير نظام القضاء الجنائي، وفهم كل أبعاد هذه الجرائم، لذا يجب إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك الجرائم على مختلف صورها وأنماطها.

ثانيا/-التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية الإقليمية والدولية، بما يحقق حصر معدلات الجريمة، ويحول دون انتشارها.

ثالثا/-تحديد سبل التعاون في مجال التدريب والتعاون التقني، وتحقيق التكامل الأمني بين الأجهزة الأمنية على المستوى الدولي.

رابعا/-إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الجرائم، ونطاق الأفعال المؤثمة فيها، مع ضمان أن يشكل نطاق التجريم كافة جوانبها ومراحلها.

خامسا/-وضع وتضييق وقائية قادرة على خلق المناخ الملائم لأعمال المكافحة وتضييق الخناق على أنشطة تلك المنظمات الإجرامية وحرمانها من البيئة الملائمة لممارسة أنشطتهم الإجرامية وزيادة الوعي العام لدى الجماهير.

سادسا/-القيام ببعض العمليات الشرطية والأمنية المشتركة تدعيما للتعاون وصقلا للمهارات.

كما أنّ التعاون الأمني بين الدول يجد له أساسا في الاتفاقية الثنائية أو المتعددة الأطراف، التي تعرب من خلالها الدول عن اقتناعها بأنّ مصالحها وأهدافها في مجال مكافحة الجريمة، لا يمكن الوصول إليها بالجهود الفردية وأنّها تتطلب تعاون مع دولة أخرى من أجل تحقيقها بشكل أفضل.

في هذا الصدد عمدت الجزائر إلى عقد اتفاقيات مع بعض الدول من أجل تحقيق تعاون معها في المسائل الأمنية، منها الاتفاق مع إسبانيا، حيث جاء هذا الأخير في سياق

المساهمة في تطوير العلاقات الثنائية وتوطيد أواصر تعاونهما في هذا المجال في سياق احترام مبادئ المساواة والمعاملة بالمثل والمساعدة المتبادلة[1].

كما تم التعاون بين الجزائر وفرنسا أيضًا في مجال الأمن ومكافحة الإجرام المنظم نظرا للتهديد الذي يشكله هذا الأخير بكل أشكاله وخدمتا لمصلحة البلدين، حيث تم الاتفاق على إقامة تعاون عملياتي وتقني في مجال الأمن الداخلي وتبادل المساعدة[2]3.

الفرع الثالث

صور التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية.

لقد أصبح من ماسة الحاجة إلى وجود كيان دولي يأخذ على عاقه القيام بهذه المهمة خاصة في مجال تبادل المعلومات وللتعاون الأمني الدولي عدّة صور أهمها:[3]

أولا/ -ربط شبكات الاتصال والمعلومات:

تحتاج الاتصالات الشرطية إلى وسائل للاتصال تحقق الشركة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية إلى تطوير الاتصال وتبادل المعلومات فيما بينها.

ثانيا/ -تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة:

تعدّ هذه الصورة من أهم الصور التعاون الدولي في مجال مكافحة الجرائم الإلكترونية لاسيما وأن أجهزة العدالة الجزائية ليست بنفس المستوى في جميع الدول، وإنّما هناك تفاوت بينها، فبعض الدول متقدمة تقنيا وتكنولوجيًا والبعض الآخر يفتقد ذلك، ممّا استوجب أن يكون هناك تعاون بين الدول.

---

[1] عادل يحي، المرجع السابق، ص 152

2-ديباجة الاتفاقية الجزائرية الديمقراطية الشعبية والمملكة الإسبانية في مجال الأمن ومكافحة الإرهاب والجرائم المنظمة، الموقعة بالجزائر في 15 جوان 2008، المصادق عليها بموجب المرسوم الرئاسي 08-427 المؤرخ في 28 ديسمبر، ج.ر.ج.ج، العدد 05، تاريخ 21 جانفي 2009.

[2]- جمال براهيمي، المرجع السابق، ص 94.

[3]-مختار الشيلي، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، الجزائر، 2013، ص183.

ثالثا/ -القيام ببعض العمليات الشرطية والأمنية المشتركة:

إنّ تعقب مجرمي المعلوماتية عامة وشبكة الانترنت خاصة، وتعقب الأدلة الإلكترونية وشبكات الاتصال، كلّها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية والفنية المشتركة، والتي من شأنها أن تساعد في تحفيز مهارات وخبرات القائمين على مكافحة لك الجرائم، وبالتالي وضع حدّ لها.

الفرع الرابع

جهود المنظّمة الدولية للشرطة الجنائية (الأنتربول) في مجال التعاون الأمني

تسعى منظمة الانتربول إلى الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانًا، وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة وضبط الأدلة والمجرمين، وذلك من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في الدول الأعضاء، بهدف توصيل اتصال فعّال وآمن بين أجهزة الشرطة في مختلف الدول على نحو يمكناها من تبادل المعلومات بشكل سريع، قامت منظمة (الإنتربول) بوضع منظومة عالمية للاتصالات الشرطية المأمونة، على نحو يمكن مستخدمي هذه المنظومة من تبادل المعلومات والبيانات الشرطية الهامة فيما بينهم والاطلاع على قواعد بيانات الإنتربول والحصول على خدماته على مدار الساعة.

ومن بين الإنجازات التي حققتها الإنتربول في ظل مواجهته للجرائم الإلكترونية تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول والمتعلقة بنشر "دودة الحب" "Love Buis" عبر الانترنت في الفيليبين.[1]

يتضح مما سبق أن مواجهة الجريمة الإلكترونية لا يتوقف على أجهزة الأمن فقط، بل لابد من إثارة الوعي العام بخطورة الجرائم الإلكترونية.[2]

[1]- نصيرة بوحمزة، المرجع السابق، ص 424.

[2]- محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، ب.ب.ن، 2016.ص160

المطلب الثاني

التعاون القضائي الدولي في الجرائم الإلكترونية

يقصد بالتعاون القضائي بين الدول: «ما تقدمه سلطات دولة ما لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتا ويتغلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى».

ويقصد به أيضا «التعاون الواقع بين السلطات القضائية لمختلف الدول في سبيل كشف الجريمة وضبط مقترفيها وإخضاعهم للجزاء المستحق عن ارتكابهم لها».[1]

والتعاون القضائي في مجال الجريمة الإلكترونية يتجلى أساسا في المساعدة القضائية والإنابة القضائية، والتحقيقات المشتركة.

الفرع الأوّل

المساعدة القضائية المتبادلة في مجال الجرائم الإلكترونية.

المساعدة القضائية المتبادلة والتي تعدّ وسيلة حتمية في ذلك، ويرجع السّبب في ذلك إلى أنّها تتوزع في الغالب عبر أقاليم عدّة دول مما يؤدي إلى تشتت الأدلة التي يمكن أن تستند عليها الدولة التي تنظر في هذه الجريمة.

أولا/ -تعريف المساعدة القضائية المتبادلة:

تعرّف المساعدة القضائية المتبادلة بأنّها: «كلّ إجراء قضائي تقوم به دولة من شأنها تسهيل مهمة المحكمة في دولة أخرى بصدد جريمة من الجرائم».2

[1]- هدى حامد قشقوش، الجريمة المنظمة، ط1، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص 85.

وتعرّف أيضا بأنّها: «قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق، وذلك لحساب سلطة قضائية مختصة تابعة كدولة أخرى من أجل الوصول إلى كشف الحقيقة في قضايا جنائية».

وعليه فإنّ المساعدة القضائية المتبادلة تقوم على فكرة التنسيق بين السلطات القضائية التابعة لدولتين على الأقل من أجل التحقيق.

والمساعدة القضائية لا تتحقق إلا من خلال خطوات ثلاث وهي:

1. **الطلب**: وتقدّمه الدولة صاحبة الاختصاص الجنائي بالمحاكمة، ويخضع هذا الطلب لقانون الدولة الطالبة وفي نطاق الاتفاقية التي تعتمدها مع الدولة التي ستقدم المساعدة.
2. **فحص الطلب**: وتقوم به الدولة التي ستقدم المساعدة، ويمنع ذلك عن طريق التحقيق من اعتبار الواقعة للمطلوب تحقيقها تعد جريمة وفقا لقانون الدولة الطالبة.
3. **تنفيذ المساعدة القضائية**: ويتم وفقا لقواعد الدولة المطلوب منها المساعدة، فالإجراء يتم وفقًا لقانون الدولة التي تنفذه[1].

ثانيا/ -صور المساعدة القضائية المتبادلة:

تتخذ المساعدة القضائية الصور التالية[2]:

1/ -تبادل المعلومات:

من أهم العناصر المتعلقة بالوقاية من الجريمة تبادل المعلوماتوالخبرات، إذ تقاسم المعلومات وسرعة الحصول عليها يعمل على تسهيل مهمة الأجهزة الوطنية في التحرّك المناسب لمواجهة الجريمة.

2-عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية،2015، ص 30

[2]- سليمان أحمد فضل، المرجع السابق، ص 421.

لهذا يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عمومًا والجريمة الإلكترونية خصوصًا، لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين بتطوير التبادل المنهجي للمعلومات بوصفه عنصرًا رئيسيًا من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها.

هكذا وينبغي للتعاون في المسائل المتعلّقة بالجريمة الإلكترونية أن يدعم بتوظيف نظم تبادل المعلومات بين الدولة الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، حيث أن تبادل المعلومات يمكن أن يتحقق من خلال المنظمات والهيئات الدولية.

وتبرز أهمية تبادل المعلومات من التعاون في ميدان مكافحة الجرائم الإلكترونية التي يلجأ مرتكبيها إلى التخفي على الشبكات الإلكترونية خلف شخصيات وهمية وأسماء مستعارة وهو ما يتطلب تعاونًا الدول خاصة في حالة توزع النشاط الإجرامي بين أكثر من دولة[1].

حيث أنّ بالإمكان إصدار نشرة دورية شهرية مثلا تتضمن أحدث الوسائل والأساليب في مجال الجرائم الإلكترونية على أن يتم تبادلها على مستوى الدولة.

وفي هذا المجال تم تقديم معلومات في قضية القرصنة الإلكترونية، حيث تلقت السلطات الجزائية شهر جويلية 2009 معلومات من سفارة ألمانيا بالجزائر مفادها أنّ مصالح الشرطة الألمانية اكتشفت بأنّ شخصا ما قام بتاريخ 30 جوان 2009 على الساعة الثامنة وخمسون دقيقة مساءًا باختراق قاعدة بيانات متواجدة بميونيخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة بـ 1500 بطاقة ائتمان باستعمال عنوان إلكتروني.

وبتاريخ 21 أكتوبر من نفس السنة تلقى كذلك مكتب الإنتربول بالجزائر مراسلة من مكتب الإنتربول بكندا مفادها أنّ مصالح شرطية (كيبك Québec) تمكنت خلال العام

[1]- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، مصر، 2012،ص 40.

الماضي من القبض على شبكة إجرامية مختصة في القرصنة الإلكترونية بتحميل المعطيات الرقمية المتبادلة بين الزبائن والبنك وتحويل الأموال من حسابات بنكية.

على إثر هذه المعلومات تمكنت المديرية العامة للأمن الوطني من إلقاء القبض على المتهم وهو شباب جزائري وتقديمه للعدالة بتهمة القرصنة الإلكترونية المرتكبة بحق مراكز معطيات إلكترونية أجنبية متواجدة بكل من ألمانيا وكندا، وصدر بحقه حكم تحت رقم 10/37560 من محكمة عنابة بتاريخ 28 جوان 2010.[1]

2/-نقل الإجراءات:

يقصد بنقل الإجراءات قيام إحدى الدول بناءً على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معيّنة، ومن أهمها: التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص بشكل جريمة في كلتا الدولتين (الطالبة والمطلوب منها) نقل الإجراءات بالإضافة إلى شرعية الإجراءات المطلوبة اتخاذها بمعنى أن تكون هذه الأخيرة مفسرة في قانون الدولة المطلوب إليها عن ذات الجريمة.

ثالثا/-محتوى طلب المساعدة القضائية:

حتى يكون طلب المساعدة القضائية مقبولاً يشترط أن يشمل على البيانات التالية والتي قسمت إلى حالتين[2]:

1-في الحالات العادية: يجب أن يتضمن الطلب:

- اسم السلطة المختصة بمباشرة التخفيضات أو الإجراءات ذات الصلة بموضوع الطلب؛
- وصف الوقائع موضوع الاتهاممرفقا بنصوص القوانين ذات الصلة بالموضوع؛
- غرض الطلب وطبيعة المساعدة القضائية المطلوبة؛

[2]- نصيرة بوحزمة، المرجع السابق، ص ص 450-451.

- طلب الحصول على الأدلة أو إجراء تفتيش أو ضبط يرفق بيان الغرض منه؛
- التفاصيل الخاصة إجراءات محددة ترغب الدولة الطالبة في إتباعها؛
- الحاجة إلى السرية وأسباب ذلك؛
- المدّة الزمنية المطلوب تنفيذ الطلب خلالها.

ب-في حالات الضرورة:

- الهوية وتاريخ الميلاد والمكان الذي يتواجد في الشّخص المطلوب شهادته؛
- وصفًا دقيقًا للمكان الذي ينبغي فيه التفتيش والبحث وكذلك الأشياء التي يجب حجزها؛
- وصفًا للإجراءات الخاصة الواجب إتباعها خلال تنفيذ الطلب؛
- عند الاقتضاء بيان عن مدى الضّرر الناتج عن ارتكاب الجريمة؛
- أيّة معلومات أخرى تقدم للطرف المطلوب منه لتسهيل تنفيذ طلب المساعدة القضائية.

رابعا/-موقف المشرع الجزائري من المساعدة القضائية الدولية المتبادلة:

لقد نص المشرع الجزائري على المساعدة القضائية الدولية، وعليه فيمكن إعمالا للقواعد المقررة أن تلتمس الدولة الطالبة من الدولة المطلوب منها المساعدة القضائية نقل الإجراءات وتبادل المعلومات، مثل القضية التي فصّل فيها مجلس قضاء باتنة بتاريخ 04 جويلية 2010 بموجب القرار رقم 10/05805 وذلك إثر رسالة صادرة من وزارة العدل الأمريكية (المكتب الفيدرالي للتحقيقات) مفادها تعرّض النظام المعلوماتي لشركة أمريكية متخصصة في حماية المعلومات والبرامج الإلكترونية تسمىSage net Works إلى الاعتراض واستغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية من طرف شباب جزائري وهو تقني سامي بالإعلام الآلي والمتهم بتهمتي التواجد غير المشروع في الأنظمة المعلوماتية والتعامل مع معطيات غير مشروعة.[1]

الفرع الثاني

الإنابة القضائية الدولية في مجال الجرائم الإلكترونية.

تعرّف الإنابة القضائية الدولية بأنّها: «قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق، وذلك لحساب سلطة قضائية مختصة تابعة لدولة أخرى من أجل كشف الحقيقة في دعوى جنائية منظورة أمام محاكم هذه الأخيرة».

وتعرف أيضًا بأنّها «طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها»[1].

ووفقا للتعريفين السابقين ،فإن الإنابة القضائية الدولية تفترض في المسائل الجنائية وجود علاقة تعاون بين دولتين ،حيث تهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول، وبموجب هذه الإنابة تقوم السلطة القضائية في الدولة المطلوبة منها تنفيذها باتخاذ إجراء أو أكثرمن إجراءات التحقيق، ووفقا لقانونها الوطني[2] الذي يفرض المساعدة القضائية المتبادلة في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية والاتفاقيات الثنائية ومبدأ المعاملة بالمثل، قبول طلب المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

1-زياد إبراهيم شيحا، الإنابة القضائية الدولية في المسائل الجنائية، ونطاق العلاقات الخاصة الدولية، دار النهضة العربية، القاهرة، مصر، 2010،ص4.

[2]- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المرجع السابق.

في حين نصت المادة 17 من نفس القانون على تبادل المعلومات واتخاذ الإجراءات التحفظية كما يلي:

- تتم الاستجابة لطلبات المساعدة وفقا للاتفاقيات الدولية والثنائية ومبدأ المعاملة بالمثل.

هذا ونصت المادة 18 من القانون أعلاه على القيود الواردة على طلبات المساعدة القضائية كالتالي:

- «يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.
- يمكن أن تكون الاستجابة لطلبات المساعدة مقيّدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب لحساب الدولة الطالبة من أجل الوصول إلى كشف الحقيقة أمام محاكم هذه الأخيرة».

فرغم ذلك فإنّ ثمة صعوبات تعترض تنفيذ الإنابة القضائية الدولية في بعض الحالات وتقلّل من فاعليتها بحيث لا يتحقق الغرض المنشود منها، كاختلاف النظام الإجرائي في كل من الدولة الطالبة والدولة المنفذة وغيرها...

فإزاء هذه الصعوبات تبدو أهميّة تقنية الاتصال المرئي المسموع كوسيلة إضافية للمساعدة القضائية المتبادلة، ويعد استخدام هذه التقنية في مباشرة إجراءات التحقيق أحد التطبيقات الهامة للتكنولوجيا في هذا المجال.

الفرع الثالث

التحقيقات المشتركة في مجال الجرائم الإلكترونية.

هذا النّوع من التعاون تفرضه طبيعة الجرائم الإلكترونية، حيث يتطلّب التحقيق فيها تشكيل فروق مشتركة بين الجهات المختصة في كل دولة من الدول التي وقعت فيها جزء من الجريمة، ومثال ذلك أجهزة الشرطة الخاصة التي شاركت بأربعة دول مجتمعة في جوان 2009 في ضبط مجموعة تطلق على نفسها اسم (محاربي شمال أوروبا الفايكينغ) في ضبط

مجموعة من مجرمي دعارة الأطفال تعمل من خلال الانترنت، وقد تمكنت هذه المجموعة من إيقاع 50 شخصًا في شبكتها، حيث قامت هذه المجموعة بتبادل صور جنسية للأطفال على الانترنت.

فعلى الرّغم مما يحققه التحقيق المشترك من تنسيق أمني بين الدول من خلال توحيد الخطوط والجهود لتعزيز أمن واستقرار الدول المعنية، لهذا التحقيق، إلاّ أنّ الواقع يثبت بطيء الوتيرة التي يسير عليها هذا التعاون.[1]

وعليه يمكن القول في هذا الصدد بأنّ التحقيق في الجرائم الإلكترونية وكشف غموضها بشكل أكثر سرعة وفعالية يتطلب عناصر مؤهلة علميا وتقنيا للتحقيق، وأنّ اللجوء إلى التعاون في مجال التحقيقات المشتركة يساهم في تدعيم التعاون الأمني بين الدول.

[1]- حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة دكتوراه في العلوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2016-2017، ص 545.

خاتمـــة

خاتمة:

نستخلص في الأخير بأن التحقيق الجنائي في الجرائم الإلكترونية التي تعد من الأنماط الإجرامية الجديدة التي فجرتها ثورة تقنية المعلومات والاتصالات عن بعد،من العمليات الصعبة والمعقدة التي تتطلب إلماما بتكنولوجيا الإعلام والاتصال.

بالتاليفإن أية محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الحديث في إطار عملية البحث والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بذلك ومن بينها القصور الذي يعتري النصوص الجزائية الإجرائية القائمة في مواجهة مثل هذه الجرائم لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بالجرائم التقليدية التي لا تعتريها أية صعوبات في مجال إثباتها أو التحقيق فيها إلى جانب خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

لكن المشرع كما سبق بيانه أنه ومن أجل تغطية وتلافي هذا القصور وتفاديا لإفلات المجرم الإلكتروني من المتابعة الجزائية والعقاب بادر إلى إعادة النظر في بعض الأحكام والقواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش والضبط حيث جعلها ممكنة الاستعمال حتى في البيئة الرقمية الإلكترونية. فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة لهذه الجرائم الجديدة من خلال تعديل قانون الإجراءات الجزائية عام 2006، وإصدار القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالومكافحتها كالمراقبة الإلكترونية واعتراض المراسلات والتسرب الإلكتروني.

كما استخلصنا أيضا أنه من المشكلات التي تواجه سلطات البحث والتحقيق فيما يتعلق بالقيمة القانونية للأدلة الإلكترونية ومدى قبولها كوسيلة إثبات من طرف القاضي الجزائي وأنه ولكون الجريمة الإلكترونية عابرة للحدود فإنها تفرض التعاون بين الدول من أجل حصرها ومكافحتها.

فنظرا لخطورة الجريمة السيبيرانية وصعوبة التحقيق فيها فإنه لا بد من:

- إصدار المزيد من القوانين المتعلقة بهذه الجرائم وتطويرها ومراجعتها.
- الاهتمام بالتأهيل المناسب لكوادر الأجهزة المكلفة بالبحث والتحقيق بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة وجدارة.
- إنشاء هيئات متخصصة في مجال تقنيات التكنولوجية لمكافحة الجرائم الإلكترونية.
- توسيع سلطات قاضي التحقيق والأجهزة المختصة بالبحث والتحري عن الجرائم المعلوماتية.
- تفعيل وتكثيف التعاون الدولي لمواجهة الجرائم الإلكترونية.
- تفعيل المساعدة القضائية بين الدول وتبادل المعلومات فيما بينها لكون الجريمة الالكترونية جريمة عابرة للحدود.
- الاعتماد على التحقيق المشترك والفعال بين الدول لمجابهة الجرائم السيبيرانية.

قائمة المراجع

قائمة المراجع والمصادر.

أولاً: الكتــب.

أ- الكتباللغة العربية:

1. أحسن بوسقيعة، التحقيق القضائي، ط7، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2008.
2. أعمر قادري، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.
3. جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجي، دار النهضة العربية، القاهرة، مصر، 2002.
3. حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009.
4. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، عنوان 84 شارع زكرياء غنيم، الإبراهيمية، الإسكندرية، ، مصر، 2008.
5. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.
6. عادل يوسف عبد النبي الشكري، الجريمة الإلكترونية وأزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، عمان، 2008.
7. عادل يحي، الأحكام العامة للتعاون الدولي لمكافحة الجريمة، ماهيته، صوره، أسسه، أهميته، ط1، دار النهضة العربية، القاهرة، مصر، 2013.
8. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، مصر، 2007.
9. عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن بين النظرية والتطبيق، د.ب، 2007.

10. عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة، ط2، دمشق، 2007.

11. محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الكثافة للنشر والتوزيع، عمان، 2004.

12. محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، بدون بلد النشر، 2016.

13. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطية، القاهرة، مصر، 2008.

14. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.

15. نادية دردار، الجهود الدولية، لمكافحة الجريمة، ط1، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017.

16. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، ط2، دار الفكر الجامعي، مصر، 2011.

17. نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2007.

19.أنيس حسين السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، الإسكندرية، 2016.

20.بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2010.

21.حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2009.

22.سليمان أحمد فضل، الخبرة في مجال التحقيق الإلكتروني، دراسة مقارنة، ط2، القاهرة، مصر، 2006.

23.زياد إبراهيم شيحا، الإنابة القضائية الدولية في المسائل الجنائية ونطاق العلاقات الخاصة الدولية، دار النهضة العربية، القاهرة، مصر، 2015.

24.عبد الفتاح عبد اللطيف، الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، ط1، دار الحامد للنشر والتوزيع، عمان، الأردن، 2011.

25.علي حسن محمد الطوالية، التفتيش الجنائي علم نظم الحاسوب والأنترنت، عالم الكتب الحديثة، الأردن، 2015.

26.ياسر أمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009.

27.هلال عبد الله أحمد، اتفاقية بودابيست لمكافحة جرائم المعلوماتي، معلقا عليها، دار النهضة العربية، القاهرة، 2011.

ب/ الكتب باللغة الأجنبية.

RODIN ADRIAN. COMPUTER CRIME AND THE LAW .CLT .1991. VOL 15 P 399

.

ثانيا: الرسائل والمذكرات الجامعية:

أ-الرسائل:

1. نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية، دراسة مقارنة، رسالة دكتوراه في العلوم القانونية، القانون الخاص، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الجيلالي اليابس، سيدي بلعباس، 2002.

2. شريف نصر أحمد، النظرية العامة للخبرة في المواد الجنائية، رسالة دكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2010.

3. إسماعيل بن يحي التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، علوم في القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد، تلمسان، 2021.

4. جمال براهيمي، التحقيق الجنائي في الجريمة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018.

5. رجاء أومدور، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشري الإبراهيمي، برج بوعريرج، 2020.

6. فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009.

7. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه في القانون، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر -1-، 2011.

8. حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة دكتوراه في العلوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2016.

ب- المذكرات:

1. إبتسام بوبعاية، التحقيق في الجريمة الإلكتروني، مذكرة ماستر أكاديمي في الحقوق، فانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022.

2. خديجة بنقة، السياسة الأمنية الأوروبية في مواجهة الهجرة غير الشرعية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، جامعة محمد خضر، بسكرة، 2013.
3. عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارنة، مذكرة ماستر في العلوم الجنائية، 2012.
4. عبد الله بن الحسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي والادعاء العام، مذكرة ماستر، كلية الدراسات العليا، الرياض، 2014.
5. عدلي دحمان، سعد الدين تامر البشير، التحقيق الجنائي في الجرائم الالكترونية. مذكرة ماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة زيان عاشور، الجلفة، 2020-2021.
6. محمد بوعمرة، سيد علي نبيال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر في العلوم القانونية، قانون الأعمال، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أكلي محمد لحاج، البويرة، 2019.
7. سعيد علي نعيم، آليات التحقيق والتحري في الجرائم المعلوماتية في القانون الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة لحاج لخضر، باتنة، 2012.
8. مريم أحمد مسعود، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة ماستر في القانون الجنائي، جامعة ورقلة، 2013.
9. نعيم سعيداني، آليات البحث والتحريات عن الجريمة المعلوماتية في القانون الجنائي، رسالة ماستر، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012.

ثالثا/ -المقالات والمداخلات والمحاضرات:

أ/ -المقالات

1. سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، المجلد عشرون (20)، العدد الرابع، الشارقة، الإمارات العربية المتحدة، 2011، ص ص 15-54.
2. عبد القادرفلاح، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلّد 04، العدد 02، 2019، ص ص 1689-1708.
3. عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والاتصالات، مجلة دائرة البحوث والدراسات القانونية والسياسة، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جامعة تبسة، جانفي 2018، ص ص48-66.
4. هدى زوزو، التسرب كأسلوب من أساليب التحرّي في قانون الإجراءات الجزائية الجزائري مجلة دفاتر السياسية والقانون، العدد 11، جامعة قاصدي مرباح، ورقلة، جوان 2014.
5. هوام علاوة، التسرّب كآلية للكشف عن جرائم الانترنت في القانون الجزائري، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012، ص ص3-4.
6. محمد السيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إليزي للبحوث والدراسات، العدد 2، المركز الجامعي، إليزي، الجزائر، 2007، ص ص 28-40.
7. نجاة زعزوقة، ليلى بن قلة، مجلة الدراسات القانونية والاقتصادية،مخبر القانون المقارن جامعة تلمسان، الجزائر،2021، ص ص292-309.

ب/-المداخلات:

1. هارون بحرية، دور الدليل الرقمي في إثبات الجريمة الإلكترونية في التشريع الجزائري، مداخلة مشارك بها في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2015.
2. آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني في الجزائر، مداخلة الملتقى الدولي حول "الإجرام الليبرالي المفاهيمي والتحديات"، 2017.

ج/-المحاضرات:

1-إسماعيل طواهري، محاضرات شرح النيابة العامة طبقا للقانون الجنائي الجزائري، سنة أولى ماستر، 2021.
1. نادية حسان، محاضرات في مادة الحماية الجنائية للنظم المعلوماتية، ماستر القانون الجنائي والعلوم الجنائية قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2021-2022.

رابعا/-الاتفاقيات:

1. ديباجة الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم الجزائري في 25 أكتوبر 2003، المصادق عليه بموجب مرسوم رئاسي رقم 07-357 مؤرخ في 01 ديسمبر.
2. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

خامسا/ -النصوص القانونية:

أ- القوانين:

1. القانون رقم 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، عدد 47 الصادر في 16 غشت 2009.
2. القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 09 جوان 1966، الصادر بالجريدة الرسمية، عدد 71، 10 نوفمبر 2004المتعلق بالإجراءاتالجزائية.
3. القانون 06-22 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية،جريدة رسمية عدد 84، صادر بتاريخ 2006/12/24 معدل ومتمم.

ب/ -الأوامر:

1. أمر رقم 66-155، مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية، معدل ومتمم لاسيما بالقانون رقم 17-07 المؤرخ في 27 مارس 2017.

2. أمر رقم 66-156، مؤرخ في 18 صفر1386، الموافق 8 يونيو 1966، يتضمن قانون العقوبات،المعدل والمتمم بالقانون 15/04 المؤرخ في 25 ديسمبر 2004.

جـ/ -المراسيم:

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة 1436 الموافق لـ 08 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53، الصادرة في 18 أكتوبر 2015.

2. المرسوم الرئاسي رقم 172/19 المؤرخ في 06 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، جريدة رسمية للجمهورية الجزائرية، العدد 37، مؤرخة في 09 يونيو 2019.

3. المرسوم الرئاسي رقم 07-357 المؤرخ في 2003/12/01، الذي يصادق عل ديباجة الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلقة بالتعاون في مجال الأمن ومكافحة الإجرام المنظم في الجزائر يوم 2003/10/25.

سادسا: المواقع الإلكترونية:

1. موقع المديرية العامة للأمن الجزائريwww.aleaifpoloce.dz.

2. موقع أرضية المجلات العلمية الجزائرية https://www.asjp.cereist.dzi

03 www.arab.legal.net.org

فهرس

ملخص:

الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام و الاتصال الحديثة و هي تختلف تماما على الجرائم التقليدية.

يعتمد البحث في هذا المجال على معطيات قانونية و أخرى فنية نظرا لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الانترنت و العلوم القانونية الإجرائية و لذلك فقد عالجنا في فصلين مختلف الجوانب المتصلة بالموضوع، حيث تناولنا في الفصل الأول الإطار المفاهيمي للتحقيق الجنائي في الجرائم الالكترونية، حيث خصصنا المبحث الأول لتعريف الجريمة الالكترونية فيما خصصنا المبحث الثاني للهيئات المختصة بالتحقيق الجنائي في الجريمة الالكترونية، أما الفصل الأول فتناولنا فيه الإطار الإجرائي للتحقيق الجنائي في الجرائم الالكترونية،حيث خصصنا المبحث الأول الأساليب الوطنية للتحقيق في الجرائم الالكترونية،أما المبحث الثاني فخصصناه للأساليب الدولية للتحقيق في الجرائم الالكترونية .

في الأخير ختمنا بحثنا بمجموعة من النتائج التي توصلنا إليها و التي تعتبر كإجابة على الإشكالية،مع تحصيل مجموعة من التوصيات القانونية التي من شأنها أن تدعم آليات البحث و التحقيق في هذا النوع من الجرائم المستحدثة.

الكلمات المفتاحية: الجرائم الالكترونية، التحقيق الجنائي الالكتروني،الاثبات الالكتروني، الأمن السيبيراني.