جامعة آكلي محند أولحاج - البويرة.

كلية الحقوق والعلوم السياسية.

قسم القانون العام.

# إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية

مذكرة لنيل شهادة الماستر في القانون العام.

تخصص: القانون الجنائي والعلوم الجنائية.

**إعداد الطالب:**

-رزيق محمد .

**تحت إشراف الأستاذ:**

- خليفي سمير.

**لجنة المناقشة:**

| الاسم واللقب | الدرجة العلمية | الجامعة الأصلية | الصفة |
|---|---|---|---|
| لوني نصيرة | أستاذة محاضرة | البويرة | رئيسا |
| خليفي سمير | أستاذ محاضر | البويرة | مشرفا ومقررا |
| مصاد رفيق | أستاذ محاضر | البويرة | عضوا ممتحنا |

السنة الجامعية 2019/2018

# إهـداء

إلى معلم البشرية ومنقذها **"رسول الله محمد صلى الله عليه وسلم"**

إلى من جعل من نبض قلبها أول صوت يسمع، ومن دفء حضنها أول مأوى يسكن

إلى من جعل الله الجنة تحت أقدامها **"أمي الحبيبة"**

إلى من كان سببا في وجودي وحرم نفسه ليعطيني وأتعب نفسه ليريحني، إلى من شجعني على طلب العلم ودفعني إليه **"أبي العزيز"**

إلى قرة عيني ابنتي **أسرار** وفلذة فؤادي إبني **عبد الحي موسى**

إلى رفيقة دربي **"زوجتي"**

إلى من لا تحلو الدنيا إلا بوجودهم وقربهم **"إخوتي"**

إلى من جمعني بهم القدر فأحببتهم وأحبوني **"أصدقائي"**

إلى من جمعني بهم القدر وطلب العلم **"أساتذتي الكرام"**

إلى كل من أمد لي بيد العون **...**

إلى كل من وسعتهم ذاكرتي ولم تسعهم مذكرتي لكم جميعا أهدي ثمرة هذا الجهد المتواضع.

# شكر وعرفان

في المقام أحمد الله سبحانه وتعالى لأنه منّ عليا بالتوفيق والقدرة الكبيرين لإنجاز هذا البحث المتواضع، فالحمد لله حمدا كثيرا طيبا مباركا فيه.

كما لا يسعني إلا أن أتقدم بجزيل الشكر والامتنان إلى أستاذي الفاضل: **خليفي سمير** الذي تكرم عليا بإشرافه وسديد توجيهاته إلى غاية إتمام هذا البحث، كما أشكر جميع أساتذة كلية الحقوق والعلوم السياسية بجامعة البويرة على المجهودات التي بذلوها من أجلنا، وجزاهم الله عنا كل خير وجعلهم نبراسا يضيء طريق كل طالب علم.

# المختصرات

## أهم المختصرات

**ق.إ.ج.ج:** قانون الإجراءات الجزائية الجزائري.

**ق.ع.ج :** قانون العقوبات الجزائري.

**ج.ر:** جريدة رسمية.

**د.ط :** دون طبعة.

**د.ب.ن :** دون بلد النشر.

**د.س.ن :** دون سنة النشر.

# المقدمة

أدى ظهور أنظمة المعلوماتية وتطبيقاتها المتعددة إلى بروز مشاكل عديدة أثرت على الجانب التشريعي في الجزائر، إذ أشابته بالقصور في مواجهتها من خلال ظهور أنماط جديدة من الجرائم التي لم تعد معهودة في السابق، وحولت الجريمة من صفتها العادية وأبعادها المحدودة إلى أبعاد مستحدثة باعتماد التقنية الحديثة، فالمجرم والجريمة في تطور وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم وبالتالي جريمة الأمس ليست كجريمة اليوم، إلا أن المشرع الجزائري تدارك ذلك بإصدار القانون 15/04 [1] المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، والذي جاء كمولود جديد في التشريع الجنائي الجزائري، كما اصطلح عليه بالجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات.

أصبحت تقنية الحاسوب تستعمل كوسيلة لارتكاب الجرائم تارة وكموضوع للجريمة تارة أخرى، وأصبح هذا النوع من الجرائم يرتكب في وسط إفتراضي غير متعارف عليه ولا يشبه الوسط التقليدي للجرائم التقليدية، مما دفع المشرع الجزائري مرة أخرى في سنة 2006 بتعديل بعض أحكام قانون العقوبات، بحيث أصدر الأمر 23/06 المعدل والمتمم لقانون العقوبات الجزائري[2]، بالإضافة إلى تعديله لقانون الإجراءات الجزائية الجزائري بالقانون 22/06 [3]، إلا أن كل هذا لم يغطي الصرح الكبير الذي تكتسيه الجريمة المعلوماتية في العالم المعلوماتية.

---

**01-** أنظر القانون رقم 15/04 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري المؤرخ في 08 جوان1966 ج ر عدد 71.

**02-** أمر رقم 06-23 المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو 1966 والمتضمن ق ع ج، ج ر عدد 84 المؤرخة في 04 ذو الحجة عام 1427 الموافق لـ 24 ديسمبر 2006.

**03-** أمر رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو 1966 والمتضمن ق إ ج ج، ج ر عدد 84 المؤرخة في 04 ذو الحجة عام 1427 الموافق لـ 24 ديسمبر 2006.

تدارك المشرع ذلك في سنة 2009 ليصدر القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جاء ببعض الإجراءات التي من شأنها إن صح التعبير أن تكمل ما جاءت به القواعد الإجرائية العامة التي نص عليها قانون الإجراءات الجزائية، كل هذا تحت ظل أزمة القانون الجنائي في مواجهة واقع المعلوماتية والذي فرض حلها البحث عن الأوضاع القانونية والإجراءات اللازمة مع مدى ملاءمتها في مواجهة هذه المشاكل.

وتكمن أهمية موضوع **"إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية"** أساسا في كون الجريمة المعلوماتية جريمة جديدة حديثة النشأة وبالتالي لا يكفي تطبيق الإجراءات المطبقة على الجرائم التقليدية، حيث نجد القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية لا يمكن أن تطبق عليها كونها تقع في عالم افتراضي، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال التي تستعمل في جميع مجالات الحياة سواء من طرف الأفراد أو المؤسسات، إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إلى إيجاد إجراءات تحري جديدة.

ونظرا للأهمية البالغة التي تكتسيه مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي، الذي يعرف تطورا سريعا في مجال تكنولوجيا الإعلام والاتصال، حيث أصبحت هذه الأخيرة الركيزة التي تقوم عليها مختلف القطاعات سواء الخاصة أو العامة، حاولنا في دراسة موضوعنا وضع الخطوط العريضة بالتعرف على الإجراءات التقليدية للمعاينة والتفتيش والحجز داخل المنظومة المعلوماتية بالإضافة إلى الإجراءات الحديثة المطبقة في هذا الشأن.

وعليه فالهدف المبتغى من دراسة هذا الموضوع هو معرفة إجراءات التحري التقليدية داخل المنظومة المعلوماتية للمعاينة، المتمثلة في معاينة مسرح الجريمة الإلكترونية وإجراءات التفتيش والحجز في النظم المعلوماتية، بالإضافة إلى معرفة إجراءات التحري المستحدثة داخل المنظومة المعلوماتية بالتطرق إلى مراقبة الاتصالات الإلكترونية وكذا قواعد التفتيش والحجز داخل المنظومة المعلوماتية وتطبيقاتها في دراسة حالة.

ولما كانت الضبطية القضائية مقيدة في الدعوى الجزائية بمبدأ الشرعية الجنائية والإجرائية، فإن هذه الأخيرة لا يمكنها اتخاذ أي إجراء قضائي دون الرجوع إلى القواعد المنصوص عليها في قانون الإجراءات الجزائية، حتى لو كانت هذه الأفعال مستنهجة ولها درجة عالية من الخطورة الإجرامية، كل هذه التغيرات ونظرا لحداثة الجريمة المعلوماتية وحساسيتها دفعنا إلى تسليط الضوء عليها واختيار الموضوع بدراسة القوانين السالفة الذكر نظريا وتطبيقيا، وعليه نطرح الإشكالية التالية :

كيف تستطيع الضبطية القضائية إجراء المعاينات، التفتيش والحجز في الفضاء المعلوماتي وتحقيق حماية معلوماتية ومكافحة الجرائم المعلوماتية دون المساس بالشرعية الإجرائية؟

ولإعطاء الإشكالية تحليل يتماشى والموضوع محل الدراسة اتبعنا المنهج التحليلي من خلال دراسة وتحليل الإجراءات الخاصة بالمعاينات والتفتيش والحجز، ومنهج تجريبي من خلال تطبيقها في دراسة حالة وليتسنى لنا ذلك يجب طرح بعض التساؤلات الثانوية والتي مفادها:

-ما هي الإجراءات التقليدية المتبعة لمعاينة والتفتيش والحجز داخل المنظومة المعلوماتية؟
-ما هي إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية، وكيف يمكن تطبيق هذه القواعد الإجرائية من طرف الضبطية القضائية ميدانيا؟

# الفصل الأول:

# إجراءات التحري التقليدية للكشف عن الجرائم داخل المنظومة المعلوماتية.

تلعب الضبطية القضائية في مجال مكافحة الجريمة الواقعة داخل النظام المعلوماتي دورا هاما كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفة عامة والجرائم الواقعة في النظم المعلوماتية بصفة خاصة، حيث تظهر طبيعة هذه الأخيرة كيان بيئة غير محسوس، وتظهر عدة عراقيل وصعوبات لجهات التحري في الكشف عن هذه الجرائم ومتابعة مرتكبيها، الأمر الذي دفع بالمشرع الجزائري إلى إيجاد وحدات متخصصة تعمل في هذا المجال، تكون مزودة بالخبراء والتقنيين وتنظيم دورات متخصصة لهم في مجال مكافحة الجريمة المعلوماتية، وذلك بتلقيهم المعلومات الخاصة بتقنية أجهزة النظام المعلوماتي والجوانب الفنية لها، حتى تسهل عليهم عملية الكشف عن الجرائم ومنع وقوعها بإحكام الرقابة على المحلات ونوادي الانترنيت..... الخ، والتي تعد مجال خصب لاقتراف مثل هذه الجرائم.

دفعت خصوصية الجريمة المعلوماتية إلى إبراز مكافحة إجرائية خاصة من الناحية القانونية والتطبيقية، كتلك التي يمكن أن تمس بالحياة الخاصة، ومن بين هذه الأساليب والإجراءات، فالمشرع الجزائري سارع لمواكبة هذا التطور بتعديل بعض المواد الإجرائية في قانون الإجراءات الجزائية والتي سنسلط عليها الضوء في هذا الفصل بالتطرق إلى معاينة مسرح الجريمة الإلكترونية (مبحث أول)، وإجراءات التفتيش والحجز في النظم المعلوماتية (مبحث ثان).

# المبحث الأول

# معاينات مسرح الجريمة الالكترونية.

إن أول ما يجب دراسته من خلال البحث والتحري عن الجريمة هو مسرح الجريمة المعلوماتية، والذي يقصد به البيئة الإلكترونية المتكونة من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الجهاز وشبكاته في ذاكرته وأقراصه الصلبة الموجودة بداخله، والتي يجب أن يكون التعامل مع الأدلة الرقمية.

فمسرح الجريمة الإلكترونية هو المكان الذي ارتكبت فيه الجريمة أو جزء منها ويشمل الأماكن التي اكتشفت فيها الجريمة أو أجزاء منها، وقد يكون مسرح الجريمة في مكان أو عدة أماكن، وفقا للجريمة وعناصرها والمراحل التي مرت بها منذ البدء في التخطيط لها والإعداد، التجهيز والتنفيذ ومرحلة التصرف في عائداتها وإخفاء معالمها[1].

بالإضافة إلى أنه المشاهدة العينية لمكان أو شيء لإثبات حالة أو ضبط كل ما يلزم للكشف عن الحقيقة، أو إثبات حالة الأماكن والبيانات في الحقل الإلكتروني أو الرقمي والتي تتطلب انتقال ضابط الشرطة القضائية لمباشرتها ولإثباتها، ويمكن دراسة معاينات مسرح الجريمة الإلكترونية من خلال التحليل الجنائي لمعلومات الحاسوب (مطلب أول) ومعاينة محل الجرائم الواقعة داخل وخارج النظم المعلوماتية (مطلب ثان).

---

**1.** حمزة نجاة، معاينة مسرح الجريمة ودوره في الكشف عن الحقيقة، مذكرة لنيل شهادة الماستر في القانون الجنائي كلية الحقوق جامعة آكلي محند أولحاج البويرة، سنة 2014.ص 01.

## المطلب الأول
## التحليل الجنائي لمعلومات الجهاز

يعد التحليل الجنائي لمعلومات الجهاز هو أحد الطرق والتقنيات التي يمكن تطبيقها على أي تحقيق جنائي، كما أن طريقة إدارتها يجب أن تتضمن أشياء تكاملية مع الأخرى من التحقيق بالإضافة إلى ضمان إتباع السياسات والإجراءات القياسية المتبعة[1].

يعتبر الهدف الأساسي من تحليل جنائيات الجهاز هو تقصي المعلومات لكشف الفاعل وما فعله، بالإضافة إلى متى وأين ولماذا قام بهذا الفعل، بناء على ذلك تعد مهمة المحققين في جنائيات الحاسوب ومعاينتها من أصعب المهام في مجال تقنية المعلومات وذلك لأنه يجب على المحقق أن يكون مؤهلا تقنيا، بالإضافة إلى إلمامه بمجال القانون[2] لذا سنتطرق إلى مفهوم التحليل الجنائي (فرع أول)، وفيما تتمثل معلومات الجهاز (فرع ثان).

[1] عصام شيبان، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني ،المطبوعات الجامعية، الجزائر سنة 2005 ص 23.
[2] نفس المرجع ،ص 24.

## الفرع الأول

## مفهوم التحليل الجنائي

التحليل الجنائي الرقمي هو استخدام تقنيات العلم والتكنولوجيا في عمليات التحقيق الجنائي للقضايا المخالفة للقانون، وتتضمن فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على الدليل الرقمي الذي يستخدم في التحقيقات القانونية[1].

كما أنه علم يجمع بين العلوم الشرطية الجنائية وعلوم الحاسوب والشبكات، بهدف استخراج الأدلة الرقمية من أجهزة الحاسب وأجهزة الشبكة والوسائط الرقمية، والأدلة الرقمية يمكن أن تكون بيانات رقمية مخزنة في أجهزة الحاسوب أو المنظومات المعلوماتية أو المنقولة بواسطتها والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

وعملية التحليل الجنائي يجب أن تتم وفق معايير وإجراءات قانونية معتمدة من قبل المحكمة، وأهم هذه الإجراءات هو المحافظة على الأدلة الرقمية التي تم اكتشافها بدون أي تعديل أو تخريب، وتوثيق كامل العمليات من لحظة الوصول لمكان الجريمة والعمليات التي تمت في مخبر التحليل الجنائي الرقمي لحين وصول الدليل الرقمي إلى المحكمة[2].

---

1.جميل حسين طويلة، التحليل الجنائي الرقمي، مكتبة النور، سوريا بدون طبعة وبدون سنة النشر، ص 1

2. نفس المرجع ص10

## الفرع الثاني

## معلومات الجهاز

تتمثل معلومات الجهاز بصفة عامة في البيانات والنصوص، الصور والأشكال والرموز، وقواعد البيانات وبرامج الحاسوب، كما أنها مجموعة من البيانات والمعطيات التي قد تمت معالجتها وتحليلها وتلخيصها وتجريبها لتحقيق الأهداف المرجوة منها واستخدامها في المجالات المختلفة، أي أنها البيانات المجهزة في شكل منظم ومفيد بتسلسل منطقي[1].

فمعلومات الجهاز إذا هي الوسيلة المادية أو المعنوية أو مجموعة وسائل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها، ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها، وتشمل بذلك جميع المدخلات والمخرجات المرتبطة بالجهاز سلكيا أو لاسلكيا في نظام أو شبكة[2].

وهذه المعلومات يتم الحصول عليها بفحص ومعاينة مكونات الجهاز المتمثلة أساسا في القطع الصلبة (Hardware)، والقطع المرنة أو البرمجيات (Softeware) وكذا معطيات المعلومات أو البيانات (Données Informatiques) وهو العنصر الذي يتوزع بين القطع الصلبة والبرمجيات[3].

---

1- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية ،أطروحة لنيل شهادة الدكتوراه في العلوم، جامعة أبو بكر بلقايد تلمسان سنة 2018.ص25.

2- نفس المرجع ص 22

3- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية ،أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو سنة 2018.ص59.

## المطلب الثاني

## معاينة محل الجرائم الواقعة داخل وخارج النظم المعلوماتي

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة، وهي من أهم إجراءات التحقيق على الإطلاق، نظرا لما قد توفره من أدلة إثبات وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الإلكترونية، والهدف من المعاينة هو ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها، كما يتعين على ضابط الشرطة القضائية حراسة هذه الأماكن مع ضرورة إخطار النيابة العامة بهذا، لذا سنتطرق إلى مفهوم المعاينة (فرع أول) ومعاينة مسرح الجريمة الإلكترونية (فرع ثان).

### الفرع الأول: مفهوم المعاينة

تعرف المعاينة بأنه إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في الكشف عن الحقيقة، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقيقة أو بناء على طلب من الخصوم، والأصل أن تجري المعاينة بحضور أطراف الدعوى الجزائية غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة [1].

وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة، والتي تكون دائما محل ثقة سلطات التحقيق والقضاء ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون انحياز أو تعديل أو نقصان [2].

---

[1]- براهيمي جمال، مرجع سابق.ص56.

[2]- نفس المرجع، ص 57.

## الفرع الثاني

## معاينة مسرح الجريمة الإلكترونية.

تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة ولمعاينة مسرح هذه الجرائم يجب التفرقة بين حالتين:

### أولا: معاينة الجرائم الواقعة على المكونات المادية للجهاز.

تتم المعاينة في جهاز الإعلام الآلي كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها، والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

### ثانيا: معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها.

المكونات غير المادية هي برامج الجهاز وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينات أو فائدتها وهذه الصعوبات يمكن تلخيصها فيما يلي:

1. نقص و قلة الآثار المادية التي تقع على المكونات غير المادية للجهاز.

2. تردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة، والتي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة و الكشف عنها[1] .

1 .ماجد ياقوت ،أصول التحقيق ،دراسة مقارنة ،الطبعة الثالثة ،منشأة المعارف ،الإسكندرية بدون سنة النشر، ص 70.

## المطلب الثالث
## القواعد الإجرائية لمعاينة مسرح الجريمة الإلكترونية

هي جملة من الإجراءات المطبقة في كافة الجرائم، إلا أن التشريع الجزائري ينص على جملة من القواعد التي تعد وجوبية للقيام بالمعاينة، فأجاز المعاينة في الجنح وجعلها وجوبية في الجنايات، وهي قد تتم في مكان عام أو خاص، فإذا كانت في مكان عام فضابط الشرطة القضائية لا يحتاج أي إذن ندب سلطة تحقيق بإجراءاتها أما إذا كان خاص فلابد من شروط خاصة.

إذ أن الجرائم التي تقع في الوسط الإلكتروني أو داخل المنظومة المعلوماتية لها أساليب خاصة، نص عليها المشرع الجزائري من خلال نصوص قانون الإجراءات الجزائية والمتمثلة في إخطار وكيل الجمهورية (فرع أول) وأوقات إجراء المعاينات (فرع ثان) بالإضافة إلى رضا صاحب السكن (فرع ثالث).

### الفرع الأول: إخطار وكيل الجمهورية.

لا يمكن معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضابط الشرطة القضائية، وهذا ما نصت عليه المادة 42 من قانون الإجراءات الجزائية [1].

وعملا بنص المواد18 و32 و42 و63 من قانون الإجراءات الجزائية، بالإضافة إلى نص المادتان 42 و49 من قانون القضاء العسكري من واجبات ضباط الشرطة القضائية إذا ما علموا بأية جريمة بأن يقوموا بإخطار وكيل الجمهورية سواء كان مدنيا[2]

1- أحمد حزيط ،الوجيز في الإجراءات الجزائية ،الطبعة الثانية منقحة، دار هومة، الجزائر،2015، ص 38.
وأنظر المادة 42 من الأمر رقم 66-155 مؤرخ في 8 يوليو سنة 1966 يتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالقانون 07/17 المؤرخ في 27 مارس 2017 ج ر، ع 20 الصادرة بتاريخ 29 مارس2017.

2- حمزة نجاة، مرجع سابق، ص19

أو عسكريا باعتباره المسؤول المباشر عن الشرطة القضائية، على أن يكون الإخطار مسبوقا بتأكيد ضباط الشرطة القضائية من وقوع الجريمة فعلا.

كما أن الإخطار يكون باستعمال كافة الوسائل المتداولة عليها، فقد يكون بالكتابة أو باستعمال الهاتف النقال أو عن طريق أجهزة أخرى كالفاكس.

## الفرع الثاني: أوقات المعاينات

ألزم المشرع الجزائري ضباط الشرطة أخذ الإذن من وكيل الجمهورية المختص من أجل الدخول إلى منازل الأشخاص للقيام بالتفتيش والمعاينات، فنطبق هذه القواعد عند الانتقال لمعاينة الجرائم الإلكترونية، حيث يجوز إجراء المعاينات في النظم المعلوماتية في كل ساعات النهار والليل، وفي محل سكاني أو غير سكاني بناء على إذن مسبق من وكيل الجمهورية المختص[1].

وبالرجوع إلى نص المادة 47 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري أجاز إجراء المعاينة والتفتيش والحجز، في كل محل سكني أو غير سكني وفي كل ساعة من ساعات النهار أو الليل دون تأخير هذه الإجراءات، عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما يجوز لضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك [2].

1 -أحمد حزيط ، مرجع سابق ،ص 39.

2- راجع المادتان 47 و49 من قانون الإجراءات الجزائية الجزائري.

## الفرع الثالث: رضا صاحب المسكن

لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المشتبه فيها إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، أو يجب أن يكون هذا الرضا صريحا وكذلك الشأن بخصوص الجرائم الواقعة على النظم المعلوماتية، وهذا ما نص عليه المشرع الجزائري في نص المادة 64 من قانون الإجراءات الجزائية[1].

و لنجاح المعاينة في الجرائم المعلوماتية يجب إتباع ومراعاة القواعد الفنية والمتمثلة فيما يلي:

– القيام بتصوير الجهاز وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة، مع التركيز على تصوير أجزائه الحلقية وملحقاته ومراعاة التاريخ والزمان والمكان الذي التقطت فيه كل صورة .

– يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات ( الخيوط الكهربائية للجهاز) اللازمة، للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.

– وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي على المسئولين بها ودور كل واحد منهم.

–ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

–إبعاد الموظفين والفضوليين على أجهزة الإعلام الآلي وكذلك عن الأماكن التي توجد بها أجهزة أخرى[2].

---

[1]– راجع المادة 64 من قانون الإجراءات الجزائية.

[2]- امحمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لقانون الإجراءات الجزائية وقانون الوقاية من جرائم الاعلام...) ،سنه 2016.ص 66.

-عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة.

- التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، بالإضافة إلى رفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة .

-القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الجهاز الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها.

-يجب أن تقتصر مباشرة عملية المعاينة على مأمور بالضبط والباحثين، ممن تتوفر فيهم الكفاءات العلمية والخبرة الفنية في مجال جهاز الإعلام الآلي، واسترجاع المعلومات وممن تلقون التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[1].

[1]- امحمدي بوزينة أمنة ،مرجع سابق.ص67.

## المبحث الثاني

## إجراءات التفتيش والحجز في النظم المعلوماتية

إن التفتيش والحجز غرضهما ضبط الأدلة المادية للكشف عن الجريمة ومرتكبيها، فكل ما يضبط بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، يكون نتيجة الحجز لتحقيق الأثر المادي للجريمة.

وللجريمة المعلوماتية عدة إجراءات تطبق أصلا على الجرائم التقليدية في حالة التفتيش والحجز، إلا أن المشرع الجزائري في قانون الإجراءات الجزائية أعطى للجرائم الماسة بالأنظمة الآلية المعالجة للمعطيات بعض الاستثناءات بخصوص إجراءات التفتيش والحجز[1] ، وهذا ما سنتطرق إليه من خلال إجراءات تفتيش نظم الحاسوب المنطقية (مطلب أول) والقواعد الإجرائية للتفتيش والحجز (مطلب ثان) بالإضافة إلى بعض البرامج المستخدمة أثناء المعاينة والتفتيش والحجز (مطلب ثالث).

[1]– احمد حزيط، مرجع سابق، ص 40.

## المطلب الأول
## إجراءات تفتيش نظم الحاسوب المادية و المعنوية.

يعرف التفتيش بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الإبتدائي أو القضائي، الغرض منه البحث عن الأدلة المتعلقة بالجريمة للوصول إلى الحقيقة في متابعة أي شخص يشتبه في أنه ارتكب الجريمة، والتفتيش في الجريمة الإلكترونية ينقسم إلى التفتيش في نظم الحاسوب المادية الذي سنتطرق له (فرع أول)، والتفتيش في نظم الحاسوب المعنوية والذي سنتناوله (فرع ثان).

### الفرع الأول: التفتيش في نظم الحاسوب المادية.

إن عملية التفتيش تكون على المكونات المادية بأشكالها المختلفة للتفتيش، أي شيء يتصل بجريمة معلوماتية يمكن الكشف عنها وعن مرتكبيها، يدخل في نطاق التفتيش التقليدي وفقا لقانون الإجراءات الجزائية الجزائري والمعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات والمتمثلة أساسا في:

– إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

–إذا كانت مكونات الكمبيوتر منعزلة عن غيرها من أجهزته أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في نظام آخر فإن عملية الكشف تصبح صعبة جدا وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن آخر يتعين مراعاة القيود والضمانات التي أوجبها المشرع الجزائري على التفتيش داخل النظم المعلوماتية والتي تضمنها قانون الإجراءات الجزائية[1].

[1]– عبد القادر عدو،الجريمة الإلكترونية إجرائيا ،الطبعة الثانية ،دار هومة ، الجزائر، 2016، ص 80.

كذلك وأنه إذا وجدت مكونات مادية محمولة لجهاز الكمبيوتر في الأماكن العامة بطبيعتها، كالمطاعم والسيارات كسيارات الأجرة..... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص على حالات التفتيش في الأماكن العامة، أي تطبيق قواعد التفتيش في الأماكن العامة على الجرائم التي تقع في داخل النظم المعلوماتية [1] .

## الفرع الثاني: التفتيش في نظم الحاسوب المعنوية.

إن الكيان المنطقي لجهاز الكمبيوتر هو مجموعة الأساليب والقواعد وكذا البرامج، أو بصورة أدق الوثائق المتعلقة بتشغيل وحدة معالجة البيانات، وهو جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي، كبرامج ونظم التشغيل وقواعد البيانات ... الخ، ولقد ثار الخلاف في التشريعات المقارنة حول مسألة ضبط وتفتيش المكونات المعنوية والمنطقية للجهاز والإجراءات القانونية للحجز والتفتيش داخل النظم المعلوماتية، وبالأحرى ضبط المكونات المعنوية أو المنطقية للحاسوب[2] .

كما أن الطابع المعنوي للبيانات والمعلومات المخزنة على جهاز حاسوب المتهم، والتي يمكن القيام بتفتيشها، فيكمن الإشكال هنا في حالة ما إذا كان هذا الجهاز متصل بجهاز آخر داخل الدولة أو خارجها، فهل يجوز إجراء التفتيش والكشف عن الوسائط الإلكترونية ؟

وبالتالي يرى البعض أن التفتيش يمتد إلى سجلات البيانات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة ضرورية لإظهار الحقيقة[3].

1 – عبد القادر عدو ،مرجع سابق،ص81.

2– نفس المرجع، ص83.

3– ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الجنائي للأعمال كلية الحقوق بجامعة العربي بن مهيدي أم البواقي، سنة 2015.ص 16.

وهو ما تبناه القانون المقارن حول تفتيش الأنظمة المعلوماتية، فقد منحت المادة 251 من قانون الإجراءات اليوناني، سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع الدليل، وكذلك المادة 487 من القانون الكندي والإنجليزي والفرنسي وفي الولايات المتحدة الأمريكية[1].

فتعددت الآراء في هذا الشأن حيث ذهب رأي إلى أن الغاية من التفتيش هي ضبط الأشياء المادية التي تفيد في الكشف عن الحقيقة، فهذا المفهوم يجب أن يمتد ليشمل البيانات الإلكترونية أي إعطاء لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، تفسيرا لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو لمعالجة آلية أو إلكترونية، بما فيها البيانات المخزنة في حاملات البيانات المادية أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمر الخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل أمام المحاكم [2] .

و لقد أجاز المشرع الجزائري من خلال القواعد الإجرائية التي نص عليها في قانون الإجراءات الجزائية على إمكانية التفتيش والحجز على مكونات الجهاز، إن لم يحدد أي نظام يمكن الحجز عليه أو تفتيشه منطقيا أو معنويا، إلا أن التعامل مع هذه الجريمة يتم وتقنين النظم المنطقية والمعنوية ويتم الحجز على الوسائل المادية للحاسوب.

[1]- ابتسام بغو، مرجع سابق، ص17.

2- صرشي نورة ،مكافحة الجريمة المعلوماتية مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة الجزائر ،سنة 2012.ص 55.

## المطلب الثاني

## القواعد الإجرائية للتفتيش والحجز.

التفتيش هو إجراء من إجراءات التحقيق يهدف إلى ضبط أدلة الجريمة موضع التحقيق وكل ما يفيد في الكشف عن الحقيقة، وذلك وفقا لقواعد إجرائية تتلخص هذه القواعد في إجراء الإذن (فرع أول) وإجراء التفتيش والحجز يكون بحضور أشخاص معينين قانونا (فرع ثان) ومواعيد التفتيش والحجز (فرع ثالث) ورضا المشتبه فيه بالتفتيش (فرع رابع) بالإضافة إلى تحرير محاضر خاصة بالتفتيش والحجز (فرع خامس).

### الفرع الأول: إجراء الإذن.

لم يشترط المشرع الجزائري كقاعدة عامة الإذن في تفتيش المنظومة المعلوماتية لكن طبق عليها القواعد التقليدية في حالة ما إذا تعلق بالانتقال إلى منزل المشتبه فيه من أجل تفتيش منظومة معلوماتية، فتطبق في هذه الحالة القواعد الخاصة بتفتيش المنازل والأماكن الخاصة، إذ ألزم المشرع إذن مكتوب صادر عن وكيل الجمهورية المختص من أجل القيام بإجراء التفتيش وإلا اعتبر التفتيش تعسف[1].

و يمكن التفرقة بين حالتين:

**الحالة الأولى:** الانتقال لتفتيش منظومة معلوماتية في الأماكن الخاصة، ويطبق على إجراء تفتيش الأماكن الخاصة كالمنازل ( بإذن مكتوب).

[1] - عبد القادر عدو، مرجع سابق، ص 86.

**الحالة الثانية:** الانتقال لتفتيش منظومة في مكان عام كمقهى أو ساحة عامة تطبق عليها نفس القواعد التي تطبق على تفتيش الأماكن العامة (لا وجود للإذن...)، ولقد نص المشرع على الإذن في الدخول إلى الأماكن الخاصة في نص المادة 44 من قانون الإجراءات الجزائية.

يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها و تفتيشها و إجراء الحجز فيها، وذلك تحت طائلة البطلان[1].

## الفرع الثاني: إجراء التفتيش والحجز بحضور أشخاص معينين قانونا.

من بين هذه الأشخاص المشتبه فيه، المتهم، القائم بالتفتيش، والشاهدين، فالأصل في التفتيش وكما عرفته القواعد الخاصة بالتفتيش يتم هذا الأخير بحضور المتهم أو من يجوز أن يمثله، وضابط الشرطة القضائية القائم بالتفتيش، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين للسلطة، إلا أن المشرع الجزائري استثنى على هذه القواعد في نص المادة 45 من قانون الإجراءات الجزائية الجزائري على أنه لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذ يمكن تفتيش المنظومة المعلوماتية بدون حضور المتهم أو الشاهدين [2] .

[1] أنظر المادة 44 من قانون الإجراءات الجزائية الجزائري.

2 - ناصر جوادي ،إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، دار العلوم، الطبعة الثالثة الجزائر سنة 2011 ،ص 47.

## الفرع الثالث: مواعيد التفتيش و الحجز.

كقاعدة عامة بخصوص الجرائم التقليدية فإن تفتيش الأماكن الخاصة لا يكون قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، والعبرة بساعة الدخول إلى المنزل إلا إذا طلب صاحب المنزل ذلك، واجهت نداءات من داخل المنزل فهو سبب من أسباب الإباحة الإجرائية للدخول إلى المنازل.

غير أن تفتيش المنظومة المعلوماتية لا يخضع لهذه القواعد إذ نص المشرع على أنه يجوز إجراء التفتيش والحجز في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في كل ساعة من ساعات النهار والليل، بناءا على إذن مسبق من وكيل الجمهورية المختص وهذا ما نصت عليه المادة 47 فقرة 3 ق.إ.ج، كونها حالة من الحالات الاستثنائية التي أقرها القانون[1].

كما أن المكونات المعنوية للحاسوب الآلي وشبكة الاتصال قد تكون عرضة للإخفاء أو التغيير أو التدمير أو التلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كاستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة[2].

---

1 - ناصر جوادي ، مرجع سابق، ص 48، وأنظر المادة 3/47 من قانون الإجراءات الجزائية الجزائري.

2- معمش زهية/غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص والعلوم الجنائية كلية الحقوق بجامعة عبد الرحمان ميرة بجاية، سنة 2012، ص 25، و راجع المادة 47 مكرر من قانون الإجراءات الجزائية الجزائري.

## الفرع الرابع: رضا المشتبه فيه بالتفتيش.

لا يجوز تفتيش المساكن أو حجز الأشياء المثبتة للمتهم إلا برضا صريح من الشخص الذي ستنفذ هذه الإجراءات و يجب أن يكون هذا الرضا مكتوب بخط يده أو من استعان به أو اختاره في حالة عدم قدرته على الكتابة شريطة اختيار بنفسه لهذا الشخص و يذكر ذلك في المحضر مع الإشارة إلى ذلك في محضر التفتيش و الحجز، غير أنه عندما يتعلق الأمر بالتحقيق في جريمة ماسة بالأنظمة المعلوماتية فتطبق الأحكام المنصوص عليها في نص المادة 47 مكرر من قانون الإجراءات الجزائية الجزائري.

وحسب المادة 45 من قانون الإجراءات الجزائية فتتم عمليات التفتيش التي تجرى طبقا للمادة 44 أعلاه على الوجه الآتي:

– إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له.

و إذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته[1].

1 – راجع المادة 47 مكرر و المادتان 44 و45 من قانون الإجراءات الجزائية الجزائري.

– إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا وأشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش وإن تعذر ذلك أتبع الإجراء المنصوص عليه في الفقرة السابقة.

ولضابط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى أعلاه الحق في الإطلاع على الأوراق أو المستندات قبل حجزها.

## الفرع الخامس: تحرير محاضر التفتيش والحجز.

المحاضر هي عبارة عن ملخص وافي وبسيط عن الواقعة، ويتضمن إثبات جميع ما قام به المحقق من إجراءات قانونية وفنية من أجل كشف الغموض عن الواقعة، وضبط الأدلة[1]..... ويكون بتكليف القائم بالتفتيش باصطحاب كاتب من أعون الضبط القضائي يحرر محضر خاص بالتفتيش سواء كان ايجابيا أو سلبيا ويتم تسجيل فيه جميع وقائع التحقيق والتفاصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل دقة وأمانة [2] .

وأوجب القانون على المحقق أن يوقع على المحاضر وكذلك الحال بالنسبة للكاتب، ويجب أن يتم التوقيع على كل صفحة من صفحات المحاضر وهذا فضلا عن نهاية المحضر، وذلك لإبعاد أية شبهة كالتزوير على أنه بالنسبة للكاتب يكفي توقيعه مع المحقق في نهاية محضر التحقيق، لأن الثقافة القائمة بالمحضر مستمدة من توقيع عضو النيابة العامة[3].

1- ابتسام بغو، مرجع سابق، ص44.
2 - غرداين حسام،الجريمة الالكترونية والإجراءات التصدي لها ،مذكرة لنيل شهادة الماستر كلية الحقوق جامعة الجزائر سنة 2015.ص87 .
3 - ابتسام بغو، مرجع نفسه، ص47.

أما بالنسبة للحجز فبالرجوع إلى نص المواد **44، 45، 47** و ما يليها من قانون الإجراءات الجزائية نجد أن المشرع الجزائري لم يحدد قواعد خاصة بالحجز داخل المنظومة المعلوماتية بل اشترط نفس القواعد المطبقة على التفتيش داخل هذه المنظومة، أي أنه لم يحدد طبيعة الحجز إما على البيانات المنطقية أو المعنوية من جهة أو على الوسائل المادية كجهاز الكمبيوتر ولواحقه، إلا أنه من الجانب الميداني تطبق القواعد المنصوص عليها في قانون الإجراءات الجزائية، أي لا تزال تطبق إجراءات الحجز التقليدي على الجرائم المعلوماتية وهو الحجز على الوسائل المادية[1] .

## المطلب الثالث

## بعض البرامج المستخدمة أثناء المعاينة والتفتيش والحجز.

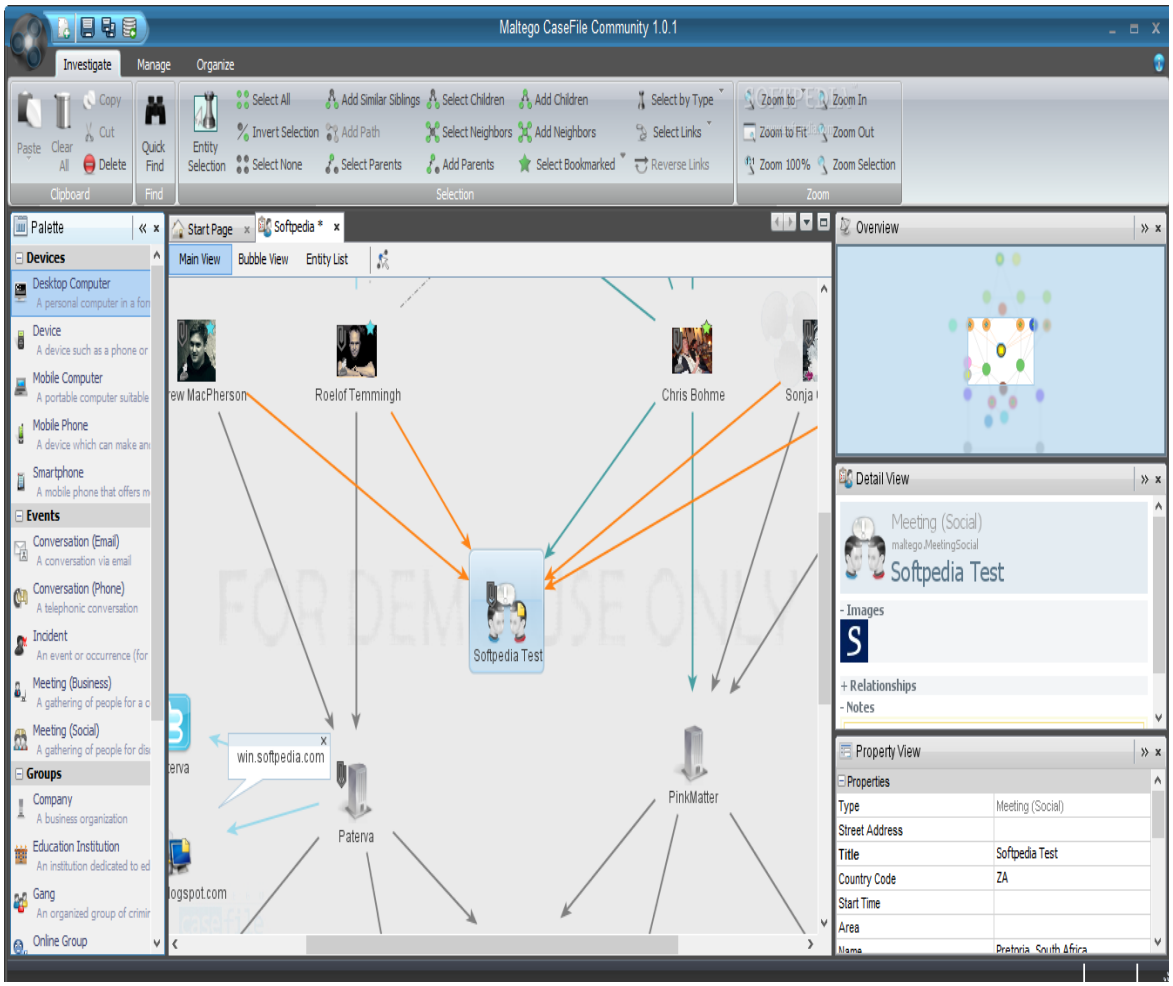
إن الجهات المكلفة بإجراءات التحري التقليدية للكشف عن الجريمة متعودة في التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات أو آثار أقدام أو بقع دم أو محررات مزورة...، ولما كانت الجريمة المعلوماتية تقع في عالم افتراضي لا تخلف أي آثار مادية محسوسة [2] وجب على الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين استخدام بعض البرامج التي تساعدهم في الكشف عن الجريمة المعلوماتية في جانبها التقني، من خلال تحليل البيانات والمعطيات الموجودة في الملفات وكشف جميع جوانبها وجذورها مع إظهار المخفية منها وفك التشفير عن المشفرة واسترجاع المخلفات ..... من أجل الوصول إلى دلائل أخرى حيث سنتطرق إلى برنامج مالتيجو"Maltego " (فرع أول) وبرنامج فورنسيك " Forensic " (فرع ثان).

1 غرداين حسام، مرجع سابق ص88.

2- سعيداني نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة باتنة ،سنة 2012.ص 04.

## الفرع الأول: برنامج مالتيجو "Maltego "

يعتبر برنامج Maltego واحدا من أفضل وأقوى البرامج الخاصة بعمل Information Gathering وجمع المعلومات عن الهدف الذي نريد معرفة بعض المعلومات عنه، وله قدرة كبيرة على جمع المعلومات المتعلقة بشخص أو عدة أشخاص بالإضافة إلى صلة الوصل بينهم بالاعتماد على الايميل، الشبكات الاجتماعية، الموقع الالكتروني وحتى رقم الهاتف والكثير الكثير من الأمور الأخرى، كما هو موضح في الصورة أدناه[1].




1.نضال أدمين، منتدى برامج الكمبيوتر والأنترنيت، على الرابط http://nidhal-technologie.own0.com/t60-topic
تاريخ الإطلاع 2019/07/10

وبرنامج Maltego هو عبارة عن أداة تفاعلية لاستخراج البيانات والمعلومات حيث تقدم رسومات بيانية توضيحية موضحة تسلسل ارتباط البيانات والمعلومات ببعضها البعض، مما يعني أنها تساعد في أيجاد الأمور المشتركة بين أجزاء مختلفة من المعلومات التي يمكن الحصول عليها من الشبكة العنكبوتية، ويستخدم في التحقيقات عبر هذه الشبكة للعثور على العلاقات بين أجزاء المعلومات من مصادر مختلفة موجودة على الانترنت، فمثلا تمكنك من إيجاد العلاقات بين: الأسماء – الأسماء المستعارة- عناوين البريد الالكتروني – الشبكات الاجتماعية الشركات والمنظمات – أسماء - والملفات وغيرها ...إلخ[1].

## الفرع الثاني: برنامج فورنسيك " Forensic "

الـ Forensic بمفهومه الشامل هو الجرائم، لكن هذه الجرائم يتم تقسيمها حسب أصناف معينة، منها الخاصة بالقتل و منها الخاصة بالسرقة والجنايات وما إلى ذلك، لكن خصص قسم خاص بالجرائم الإلكترونية، وهو ما يطلق عليه بـ Digital Forensic، وهو المتعلق بموضوعنا اليوم، بحيث يقوم على تعقب وحجز الأعمال والمهمات غير المشروعة و غير القانونية والتي يتم ممارستها باستخدام الشبكة العنكبوتية أو الأجهزة الإلكترونية (شاملة كل الأجهزة ) [2].

1.مهند- أدوات جمع المعلومات، على الرابط https://th3expert.net/maltego تاريخ الإطلاع 2019/07/15
2. رضا دحان، كل ما تحتاج معرفته حول الـ Digital Forensic و الجرائم الإلكترونية و كيفية احترافها، على الرابط https://www.aqweeb.com/2016/08/All-About-digital-forensic.html تاريخ الإطلاع 2019/10/15

يقوم مجموعة من المحترفين في مجال المعلوماتية بالسهر على القيام بعمل الـ Forensic ، أغلبهم من White Hackers أو Ethical Hackers إن صح التعبير، إذ هؤلاء الأشخاص لديهم خبرات كافية و قوية من أجل المساهمة في كشف وإبطال الأعمال غير القانونية السائرة ضمن الشبكات العنكبوتية[1].

كما يقوم برنامج Forensic بتصوير القرص بواسطة حزم برمجيات ونظرًا إلى أن هذه الحزم مصمَّمة للمحققين الجنائيين، فإنها تتضمن أدوات لنحت الملف (أي تجميع ملف كامل من بيانات مجزأة)، كما أنه يقوم بأعمال التحري والفحص للأدلة الرقمية واخذ نسخ منها وتجميعها وتحليلها وفك التشفير واستعادة الملفات المحذوفة وكلمات المرور وتحليل البريد الالكتروني والبحث المتقدم، وتوليد تقارير لاستخدامها في المحكمة[2].

1 .رضا دحان، مرجع سابق، تاريخ الإطلاع 2019/10/15

2.إيناس محمد راضي، الأجهزة التحليلية الحديثة في كلية علوم الأدلة الجنائية، على الرابط http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid تاريخ الإطلاع 2019/07/12

وترتيبا على ما سبق ذكره فإن الجريمة المعلوماتية هي من جرائم العصر، بحيث أن أغلب الجرائم المرتكبة تستعمل فيها منظومة معلوماتية من جهاز حاسوب أو هاتف نقال وغيرها، وتتطلب لارتكاب هذه الجريمة وسائل معلوماتية ذات تقنية عالية بالإضافة إلى ذكاء وخبرة المجرم في هذا المجال، وفي هذا الفصل تم التطرق إلى إجراءات التحري عن الجرائم المعلوماتية وفق ما هو منصوص عليه في قانون الإجراءات الجزائية.

ومن هذه الإجراءات معاينة مسرح الجريمة المعلوماتية التي تتم من خلال معاينة المكونات المادية للجهاز ومعاينة الجرائم الواقعة في النظم المعلوماتية، كما يمكن أن تقترن الجريمة المعلوماتية بجريمة أخرى مثل الانتحار في قضية الحوت الأزرق.

بعدها تم التطرق إلى الإجراءات القانونية للتفتيش الحجز بحيث وجدنا أن المشرع الجزائري لم يحدد الغاية من التفتيش في الجرائم المعلوماتية هل يقع على المنظومة المعلوماتية أم للوصول فقط إلى الوسائل المستعملة لارتكاب الجريمة في حد ذاتها، كما أنه لم يحدد أيضا طبيعة الحجز إما على البيانات المنطقية من جهة أو على الوسائل المادية كجهاز الكمبيوتر ولواحقه من جهة أخرى.

# الفصل الثاني:
# إجراءات التحري المستحدثة للكشف عن الجرائم داخل المنظومة المعلوماتية.

إن الإجراءات المطبقة على الجرائم المنصوص عليها في قانون الإجراءات الجزائية لم تعد تجدي نفعا لمواجهة الجرائم المعلوماتية نظرا لخصوصية هذه الجرائم، والتي تقع في عالم خاص، فالمشرع الجزائري سارع إلى مواكبة هذا التطور بإصدار تشريع جديد ألا وهو القانون 04/09 الصادر في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009[1]، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بحيث تضمن قواعد إجرائية جديدة تكمل القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية بخصوص التفتيش والحجز وكذلك المراقبة التي تقع على هذه الجرائم .

وعليه يمكن دراسة هذا القانون دراسة تحليله لمضمونه قبل التطرق للأحكام التي تستوجب التفصيل فيها.

**أولا:** نص على الأحكام العامة التي تبين الأهداف المتوخاة من هذا القانون وتحديد مفهوم المصطلحات التقنية ومجال تطبيق أحكامه، وتضمن الأشخاص أو الكيانات العامة أو الخاصة التي تقدم خدمات للاتصالات بواسطة المنظومة المعلومة أو لنظام الاتصال.

**ثانيا:** جسد الأحكام الخاصة بمراقبة الاتصالات الالكترونية إذ يراعى فيها التهديدات المحتملة وأهميته للمصالح المحمية، إذ نص القانون على أربعة حالات يسمح فيها للسلطات الأمنية مراقبة الاتصالات والمراسلات الالكترونية وجاءت على سبيل الحصر[2] .

**ثالثا:** تضمن القواعد الإجرائية الخاصة بالتفتيش والحرز في مجال الجرائم الالكترونية والتي سلطنا عليها الضوء من خلال مضامين هذا الفصل وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، مع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة إلا أن المشرع الجزائري بإحالته إلى هذا الأخير قضى على مبدأ من مبادئ القانون والتي تنص على أن القاعدة الخاصة تقيد العامة في جميع الأحوال، إذا أصبح القانون 04/09 السالف الذكر يتقيد بالقواعد العامة لقانون الإجراءات الجزائية وقانون العقوبات.

**رابعا:** تطرق فيه إلى التزامات المتعاملين في مجال المعلوماتية بتحديد هذه الالتزامات لاسيما إلزامية حفظ المعطيات المتعلقة بحركة سير، والتي من شانها المساعد في الكشف عن

1 - قانون رقم 04/09 الصادر في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج ر عدد 47 المؤرخة في 16 غشت سنة 2009

2- حسين نوارة، مظاهر الاعتداء على الحياة الخاصة، الملتقى الوطني حول تأثير التطور العلمي والتقني على حقوق الإنسان ،كلية الحقوق جامعة عبد الرحمان ميرة بجاية 2009 ،ص 46

الجرائم الواقعة في الصرح المعلوماتي وكذلك مرتكبيها، وألزم القانون مقدمي خدمات الانترنت التدخل الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة لمخالفتها القانون أو جعل الدخول إليها أمر غير ممكن[1] .

**خامسا:** أشار إلى الهيئة الوطنية للوقاية من الجرائم المعلوماتية ومكافحتها وتمت الإحالة إلى التنظيم الذي حدد كيفيات تشكيل هذه الهيئة.

**سادسا:** لقد نص هذا على التعاون والمساعدة القضائية الدولية وتناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام.

فيما يخص الاختصاص القضائي تم توسيع اختصاص المحاكم الجزائية للنظر، في هذه الجرائم ولو ارتكبت من طرف الرعايا الأجانب عندما تكون المصالح الإستراتيجية للجزائر مستهدفة.

أما فيما يتعلق بالتعاون والتبادل الدولي فيقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي فيما يخص مكافحة هذه الجرائم خاصة ما يتعلق بالمساعدة والتبادل للمعلومات حيث تم اعتماد التعاون على أساس مبدأ المعاملة بالمثل[2].

إن صدور هذا القانون كان نتيجة القصور الذي عرفه القانون 15/04 المؤرخ في 10 نوفمبر 2004[3] الذي نص على الحماية الموضوعية، وذلك في قانون العقوبات الجزائري أما بخصوص الجانب الإجرائي الخاص بمكافحة هذه الجرائم فلم يتضمن النصوص التي سبقت القانون 09|04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الإجراءات الجزائية من جهة أخرى والتي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها وعليه سوف نحدد من خلال هذا الفصل القواعد المستحدثة التي جاء به هذا القانون والمتمثلة في مراقبة الاتصالات الالكترونية (مبحث أول) وقواعد التفتيش والحجز في النظم المعلوماتية وتطبيقاتها في دراسة حالة (مبحث ثان).

---

1. حسين نوارة، مرجع سابق، ص 47
2. عبد القادر عدو، مرجع سابق، ص 89
3. أنظر القانون رقم 15/04 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري المؤرخ في 08 جوان1966 ج ر عدد 71.

# المبحث الأول

# مراقبة الاتصالات الإلكترونية.

سارع المشرع الجزائري بتعديله لقانون الإجراءات الجزائية تماشيا مع تطور المعلوماتية الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الجرام، حيث وضع القواعد والأحكام الخاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها.

وردت هذه الأساليب في قانون الإجراءات الجزائية المعدل والمتمم بموجب قانون 22/06 الصادر في سنة 2006 [1] وقانون الوقاية من الفساد ومكافحته 01/06 المؤرخ في 20 فيفري 2006 [2] والقانون 04/09 [3] بخصوص قواعد الاختصاص المحلي، لذلك لابد من شرح هذه الأساليب و كيفية إجراء المراقبة الالكترونية وكذلك أساليب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وكذلك أسلوب التسرب مع ذكر الحالات التي يمكن اللجوء فيها إلى المراقبة الالكترونية[4] حيث سنتطرق في هذا المبحث إلى توسيع الإجراءات الخاصة بالاختصاص الإقليمي (مطلب أول) وتجميع الاتصالات الإلكترونية ومراقبتها (مطلب ثان) بالإضافة إلى حالات المراقبة الإلكترونية (مطلب ثالث) .

---

1- قانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو 1966 والمتضمن ق إ ج ج، ج ر عدد 84المؤرخة في 04 ذو الحجة عام 1427 الموافق لـ 24 ديسمبر 2006.

2- قانون 01/06 المؤرخ في 21 محرم عام 1427 الموافق لـ 20 فبراير سنة 2006، يتعلق بالوقاية من الفساد ومكافحته ج ر عدد 14 المؤرخة في 08 صفر 1427 الموافق لـ 08 مارس 2006.

3- قانون 09 /04 مرجع سابق.

4– ناصر جوادي ،إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري، دار العلوم، الطبعة الثالثة الجزائر سنة 2011،ص 63.

## المطلب الأول
## توسيع الإجراءات الخاصة بالاختصاص الإقليمي.

بالرجوع إلى قانون الإجراءات الجزائية نجده يجيز تمديد الاختصاص المحلي والنوعي للمحاكم الجزائرية من خلال نص المادة 329 الفقرة الأخيرة حيث تجيز تمديد الاختصاص المحلي للمحاكم ليشمل اختصاص محاكم أخرى، وذلك عن طريق التنظيم في الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات (المرسوم التنفيذي رقم 348/06 المؤرخ في 05 /10 /2006).

أنشئت كذلك الأقطاب القضائية المتخصصة بموجب القانون 14/04[1] المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم المعلوماتية التي تختص المحاكم وذلك حسب المواد 37، 40 و329 من قانون الإجراءات الجزائية [2].

كذلك نظم المشرع الجزائري في القانون 04/09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أحكام جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية والتي تتماشى والتطور الذي لحق هذه الجريمة، ومن بين هذه القواعد ما نصت علية المادة الثالثة التي تتضمن الإجراءات الجديدة حول التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى نص المادة 15 من القانون 04/09 التي نصت على أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائية الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي وتستهدف مؤسسة الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[3] .

1 أنظر القانون رقم 14/04 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155/66 المتضمن ق إ ج ج، ج ر عدد 71

2 محمد معمر الصغير، الوافي في الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الحديث، الجزائر، 2010, ص22.

3 ناصر جوادي، مرجع سابق، ص 65.

بالرجوع إلى نص المادة 37 من قانون الإجراءات الجزائية نجدها توسع من مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم تكن مرخصة لها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف كذلك تم سحب مبدأ الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع في هذا الشأن بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد، 144 مكرر، 144 مكرر 2 من قانون العقوبات الجزائري [1] .

وبالرجوع إلى المواد السالفة الذكر نجد أن المادة 144 مكرر تنص على أنه "يعاقب بغرامة 100.000 إلى 500.000 دج، كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سب أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراءات المتابعة التلقائية.

وفي حالة العود تضاعف الغرامة .

أما المادة 144 مكرر 02 :فقد قيدت النيابة العامة في إجراءات المتابعة بتلقائية الدعوة الجزائية ضد كل من أساء إلى الرسول صلى الله عليه وسلم أو بقية الأنبياء بأية شعيرة من شعائر الإسلام سواء عن طريق الكتابة أو الرسم أو التصريح أو بأية وسيلة أخرى.

تباشر النيابة العامة إجراءات المتابعة تلقائيا [2] .

---

[1] صرشي نورة، مرجع سابق، ص57

[2] قانون العقوبات العقوبات الجزائري المعدل والمتمم بالقانون رقم 16-02 المؤرخ في 14 رمضان 1437 الموافق لـ 19 يونيو سنة 2016 ج ر عدد 37 المؤرخة في 17 رمضان 1437 الموافق لـ 22 يونيو سنة 2016.

## المطلب الثاني
## تجميع الاتصالات الالكترونية و مراقبتها.

مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون 04/09 وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بالإجراءات الخاصة واللازمة لذلك.

أعطى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري، ألا وهو الدستور وهذه القواعد العامة التي تعنى بالحماية القانونية للحياة الخاصة للأفراد، وهو ما ينطوي عليه بضرورة حماية البيانات الشخصية للمعالجة الآلية، بحيث اعترف المشرع الجزائري في نص المادة 77 من الدستور على أن يمارس كل واحد جميع حريته في إطار احترام الحقوق المعترف بيها للغير في الدستور لا سميا احترام الحق في الشرف وستر الحياة الخاصة ... وأضافت نص المادة 46 من دستور 1996 على أنه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل شكل من أشكالها مضمونة [1].

إلا أنه في التعديل الدستوري لسنة 2016، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة 46 أعلاه تنصان على أنه لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطات القضائية ويعاقب القانون انتهاك هذا الحكم [2].

إذ يقصد بالأمر الذي يصدر من المحكمة هو الإذن بالمراقبة الإلكترونية بعد إخطار النيابة العامة المتمثلة في وكيل الجمهورية وكذلك الشأن بخصوص اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، كما أضافت الفقرتين الثالثة والرابعة في التعديل الأخير أنه يتم اقتناع المشرع بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات

---

[1] قانون رقم 01/16 المؤرخ في 26 جمادى الأولى عام 1437 الموافق ل .06 مارس سنة 2016، يتضمن التعديل الدستوري ج ر عدد63.

[2] محمد معمر الصغير، مرجع سابق , ص 26

الخاصة بالأشخاص الطبيعيين خلال المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بحماية البيانات ومسألة وقت وفقط خاصة في ضل النشاط التشريعي في العشرية الأخيرة.

وزارة البريد وتكنولوجيا الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حماية البيانات الشخصية على الانترنيت والذي يفترض أن يصدر قريبا، إن الإجراءات المتعلقة بالتحري والكشف عن الجريمة المعلوماتية في إطار المكافحة الإجرائية للجرائم المعلوماتية كما سبق ذكرهم تم توسيع مجال النيابة العامة في البحث والتحري عن هذه الجرائم بمنح الإذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور خاصة في المجال المعلوماتي[1] .

وقد نصت المادة 65 مكرر 5 من قانون الإجراءات الجزائية على أنه "إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو في الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جريمة تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية أن يأذن بما يلي :

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.
- يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن[2] .

[1] محمد معمر الصغير، مرجع سابق ،ص28.

[2] راجع قانون الإجراءات الجزائية الجزائري.

- إن الكشف عن الجرائم المعلوماتية بواسطة اعتراض المراسلات، وتسجيل الأصوات والتقاط الصور لا يتم إلا من خلال الشروط التي أوجبها المشرع الجزائري على ضابط الشرطة القضائية للقيام بهذه الصلاحية وخصوصا في الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات، إذ تعتبر إجراءات تباشر بشكل خفي على الرغم من تناقضها مع النصوص المقررة في حماية الحياة الخاصة والتقاط الصور يكون بالتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ويتم استخدام هذه الوسيلة في المحلات السكنية والأماكن العامة والخاصة .

- أما تسجيل الأصوات فيتم عن طريق وضع رقابة على الهواتف وكذلك الوسائل المعلوماتية وتسجيل الأحاديث التي تتم عن طريقها كما يتم أيضا عن طريق الميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، قد يتم عن طريق التقاط إشارات لاسلكية أو إذاعية.

إن مثل هذه الإجراءات يمكن أن تمس بالحقوق والحريات الشخصية خصوص إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون 04/09 المؤرخ في 05 أوت 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو مستلزمات الحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[1].

[1] - أحمد حزيط، مرجع سابق ،ص 74 .

كما يجوز إثبات أو نفي الاتهام عن المشتبه فيه، إعمالا بالقاعدة الجنائية "المتهم بريء حتى تثبت جهة قضائية إدانته" وذلك باللجوء إلى وسيلة التسجيل الصوتي واعتراض المراسلات أو التقاط الصور في الأماكن العامة أو الخاصة، وخصوصا أن هذه الإجراءات قد تمس بشخص المتهم أو المشتبه فيه ويمكن أن تتعدى ذلك لتمس كل من يحيط به من الأقارب أو معارفه، كما تجدر الإشارة إلا أن هناك فرق بين اعتراض المكالمات الهاتفية ووضع الخط الهاتفي تحت المراقبة فالأول يكون بدون علم أو رضا صاحب الشأن، أما الثاني فيكون برضاه وطلبه وبعلم صاحب الشأن وهذا تحت السلطة التقديرية للجهة القضائية بعد تسخير مصالح البريد والمواصلات لذلك[1].

ويعتبر هذا الإجراء حديث ومن أهم إجراءات التحقيق التي يمكن لضابط الشرطة القضائية من ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر5 من قانون الإجراءات الجزائية، تباشر الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل بمعنى أنها إجراء للتحري والتحقيق[2] .

وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على انه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة بعد أن صعب الوصول إليها بوسائل البحث العادية، فنجد أن المشرع حاول أن يوافق بين هذه المتعارضات بأن أجاز هذه الأساليب ولكن بضوابط، وهي مباشرة التحري بإذن من وكيل الجمهورية المختص والتزام أعوان وضباط الشرطة القضائية بإجراء بالسر المهني فالمشرع الجزائري على الرغم من إقراره بأساليب التحري الخاصة والتي قد تمس بحرمة حرية الحياة الخاصة إلا انه يعاقب في حالة اللجوء إلى استعمالها بطريقة غير مشروعة وعليه يمكن شرح الإذن والالتزام بالسر المهني كشرطين لمباشرة التحري[3].

## الفرع الأول: ضرورة الحصول على إذن مسبق لإجراء التحري.

يتم إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات بإذن من وكيل الجمهورية المختص وتباشر تحت مراقبة وكيل الجمهورية، وبالرجوع إلى المادة 04 من القانون 04/09 الذي جاء فيه انه لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطات القضائية المختصة.

---

[1] - محمد معمر الصغير، مرجع سابق، ص 36.

[2]- ناصر جوادي ،إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري ،دار العلوم ،الطبعة الثالثة الجزائر،سنة 2011 , ص 70

[3] عبد القادر عدو، مرجع سابق، ص 97

يحرر ضابط الشرطة القضائية عند مباشرة التحريات والتحقيقات محضر عن كل عملة اعتراض للمراسلات وتسجيل الأصوات والتقاط الصور وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها بعد أن يصنف وينسخ ضابط الشرطة القضائية المراسلات أو الصور أو المحادثات المسجلة أو المقيدة في إظهار الحقيقة في محضر يودع بملف، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء بمساعدة مترجم مسخر لهذا الغرض[1].

## الفرع الثاني:الالتزام بالسر المهني.

إن إجراءات التحري والتحقيق سرية كما نص عليها قانون الإجراءات الجزائية ومن ثم فإنها تعني القيام بقدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس لها هدفا كما كان عليه من قبل وهو تسهيل قمع المتهم بل صار وسيلة لضمان الحريات الشخصية، ولقد نص المشرع على أن عملية اعتراض المراسلة أو التقاط الصور تتم بمراعاة السر المهني ودون المساس به فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام السر المهني[2].

كما نص في قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية ما لم ينص القانون على خلاف ذلك ودون الإضرار بحقوق الدفاع وكل شخص يساهم في هذا الإجراء ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات، وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات تتم بالسرية المطلقة فيمنع منعنا باتا أن يجبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون بالعملية أن يفصح على مضمون

[1] ناصر جوادي، مرجع سابق, ص 70

2.حسني ثابت، الجريمة الاكترونية في ظل تطور تكنولوجيات المعلومات، على الخط :http:// kenona online .com
تاريخ الإطلاع 2019/07/03

محضر التحريات لأي شخص كان وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضابط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات لان سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة[1].

أدرج المشرع الجزائري تقنية جديدة أصطلح عليها بالتسرب في تعديله لقانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورة التحري والتحقيق في احدي الجرائم المذكورة في المادة 65 مكرر5 من قانون الإجراءات الجزائية، كما يجيز وكيل الجمهورية وتحت رقابته حسب الحالة لمباشرة عملية التسرب ضمن شروط محددة، ويشترط حصول الضابط المكلف بالتسرب على إذن من وكيل الجمهورية المختص بذلك، ثم يقوم بمنح الإذن المكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه وكل هذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوب يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضابط وأعوان الشرطة المأذون لهم بالتسرب، ويمكن استخلاص مواصفات الإذن بالتسرب وطبيعته من قانون الإجراءات الجزائية وهي :

- أن يسلم الإذن فقط لضرورة التحري أو التحقيق القضائي .
- أن يكون الإذن مكتوبا ومسببا.
- أن يذكر في الإذن طبيعة الجريمة التي يجب أن ينص عليها الإذن.
- يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته.
- يحدد فيه المدة المقررة للعملية والمحددة بأربعة أشهر وهي قابلة للتجديد لمدة 04 أشهر أخرى كل ما دعت الضرورة لذلك.
- أن تودع الرخصة أي الإذن في ملف الإجراءات بعد الانتهاء من عملية التسرب[2].

والتسرب المعلوماتي هو قيام ضابط الشرطة القضائية والأعوان المختصون الذين لهم مهمة المعاونة في العملية، التي ذكرتهم المادة 21 من قانون الإجراءات الجزائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بالتنسيق مع العملية بمراقبة الأشخاص المشتبه

[1] عبد القادر عدو، مرجع سابق، ص 101.

[2] غرداين حسام، مرجع سابق، ص 90.

فيهم، بإيهامهم انه شخص عام أو شريك معهم في العملية، فالتسرب إذا هو قيام المأذون له في التحقيق في الجريمة بمراقة الأشخاص المشتبه في ارتكابهم لجرائم ما أو إعدادهم لارتكاب هذه الجريمةّ، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم دون أن يكون مسئولا جزائيا وذلك بهدف مراقبة الأشخاص المشتبه فيهم والكشف عن أنشطتهم الإجرامية بإخفاء الهوية الحقيقية[1].

ولهذا يجوز لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسهرون لهذا الغرض دون أن يكونون مسئولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء وثائق أو منتجات أو معلومات متحصل عليها من ارتكاب الجرائم معينة (الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات) في المجال المعلوماتي .
- استعمال أو وضع تحت تصرف مرتكبي الجرائم المعلوماتية الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل المعلوماتي والتخريب أو الحفظ أو الاتصال بوسائل إلكترونية أخرى.
- يحضر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر[2] .
- هذا ما أكده المشرع بموجب المادة 65 مكرر 16 من قانون الإجراءات الجزائية بان نصت صراحة بأنه " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين يباشرون التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات"[3].

---

[1] غرداين حسام، مرجع سابق، ص 90.

2 فاطمة الزهراء خبازي، الجريمة الالكترونية في ظل الجرائم المرتبطة بتكنولوجيات المعلومات على الخط: salahgardafi .eb 2a .com.content. تاريخ الإطلاع 2019/07/08

3 أنظر قانون الإجراءات الجزائية الجزائري.

- لنجاح عملية التسرب وللكشف عن الجرائم المعلوماتية يلتزم المتسرب القيام بهذه العملية بكل الإجراءات المحددة قانونا وأهمها حصوله على الإذن المكتوب من قبل وكيل الجمهورية المختص بحيث يلتزم هذا الأخير بالإشراف والمراقبة على نجاح العملية، وكما يلتزم حفاظا على أمن وسلامة العملية بعدم الكشف عن هويته وذلك لخطورة مهمته التي تتطلب جرأة وكفاءة ودقة في العمل.

وعلى الرغم من إجازة المشرع الجزائري لمثل هذه الأفعال التي تعتبر في الحقيقة جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون مع ذلك، منع المشرع الضباط والأعوان من أن يحرضوا المشتبه فيهم على ارتكاب الجريمة، بمعني أنه على الضباط والأعوان المتسربين أن لا يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه إلى ارتكاب الجريمة فهذا الفعل ممنوع تحت طائلة بطلان الإجراءات[1].

## المطلب الثالث: حالات المراقبة الالكترونية.

نص القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة الرابعة منه على الحالات التي تسمح بتطبيق الإجراءات الجديدة المتمثلة في مراقبة الاتصالات الالكترونية وذلك على سبيل الحصر .

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريبية أو الماسة بأمن الدولة .
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية في إطار تنفيذ المساعدة القضائية المتبادلة[2].

1- أحمد حزيط ، مرجع سابق، ص 78.

2- محمد معمر الصغير، مرجع سابق، ص 88

- بتحليل هذه النقاط واستقراءنا لنص المادة، نجد أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها من خلال وضع المشتبه فيهم تحت المراقبة الالكترونية وهي على عكس المراقبة الشخصية والتي هي أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا انه من جهة أخرى فإن وضع الشخص تحت المراقبة الالكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الانترنت من شانه انتهاك حرمة البيانات ذات الطابع الشخصي له باعتبار أنه لدواعي فرز المعلومة والتأكد من قيمتها كدليل إثبات أو نفي يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شانه الوصول إما أنها معلومة ضرورية لاستكمال التحقيقات أو أنها معلومات شخصية لا دخل لها في القضية، كما يمكن أن يسار إلى تبرئة الشخص تماما[1].

بوضع المشرع لهذه الضمانان توجد بعض منها تخص هذه المراقبة والتي نص عليها القانون 04/09 سالف الذكر.

## الفرع الأول: وضع الإذن بالمراقبة الالكترونية تحت سلطة القضاء .

لقد نصت المادة الرابعة في الفقرة الثانية من القانون 04/09 على انه لا يجوز إجراء عملية المراقبة إلا بإذن مكتوب من وكيل الجمهورية.

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضابط الشرطة القضائية إذن لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[2] .

1 – محمد معمر الصغير، مرجع سابق ، ص89.

2 - القانون 09 /04 الصادر في 14 شعبان عام 1930 الموافق ل 05 غشت سنة 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 المؤرخة في 16 غشت سنة 2009 .

### الفرع الثاني: تحديد تقنية الرقابة وحدود استعمال المعطيات المتحصل عليها.

تكون الترتيبات التقنية الموضوعة لأغراض المراقبة الإلكترونية الموجهة حصريا لتجميع وتسجيل المعطيات ذات الصلة بالحالات الواردة على سبيل الحصر للمادة الرابعة من قانون 04/09 السالف الذكر على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة، أما التقنيات التكنولوجية التي تستعمل في إطار المراقبة فهي تتمثل في اعتراض المراسلات الإلكترونية والتقاط الصور وكذلك الشأن بالنسبة لتفتيش المنظومة المعلوماتية وحجزها كليا أو جزئيا وفق ما نصت عليه المواد 5 و 7 من القانون سالف الذكر 04/09.

إلا أن مصير المعلومات المتحصل عليها جراء التفتيش نصت عليه المادة 09 من نفس القانون المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عملية المراقبة إلا في الحدود الضرورية للتحريات والتحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الالكترونية يتحدد بحدود ضرورة التحقيقات وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار[1].

## المبحث الثاني

## قواعد التفتيش و الحجز في النظم المعلوماتية وتطبيقاتها في دراسة حالة

التفتيش في الجريمة التقليدية لا يختلف عن الجريمة المعلوماتية، فهو إجراء من إجراءات التحقيق هدفه الوصول إلى الأدلة من أجل إظهار الحقيقة وإسناد الفعل المجرم إلى مرتكب الجريمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات ومخرجات من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة بالتفتيش وحجز الأدلة التي تم ضبطها، إلا أنها تخضع لقواعد سنتطرق لها من خلال قواعد التفتيش والحجز داخل المنظومة المعلوماتية (مطلب أول)، وطرق الحصول والتعامل مع الدليل الرقمي أثناء التفتيش والحجز (مطلب ثان)، بالإضافة إلى تطبيق الإجراءات في دراسة حالة (مطلب ثالث).

1 امحمدي بوزينة أمنة ،إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية المرجع السابق، ص74.

## المطلب الأول: قواعد التفتيش والحجز داخل المنظومة المعلوماتية.

حاول المشرع الجزائري كباقي الدول في توفير الحماية والوقاية الجنائية اللازمة لمنع المساس بالأنظمة المعالجة الآلية للمعطيات، بالرغم من تخوفها من هذا التطور الذي اقتحم المجال المعلوماتي دون سابق إنذار، مع أنه قام بوضع مجموعة من القواعد الموضوعية لحماية المتعاملين في هذا المجال من جهة والمنظومة المعلوماتية من جهة أخرى.

إلا أن هذا لم يجدي بأي نفع ما لم يتوج بحماية إجرائية فمثلما تتميز الجرائم المرتكبة في هذا العالم الافتراضي المعلوماتي بخصوصية تجعل من الصعب تطبيق القواعد الموضوعية التقليدية عليها نجد نفس الصعوبة في تطبيق القواعد الإجرائية التقليدية عند ارتكاب هذا النوع من الجرائم.

إلا أنه كما تم الإشارة آنفا أن المشرع الجزائري استدرك الأمر بإصداره للقانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وخص التفتيش والحجز بإجراءات مستحدثة تكمل تلك المنصوص عليها في قانون الإجراءات الجزائية الجزائري حيث سنتطرق إلى قواعد التفتيش داخل المنظومة المعلوماتية (فرع أول) وقواعد الحجز داخل المنظومة المعلوماتية (فرع أول).

### الفرع الأول: قواعد التفتيش داخل المنظومة المعلوماتية.

بالرجوع إلى القانون 04/09 في المادة 05 نجد أن المشرع أجاز للسلطات القضائية المختصة، وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها وكذلك المعطيات المخزنة فيها ومنظومة تخزين معلوماتية.

-في الحالة المنصوص عليها في الفقرة/ أ من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك [1].

[1]— راجع القانون 09 /04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إذا تبين مسبقا بان المعطيات المبحوث عنها والتي يمكن الدخول إليها من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل ونأخذ المثال في هذا الشأن بالمساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية بومرداس بعد تقديم المكتب الفدرالي الأمريكي شكوى ضده مفادها أن هذا الشاب قد بعث برسالة إلكترونية إلى هذا المكتب مهدد فيها بوضع قنبلة بأحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم[1].

المشرع الجزائري من خلال نص المادة 05 من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية وهذا بالإحالة التي تضمنتها المادة غير أن القانون 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا الإجراء يمكن من الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب والتفتيش عن الأدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.

كما أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، كما اقر المشرع في نفس القانون 04/09 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 05 وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كخبراء وتقنيين مختصين في الإعلام الآلي وفن الحاسوب لإجراء عملية التفتيش على المنظومة المعلوماتية وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات[2].

---

1- امحمدي بوزينة أمنة، مرجع سابق ص 75.
2- أنظر القانون رقم 09 /04.

## الفرع الثاني: قواعد الحجز داخل المنظومة المعلوماتية.

نص القانون 04/09 في المادة السادسة على أنه عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مقيدة للكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

يجب في كل الأحوال على السلطات التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري فيها التفتيش، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلي المساس بالمعطيات، وإذا استحال إجراء الحجز وفق ما هو منصوص عليه في أحكام المادة السادسة من نفس القانون لأسباب تقنية، يتعين علي السلطات المعنية التي تقوم بالتفتيش باستعمال التقنيات المناسبة لمنع الوصول إلي المعطيات التي تحتويها المنظومة المعلوماتية والتي تم نسخها، الموضوعة تحت تصرف الأشخاص المرخص لها باستعمال هذه المنظومة[1].

كما يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع علي المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك [2] .

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به لا يجوز استعمال المعلومات المتحصل عليها عن طريق عملية المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

1 راجع القانون رقم 09 /04.

2 عبد القادر عدو، مرجع سابق، ص 109

في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم مساعدات إلى السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوي الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون 04/09 تحت تصرف السلطات المذكورة وذلك لتمكين سلطات التحقيق من مستعملي الخدمات.

ويتعين علي مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

كما حدد القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من قانون رقم 04/09 على مقدمي الخدمات التزامات خاصة وهي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية و تقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و أن يخبروا المشتركين لديهم بوجودها [2].

إن للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها دور فعال، إذ تعتبر سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وأساسا أعضاء من الحكومة وكلفت الهيئة بتنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها[3].

1 — صرشي نورة ، مرجع سابق، ص 63
2- أنظر القانون رقم 09 /04.
3- صرشي نورة ، المرجع نفسه، ص 65

تتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل و ثلاثة مديريات ومركز العمليات التقنية وملحقات جهوية، كما يتمثل أعضاؤها في الوزير المكلف بالداخلية الوزير المكلف بالبريد وتكنولوجيا الاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني ممثل عن الرئاسة الجمهورية، ممثل عن وزارة الدفاع، قاضيان من المحكمة العليا، وبهذا ضمت الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكري والدرك الوطني و الأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية[1].

و يتمثل دور هذه الهيئة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم التي تمس بأمن الدولة وذلك تحت سلطة القاضي المختص وبإنشاء هيئة وطنية أخري، أما فيما يخص تطبيق الوقاية من الجرائم مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية[2] .

1– صرشي نورة ، مرجع سابق، ص65

2 - فاطمة الزهراء خبازي، مرجع سابق، تاريخ الإطلاع 2019/07/08

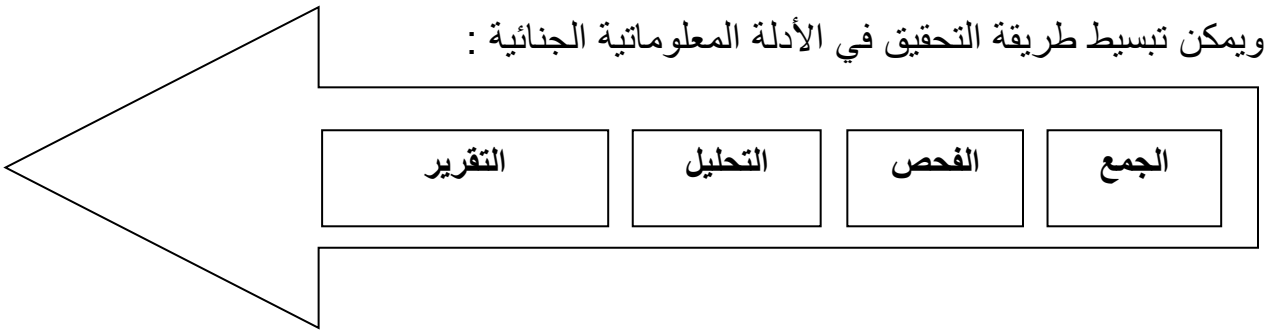
## المطلب الثاني

## طرق الحصول والتعامل مع الدليل الرقمي أثناء التفتيش والحجز.

بعد عملية التفتيش تتم عملية التحقيق من الأدلة الرقمية بحيث يجب أن يمر الدليل الرقمي المراد حجزه بمراحل حتى يتم اعتباره دليل رقمي معتمد كدليل للإثبات ويمكن حصر هذه المراحل فيما يلى :

- جمع الدليل .
- فحص الدليل .
- تحليل ومراجعة الأدلة.
- عمل تقرير بجمع الإثباتات الرقمية المستخرجة من الأدلة مع العلم بأن المراحل الموضحة يمكن الاعتماد عليها على أي نوع من أنواع الأدلة مثل: الملفات، التغيرات في أنظمة التشغيل، بيانات الشبكة وغيرها من المصادر التي تأخذ كدليل الإثبات.
- وعلى ذلك يجب على الجهات المسؤولية رغم سياسة استخدام أدوات التحقيق الجنائي بالطرق الصحيحة والمثبتة مع التأكد من أن المساعدون الذي نص عليهم القانون 04/09 وكذلك الهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تساهم في حل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

ويمكن تبسيط طريقة التحقيق في الأدلة المعلوماتية الجنائية :




1 - فاطمة الزهراء خبازي، مرجع سابق، تاريخ الإطلاع 2019/07/08

## الفرع الأول: جمع الدليل والحصول عليه

الخطوة الأولى في عملية التحقيق الجنائي هي تحديد مصدر الدليل الرقمي المتوقع حتى يتم الحصول عليه بصورة رقمية تمهيدية لفحصه وتحليل مصادر البيانات تختلف فقد تكون أقراص صلبة، ذاكرة عشوائية، أقراص خارجية وغيرها.

وللحصول على البيانات يجب المرور بعدد من الخطوات للتأكد من صحة الدليل، وقبل وبعد تفتيش المنظومة يجب على الشخص المسؤول على مسرح الجريمة رسم خطة قبل الوصول أو الحصول على البيانات أي يجب عليه تحديد مسبقا الطريقة التي سوف يقوم باتخاذها، وما هي الأدوات وكيفية استخدامها والمنهج المتبع للحصول على الدليل من الحاوية مع الحرص على عدم تعديل الدليل أو المساس به بأي شكل من الأشكال من خلال عملية تحويل أو نسخ جزء من المنظومة أو البيانات .

بناء على الخطوة السابقة، يجب على القائم بعملية التفتيش للمنظومة المعلوماتية أو الحجز عليها البدء في عملية استخراج البيانات من المنظومة، مع التأكد من سلامة البيانات بعد تحويلها بأنه لم يطرأ أي تغيير، ويمكن القيام بهذه العملية عن طريق مقارنة توقيع الحاوية الأصلية والبيانات المنسوخة، بالإضافة إلى عمل نسخ أخرى من البيانات مع التأكد من سلامتها بنفس الخطوة السابقة وحفاظها في مكان آمن في حالة حدوث أي عطب في البيانات المستخدمة [1].

1 - فاطمة الزهراء خبازي، مرجع سابق، تاريخ الإطلاع 2019/07/08

## الفرع الثاني: فحص البيانات الرقمية.

يقوم المحقق الجنائي في عملية فحص البيانات بفصل الأدلة المتعلقة بالقضية واستخراج من البيانات التي تم الحصول عليها من الخطوة السابقة حسب نوع الحاوية للبيانات، ويجب على المحقق مراعاة استخدام نوع الأدلة المناسبة لاستخراج الدليل الرقمي ومن بين الأمثلة لبعض الأدوات المستخدمة في عملية استخراج الأدلة .

| الأدوات المحتملة | نوعية الحاوية أو البيانات |
|---|---|
| Pe tools ،volatility toolkit | الذاكرة العشوائيةrom |
| .....etc،sleuth kit، ftk، EN cqse | الأقراص الصلبة أو الذكريات الخارجية |
| Xplico، network miner wire shark any enterprise entsleuth or alternative. | بيانات الشبكة |
| ENCASE Forensics v ٧and abve | الأجهزة المحمولة والأجهزة اللوحية |

نوع الحاوية أو البيانات (الذاكرة العشوائية rom ،الأقراص الصلبة بيانات الشبكة ،الأجهزة المحمولة والأجهزة اللوحية) [1].

الأدوات المطروحة في الأعلى هي أكثر شيوعا مع العلم بان اختلاف البيانات أو الحاويات قد يتطلب نوع خاص من الأدوات لعملية الفحص على سبيل المثال تحليل الصوت واستخراجه.

1- حسني ثابت، الجريمة الاكترونية في ظل تطور تكنولوجيات المعلومات على الخط:
http:// kenona online .com تارخ الاطلاع 2019/07/03

## الفرع الثالث: تحليل و مراجعة الأدلة.

تتم عملية التحليل على البيانات التي تم استخراجها في عملية الفحص، حيث يتم تحديد الاستنتاجات من خلال عملية التحليل، في هذه المرحلة سوف يتم تحديد وربط الأحداث المشتبه بهم وغيرها ومن المستحسن يفضل أن يقوم بعملية التحليل أكثر من محقق حيث كل شخص قد يكون له طريقته الخاصة في البحث والتحليل وبالتالي الحصول على عدد اكبر من الأدلة لدعم ملف القضية.[1]

كما يقوم المحقق الجنائي بتدوين عملية التحقيق منذ البداية إلى غاية نهايتها، على محاضر وتقارير التي ترفق كملف مجمل لأجل إثبات الدليل الذي تم نقله من مصدر مسرح الجريمة المعلوماتية [2] .

1 - حسين نوارة، مرجع سابق، ص98.
2 -- نفس المرجع, ص100.

## المطلب الثالث: تطبيق الإجراءات في دراسة حالة.

### الفرع الأول : القذف والتشهير عن طريق منظومة معلوماتية (فايسبوك)

تعود الوقائع إلى تعرض المدعو/ س للقذف والتشهير عن طريق منظومة معلوماتية من قبل مجهول فإن الوقائع تعود الى منذ حوالي 15 يوما، أين ورده طلب الصداقة عبر موقع التواصل الاجتماعي فيسبوك من صاحب العلبة الالكترونية الحاملة للاسم المستعار **bbbbbbbbb** مرفقة برسالة نصية تتضمن عبارات مشينة لشخصه غير أنه مسحها، وبعد حوالي يومين تقريبا قام المعني بالأمر بنشر صور الضحية ضمن الإعلانات بعلبة لإلكترونيه فيسبوك لهذا الاخير مع إرفاقها بعبارات القذف لشخصه، مضيفا أن المشتكي منه قام بأخذ الصور التي قام بنشرها من علبته الإلكترونية (الصور الشخصية) ثم نشرها بالموقع (فيسبوك) دون علمه أو رضاه، وكذلك نشر نفس الصور مكتوب عليها عبارات فاضحة بالحي الذي يقيم فيه.

الإجراءات المتبعة: وفق قانون الإجراءات الجزائية قبل صدور القانون 04/09 وإنشاء فرق مكافحة الجرائم المعلوماتية .

- ترسيم شكوى الضحية وإخطار وكيل الجمهورية، مع قيام الشاكي بمعاينة الجريمة وإحضار نسخ من صفحة الإعلانات التي تم فيها نشر الصور وأفعال القذف .
- قيام الشاكي بإحضار الرابط أو رقم هاتف المشتبه فيه، بعدها تم تكليف المتعامل أوريدو في تحديد صاحب الشريحة 0555.....من أجل تحديد هوية المشتبه فيه، أو تسخير وكالات الاتصالات الجزائر من اجل تحديد مستخدم الرابط واسم الجاهز الذي يستخدمه المشتبه فيه.
- رد وكالة أوريدو أو اتصالات الجزائر ايجابي بتحديد الهوية الكاملة للمشتبه فيه ونوعية الجهاز المستعمل.
- طلب الإذن من وكيل الجمهورية من أجل تفتيش مسكن المشتبه فيه للحصول على الجهاز بعد الحصول على الإذن بالتفتيش، تم الانتقال إلى مسكن المشتبه فيه للقيام بالتفتيش.
- حجز الوحدة المركزية لجهاز الإعلام الآلي، وكذلك صور الضحية التي تم ضبطها بمنزل المشتبه فيه، توقيف المشتبه فيه وسماعه على محضر، تقديم الأطراف .

ملف الإجراءات :

- محضر شكوى (01)، محضر سماع (01)، استمارة معلومات (01)، صور فوتوغرافية مأخوذة من الفيسبوك (04)، شهادة ميلاد (01)، تكليف شخصي ورد وكالة أوريدو (01) محضر تفتيش وحجز(01)، تقرير مصور (01).

**الفرع الثاني : انتهاك حرمه الحيات الخاصة عن طريق خرق منظومة معلوماتية**

تعود الوقائع إلى تعرض المسماة / ح ل إلى اختراق موقعها المعلوماتي فايسبوك وكذلك SKYPE من قبل المدعو/ Zohir باسم مستعار الذي طلب منها الصداقة، وبمجرد قبول صداقته سيطر على علبتها الالكترونية، وفي محاولة منها للدخول عبر السكايب وجدت نفس الشخص يطلب منها الصداقة، وبنفس الفعلة تم السيطرة على SKYPE، حيث قام بالتقاط صور للضحية وهي شبه عارية دون علمها أو رضاها، بعدها قامت الضحية بفتح علبة فايسبوك أخرى لتفاجئ بوجود صورها على موقع التواصل الاجتماعي والتي التقطها الفاعل.

الإجراءات المتبعة بخصوص المعاينات والتفتيش والحجز بموجب قانون الإجراءات الجزائية وكذا القانون 04/09 الخاص للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام والاتصال ومكافحتها

-ترسيم شكوى الضحية وإخطار وكيل الجمهورية.

-البحث عن صاحب الاسم المستعار / Zohir وتحديد الرابط الخاص به من اجل معرفة معلومته الشخصية ومراقبة أماكن اتصاله والوسيلة المستعملة في التواصل عبر موقع التواصل الاجتماعي .

-بعد تكليف مصالح اتصالات الجزائر ( قطب جواب) تم موافاتنا بهوية المشترك الذي استعمل من خلاله ذلك العنوان و يتعلق الأمر بالمدعو /----------

-بالوصول إلى المعلومات حول الشخص والجهاز المستعمل.

-طلب الإذن بتمديد الاختصاص.

- طلب الإذن من وكيل الجمهورية بتفتيش مسكن المشتبه فيه للبحث عن الأجهزة المستعملة.
- انتقلنا إلى مقر السكن موضوع الإذن بالتفتيش الكائن ---------- العملية التي كانت إيجابية.
- إجراء عملية معاينة تقليدية حيث تم حجز الوحدة المركزية لجهاز الإعلام الآلي تحمل علامة Emachines، بعد طلب الإذن بإخضاع الوحدة المركزية للتفتيش إلكتروني، تم تفتيش المعطيات ومعاينة داخل الذاكرة المنطقية للوحدة المركزية.
- حجز المعطيات في قرص صلب يحتوي على المجلد الذي يحتوي على جميع المعلومات والصور المذكورة في المحضر.
- طلب مراقبة إلكترونية للإيميلات المشتبه فيه، بعدها تم تقديم الأطراف .
- ملف الإجراءات يتكون من: محضر شكوى (01)، محضر سماع(01)، استمارة معلومات (01)، رد وكالة اتصالات الجزائر (01)، شهادة ميلاد (01)، محضر تفتيش وحجز تقني (01)، محضر مراقبة تقني(01)، محضر تحريات تقني (01)، كما تم حجز الوحدة المركزية من نوع Emachines

## الفرع الثالث: نموذج عن محضر تفتيش تقني حول قضية المساس بحرمة الحياة الخاصة عن طريق منظومة معلوماتية

### محضر تفتيش وحجز إلكتروني

-/ **انه في يوم**: الإثنين الموافق للثاني عشر من شهر جانفي----------

**قضية :** -/ **من سنة**: ألفين وخمسة عشر(2015).-------/**الساعة**: الثامنة صباحا. ----------

-/ **نحن**: ملازم أول للشرطة ----------، بمديرية الشرطة القضائية. ----------

-/ **ضابط الشرطة القضائية** بدائرة الاختصاص بمساعدة..... بفرقة مكافحة الجرائم المعلوماتية ----------

-/في إطار التحقيق المفتوح في قضية المساس بحرمة الحياة الخاصة التي راحت ضحيتها المدعوة/ .....

-/بناءا على نص المادة 05 من قانون رقم 04/09/ المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال، وبناءا على الأمر بتمديد الاختصاص والإذن بالتفتيش المنظومة المعلوماتية الحاملين للرقم 14/000615 بتاريخ 2015/01/05 الصادرين عن السيد/ وكيل الجمهورية لدى محكمة الحراش، الناص على تمديد الاختصاص إلى محكمة عين تموشنت، المؤشر عليه من طرف السيد/ وكيل الجمهورية لدى نفس المحكمة بتاريخ 2015/01/07، و الإذن بالتفتيش الناص على تفتيش مسكن المدعوة/ ف ق، نقول أننا بتاريخ 2015/01/07 انتقلنا إلى مقر السكن موضوع الإذن بالتفتيش الكائن..... العملية التي كانت إيجابية و تم من خلالها حجز الوحدة المركزية لجهاز الإعلام الآلي التي تحمل علامة Emachines، ملك المشتبه فيه المدعو/ ...../----------

**الموضوع:**

-/ أنه بتاريخ اليوم و الساعة المشار إليهما أعلاه إجراء عملية معاينة و تفتيش إلكتروني.

-/ يتبين من خلال فحص الجهاز أن المشتبه به قام بحذف نظام التشغيل السابق وتثبيت نضام WINDOWS 7 جديد بتاريخ 2014/11/18 (صورة01)----------

**صورة خاصة بالضحية**

**صورة01**

-/في الوهلة الأولى قمنا بمعاينة متصفح الأنترنات « Google Chrome » المثبت على جهاز الكمبيوتر الخاص بالمشتبه فيه، أين عثرنا على عنوان البريد الإلكتروني «---------- » (صورة02)، المستعمل في إنشاء حساب الفيسبوك « -----Ka » الذي قام من خلاله بالاتصال بالضحية بعد قرصنة جهازها، مع العلم أنه قام بتغيير إسم حسابه من إسم « ----- إلى « o----- »

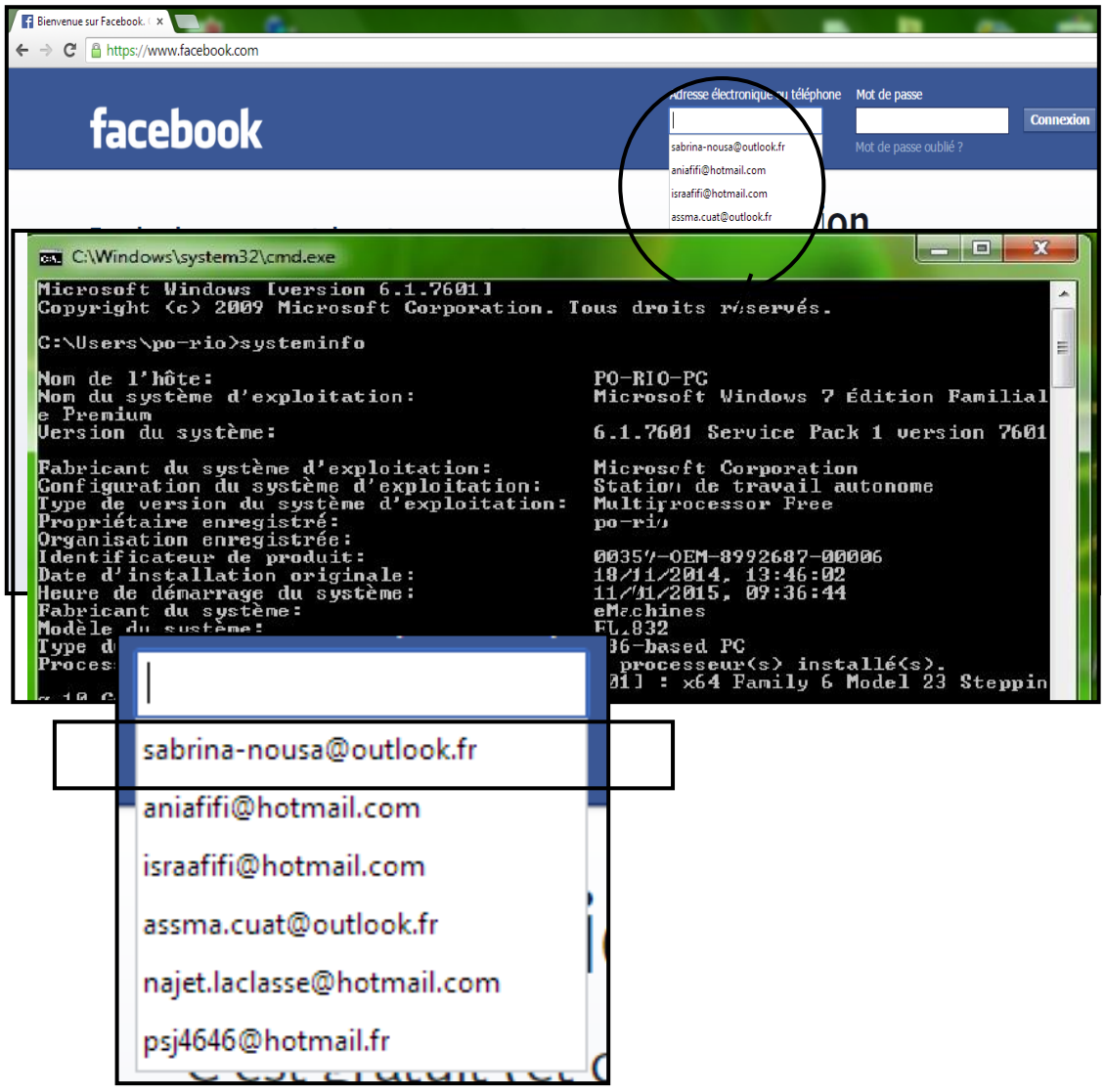
-/عملية تفتيش الأقراص الصلبة بينت أن عملية الولوج إليها محمية بكلمة سر ----------

/ تفتيش القرص الصلب C لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق، كما أنه لا يوجد أي برنامج يستعمل في القرصنة مثبت على الجهاز بعد تاريخ حذف نظام تشغيل الجهاز المذكور أعلاه----------

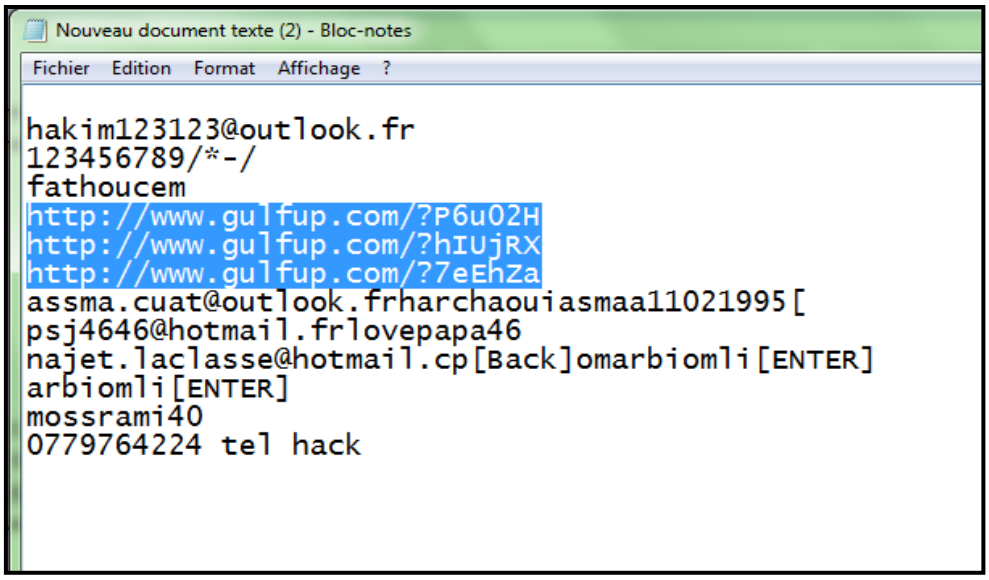
-/ تفتيش القرص الصلب D لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق مع وجود بعض البرامج التي قد تستعمل في عمليات القرصنة----------

-/تفتيش القرص الصلب الأخير E بين مايلي:----------

-/ وجود ملف باسم Nouveau document texte(2).txt يحوي ثلاثة (3) روابط على موقع www.golfup.com حيث قام المشتبه فيه بوضع الفيروس يقوم الضحايا بتحميله على أساس أنه ملف أخر (صورة03) ----------

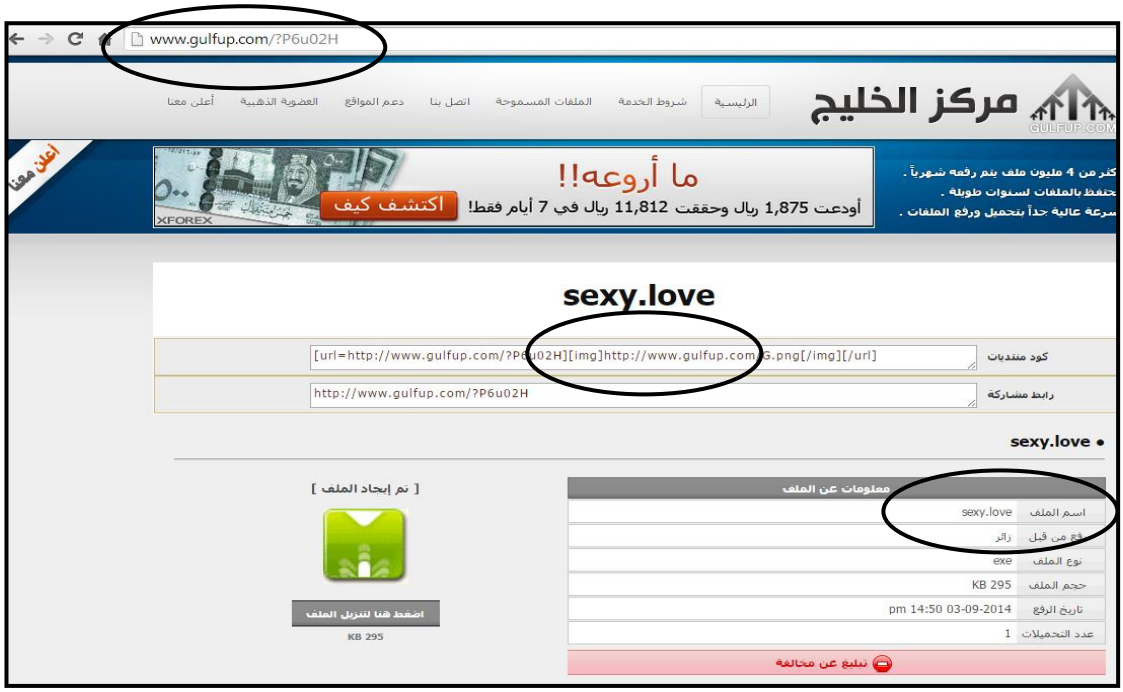



صورة 02



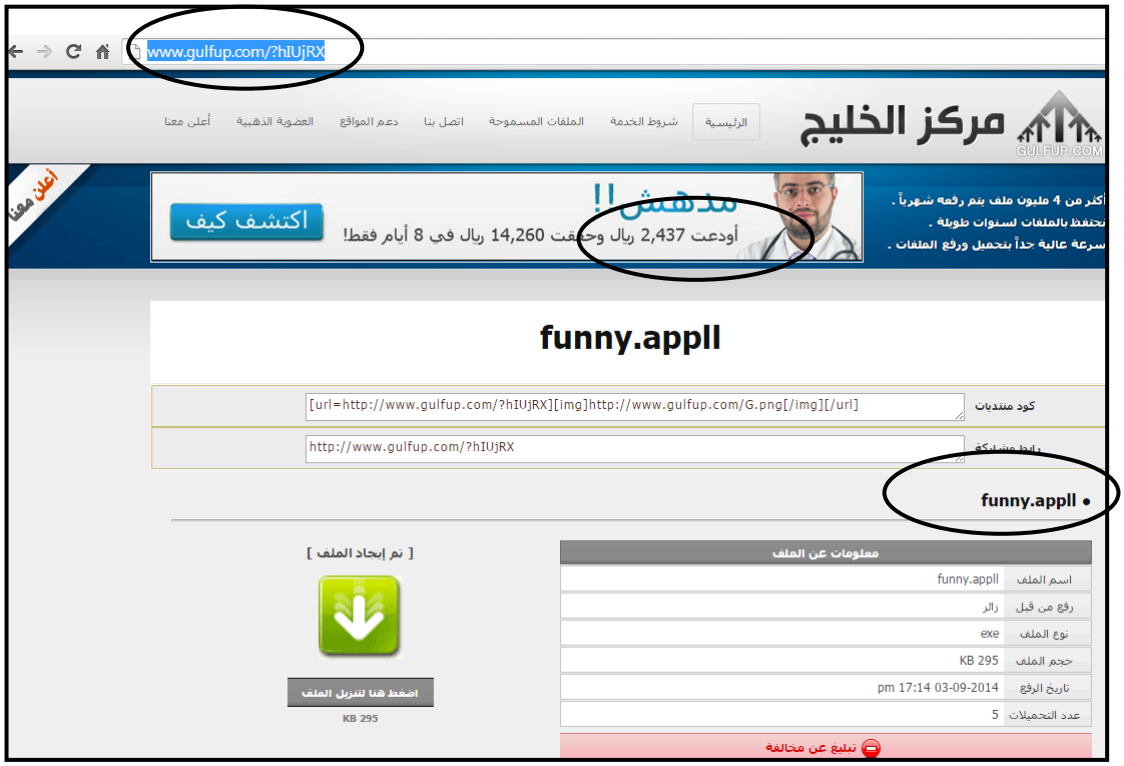

صورة 03

-/الرابط الأول http://www.gulfup.com/?P6u02H يقود إلى تحميل الفيروس على أساس أنه برنامج جنسي sexy.love.exe (صورة04) ----------




صورة 04

-/الرابط الثاني http://www.gulfup.com/?hIUjRX يقود إلى تحميل الفيروس على أساس أنه برنامج تسلية funny.appll.exe (صورة05) ----------



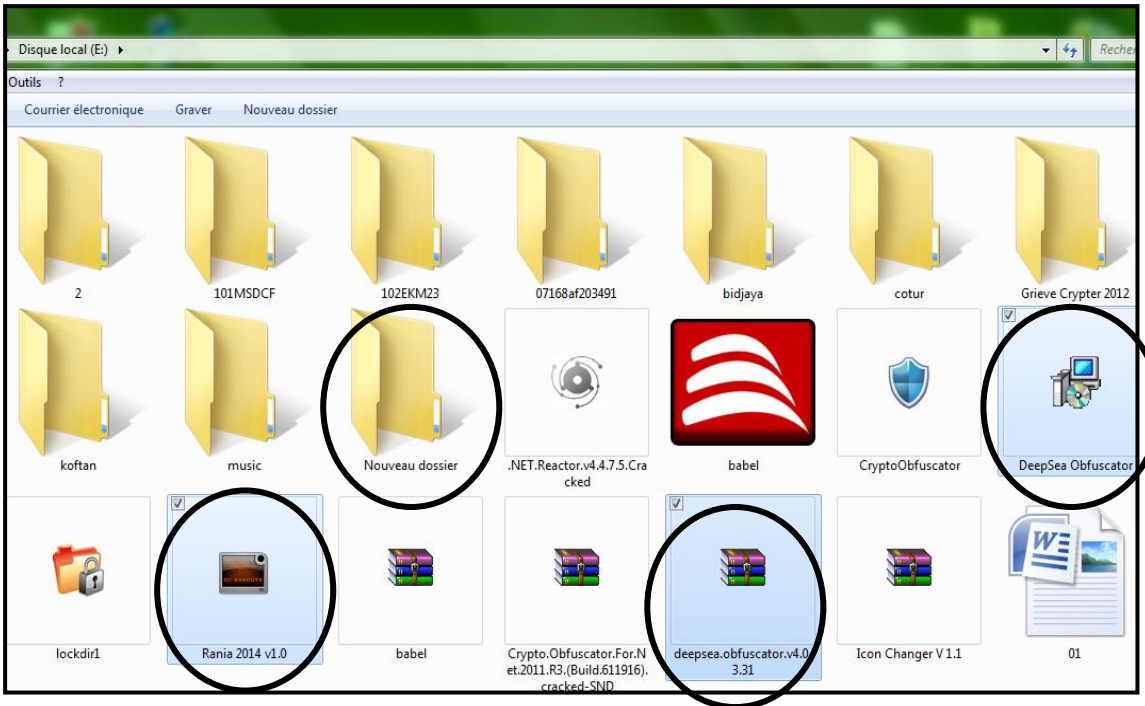

صورة05

**صورة06**

-/الرابط الثالث http://www.gulfup.com/?7eEhZa يقود إلى تحميل الفيروس على أساس أنه برنامج انترنت nat.exe (صورة06) ----------

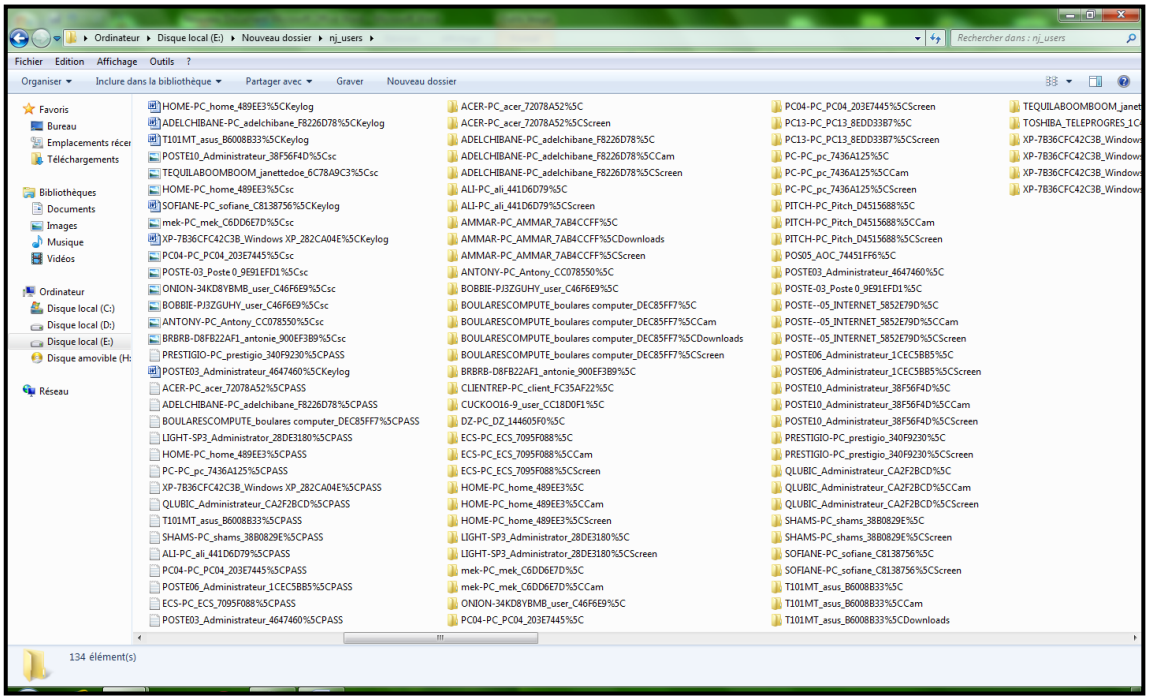
-/ وجود البرنامجين Rania 2014 v1.0 و DeepSea Obfuscator المستعملين في تشفير الفيروس من طرف المشتبه فيه لكي لا تتعرف عليه برامج الحماية (صورة07) ----------

-/وجود ملف مسمى Nouveau dossier يحتوي ملفات (صورة07) خلفها برنامج Nijrat الذي يقوم بتحضير الفيروسات




**صورة 07**

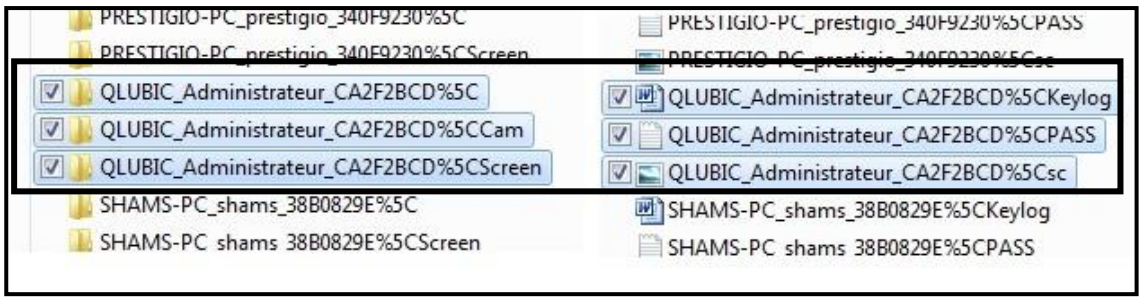
-/داخل المجلد nj_users الموجود داخل المجلدNouveau dossier يوجد العديد من الملفات والمجلدات التي قام الفيروس بإرسالها للمشتبه فيه من أجهزة الكمبيوتر الخاصة بالضحايا




**صورة 08**

-/ من ضمن هذه الملفات توجد ملفات word تنتهي جميعها بكلمة keylog قام برنامج keyloger بإنشائها (برنامج يقوم بإرسال ما يكتب الضحية على لوحة المفاتيح)، من بين هذه الملفات يوجد ملف باسم QLUBIC_Administrateur_CA2FBCD%5Ckeylog خاص بالقضية محل التحقيق يحتوي على ما كتبته الضحية خلال استعمالها للجهاز(صورة09) ----------

-/كما يوجد ملفات بصيغة TXT تنتهي جميعها بكلمة PASS تحتوي على اسم المستخدم وكلمات المرور لمختلف الحسابات الخاصة بالضحايا، من بين هذه الملفات يوجد ملف باسم QLUBIC_Administrateur_CA2FBCD%5CPASS خاص بالقضية محل التحقيق يحتوي على حسابات الشاكية (صورة09 )، كما توجد مجلدات كل مجلد خاص بضحية تحتوي على صور قام المشتبه فيه بأخذها أو تصويرها من أجهزة الضحايا، من بين هذه المجلدات يوجد ثلاث (03) مجلدات خاصة بالقضية محل التحقيق (صورة09) ----------




**صورة09**

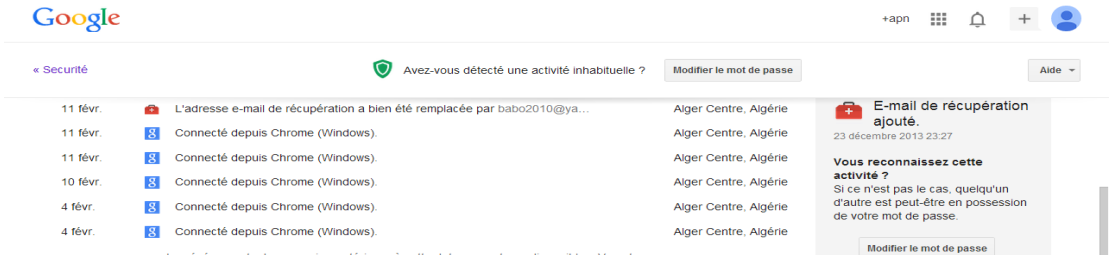
-/ المجلد الأول باسم QLUBIC_Administrateur_CA2FBCD%5C لا يحتوي على أي ملف ----

-/ المجلد الثاني باسم QLUBIC_Administrateur_CA2FBCD%5CCam يحتوي على ثمانية عشر(18) صورة قام المشتبه فيه بتصويرها عند تمكنه من فتح كميرا جهاز الكمبيوتر الخاص بالشاكية هذه الصور خاصة بالشاكية المدعوة/ ح ل و ابنة أخيها المدعوة/ ------- وهي كالتالي: الصور الخاصة بالشاكية المدعوة/ --------/الصور الخاصة بالمدعوة/ ----------:

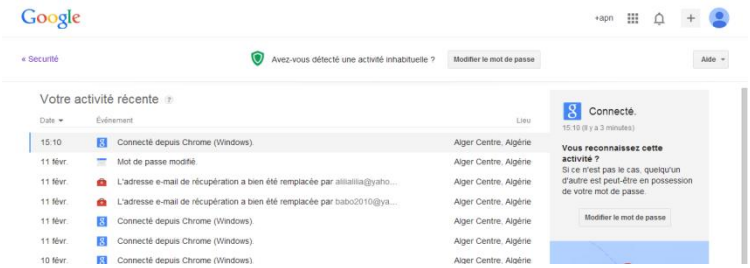
-/ المجلد الثالث باسم QLUBIC_Administrateur_CA2FBCD%5CScreen يحتوي على أربعة عشر (14) صورة قام المشتبه فيه بتصويره لسطح المكتب تظهر فيها الشاكية المدعوة/ ح ل أثناء محادثة شخصية في برنامج SKYPE بينها و بين حساب يسمى « Zohir » خاص برجل كما هو مبين بالصور أسفلها،كما يوجد خمسة (05) مجلدات أخرى تحتوي على صور لأشخاص تم اختراق أجهزة الكمبيوتر الخاصة بهم من طرف المشتبه فيه، هذه المجلدات موجودة بالقرص المضغوط المرفق وتسمى على التوالي:
/المجلد الأول « BOULARESCOMPUTE_boulares computer_DEC85FF7%5CDownloads» ---------
/المجلد الثاني « ECS-PC_ECS_7095F088%5CScreen »----------
-/المجلد الثالث « PITCH-PC_Pitch_D4515688%5CScreen »----------
-/المجلد الرابع « POSTE--05_INTERNET_5852E79D%5CScreen »----------
-/ المجلد الخامس « XP-7B36CFC42C3B_Windows XP_282CA04E%5CDownloads » -------
-/نرفق لكم مع هذا المحضر قرص صلب يحتوي على المجلد الذي يحتوي على جميع المعلومات والصور المذكورة في المحضر. ----------

-/أثناء عملية التفتيش الإلكتروني استعملنا برتوكول الأنترنت التالي.....

-/عاينا بأن المدعو/++++++++ قام بالولوج للإيميل محل التفتيش الإلكتروني بتاريخ 2013/12/23، مستعملا برتوكول الأنترنت 41.103.239.124 و41.109.229.247.، أنظر صورة رقم 10-11---/




**صورة رقم 10**




**صورة رقم 11**

-/قمنا بتفتيش الحساب الإلكتروني الحامل للاسم المستعار aaaaaa.sec والمربوط بالإيميل aaaaaaaaaaaa@gmail.com ( صورة 12)----------

**صورة 12**

-عاينا بأن الحساب الإلكتروني محل التفتيش مربوط بالإيميل aaaaaaa@gmail.com، أنظر صورة رقم 13.

**صورة رقم 13**

-/ كما أننا أثناء معاينة الصفحة المجرمة الحاملة للاسم المستعار " أسرار المجلس الشعبي الوطني" عاينا بأن الحساب الإلكتروني الحامل للإسم المستعار " aaaaaa.sec " يعتبر عضو مؤسس ومسير الصفحة (الصورة رقم 14)---- ----------/

**صورة رقم 14**

-/تمت عملية التفتيش و المراقبة الإلكترونية في ظروف حسنة دون تسجيل أي يشيء يستحق الذكر.-----

-/ لما سبق ذكره حرر هذا المحضر في يومه و ساعته ووقعناه رفقة المعني بالأمر و مساعدينا.-------

**المعني بالأمر** **المساعدين** **ضابط الشرطة القضائية**

خلاصة لما سبق ذكره عن القواعد العامة للتفتيش وحجز والمعاينات، يمكن القول أن القانون 04/09 لم يتضمن المعاينات داخل المنظومة المعلوماتية، أما بالنسبة لتفتيش المنظومة المعلوماتية فلقد نصت المادة 05 من هذا القانون على نوعان من التفتيش:

التفتيش عن طريق الانتقال والتفتيش عن بعد الذي نص عليه المشرع كإجراء جديد يخص الجرائم المعلوماتية، لكن لم يضع القواعد الخاصة به وإنما أحالنا إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، وبهذا نجده يمس بمبدأ قانوني الخاص يقيد العام في جميع الأحوال فأصبحت القواعد الخاصة تتقيد بالقواعد العامة أما من الجانب العملي فلا يتم إجراءه.

وبالرجوع إلى نص المواد 06، 07، 08، 09 من القانون 04/09 السالف الذكر نجدها تحدد قواعد للحجز داخل المنظومة المعلوماتية، وفي حالة استحالة الحجز لأسباب تقنية: يتعين على السلطات التي تقوم بالتفتيش استعمال تقنيات منع الوصول والاطلاع إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو نسخها.

وفي الأخير تم التطرق إلى دراسة حالة بمعالجة قضيتين حول الجريمة الإلكترونية وإجراءات التحري المتبعة بخصوص المعاينات والتفتيش والحجز داخل المنظومة المعلوماتية، فالأولى تم معالجتها قبل صدور القانون 04/09 أما الثانية فتم معالجتها بعد صدور هذا القانون 09/04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

# الخاتمة

لقد أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها فقد مكنت طرق المعالجة الآلية للمعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية نظرا لكون التكنولوجية أو الجريمة هي عابرة للحدود.

أمام هذا التطور فقد ارتبطت به ما يعرف بالإجرام المعلوماتي وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتجت عنه عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد من جهة أخرى، لأن الحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة فهي لا تستطيع مواكبة الجريمة المعلوماتية ومقاومتها أمام التطور التقني الذي تشهده تقنية الاختراق، وكذا عجز النصوص التشريعية في توفير الحماية خاصة من الناحية الإجرائية.

قد حاولنا من خلال موضوع **"إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية"** الوقوف على هذه الإجراءات، حيث وجدنا أن للجريمة المعلوماتية خصوصية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري، وكذا القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذ أن قانون الإجراءات الجزائية ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية أما بالنسبة للقانون رقم 04/09 فقد وضع لمتابعة الجريمة المعلوماتية من خلال بعض الإجراءات الخاصة المتمثلة في حجز المعطيات ومراقبة الاتصالات الإلكترونية وحفظ المعطيات.

في الأخير يمكن القول أن المشرع الجزائري لا يوفر آلية تشريعية قادرة على الاضطلاع بالآثار الخطيرة، التي ترتبها جرائم المساس بالأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الإطارات البشرية والأجهزة المتخصصة لمواجهة هذا النوع من الجرائم، وفي ظل تشتت النصوص القانونية الخاصة بالجريمة المعلوماتية بين قانون العقوبات وقانون الإجراءات الجزائية والقوانين المكملة له والتضارب بين القواعد العامة والخاصة وصعوبة تطبيقها ميدانيا، تبقى كلها عراقيل تحذو دون التطبيق الدقيق لفحوى النصوص القانونية من قبل الضبطية القضائية من جهة وسهولة إفلات المجرمين من العقاب من جهة أخرى.

وعليه فإن عدم وجود أخصائيين تقنيين في مجال مكافحة الجريمة المعلوماتية على مستوى الجهات الأمنية، تبقى كلها حواجز تحول دون توفير الحماية المعلوماتية من جهة ومكافحة الجرائم المعلوماتية من جهة أخرى، كذلك وأن القانون 04/09 المذكور أعلاه يبقى حبر على ورق ما لم يتوج بتطبيق صارم ودقيق لفحوى المواد الخاصة بقواعد المراقبة والتفتيش والحجز في النظم المعلوماتية، كما ختمنا هذه الدراسة ببعض الاقتراحات والتوصيات والتي من شأنها التقليل من الآثار السلبية للكثير من التحديات المصاحبة لوسائل الاتصال الجديدة والمتمثلة في:

- التدريس والتكوين المستمر للإطارات البشرية العاملة في مجال الجرائم المعلوماتية، واستخدام شهادات عليا متخصصة في المجالات التقنية والقانونية المتعلقة بمكافحة الجرائم المعلوماتية، وحث المصالح المتخصصة والمراكز البحثية على تسليط الضوء أكثر على مثل هذه الجرائم مع تكثيف الندوات والملتقيات والأيام الدراسية حول الموضوع .
- ضرورة مراجعة التشريعات الوطنية من خلال دق ناقوس الخطر والضرب بتقنين خاص يحدد الإطار الإجرامي للجريمة المعلوماتية، مع تشديد الوصف الجنائي والعقوبات المقررة لأنماطها الإجرامية، مع تحديد الإجراءات المتخذة بدقة ليتماشى وحساسية الجريمة وخطورتها بغية تحقيق الردع والقضاء على الإجرام المعلوماتي .

- عقد دورات مكثفة للإطارات العاملة في حقل التحري والتحقيق، حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها والنظر في مضامين منهاج التحقيق .
- ضرورة إيجاد وسائل مناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية، والتطبيق الفعلي لمواد القانون 04/09 في مجال التعاون الدولي، أي التوفيق بين التشريع الخاص بهذه الجرائم والتعاون الدولي على تبادل المعلومات، وقبول أي دولة للأدلة المجموعة في دولة أخرى لضمان الحماية العالمية الفعلية لبرنامج المعطيات وشبكة الانترنت ككل .
- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بيانات الشخصية، وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة .
- ضرورة قيام ضباط الشرطة القضائية ومن يعاونه (أعوان الضبط القضائي) بمعاينة وتفتيش وحجز تقني للأجهزة في المكان الذي تم فيه ضبط الأجهزة قبل الحجز عليها، تفاديا لأي حذف أو تغيير للمعطيات والبيانات خاصة منها المتصلة بالانترنت من جهة وعدم المساس بممتلكات الأشخاص من جهة أخرى في حالة ما إذا كان التفتيش سلبي.

# قائمة المصادر والمراجع

- **الكتب:**

**1.** أحمد حزيط، الوجيز في الإجراءات الجزائية ،الطبعة الثانية منقحة دار هومة الجزائر،2015.
**2.** جميل حسين طويلة، التحليل الجنائي الرقمي، مكتبة النور، سوريا بدون طبعة وبدون سنة النشر.
**3.** عبد القادر عدو، الجريمة الإلكترونية إجرائيا، الطبعة الثانية، دار هومة، الجزائر 2016.
**4.** عصام شيبان، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، المطبوعات الجامعية، الجزائر سنة 2005 .
**5.** ماجد ياقوت، أصول التحقيق، دراسة مقارنة، الطبعة الثالثة، منشأة المعارف الإسكندرية بدون سنة النشر.
**6.** محمد معمر الصغير، الوافي في الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الحديث، الجزائر، 2010.
**7.** ناصر جوادي، إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية الجزائري دار العلوم، الطبعة الثالثة الجزائر سنة 2011 .

- **الرسائل والمذكرات:**

**1.** براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية ،أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو سنة 2018.
**2.** رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه في العلوم، جامعة أبو بكر بلقايد تلمسان سنة 2018.
**3.** سعيداني نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة الحاج لخضر باتنة ،سنة 2012.
**4.** صرشي نورة، مكافحة الجريمة المعلوماتية مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة الجزائر ،سنة 2012.
**5.** ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الجنائي للأعمال كلية الحقوق بجامعة العربي بن مهيدي أم البواقي سنة 2015.
**6.** حمزة نجاة، معاينة مسرح الجريمة ودوره في الكشف عن الحقيقة، مذكرة لنيل شهادة الماستر في القانون الجنائي كلية الحقوق جامعة آكلي محند أولحاج البويرة، سنة 2014.

**7.** معمش زهية/غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص والعلوم الجنائية كلية الحقوق بجامعة عبد الرحمان ميرة بجاية سنة 2012

**8.** غرداين حسام، الجريمة الالكترونية والإجراءات التصدي لها، مذكرة لنيل شهادة الماستر كلية الحقوق جامعة الجزائر سنة 2015.

- **المقالات**

**1.** امحمدي بوزينة أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لقانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام...)، سنه 2016.

**2.** حسين نوارة، مظاهر الاعتداء على الحياة الخاصة الملتقى الوطني حول تأثير التطور العلمي والتقني على حقوق الإنسان ،كلية الحقوق جامعة عبد الرحمان ميرة بجاية 2009.

- **المواقع الالكترونية:**

**1.** إيناس محمد راضي، الأجهزة التحليلية الحديثة في كلية علوم الأدلة الجنائية، على الرابط **http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid**

**2.** .حسني ثابت، الجريمة الالكترونية في ظل تطور تكنولوجيات المعلومات، على الخط : **http:// kenona online .com**

**3.** رضا دحان، كل ما تحتاج معرفته حول الـ **Digital Forensic** و الجرائم الإلكترونية و كيفية احترافها، على الرابط -**https://www.aqweeb.com/2016/08/All-About-digital-forensic.html**

**4.** فاطمة الزهراء خبازي، الجريمة الالكترونية في ظل الجرائم المرتبطة بتكنولوجيات المعلومات على الخط: **http:// salahgardafi .eb 2a .com.content.**

**5.** مهند، أدوات جمع المعلومات، على الرابط **https://th3expert.net/maltego**

**6.** نضال أدمين، منتدى برامج الكمبيوتر والانترنيت، على الرابط **http://nidhal-technologie.own0.com/t60-topic**

- **القوانين:**

**1.** قانون رقم 01/16 المؤرخ في 26 جمادى الأولى عام 1437 الموافق ل 06- مارس سنة 2016 يتضمن التعديل الدستوري، ج ر عدد 63.

**2.** قانون الإجراءات الجزائري.

**3.** قانون قانون العقوبات الجزائري.

**4.** قانون 01/06 المؤرخ في 21 محرم عام 1427 الموافق لـ 20 فبراير سنة 2006 يتعلق بالوقاية من الفساد ومكافحته، ج ر عدد 14 المؤرخة في 08 صفر 1427 الموافق لـ 08 مارس 2006.

**5.** قانون رقم 04/09 الصادر في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 المؤرخة في 16 غشت سنة 2009.

# الفهرس

## الفهرس: إجراءات المعاينات، التفتيش والحجز داخل المنظومة المعلوماتية


***التشكرات والإهـــداء***

المقـــــــدمة..... 3-1

الفصل الأول: إجراءات التحري التقليدية للكشف عن الجرائم داخل المنظومة المعلوماتية..04-28

المبحث الأول: معاينات مسرح الجريمة الالكتروني..... 05

المطلب الأول: التحليل الجنائي لمعلومات الجهاز..... .....06

الفرع الأول: مفهوم التحليل الجنائي.....07

الفرع الثاني: معلومات الجهاز.....08

المطلب الثاني: معاينة محل الجرائم الواقعة داخل وخارج النظم المعلوماتي.....09

الفرع الأول: مفهوم المعاينة.....09

الفرع الثاني: معينة مسرح الجريمة الالكترونية.....10

المطلب الثالث: القواعد الإجرائية لمعاينة مسرح الجريمة الالكترونية.....11

الفرع الأول: إخطار وكيل الجمهورية.....11

الفرع الثاني: أوقات المعاينة.....12

الفرع الثالث: رضا صاحب المسكن.....13

المبحث الثاني: التفتيش و الحجز في النظم المعلوماتية.....15

المطلب الأول: إجراءات تفتيش نظم الحاسوب المادية والمعنوية.....16

الفرع الأول: التفتيش في نظم الحاسوب المادية.....16

الفرع الثاني: التفتيش في نظم الحاسوب المعنوية.....17

المطلب الثاني: القواعد الإجرائية للتفتيش والحجز.....19

الفرع الأول: إجراء الإذن.....19

الفرع الثاني: إجراء التفتيش والحجز بحضور أشخاص معينين قانونا.....20

## الفهرس: إجراءات المعاينات، التفتيش والحجز داخل المنظومة المعلوماتية


الفرع الثالث: مواعيد التفتيش والحجز.....21

الفرع الرابع: رضا المشتبه فيه بالتفتيش.....22

الفرع الخامس: تحرير محاضر التفتيش والحجز.....23

المطلب الثالث: بعض البرامج المستخدمة أثناء المعاينة والتفتيش والحجز.....24

الفرع الأول: برنامج مالتيجو "Maltego ".....25

الفرع الثاني: برنامج فورنسيك " EnCase Forensic ".....26

الفصل الثاني: إجراءات التحري المستحدثة للكشف عن الجرائم داخل المنظومة المعلوماتية .....29-62

المبحث الأول: مراقبة الاتصالات الالكترونية .....31

المطلب الأول : توسيع الاجراءات الخاصة بالاختصاص الإقليمي.....32

المطلب الثاني: تجميع الاتصالات الالكترونية و مراقبتها.....34

الفرع الأول: الإذن كضابط لإجراء التحري.....37

الفرع الثاني: الالتزام بالسر المهني كضابط لإجراء التحري.....38

المطلب الثالث: حالات المراقبة الالكترونية .....41

الفرع الأول: وضع الإذن بالمراقبة الالكترونية تحت سلطة القضاء.....42

الفرع الثاني: تحديد تقنية الرقابة وحدود استعمال المعطيات المتحصل عليها.....43

المبحث الثاني: قواعد التفتيش و الحجز في النظم المعلوماتية وتطبيقاتها في دراسة حالة..... 43

المطلب الأول: قواعد التفتيش والحجز داخل المنظومة المعلوماتية.....44

الفرع الأول: قواعد التفتيش داخل المنظومة المعلوماتية.....44

الفرع الثاني: قواعد الحجز داخل المنظومة المعلوماتية.....46

المطلب الثاني: طرق الحصول والتعامل مع الدليل الرقمي أثناء التفتيش والحجز.....49

الفرع الأول: جمع الدليل والحصول عليه.....50

**الفهرس: إجراءات المعاينات، التفتيش والحجز داخل المنظومة المعلوماتية**

الفرع الثاني: فحص البيانات الرقمية.....51

الفرع الثالث: تحليل ومراجعة الأدلة.....52

المطلب الثالث: تطبيق الإجراءات في دراسة حالة.....53-62

الفرع الأول: القذف والتشهير عن طريق منظومة معلوماتية (فايسبوك).....53

الفرع الثاني: انتهاك حرمه الحيات الخاصة عن طريق خرق منظومة معلوماتية.....54

الفرع الثالث: نموذج عن محضر تفتيش تقني حول قضية المساس بحرمة الحياة الخاصة عن طريق منظومة معلوماتية..... 55

الخـــاتمة.....63

قائمة المصادر والمراجع.....66