جامعة زيان عاشور -الجلفة-
Zian Achour University of Djelfa
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

قسم الحقوق

# التحقيق الجنائي في الجرائم الالكترونية

مذكرة ضمن متطلبات
نيل شهادة الماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية

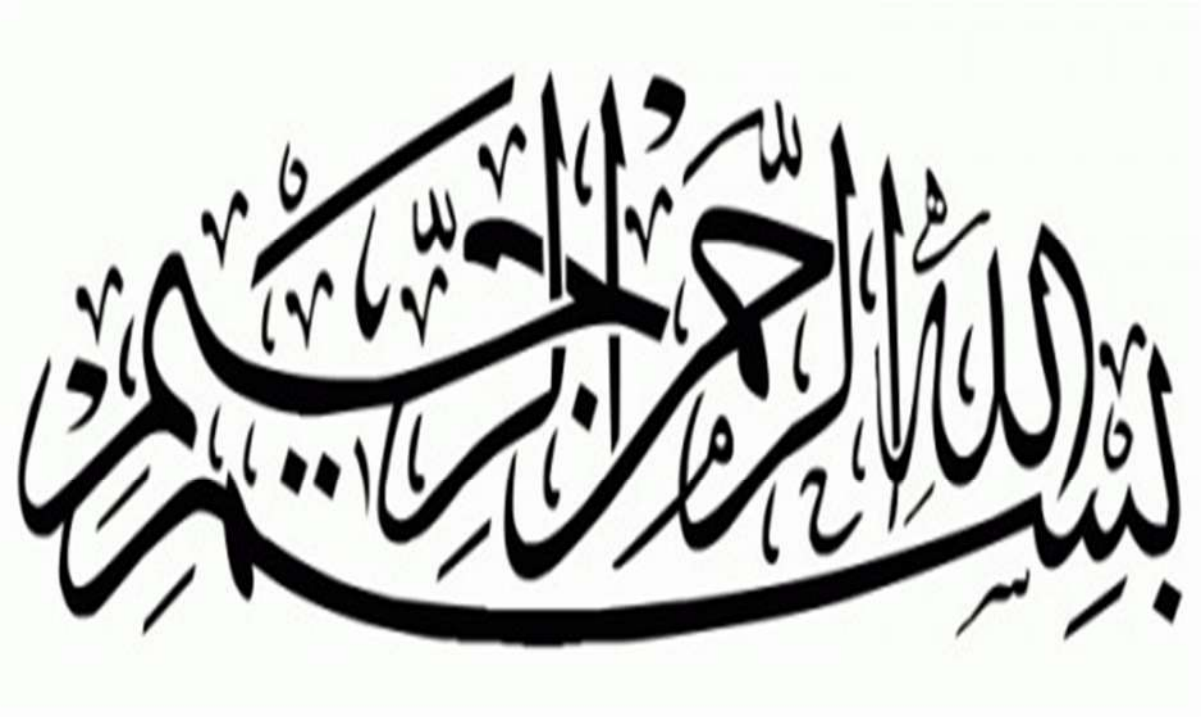
إعداد الطالب :
- عدلي دحمان
- سعد الدين ثامر البشير

إشراف الأستاذ:
-د. قراشة محمد رشيد

لجنة المناقشة

| | |
|---|---|
| -د/أ. بن مسعود احمد | رئيسا |
| -د/أ. قراشة محمد رشيد | مقررا |
| -د/أ. سابق طه | ممتحنا |

الموسم الجامعي 2021/2020


بسم الله الرحمن الرحيم

# شكر وعرفان

أحمد الله الذي أنار لنا طريق العلم ووفقنا لإتمام عملنا المتواضع هذا ، رغم كل الصعاب

بادئ ذي بدء نتقدم بالشكر الجزيل والامتنان العميق إلى الأستاذ المشرف الدكتور "قراشة محمد رشيد" على جهوده وتوجهاته وعلى قلبه الكبير وكلمته الطيبة

كما نتقدم بالشكر لكل من ساعدنا وقدم لنا يد العون في إنجاز هذا العمل المتواضع من قريب أو من بعيد

إلى كل الأساتذة الكرام بقسم الحقوق، وإلى كل عمال كلية الحقوق والعلوم السياسية

و إلى كل إطارات وعمال جامعة الجلفة.

سعد الدين ثامر البشير-عدلي دحمان

# الاهداء

اهدي ثمرة جهدي إلى روح أخي وحبيبي وفقيدي حناني خضر رحمة الله عليه

" وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُلْ رَّبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيراً"

الآية(24) من سورة الإسراء

على ذكر آيات المولى العزيز الحكيم

إلى التي يرتاح إليها البال وتهدأ العواطف إلى التي أسعد بسعادتها وأهنأ بهنائها ... إلى التي منحتني الأمل والتفاؤل إلى منبع العطف والحنان، أمي، أمي، أمي... ثم أمي.

إلى من كان دوما روائي ولم يبخل علي، أبي العزيز الذي مهما عملت لن أرد له خيره.

إلى أخوتي وأخواتي وأولاد إخوتي.

إلى كل من ساهم من قريب أو بعيد في مديد العون.

سعد الدين ثامر البشير

# الاهداء

إلى التي نقشت اسمها في الفؤاد ، قرة عيني ونور حياتي ودربي ،

وعماد روحي يا أغلى جوهرة في وجودي أمي

إلى أحق الناس بصحبتي والذي جند حياته لتربيتي إلى الذي منحني الثقة في ذاتي ،

منير دربي وقدوتي وافتخاري أبي .

إلى إخوتي وأخواتي والى أكاليل الزهور البريئة التي غمرتني بروائحها الذكية

أبناء إخوتي و أخواتي .

إلى من لا يستطيع القلب فراقهم بعدما تعود لقائهم ....

إلى كل عائلة عدلي جميعا .

عدلي دهمان

مقدمة:

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري والمعرفي الهائل غير المعهود، وذلك بفضل الثورة العلمية التكنولوجية في مجال الاتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة، ووفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة، الاقتصادية، الاجتماعية، الثقافية، والعلمية، تهاوت أمامها الحدود السياسية والحواجز بين الدول والشعوب، وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت وطوت الأبعاد، بما تتميز به من عنصري السرعة والدقة في تجميع المعلومات، تخزينها ومعالجتها، ومن ثم نقلها و تبادلها عن بعد بين الأطراف المختلفة داخل الدولة الواحدة أو بين عدة الدول، حتى أضحت فيه الكرة الأرضية قرية صغيرة تسبح في فضاء الكتروني، وهو ما دعا بالكثير من المفكرين إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر، ففي حين كان الهدف من الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فان هدف الثورة الثانية إحلال الآلة محل النشاط الذهني للإنسان.

وبالرغم من المزايا والفوائد الجمة التي تحققت وتتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات وسائل تكنولوجيات المعلومات والاتصال، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى، في الوقت ذاته، على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات. الشيء الذي استتبعه ظهور نمطا جديدا من الجرائم، لم يكن معهودا من قبل سمي بجرائم تقنية المعلومات أو الجرائم الإلكترونية.

ولا جدال في اعتبار الجرام الإلكترونية من أخطر وأعقد الجرائم على الإطلاق وتأتي في مقدمة الأشكال الجديدة للجريمة المنظمة، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها وخصوصية مرتكبيها ووسائل كشفها. فهي جريمة تقنية سهلة الارتكاب، تنشأ في الخفاء وفي بيئة الكترونية افتراضية مكونة من إشارات وذبذبات مغناطيسية تتساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصالات بصورة آلية دون أن تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات

وخبرات تقنية عالية، فضلا على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأية سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي.

وقد أدت هذه الخصائص التي تميز الجريمة الإلكترونية إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية مع ما قد يشكله ذلك من مساس بمبدأ الشرعية الجزائية والتفسير الضيق للنص الجنائي وحضر القياس، وهو ما ألقي مسؤولية كبيرة على عاتق المشرع الجزائي في اتخاذ الخطوات التشريعية الضرورية لمواجهة الجرائم الإلكترونية الناشئة عن إساءة استخدام الأنظمة المعلوماتية. وذلك بسن نصوص جنائية جديدة تتوافق مع هذه الأنشطة الإجرامية المستحدثة، وتمكن مرفق العدالة الجنائية من تطوير آليات ووسائل التصدي للجرائم التي أفرزتها تكنولوجية الإعلام والاتصال، والاستفادة من معطيات هذه التكنولوجيا الحديثة في الكشف عن الجرائم وإثباتها وملاحقة مرتكبيها لتقديمهم إلى العدالة.

ولا تقتصر الصعوبات والمشكلات التي تثيرها ظاهرة الإجرام الالكتروني فقط على القانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الإجرام، بل امتدت إلى نطاق القانون الجنائي الإجرائي، حيث صيغت نصوصه لتنظم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كثيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتتجسد أولى المشكلات الإجرائية في مجال الجرائم الالكترونية، في التحديات القانونية والعملية التي تثيرها عملية البحث والتنقيب أمام سلطات التحقيق بجميع مستوياتها وباختلاف أدوارها. وبالتحديد فيما يخص إثبات هذه الجرائم والآلية المناسبة لمباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية وصولا إلى الحقيقة. إذ أن الجهات المكلفة بالبحث والتحري متعودة على التعامل مع الجريمة التقليدية، التي ترتكب في عالم مادي وملموس يلعب فيه السلوك المادي الدور الأكبر والأهم، ويسهل التحري والبحث فيها بالنظر إلى ما تتضمنه من عناصر مادية يمكن إدراكها بالحواس، وما يمكن أن يخلفه المجرم من أثار محسوسة في مسرح الجريمة من بصمات أو قطرات دم أو محررات مزورة...، على خلاف الجريمة الالكترونية

التي ترتكب في مسرح الكتروني غير مادي يختلف تماما عن المسرح التقليدي، ولا يخلف مرتكبها أي أثار، بسبب دقة وسرعة اقترافها، وإمكانية محو أثارها، وإخفاء الأدلة المحصلة عقب وقوعها مباشرة. وهو ما يجعل سلطات البحث والتحقيق في حيرة من أمرهم إزاء هذه الوقائع الاستثنائية غير المألوفة.

ويزداد الوضع تعقيدا بالنسبة لجهات الاستدلال حينما يتعلق التحقيق بجريمة الكترونية امتد أثارها إلى خارج الإقليم الوطني، بحيث تثير مسألة تتبعها والدخول إليها قصد جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق مشكلات تتعلق بسيادة الدولة والولاية القضائية، والتي لا يحتاج حلها إلى تعاون دولي في هذا المجال.

ومع إدراك الصعوبة التي تطرحها المواجهة الإجرائية لأشكال الإجرام الجديدة التي أفرزتها بيئة المعالجة الآلية للمعطيات والتنبه لأثارها السلبية، بدأت مهمة معالجتها تحظى باهتمام متزايد من الحكومات وحتى العديد من الهيئات الدولية، فأخذ الفنيون وخبراء الحسابات والإعلام الآلي، يركزون جهودهم البحتة وتجاربهم العلمية على سد ثغرات الأنظمة الأمنية وتحسين وتطوير أساليب الحماية الفنية للنظم والبرامج المعلوماتية لتصل إلى أقصى درجة ممكنة من الفعالية تجنبا لوقوع اعتداءات عليها أو بواسطتها، وتكفل الفقه الجنائي بإبراز أوجه القصور التي تعتري تطبيق النصوص الإجرائية للتشريعات التقليدية القائمة على النمط الإجرامي الجديد الذي أسفرت عنه المعلوماتية، وسعى المشرع إلى تدارك هذا القصور باستحداث نصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، تمكن رجال العدالة الجنائية من البحث والتحقيق واستنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم. ومن ثم تحقيق التوازن بين الضرورة الملحة في عصرنا إلى الاستفادة من إمكانات الحسابات و تقنيات التكنولوجيا الحديثة، وبين الحاجة الفردية والاجتماعية إلى الحماية الجزائية من انعكاسات هذه التقنيات.

**من هنا تظهر أهمية موضوع " التحقيق الجنائي في الجرائم الالكترونية" وسبب اختيارنا له رغم ما يكتنفه من صعوبات ترجع في الأساس إلى حداثة هذا الموضوع وما** يتسم به من صبغة علمية بحتة جديدة غريبة في تصورنا على رجال القانون، إذ لم ينل حظه بعد من البحث والتمحيص على المستوى الفقه الجنائي، كما أن معظم الدراسات والأبحاث القانونية التي عنيت بالجرائم الالكترونية تركز على الجانب الموضوعي فقط، ما نتج عنه قلة وندرة المراجع

والمؤلفات التي تعرضت للجانب الإجرائي. وهو ما أثار اهتمامنا للبحث وإثراء النقاش القانوني في هذا الموضوع، بالتالي ومن خلال مشكلة الدراسة يمكننا أن نتساءل عن: أي مدى استطاعت أجهزة التحقيق في الجريمة الإلكترونية مواكبتها ومواجهتها؟ هذه الإشكالية يمكن أن تتفرع منها عدة تساؤلات منها:

1- ما هي الجريمة الإلكترونية وما هو المجرم الإلكتروني؟

2- ما المقصود بالتحري والضبط في الجرائم الإلكترونية؟

3- ما هي الإجراءات المتعلقة بالتحقيق في الجريمة الإلكترونية؟

وعلى هذا الأساس اعتمدنا على المنهج الوصفي التحليلي، الذي يقوم بوصف هذه الظاهرة وتحليل المواد التي تناولتها، ذلك لأن الدراسة تهتم بسبل التحقيق في الجرائم الإلكترونية وكشفها من الناحية الفنية والقانونية.

وحتى نتمكن من معالجة الإشكالية المطروحة ارتأينا إلى تقسيم الخطة إلى فصلين معتمدين على تقسيم ثنائي للخطة، ففي الفصل الأول سنتناول فيه مفهوم جهاز التحقيق للجريمة الإلكترونية والذي أدرجناه في مبحثين تناول كل منهما كيفية التحقيق في الجريمة الإلكترونية وكذا السلطات المخصصة بالتحقيق في الجريمة الإلكترونية، أما الفصل الثاني فتطرقنا إلى إجراءات التحقيق في الجرائم الإلكترونية وأدرجناه كذلك في مبحثين هما: المبحث الأول: محدودية سريان إجراءات التحقيق المألوفة على الجرائم الإلكترونية، أما المبحث الثاني: استحداث إجراءات تحقيق خاصة بالجرائم الإلكترونية.

لا يفوتنا القول أنه تلقينا صعوبات كثيرة في اختيار موضوع البحث في حد ذاته كونه حديث ولم يسبق بحثه بوضوح وتعمق، ولو أن هناك مراجع ومقالات تناولت الموضوع إلا أنها لم تعالجه من كل جوانبه أو أدرجته بشكل سطحي إضافة إلى أن الجرائم محل الدراسة ترتبط بالحاسب الآلي مما يتطلب الإلمام بمكوناته وبنظام المعالجة الآلية للمعلومات والشبكات الإلكترونية.

# الفصل الأول:

# مفهوم جهاز التحقيق للجريمة الالكترونية

## مقدمة

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقد بدا لنا أنه وقبل الخوض في الإجراءات التي تطبق على الجرائم الإلكترونية، إذا يجب الإلمام الجريمة الإلكترونية وخصائصها وأيضا التطرق إلى الأجهزة المختصة في التحقيق في الجريمة الإلكترونية.

وعلى ضوء ذلك سنقسم الفصل الأول إلى الجريمة الإلكترونية وكيفية التحقيق فيها في المبحث الأول أما المبحث الثاني سيكون تحت عنوان السلطات المختصة في الجريمة الإلكترونية.

## المبحث الأول: الجريمة الإلكترونية والتحقيق فيها:

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عدة آراء فقهية في محالة فهم المقصود بالجريمة الإلكترونية.

وعليه سنحاول من خلال هذا المبحث أن نتطرق إلى الجريمة الإلكترونية والتحقيق فيها، حيث يتضمن المطلب الأول التعريف بالجريمة الإلكترونية وخصائصها وأنواعها، أما المطلب الثاني سنتطرق إلى التحقيق فيها في التشريع الجزائري.

### المطلب الأول: مفهوم الجريمة الإلكترونية.

ظهرت تعاريف كثيرة حول تعرف الجريمة الإلكترونية ما بين مضيف لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم استخدام الحسابات أو جرائم المعالجة الآلية للبيانات والبعض الآخر أطلق عليها اسم الإجرام المعلوماتي، وفيما يلي: تفصيل لمفهوم هذه الجريمة من حيث التعريف والخصائص.

#### الفرع الأول: تعريف الجريمة الإلكترونية:

تعتبر الجريمة الإلكترونية من الظواهر الحديثة لارتباطها بتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل إن بعض الفقهاء، ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني)[1].

**أولا: تعريف الجريمة الإلكترونية لغة.**

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجرمه الرجل على قومه وإليهم، ذنب وجني جنتئة[2].

**ثانيا: تعريف الجريمة اصطلاحا:**

معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الموارديي في الأحكام السلطانية بقوله: "الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير

[1] خالد ممدوح، **أمن الجريمة الإلكترونية**، الدار الجامعية، الإلكترونية، الإسكندرية، 2008، ص 41.

[2] ضياء مصطفى عثمان، **السرقة الإلكترونية**، دار النفائس، عمان، الطبعة الأولى، 2011، ص32.

يعني إذا كانت ممن يتعمد ارتكابها، أما الإمام أبو زهرة فبعدها ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريف آخر للجريمة فقال "هي المعصية التي يكون فيها عقاب يقرره القضاء "[1].

## ثالثا: تعريف الجريمة الإلكترونية فقها وقانونا.

**أ- التعريف الفقهي:** انقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها، الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية.

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها ومن التعريفات التي وضعها أنصار هذا الاتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى.

وفي هذا الاتجاه أيضا الجانب الفقهي بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة الإلكترونية هي اعتداءات ترتكب بواسطة المعلومات بغرض تحقيق ربح.

**ب- التعريف القانوني:** أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها: « جرائم المساس بأنظمة المعالجة الآلية اللامعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية »، وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية. ولول هذه النظم المعلوماتية وشبكات الاتصال ما كان أن نسبغ صفة المعلوماتية على هذه الجرائم.

وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 على أنها: « جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية»، ويلاحظ على هذا التعريف ما يلي:

[1] بخي فاطمة الزهراء، **إجراءات التحقيق في الجريمة الإلكترونية**، 2014، ص09.

– أن المشرع قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معاير موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثا معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[1].

– كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري[2].

### الفرع الثاني: خصائص الجريمة الإلكترونية وأنواعها.

إذ ما نقصد به ذاتيه الجرائم الإلكترونية هو استقلاليتها وتميزها من غيرها من الجرائم سيما التقليدية منها، وذلك بمجوعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن تبرز أهم خصائص المجرم الإلكتروني والمجني عليه الجريمة الإلكترونية وأنواع المجرمين الإلكترونيين وصفاتهم[3].

## أولا: خصائص الجريمة الإلكترونية.

### الفرع الأول: خصائص الجرائم المعلوماتية

إن ما نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي:

**أ– الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية):**

إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات

---

[1] بوضياف اسمهان، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، العدد 11 سبتمبر2018، ص 353. -352

[2] محمد بوعمرة – سيد علي بنينال، **جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري**، مذكرة تخرج لنيل شهادة الماستر في قانون الأعمال، كلية الحقوق، جامعة البويرة، 2013، ص06.

[3] سعيداني نعيم، **آليات البحث والتحري** عن **الجريمة المعلوماتية في القانون الجزائري**، 2013، ص 31.

كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدا.

فالجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث، أو القيام بإعداد أحد البرامج الخبيثة (Virus) في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم.

وتظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الاتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات.

ومفاد ما سبق ذكره أن الجرائم المعلوماتية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أو خارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الاعتداء.

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى

إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية. وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

**ب- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها:**

تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من المجني عليهم. كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام وإنما هي معلومات وبيانات تغير أو تعدل أو تمحي كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي فلا تترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها.

فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.

كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات

وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها .فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم.

بالإضافة إلى صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية ويمكن اعتبار أنه من بين الأسباب أيضا التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية وإثباتها المجني عليهم أنفسهم، ذلك أن هؤلاء قد يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه، وهو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها.

**ثانيا: أنواع الجريمة الإلكترونية.**

نظرا لانتشار الجريمة الالكترونية بشكل كبير فقد تعددت أنواع هذه الجرائم وأهمها ما يلي:

**الجريمة المادية:** هي التي تسبب أضرارا مادية على الضحية أو المستهدف من عملية النصب وتؤخذ واحدة من الأشكال الثلاثة التالية:

- عملية السرقة الإلكترونية كالاستيلاء على ماكنات الصرف الآلي، والبنوك كتلك المنتشرة في الكثير من الدول وبها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ثم استخدامها الصرف أموال حساب الضحية.
- إنشاء صفة إنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة.

– الرسائل البريدية الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج من الوعد بنسبة من المبلغ أو تلك التي توهم صاحب البريد الالكتروني بفوزه بإحدى الجوائز أو الينا صيب.

الجريمة الثقافة: هي استيلاء المجرم على الحقوق الفكرية ونسبتها لهم دون موافقة الضحية وتكون على إحدى الصور الآتية:

– قرصنة البرمجيات وهي عملية نسخ أو تقليد البرامج إحدى الشركات العالمية على اسطوانات وبيعها للناس بسعر أقل.

– التعدي على القنوات الفضائية المشفرة واتاحتها عن طريق الانترنت من خلال تقنية Soft Copy .

– جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة.

**الجريمة السياسية والاقتصادية:** تستخدم المجموعات الارهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويل بعض الأموال في سبيل تحقيق أهدافهم.

– الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات.

– نشر الأفكار الخاطئة بين الشباب كالإرهاب والادمان والزنة لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

**الجريمة الجنسية:** هذا النوع من الجريمة يمكن أن يتمثل في إحدى الصور الآتية:

**الابتزاز:** من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وفيه مجموعة من صورها واجبارها على الخروج معه أو فضحها بما يملكه من صورها.

**التغرير والاستدراج:** في العادة هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر برامج المحادثة يكون مع علاقة معها ثم يستدرجها بالكلام ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها بما يملكه من صور وتسجيلات من صوتها إن لم تستجب لطلباته[1].

**جرائم حسب الأفراد:**

[1] نواوي سليمة، **دور الدرك الوطني في محاربة الجريمة الالكترونية**، جامعة المسيلة، 2018/2019، ص 25–27.

هي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير شرعية، حسابات البريد الإلكتروني وكلمات السر التي تخصهم وقد تصل إلى انتحال شخصياتهم وأخذ صور وملفات المهمة من أجهزتهم بهدف تهديدهم وينطوي تحت هذا القسم من الجرائم كل من:

- جرائم التشهير بهدف تشويه سمعت الأفراد.
- جرائم السب والشتم والقذف.
- جرائم المطاردة الالكترونية[1].

## ثالثا: المجني عليه في الجريمة الإلكترونية.

المعتدي عليه في الجريمة الإلكترونية هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا، شركة، أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، الاقتصادية والسياسية التي ينبغي أن يستغل الحاسوب في إدارة أعمالها، وحسب تقديرات بعض خبراء الصندوق الدولي للبنوك، فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجريمة الإلكترونية التي لا يعلم ضحاياها عنها شيئا إلا عندما تكون النظم المعلوماتية المملوكة لهم هدفا للجريمة الإلكترونية، حتى في حالة عملهم بذلك فهم يفضلون عدم إفشاء الفعل لأنه لا يوجد من يريد الاعتراف بأنه تم انتهاك نظامه المعلوماتي[2].

والجدير بالذكر أن سلبية المجني عليهم أو ضحايا الجريمة الإلكترونية، وخوفهم من الإبلاغ حفاظا على سمعتهم التجارية ومكانتهم المرموقة، غير معين على التمادي في اقتراف مثل هذه الجرائم، وتوجد هذه الجرائم بصفة خاصة إلى البنوك، وإلى المواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي تعتمد أكثر من غيرها على أجهزة الحاسوب، وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضررا[3].

---

[1] بن سولة نور الدين، **الجرائم الالكترونية في ضوء التشريع الجزائري**، المجلد التاسع، العدد 1، مارس 2018، ص272.

[2] محمد بوعمرة – سيد علي بنينال، مرجع سابق، ص11.

[3] عبد الفتاح البيومي حجازي، **مكافحة جرائم الأنترنت**، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص ص 96-97.

## رابعا: أنواع المجرمين الإلكترونين وصفاتهم.

قد يكون الجاني في الجريمة الإلكترونية، إما شخص يعمل بمفرده أو ضمن منظومة بغض النظر عن هذه الأخيرة، فقد تكون تجارية، سياسية، أو عسكرية[1]، ويمكن تقسيم أنواع المجرمين إلى فئتين.

**الفئة الأولى: صغار نوابغ المعلوماتية:** ويقصد بهم البالغ المفتون بالمعلوماتية والحسابات الآلية، وكثيرا ما لفتوا النظر في الآونة الأخيرة، ويرتكب هؤلاء الأشخاص الجرائم بغرض التسلية والمزاج مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم.

الفئة الثانية: المحترفون في الجريمة الإلكترونية.

ويتمتع أصحابها بخيرة ودراية أكبر ويتقسمون إلى: فئة المتسللين الهواة Hackers: هم لا يهدفون في حربهم المعلوماتية إلا للمغامرات وإظهار القدرات أمام الأقران فلا توجد عادة عندهم هؤلاء أطماع مالية.

**فئة القراصنة الخبيثون MALICIOUSHACERS** : هم أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية، ويندرج تحت هذه الفئة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

فئة حلالي المشاكل الشخصية: هم الأكثر شيوعا يترتب على إجرامهم في الكثير من الأحيان خسائر كبيرة تحلق بالمجني عليهم، رغبة منهم في إيجاد حلول لمشكلات مادية تواجههم، والتي لا يتم حلها بالوسائل الأخرى وغالبا ما يكون المجني عليه المؤسسة التي يعملون بها. فئة المجرمين المهنيين: وتظم مجرمي الجريمة الإلكترونية الذي يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، ويعمل المنتمون إلى هذه الفئة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة.

**فئة أصحاب الدعوة المتطرفة:** وتدخل في عدادها الجماعات الإرهابية أم المتطرفة، والتي تتكون بدورها مجموعة أشخاص لديهم معتقدات وأفكار اجتماعية سياسية أو دينية، يرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامية أحيانا[2].

---

[1] عبد الفتاح مراد، **مرجع سابق**، ص45.

[2] بخي فاطمة الزهراء، **مرجع سابق**، ص 23-25.

وقد بدأ اهتمام الجماعات الإرهابية وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة بأوروبا باسم THERED BRIGADES بتدمير ما يزيد من 60 مركز للحاسبات الآلية خلال الثمانينات لتلف الأنظار إلى أفكارها ومعتقداتها[1].

**فئة الجناة المقصرية:** تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية وهي الإهمال، ولا شك في أن الاهتمام في مجال الحسابات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح ففي نيوزيلندا مثلا: قام الاثنان من مبرمجي الحسابات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائر بهذا التغيير، مما أنجم عن مقتل 60 راكب بعد تحطم الطائرة إثر اصطدامها بأحد الجبال وتمت محاكمتها بتهمة القتل الخطأ[2].

## المطلب الثاني: التحقيق في الجريمة الإلكترونية.

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

والتحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم العادية من حيث الإجراءات وذلك لحادثة هذه الجريمة ومهارة مرتكبيها في الإجرام ومحو الأدلة[3].

### الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية.

لا يختلف التحقيق في الجريمة الإلكترونية عن الجرائم الأخرى وسنتناول تعريفه لغة واصطلاحا، ولكي يكتمل هذا التعريف يجدر التطرق إلى تعرف المحقق الذي هو بدوره القائم بجميع وكافة اجراءات التحقيق. أولا: المقصود بالتحقيق الجنائي في الجريمة الإلكترونية. يهدف التحقيق إلى جمع الأدلة والتنقيب عليها.

---

[1] محمد بوعمرة – سيد علي بنينال، **مرجع سابق**، ص13.

[2] بخي فطيمة الزهراء، **مرجع سابق**، ص ص 23–25.

[3] سعيد (أبي نعيم)، **مرجع سابق**، ص 102.

أ- **تعريف التحقيق لغة:** التحقيق مأخوذ من حقق يحقق تحقيقا، حقق الظن بالله صدقه، الأمر أحكمه – مع فلان- في قضيته: أخذ رأيه فيها.

ب- تعريف التحقيق اصطلاحا: عرف التحقيق بمعناه العام أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها.

وعرف التحقيق أنه: مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها الإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة[1].

وكذلك عرف التحقيق بأنه: "مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهذا التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت كتقدير لزوم محاكمة المدعي عليه أو عدم لزومها"[2].

**ثانيا: تعريف المحقق.**

ذهب جانب من الفقه إلى تعريف المحقق بأنه: "كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غموضها وصولا إلى معرفة حقيقية الحادث وكشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة".

كما عرف البعض المحقق أو الباحث الجنائي بأنه الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها.

وعرف المحقق بأنه: "ذلك الشخص الذي عهد غليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى عمله من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة "[3].

---

[1] عمر بن إبراهيم بن حماد العمر، **إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي**، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007، ص 22.

[2] حسن الجوخندار، **التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية**، دار الثقافة عمان، الطبعة الأولى، 2008، ص 11.

[3] بخي فاطمة الزهراء، **مرجع سابق**، ص 40.

أما المشرع الجزائري فقد وضع تعرفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي: "يقوم قاضي التحقيق وفقا لقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي"

## الفرع الثاني: خصائص التحقيق الجنائي في الجريمة الإلكترونية:

تعد مرحلة التحقيق الابتدائي 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، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوة برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم،

ففي كثيرا من الجرائم المعلوماتية لم يترك الجاني ورائه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[1].

أولا: خصائص التحقيق.

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة.

وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[2].

ذلك أن الفكر البشري المتعلق بالجرم الإلكتروني يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يكون متغيرا أو متطورا أيضا، وذلك كنتيجة طبيعية لمواجهة المجرم الإلكتروني.

### 1/ أسلوب التحقيق الابتدائي في الجريمة الإلكترونية:

---

[1] محمد طارق عبد الرؤوف، **جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية**، الطبعة الأولى، 2011، ص 230.

[2] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، دار الفكر الجامعي، الطبعة الأولى، 2009، ص56.

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم للمحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمضاهاة البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع الجريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى.

**أ/ وضع خطة عمل التحقيق:** يبدأ المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوفرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي:

– وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.

– التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب التعامل مع هذه الجرائم.

– عمل دراسة جادة لكافة الإجراءات التحقيق خطة مسبقة التي يتم وضعها ومناقشتها من طرف العاملين في فريق التحقيق[1].

– تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في انجاز العمل من أجل ضمان مستوى جيد من الأداء.

– تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطار الفردية التي قد تنتج عن قلة الخبرة أنقص المعرفة، والتي تساعد في التقيد بالمستوى المطلوب والتي تضمن الخطوات التي يقوم بها المحقق خلال مراحل التحقيق).

**ب/ تشكيل فريق التحقيق:** إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة، ويجب

[1] محمد نصير السرحاني، **مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير**، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 72.

أن يتشكل فريق التحقيق من فنيين أخصائيين ذوي خبرة في مجال الحاسوب الأنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني وفي شكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرقها ظروف وملابسات كل جريمة[1].

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا 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 ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق من:

- خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادثة وكيفية التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي[2].

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية إستعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك[3].

**2/ العناصر الأساسية للتحقيق الابتدائي في مجال البرمجة الإلكترونية:**

نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات

---

[1] عبد الله حسين محمود، **إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية**، دبي، 2003، ص 612.

[2] عبد الله حسين محمود، **مرجع سابق**، ص 613.

[3] أنظر المادة 05 الفقرة الأخيرة من القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المعدل والمتمم في 2019.

واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي[1].

**أ/ الإجراءات التي يجب مراعاتها قبل البدء في التحقيق.**

– تحديد نوع نظام المعالجة الأولية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

– وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

– إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.

– مراعاة صعوبة 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.

– فصل خطوط الهاتف حتى لا يسيئ الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.

– التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه 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 الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.

– تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل .

**ب/ الإجراءات التي يجب مراعاتها أثناء التحقيق:**

– عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ.

– نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

[1] عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير المعلوماتي**، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، ص84.

– العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

– حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

– العمل على فحص وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلومات.

– أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة، وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب[1].

**ثانيا: الخصائص الفنية للمحقق.**

تلعب الأجهزة الفنية دروا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع ارتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص اقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلب التصدي لهذه الجرائم من قدرات فيه لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، ما يستلزم ضرورة توفير المهارات المطلوبة في هذا المجال.

والمشكلة الأساسية التي تواجب المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة التقديم المتهم للمحاكة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية، ولكن من الناحية يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[2].

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة و مناقشة الشهود وغير تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه

[1] سعيداني نعيم، **مرجع سابق**، ص ص 112–114.

[2] سعيداني نعيم، **مرجع سابق**، ص 115.

عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية يقوم بعمله على أحسن وجه ونذكره منها:

معرفة الجوانب الفنية والتقنية لأجهزة الأجهزة الحاسوب الإنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية التأهيل الكافي في الميدان التقي قد يغطي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية وتدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات، وبالتالية فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها[1].

## المبحث الثاني: السلطات المختصة بالتحقيق في الجريمة الإلكترونية.

### المطلب الأول: جهاز التحقيق الجنائي في الجريمة الإلكترونية وأقسامه.

نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.

#### الفرع الأول: تعريف جهاز التحقيق في الجريمة الإلكترونية.

جهاز التحقيق في الجريمة الإلكترونية هو عبارة عن الوظائف المتخصصة إلكترونيا وقانونيا، التي يصدر بها قرار إداري وتشغل بنوعين من الأفراد الضباط وضباط الصف والمدنيين وتحكم علاقاتهم الوظيفية التسلسل النظامي للرتب العسكرية وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية الإلكترونية الرقمية ونظامها وبرامجها وشبكاتها[2].

#### الفرع الثاني: أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية.

أصبحت الجرائم في عصر التقنية الحديثة أربعة أنواع، جرائم الاعتداء على النفس، جرائم الاعتداء على المال، جرائم الاعتداء على المصلحة العامة، والجرائم الإلكترونية بعد أن كانت ثلاثة أنواع فقط[3].

---

[1] جميل عبد الباقي صغير **أدلة الإثبات الجنائي والتكنولوجي الحديثة**، دار النهضة العربية، القاهرة، 2002، ص115.

[2] محمد مصطفى موسى، **التحقيق في الجرائم الإلكترونية، مطابع الشرطة**، القاهرة، 2009،ص 286.

[3] محمد بوعمرة – سيد علي بنينال، **مرجع سابق**، ص24.

وعلى هذا الأسس قسمت الأجهزة التي تتولى التحقيق في هذه الجرائم إلى:

**أولا: أجهزة الأمن العام:**

وتختص بالتحقيق في جرائم الاعتداء على النفس والمال[1].

**أ- الجرائم الواقعة على الأشخاص:**

إن الحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال على ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الخاصة.

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها على الانترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإدارة على ذلك[2].

**ب- الجرائم الواقعة على الأموال:**

لقد صاحب ظهور شبكة الانترنت تطورات في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما انجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من هذه المعاملات.

وفي ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجز عنه من تطور ووسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

- السطو على بطاقات الائتمان والتحويل الإلكتروني وفي غير المشروع.
- القمار وغسل الأموال عبر الانترنت.
- جريمة السرقة والسطو على أموال البنوك.
- تجارة المخدرات عبر الانترنت[3].

ثانيا: أجهزة التحقيق في الجرائم المخلة بأمن الدولة. وتنقسم إلى :

---

[1] محمد مصطفى، **مرجع سابق**، ص 286.

[2] يوسف خليل يوسف العطيفي، **الجرائم الإلكترونية في التشريع الفلسطيني**، غزة، 2013، ص13.

[3] صغير يوسف، **الجريمة الإلكترونية**، عبر الانترنت، تيزي وزوو، 2013، ص44.

– أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولها أجهزة متخصصة مثل مباحث أمن الدولة في مصر، فرنسا والكويت[1].

– أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة متخصصة مثل المخابرات العامة في مصر[2].

وقد اشتغل الكثير من الجماعات المتطرفة الطبعة الاتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الانترنت التي سمحت لهم في ارتكاب جرائم غاية الشلك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الانترنت الكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت[3].

ثالثا: جهاز التحقيق في الجرائم الإلكترونية.

وهذا النوع من الأجهزة لم ينشأ بعد في كل الدول العربية وإن كانت بعض الدول قد أنشأته منذ أن استخدمت الحاسب الآلي وشبكات المعلومات، ويرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية إلى تحقيق الضبط الاجتماعي الإلكتروني حماية للمجتمع من الجرائم الإلكترونية وذلك للحد منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة[4].

ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد وضح أن تقنية المعلومات ستزيد التفاعل بين الإرهابيين، ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شكليا سيكون هناك مدخل للمعلومات والتقنية والتمويل والخداع المعقد وتقنيات الأفكار الهدامة، واذا تم استخدام تلك سواء عن طريق الدول أو فاعلين غير دوليين سيصبح ذبك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول.

---

[1] محمد مصطفى، **مرجع سابق** ، ص 286.

[2] محمد مصطفى، **مرجع سابق** ، ص287.

[3] بوضياف إسمان، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018، ص258.

[4] محمد مصطفى، **مرجع سابق**، ص287.

أما الجزائر فلا زالت إلى الآن تفتقر لجهاز خاص بالتحقيق في الجريمة الإلكترونية إلا أنه انعقدت عدة ملتقيات حول مخاطر هذه الجريمة وناشدت بإنشاء جهاز خاص بالتحقيق في الجريمة الإلكترونية في الجزائر، منها الملتقى الوطني للجريمة الإلكترونية الذي يضم بدائرة قديل بمبادرة من نقابة المحامين لولاية وهران، حيث أختتم بمجموعة من التوصيات منها: أنه لابد من الإسراع في إنشاء الهيئة الوطنية المكلفة بتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الإلكترونية، ومدها بالمساعدة والاستشارة اللازمة، وحث الخبراء على ضرورة الإسراع في إنشاء هذه الهيئة الوطنية التي ينص على استحداثها القانون رقم: 04-09 الصادر في 05 أوت 2009 والخاص بالوقاية من الجرائم الإلكترونية ومحاربتها والمكافحة ضدها والقضاء عليها[1].

## الفرع الثالث: معوقات وصعوبات التحقيق في الجريمة الإلكترونية.

يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق، لا تجاري خبرته وعلمه بالأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من الجرائم التي تكون أكثر فداحة وأشد ضررا على المجتمع[2].

**أولا: قلة خبرة القائمين بالتحقيق في الجرائم.**

توجد معوقات للتحقيق في الجريمة الإلكترونية تتعلق بالسلطة القائمة بالتحقيق وتجمع العدة أسباب نذكرها كالآتي:

**أ- قلة خبرة القائمين بالتحقيق في هذه الجرائم:**

لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم وتقص المهارات في استخدام جهاز الحاسوب والانترنت وعدم توافر المعرفة بأساليب ارتكاب الجريمة الإلكترونية، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب والانترنت وقلة المعرفة باللغة الأجنبية

[1] بخي فاطمة الزهراء، **مرجع سابق**، ص ص،50-51.

[2] محمد بوعمرة – سيد علي بنينال، **مرجع سابق**، ص28.

لاسيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لديهم تعرف بلغة المختصرات[1].

**بـــ- الصعوبات التقنية لاستخدام بروتوكول TCP/IP في الإثبات:**

هناك تحديات عند استخدام المحقق بروتوكول TCP/IP كدليل إلكتروني في الإثبات وهي:

- بروتوكول IP : وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محدد أحدث الفعل غير المشروع، ومع ذلك يمكن أي يستخدم كقرينة قضائية ضد مالك الجهاز على أن يثبت العكس.

- الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الاتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا موزعا على عدة عناوين.

- تكون المعلومات المحلية لمصدر عنوان IP غير حقيقية أو زائفة وهذا ممكن باستخدام مصدر زائف لمصدر IP بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر.

**ج- ارتفاع تكاليف جمع الأدلة:**

إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بالتكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا[2].

**ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها.**

المعوقات المتعلقة بالجريمة الإلكترونية تتمثل في:

---

[1] يوسف جفال، **التحقيق في الجريمة الإلكترونية**، 2016/2017، ص ص 41-42.

[2] يوسف جفال، **مرجع سابق**، ص ص 42-43.

- خفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه.
- الإعاقات المتعلقة بالوصول إلى الدليل لإحاطته بوسائل الحماية الفنية.
- سهولة محو الدليل أو تدميره في زمن فصير جدا.

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ نظام الحاسوب الآلي أو الشبكة أو في الأجهزة.

أما المعوقات المتعلقة بالجهات المتضررة من جرائم الحاسوب والانترنت، وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسؤولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالأنترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة وإذا تعلق الأمر بالمؤسسات المالية أو ما شابهها[1].

## المطلب الثاني: أجهزة التحقيق في الجريمة الإلكترونية.

نظرا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم الأخر ونظرا إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة الإلكترونية (المعلوماتية)، لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الإنتربول واليوروبول.

أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني.

[1] يوسف جفال، **مرجع سابق** ، ص ص 43-44.

## الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الإلكترونية.

الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الإلكتروني[1].

**أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.**

وقد استحدثها المشرع الجزائري بموجب قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015[2]، ومن مهامها تفعيل التعاون القضائي والأمني الدولي وغدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكاليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[3].

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

تنظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية.

---

[1] ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، جامعة باتنة، 2015-2016، ص 171.

[2] المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 53، في 08/10/2015

[3] فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، دراسة منشور بكتاب أعمال الملتقى الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017، طرابلس.

وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 100 جريمة إلكترونية منها 30% على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخصا متورطا في قضايا إرهاب الكتروني تمت إحالتهم على القضاء. هذا وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق، سوريا وليبيا كما تمكنت من فك شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجميده عبر مواقع الأنترنت ومنصات التواصل الاجتماعي خاصة الفيسبوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منتديات إرهابية غلى جانب اتصالات محلية ودولية[1].

**ثانيا: جهازي الأمن الوطني والدرك الوطني.**

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[2].

---

[1] آمال بن صوليح، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر**، مداخلة الملتقى الدولي حول " الإجرام اليبيرالي المفاهيم والتحديات "، 11-12 أفريل 2017.

[2] محمد السعيد زناتي، **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017، المركز الجامعي إليزي، الجزائر، ص 34-35.

**أ- الوحدات التابعة لسلك الأمن الوطني:**

تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[1].

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالآتي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لنقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن[2].

**ب- الوحدات التابعة للقيادة العامة للدرك الوطني:**

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

- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.

---

[1] د يوسف جفال، **التحقيق في الجريمة الإلكترونية**، 2016/2017، ص 20.

[2] سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر 2019، ص 53.

يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، 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 من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني[1].

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية حيث يوجد بهذا المركز قسم الإعلام الآلي والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية[2].

**الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.**

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون رقم 04-14 المؤرخ في a1 نوفمبر 2004[3]، وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم[4].

ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية: دعم حقوق الإنسان وتسهيل حق اللجوء غلى القضاء وإعادة الاعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة، ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع

[1] يوسف جفال، مرجع سابق، ص 21.

[2] سعيدة بوزنون، مرجع سابق، ص ص 53-54.

[3] القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004.

[4] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016، ص52.

من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايد في العلميات الإرهابية وتزايدا في أعمال المنظمات الإجرامية واستعمالها القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية[1].

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف[2].

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 35-4- المعدلة للمواد 3-4-5 من المرسوم السابق وجاء التقسيم كالتالي[3]:

محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، وبومرداس، البويرة، وعين الدفلى.

محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي باتنة بجاية، تيسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.

---

[1] محمد بوعمرة – سيد علي بنينال، مرجع سابق، ص35.

[2] كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 01-2015، ص 117.

[3] سعيدة يوزنون، مرجع سابق، ص 54

محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، وغرداية.

محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تسمسيلت، النعامة، عين تيموشنت، وغليزان.

بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنوبا، شرقا، وغربا، وذلك لدى أربع محاكم تسمي أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيه الجريمة الإلكترونية[1].

[1] سعيدة بوزنون، مرجع سابق، ص 55.

# الفصل الثاني:

# إجراءات التحقيق في الجرائم الإلكترونية

**مقدمة**

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت 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، فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الجزائي الإجرائي. وتزداد المشكلات الإجرائية في مجال الجرائم الالكترونية بتعلقها في العديد من الأحيان ببيانات المعالجة الآلية وكيانات منطقية غير مادية، ومن ثم يصعب الكشف عنها وإثباتها نظرا للسرعة الفائقة والدقة غير المتناهية في تنفيذها، ناهيك عن إمكانية محوها و تمويه آثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية.

ولقد امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي من القانون الجزائي بشكل أوسع مع مرور الوقت، لأن نصوص هذا القانون صيغت ووضعت التحكم الإجراءات المتعلقة بجرائم تقليدية، ترتكب في عالم محسوس وملموس يؤدي فيه السلوك المادي الدور الأكبر والأهم على خلاف الجريمة الالكترونية التي ترتكب في مسرح إلكتروني افتراضي وغير مادي يختلف كليا عن المسرح التقليدي.

## المبحث الأول محدودية سريان إجراءات التحقيق المألوفة على الجرائم الإلكترونية

ومما لا شك فيه، أن المشرع حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الالكترونية، فانه يقصد بها تلك الإجراءات التي تثير إشكالات وعقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش، الضبط، المعاينة والخبرة، والتي هي في حاجة إلى تطوير وتحيين لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها[1]. أما غيرها من الإجراءات كسماع المتهم أو الشهود، الاستجواب والمواجهة، فإنها مستبعدة نظرا لعدم وجود أية صعوبات في اتخاذها. استرشادا بذلك، فإننا سوف نركز على دراسة إجراءات التحقيق.

### المطلب الأول التفتيش في البيئة الإلكترونية

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق، المتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات[2]، إلا أنه يخول استثناء لرجال الضبطية القضائية في حالات محددة قانونا[3].

---

[1] محمد قدري حسن عبد الرحمن، مرجع سابق، ص 172.

[2] تتباين تشريعات الدول في تحديد السلطة المختصة بالتحقيق الابتدائي، ففي القوانين الإجرائية اللاتينية في مقدمتها القانون الإجرائي الفرنسي، نجد قاضي التحقيق هو سلطة التحقيق الأصلية و استثناء النيابة العامة. الشيء نفسه في القانون الإجرائي الجزائري، على عكس المشرع المصري الذي يخول تلك السلطة مبدئيا للنيابة العامة واستثناء لقاضي التحقيق. في حين نجد في التشريعات الانجلو سكسونية جهاز الضبطية القضائية هو وحده الذي يضطلع بمهمة التحقيق الابتدائي، كما هو الحال في القانون الانجليزي و الكندي، انظر في هذا الشأن:

– إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1995، ص 105.

[3] من بينها حالة التحقيق في جناية أو جنحة متلبس بها المنصوص عليها في المادة (41) من ق اج ج، وفي التحقيق الابتدائي المنصوص عليه في المواد (63) وما يليها من ق إ ج ج. أنظر أمر رقم (66–155) مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم.

وقد أجمع الفقه الجنائي، على أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا[1].

يتبين من هذا التعريف، أن التفتيش ما هو إلا وسيلة للإثبات المادي، غايته هي ضبط الأدلة المادية الخاص بالجريمة، مما يجعله يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت التي ليس لها أي مظهر مادي محسوس في العالم الخارجي، ومن هنا يثار التساؤل عن مدى جواز إخضاع هذه المكونات المعنوية لعملية التفتيش؟

وللإجابة عن هذا التساؤل، يقتضي الأمر منا الوقوف عند الضمانات والضوابط التي يجب على المحقق احترامها والتقيد بها قبل وأثناء قيامه بعملية التفتيش، منها ما يتعلق بمحل التفتيش وما هو إجرائي[2].

## الفرع الأول: محل التفتيش الإلكتروني

يقصد بمحل التفتيش، المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة[3].

ولما كان المستودع في الجرائم الالكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية (Hard Ware) كوحدات المعالجة المركزية (processeur)، وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم (Unité De Control)، ومكونات أخرى منطقية (Soft Ware) كبرامج النظام الأساسية، البرامج التطبيقية، والبيانات

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 192.

[2] براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون،كلية الحقوق، جامعة تيزي وزو، 2018 ص14.

[3] بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010، ص.ص 76-80.

المعالجة آليا، كما أن له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي والدولي[1]، فإن الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش.

**أولا : تفتيش المكونات المادية للحاسب**

ليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الالكترونية ومرتكبيها يخضع لإجراءات التفتيش المألوفة، الأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد فيه ما إذا كان عاما أو خاصا[2]. فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكمه، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاتها وبالإجراءات والضمانات المقررة قانونا في التشريعات المختلفة لذلك[3]. ففي القانون الجزائري مثلا تشترط المواد من (44إلى47) من قانون الإجراءات الجزائية للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها، الحصول مسبقا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار بهذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش[4]، على أن يتم التفتيش نهارا في الفترة الممتدة من الخامسة صباحا إلى الثامنة مساء وبحضور صاحب المسكن أو ممثله وإن تعذر ذلك استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته[5].

---

[1] على محمود على محمودة، **الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي**، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 الى 28 أفريل 2003، ص 135.

[2] عادل عبد الله خميس المعمري، **التفتيش في الجرائم المعلوماتية**، مجلة الفكر الشرطي، مجلد 22، عدد 86، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، 2013، ص 260.

[3] خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، دار الفكر الجامعي، إسكندرية، 2009، ص 195.

[4] تجدر الإشارة إلى أنه إذا تعلق الأمر بتفتيش المساكن في إطار التحقيق الابتدائي، فتشترط المادة (64) من ق.إ.ج قبل البدء في التفتيش، الحصول على رضا صريح ومكتوب بخط اليد من قبل صاحب المسكن، وإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.

[5] ونشير في هذا الشأن، أن المشرع الجزائري بعد التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 06/22 المؤرخ في 20 ديسمبر 2006 استغنى بموجب الفقرة الأخيرة من المادة (45) و كذا الفقرة الثانية من المادة (47) والفقرة الثالثة من المادة (64) عن تطبيق كل الضمانات المقررة لتفتيش المساكن عندما يتعلق الأمر بالتفتيش في الجرائم الالكترونية. بحيث أصبح من الممكن القيام بتفتيش مسكن المتهم في جريمة الكترونية في أي ساعة من الليل أو النهار ودون حاجة إلى رضائه ولا لحضوره أثناء التفتيش.

وينبغي التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة أم أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة يجب على المحقق مراعاة القيود و الضمانات التي يشترطها القانون التفتيش هذه الأماكن[1].

أما إذ كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء أكانت عامة بطبيعتها كالحدائق العامة والطرق العامة، أم أماكن عامة بالتخصيص كمقاهي الانترنت ومحلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن. ويستوي الأمر بالنسبة للمكونات الموجودة بحوزة شخص ما، فبغض النظر عن صفة هذا الشخص، مبرمجا كان أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات القانونية المحددة لذلك[2].

بناء على ما سبق، يتضح أن تفتيش المكونات المادية لجهاز الحاسب وملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، كمراعاة وقت التفتيش، الإذن بالتفتيش، الأشخاص القائمين بالتفتيش، والأشخاص المطلوب حضورهم عند التفتيش، مع مراعاة الاختصاص المكاني وعدم فض الأوراق المحرزة. كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الالكترونية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى[3].

---

[1] أحمد بن زايد جوهر الحسن المهدي، **تفتيش الحاسب الآلي وضمانات المتهم**، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق، جامعة القاهرة، 2009، ص ص 118-119.

[2] بوكر رشيدة، **جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن**، منشورات الحلبي الحقوقية، بيروت، 2012، ص 395.

[3] فايز محمد راجح غلاب، **الجرائم المعلوماتية في القانون الجزائري و اليمني**، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2011، ص 309.

**ثانيا: مدى صلاحية مكونات الحاسب المنطقية للتفتيش**

تعرف الكيانات المنطقية للحاسب بأنها "مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات"[1].

وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش، فان امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول مدى صلاحيتها لان تكون محلا للتفتيش تمهيدا لضبط الأدلة[2].

فالخلاف حاصل في مسألة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الالكترونية في نظم وبرامج الحاسب نوعا من التفتيش، باعتبار أن البيانات الالكترونية أو البرامج في حد 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[3].

وإزاء هذا التشكيك سعي جانب من الفقه إلى إزالته و تجنبه على نحو يسمح بتضمين التفتيش بمعناه التقليدي، البحث والتنقيب في نظم وبرامج الحواسب عن أدلة الجريمة الالكترونية[4]، وحجتهم في ذلك هي أنه وإن كانت هذه النظم والبرامج عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط و دعائم مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا إخضاعها لقواعد التفتيش التقليدية.

---

[1] عفيفي كمال عفيفي، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، دراسة مقارنة، طبعة ثانية، منشورات الحلبي القانونية، دمشق، 2007، ص 61.

[2] علي محمود علي حمودة، **مرجع سابق**، ص 81.

[3] يعرف الدليل المادي بأنه الدليل الذي ينبعث من عناصر مادية ناطقة بنفسها و يؤثر في اقتناع القاضي بطريقة مباشرة، أنظر :أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق جامعة عين الشمس، القاهرة ، ص 374.

[4] أبرز مثال على ذلك الفقه الكندي الذي وسع تفسير معنى التفتيش المنصوص عليه في المادة (487) من قانون العقوبات ليشمل تفتيش المكونات المنطقية للحاسوب، والشيء نفسه فيما يخص قانون إساءة استخدام الحاسوب الانجليزي العام 1990 ساري المفعول الذي نص على إمكانية تفتيش المكومات المادية و المعنوية للحاسوب. راجع: هلالي عبد الله، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي "دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 201.

وعلى النقيض من ذلك، يرى جانب آخر من الفقه بأنه من غير الممكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لان هذه القواعد وضعت في وقت لم تكن نظم المعالجة الآلية والحواسيب موجودة وتطبيقاتها غير معروفة، بالتالي فطبيعة هذه المكونات تتطلب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تتلاءم أحكامها مع متطلبات هذه التقنية الجديدة[1].

ويبدو أن غالبية تشريعات الدول المتقدمة تميل إلى هذا الاتجاه، وكان المشرع الأمريكي سباقا إلى ذلك حينما نظم بنصوص جديدة إجراء التفتيش والضبط في بيئة الحاسب الآلي في القسم 2000 من القانون الإجرائي الاتحادي الخاص بجرائم الحاسب[2].

ثم تلاه المشرع الانجليزي بنصه في قانون إساءة استخدام الحاسب الآلي لعام 1990 على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي، وتبعه المشرع الفرنسي الذي قام بتعديل نصوص التفتيش التقليدية لتواكب التكنولوجيات الحديثة، إذ أضاف بموجب المادة (42) من القانون رقم (545-2004) المتعلق بالثقة في الاقتصاد الرقمي عبارة "المعطيات المعلوماتية" مشيرا إلى المادة (94) من قانون الإجراءات الجزائية، لتصبح هذه المادة على النحو التالي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة[3].

ولم يبق المشرع الجزائري مكتوف الأيدي تجاه 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 المتصلة 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 هذا

---

[1] موسي مسعود أرحومة، **الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، بحث مقدم إلى المؤتمر المغاربي الأول حول "المعلومات والقانون" المنعقد بأكاديمية الدراسات العليا، طرابلس، في 29/10/2009-28، ص8.

[2] نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات**، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص226.

[3] FOURMENT F, procédure pénale- la perquisition du disque d'un ordinateur a chaud, CPU, Paris, 2002-2003, mise a jour de2004, P05.

القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية[1].

وفي هذا الصدد، نصت الاتفاقية الأوروبية حول الجرائم الالكترونية صراحة على حق الدول الأعضاء في تفتيش النظم المعلوماتية وحثتها على تجسيد هذا الحق بكل وضوح في قوانينها الإجرائية لتفادي أي إشكال يمكن أن يثار حول الموضوع، وذلك من خلال المادة (19/1) التي نصت على أن "لكل طرف الحق في سن من القوانين ما هو ضروري لتمكين السلطات المختصة من تفتيش أو الدخول إلى:

- نظام الحاسب أو جزء منه أو المعلومات المخزنة فيه.
- الوسائط التي يتم تخزين معلومات الحاسب بها ما دامت مخزنة في إقليمها[2].

## الفرع الثاني: ضمانات التفتيش في البيئة الإلكترونية

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد وحرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى. ويمكن تقسيم هذه الضمانات إلي ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:

**أولا: الضمانات الموضوعية للتفتيش الإلكتروني:** تتمثل هذه الضمانات في الشروط الواجب توفرها حتى يكون التفتيش صحيحا، وتتلخص في ثلاثة شروط أساسية هي: سبب التفتيش، محل التفتيش، والسلطة المختصة بالتفتيش[3].

**أ. سبب التفتيش:** يعتبر عنصر السبب ضمانة قانونية لصحة و مشروعية إجراء التفتيش، 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، عملا بمبدأ الشرعية الجزائية

---

[1] أنظر المادة (05) من القانون رقم (09/4) المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، جر عدد 47، صادر بتاريخ 25 شعبان 1430 الموافق ل 16 أوت 2009.

[2] راجع نص المادة (19/1) من الاتفاقية الأوروبية حول الجرائم المعلوماتية، مرجع سابق.

[3] براهيمي جمال، **مرجع سابق**، ص14.

القاضي بأن "لا جريمة ولا عقوبة إلا بالنص"[1]. إذ بدون وقوع جريمة، وتوجيه اتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية، يكون التفتيش باطلا لانتفاء السبب الذي يبرره.

وتطبيقا لما سبق، فان سبب التفتيش في الجرائم الالكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية:

**1- وقوع جريمة الكترونية تحمل وصف جناية أو جنحة**

اتفقت معظم تشريعات الدول على أنه لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية على أنها ستقع بالفعل يعد إجراء غير مشروع ماله البطلان[2].

ولا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة، بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة[3]، ويستثنى من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم من أجلها[4].

**2- اتهام شخص أو أكثر بمساهمته في ارتكاب الجريمة الإلكترونية**

يشترط لقيام سبب التفتيش إلى جانب وقوع جريمة الكترونية تحمل وصف جناية أو جنحة، أن تتوفر في حق الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو ثانويا، مما يستوجب اتهامه بها.

---

[1] وهو ما أقرته محكمة النقض المصرية باعتبارها أن "الإذن بالتفتيش لا يصح إصداره إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين وهناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية". طعن نقض جنائي، جلسة 16/10/1967 ، مجموعة أحكام النقض، س18 رقم 165، ص965. نقلا عن: خالد ممدوح إبراهيم، مرجع سابق، ص 209.

[2] نشير إلى أن المشرع الجزائري خرج عن هذه القاعدة من خلال المادة (05) من القانون (09/04) التي تجيز إمكانية اللجوء إلى تفتيش النظم المعلوماتية للوقاية من جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة (04) من القانون نفسه.

[3] وهذا تصديقا للمادة (66) من قانون الإجراءات الجزائية التي تنص على أن " التحقيق الابتدائي وجوبي في مواد الجنايات. أما في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة..."

[4] نبيلة هبة هروال، **مرجع سابق**، ص 232. وعادل عبد الله خميس المعمري، **مرجع سابق**، ص 263.

ومن هنا كان عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى ضد مجهول سببا لحفظ ملف القضية وإصداره لأمر بأن لا وجه للمتابعة[1].

وقد أجمع الفقه الجنائي على أن المقصود بالدلائل الكافية بصفة عامة هو " الشبهات المستمدة من الواقع والقرائن التي تنبئ عن اقتراف الشخص جريمة من الجرائم[2].

أما في الجرائم الالكترونية فيقصد بها مجموعة من المظاهر أو الإمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للمحقق والتي ترجح نسبة الجريمة الالكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا".

وعلى هذا الأساس فسبب التفتيش في البيئة الالكترونية لا يتوقف على وقوع جريمة من الجرائم الالكترونية فقط، إنما لابد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء[3].

**3- توافر إمارات قوية توحي إلى وجود أدلة مادية تفيد في كشف الجريمة**

لا يكفي وقوع جريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الالكترونية، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية و قرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو أية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة[4].

---

[1] هذا ما نصت عليه المادة (163) من قانون الإجراءات الجزائية الجزائري " إذا رأى قاضي التحقيق ...انه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة ما يزال مجهولا، اصدر أمرا بأن لا وجه لمتابعة المتهم".

[2] بوكر رشيدة ، **مرجع سابق**، ص 407.

[3] وهو ما يستشف من المادة 44 من قانون الإجراءات الجزائي الجزائري بنصها على أنه "لا يجوز لضباط الشرطة القضائية الانتقال الى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا..."

[4] هذا ما أقرته محكمة النقض المصرية في حكمها الصادر في الطعن رقم 25380-جلسة 20/01/2002 عندما قضت بان كل ما يشترط لصحة التفتيش الذي تجريه النيابة او تأذن بإجرائه في مسكن المتهم او ما يتصل بشخصه، هو أن يكون رجل الضبط القضائي قد علم من تحرياته واستدلالاته ان جريمة معينة قد وقعت من شخص معين و يكون هناك من الدلائل الإمارات الكافية و الشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحريته او الحرمة مسكنه في سبيل كشف اتصاله بتلك الجريمة" نقلا عن: أحمد بن زايد جوهر الحسن المهندي " تفتيش الحاسب الآلي وضمانات المتهم" رسالة لنيل درجة الماجستير، كلية الحقوق، جامعة القاهرة، 2009، ص165.

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

وينطبق على هذه الضمانة ما قيل في سابقتها بأنها لا تجدي في مجال الجرائم الالكترونية، بخلاف ما هي عليه في الجرائم التقليدية. لأن التوصل إلى قرائن أو إمارات قوية كسبب لقيام التفتيش في جريمة الكترونية ليس بالأمر الهين، نظرا للصعوبات الكثيرة والعقبات الجمة التي تواجه سلطات التحري والاستدلال في ذلك، كنقص خبرتها في تقنيات التحري في العالم الالكتروني الافتراضي، مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، تغيرها وإتلافها بكل سهولة وبسرعة فائقة[1]. وهو ما قد يشكل دافعا كافيا الانتفاء سبب التفتيش الذي يعتبر شرطا جوهريا لصحة إجراء التفتيش.

**ب. محل التفتيش:** يشترط كذلك لصحة ومشروعية التفتيش في الجرائم الالكترونية أن ينصب على محل، ويقصد بالمحل هنا كل المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الالكترونية[2].

وكما أسلفنا الذكر، فالمحل في الجرائم الالكترونية لا يكون قائما بذاته، بل يكون إما مقترنا بمكان معين كمسكن المتهم أو بشخص معين (مالك أو حائز) كما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك قبل مباشرة التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الالكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لان حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.

ويشترط في المحل الذي يقع عليه التفتيش، أن يكون معينا تعيينا نافيا للجهالة[3]، ويكون مما يجوز تفتيشه، فأما الشرط الأول، فهو نتيجة منطقية للمحافظة على حقوق وحرمات

---

[1] رشاد خالد عمر، **مرجع سابق**، ص 130.

[2] علي محمود علي حموده، **مرجع سابق**، ص94.

[3] وقد أكدت محكمة النقض المصرية هذا الشرط في حكمها الصادر في 22-5-1972 تحت رقم 177 ، وجاء فيه انه "يجب أن يكون محل التفتيش محددا تحديدا نافيا للجهالة، فيجب أن يتضمن الإذن بالتفتيش تحديد المسكن الذي يأمر بتفتيشه وكذلك المتهم الذي يقيم في هذا المسكن" مشار إليه في: سامي جلال فقي حسين "**التفتيش في الجرائم المعلوماتية**"دار الكتب القانونية، القاهرة، 2011، ص130.

وحريات الأفراد، لذا لا يمكن القيام بتفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة الواحدة[1].

وأما الشرط الثاني، فلأن القانون يستثني من التفتيش بعض الأشخاص و الأماكن مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية[2]، وكذا مكاتب المحامين لتمتعهم بالحصانة[3]، وعليه فأي تفتيش لأجهزة الحواسيب أو الوسائل الالكترونية الأخرى الموجودة بحوزة هذه الفئة من الأشخاص أو في منازلهم أو على متن سياراتهم يعد منافيا للقانون وماله البطلان.

كذلك الحال بالنسبة للتفتيش عن بعد عبر شبكات الاتصال أو التفتيش الالكتروني الذي لا يستلزم الاعتداء المادي لحرمة المكان أو الشخص المراد تفتيشه، فهو يخضع لقواعد الحصانة مثله مثل التفتيش المادي، لأن الاعتداء المعنوي على الحياة الخاصة يرتب عادة الآثار نفسها التي يرتبها الاعتداء المادي أو اخطر منها، وذلك نظرا للكم الهائل من المعلومات والبيانات التي تحويها الوسائل الالكترونية الشخصية، والتي يسهل الولوج إليها والإفشاء عنها والاعتداء على سريتها.

وتجدر الإشارة في هذا الشأن، إلى أن المشرع الجزائري استحدث نصوصا قانونية سمح من خلالها لسلطات التحقيق تفتيش الأنظمة المعلوماتية، أو جزء منها، والمعطيات المخزنة بتلك الأنظمة، وجعلها محلا للتفتيش الالكتروني، كما وسع نطاق هذا المحل، بحيث لم يعد قاصرا على تفتيش الأجهزة الالكترونية تبعا لتفتيش المكان والأشخاص، بل جعله يمتد ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى نهاية طرفية أخرى التي يمكن الدخول إليها من المنظومة الأولى وذلك كلما استدعت ضرورة التحقيق إلى ذلك[4].

---

[1] سامي جلال فقي حسين، **مرجع سابق**، ص 129.

[2] راجع في هذا الشأن المادتين (29 و 30) من اتفاقية فيينا للعلاقات الدبلوماسية لسنة 1961 وكذا المادة ( 126) من القانون رقم (16-01) مؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري الجزائري، ج.ر عدد 14، صادر في 7 مارس 2016 .

[3] راجع المادة (45) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[4] راجع المادة ( 05 ) من القانون رقم ( 09-04 المؤرخ في 05-08-2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

ج – السلطة المختصة بالتفتيش لكي يكون التفتيش في الجرائم الالكترونية أو غيرها من الجرائم صحيحا و منتجا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية[1] باختلاف تشريعات الدول[2]، مع مراعاة الاختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة، وإما بمكان إقامة المتهم، أو مكان القبض عليه[3].

إلا أنه استثناء، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية وذلك وفقا للشروط والإجراءات المنصوص عليها في القانون[4]، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناء على إذن بالتفتيش صحيح[5]، صادرا من هيئة مختصة. وفي غياب هذا الإذن، أو عدم صحته يصبح عدم مشروعية التفتيش أمرا مؤكدا[6].

وفي نطاق تفتيش الأجهزة الالكترونية يثار التساؤل حول ما إذا كان يجب تحديد محل التفتيش في الإذن بالتفتيش تحديدا دقيقا، كتحديد نوع الجهاز الالكتروني أو إحدى مكوناته (مثل الذاكرة، الوحدة المركزية، القرص الصلب...) أو ملحقاته (كالطباعة، جهاز المسح الضوئي scanner...) الذي سوف يرد عليه التفتيش دون غيره، أم أنه يكفي الحصول على الإذن بتفتيش المكان الذي تتواجد فيه تلك الأجهزة حتى يشملها جميعها؟ أو بعبارة أخرى هل يجوز لضابط الشرطة القضائية بمقتضي الإذن بتفتيش مسكن المتهم الولوج إلى الأجهزة الالكترونية

---

[1] يقصد بسلطات التحقيق الأصلية، السلطات القضائية التي تملك صلاحية مباشرة التحقيق بنفسها ( أي بقوة القانون) ولا تحتاج إلى تفويض من غيرها.

[2] ففي معظم الدول الأوروبية كفرنسا، ايطاليا مثلا السلطة المختصة أصلا بالتحقيق هو قاضي التحقيق، أما في مصر فهو النيابة العامة و قاضي التحقيق معا، في حين أن المملكة المتحدة تؤول هذا الاختصاص أصلا الى رجال الضبطية القضائية، أما في الجزائر فيؤول حسب المواد (38/1–2 و67/1) من ق إج إلى قاضي التحقيق بناءا على طلب من وكيل الجمهورية أو المدعي المدني . راجع : أحمد بن زايد جوهر الحسن المهدي، مرجع سابق، ص 172.

[3] تنص المادة (40) من ق إج ج " يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على احد هؤلاء الأشخاص حتى ولو كان سبب القبض قد حصل لسبب أخر.

[4] راجع المادة ( 68/6) والمواد من (138 إلى 142) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[5] كي يكون الإذن بالتفتيش صحيحا يجب أن يتوفر على الشروط التالية: أن يكون الإذن بالتفتيش مكتوبا وموقعا من طرف السلطة المختصة نوعيا و إقليما، ومسببا، ويحدد نوع الجريمة ومحل التفتيش، تاريخ القيام بالتفتيش ومدته ونطاقه. راجع: خالد ممدوح إبراهيم، **مرجع سابق**، ص ص 220–224.

[6] راجع نص المادة (44) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

التي تصادفهم فيه والتغلغل في منظومتها المعلوماتية للبحث عن أدلة إثبات يمكن أن تكون محل ضبط.

والجواب عن هذا السؤال هو أن غالبية التشريعات المقارنة استقرت على انه يكفي الحصول على الإذن بتفتيش مسكن المتهم حتى يكون لضباط السلطة القضائية الحق في تفتيش كل الأجهزة الالكترونية ومختلف ملحقاتها المتواجدة في هذا المسكن وكل الملفات والبيانات التي تحتويها تلك الأجهزة[1]، وحجتهم في ذلك هي، أن الأجهزة الالكترونية الرقمية بمختلف أنواعها تمثل مجالا حيويا ضخما لتخزين مئات الآلاف من الملفات ومليارات من المعلومات والبيانات، لذلك فلا يعقل مع هذه القدرة التخزينية الهائلة واللامتناهية تصور إصدار إذن بالتفتيش حسب عدد الملفات التي تحتويها.

أما عن موقف المشرع الجزائري إزاء هذه المسألة فهو غير واضح وغير حاسم، لأن بالعودة إلى القواعد الخاصة بالتفتيش المذكورة في قانون الإجراءات الجزائية فهي تتعلق بالتفتيش التقليدي الذي ينصب عادة على الفضاءات والمكونات المادية وما في حكمها كالمساكن وملحقاته[2]، أما في القواعد المتعلقة بالتفتيش الالكتروني الواردة في القانون رقم (09/04 )، فالمشرع لم يحسم أمره. وإنما اكتفي فقط بالإشارة إلى ضرورة قيام جهات التحقيق بإعلام السلطة القضائية المختصة مسبقا قبل تمديد التفتيش إلى منظومة معلوماتية أخرى مرتبطة بالجهاز المأذون بتفتيشه[3].

ومن خلال هذا السكوت وطبقا لمبدأ حرمة الخصوصية التي يحميها المشرع، نفهم بأن المشرع الجزائري يميل إلى عدم جواز الولوج إلى النظام المعلوماتي وما يمكن أن يحتويه من معلومات وبيانات سرية وخصوصية الأشخاص، لتفتيشه دون إذن خاص من السلطة القضائية المؤهلة، ومؤدى ذلك أن ضابط الشرطة القضائية يحتاج في الغالب لتفتيش منظومة معلوماتية

[1] على خلاف هذه التشريعات اتجه القضاء الأمريكي إلى أن كل ملف واحد في الحاسوب الآلي يعتبر حاوية مغلقة ويتطلب إذنا خاصا بالتفتيش، وأساسه في ذلك هو أن الحاسب يمكن أن يحتوي على ملفات تتعلق بالحياة الخاصة لصاحبه ولا علاقة لها بالجريمة، بالتالي فتح رجال الضبطية القضائية لهذه الملفات يعد تعد على الخصوصية. انظر مجموعة أحكام القضاء الأمريكي الصادرة في هذا الشأن في: عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، د.د.ن ، 2008، ص.ص 60-61.

[2] راجع المادة (44) وما يليها من القانون الإجراءات الجزائية الجزائري، مرجع سابق.

[3] انظر نص المادة (05) من القانون رقم (09-04)، مرجع سابق

إلى إذنين بالتفتيش، الأول يخص المسكن الذي يتواجد فيه الجهاز الالكتروني، والثاني يتعلق بتفتيش مكونات الجهاز أو المنظومة المعلوماتية في حد ذاتها. أو على الأقل يحتاج إلى إذن واحد يسمح بتفتيش الجهاز الالكتروني الخاص بالمتهم ومسكنه معا.

وعلى ضوء هذا الإبهام، يتعين على المشرع الجزائي الجزائري التدخل وسن نصوص قانونية واضحة تفصل في هذه المسالة، والحل في رأينا هو الأخذ بما ذهبت إليه معظم تشريعات الدول المتقدمة، والمتمثل في جواز تفتيش مسكن المتهم وكل الأجهزة الإلكترونية بمكوناتها وملحقاتها وملفاتها المتواجدة فيه، مع إمكانية تمديد التفتيش عن بعد على جناح السرعة إلى أية منظومة معلوماتية أخرى مرتبطة بها، كل ذلك بموجب إذن بتفتيش واحد.

**ثانيا- الضمانات الشكلية للتفتيش الإلكتروني**

إن الغرض من إحاطة التفتيش بضمانات شكلية إلى جانب الضمانات الموضوعية هو ليس تحقيق مصلحة القضاء في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة، وضمان مشروعية هذه الأخيرة فقط، إنما تعتبر كذلك بمثابة سياج أمني لحماية الحقوق والحريات العامة الفردية .

ومع هذا فتطبيق تلك الضمانات في مجال التفتيش الالكتروني من شأنها أن تتحول إلى عقبات تحول دون تحقيق الهدف من إجراء التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي. وهو ما سوف نبرزه عند دراسة هذه الضمانات التي تتلخص فيما يلي:

**1-احترام الميقات الزمني لإجراء التفتيش**

إن فرض قيود زمنية لإجراء التفتيش يعد ضمانة إجرائية مهمة جدا لحماية الحريات والحقوق العامة للأفراد من أي اعتداء.

ومع ذلك اختلفت التشريعات الإجرائية للدول في تنظيمها للوقت الذي يسمح فيه القيام بالتفتيش، فمنها من حددته بشكل عام على أن يتم التفتيش في النهار فقط، مثل قانون الإجراءات الجنائية القطرية[1]، ومنها من حددت وقت التفتيش بشيء من التفصيل من خلال تحديد الساعة التي يمكن البدء فيها بالتفتيش والساعة التي يجب التوقف عندها من ساعات النهار[2]، ومنها

[1] نصت المادة (53) منه على انه "لا يجوز أن يجري تفتيش المساكن إلا نهارا..." نقلا عن سامي جلال فقي حسين، مرجع سابق، ص 165.

[2] حدد قانون الإجراءات الجنائي الاتحادي الأمريكي في المادة (228) وقت التفتيش بالفترة المحصورة بين الساعة السادسة صباحا و العاشرة مساءا، و حدده قانوني الإجراءات الجنائية الفرنسي في المادة (59) بالفترة الممتدة بين السادسة صباحا و

كذلك من لم يقيد القيام بهذا الإجراء بوقت معين وترك الأمر لتقدير القائم بالتفتيش لاختيار الوقت الملائم من الليل أو النهار لتنفيذه ضمن المدة المحددة بالإذن مثل قانون الإجراءات الجنائية المصري، القانون العراقي والقانون الأردني.

وعلى خلاف ذلك كله، نجد أن المشرع الجزائري وضع قيودا زمنية على تفتيش المنازل وما في حكمها، ولم يسمح به بمقتضى المادة (47) من قانون الإجراءات الجزائية إلا في الوقت المحصور بين الساعة الخامسة صباحا والثامنة مساء[1]، وفي الوقت نفسه أقر حالات استثنائية أجاز فيها الخروج عن هذا الميقات ليصح إجراء التفتيش في أية ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها في المواد من (342) إلى(348) من قانون العقوبات المرتكبة في أماكن معينة، وفي حالة الرضي الصريح لصاحب المسكن[2].

وقد اشتمل هذا الاستثناء التفتيش في الجرائم الالكترونية، بحيث استغنى المشرع الجزائري نهائيا عن شرط الميقات الزمني وسمح لرجال الضبطية القضائية بإجراء التفتيش في مثل هذه الجرائم في كل ساعة من ساعات الليل والنهار كما جاء في الفقرة الثالثة من نص المادة (47) ق إ ج " ... **عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بالمعالجة الآلية للمعطيات و ...فانه يجوز إجراء التفتيش... في كل محل سكني او غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية**".

**2- إجراء التفتيش بحضور المتهم أو من ينوب عنه**

حرصا على تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، تسهر 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.

---

التاسعة مساءا، في حين لا يسمح القانون الكرواتي بالتفتيش إلا في الفترة المحصورة بين السابعة صباحا والتاسعة مساءا. نقلا عن: هلالي عبد الله احمد، مرجع سابق، ص 175.

[1] تنص المادة (47) ق آج ج على أنه "لا يجوز البدء في تفتيش المساكن او معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا..."

[2] أنظر المادتين (47/1و 2) و (82) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

وغني عن البيان أن الشخص الذي يستوجب القانون حضوره في الأصل هو المتهم، وهذا الشرط يكون قائما حتما في تفتيش الأشخاص على اعتبار التفتيش يقع عليه[1]، وفي هذا الإطار لم تشترط التشريعات الإجرائية حضور الشهود عند تفتيشه. أما عندما يتعلق الأمر بتفتيش المساكن وما في حكمها، فقد تباين موقف التشريعات الإجرائية بين من يشترط الصحة التفتيش حضور إما المتهم بنفسه أو من يمثله أو شاهدين من غير المعنيين بالتحقيق[2]، وبين من يستوجب إلى جانب حضور المتهم حضور شاهدي عدل[3]، كما هو الحال في قانون الإجراءات الجنائية اليمني الذي نص في المادة (134) على أن "يحصل التفتيش بحضور المتهم أو من ينوبه وبحضور شاهدين من أقاربه أو جيرانه"[4].

وعلى العكس من ذلك، فالمشرع الجزائري يقضي لإجراء التفتيش بحضور المشتبه به أو من يمثله ولم يتطلب حضور الشهود إلا في حالة تعذر حضور هؤلاء، وهو مقتضي المادة (45/1 ق إ ج) بأنه " إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فان ضابط الشرطة القضائية ملزم بان يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته"[5].

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 نفسها[6]، واستثنى هذه الجرائم من

---

[1] بوكر رشيدة، **مرجع سابق**، ص 414.

[2] وهو الموقف الذي تبناه كل من المشرع الفرنسي في المادة (57) من قانون الإجراءات الجنائية، و المشرع المصري في المادة (51) قانون الإجراءات الجنائية ، مشار إليه في: فايز محمد راجح غلاب، مرجع سابق، ص 335.

[3] ومن التشريعات التي أخذت بهذا الموقف نذكر قانون الإجراءات الجنائي الاتحادي الأمريكي، قانون الإجراءات الجنائية الايطالي في المادة (250/10) منه، انظر: سامي جلال فقي حسين، مرجع سابق، ص ص 168-169.

[4] المادة (134) من قانون الإجراءات الجزائية اليمني رقم 13 لسنة 1994 .

[5] انظر المادة (45) والمادة (83) من القانون الإجراءات الجزائية الجزائري، مرجع سابق.

[6] تنص الفقرة الأخيرة من المادة (45 من ق إج ج) على أنه " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...باستثناء الأحكام المتعلقة بالحفاظ على السر المهني".

تطبيق أحكام المادة السابقة، وأصبح بإمكان الضبطية القضائية إجراء التفتيش في الجرائم المعالجة الآلية دون التقيد بشرط حضور المتهم أو من ينوب عنه أو حتى الشهود.

وفي رأينا، ما فعله المشرع الجزائري باستبعاد تطبيق أحكام المادة (45 ق ا ج) على الجرائم الالكترونية هو الصواب، وذلك نظرا للطبيعة التقنية المحضة التي تتميز بها هذه الجرائم وطبيعة الدليل الذي تتطلبه لإثباتها، وما يقتضيه من السرعة في استخلاصه قبل فقدانه والذي يتطلب أحيانا عدم إعلام المتهم بعملية التفتيش.

**3- تحرير محضر التفتيش**

إضافة إلى الضمانات المتعلقة بالميقات الزمني للتفتيش والأشخاص المطلوب حضورهم، يشترط كذلك أن يحرر محضر بالتفتيش تدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش، وما أسفر عنها من أدلة لكي يكون حجة على الجميع.

ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية، تاريخ تحريره، توقيع محرره، ويتضمن كافة إجراءات التفتيش[1].

ومن الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش، وجوب استعانة المحقق بكاتب يتم اصطحابه لتحرير المحضر وتدوين ما تم من إجراءات والتأشير عليه تحت طائلة البطلان، وهو ما نصت عليه المادة (68/2) قانون الإجراءات الجزائية الجزائري "وتحرر نسخة من هذه الإجراءات وجميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"، وأكدت عليه المادة (79) من القانون نفسه بنصها على " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من **إجراءات**[2].

ولا يختلف محضر التفتيش في مجال الجرائم الالكترونية عن غيره في الجرائم التقليدية سوى أنه بالإضافة إلى الشكليات السابقة لابد من إحاطة القائم بالتفتيش في الجرائم الالكترونية

[1] فايز محمد راجح غلاب، **مرجع سابق**، ص 338.

[2] أنظر الفقرة 2 من المادة (68) و المادة (79 من ق.ا. ج. ج)، مرجع سابق.

بتقنية المعلوماتية الرقمية، أو استعانته بأهل الخبر الفنية والاختصاص في هذا المجال ليساعده في صياغة وتحرير محضر يغطي كل الجوانب الفنية للتفتيش.

وأشير إلى أنه بالإضافة إلى شرط تحرير محضر التفتيش، حرصت معظم الدول على تضمين تشريعاتها الإجرائية نصوص تمنع فيها الاطلاع أثناء التفتيش على الأشياء والأوراق المختومة التي تمس الأسرار الشخصية للعائلة[1]، وتفرض على القائم بالتفتيش اتخاذ الاحتياطات الضرورية لتفادي انكشاف مثل هذه الأسرار.

وقد نص القانون الجزائري على هذه الضمانة في المادة (84 من ق إ ج) على الشكل التالي: "إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق وما توجبه المادة (83/3 ق إ ج). ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة. ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا ...[2].

## المطلب الثاني ضبط الأدلة في الجرائم الإلكترونية

يعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها وعن مرتكبيها، ووضعها في أحراز مختومة ولتقدم إلى الجهة القضائية المختصة كدليل إثبات[3].

وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، الأقراص والأشرطة الممغنطة، الطباعة، البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي

[1] من بين التشريعات التي نصت على هذه الضمانة، نذكر نص الماد (52 من قاج) المصري، و نص المادة (140 ق إج) اليمني، والمادة (35/1) من قانون أصول المحاكمات الجزائية السوري.

[2] أنظر المادتين (83/3 و 84 ) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[3] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة للنشر و التوزيع، عمان، 2011، ص 170.

هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية[1].

وقد يرتبط الدليل الالكتروني بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيرا حول مدى إمكانية ضبطها وفقا القواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية[2].

ولقد حسمت الاتفاقية الأوروبية لجرائم المعلوماتية لعام 2001 هذه المسألة، بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الالكترونية لأن تكون محلا للضبط وذلك من خلال الفقرة (03) من المادة (19) التي نصت على "... 3- يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئاتها المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين (01) و (02)... ".

فبالرجوع إلى هذه الفقرة، نجدها تخول سلطات البحث والتحري طريقتين لضبط البيانات المعلوماتية والأدلة الرقمية التي كانت موضوع التفتيش أو الولوج بطريقة مشابهة عملا بالفقرتين (1 و2) من المادة (19)، تتحقق الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية (كالأقراص الممغنطة، بطاقات الذاكرة، فلاش ديسك)، وتكون هذه الأخيرة قابلة للضبط والوضع في أحراز مختومة حسب ما هو مقرر في قواعد تحريز الدليل التقليدية المنصوص عليها في قوانين الإجراءات الجزائية، وهي الطريقة المقصودة في المادة أعلاه بمصطلح " الضبط saisir"[3]. أما الطريقة الثانية فتتضمن تدابير جديدة مستحدثة خصيصا لضبط الأدلة الجنائية الرقمية، وهي المعبر عنها في هذه المادة

---

[1] راجع في ذلك المواد (45 و 46 و 84 ) من القانون الإجراءات الجزائية الجزائري.

[2] أنقسم الفقه في هذه المسألة بين من يعترف بالطبيعة المادية للأدلة الالكترونية و بالتالي إمكانية إخضاعها إلى إجراءات الضبط التقليدية، و بين من يرى هذه الأدلة ذات طبيعة لا مادية ولها خصوصيات استثنائية تستلزم تقنيات الضبط و تحليل جديدة ومتطورة تختلف عن التقنيات المألوفة. للمزيد من التفاصيل أنظر: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص ص218 .

[3] هلال عبد الله أحمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها**، دار النهضة العربية، القاهرة، 2011، ص251.

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 اجل منع الأشخاص المرخص لهم باستخدام المنظومة المعلوماتية والوصول إلى المعطيات والبيانات الأصلية التي تحتويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات والبيانات وفق الطريق الأول[1].

أما إذا كانت هذه المعطيات والبيانات تتضمن خطرا على النظام العام و الآداب العامة كتحريض الأطفال على الشذوذ الجنسي أو التحريض على التمييز العنصري أو على الإرهاب، أو أنها تحتوي على برامج وفيروسات، ففي هذه الحالة يمكن السلطات التحقيق القيام بتعطيل تشغيل هذه المعطيات (blocage des données) أو محوها بعد أخذ نسخة منها[2].

فضلا عن الإجراءات الاستثنائية التي أقرتها الاتفاقية المذكورة لضبط الأدلة الالكترونية الرقمية، فقد نصت كذلك في ( المادة19/3) على مجموعة من التدابير الخاصة لضمان تحريز هذه الأدلة ذات الطبيعة الخاصة وحمايتها فنيا وصيانتها من أي تغيير أو إتلاف أو عبث يمكن أن يصيبها والتي نلخصها فيما يلي[3]:

– استخراج نسخ احتياطية من دعائم البيانات و المعطيات المضبوطة والعمل عليها لتفادي المساس بالدليل الأصلي.

– عدم طوي القرص لتفادي تلفه وتحطمه وفقدان المعلومات المسجلة فيه.

– تأمين البرامج المعلوماتية المضبوطة فنيا قبل تشغيلها.

– مراعاة ظروف الحرارة والرطوبة المناسبة في أماكن تخزين الأقراص والأشرطة الممغنطة المحرزة، والتي يجب أن تتراوح درجة الحرارة فيها بين (4–32 درجة) وتكون درجة الرطوبة فيها ما بين ( 20 – 80%)، مع تفادي تعريضها للأضواء أو لأي سائل من

---

[1] أنظر: تقرير لجنة منع الجريمة والعدالة الجنائية " دراسة شاملة عن مشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها " الجمعية العامة لمنظمة الأمم المتحدة، من 25 إلى 28 فيفري 2013، ص 12.

[2] ROGGEN François et DE VALKENEEK Christian, Actualité de droit pénal, bruyant, Bruxelles , 2005, p128.

[3] براهيمي جمال، **مرجع سابق**، ص47.

السوائل، مع العلم أنه في مثل هذه الظروف يمكن أن تصل مدة صلاحية تخزين هذه الأقراص إلى ثلاث سنوات دون أن يصيبها تلف أو تعديل أو تحول[1].

– منع الأشخاص غير المرخص لهم من الوصول إلى المعطيات والبيانات التي تم ضبطها داخل دعامة مادية للتخزين ، من خلال إحاطتها بتدابير الحماية الفنية كالترميز والتشفير أو بأية وسيلة الكترونية أخرى تمنع الدخول إليها، و صيانتها ببرامج منع التحريف والتغيير في البيانات مثل برامج منع الكتابة[2].

وفي هذا الصدد، أضافت الهيئة الدولية لدليل الحاسب الآلي ( Organisation on international computer évidence) ضوابط أخرى للتحريز الجيد والمحافظة على الدليل الرقمي، منها مراعاة عدم تسبب إجراءات التحريز في تغيير طبيعة الدليل الرقمي المضبوط، وتوثيق كل المراحل المتعلقة بتحريز هاته الأدلة الرقمية والدخول إليها ونقلها توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة[3].

إلى جانب الإجراءات الجديدة التي تبنتها المادة (19) سالفة الذكر بخصوص ضبط الأدلة الجنائية في الجرائم الإلكترونية من خلال الفقرات (1، 2، 3)، تضمنت كذلك النص على بعض الإجراءات المسهلة والمساعدة لعملية الضبط من خلال الفقرة (4)، ولم تقتصر على وضع تلك الإجراءات فقط، بل أحاطتها بضمانات كافية تضمنتها الفقرة (5) أيضا[4].

فأما عن التدابير التي تضمنتها الفقرة (4) من المادة (19)، فتتمثل في منح السلطات المخولة بإجراء التفتيش والضبط صلاحيات الاستعانة بأي شخص لديه خبرة ومعرفة فنية في

---

[1] حسام محمد نبيل الشنراقي، **الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني**، دار الكتب القانونية، القاهرة، 2013، ص 525.

[2] انظر الفقرة الثالثة من المادة (19) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001، مرجع سابق.

[3] FIRAL-SCHUHL Christiane, cyber droit- le droit a l'épreuve de l'internet , 6ém édition Dalloz , Paris, 2011-2012, P 998.

[4] تنص الفقرتين (4) و(5) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001 على ما يلي:

4- chaque partie adopte des mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes a ordonner a toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatique qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visée par les paragraphes 1 et 2. 5- les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15

تشغيل المنظومة المعلوماتية محل البحث و الإجراءات المطبقة من أجل حماية البيانات والمعطيات التي تتضمنها هذه المنظومة، وإلزامه بالتعاون معها بتقديم المساعدة اللازمة والضرورية لتسهيل عملية تفتيش وضبط هذه البيانات والمعطيات، وجعلهما أكثر فعالية واقل تكلفة[1].

بشرط أن تقتصر هذه المساعدة على تقديم المعلومات الضرورية فحسب دون الإخلال بحرمة الحياة الخاصة للإفراد ولا تتعارض مع قواعد السر المهني.

وأما الفقرة (5) من المادة نفسها، فقد ألزمت سلطات التحقيق أثناء قيامها بعملية التفتيش والضبط أو أي إجراء آخر مما نصت عليه الاتفاقية، مراعاة الضمانات المنصوص عليها في المادتين (14 و15) من الاتفاقية والمتمثلة بشكل عام في احترام حقوق الإنسان والحريات الفردية، مراعاة خصوصية الأشخاص وحرمة أسرارهم والمدة القانونية المقررة لكل إجراء[2].

اقتداء بالاتفاقية الأوروبية حول الجرائم المعلوماتية، تدخلت عدة دول لتعديل قوانينها واستكمال ما بها من فراغ تشريعي في مجال ضبط الأدلة الالكترونية الرقمية وقواعد تحريزها[3]، في مقدمتها فرنسا التي قامت بتعديل قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي رقم (239) لسنة 2003، واستحدثت الفقرة (03) من المادة (57-1) التي نص فيها على أن " المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في هذه المادة ، يتعين نسخها على أية دعامات التخزين المعلوماتية، والتي ينبغي تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون[4].

---

[1] جميل عبد الباقي الصغير، **أدلة الإثبات الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية، القاهرة، 2002، ص 107. وهلال عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، مرجع سابق، ص 252.

[2] أنظر نص المادتين (14 و 15) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001، مرجع سابق.

[3] من بين هذه الدول التي استحدثت قواعد خاصة بضبط الأدلة الالكترونية، دولة بلجيكا من خلال الفقرات من (1 الى 6) من المادة (39) مكرر و المادة (88) من قانون التحقيق الجنائي البلجيكي، دولة اليونان من خلال المادة (251) من قانون الإجراءات الجنائية، ودولة كندا من خلال المادة (487) من القانون الجنائي الكندي. انظر: أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، أطروحة لنيل درجة دكتورة في القانون، كلية الحقوق بجامعة عين الشمس، القاهرة، 2012، ص.ص 19- 20.

[4] Art (57-1-3) du CPCP dispose que « les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent êtres copiées sur tout supports. Les supports de stockage informatique peuvent etre saisis et placés sous scellés dans les conditions prévues par le présent code >>

أما فيما يخص قواعد تحريز المضبوطات المعلوماتية وتأمينها فنيا فقد قام المشرع الفرنسي بتعزيزها من خلال المواد (41 إلى 43) من قانون الثقة في الاقتصاد الرقمي الصادر في 21 جوان 2004 وجعلها تتطابق مع تلك المذكورة في الاتفاقية الأوروبية حول الجرائم المعلوماتية1.

وعلى غرار المشرع الفرنسي تنبه المشرع الجزائري بدوره لهذا القصور، وتبني في القانون رقم (09/4) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 05/08/2009، إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها اللامادية، تحت عنوان "حجز المعطيات المعلوماتية[2] وخصص لها عددا من المواد التي نذكرها على النحو التالي:

– نصت المادة (06) على أنه "عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات محزنة مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية..."

– أضافت المادة (07) فيما يخص الحجز عن طريق منع الوصول إلى المعطيات بأنه " إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

---

[1] voir Arts( 41-42-43)de la loi pour la confiance dans 1 économie numérique in: QUEMENER Myriam - CHARPENEI Yves «cybercriminalité droit pénal appliqué >> édition Economica, Paris, 2010, p178.

[2] تجدر الإشارة إلى أن المشرع الجزائري استعمل في هذا القانون (09-04) عبارة " الحجز saisie" للتعبير عن عملية الضبط كإجراء من إجراءات التحقيق بدلا من عبارة " الضبط saisie" التي اعتاد على استعمالها في قانون الإجراءات الجزائية، وفي اعتقادي هذا الاختيار أمر مقصود، لان عبارة " الحجز" لا تتعارض مع الضبط المادي التقليدي من جهة، وهي أكثر تلاؤما و تماشيا مع الطبيعة المنطقية واللامادية للأدلة الالكترونية و الرقمية من جهة أخرى.

– أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت الماد (08) على أنه " يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك"[1].

بالإضافة إلى هذه التدابير، وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت جملة من الالتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش والضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحقيق[2]. سيتم تناولها بشيء من التفصيل في موضع آخر من هذه الأطروحة .

ويتضح من خلال النصوص السابقة، بأن المشرع الجزائري أدرك خطورة الجرائم الالكترونية وأن الجزائر ليست بمنأى عنها، فقام بتلافي القصور الموجود في قانون الإجراءات الجنائية فيما يخص ضبط الكيانات المنطقية للحاسب أسوة بالاتفاقية الأوروبية وتشريعات الدول المتقدمة، واعتقد أن موقفه هذا ليس اختيارا بل حتمية لا مفر منها ما دام أنه قد أجاز تفتيش هذه الكيانات كما – رأينا سابقا – وهو ما يقتضي بحكم المنطق القانوني والعقلي ضرورة إباحة ضبطها لأن الغاية من التفتيش هو ضبط كل ما يفيد في كشف الحقيقة، بالتالي لا يعقل أن ينظم المشرع مرحلة من مراحل التحقيق ويغفل عن الأخرى.

والجدير بالذكر، أنه رغم محاولة استحداث قواعد وإجراءات جديدة تواكب الطبيعة الخاصة للأدلة المستمدة من البيئة الرقمية والالكترونية وتسمح بضبطها وتحريزها بشكل سليم، إلا أن الواقع يثبت وجود صعوبات كثير ما زالت تواجه عملية ضبط هذه الأدلة ولعل أهمها ما يلي:

– الحجم الهائل للمعلومات المعالجة الكترونية التي تحتويها الشبكة المعلوماتية الواجب فحصها من طرف المحقق للوصول إلى استخلاص البيانات التي تصلح كأدلة جنائية وضبطها[3].

---

[1] أنظر المواد ( 6، 7، 8) من القانون (09/04 ) المؤرخ في 05/08/2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] أنظر في هذا الشأن، أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09–04، مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح بجامعة ورقلة، 2013، ص103.

[3] حسام محمد نبيل الشنراقي، مرجع سابق، ص. ص 671–672.

– قد يكون محل الأدلة الالكترونية جزء لا يمكن عزله عن المنظومة أو الشبكة المعلوماتية، مما يتعين بالضرورة ضبط النظام أو الشبكة بأكملها لتحصيل الدليل، وهو الأمر الذي يترتب عنه التوقف عن العمل المشروعات صاحب النظام مدة زمنية قد تطول أو تقصر، ففي هذه الحالة يضطر المحقق إعمال مبدأ التناسب الذي يقضي باقتصار الضبط على الأدلة الضرورية التي تفيد كشف الحقيقة ولها علاقة بالجريمة[1].

– كما قد تكون هذه الأدلة في شبكات أو أجهزة تابعة لدولة أجنبية، مما يعيق أجهزة التحقيق الوطنية من الوصول إليها وضبطها دون تعاون ومساعدة أجهزة التحقيق التابعة لتلك الدولة[2].

– كما أن الضبط في البيئة الالكترونية، قد يشكل أحيانا اعتداء على الحقوق والحريات الفردية، ويتصادم مع حرمة الحياة الخاصة والسر المهني خاصة عند عدم مراعاة الضمانات المقررة لذلك، مما قد يعرضه للبطلان[3].

– أضف إلى ذلك، فمن المشكلات التي يمكن أن تثار بمناسبة ضبط البيانات المخزنة في نظام جهاز الحاسب أو شبكة المعلومات مشكلة مدى قبول القاضي النسخة المأخوذة عن تلك البيانات في حالة صعوبة ضبط النسخة الأصلة كدليل إثبات، لأن القضاء في عدة دول خاصة الدول الأجلوسكسونية يشكك في حجيتها ولا يعتبرها كالنسخة الأصلية لاحتمال التلاعب[4].

– ومن الصعوبات التي تعيق الوصول إلى ضبط الدليل الرقمي كذلك، تلك الأحزمة الأمنية المفروضة من طرف مستخدم النظام للحد من الدخول والاطلاع على البيانات التي يحتويها هذا النظام. وما يزيد الأمر تأزما هو عدم معرفة المحقق الجنائي لكلمات السر أو شفرات المرور أو

---

[1] وفي هذا الشأن قضت المحكمة الفيدرالية الألمانية بإلغاء محضر الضبط الذي ورد على 220 قرص صلب بالإضافة إلى الوحدة المركزية للحاسب الآلي بحجة مخالفة سلطة التحقيق لمبدأ التناسب. نقلا عن: فايز محمد راجح غلاب، مرجع سابق، ص 345.

[2] أحمد بن زايد جوهر الحسن المهندي، **مرجع سابق**، ص 224.

[3] EL CHAER Nidal « la criminalité informatique devant la justice pénal » thèse de doctorat en droit, faculté de droit de l'université Poitiers, 2003, p 231.

[4] أثارت محكمة النقض الفرنسية هذه المسألة في أحد قراراتها و اعتبرت ضبط نسخة من البيانات المسجلة في الحاسب الآلي دون ضبط الجهاز نفسه بما فيه الذاكرة التي تحتوي تلك المعلومات لا يعد من قبيل الضبط الصحيح بمفهوم المادتين (76 و 97) من قانون الإجراءات الجنائية. انظر: عمر محمد أبو بكر بن يوسف، الجرائم الناشئة عن استخدام الانترنت – الأحكام الموضوعية و الجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004، ص.ص872–873.

شفرات ترميز البيانات وما يقابله من حق المشتبه به في الصمت وعدم الكشف عن هذه الشفرات تطبيقا لمبدأ عدم اتهام الشخص لنفسه[1].

## المبحث الثاني استحداث إجراءات تحقيق خاصة بالجرائم الإلكترونية

إذا كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها بظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية، فإنها في المقابل أثرت على وسائل إثبات هذه الجرائم، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الإجرامي المستجد الذي يحتاج إلى طرق وتقنية جديدة تتناسب مع طبيعته، ويمكنها فك رموزه وترجمة نبضاته وذبذباته الى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة[2].

### المطلب الأول التسرب الإلكتروني

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الالكترونية[3]، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية سباقة إلى احتواء هذا الإجراء بنصها في المادة (20) على أساليب التحري الخاصة بما فيه التسرب الذي عبرت عنه ب" الأعمال المستترة". أما المشرع الجزائري فقد تبني بدوره هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم (05/02) المؤرخ في02/02/2002 بتحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19.

وقد ورد النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون رقم (06/01 ) المتعلق بالوقاية من الفساد ومكافحته في عام 2006، الذي نص في الماد (56) على أنه" **من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن**

---

[1] نص المشرع الجزائري على حق المشتبه به في الصمت وعدم الإدلاء بأي إقرار أثناء التحقيق في المادة (100) من قانون الإجراءات الجزائية، انظر في هذا الشأن أيضا : لجنة منع الجريمة والعدالة الجنائية، مرجع سابق، ص 13.

[2] براهيمي جمال، **مرجع سابق**، ص81.

[3] نظم المشرع الفرنسي عملية التسريب "Infiltration" في المواد (694/ 07، 9/694، 81/706 ، 87/706 من القانون رقم ( 2004/207 ) المؤرخ 09/03/2004 المتضمن قانون الإجراءات الجزائية، المعدل و المتمم

**اللجوء إلى التسليم المراقب وإتباع أساليب تحري خاصة كالترصد الإلكتروني أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة"[1].**

ولكن نظرا للغموض الذي انتاب هذا النص بخصوص المقصود بالاختراق أو التسرب شروطه وآليات مباشرته، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون (06/ 22) المؤرخ في 20/12/2006، أين تم تحديد معالم إجراء التسرب من خلال تعريفه و تحديد ضوابطه والآثار المترتبة عنه. وهي النقاط التي سوف ندرسها بشيء من التفصيل من خلال الفرعين التاليين:

**الفرع الأول: المقصود بالتسرب**

تعرف المادة (65 مكرر12) من القانون الإجراءات الجزائية الجزائري التسرب على أنه: "**قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك[2].**

انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية[3]، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية. لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب[4].

---

[1] أنظر نص المادة (56) من القانون رقم (06-01) مؤرخ في 20/02/2006 ، يتعلق بالوقاية من الفساد ومكافحته، ج رج ج عدد 14، صادر بتاريخ 08-03-2006.

[2] هو التعريف الذي تبناه المشرع الفرنسي في المادة 706-81 من قانون الإجراءات الجزائية التي تنص:

« ...un officier ou un agent de police judicaire spécialement habilité, et agissant sous la officier de police judicaire charger de cordonner l'opération responsabilité d'un peut...surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs co-auteurs, complices ou receleurs >> voir la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF 16 nov 2001.

[3] أنظر المادة (65 مكرر14) من القانون الإجراءات الجزائية.

[4] أنظر المادة (65 مكرر14) فقرتها الأخيرة من القانون الإجراءات الجزائية.

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة (65 مكرر16) من قانون الإجراءات الجزائية بأنه "**لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء** "[1].

وما تضمنته كذلك المادة (65 مكرر17) من القانون نفسه بأنه " **إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة (65 مكرر 14) أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر**" .

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة (65 مكرر) وهي: جرائم المخدرات، الجريمة المنظمة، جرائم تبييض الأموال و الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2].

ويمكن تصور عملية التسرب في الجرائم الالكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعات أو نوادي الهاكر، مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا فيها بمظهر طبيعي كما لو كان واحد مثلهم قصد استدراجهم والكشف عنهم وعن أعمالهم الإجرامية.

## الفرع الثاني: الضوابط التي تحكم التسرب في الجرائم الإلكترونية

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

---

[1] وقد فرض المشرع الجزائري في الفقرات (1، 2 و3 من المادة 65 مكرر 16) من قانون الإجراءات الجزائية على من يكشف هوية المتسرب عقوبات صارمة تتفاوت درجتها حسب الضرر الذي يرتبه الكشف على المتسرب أو على احد أفراد أسرته قد تصل إلى 20 سنة حبسا وغرامة مليون دينار.

[2] أنظر المادة (65 مكرر ) من القانون الإجراءات الجزائية.

**أولا–الضوابط الإجرائية:** تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، 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 والمتمثلة حسب أحكام المادة (65 مكرر 11 ق إ ج) في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه[1]. على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتلافي حدوث تجاوزات وتعسف في استعمال هذا الحق.

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وإلا كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة (65 مكرر 15 ق.ج) بنصها "**يجب أن يكون الإذن المسلم طبقا للمادة (65 مكرر 11) مكتوبا تحت طائلة البطلان**".

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن الشروط نفسها. وفي الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة[2].

**ثانيا– الضوابط الموضوعية:** إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسين هما:

–الأول هو عنصر التسبيب، تضمنته المادة (65مكرر15 ق إ ج)، ويتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.[3]

---

[1] تنص المادة ( 65 مكرر 11 ) من قانون الإجراءات الجزائية على أنه " ... يجوز لوكيل الجمهورية او لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب"

[2] أنظر المادة (65 مكر 15) من قانون الإجراءات الجزائية الجزائري.

[3] علاوة هوام " **التسرب كآلية للكشف عن جرائم في القانون الجزائري** " مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012 ، ص 03.

– أما العنصر الثاني، فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددتها على سبيل الحصر المادة (65 مكرر5) المشار إليها أعلاه. والناظر إلى هذه الطائفة من الجرائم التي خصها المشرع الجزائري بإمكانية الأمر بإجراء عمليات التسرب بخصوصها، يجدها تندرج ضمن الجرائم الخطيرة جدا لسرعة انتشارها وامتداد آثارها خارج الحدود الوطنية، كما أنها تسخر عددا كبيرا من المجرمين الأذكياء، وقائمة على التخطيط واستخدام كل الوسائل محو آثار الجريمة وطمس معالمها[1]. مما يجعل الاستعانة بإجراء التسرب للكشف عن مثل هذه الجرائم والإطاحة بمرتكبيها أمرا مبررا ومفيدا.

## المطلب الثاني اعتراض المراسلات والمراقبة الإلكترونية

إن الإقدام الهائل للأفراد والمؤسسات على وسائل الاتصال الحديثة والاستخدام المفرط الشبكات المعلوماتية في الآونة الأخيرة ، جعل المشرع في العديد من الدول يدرك الصعوبات الكثيرة التي تثيرها محاولة مد نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية، لذلك عمدت العديد من هذه الدول إلى مراجعة قوانينها الإجرائية، بوضع نصوص صريحة تنظم هذه العملية[2].

فكان المشرع الفرنسي سباقا إلى تبني عملية اعتراض ومراقبة الاتصالات الالكترونية ضمن إجراءات التحري و التحقيق الجنائي من خلال قانون إجراءات الجزائية لعام 1991، ثم تلاه المشرع الأمريكي في عام 2000 بمناسبة تعديل القانون الاتحادي الإجرائي الأمريكي، أين تم توسيع مجال تطبيق إجراء الاعتراض والمراقبة ليشمل كل المراسلات السلكية واللاسلكية[3]. ونظرا لثبوت نجاعة هذا الإجراء في تعقب الدليل وإثبات الجرائم الالكترونية، فقد أوصت الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 من خلال نص المادة (21) جميع الدول الأعضاء بضرورة تبني اعتراض المراسلات والمراقبة الالكترونية للاتصالات في

[1] زورو هدي، **التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري**، مجلة دفاتر السياسة والقانون، العدد الحادي عشرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2014، ص 121.

[2] براهيمي جمال، **مرجع سابق**، ص87.

[3] VERGUCHT Pascal, op.cit., p 384

تشريعاتها الإجرائية الداخلية ضمن إجراءات البحث والتحقيق[1]، الأمر الذي لقي استجابة واسعة من طرف غالبية الدول الأوروبية.

ولم يتخلف المشرع الجزائري عن هاته الدول، بل تدخل بموجب قانون الإجراءات الجزائية رقم (06/22) المؤرخ في 20/09/2006 المعدل والمتمم فاستحدث لهذا الإجراء الفصل الرابع كاملا تحت عنوان "**اعتراض المراسلات وتسجيل الأصوات والتقاط صور**" تناول فيه المقصود بهذا الإجراء، نطاقه وضمانات استخدامه. ثم عززه بالقانون رقم (09/04) المؤرخ 5 أوت 2009 . وسنبين كل ذلك في الفرعين التاليين:

## الفرع الأول: مفهوم الاعتراض و المراقبة الإلكترونية

عرفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بستراسبورغ في 06/10/2006 لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها "عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة"[2].

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة (65 مكرر5) من قانون الإجراءات الجزائية، إذ اعتبر عملية مراقبة المراسلات بأنها "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين، الاستقبال والعرض. مع العلم ان هذا النص هو إعادة صياغة المادة (100) من قانون الإجراءات الجزائية الفرنسي[3].

---

[1] Article( 21); Interception de données relatives au contenu ;

1- chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves a définir en droit interne : aa collecter ou enregistrer par l'application par de moyens techniques existant sur son territoire,et ... ». voir ; http://convention.coe.int/Treaty/fr/Treaties/Html/185.htm

[2] بوكر رشيدة، **مرجع سابق**، ص 442.

[3] l'article( 100) stipule "... les autorités judiciarises peuvent intercepter, enregistrer et transcrire des correspondances émises par la voie des télécommunications ... » voir la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales Français, JORF, 16 nov., 2001.

فبالرجوع الى نص هذه المادة، نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات[1]، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها ( كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها ( ورقية أو رقمية)، أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفاكس، تلغرام) أم لاسلكية (البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلات والرسائل والحوليات التي تعد مراسلات خاصة[2].

وقد تأكد هذا الأمر في المادة (2) فقرة "و") من القانون رقم (09/04 ) التي عرفت الاتصالات الالكترونية بأنها "**أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية**"[3].

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين[4]، وذلك لغرض التصنت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم[5].

---

[1] BENNOUAR Abdelhakim, Les techniques spéciales d'enquête et d'investigation en Algérie, article publier sur ; www.Mémoire Online 2000-2013, pp 2-3

[2] وهو ما يستشف كذلك من خلال نص المادة (09/6) من القانون رقم (2000/03) المؤرخ في 05/08/2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات التي اعتبرت المراسلات بانها "كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها الى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مرسلات".

[3] وهو التعريف الذي كرره المشرع الجزائري في المادة (05) من المرسوم الرئاسي رقم (15-261) المؤرخ في 8 أكتوبر 2015، المحدد تشكيلة وتنظيم و كيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جريدة رسمية عدد 53، صادر في 8 أكتوبر 2015 .

[4] من أشهر تقنيات المراقبة الالكترونية تقنية برنامج كارنيفور التي طورتها إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي (FBI ) من أجل تعقب وفحص رسائل البريد الالكتروني المرسلة والواردة عبر أي حاسب خادم يستخدمه أي مزود خدمة الانترنت، ويشتبه في أن المراسلات المارة عبر خدماته تحمل معلومات مهمة عن جرائم ما. للمزيد من التفاصيل انظر: مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، القاهرة، 2003، ص180.

[5] ربيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، الجزائر، 2011، ص157.

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلة إثبات الجرائم الالكترونية، المراسلات عبر البريد الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز. فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية[1].

## الفرع الثاني: القيود الواردة على عملية اعتراض ومراقبة المراسلات

إذا كان أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها قد اثبت جدارته في كشف وإثبات الكثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الالكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيرا لحرمة الحياة الخاصة للإفراد، واعتداء صارخا على سرية مراسلاتهم واتصالاتهم التي كفلتها معظم الدساتير والتشريعات العقابية بالحماية[2].

ولتحقيق 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 تعسف السلطات العامة وتصون الحرية الفردية. والتي نلخصها فيما يلي[3]:

**أولا- الحصول على إذن السلطة القضائية المختصة:** قيد القانون اللجوء إلى عملية اعتراض او مراقبة المراسلات بشرط الحصول المسبق على إذن مكتوب ومسبب من الجهات القضائية المختصة المتمثلة عادة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي[4]، أو قاضي التحقيق

---

[1] ربيحة زيدان، **مرجع سابق**، ص 159.

[2] نذكر منها المادة ( 46/2) من الدستور الجزائري لسنة 2016 التي تنص على "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة" تقابلها المادة (09) من الدستور التونسي و المادة (45) من الدستور المصري و المادة 15 من الدستور الايطالي والمادة (72) من الدستور البولندي. اما عن التشريعات العقابية نذكر المادتين (303 و 303 مكرر) من قانون العقوبات الجزائري.

[3] براهيمي جمال، **مرجع سابق**، ص94.

[4] غير انه استثناء لهذه القاعدة عندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة يكون النائب العام لدى مجلس قضاء الجزائر هو المختص بمنح الإذن لإجراء عملية المراقبة، أنظر (الفقرتين 6 و 7 من المادة 04) من القانون (09-04).

في مرحلة التحقيق القضائي وإلا كان هذا الإجراء باطلا، فالسلطة القضائية وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية الإجراء[1].

وحتى يكون الإذن صحيحا ومنتجا لآثاره، يجب أن يتضمن جملة من العناصر الأساسية وهي:

**1- طبيعة الجريمة التي تبرر الإجراء:** والتي ينبغي أن تكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية[2]، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تبطل الإجراءات العارضة.

**2- التعريف بالعملية:** بمعنى تحديد المراسلات والاتصالات المطلوب اعتراضها وتسجيلها، تحديد الأماكن المقصودة ( سكنية او غير سكانية، عامة أو خاصة)، إلى جانب تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الاعتراض، والتي يجب أن لا تتجاوز أربعة أشهر قابلة للتجديد ضمن الشروط نفسها، حسب تقدير السلطة مصدرة الإذن لمقتضيات التحري والتحقيق[3]. وهي المدة نفسها التي حددها المشرع الفرنسي في المادة (100-1) من قانون إجراءات الجزائية الفرنسي[4].

ولا يكفي الحصول على إذن مشمول بالعناصر المذكورة لإتمام عملية اعتراض المراسلات أو المراقبة، إنما لا بد أن تنفذ هذه العمليات تحت الرقابة المباشرة للسلطات التي أذنت بها، وذلك من خلال قيام ضابط الشرطة القضائية المأذون له بإحاطتها علما بكل خطوات وتطورات عملية الاعتراض والمراقبة وإخبارها بشكل دوري ومستمر عن عمليات وضع

---

[1] ورد هذا الشرط بالنسبة لعملية الاعتراض في المادة (65 مكرر 5) من قانون الإجراءات الجزائية بالشكل التالي:" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ... وفي حالة فتح تحقيق قضائي تتم العملية المذكورة بناء على إذن من قاضي التحقيق و تحت مراقبته المباشرة. أما بالنسبة لإجراء المراقبة الالكترونية نص عليه في المادة (04/6) من القانون ( 09/04 ) على النحو التالي: "... لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية المختصة".

[2] وهي الجرائم المحددة على سبيل الحصر في المادة (65 مكرر 5) من ق ج والمادة (04) من قانون (09-04).

[3] استثناء لهذه القاعدة إذا تعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة تكون مدة الإذن بالمراقبة الالكترونية 06 أشهر قابلة للتجديد، انظر المادة (04/ 7) من قانون (09-04).

[4] voir l'article ( 100-1) de la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF, 16 nov, p 18215.

الترتيبات التقنية لهذا الغرض، ساعة بداية وانتهاء هذه العمليات، على أن يدون كل ذلك في محاضر مرقمة[1]. وبهذه الطريقة فقط نكون قد حققنا الغرض الحقيقي من هذه العمليات.

**ثانيا- تسبيب اللجوء إلى اعتراض أو مراقبة المراسلات:** يقصد به المبرر الشرعي والضرورة الملحة التي تستدعي القيام بعملية اعتراض أو مراقبة المراسلات[2]، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى هذه العملية، وفي هذا الشأن يشترط على وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة تقدير جدواها وجدية دواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة والجناة مسبقا، ثم موازنة كل هذه العناصر للتأكد مما إذا كانت كافية لخرق مبدأ حرمة الحياة الخاصة. فإذا ارتأى بان التسبيب غير كاف رفض طلب الإذن.

والجدير بالذكر هنا هو أنه إلى جانب إمكانية القيام بمراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء، فقد أجاز المشرع الجزائري كذلك تطويع هذه التقنية الغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما قررته المادة الرابعة (4) من القانون (09/04)[3]. وهنا يصبح مفهوم الضرورة الملحة التي تستدعي القيام بإجراءات المراقبة الالكترونية مبهما وغير واضح، خاصة إذا تعلق الأمر بالجرائم التي تهدد النظام العام لأن مصطلح النظام العام غير محدد المعالم وقد تنجر عنه اختلالات كبيرة من شأنها المساس بحرية الأفراد[4].

---

[1] أنظر نص المادة (65 مكرر 9) من قانون الإجراءات الجزائية، تقابلها المادة (1003/1) من قانون الإجراءات الجزائية الفرنسي.

[2] MICHEL Prud'homme, droit criminel, écoutes et enregistrements clandestins, R.D.P, N 59, Paris, 2010, p47.

[3] تنص المادة (4/ 1و 2) من القانون ( 09/04 ) على انه " يمكن القيام بعمليات مراقبة الاتصالات الالكترونية في الحالات الآتية: 1-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. 2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني".

[4] BENNOUAR Abdelhakim, op cit, p 03.

**ثالثا- تحديد الجرائم محل الاعتراض والمراقبة:** إن الاستعانة بعملية اعتراض أو مراقبة المراسلات الالكترونية لغرض التحقيق غير مسموح في كافة الجرائم إنما مجال تطبيقها يتوقف عند نوع محدد فقط وهي كالتالي:

- الجرائم المذكورة على سبيل الحصر في نص المادة (65 مكرر(5) من قانون الإجراءات الجزائية، وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية[1].

- الجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة (04) من قانون (09/04) المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني[2].

**رابعا- سرية الإجراءات وكتمان السر المهني:** أي ينبغي أن تنفذ عملية الاعتراض والمراقبة في سرية تامة و دون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة (45 فقرة 4) ق إ ج ج.

وينبغي التنبيه كذلك، إلى أن المشرع الجزائري لم يشر صراحة إلى كيفية وضع الأدلة المحصل من عملية اعتراض ومراقبة المواصلات (التسجيلات السمعية البصرية، البيانات الرقمية) في أحراز مختومة، مما يطرح التساؤل حول مدى اعتبارها من قبيل الأشياء المضبوطة التي تخضع لأحكام المادة (84) من قانون الإجراءات الجزائية وحكم المادة(45/5) من القانون نفسه[3].

علما بأن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية أصلية تقتضي الشرعية الجزائية حفظها بطريقة خاصة بوضعها في أحراز مختومة تضمن عدم التلاعب والعبث فيها بالحذف أو الإضافة، وضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.

---

[1] أنظر نص المادة (65مكرر5) من قانون الإجراءات الجزائية.

[2] أنظر نص المادة (04 ) من القانون (09/04).

[3] تنص المادة (84) من قانون الإجراءات الجزائرية على "... ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة..."

ومن ذلك كانت الحاجة إلى فتح المشرع المجال أمام سلطات التحقيق والاستدلال للاستعانة بذوي الاختصاص سواء عن طريق تسخير كل من لديهم دراية و مؤهلات في مجال سير تكنولوجيات الإعلام والاتصال من اجل تزويدهم بالمساعدة الفنية والتقنية الممكنة لتسهيل وإنجاح أية عملية من عمليات التحقيق بما فيها المراقبة الالكترونية للاتصالات كما هو منصوص في المادة (05) فقرة أخيرة من القانون رقم (09/04)[1]. أو عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول الى المعطيات التي تشكل محل الجريمة أو تحتوي أدلة لها، الموجودة داخل المنظومة المعلوماتية و منع الاطلاع عليها أو نسخها أو تهريبها أو تدميرها وفقا لما تقتضيه المادتين (7و8) من القانون رقم (09/04).

ويجب الاعتراف بأن تكريس المشرع الجزائري لإجراءات اعتراض المراسلات والمراقبة الالكترونية يعد خطوة جريئة تحسب له، على اعتبار أنها من اخطر إجراءات التحري والتحقيق عبر العالم الافتراضي نظرا لما تحمله من انتهاكات مباشرة لخصوصيات الإنسان هذا من جهة، ومن جهة أخرى لان الفقه الجنائي لم يحسم الأمر بعد ويرى بان المراقبة الالكترونية لا تزال محل نظر في القانون لضرورة الالتزام بما هو مقرر في القوانين والدساتير من ضمانات احترام الحق في الخصوصية.

وفصل الحديث، أنه رغم المخاوف الكثيرة التي أبداها الفقه حيال إجراءات التحقيق المستحدثة لما تحمله من عدوان على الحق في الخصوصية الذي يعد من أقوى الحقوق الدستورية الفردية، إلا أن الواقع يثبت بأن الاستعانة بهذه الإجراءات أصبح ضرورة ملحة للتصدي الفعال لظاهرة الإجرام المعلوماتي. والضرورة هنا ترجع من الناحية إلى الارتفاع المتزايد لمعدل الإجرام الالكتروني نتيجة اقتحام المعلوماتية كل مجالات الحياة، ومن ناحية أخرى إلى ثبوت عجز وقصور تقنيات التحقيق التقليدية في مواجهة الجرائم الالكترونية الحديثة نتيجة عدم ملائمتها مع الطبيعة الخاصة لهذه الجرائم.

[1] أنظر المادة (05) من القانون رقم (09/04)، مرجع سابق.

# الخاتمـــــــــــة

## الخاتمة

تتضمن هذه الدراسة في متنها إيضاحا لرؤية إجرائية تتناول مسألة البحث والتحقيق الجنائي في الجرائم الإلكترونية، والمشكلات الإجرائية المترتبة عليها، وكذا الحلول الممكنة المقترحة لمعالجة تلك المشكلات.

وقد اتضح لنا أن الجرائم الإلكترونية تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، والتي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، وأنها من المستجدات التي لم تكن معروفة في القانون الجزائي بشقيه الموضوعي والإجرائي، من ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الجديد في إطار عملية البحث والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بهذه العملية.

وتتجلى أولى هذه الإشكالات في القصور الذي يعتري النصوص الجزائية الإجرائية القائمة في مواجهة مثل هذه الجرائم، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها المبدأ حرية القاضي الجزائي في الاقتناع.

بالموازاة مع ذلك اتضح أن عملية البحث والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الحديثة تتخللها عقبات كثيرة، يعود البعض منها إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، فالطابع العابر للحدود الذي تتسم به الجريمة الالكترونية قد يثير العديد من المشاكل القانونية، من بينها تحديد الدولة التي يختص قضاءها بملاحقة مرتكب هذه الجريمة، والمعيار المعتمد في ذلك، ناهيك عن مشكلة احترام سيادة الدولة التي تقف حاجزا أمام سلطات التحقيق عندما يستوجب البحث عن أدلة إثبات جريمة الكترونية خارج الإقليم الوطني وفي أقاليم عدة دولة أجنبية، خاصة إذا اقترن ذلك بغياب وسائل وآليات دولية فعالة تضمن التعاون القضائي والأمني بين الدول في هذا المجال.

أما البعض الأخر فمرده هو قصور القواعد الإجرائية عن مواكبة تطورات ومتغيرات الجرائم الالكترونية المتسرعة، ما قد يقف حجر عثرة في سبيل الاستفادة من معطيات التكنولوجيا الحديثة في الكشف عن الجرائم الالكترونية وملاحقة مرتكبيها.

ومن أجل تجاوز هذه العقبات والمشكلات، نقدم جملة من الحلول التي نعتقد انها فعالة وممكنة التجسيد، وهي حلول مستوحاة من تجارب بعض الدولة المتقدمة وكرستها عدد من القوانين والاتفاقيات الدولية على رأسها الاتفاقية الأوروبية حول الجريمة الالكترونية المبرمة في بودابست عام 2001، والتي أردنا أن نعرضها في شكل اقتراحات على النحو التالي :

– يتعين على الدول التي لم تسن بعد قوانين جزائية موضوعية وإجرائية خاصة بالجرائم الالكترونية، كما هو الحال بالنسبة لغالبية الدول العربية، الإسراع إلى تعديل وترشيد قوانينها القائمة بما يجعلها تسري وتطبق على مثل هذه الجرائم، وذلك لتفادي القصور التشريعي وتخطي الثغرات القانونية الحاصلة في هذا المجال، التي قد يستفيد منها المجرم الالكتروني للإفلات من المتابعة الجزائية والعقاب.

– لا يكفي الاعتماد على التشريعات القائمة لتجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم الالكترونية، بل لا بد من تدعيمها بنصوص خاصة حديثة تتضمن إجراءات تحقيق ملائمة مع طبيعة هذا الشكل الجديد من الإجرام، ومسايرة للمتغيرات والتطورات الحاصلة في تقنيات وأساليب ارتكابها. كما فعل المشرع الجزائري من خلال القانون رقم (09–04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حينما استحدث تقنيات ومعالم جديدة توضح القواعد الإجرائية في مجال تحريك و مباشرة الدعوى الجزائية وإتباع آثار المجرم الالكتروني من خلال تحديد الترتيبات التقنية للمراقبة الالكترونية، وكيفية تفتيش المنظومة المعلوماتية عن بعد، ثم إجراءات حجز المعطيات الالكترونية، ورسم معالم الاختصاص القضائي تحسبا للطابع الدولي الذي تكتسيه الجرائم الالكترونية .

– ضرورة تكثيف التعاون والتنسيق الدولي بين الدول من أجل تطوير وتوحيد التشريعات الجزائية الموضوعية والإجرائية التي تعنى بمكافحة الجرائم الالكترونية، عن طريق إبرام اتفاقيات دولية وإقليمية ثنائية ومتعددة الأطراف في هذا المجال، أو الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص كالاتفاقية الأوروبية حول الجريمة الالكترونية المبرمة في بودابست عام 2001، مع مراعاة المصلحة الوطنية و مبدأ السيادة .

– ضرورة اعتماد سياسة واضحة وفعالة بخصوص التعاون الأمني المتبادل والمساعدة القضائية والفنية بين الدول في مجال مكافحة الجريمة الالكترونية، من خلال تبني إجراءات

التحقيق والمتابعة الجزائية السريعة والمناسبة، وخلق قنوات اتصال ثنائية أو متعددة الأطراف تسمح للسلطات القائمة على التحقيق، الاتصال بسهولة بمثيلتها الأجنبية والتنسيق معها. أو التدخل السريع للتحقيق في إقليم دولة أجنبية دون أن يشكل ذلك مساسا بسيادة هذه الدولة.

– دعوة الدول العربية إلى إنشاء منظمة شرطة عربية تهتم بالتنسيق الأمني في مجال مكافحة الجرائم المعلوماتية عبر الانترنت، مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي.

– ضرورة إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة الجرائم الالكترونية، يكون لديهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، مع إخضاعهم لبرامج تدريبية خاصة دورية، تساعدهم على تحيين و تحديث معارفهم وخبراتهم واطلاعهم بآخر المستجدات الحاصلة مجال التقنية المعلوماتية.

– تفعيل دور المجتمع المدني و الحراك الجمعوي المؤهل في التحسيس والوقاية من الوقوع في الممارسات الخاطئة والسلوكيات الإجرامية عبر شبكة الانترنت.

– يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ما قبل الجامعي.

– دعوة المؤسسات التعليمية المعنية بتأهيل الأطر القانونية إلى تضمين موضوع الإجرام الالكتروني أو المعلوماتي ضمن خططها الدراسية.

– ضرورة اهتمام الباحثين ورجال القانون الجزائريين بالدراسات القانونية التي تعنى بالجوانب الإجرائية للجرائم الالكترونية والعمل على إثراء محتواها، لأنها لم تنل بعد حظها من البحث والتشريح، ولا تزال لحد اليوم في منطقة الظل في بلادنا رغم ما يثيره الزحف الهائل للإجرام الالكتروني من مخاطر.

في الختام، فإنني لا أزعم من خلال هذا البحث بلوغي جادة الصواب، ولكن أملي أن يحقق قدر من العزم منه، وما أنا إلا بشر اجتهد فأخطئ و أصيب، فان أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين، ولله الأمر من قبل ومن بعد، والحمد لله رب العالمين.

# الملخـــــــــص

# الملخـــــــص

ملخص:

تعد الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام والاتصال الحديثة، فهي تختلف تماما عن الجرائم التقليدية، في ذاتية أركانها و أساليب ارتكابها والبيئة الافتراضية و اللامادية التي ترد عليها و خصوصية مرتكبيها. مما جعلها ظاهرة غريبة عن نصوص القانون الجزائي التقليدي بشقيه الموضوعي و الإجرائي، من ثمة فأية محاولة إخضاع هذا النمط الإجرامي الجديد لإجراءات التحقيق و الإثبات المألوفة سيؤدي حتما إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية، وينجر عنه عقبات كثيرة أمام سلطات التحقيق .ولكن مع ت ازيد معدلات الجرائم الالكترونية وامتداد آثارها إلى كافة مجالات الحياة بسبب ارتباطها بشبكة الانترنت، اضطرت الدول إلى ترشيد نصوصها الإجرائية التقليدية لتصبح نافذة في مواجهة هذه الجرائم. إلى حين إرساء نصوص جديدة تتلاءم مع الطبيعة الخاصة لظاهرة الإجرام الالكتروني، وتواكب التطورات و المتغيرات التي صاحبتها .فإلي أي مدى يمكن التعويل على هذه النصوص الإجرائية للتصدي لهذا النمط الإجرامي المتجدد والمتطور ؟ تلك هي الإشكالية التي حاولنا الإجابة عنها من خلال المذكرة

**Résumé** ; Les infractions électroniques sont l'un des nouveaux types de la criminalité engendré par les technologies modernes de l'information et de la communication, qui se diffère des infractions classiques par ses éléments particulières, en l'occurrence ses modes de commission, son environnement virtuel et les caractéristiques de ses auteurs, se qui en fait un phénomène étrange aux textes objectifs et procédurales de droit pénal actuel. Alors toute tentative de soumettre cette nouvelle forme de criminalité aux procédures d'enquête et de preuve familières, ne satisfera pas aux exigences du principe de légalité procédurale et créera de nombreux obstacles aux autorités chargées d'enquête. Cependant, comme les cyber crimes ont augmentés et leurs effets se sont étendus a tous les domaines de la vie en raison de leur connexion a l'internet, les Etats ont du rationaliser leurs lois procédurales traditionnelles pour devenir applicables et efficaces contre ces infractions. Jusqu'à la mise en place de nouveaux textes adaptés a la nature particulière de la cybercriminalité, et aux évolutions et changements qui les accompagnent. Dans quelle mesure ces procédures peuvent-elles être invoquées pour répondre a ce type de criminalité renouvelé et évolutif ? Telle est la problématique a la quelle nous avons essayé de répondre a travers cette thèse.

# قائمـــــــة المصادر والمراجع

**قائمة المراجع**

**أولا: المراجع باللغة العربية:**

**1-الكتب:**


01 إسحاق إبراهيم منصور، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1995.

02 بخي فاطمة الزهراء، **إجراءات التحقيق في الجريمة الإلكترونية**، 2014.

03 بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016.

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

05 بوكر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012.

06 جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.

07 حسن الجوخندار، **التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية**، دار الثقافة عمان، الطبعة الأولى، 2008.

08 خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر و التوزيع، عمان، 2011.

09 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، إسكندرية، 2009، ص 195.

10 خالد ممدوح، **أمن الجريمة الإلكترونية**، الدار الجامعية، الإلكترونية، الإسكندرية، 2008.

11 ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.

12 ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2015-2016.

13 سامي جلال فقي حسين "التفتيش في الجرائم المعلوماتية "دار الكتب القانونية، القاهرة، 2011.

14 سعيداني نعيم، **آليات البحث والتحري** عن **الجريمة المعلوماتية في القانون الجزائري**، 2013.

15 صغير يوسف، **الجريمة الإلكترونية**، عبر الانترنت، تيزي وزو، 2013.

16 ضياء مصطفى عثمان، **السرقة الإلكترونية**، دار النفائس، عمان، الطبعة الأولى، 2011.

17 عبد الفتاح البيومي حجازي، **مكافحة جرائم الأنترنت**، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.

18 عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير المعلوماتي**، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى.

19 عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

20 عبد الله حسين محمود، **إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية**، دبي، 2003.

21 عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، 2008.

22 عمر محمد أبو بكر بن يوسف، الجرائم الناشئة عن استخدام الانترنت – الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004.

23 محمد طارق عبد الرؤوف، **جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية**، الطبعة الأولى، 2011.

24 محمد مصطفى موسى، **التحقيق في الجرائم الإلكترونية، مطابع الشرطة**، القاهرة، 2009.

25 نواوي سليمة، **دور الدرك الوطني في محاربة الجريمة الالكترونية**، جامعة المسيلة، 2018/2019.

26 هلال عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، 2011.

27 يوسف جفال، التحقيق في الجريمة الإلكترونية، 2016/2017.

28 يوسف خليل يوسف العطيفي، **الجرائم الإلكترونية في التشريع الفلسطيني**، غزة، 2013.

**2 – الرسائل والمذكرات**

01 أحمد بن زايد جوهر الحسن المهدي، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق، جامعة القاهرة، 2009.

02 أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة ماجستير في القانون الجنائي، جامعة ورقلة، 2013.

03 براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون، كلية الحقوق، جامعة تيزي وزو، 2018.

04 عمر بن إبراهيم بن حماد العمر، **إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي**، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007.

05 فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2011،

06 محمد بوعمرة – سيد علي بنينال، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في قانون الأعمال، كلية الحقوق، جامعة البويرة، 2013.

07 محمد نصير السرحاني، **مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير**، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

**3-المقالات والبحوث:**

01 آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام الييبرالي المفاهيم والتحديات "، 11-12 أفريل 2017.

02 بن سولة نور الدين، **الجرائم الالكترونية في ضوء التشريع الجزائري**، المجلد التاسع، العدد 1، مارس 2018.

03 بوضياف إسمان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018.

04 حسام محمد نبيل الشنراقي، الجرائم المعلوماتية دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013.

05 زورو هدي، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد الحادي عشرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2014.

06 سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر 2019.

07 عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد 22، عدد 86، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، 2013.

08 عفيفي كمال عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، طبعة ثانية، منشورات الحلبي القانونية، دمشق، 2007.

09 علاوة هوام " التسرب كآلية للكشف عن جرائم في القانون الجزائري " مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012.

10 على محمود على محمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 الى 28 أفريل 2003.

# فهرس المحتويات

# فهرس المحتويات

**الفصل الثاني إجراءات التحقيق في الجرائم الإلكترونية**