جـــامعة غـــرداية
كلية الحقوق والعلوم السياسية
قسم: الحقوق

ملخص لمذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق
تخصص قانون جنائي وعلوم جنائية

# اجراءات البحث والتحري في الجرائم المعلوماتية

إعداد الطالبتين:
- فاطيمة دهان
- كلثوم دهان

تحت إشراف الدكتور:
د. مختار بن حمودة

**لجنة المناقشة:**

| اسم و لقب الاستاذ | الرتبة | الجامعة | الصفة |
|---|---|---|---|
| أ / نسيم هوام | أستاذ مساعد" أ " | غرداية | رئيسا |
| د/ مختار بن حمودة | أستاذ محاصر " أ " | غرداية | مشرفا ومقررا |
| أ / محمد الطيب سكريفية | أستاذ مساعد " أ " | غرداية | عضوا مناقشا |

السنة الجامعية

1442 -1443 هـ / 2021-2022 م

السلام عليكم ورحمة الله وبركاته

# إهداء

إلى ذلك الصرح الذي علمني الخلق الكريم والارتقاء لسلم الحياة بحكمة وصبر

والدي سحائب الرحمة تحف روحه الطاهرة

إلى من أنارت دربي وعلمتني الصبر والعزيمة

والدتي أدام الله عليها الصحة والعافية

سندي وخليلي من كان لي في الشدة عون وفي الرخاء رفيق

رفيق البيت الطاهر زوجي الغالي

إلى كبدي زينة حياتي ومصدر بهجتي ونور عيناي ابنتاي

هبة الرحمان ملهمتي، بشرى عزوتي

إلى شقائق الوسادة من تقاسمت معهم تفاصيل الطفولة وأحلام الشباب والواقع

إخوتي وأخواتي

إلى رفيقات المشوار من سرنا سويا لنشق معا الطريق نحو النجاح

زميلاتي وزملائي

أخوات لم تلدهم أمي، مؤنسات غاليات نعيمة، مريم

كلثوم

# إهداء

إلى الذي علمني معنى الحياة فامسك بيدي وحملني على صفحات الدنيا

وأوصلني إلى بر الأمان ولم يبخل عليا بحبه وعطفه وحنانه أقولك

أبي العزيز " رحمك الله وجعلك في أعلى

إلى من علمتني الصمود مهما تبذلت الظروف إلى ينبوع الحنان والحب

أمي أطال الله في عمره

إلى زوجي الغالي وأعزاء القلبي الذي ينبض بالحب والصدق

أولادي حسان وحسناء

إلى إخوتي وأخواتي وكل العائلة الكريمة

إلى كل من كانت له لمسة في مشواري الدراسي

إلى من وقف جانبي وساندني خاصة رفيقة دربي كلثوم وزوجها ياسين

إلى أستاذي المشرف

إلى كل هؤلاء ثمرة جهدي

فاطيمة

**قال رسول الله صلى الله عليه وسلم «من لم يشكر الناس لم يشكر الله ومن أسدى إليكم معروفا فكافئوه فإن لم تستطيعوا فادعوا له»**

**وعملا بقول نبينا الكريم، نحمد الله ونشكره أن وفقنا لإتمام هذا العمل**

**لكم أستاذي المشرف مختار بن حمودة**

**يا من رافقتنا في إعداد هذه المذكرة وصغت لنا من العلم حروفا وكنت الأستاذ الناصح**

**أسمى عبارات الشكر والامتنان سدد الله خطاكم**

**لكم أساتذتي بقسم الحقوق يا من كنتم مصابيح تضئ للطلبة متاهات البحث والتحري**

**أسمى معاني التقدير**

**إلى كل من ساعدنا من قريب أو من بعيد في إنجاز هذه المذكرة**

# المقدمة

**مـــــــقدمة:**

تعد الجريمة المعلوماتية من الجرائم المستحدثة فقد تزامن ظهورها مع ظهور أعظم اختراع في العالم الحديث الحاسب الآلي والأنترنت، وهي إفراز لما نعيشه من ثورة معلوماتية، فرغم حداثتها إلا أنها تشكل تهديدا حقيقا لاقتصاديات الدول وخصوصيات الأفراد .إن هذه الجرائم تتميز بطبيعة خاصة تختلف عن الجرائم العادية فهي لا تترك آثار مادية يمكن من خلالها التوصل إلى الجاني كما في الجرائم العادية، كما أنه يمكن إتلاف أو تغيير الأدلة في هذه الجرائم خلال لحظات دون أن يترك هذا التغيير آثار مادي .ومن ناحية أخرى فإن الصعوبة في مواجهة الجريمة المعلوماتية تبدأ من الطبيعة الافتراضية التقنية التي ترتكب فيها، فمن السهل ارتكاب جريمة ما حيث أن نقرة بسيطة من الكمبيوتر كافية للتصرف أو الوصول على الضحية المحتمل رغم أن التقنيات المستحدثة في كثير من الأحيان تكون دقيقة جدا، كما تتم في الخفاء فكثيرا ما يعمد ارم المعلوماتي إلى إخفاء نشاطه عن طريق تلاعبه بالبيانات فضلا عن سهولة تدمير الدليل .وعلى ضوء ذلك فإن الظاهرة الإجرامية المعلوماتية باتت تشكل بعض التحديات القانونية والعملية التي وضعت لمكافحتها ونتج عن ذلك مشكلة في تفسير النصوص القانونية وحظر القياس في المواد الجنائية وهذه العوامل تؤدي إلى إفلات الكثير من مجرمين كغيرها من الدول ليست في منأى عن هذه الأشكال من الجرائم كونها خطت خطوات لا بأس بها في مجال المعلوماتية وطبيعي أن المشرع لم يبقى مكتوف الأيدي إزاء هذه الوضعي.

- **ففيما تتمثل الجريمة المعلوماتية والإجراءات المعتمدة من طرف الدولة الجزائرية لكشف عنها؟**
- ويتفرع هذا الإشكال إلى تساؤلات فرعية كالاتي: فيما تتمثل الجريمة الإلكترونية وما معوقاتها وفيما تتمثل ماهي أليات الإجرائية في كشف عنها.

- حدود هذه الدراسة تتطرق الجرائم الإلكترونية الجزائر مع التطرق إلى بعض النماذج القطاعية التي حققت قفزة نوعية من خلال تقديم وأليات الكشف عنها.
- الإطار المكاني لموضوع الدراسة فهو يركز على الجرائم المعلوماتية في الجزائر، أما الإطار الزماني فتم التركيز على معلومات حديثة وعصرية حداثة الموضوع في الجزائر.

فرضت طبيعة الموضوع توظيف عدد في المناهج تتمثل في الوصف الدقيق والتفصيلي لموضوع محدد للحصول على نتائج علمية بطريقة موضوعية، ويتجلى ذلك من خلال سرد مفهوم وتعريف الإدارة الإلكترونية وأهم خصائصها ومعوقاتها وكذا بناء وتركيبة الإدارة العمومية الإلكترونية من خلال متطلبات تجسيدها.

كما تم تناول هذا المنهج من خلال إبراز تطبيقات الخدمات العامة الإلكترونية عبر النماذج القطاعية، وتحليل مضامين القوانين والتشريعات والمواد القانونية وكذلك جمع معطيات ومعلومات حول حالة ما أو نموذج ما، وهو ما تم من خلال التطرق لنماذج الجرائم المعلوماتية في الجزائر عرفت الجريمة من بدء البشرية فهي قديمة قدم الوجود الإنساني، فالإنسان باعتباره شخص اجتماعي تحكم حباته رابطة مع أفراد مجتمعه في شتى مجالات الحداة، وبما أن تركيبة الإنسان هي مزج من الخبر والشر ونظرا لفطرته في إشباع حاجاته ورغباته والظروف الحتاتة وما تمخض عنها من صراعات لا زالت تعاني منها البشرية إلى البوم نتج عنها ارتكاب شتى أنواع الجرائم. إن مجال الجريمة متطور على الدوام بتطور الحداة وأساليبها وظروفها، فالجرائم التي كانت ترتكب في بداة العصور الأولى غر تلك التي ارتكبت في العصور التي ما بعدها لاختلاف نمط الحداة وحاجات الإنسان، ففي الماضي كان سعى إلى ضمان بقاءه عن طرق الصراع من اجل البقاء، وبعد التطور الحاصل في المجتمعات تطورت تطلعات الإنسان بتطور مجالات الحداة وكذلك بتطور واختلاف الزمان والمكان. فعندما تعارض المجتمع مع ما رده الإنسان، فهذا أولد لدته إحساس بالرغبة في

الانتقام ودافع للحصول على الكمال و الحداة الوفيرة وكما أن للجانب التربوي وتنشئة الإنسان و بعده عن الوازع الديني لها دور كبتر في اضطراب سلوكه، فالجانب الأخلاقي للفرد هو من وجه سلوكه للوجهة الصحيحة.

في الماضي كانت ترتكب جرائم تقليدية معهودة وضعت لها قوانسنا و قواعد تحكمها كما سلط المشرع لها عقوبات ملائمة لطبيعتها و جسامتها كجرائم السرقة و القتل و التهريب و الاختطاف على سبيل المثال، و كان المشرع قد عالج هذه الجرائم بنصوص ترجمة و أخرى إجرائية من اجل الوصول لكشف الحقائق و معاقبة الجاني.

و البوم بعد تطور مفهوم الجريمة و أساليب ارتكابها، تولدت نوعية من الجرائم حديثة العهد مثل الجرائم الإرهابية و الجرائم المنظمة العابرة للحدود و الجرائم المعلوماتية التي لها خاصية تجعلها تتطبع بخصوصية المجرم الذي أصبح طلق عله بالمجرم المعلوماتي، لان مرتكبها هم من فئات مميزة ممن لهم درابة و علم بالتقنيات الحديثة و تولدت لدمهم فكرة عن كفة ارتكاب الجرمة و كفة إخفاء أثرها لإبعاد الشبهة عنهم.

لقد ساعد المجرم المعلوماتي في ارتكاب الجرمة طبيعة البيئة الرقمية التي ارتكبت فاها و طابعها المادي و المعنوي، لأنها قد تطبعت بتطبع الواقع التكنولوجي و التقني الذي مكن المجرم من التفنن في الأعمال الإجرامية إلى ابعد الحدود مستعينا في ذلك بمختلف الوسائل العلمية و التكنولوجية التي لها طابع خاص، من بنها نظم الإعلام الآلي والشبكات العنكبوتية التي حولت العالم إلى قرة صغيرة شملت استعمالاتها مختلف نشاطات الإنسان التجارية إلى مجالات التعليم و الترفيه مما أدى إلى بروز أثارها في مجال الاتصالات و تبادل الأفكار نتج عنها عدة أنشطة إجرامية عابرة للحدود. لقد أثار البحث عن هذه الجرائم مشاكل و صعوبات في استخلاص الأدلة التي تثبت وقوعها و تدن مرتكبها، كونها تختلف عن الأدلة التقليدية في الجرائم العادية من حيث خصائصها و أنواعها و سبل جمعها ووسط ارتكابها وحتى صفات مرتكبها، كما ثر الدليل الالكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي و فقدان الآثار التقليدية للجريمة المعلوماتية، بالإضافة إلى صعوبات متعلقة بسلطات

الاستدلال و التحقيق من حيث إحجامهم عن الإبلاغ حرصا على ثقة العملاء أو لصعوبة اكتشافها من قبل الأشخاص العدان، فضلا عن نقص خبرة سلطات الاستدلال و التحق.

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجرمة والمجرمان متعودة على التعامل مع الجرمة بصورها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن خلفه مرتكبوها من آثار مادية في مسرح الجرمة من بصمات أو آثار أقدام أو بقع دم أو محررات مزورة فإن المشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجرمة المعلوماتية تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فاها، فهي لا تخلف أي آثار مادية محسوسة كما

أن هذه الجرمة تتم في الخفاء، فكثيرا ما عمد المجرم المعلوماتي إلى إخفاء نشاطه الإجرامي عن طرق تلاعبه بالبيانات والذي غالبا ما تحقق في غفلة من المجني عله فضلا عن سهولة تدمير الدليل ومحوه من مسرح الجرمة مما عقد أمر كشفها وتحديد مرتكبها. و على ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبرة في إثباتها أو التحقيق فاها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي.

كذلك ثر تساؤلات عديدة حول مشروعية وجود الدليل الالكتروني و مشروعية الحصول عله وأدلة الإدانة ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الحاسوب ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، وقد أثارت أمام القضاء مشكلات من حيث مدى قبولها وحجيتها والمعار المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية. إذن فإن البعد الإجرائي لجرائم الحاسوب والإنترنت نطوي على تحديات ومشكلات عناوينها الرئيسة، الحاجة إلى سرعة الكشف خشة ضياع الدليل، وخصوصية قواعد التفتيش و الضبط الملائمة لهذه الجرائم، وقانونية وحجية أدلة جرائم الحاسوب والإنترنت، والحاجة إلى

تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي.

كل هذا سنتناوله خلال تقسيمنا لهذا البحث ففي الفصل الأول تناولنا فآه مفهوم الجريمة المعلوماتية و أنواع تعريفاتها به و ما مزها من سمات و الدافع لارتكابها .

و في الفصل الثاني تطرقنا إلى الآليات الإجرائية للتحري عن الجريمة المعلوماتية و الإجراءات التقليدية و المستحدثة للتحري بهذا النوع من الجرائم التي نص علبها قانون 04/09المؤرخ في 14شعبان 1430 الموافق لـ 05أوت 2009المتضمن بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال .

و قد اتبعت في هذا البحث عدة مناهج منها المنهج الوصفي و يتجلى من خلال وصف طبيعة و أساليب البحث و التحري عن الجرائم المعلوماتية و المنهج التحليلي من خلال تحليلي و تفصيلي لإجراءات التفتيش و الضبط و التفاصيل المميزة للدليل الرقمي، كذلك المنهج المقارن حيث استخدمت هذا المنهج نظرا للطبيعة العالمية للجرائم المعلوماتية حيث بينت المعالجة التشريعية لها في النظم المقارنة و ما هي الوسائل التي استعملتها في معالجة هذا النوع من الجرائم.

تظهر أهمية هذه الدراسة من خلال ارتباطها الوثيق والمباشر بظاهرة جديدة، وهي الجرائم الإلكترونية التي بدأت في الظهور والانتشارً حالا، حيث تعتبر من المواضيع الشائكة التي بدأت تشغل فكر فقهاء القانون الجنائي، وتتطلب أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مسائل الإثبات الجنائي خاصة مسألة قبول وحجية الدليل الالكتروني حيث كانت من المسائل الهامة التي تعرضت لها المؤتمرات الدولية.

وتكمن أهمية هذه الدراسة في إلقاء الضوء على الآليات الإجرائية للتحري عن الجريمة ا المعلوماتية، وسنحاول من خلال الدراسة التعرف على مفهوم الجريمة و الآليات الإجرائية للتحري عن الجريمة المعلوماتية وكذلك التعرف الإجراءات التقليدية و المستحدثة للتحري.

تسعى هذه الدراسة لتحقيق هدف أساسي تمثل في التعرف على كافة الجوانب المتعلقة بإجراءات التفتيش والمعاينة والتحري في نظم الحاسب الآلي والإنترنت وطبعتها الخاصة المختلفة عن القواعد الإجرائية التقليدية والمستحدثة، بموجب قانون الإجراءات الجزائية وبموجب قانون 04/09.

تأثرت الجرمة بالتقدم العلمي والتكنولوجي المعاصر، وبرزت أساليب إجرامية بتقنيات لم تكن معروفة من قبل، وطوعت التقنيات الحديثة لارتكاب الجرمة في مراحلها المختلفة من تخطيط عداد واج وتنفذ وتضليل وتموه للإفلات من العدالة، فاستخدمت الأجهزة والأدوات والتقنيات الحديثة في ارتكاب الجرائم التي تميزت بالعنف. ومن الطبيعي أن صاحب التقدم العلمي ظهور أنماط من الجرمة لم تتضمنها التشريعات العقابية القائمة، وتبدو النصوص الجزائية قاصرة عن ملاحقتها، ذلك أن التشريع ولاد الحاجة لذا لم تتطرق التشريعات العربية إلى الجرائم المعلوماتية إلا نادرا، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية لمّ تتعد العقد الواحد، وإن كان دخوله إليها قد بدأ قبل ذلك بفترة طويلةً نسبا.

وتكمن صعوبة التعامل مع الجرائم المعلوماتية في صعوبة إجراء التفتيش القانوني، فإذ كانت الجرمة واقعة على المكونات المادية للكمبيوتر، فلا عائق حول دون تطبيق الإجراءات التقليدية و إجراء التفتيش، إذا كانت الجرمة واقعة على برامج الحاسب وبياناته، فإن الصعوبات تبرز على اعتبار أنه بإمكان الجاني التخلص من البيانات التي ستهدفها التحري عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر، وعلى اعتبار أن التحري عن هذه البيانات يستوجب الكشف عن الرقم السري إلى ملفات البيانات وهذا الرقم السري عرفه المتهم ولا يمكن إجباره على البوح به.

# الفصل الأول

# مفهوم الجريمة المعلوماتية

## المبحث الأول: تعريف الجريمة المعلوماتية

### المطلب الأول: تعريف الجريمة المعلوماتية

لم يتفق الفقه الجنائي على ايراد تسمية موحدة للجريمة المعلوماتية، فهناك من يطلق عليها تسمية الجرائم الإلكترونية، وهناك من يطلق عليها تسمية جرائم المعلوماتية، في حين يذهب اخرون الى تسميتها جرائم اسما استمدا تكنولوجيا المعلومات والاتصال، ويسميها اخرون جرائم الكومبيوتر والأنترنيت، وهناك من يطلق عليها الجرائم المستحدثة.

فمن يتصدى لتعريف هذه الجريمة قد يتناول تعريفها من زاوية تقنية (فنية) اومن زاوية قانونية.

فالقائلون بالتعريف التقني يذهبون الى القول بأن الجريمة المعلوماتية هي نشاط اجرامي تستمد فيه تقنية الحاسب الآلي بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الفعل الإجرامي المقصود.

ويذهب أنصار هذا الاتجاه الفقهي الى القول بان تعريف جرائم الحاسب الآلي من الناحية القانونية وتصنيف صورها يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جريمة الحاسب الآلي وهي: الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات الحيوية.

وهناك جانب اخر من الفقه يذهب الى تعريف جريمة الحاسب الآلي بأنها الجريمة التي تقع بواسطة الحاسب الآلي او عليه او بواسطة شبكة الأنترنيت، ويرى انصار هذا الجانب الفقهي ان من سمات هذه الجريمة انها جريمة مستترة، وتتسم بالسرعة والتطور في وسائل ارتكابها، وهي أقل عنف في التنفيذ من الجرائم التقليدية ، وعابرة للحدود ، ويصعب اثباتها

لعد وجود ادلة مادية عليها ، كما يسهل اتلف الأدلة لخاصة بها ، ونقص المبرة العلمية لدى الجهات القائمة على ضبطها ، وعد كفاية القوانين القائمة التي تعالجها . [1]

على الرغم من وضوح وبساطة التعريف الذي اورده أنصار هذا الجانب الى ان هناك من يأخذ عليه قصوره في عد الاشارة الى وقوع الجريمة المعلوماتية على شبكة الأنترنت كما في حالة تعطيل الشبكة عن العمل او العمل على بطئ سرعتها او اتلاف المواقع على هذه الشبكة.

وهناك اتجاه في الفقه يذهب الى تعريف الجريمة المعلوماتية اعتمادا على وسيلة ارتكاب الجريمة ، لذلك عرفها الفقيه الألماني تاديمان بأنها هي كل اشكال السلوك غير المشروع او الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي وفي ذات الاتجاه عرفت بانها الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل ايجابيا اكثر منه ا نظام الحاسوب وبعبارة اخرى هي تلك الجرائم التي يكون دور الحاسوب فيها سلبيا ، كما تعرف ا دورا لتمامه على ان يكون هذا الدور على قدر من الأهمية ابأنها كل نشاط اجرامي يؤدي فيه نظام الحاسب الآلي ويؤخذ على التعريفات التي اوردها انصار هذا الاتجاه اعتمادها على وسيلة ارتكاب الجريمة في تعريف الجريمة المعلوماتية ، ذلك ان تعريف الجريمة المعلوماتية يقو في الأساس على العمل الرئيسي المكون لها ولي س فقط على الوسائل المستخدمة فيها. ذلك انه ال يمكن ان يطلق على جريمة ما انها من جرائم الحاسب الآلي لمجرد ان الحاسب قد استمد في ارتكابها.

[1] – موقع يعني بشعبة القانون، موقع يعني بشعبة القانون، محاضرات، ندوات، كتب جامعية، مقالة و كل ما له علاقة القانون من منظور أكاديميUNIVERSITYLIFESTYLE.NET

ويذهب اتجاه اخر في الفقه الى التركيز على الجانب الموضوعي في تعريف الجريمة المعلوماتية باعتبار ان هذه الجريمة ليست الجريمة التي يستمد الحاسب الآلي كأداة في ارتكابها حسب بل تقع على الحاسب الآلي او في داخل نظامه.

فعرفت الجريمة المعلوماتية من قبل أنصار هذا الاتجاه بانها نشاط غير مشروع لنسخ او تغيير او حذف او الوصول الى المعلومات المخزونة داخل الحاسب او التي تحول عن طريقه (وعرفت كذلك بأنها) غش معلوماتي ينصرف الى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة.[2]

**الفرع الأول: التعريف اللغوي للجريمة المعلوماتية**

نتجت هذه الجرائم عن الاستعمال السيء للتكنولوجيا الحديثة والتطور الهائل التي عرفته وينتج عن ارتكاب هذه الجرائم خسائر كبيرة تقدر ب بملايين الدولارات ولا يقصد بهذه الجرائم سرقة الحواسب او إتلافها وإنما المقصود تلك الجرائم التي يتصرف على مكونات الحاسوب المتضمنة فيه كالبرامج والأنظمة.

وهناك تعريفات مختلفة لجرائم الحاسوب كمحاولة:

1 – تعريف يستند إلى وسيلة ارتكاب الجريمة يشترط في ارتكاب هذه الجريمة أن يكون الحاسوب وسيلة (Tiodeman) يعرفها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام أم الحاسوب

2– وتعريف يستند إلى موضوع الجريمة ويشترطون في ذلك وجوب كون الحاسوب محل الجريمة أي أن يتم الاعتداء على الحاسوب أو نظامه R.sembalatt عرفها بأنها نشاط غير مشروع موجه لنسخ أو تغيير او حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تخول عن طريقه .

[2] – موقع يعني بشعبة القانون، موقع يعني بشعبة القانون، محاضرات، ندوات، كتب جامعية، مقالة و كل ما له علاقة القانون من منظور أكاديميUNIVERSITYLIFESTYLE.NET

3- تعريف يستند على وجوب إلهام الفاعل بتقنية المعلومات واستخدام الحاسوب فقد عرفها (David Thompson) بأنها أية صريحة تتطلب لاقترافها دراية الشخص بتقنية الحاسوب وعرفها steim Schiolberg ) بأنها أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا .

4- تعريف يستند إلى معايير مختلفة: منظمة OCOE عرفتها بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المؤدية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية عرفها Man في اعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح وأيضا تعريف الخير الأمريكي Done B.Barker هي فعل جرمي له صلة بتقنية المعلومات يتكبد فيه المجني عليه نتيجة له خسارة ويتحقق الفاعل ربحا عمديا .[3]

**الفرع الثاني: التعريف الفقهي والقانوني للجريمة المعلوماتية**

التعريف الفقهي: نقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها، الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية. يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها ومن التعريفات التي وضعها أنصار هذا الاتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى وفي هذا الاتجاه أيضا الجانب الفقهي بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة الإلكترونية هي اعتداءات ترتكب بواسطة المعلومات بغرض تحقيق ربح.

كما عرف الأستاذ PARKER الجريمة الإلكترونية بأنها كل فعل إجرامي متعمد أيا كان صلة بالمعلوماتية ينشأ عنها خسارة تحلق بالمجني عليه أو كسب يحققه الفاعل الاتجاه الذي يوسع من مفهوم الجريمة الإلكترونية: عرف أصحاب الاتجاه الموسع الجريمة

- - [3]محمد أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة ص 14

الإلكترونية بأنها سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي جريمة تتم في محيط أجهزة الكمبيوتر، أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها، كما عرفها الفقيهان Michels&credo بأنها سوء استخدام الحاسب أو جريمة الحسابات تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه البيانات الخاصة، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وأيضا الاستخدام غير المشروع أو سرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته .[4]

التعريف القانوني:

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والاتصال فإنه يعرفها بأنها جرائم المساس بأنظمة المعالجة الآلية لمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية. وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نضم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية. ولول هذه النظم المعلوماتية وشبكات الاتصال ما كان أن نسبغ صفة المعلوماتية على هذه الجرائم. وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة 02من القانون 04-09على أنها جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. « ويلاحظ على هذا التعريف ما يلي:

[4]- مذكرة تخرج – جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري – الطالب مجمد بوعمرة وعلي بنينال – جامعة أكلي محمد الحاج – البويرة – 2019-2020 ص4.

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

- كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري.[5]

## المطلب الثاني: خصائص الجريمة المعلوماتية

نظرا للطبيعة المميزة للجريمة المعلوماتية باعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظيرها التقليدية بمجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، وتتلخص هذه السمات فيما يلي:

- خفاء الجريمة وسرعة التطور في ارتكاها، حيث تتسم أنها خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنا قد تقع أثناء وجوده على شبكة الاتصالات، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم. وقد تتم في ثانية وجزء من الثانية في بعض الجرائم.
- ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات وتجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب)،(hardware ومكوناته البرمجيات.
- يقوم مجرم ذو طبيعة خاصة وإمكانات خاصة علمية معلوماتية، يستخدم في ارتكاب جريمته الموارد المعرفية والأساليب الاحترافية.

[5] – مذكرة تخرج – جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري – الطالب مجمد بوعمرة و علي بنينال – جامعة أكلي محمد الحاج – البويرة – 2019–2020 ص 5

- صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر. ولعل صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثار تدل عليهم
- الجريمة الإلكترونية تستلزم طرقا خاصة مستحدثة للإثبات، قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسب الآلي، لذا فإنا تقتضي وجود رجل شرطة إلكتروني، ومحقق إلكتروني، وقاضي إلكتروني، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الاستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.
- هذه الجريمة لا يحدها مكان، فهي عالمية، إذ يمكن عن طريق الحاسب الآلي– أو حتى هاتف نقال الشخص في الصين مثلا أ ن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ضد شخص طبيعي أو معنوي في الو.م. أ، أو العكس.[6]
- تدني نسبة الإبلاغ عن الجريمة من طرف الجاني عليه خاصة في حالة شركات ومؤسسات، البنوك، وهو بنك " marchant Bank city" في بريطانيا لسرقة ثمانية مليون جنية إسترليني من إحدى أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته، قام البنك بدفع مليون جنية له، بشرط التزام الفاعل بعدم الإعلام عن جريمته، وإعلام البنك عن الألية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي. غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه.
- ذاتية الجريمة المعلوماتية تبرز بوضوح في أسلوب ارتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر، وتقليد لمفاتيح كما هو الحال في جريمة السرقة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية– الأنترنت – مع وجود مجرم يوظف خبراته وقدراته على التعامل مع

[6]– نايري عائشة – مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق والعلوم السياسية –جامعة أحمد داريه – أدرار – ص 15

الشبكة، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغرير أو التغرير بالقاصرين، كل ذلك دون الحاجة لسفك الدماء.

- الجريمة ا المعلوماتية تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بجاني عليه، وغالبا ما يشترك في إ خراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة الجاني عليها، لتغطية عملية التلاعب وتحويل المكاسب.

**الفرع الأول: الجريمة المعلوماتية عابرة للحدود**

إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير.[7]

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

[7] -مرجع سبق ذكره ص – 16-17

شخصا آخر موجود في بلد ثالث، أو القيام بإعداد أحد البرامج الخبيثة (Verus) في ثم ما بلد يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم.

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

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

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.[8]

[8] – مذكرة تخرج – جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري – الطالب مجمد بوعمرة و علي بنينال – جامعة أكلي محمد الحاج – البويرة – 2019–2020 ص 7–8

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى.

ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الاتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية.

**الفرع الثاني: الجريمة المعلوماتية صعبة الإثبات**

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

التي لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.[9]

كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ف ثم إنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها .فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم .

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

[9] – مذكرة تخرج – جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري – الطالب مجمد بوعمرة وعلى بنينال – جامعة أكلي محمد الحاج – البويرة – 2019–2020 ص 9–10

تم وقد طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الالتزام. وعرض ذات الاقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة.[10]

## المبحث الثاني: مفهوم المجرم المعلوماتي

يمكن القول ان فكرة المجرم المعلوماتي فكرة جديدة في الفقه الجنائي ففي الجرائم المعلوماتية لا نكون بصدد مجرم عادي بل نكون امام مجرم دي مهارات تقنية ودي علم بتكنيك المستخدم في نظام الحاسبات الالية فشخصية للمجرم المعلوماتي سواء اكان طبيعيا ام معنويا و الية ارتكابه الجريمة تجعل منه شخصا يتسم بسمات خاصة تضاف الى الصفات الاخرى التي يجي ان تتوافر مع المجرم العادي و لعل اهم ما يتميز به الشخص المذكور ان يتوافر لديه كشرط اساسي (داريه بالمسائل المعلوماتية) ومعرفة كافية بالية عمل الحاسب الألي وتشغيله باعتبار ان الاجرام المعلوماتي ينشا من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية او البيانات بيد ان دالك لا يعني تصور العنف الموجه ضد النظام المعلوماتي قد يكون محل الجريمة اتلاف الحاسب الالي او وحدة المعالجة المركزية اي ان ما يمكن الاعتداء عليه قد يكون بهيكلية الحاسبات لا بمعلوماتها المنتقلة عبر شبكة المعلومات واختلف اسباب ارتكاب الجريمة المعلوماتية من دوافع داخلية تجلت في كسب السريع من مال وبين اخرى خارجية اغلبها بدافع الانتقام يرتكبها المجرم المعلوماتي على حسب طائفة الاي ينتمي اليها فقد يكون هاكرز او هاوي كما قد ينتمي لطائفة اخرى اشد خطورة.

[10] – مرجع سبق ذكره ص 10 –11

## المطلب الأول: تعريف المجرم المعلوماتي

### الفرع الأول: المجرم المعلوماتي شخص طبيعي

لا شك ان الشخص الذي يرتكب الفعل غير مشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظر القانون مجرما ويتعرض للعقاب إذا ما اقترف جريمته ولذلك فإن فان العقوبة لكي تحقق هدفا مباشرا او غير مباشر لتحقيق هدفها في مجال الردع العام او الخاص وإذا كنا في مجال الاجرام المعلوماتي من حيث الظروف التي دفعته لارتكاب الجريمة واسبابها وصفاته وذلك حتى يمكن اعادة تأهيله اجتماعيا ويعود الى حظيرة المجتمع كمواطن صالح ينفع المجتمع ويضره.

والمجرم المعلوماتي هو المجرم الذي له القدرة على تحويل لغته الى لغة رقمية وخزينها واسترجاعها باستخدام الحاسب الالكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل او امتناع عنه مما يحدث اضطرابات في المجتمع الدولي او المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا او دوليا.[11]

بينما عرف الدكتور مصطفى يوسف كافي على انه مجرم " مختص و على مستوى عالي من المهارات و الحرفية و لابد ان يكون على مستوى عال من التعليم الا ان دالك كله لا ينفي عنه صفة الاجرام و المجرم المعلوماتي يحتاج لممارسة جريمته الى الولوج غير المشروع على ذاكرة الحاسب الالي لكي يلتقط المعلومات المخزنة او يعدل عليها و لطالما ارتبطت شخصية المجرم المعلوماتي بصورة الطالب في مجال العلوم المعلوماتية او بصورة دالك الشخص المهووس تقنية المعلوماتية غير ان التحول الجدري من حيث مدى خطورة هذه الافعال دفع و بصفة تدريجية الة تصنيفها ضمن مجال الاعتداءات التي تندرج في صنف الجريمة المنظمة .

[11] – مذكرة تخرج _ المجرم المعلوماتي _ جامعة عبد الحميد بن باديس _مستغانم _ كلية الحقوق والعلوم السياسية _ طالب عامر محمد الحبيب عبد القادر _2019–ص 42–43

و يعتبر تحديد الملامح الرئيسية لشخصية المجرم المعلوماتي من اهمية القصوى التي لا يمكن الاستغناء عنها من اجل شرح ظاهرة إجرامية في حد ذاتها و لعل ان الطريقة المثلى لفعل دالك هي اعتماد تجميع المجرمين المعلوماتيين الذين يشكلون الحد الأدنى من الملامح المنتشرة في المجموعات و زمر خاصة على الرغم من اختلافهم في اوصاف أخرى ان عدم اعتماد هذا الاسلوب في التصنيف يجعل من امر تفسير الظاهرة الاجرامية المعلوماتية امرا مستحيل و هو التفسير الملائم لضرورة رسم نموذج مجرم المعلوماتي يجتمع فيه اهم الملامح الرئيسية المميزة له عن غيرهن المجرمين . هذا الفاعل قد يكون بعمله الغير مشروع هذا اما يحشن نية او سوء نية فيرتكب اعمال الإتلاف او الاحتيال او السرقة او اساءة الامانة او الغش او الاعتداء على مواقع الانترنت مثلا او تخريب البيانات او المعلومات الموجودة على جهاز اخر او تشويه سمعة شخص او مؤسسة ونحوها وقد يسبب بفعله الضرر العظيم وقد لا يسبب منه شيئا.[12]

**الفرع الثاني: تعريف المجرم المعلوماتي المعنوي**

**موقف الشريعة الإسلامية:**

يفهم من كتب الفقهاء ان الشخصية الاعتبارية للشركات ونحوها تكون المسؤولة مسئولية مدنية وجنائية عما يصدر عنها فقد جعل الفقهاء ناظرا الوقف مسئولا عن الوقف و ما يتعلق به من متطلبات تجاه الغير لذا فان الشركات تكون مسؤولة من شخص مدير كما تقرر القوانين الوضعية.

**موقف القانون:**

نص عن الجرائم المستحدثة عن طريق الانترانت في للماظة 76 من القانون المصري على ان " يعاقب المسؤول عن الادارة الفعلية للشخص الاعتباري بذات العقوبات

[12] – مذكرة تخرج _ المجرم المعلوماتي _ جامعة عبد الحميد بن باديس _مستغانم _ كلية الحقوق والعلوم السياسية _ طالب عامر محمد الحبيب عبد القادر _2019–ص 47

المقررة عن الافعال التي ترتب بالمخالفة لا حكام هذا القانون إذا تبث علمه بها وكان اخلاله بالواجبات الي تقرضها عليه تلك الادارة قد أسهم في وقوع الجريمة.

ويكون الشخص الاعتباري مسؤولا بالتضامن عن الوفاء بما يحكم من عقوبات مالية وتعويضات. ومنه نستخلص ان المجرم المعلوماتي الاعتباري لا ت قع عليها عقوبات سالبة للحرية وانما يكون جزاءه عقوبات مالية بالإضافة لتعويضات يتم الحكم عليه بها نظير اقترافه لهذه الجرائم.

**العقوبة التكميلية المقررة للمجرم المعلوماتي الاعتباري:**

تطرق المشرع الجزائري الى عقوبات التكميلية للشخص المعنوي بالنسبة لجرائم اتلاف نظم المعلومات من خلال نص المادة 18 مكرر (معدلة) ولم يخرج المشرع الجزائري صراحة نظيره الفرنسي حيث وضحها هذا الاخير في نص المادة 313 – 39 من قانون العقوبات الفرنسي سوف نذكر منها:

- حل الشخص المعنوي منع ممارسة نشاط او عدة انشطة مهنية او اجتماعية سواء لمدة غير محدودة او لمدة خمس سنوات او أكثر
- الوضع تحت الرقابة القضائية لمدة خمس سنوات او أكثر.
- الغلق لمدة خمس سنوات او أكثر للمؤسسة او عدة مؤسسات هده الجرائم.
- المنع من التعامل مع الاسواق العانة لمدة غير محدودة او لمدة 5 سنوات.
- المنع من دخول مناقصة العان لمدة غير محدودة او لمدة خمس سنوات.

وبالتالي نتوصل ان المشرع الجزائري سلك نهج المشرع الفرنسي في وجه النصوص تشريعية خلاصة لمواجهة المجرم المعلوماتي الاعتباري بهدف التصدي لأثارها السلبية على المجتمع وتحدياتها الصعبة ودالك عن طريق سن القوانين في

مواجهة. الاشخاص الاعتبارية التي تقوم بالاقتراف هدا النوع من الجرائم بهدف الردع. [13]

**الفرع الثالث: خصائص المجرم المعلوماتي**

يتسم المجرم المعلوماتي وخاصة في مجال التجارة الإلكترونية بعدة صفات تميزه عن غيره من الجناة أو المتورطين في أشكال الانحراف أو الإجرام الأخرى، وهذه الصفات أهمها ما يلي:

**أولاً: أنه مجرم متخصص ويتمتع بالسلطة تجاه النظام المعلوماتي:**

غالباً ما يكون المجرم المعلوماتي متخصصاً ومحترفاً لجرائم الحاسب الآلي، وذلك للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسب الآلي من شرورهم، كما هو الحال في البنوك والتجارة الإلكترونية بشكل عام.

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، فتنفيذ جرائم التجارة الإلكترونية يتطلب قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الأخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو أن يكون لديه خبرة كبيرة فيه، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال بالإضافة إلى أن معظم مرتكبي جرائم التجارة الإلكترونية وجرائم المعلوماتية بشكل عام ليسوا من أصحاب السوابق، بل يكونوا على درجة عالية من المهارة التي تطلبها استخدام التقنية العلمية الحديثة والتكنولوجيا.

ونقصد بالسلطة التي يتمتع بها المجرم المعلوماتي تجاه النظام المعلوماتي هي الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطات مباشرة أو غير مباشرة في مواجهة المعلومات محل

[13]– طالب عامر محمد الحبيب عبد القادر _ مذكرة تخرج _ المجرم المعلوماتي _ جامعة عبد الحميد بن باديس _مستغانم _ كلية الحقوق والعلوم السياسية _ _2019–ص47–48

الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات التي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها. وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة. [14]

**ثانياً: المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء:**

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والإنترنت بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آلياً، فتنفيذ الجريمة المعلوماتية بشكل عام يتطلب قدراً من المهارة لدى الفاعل التي قد يكتسبها عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.

كما يتمتع المجرم المعلوماتي بقدر كبير من الذكاء وذلك نتيجة خبرته في هذا المجال واحترافه، فهو يستخدم الحاسب الآلي في تنفيذ مخططه الإجرامي، وهذا يستدعي تمتعه بقدر من الذكاء قد لا يتأتى للمجرم العادي، وذلك كي يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته، ولذلك غلب على المجرم المعلوماتي ارتكابه جريمة النصب باستخدام الحاسب الآلي، لأنها تتطلب قدراً من الذكاء. لذلك يقال عادة أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف.

كما أنه على درجة من العلم والمعرفة وهو ما يجعله ماهراً في ارتكاب جرائم ذوي الياقات البيضاء ،كما يتفق مرتكب جرائم التجارة الإلكترونية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق ، وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الأضرار بالأشخاص ـ الأمر الذي يعدونه غاية في اللاأخلاقية ـ وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم .

[14]– المحامي الدكتور مفيد عبد الجليل الصلاحي – صفاة المجرم المعلوماتي في التجارة الإلكترونية

**ثالثاً: إنه مجرم لا يستخدم العنف:**

يرتكب المجرم المعلوماتي نوعاً من الجرائم ينتمي إلى إجرام الحيلة، فهو لا يلجأ إلى استخدام القوة والعنف في ارتكاب جريمته، لا سيما وأنه لا يتعامل مع اشخاص حقيقين، بل يتعامل في مقومات غير مادية متمثلة في البيانات والمعلومات المخزنة في جهاز الحاسب الآلي، ولهذا فليس هناك مبرر للجوئه إلى العنف.

فالوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبياً بالبساطة وبسهولة الحصول عليها، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو ابتكار الأساليب التي تقلل من

الوسائل اللازمة لإتمام النشاط الإجرامي دون عنف.[15]

**رابعاً: إنه مجرم عائد إلى الإجرام:**

المجرم المعلوماتي يتميز بأنه يعود للجريمة دائماً، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات، لذا تدفع الرغبة في سد الثغرات التي أدت إلى التعرف على مرتكبي جرائم التجارة الإلكترونية وتقديمهم إلى المحاكمة في المرة السابقة ـ كثير من مجرمي المعلوماتية ـ إلى ارتكاب جرائم أخرى في مجال الحاسب الآلي، لتكون الجريمة أكثر إحكاماً عن تلك الجرائم التي ارتكبوها في المرات السابقة، ويؤدي ذلك إلى العودة إلى الإجرام وقد ينتهي بهم إلى تقديمهم للمحاكمة الجنائية مرة أخرى.

ويرى ستيفنسون أن الهاكر الهواة الذين يستخدم لوصفهم مصطلح (Crackers) غالباً ما يخترقون الحواسيب بدافع الفضول وحب التعلم، ولذلك فإنهم نادراً ما يقومون بتدمير البيانات أو الاحتيال أو غير ذلك من الأفعال التي حصر القيام بها في المجرمين المحترفين، لذلك كان الهاكر الهواة أولئك أكثر المجرمين عوداً إلى ارتكاب جرائمهم الإلكترونية لمرات عديدة بعد فضحهم ومتابعتهم قضائياً.

[15]– المحامي الدكتور مفيد عبد الجليل الصلاحي – صفات المجرم المعلوماتي في التجارة الإلكترونية –

**خامساً: المجرم المعلوماتي إنسان اجتماعي:**

المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية، وعادة ما يكون محل ثقة داخل الشركات التي يعمل بها، وعادة ما يكون على أهبة الاستعداد للعمل ويكون أول من يصل وآخر من يغادر العمل ويأخذ القليل من العطلات أو لا يأخذها وأيضاً دائماً يبرر أعماله الإجرامية أمام الآخرين عن طريق عرضها على أنها مجرد لعبة (Game) .بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه فهو إنسان شديد الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس القدرة على التكيف ولا يعني ذلك تقليلاً من شأن المجرم المعلوماتي، بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه.

كما أن شعور المجرم أنه محل ثقة من مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة في الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.[16]

## المطلب الثاني: الدوافع لارتكاب الجريمة المعلوماتية

### الفرع الأول: الدوافع الشخصية لارتكاب الجريمة المعلوماتية.

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة المعلوماتية، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين.

**1-الدوافع المادية:**

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية ، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع المجرم المعلوماتي إلى

[16] – المحامي الدكتور مفيد عبد الجليل الصلاحي – صفاة المجرم المعلوماتي في التجارة الإلكترونية

تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الألية لها من خلال اكتشافه لفجوات الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحساهم إن كان من خارج المؤسسة.

كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، وقد أشارت هذا الإطار مجلة " sécurité informatique" وهي مجلة متخصصة في الأمن المعلوماتي، أن 43%من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و 23%من أجل سرقة معلومات، و 19%أفعال إتلاف، و 15%الإستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المجرم المعلوماتي في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها ا المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة المعلوماتية ، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64%لحقت بهم خسائر مادية جراء هذه الاعتداءات. [17]

## 1- الدوافع الذهنية لارتكاب الجريمة المعلوماتي:

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات. وقد تكون هذه الدوافع مجرد شغف المعلوماتية والرغبة في تحدي وقهر النظام

[17]- نايري عائشة – مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق والعلوم السياسية –جامعة أحمد داريه – أدرار – ص 14

والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم المعلوماتي على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي و إثبات المقدرة.

**الفرع الثاني: الدوافع الخارجية لارتكاب الجريمة المعلوماتية:**

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال وأهم هذه الدوافع.[18]

**1-دافع الانتقام وإلحاق الضرر برب العمل:**

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته ،كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل معها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم المعلوماتي الرغبة في الانتقام من رب العمل، ومثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

[18]-نايري عائشة – مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق والعلوم السياسية –جامعة أحمد داريه – أدرار – ص 12-13

**2 –دافع التعاون والتواطؤ :**

هذا النوع يتكرر كثيرا في الجرائم المعلوماتية ، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة الجاني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة المعلوماتية ، مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة المعلوماتية قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.

# الفصل الثاني

# آليات التحري عن الجريمة المعلوماتية في القانون الجزائري

# الفصل الثاني: آليات التحري عن الجريمة المعلوماتية في القانون الجزائري

## المبحث الأول: الإجراءات التقليدية للتحري عن الجريمة المعلوماتية

إن التطور التقني الذي لحق نظم المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي، أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل، وهو ما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية.

### المطلب الأول: معاينة الجريمة المعلوماتية

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:

**1- معاينة الجرائم الواقعة على المكونات المادية للجهاز:**

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

**2- 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:

- نقص وقلة الآثار المادية التي تقع على المكونات غير المادية للجهاز.

- تردد عدد كبير من الأشخاص على مسرح الجريمة خال فترة زمنية قصيرة، والتي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة و الكشف عنها[19].

**الفرع الأول :المقصود بإجراء معاينة الجريمة المعلوماتية**

هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه وتقتضي المعاينة إثبات حالة الأشخاص والأشياء ،وكل ما يعتبر في كشف الحقيقة، وهذا المعنى تستلزم المعاينة الانتقال إلى محل الواقعة أو أي محل توجد به أشياء، أو آثار يرى المحقق أن لها صلة بالجريمة، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملابسا وتوفير أدلة مادية، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها.[20]

لأن الجريمة التقليدية غالبا لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية، على خلاف الجريمة الإلكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة، لأن الجريمة الإلكترونية قلما تخلف آثار مادية، وأن كثير من الأشخاص يردون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة، وحتى اكتشافها أو التحقيق فيها وهي طويلة نسبيا، الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالأثار المادية للجريمة إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة، 2ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي: تصوير جهاز الحاسوب وما قد يتصل به من أجهزة

[19]– جامعة أكلي محند اولحاج – البويرة كلية الحقوق والعلوم السياسية قسم القانون العام –اجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتي– ذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية11

[20]– مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق و العلوم السياسية –جامعة أحمد دارية – أدرار –طالية نايري عائشة ص 47

طرفيه ومحتوياته– عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغنطيسية في العالم الخارجي– حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية– ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغييرها.[21]

الفرع الأول: المعاينة

يقصد بالمعاينة مشاهدة و إثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها و هي من إجراءات التحقيق الابتدائي و يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، و تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لبيان مدى صحتها في الإثبات فليس الحال كذلك بالنسبة للجرائم المعلوماتية، حيث نادرا ما يتخلف عن ارتكابها آثار مادية و قد تطول الفترة الزمنية بين وقوع الجريمة و اكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها ،[22] وينبغي التعامل مع مسرح الجريمة الإلكترونية على أنها مسرحان:

**1–مسرح تقليدي:** ويقع خارج بيئة الحاسوب والانترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح جريمة تقليدية يترك فيها الجاني آثار كالبصمات أو وسائط تخزين رقمية و يتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

**2–مسرح افتراضي:** يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله1) (و التعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة

[21]– مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق و العلوم السياسية –جامعة أحمد دارية – أدرار –طالية نايري عائشة ص 47

[22]– هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتب الآلات الحديثة، د.ط، مصر، ،2002ص .39

الرقمية [23]. و عند تلقي بلاغ عن وقوع إحدى الجرائم المعلوماتية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، و يرى الفقه الجنائي ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية مثل تصوير الحاسب و الأجهزة الطرفية و إخطار الفريق الذي يتولى المعاينة والذي يعد خطة موضوعية بالرسومات، كما عليه إثبات حالة التوصيلات والكابلات ليتمكن من إجراء المقارنة عند العرض على المحكمة مع ضرورة عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل التأكد من خلو المحيط من أي قوى مغناطسية قد تتسبب في محو البيانات، كما يجب أن يتم التحفظ على محتويات سلة المهملات التي قد تكون ذات صلة بالجريمة، ومن الضروري أن تتم المعاينة من طرف المحققين ذوي الكفاءة العلمية و الخبرة الفنية في مجال المعلوماتية و أن تتم وفق مبدأ المشروعية **(3)**

**الفرع الثاني: قواعد اجراء معاينة الجريمة المعلوماتية**

هي جملة من الإجراءات المطبقة في كافة الجرائم، إلا أن التشريع الجزائري ينص على جملة من القوا اعد 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 ال يحتاج أي إذن ندب سلطة تحقيق بإجراءاتها أما إذا كان خاص فالبد من شروط خاصة .إذ أن الجرائم التي تقع في الوسط الإلكتروني أو داخل المنظومة المعلوماتية لها أساليب خاصة، نص عليها المشرع الجزائري من خال نصوص قانون الإجراءات الجزئية والمتمثلة في إخطار وكيل الجمهورية وأوقات إجراء المعاينات) بالإضافة إلى رضا صاحب السكن.

[23]– بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسة القانونية، العدد الأول68 ، ص2013

- **إخطار وكيل الجمهورية:**

يمكن معاينة الجرائم الماسة بأنظمة المعالجة الية للمعطيات إلا بعد إخطار وكيل الجمهورية بدائرة الاختصاص من قبل ضابط الشرطة القضائية، وهذا ما نصت عليه 1 المادة 42 من قانون الإجراءات الجزائية وعمال بنص المواد18 و32 و42 و63 من قانون الإجراءات الجزائية، بالإضافة إلى نص المادتان 42 و49 من قانون القضاء العسكري من واجبات ضباط الشرطة 2القضائية إذا ما علموا بأية جريمة بأن يقوموا بإخطار وكيل الجمهورية سواء كان مدنيا أو عسكريا باعتباره المسؤول المباشر عن الشرطة القضائية، على أن يكون الإخطار مسبوقا بتأكيد ضباط الشرطة القضائية من وقوع الجريمة فعال .كما أن الإخطار يكون باستعمال كافة الوسائل المتداولة عليها، فقد يكون بالكتابة أو باستعمال الهاتف النقال أو عن طريق أجهزة أخرى كالفاكس[24].

- **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 1 الجمهورية المختص .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 و في كل ساعة من ساعات النهار أو الليل دون تأخير هذه الإجراءات، عندما يتعلق الأمر

[24]– جامعة أكلي محند اولحاج – البويرة كلية الحقوق والعلوم السياسية قسم القانون العام –اجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتي– ذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية ص 11

بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما يجوز لضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك عن الجرائم داخل المنظومة المعلوماتية .

- **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 . 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 و مراعاة التاريخ والزمان والمكان الذي التقطت فيه كل صورة .واثبات الحالة التي تكون عليها توصيلات الكابلات ) الخيوط الكهربائية .
- يجب ملاحظة للجهاز( اللازمة، للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى ال يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجل.
- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي على المسئولين بها ودور كل واحد منهم
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن ملاحظة إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء .أجهزة أخرى

- إبعاد الموظفين والفضوليين على أجهزة العالم الآلي وكذلك عن الأماكن التي توجد بها .أمنة، إجراءات التحري الخاصة في مجال مكافحة الجرائم...( الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي ).[25]
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء ال يحدث أي إتلاف للبيانات المخزنة ومحو البيانات المسجلة .
- التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأو ارق الكربون المستعملة، و الشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، بالضاقة 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 العالم الآلي، واسترجاع المعلومات وممن تلقون التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة. [26]

## المطلب الثاني: التفتيش في الجريمة المعلوماتية

إن التفتيش في الجريمة المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه والذي يسهل إخفاءه وتدميره، وقد يتصل بدول أخرى مما يزيد صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها. كما أن التفتيش في الأنظمة الإلكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة. كما يجوز أن يصدر إذن

[25]– طالبة نايري عائشة مرجع سبق ذكره ص12

[26]– جامعة أكلي محند اولحاج – البويرة كلية الحقوق والعلوم السياسية قسم القانون العام –اجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتي– ذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية ص 13

التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعين توفر شروط تفتيش المساكن، أما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنه يكفي توفر شروط تفتيش الشخص. عند صدور إذن بتفتيش نظام معين لمعالجة المعلومات آليا للحصول على دليل يفيد في كشف الحقيقة عن جريمة معلوماتية معينة، يجوز تفتيش كل الملفات المتواجدة في النظام. إذا أسفر التفتيش عن ضبط البيانات المتواجدة في نظام المعالجة الآلية، فيمكن ضبطها دون ضبط النظام كله، وذلك بأخذ نسخة من البيانات الموجودة، ويلتزم المحقق بالتحفظ عليها بشكل يمنع العبث بها[27]. .

**الفرع الأول: تعريف اجراء التفتيش الجريمة المعلوماتية**

يعبر التفتيش من أخطر الحقوق التي منحت للمحقق وذلك لمساسها بالحريات التي تكلفها الدساتير عادة ، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن .

أن الأنظمة الجنائية عرفت في مراحل تطورها أنواعاً من الإجراءات تنطوي على انتهاك لحقوق الفرد الاولية في سبيل تتبع الجناة ومحاكمتهم ومنها القبض والتفتيش فاذا ما تخلت يد العدالة عن التعرض لحقوق الافراد لأصبحنا إزاء فوضى إجرامية ، ومن ثم يجب أن يتاح للقائمين على تنفيذ القانون نوع من السلطة في أنكار الحريات الشخصية بالقدر الذى يحول دون تسلط الاجرام على مقدرات الناس وإنما لا ينبغي أن يتجاوز هذا القدر ، إذ لا فارق بين أن تنتهك حريات الأفراد بمعرفة أشخاص يعملون تحت ستار القانون أو بمعرفة مجرمين يرتكبون أثماهم بمنأ عن سطوة القانون ومن هذه الاجراءات التفتيش

[27]– ليندا بن طالب مجلة العلوم القانونية و السياسية– التفتيش في الجريمة المعلوماتية

ومن أخطر الإجراءات التي يجريها مأمور الضبط القضائي في أثباته للجريمة اجراءات التفتيش سواء ما تعلق بشخص المتهم أو مسكنه لأنه ماس بحريته وسكينته ولخطورة ما يسفر عنه من أدلة تكشف وجه الحقيقة ، وقد حرص الدستور الدائم في جمهورية مصر العربية على تقرير حرمة الاشخاص والمساكن وجعلها مصونة لا يجوز المساس بها الا بأمر قضائي مسبب أو في حالة تلبس .

التفتيش عبارة عن الاطلاع على محل منح له القانون حرمة خاصة باعتباره مستودع سر صاحبه ، فلا يجوز الاطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها في القانون أو برضاء صاحبه ، وقد يكون محل التفتيش الشخص أو المسكن أو محل أخر الحقه القانون في حكم المسكن .

يعرف التفتيش بوجه عام بأنه عبارة عن " إجراء من إجراءات التحقيق التي تهدف إلي البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات ارتكابها أو نسبتها إلي المتهم وفقا لإجراءات قانونية محددة ".[28]

وعرفه البعض بأنه " البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون " . وعرفه أخرون بأنه هو " البحث عن الحقيقة في مستودع سرها حيثما تكون مع الشخص أو في منزل الحقيقة التي تتمثل في ثبوت أو انتفاء ارتكاب شخص معين لجريمة معينة وقعت بالفعل وأتهم هذا الشخص بارتكابها على أساس من الجدية التي تؤيدها أمارات قوية ".

ونخلص مما سبق أن المقصود بالتفتيش القانوني هو :

– الذى ينصرف على تفتيش الشخص أو المسكن وبالتالي تفتيش المحال العامة والتفتيش تلك الحالة يعد أجراء أدارى .

[28]– راجع في ذلك مؤلف : دكتور / خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، 2009

– التفتيش عملاً وأجراء من اجراءات التحقيق أي لابد من وقوع جريمة وأن يؤدى الى التوصل لحقيقتها وفاعلها .
– التفتيش عمل قضائي لا يجوز أن يقوم به إلا من خوله القانون صفة الضبطية القضائية .

وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبرراً في القانون لهذا الانتهاك ، لذا فهو يعد من بين أقصي الصلاحيات التي قد تمارسها الدولة ضد المواطن ويعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها .

يعرف التفتيش بوجه عام بأنه عبارة عن " إجراء من إجراءات التحقيق التي تهدف إلي البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات ارتكابها أو نسبتها إلي المتهم وفقا لإجراءات قانونية محددة " .

وعرفه البعض بأنه " البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد فى كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون " . وعرفه أخرون بأنه هو " البحث عن الحقيقة في مستودع سرها حيثما تكون مع الشخص أو في منزل الحقيقة التي تتمثل في ثبوت أو انتفاء ارتكاب شخص معين لجريمة معينة وقعت بالفعل وأتهم هذا الشخص بارتكابها على أساس من الجدية التي تؤيدها أمارات قوية " .

ونخلص مما سبق أن المقصود بالتفتيش القانوني هو :
– الذى ينصرف على تفتيش الشخص أو المسكن وبالتالي تفتيش المحال العامة والتفتيش تلك الحالة يعد أجراء أدارى .
– التفتيش عملاً وأجراء من اجراءات التحقيق أي لابد من وقوع جريمة وأن يؤدى الى التوصل لحقيقتها وفاعلها .
– التفتيش عمل قضائي لا يجوز أن يقوم به إلا من خوله القانون صفة الضبطية القضائية .
وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن

هناك مبرراً في القانون لهذا الانتهاك ، لذا فهو يعد من بين أقصي الصلاحيات التي قد تمارسها الدولة ضد المواطن ويعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها .[29]

**الفرع الثاني: قواعد إجراء التفتيش في الجريمة 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 الحالة 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 13هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك – 1 .راجع القانون 09/ 04 المتضمن القواعد الخاصة ل لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها.[30]

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

[29]– راجع في ذلك مؤلف : دكتور / خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، 2009 .

[30]– جامعة آكلي محند أولحاج – البويرة .كلية الحقوق والعلوم السياسية – مذكرة لنيل شهادة الماستر في القانون العام– تخصص القانون الجنائي والعلوم الجنائية ..قسم القانون العام .إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية ص 44–45

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 جوهانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم .

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 05وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كخبراء وتقنيين مختصين في العالم الآلي وفن الحاسوب لإجراء عملية التفتيش على المنظومة المعلوماتية وجمع

المعطيات 2المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات [31].

**1-إجراءات التفتيش في المنظومة المعلوماتية:**

**أ-تفتيش منظومة الحاسب الآلي المادية:**

إن الدخول للمكونات المادية للحاسب بحثا عن ما يتصل بجريمة معلوماتية للكشف عن مرتكبيها لا خلاف فيه بين الفقهاء طالما تم وفقا للإجراءات القانونية المقررة، فان كانت في مكان خاص كمسكن المتهم كان لها حكمه فلا يجوز تفتيشها إلا في حالات يجوز فبها تفتيش مسكنه بنفس الضمانات المقررة قانونا في التشريعات المختلفة و إن كانت في مكان عام كالمقاهي الشوارع كان لها حكمة [32]إلا أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية القانون 06-22 [33](2) استثنى بموجب المادة 45و كذا الفقرة 02من المادة 47و الفقرة الثالثة من المادة 64تطبيق هذه الضمانات عند التفتيش بخصوص جرائم المعلوماتية، أي أن المشرع لا يشترط حضور الشخص المشتبه فبه عند تفتيش مسكنه، و انه يجوز القيام بذلك في كل ساعة من ساعات الليل أو النهار و دون الحاجة إلى رضا صاحب الشأن[34] و قد نص المشرع الجزائري في المادة 44من ق.إ.ج أن التفتيش يرد على أشياء و هي كلمة تنصرف في الأرجح على المكونات المادية و بالتالي لا يوجد مانع قانوني أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته ومعداته.

---

[31]-جامعة آكلي محند أولحاج – البويرة .كلية الحقوق والعلوم السياسية – مذكرة لنيل شهادة الماستر في القانون العام- تخصص القانون الجنائي والعلوم الجنائية ..قسم القانون العام .إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية ص 45

[32]- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي في النظام القانوني لحماية المعلوماتية دون طبعة، دار الجامعة الجديدة، مصر، ص . 397

[33] – قانون 06-22المتضمن تعديل قانون الإجراءات الجزائية )الامر 66-155المؤرخ في 08يونيو ،1966يتضمن قانون الإجراءات الجزائية المعدل و المتمم- الجريدة الرسمية رقم 49سنة .(1966

[34] – المواد64 : ،47 ،45من قانون الإجراءات الجزائية

**ب- تفتيش مكونات الحاسب الآلي المعنوية:**

إذا كانت المكونات المادية للحاسوب صالحة للتفتيش كمحل فان امتداد ذلك إلى مكونات غير مادية هو محل جدل كبير حول مدى صلاحيتها أن تكون محل للبحث عن الأدلة المادية لتقديمها للمحكمة المختصة كدليل إدانة، لذا يثور الشك في ما إذا كان البحث عن الأدلة في الحاسوب نوعا من التفتيش باعتبارها ليس لها مظهر مادي، فنجد القانون اليوناني في المادة 251تعطي سلطة التحقيق إمكانية القيام بأي شيء يكون ضروري لجمع و حماية الدليل و يفسر الفقه اليوناني عبارة "أي شيء" تشمل البرامج و البيانات المعالجة الكترونيا وهناك جانب من التشريعات الإجرائية قد حدد الهدف من التفتيش في البحث عن الأشياء و ضبطها هذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس لا يمتد في نطاق شموله إلى الكيانات المنطقية، و قد عملت الدول التي تأخذ بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية، و يتضح موقف المشرع الجزائري من خلال قانون 09-04 حيث نص في المادة 05 على جواز تفتيش المنظومة المعلوماتية، و كذلك المشرع الفرنسي الذي قام بتعديل النصوص التي تحكم التفتيش و أضاف عبارة"المعطيات المعلوماتية" و قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي أخر أو في بلد أخر و نميز هنا بين احتمالين:

**الاحتمال الأول:** اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان أخر داخل الدولة: يثار هنا التساؤل عن مدى امتداد الحق في التفتيش إذا تبين إن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بنهاية طرفية في مكان أخر مملوك لشخص غير المتهم يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 163من قانون الإجراءات الألماني.

و يعتبر المشرع الجزائري من بين هذه التشريعات حيث نص في الفقرة الثانية من المادة 05 من قانون 09-04إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك. و المشرع الفرنسي قد حسم هذه المسالة بتعديله قانون الإجراءات الجزائية بموجب القانون2003/239 المتعلق بالأمن الداخلي الصادر في 18 /2003/03المادة 17 أجازت لضباط الشرطة القضائية أو تحت مسؤولياتهم الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي فيها التفتيش عن المعطيات التي تهم التحقيق و المخزنة في النظام المذكور أو في نظام أخر بما أن هذه المعطيات يتم الدخول إليها أو نكون متاحة انطلاقا من النظام الرئيس3)

**الاحتمال الثاني:** اتصال حاسب المشتبه فيه بحاسب آخر أو نهاية طرفية موجودة في مكان أخر خارج الدولة: يتم تخزين بياناته في أنظمة معلوماتية خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة 4) (في هذه الحالة فان امتداد الإذن بالتفتيش إلى خارج إقليم الدولة التي صدر من جهتها المختصة الإذن و دخول في إقليم دولة أخرى و التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك الدولة بسيادتها لذا لا بد من أن يتم التفتيش في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد أو عقد بين الدول المعنية، و هذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الالكتروني بموجب المادة 5/ القانون 04/09.

**ثانيا: ضوابط التفتيش**

**-الضوابط الشكلية للتفتيش**

إن القواعد الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات الفردية ولعل أبرز هذه الشروط هي:

**-إجراء التفتيش بحضور أشخاص معنين في القانون**

إن من التشريعات المقارنة من أوجب حضور عملية التفتيش الذي تجريه الضبطية القضائية المشتبه فيه أو شهود و أوجبت تشريعات أخرى حضور أشخاص معنين في القانون وأجازت في أحوال أخرى إجراء التفتيش دون حضور أحد، وهناك تشريعات سكتت تماما عن التعرض لهذا الشرط2) (والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء، و المشرع الفرنسي استوجب في الفقرة الأولى من المادة 57من قانون الإجراءات الجنائية حضور صاحب المسكن وعدم حضوره يترتب عليه البطلان .غير أن المشرع الجزائري بموجب المادة 45 من القانون رقم 06 – 22المؤرخ في 20 ديسمبر 2006 استثنى إجراء الحضور لبعض الأشخاص إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه اوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات.

**-محضر تفتيش نظم الحاسب الآلي**

التفتيش من أعمال التحقيق لذا ينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[35].

**-الميعاد الزمني لإجراء التفتيش :**

حرصت التشريعات الإجرائية على حضر تفتيش المنازل وما في حكمها في وقت معين فالقانون الفرنسي ينص في المادة 59من قانون الإجراءات الجزائية على أن التفتيش لا يمكن

[35] – مذكرة تخرج الطالبة غرباوي نادية – أساليب البحث و التحري في الجرائم المعلوماتية – جامعة اكلي محمد اولحاج – البويرة– كلية الحقوق و العلوم السياسية –قسم قانون عام 2017/2016 ص 63-62

أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساء، أما بالنسبة لتشريعات الدول الأنجلوسكسونية كالقانون الإنجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين والمشرع الجزائري ذهب إلى حضر تفتيش المساكن وما في حكمها في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساء و استثناء يصح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد 342إلى 348 (2)من قانون العقوبات المرتكبة في أماكن معينة أو في حالة رضا صاحب المسكن صراحة وفي نطاق التفتيش المتعلق بالجرائم المعلوماتية فإن الاستثناء الوارد بالفقرة الثالثة من المادة 47ق.إ.ج3) (المعلوماتية حيث جاء في نصها".... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ... فإنه يجوز إجراء التفتيش...في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص."

**-الإذن بالتفتيش:**

لم ينص المشرع في القانون 04/09صراحة على وجوب استصدار الإذن بتفتيش نظم المعلوماتية في حالة التحريات المتعلقة بالجرائم المتلبس بها أو التحريات الأولية لكن بالرجوع إلى الفقرة 05التي نصت على انه "يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ..." أي أن قيام ضباط الشرطة القضائية بالتفتيش يكون بناء على قواعد قانون الإجراءات الجزائية التي تفرض أن يتم التفتيش المساكن على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.

**-تحديد مجال الإذن بالتفتيش:**

أورد المشرع الجزائري على تطلب شرط التحديد لصحة الإذن بالتفتيش إذ نصت المادة ... 44 "يجب أن يتعين الإذن بالتفتيش بيان وصف الجرم وعنوان

**-الأماكن التي يتم زيارتها وتفتيشها:**

وذلك تحت طائلة البطلان" إلا انه وفي نطاق تفتيش الأنظمة المعلوماتية فان المادة المطلوبة قد تختلط بكميات من البيانات الأخرى التي لا تناسب الموضوع قيد التحقيق لذلك فإنه لا يستقيم الأمر مع مبدأ الخصوصية، كما أن ضبط النظام برمته قد يسبب خسارة ، ويثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه يرى البعض في هذه الحالة عدم امتداد البحث لديه إلا في حالتي التلبس أو رضائه بالتفتيش و يثور التساؤل حول ما إذا كان كل ملف يلزم إذن قضائي مستقل عن الأخر و المشرع الجزائري كأغلب التشريعات لا يقدم حلا لهذه المسألة، و في الولايات المتحدة الأمريكية وجد تضارب بين الأحكام القضائية بخصوص هذه المسألة ففي ما اعتبرت بعض الأحكام أن جهاز الحاسوب بما يحتويه من ملفات ومعلومات صندوقا واحدا ولا يستوجب تفتيشه إلا إذنا واحدا فقط، اعتبرت على خلاف ذلك أحكام أخرى أن كل ملف في الحاسوب يتطلب إذنا خاصا لتفتيشه و من الدول التي حددت مجال الإذن بالتفتيش الولايات المتحدة وكندا محل التفتيش يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سـر و محل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال. وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجود فيه فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا لاسيما اشتراط الإذن بالتفتيش من السلطات القضائية المختصة وهو ما نصت عليه المادة 44من قانون الإجراءات الجزائية[36].

**2-الضوابط الموضوعية للتفتيش لضوابط الموضوعية للتفتيش**

**-السبب:**

**أ- وقوع جريمة معلوماتية:**

[36]-الطالبة غرباوي تادية أساليب البحث و التحري في الجرائم المعلوماتية- نفس المرجع السابق 64

ضرورة وقوع جريمة من الجرائم المعلوماتية التي نص عليها المشرع في نصوص التجريم والعقاب، كما هو الحاصل في التشريع الجزائري الذي أدرج فصلا خاصا– الفصل السابع –في قانون العقوبات لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات ذلك أن التفتيش الذي يقع من أجل فعل لا بشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية غير مشروعة وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29يونيو 1990(2) .

**ب– ضرورة الاشتباه في شخص معين:**

لا يكفي لقيام سبب التفتيش وقوع جريمة معلوماتية بل لا بد أن يكون هناك اتهام موجه ضد شخص معين أو أن تتوافر دلائل كافية تدعو للاعتقاد بارتكابه للجريمة حتى يمكن انتهاك حق الخصوصية لديه وتفتش حاسوبه وبرامجه الخاصة ويمكن الاستدلال على ذلك بما نصت عليه المادة 46ق.إ.ج، ومن الدلائل المستمدة من القرائن التي تنبئ عن ارتكاب الشخص لجريمة معلوماتية وأن يتم تحديد هوية الحاسوب وكان يخص شخصا بعينه.

**ج–توافر قرائن لدى المتهم تفيد في كشف الحقيقة**

يجب توافر أمارات وقرائن قوية على وجود أشياء في كشف الحقيقة لدى المشتبه فيه أو غيره ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله. إلا أنه وبالرجوع إلى نص المادة 05(3)من القانون 09–04نجد أن المشرع قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة من نفس القانون، وهو الأمر الذي يفهم صراحة بقراءة نص المادتين معا .[37]

[37]– سعداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسة – قسم الحقوق– جامعة الحاج لخضر،2012/2013 ص 154

## المبحث الثاني: الاجراءات المستحدثة للتحري عن الجريمة المعلوماتية

### المطلب الأول: الاجراءات المستحدثة بموجب قانون الاجراءات الجزائية

إن القواعد الإجرائية التقليدية للتحقيق في الجرائم المعلوماتية هي قواعد عامة لا بد منها و لا يخلو أي تحقيق من اللجوء إليها إلا أنها و أمام الثورة المعلوماتية لا يمكن أن تكون الإجراءات الوحيدة التي تقود المحقق إلى العثور على الدليل لما تميز به هذه الجرائم المستحدثة من خاصية تختلف عن الجرائم العادية ومن ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية ما جاء به في القانون 22/06المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية الأمر 6156/66خلال إجرائي التسرب واعتراض المراسلات ثم من خلال القانون09/04 استحداث اجرائين آخران وهما المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير [38].

كما أن التعديل الأخير الذي قام به المشرع الجزائري لقانون الإجراءات الجزائية من خلال الأمر رقم 02/15 المؤرخ في 23 جويلية 2015 جاء بمجموعة من الأحكام والضوابط التي تعبر في مجملها عن نية المشرع في إضفاء نوع جديد من الآليات التي تدخل في إطار عصرنة قطاع العدالة، هذا المشروع الذي تبناه فخامة رئيس الجمهورية عبد العزيز بوتفليقة سنة 2005 وعكف على مواكبة التطورات الحاصلة لجعل القانون الجزائري يحقق الغاية التي يطمح إليها المواطن وهي حق المواطن في محاكمة عادلة وفق جهاز قضائي محكم، وهو الأمر الذي نلمسه في التعديل السابق ذكره، حيث جاء المشرع ببعض الأحكام التي تضمن أكثر من أي وقت مضى حقوق المتقاضين، وذلك من خلال تغيير جذري في بعض أنماط المحاكمة مثل المثول الفوري، مراقبة الحبس المؤقت..، وعمل على

[38]– مذكرة تخرج الطالبة غرباوي نادية – أساليب البحث و التحري في الجرائم المعلوماتية – جامعة اكلي محمد اولحاج – البويرة– كلية الحقوق و العلوم السياسية –قسم قانون عام 2017/2016 ص 76

حفظ حقوق المحبوسين المتهمين في جميع مراحل التحقيق بدءاً من الحبس المؤقت حتى الحكم، وهو المطلب الذي نادى به الحقوقيون، وقد جاء المشرع بمجموعة من الأحكام الإجرائية التي تصب في مصلحة المتهم مطبقاً في ذلك مبدأ المتهم بريء حتى تثبت إدانته[39].

**الفرع الأول: إجراء التسرب:**

يعتبر التسرب واحد من أهم وأخطر طرق البحث والتحري وأكثرها تعقيدا حيث يعتمد على المهارات والقدرات الشخصية لضباط وأعوان الشرطة القضائية القائمين بالعملية والتي تعتمد على الكفاءة والخبرة والحيلة والذكاء، وتستخدم فيها مختلف الأساليب من أجل كسب ثقة المشتبه فيهم وتحديد طبيعة ومدى النشاط الإجرامي .حيث يقوم ضابط أو عون الشرطة القضائية باختراق جماعة إجرامية باستعمال هوية مستعارة وا بغية مراقبة الأشخاص بإجرامهم بأنه فرد لا يتجزأ من العصابة الإجرامية المشتبه فيهم والحصول على المعلومات المتعلقة بمخططات العصابة والكشف عن أنشطتها الإجرامية والوسائل التي تستعملها في ذلك، وغيرها من المعلومات المتعلقة بالجريمة والمجرمين والتصرف في الوقت المناسب، شرط ألا يشكل هذا التصرف تحريضا على ارتكاب الجريمة.

وقد أطلق المشرع الجزائري على هذا الأسلوب مصطلح "التسرب" في قانون الإجراءات الجزائية بينما أطلق تسمية "الاختراق" في المادة 56 من قانون مكافحة الفساد، وقد ورد تعريف التسرب في المادة 65 مكرر 12 إي أنه: "يقصد بالتسرب قيام ضابط عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو

[39]– الكاتب : لهزيل عبد الهادي . لقليب سعد . مجلة الدراسات والبحوث القانونية– الآليات القانونية المستحدثة في التعديل الجديد لقانون الإجراءات الجزائية

خاف" فمن خلال هذا التعريف يتبين لنا أن المشرع الجزائري سمح لضابط أو عون الشرطة القضائية بالتسلل والتوغل داخل جماعة إجرامية بناء على إذن من السلطة القضائية )وكيل الجمهورية أو قاضي التحقيق )يهاجمهم باستعمال هوية مستعارة بأنه فاعل أو شريك أو خاف لهم في الجريمة، وذلك من أجل كسب ثقة أفراد الجماعة الإجرامية. فالتسرب بهذا المعنى مشارك إرادية لعناصر الشرطة في جماعة إجرامية.[40]

تعتبر الجريمة المعلوماتية من بين الجرائم التي يمكن فيها اللجوء إلى إجراء التسرب إذا اقتضت ذلك الضرورات التحري أو التحقيق بشأنها هو تقنية حديثة في التحري و التحقق عن أنواع الجرائم الواردة على سبيل الحصر في القانون، استحدثه المشرع الجزائري بمقتضى تعديل قانون الإجراءات الجزائية في . 2006 و التسرب هو قيام ضابط أو عون الشرطة الفضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك، ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال.[41]

أو يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم. وتظم أحكامه بموجب المواد من 65 مكرر 11إلى 65مكرر 18 منه. وقد ورد تعريف التسرب في المادة 65 مكرر 12(1) من ق. إ.ج التي يفهم منها ان عملية التسرب

[40]أ. معـزيز أمينة – التسرب في قانون الإجراءات الجزائية الجزائري كلية الحقوق والعلوم السياسية بجامعة مستغانم. 247-246

[41]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، ص 76

تتمثل في اقتراف ضابط الشرطة أو عون الشرطة القضائية لتنظيم اجرامي بما يمكنه من معرفة نشاط غير مشروع وتحديد دور كل عنصر من عناصره.[42]

**أولا: شروط التسرب:**

الجزائري في هذا الصدد كما أعطى لسلطات التحقيق إمكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم واخفاء أي أثر يدل عليهم، فمن ناحية أخرى لم يفتح الباب على مصراعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

**1-الشروط الشكلية:**

تنحصر الشروط الشكلية للتسرب في الإذن و ما يجب أن يتضمنه فلا يمكن أن يباشر ضابط الشرطة القضائية عملية التسرب بمفرده دون إذن من قبل الجهات القضائية و هذا ما نصت عليه المادة 65مكرر 11من قانون الإجراءات الجزائية، و يجب أن يكون الإذن مكتوبا و إلا كان الإجراء باطلا3) (كما يجب ان يتضمن ذكر هوية الضابط الذي تتم على يديه عملية التسرب و تحديد المدة المطلوبة في عملية التسرب و التي لا يتجاوز إجراء التسرب 04 أشهر تحدد حسب المقتضيات.

**2-الشروط الموضوعية:**

الأول يتمثل في تحديد نوع الجريمة والتي يجب ألا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65مكرر 5(4)أما الشرط الموضوعي الثاني فهو أن يكون الإذن

[42]- حزيط محمد، مذكرات في قانون الإجراءات الجزائية، ط 8،دار هومة للطباعة و النشر و التوزيع، الجزائر، 2013 ص 115

التسرب مسبباً، فمن خلال التسبب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن، لذلك فكان لزاماً عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية1.

**ثانيا: طرق التسرب في مجال الجريمة المعلوماتية:** يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أوصفات هيآت مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام الهاكر للموقع2).( من اجل القيام بعملية التسرب فقد أجاز المشرع استعمال أسالب و طرق خاصة أتاحت بدورها إمكانية اللجوء إلى استخدام عدد الوسائل و التقنيات هي في الأصل ليست مسموح بها قانونا لأنها تعتبر مساسا لمبدأ حرمة الحياة الخاصة غير انه لكل قاعدة استثناء و هو ما فعله المشرع الجزائري عندما تدخل بواسطة القواعد الإجرائية ليقيد أحيانا هذه الحرمة للحياة الخاصة .[43]

**الفرع الثاني : إجراء اعتراض المراسلات:**

الإذن المكتوب المسلم لضابط الشرطة القضائية المنتدب من قاضي التحقيق لتولي تدابير اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، يعطي الحق لحامله الاستعانة بأهل الخبرة، إذ له أن يسخر لأداء مهامه خاصة عند اعتراض المراسلات كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعملية (02 .مكرر2من ق. إ. ج. ج.)

[43]– الطالبة غرباوي تادية أساليب البحث و التحري في الجرائم المعلوماتية– نفس المرجع السابق ص78

ولكن ما لم يشر إليه المشرع في النصوص المنظمة لهذه التدابير، على من يقتصر الاطلاع على التسجيلات المتحصل عليها من إجراء هذه العمليات، هل على سبيل المثال بإمكان الفنيين المسخرين من ضابط الشرطة القضائية المنتدب الاطلاع على التسجيلات الصوتية أو السمعية البصرية والمراسلات التي تم تسجيلها أم لا؟ أم أن هذا الأمر يقتصر على قاضي التحقيق وضابط الشرطة القضائي المنتدب لإجراء العمليات فقط، على أن يقتصر دور من تم تسخيرهم من فنيين على إنجاح الترتيبات التقنية والفنية والضبط دون الاطلاع.

هذا ويخول الإذن كذلك لضابط الشرطة القضائية المنتدب لإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور الحق في وضع الترتيبات التقنية اللازمة دون انتظار موافقة من سيكون محلا له (م02 .مكرر 2/0من ق. إ. ج.).

والمشرع الجزائري لم يقيد في هذه العمليات كلها قاضي التحقيق أو الضابط المنتدب لإجراء هذه العمليات إلا باتخاذ الإجراءات اللازمة لضمان عدم المساس بالسر المهني (م02 .مكرر0من ق. إ. ج. ج.). اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في023...

فالمشرع الجزائري أطلق العنان لمنفذ إذن قاضي التحقيق، لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، فبخلاف القيد المقرر في المادة02 مكرر المذكورة أعلاه، فإن كل الوسائل تصبح مشروعة لبلوغ الهدف، فالحريات الفردية وحرمات الأمكنة وحرية الاتصال وحرمة الحياة الخاصة كمبادئ دستورية تصبح بدون معنى أمام هذا الإذن بمجرد تسبيبه بعبارة "لقد اقتضى التحقيق."

ومما تقدم فإن السؤال المطروح، ألا يجد قاضي التحقيق والمنتدب لإجراء هذه العمليات في الإذن الغطاء القانوني لعدم تحمل المسؤولية الجنائية وبالتالي التعسف؟

كان على المشرع على الأقل تفاديا للتعسف في استعمال السلطة أن يرتب بعض الجزاءات عند مخالفة بعض أحكام المواد المنظمة لهذه العمليات، فالواقع أثبت أن قاضي التحقيق ما هو إلا إنسان يتصرف بمفرده وهو دوما معرض للخطأ ينبغي على المشرع أن

يضع نصوصا تكون ضابطا لتصرفاته، ولا يترك له مطلق الحرية في التصرف دون رقيب أو حسيب.[44]

استحدث المشرع الجزائري بموجب القانون رقم 06-22المؤرخ في 20/12/2006 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وقد ضمنه ستة مواد من المادة 65مكرر إلى المادة 65مكرر 10وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه، و تتمثل في اعتراض كل المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية التي يقصد بها التنصت التليفوني و هي تقنية يتم من خلالها لاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء إلى تسجيل المكالمات فيأشرطة ممغنطة.[45]

*** شروط اعتراض المراسلات**

**1-ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:** طبقا للمادة 65مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الاعتراض وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا، و عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص

---

[44]- فوزي عمارة كلية الحقوق والعلوم السياسية جامعة منثوري قسنطينة الجزائر-اعتراض المراسلات و تسجيل الاصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائي

[45]- شيخ ناجية، أساليب البحث و التحري المستحدثة في قانون رقم 06-22المعدل و المتمم لقانون الاجراءات الجزائية، المجلة النقدية للعلوم السياسة، كلية الحقوق و العلوم السياسة، جامعة مولود معمري، تيزي وزو، ،2013ص . 29

بإعداد محضرا عن كل عملية اعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

**2-تحديد طبيعة المراسلة ومدة الاعتراض** : وهذا ما يفهم صراحة من نص المادة 65 مكرر 7التي نصت على أنه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها، كما أن المشرع قد أستوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق .[46]

## المطلب الثاني: الاجراءات المستحدثة بوجوب القانون 04/09

أدى التطور الكبير في عالم تكنولوجيا المعلوماتية وأجهزة الاتصال لاسيما منها الحواسيب وشبكة الانترنت إلى احتلالها مكانة خاصة في الحياة اليومية للمواطنين، لكن في المقابل ساهمت في بروز العديد من الجرائم المتصلة بها، التي أصبحت تشكل هاجسا حقيقيا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، الأمر الذي دفعها إلى العمل على مكافحتها، سواء من خلال إبرام اتفاقيات ثنائية ودولية أو وضع تشريعات وطنية للحد منها ومكافحتها، ولأن إفراد قانون خاص للحد ومكافحة الجرائم الالكترونية بات اليوم أكثر من ضرورة، حاولت الجزائر استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم، من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الجزائية، وتم تدعيمها بالقانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[47] .

---

[46]- الطالبة غرباوي تادية أساليب البحث و التحري في الجرائم المعلوماتية- نفس المرجع السابق ص79

[47]- الكاتب- شيخ عبد الصديق - الوقاية من الجرائم الالكترونية في ظل القانون رقم 09-04- معالم للدراسات القانونية والسياسية

**الفرع الأول: مفهوم إجراء المراقبة الالكترونية**

يقوم نظام المراقبة الإلكترونية على فكرة مؤداها ترك المحكوم عليه في الوسط الخارجي وعدم الحكم عليه بعقوبة سالبة للحرية قصيرة المدة، مع إخضاعه لعدد من ن بعد، ويتحقق ذلك فنيا عن طريق ارتداء الالتزامات ومرقبته في تنفيذها إلكترونيا المحكوم عليه أسورة إلكترونية في كاحله تقوم بإرسال مجموعة من الإشارات، تستقبل تلك الإشارات على جهاز مثبت في مكان يحدده قاضي تطبيق العقوبات، ويتصل 1بمركز المتابعة الموجود في المؤسسة عن طريق خط الهاتف. "

عرف نظام المراقبة الإلكترونية على أنه: "طريقة حديثة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج السجن، وذلك بإلزام المحكوم عليه بالمكوث في مقر إقامته أو في أي مقر آخر محدده خلال ساعات معينة يحددها القاضي، وللمحكوم عليه الالتحاق بعمله أو الاستمرار في دراسته، وكذلك الوفاء بمتطلباته السرية كافة وغيرها؛ ويتم تطبيق هذا النظام من خلال استخدام التكنولوجيا الحديثة، حيث تعهد المحكوم عليهّ هذه المهمة في مراقبة المحكوم عليه إلى جهاز إرسال يوضع على يدّ ن مؤسسة الصالح والتأهيل )المؤسسة العقابية( من التأكد من تنفيذ العقوبة "يمك . 2ولتطبيق هذا النظام يستوجب بعد صدور حكم نهائي يقضي بعقوبة سالبة للحرية، ثم يقوم قاضي تطبيق العقوبات أو مدير المؤسسة العقابية) حسب نظام الإشراف على تنفيذ الجزاء الجنائي (إخضاع المحكوم عليه لهذه الوسيلة متى توافرت الشروط المنصوص عليها قانونا، شأنها في ذلك شأن تطبيق نظام الوضع تحت الاختبار أو نظام الإفراج المشروط.

كما يمكن تطبيق هذا النظام من قبل قاضي الحكم إذا أعطى له القانون صراحة هذا الدور، وهذا نزولا عند مبدأ التفريد القضائي للعقوبة كما هو الحال بالنسبة إلى تطبيق نظام وقف تنفيذ العقوبة أو العمل لصالح النفع العام أو تجزئة العقوبة .وقد أدخل هذا النظام

كبديل للعقوبات السالبة للحرية قصيرة المدة في التشريعات العقابية في الولايات المتحدة الأمريكية ويدعى( monitoring-Electronic) وأقترح إدخاله منذ عام 0640 لكن التطبيق العملي لهذا النظام كان في عام 0604 ،وأدمج السوار الإلكتروني مع تدبير آخر وهو البقاء في البيت، وقد تطور هذا النظام في العشرين 01 سنة التالية، فطبقته كل من كندا وبريطانيا في عام 0606 ،والسويد في عام 0668 ،وهولندا في العام 0668 ،وفرنسا من خلال القانون رقم 64/0086 بتاريخ: 06 كانون الأول 0664 ،وأكمل بالقانون رقم: 0111/809 ثم أخذ سنده 1التشريعي في المادة 08/406 من قانون الإجراءات الجزائية الفرنسي ".

هذا وقد درس الفقيهان الأمريكيان (Lilly R–J et Ball A–R) تاريخ الوضع تحت نظام المراقبة الإلكترونية في الولايات المتحد الأمريكية، فوجد أن السوار الإلكتروني يحقق كل أغراض الردع والإصلاح والنفع المرتبطة بالعقوبات التقليدية، وهو يمثل جواب للحد من المشكلات العملية للعقوبات السالبة للحرية قصيرة المدة، ويعول اليوم على نظام الوضع تحت المراقبة الإلكترونية في تخفيف من أضرار تكدس السجون وتقليص نفقاتها، والحيلولة دون الآثار السلبية للسجن، بتجنيب المحكوم عليه الاختلاط بوسط السجن الفاسد.

والجدير بالذكر أنها بهذا النظام يتم تجنب مثالب العقوبات السالبة للحرية قصيرة المدة وما تعكسه من أثار ترجع بالضرر على المحكوم عليه وأسرته، كما يمكن أن ترجع بالضرر على الدولة من اكتظاظ لسجون ونفقات إيواء ورعايته.

**الفرع الثاني: خصائص إجراء المراقبة الإلكترونية:**

يمتاز نظام المراقبة الإلكترونية بمجموعة من الخصائص تميزه عن غيره من البدائل العقابية المقترحة للحد من مشكلة العقوبات السالبة للحرية قصيرة المدة وهي كالآتي:

**أولا: خضوع نظام المراقبة الإلكترونية لمبدأ الشرعية:**

يتميز نظام المراقبة الحكم الإلكترونية أنه ال يقرر إلا بموجب نص قانوني، وا بعدم مشروعيته، فالنص القانوني هو من يحدد كيفية تطبيق هذا النظام وما هي شروطه والحالات التي يفرض فيها، فالشرعية ال تشمل شرعية التجريم فقط ولكنها تشمل كذلك شرعية العقاب. إلا أنه يجب النظر في شرعية تطبيق نظام المراقبة الإلكترونية، ولا شك أن هذا يؤدي إلى فاعلية هذا النظام في إصلاح الجاني وتأهيله إعادة اندماجه في المجتمع مرة أخرى .

**ثانيا: خضوع نظام المراقبة الإلكترونية لمبدأ الشخصية**

لا يطبق نظام المراقبة الإلكترونية إلا على الشخص الذي تثبت إدانته بارتكاب جريمة معينة، فلا ينفذ هذا النظام إلا على من تبثث مسؤوليته الجنائية اتجاه ذلك الفعل، فلا يجوز أن يمتد هذا النظام لأفراد أسرته أو عائلته .

**ثالثا: تحقيق نظام المراقبة الإلكترونية أغراض العقوبة:**

سعى نظام المراقبة الإلكترونية إلى إصلاح الجاني وتأهيله إعادة الاندماج في النسيج الاجتماعي عقب تطبيق هذا النظام عليه وردعه وزجره هو وغيره من تسول له نفسه من ارتكاب هذا الجرم مستقبلا، وان كان تحقيق هذا النظام لأصالح الجاني وتأهيله لإعادة الاندماج في النسيج الاجتماعي ليس محل شك، حيث أن ارتداء أسورة إلكترونية قد حساسة أنه غير عادي بارتدائه هذا السوار يحقق إيلام الجاني ما يزيد اللوم في نفسه ويشعره بالذنب.

**رابعا: التقليل من النفقات المالية**

إن تكلفة نظام المراقبة الإلكترونية أقل من تكلفة الوضع في مؤسسة عقابية، فمجتمع السجن كما هو معروف مكلف ماليا، وقد أشار السيد Othily Georges في تقريره المقدم إلى مجلس الشيوخ الفرنسي إلى أن التكلفة اليومية لسجين في فرنسا ، عدا المصاريف الهامشية والطارئة، في فرنسيا مثال تبلغ بين 611-811 فرنكا حين قدر التكلفة اليومية

لموضوع تحت المراقبة الإلكترونية بقرابة 01-001 فرنكا فرنسا يوميا وهو الدليل على أن نظام المراقبة الإلكترونية يوفر العديد من النفقات مقارنة بالمصاريف التي كانت تصرف في ظل النظام العقابي التقليدي

هذا وبناء على إحصائيات ومقارنات بين نظام الوضع تحت الاختبار، تبين أن نظام المراقبة الإلكترونية أقل تكلفة من نظام الوضع في السجن، على الرغم من كبيرة نظرا ما ستلزمه من نفقات إطلاق نظام الوضع تحت المراقبة الإلكترونية ل تجهيزات وأمور تقنية، وبالرغم من ذلك إلا أن فرنسا وفرت من التكاليف الكثير في نهاية الامر إذ تقدر نفقات اليوم في الوضع تحت المراقبة الإلكترونية أقل بأربع مرات من يوم سجن.

**خامسا: التقليل من اكتظاظ السجون :**

أكدت المؤتمرات الدولية لمنع الجريمة والعدالة الجنائية على ضرورة الالتجاء إلى بدائل العقوبات السالبة للحرية ومنها نظام المراقبة الإلكترونية، وذلك بغية التخلص من مشكلة اكتظاظ السجون التي باتت تؤرق نظم العدالة الجنائية في جميع دول العالم، وتهدر حقوق المساجين ورعايتهم على أكمل وجه[48]

[48] فوزي عمارة كلية الحقوق والعلوم السياسية جامعة منثوري قسنطينة الجزائر-اعتراض المراسلات و تسجيل الاصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي

# الخاتمة

**الخاتمة:**

أصبحت المعلوماتية سمة العصر وبات استخدام الأنظمة المعلوماتية من قبل الأفراد والمؤسسات المقياس الذي يحدد مدى تطور الشعوب وتقدمها، فتكنولوجيا المعلومات ساهم في تسريع إنجاز الأعمال، الأمر الذي يعني تنفيذ الأهداف والخطط التي ترسمها الدول وذلك في وقت قياسي .فمن البديهي ان تكون نتيجة هذا التطور السريع والمتواصل في مجال المعلوماتية وتكنولوجيا الإعلام والاتصال ظهور أنماط جديدة من الجرائم لم تكن معهودة في السابق، إذا ان ارم والجريمة في تطور مستمر حيث أضحى النظام المعلوماتي ذاته محلا للاعتداء .ولقد ألقى هذا التطور المعلوماتي مسؤولية كبيرة على عاتق المشرع الجزائري مما أدى إلى تعديل قانون العقوبات وظهور قوانين خاصة لمكافحة جريمة المعلوماتية وكان يهدف من خلاله لخلق قاعدة قانونية موضوعية تحدد بالتفصيل كل الجرائم المتعلقة بتقنية المعلوماتية ووضع إطار لها حتى يتسنى للقضاء متابعتها وفقا لإجراءات خاصة .وفيما يلي بعض الاقتراحات التي ارتأينا أن تكون ناجعة لتعزيز لمكافحة جريمة المعلوماتية.

- التوقيع على اتفاقيات الدولية بشأن التعاون القضائي مع أكبر عدد ممكن البلدان.
- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.
- الاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن صورة...إلخ.
- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية والحد من أوثاره.

# المراجع

**المراجع:**

– موقع يعنى بشعبة القانون، موقع يعني بشعبة القانون، محاضرات، ندوات، كتب جامعية، مقالة وكل ما له علاقة القانون من منظور أكاديميUNIVERSITYLIFESTYLE.NET

– محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة.

– مذكرة تخرج – جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري – الطالب محمد بوعمرة وعلى بنينال –جامعة أكلي محمد الحاج – البويرة – 2019–2020.

– نايري عائشة –مذكرة تخرج –الجريمة الإلكترونية في التشريع الجزائري –كلية الحقوق والعلوم السياسية –جامعة أحمد داريه – أدرار.

– مذكرة تخرج _ المجرم المعلوماتي _ جامعة عبد الحميد بن باديس _مستغانم _ كلية الحقوق والعلوم السياسية _ طالب عامر محمد الحبيب عبد القادر _2019.

– المحامي الدكتور مفيد عبد الجليل الصلاحي – صفات المجرم المعلوماتي في التجارة الإلكترونية.

– جامعة أكلي محند اولحاج – البويرة كلية الحقوق والعلوم السياسية قسم القانون العام – اجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتي–مذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية 11.

– هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتب الآلات الحديثة، د. ط، مصر، 2002.

– بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسة القانونية، العدد الأول 68، 2013.

ليندا بن طالب، مجلة العلوم القانونية والسياسية، التفتيش في الجريمة المعلوماتية.-

– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009.

– طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي في النظام القانوني لحماية المعلوماتية دون طبعة، دار الجامعة الجديدة، مصر.

– قانون 06–22المتضمن تعديل قانون الإجراءات الجزائية) الامر 66–155المؤرخ في 08 يونيو، 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم–الجريدة الرسمية رقم 49سنة، 1966.

– المواد: 64، 47 ،45 من قانون الإجراءات الجزائية.

– مذكرة تخرج الطالبة غرباوي نادية – أساليب البحث والتحري في الجرائم المعلوماتية – جامعة اكلي محمد اولحاج –البويرة–كلية الحقوق والعلوم السياسية –قسم قانون عام 2017/2016.

– سعداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسة – قسم الحقوق– جامعة الحاج لخضر،2012/2013.

– الكاتب: لهزيل عبد الهادي . لقليب سعد . مجلة الدراسات والبحوث القانونية– الآليات القانونية المستحدثة في التعديل الجديد لقانون الإجراءات الجزائية.

– معـزيز أمينة –التسرب في قانون الإجراءات الجزائية الجزائري كلية الحقوق والعلوم السياسية بجامعة مستغانم.

– حزيط محمد، مذكرات في قانون الإجراءات الجزائية، ط ،8دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

– فوزي عمارة كلية الحقوق والعلوم السياسية جامعة منثوري قسنطينة الجزائر–اعتراض المراسلات وتسجيل الاصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائي.

– شيخ ناجية، أساليب البحث والتحري المستحدثة في قانون رقم 06–22المعدل والمتمم لقانون الاجراءات الجزائية، المجلة النقدية للعلوم السياسة، كلية الحقوق والعلوم السياسة، جامعة مولود معمري، تيزي وزو، 2013.

الكاتب– شيخ عبد الصديق – الوقاية من الجرائم الالكترونية في ظل القانون رقم 09–04– معالم للدراسات القانونية والسياسية.

**الملخص**

ان الحاسوب أصبح على مدى العقود الماضية ركيزة اساسية لأهداف التطور في كل مجالات الحياة بما فيها من انشطة مختلفة سواء اقتصادية ام علمية ام اجتماعية.... الخ وقد ادى الاستخدام المطرد للمعلوماتية سواء في شكل اموال معلوماتية ام اساليب مستحدثة إلى ظهور ما يعرف بالإجرام المعلوماتي اذ أن هذه نتيجة حتمية لكل تقدم علمي او تقني مستحدث ويرتكز هذا النوع من الاجرام على محورين أحدهما ضد المال والاخر ضد الاشخاص ويستمد نشاطه من الامكانيات الهائلة للحاسوب. فالحاسوب الالي بوصفه اداة للتخزين لديه قدرة على التخزين وتنظيم واستغلال عدد غير محدد من المعلومات وله في الوقت نفسه قدرة على استرجاعها في فترة زمنية وجيزة. ولكي يتحدد الاطار القانوني لهذه الجرائم بشكل اكثر وضوحا ينبغي التمييز بين نوعين من الجرائم او الاعتداءات المعلوماتية الاول عندما تكون تكنلوجيا المعلوماتية والاتصالات عن بعد قد استخدمت وسيلة لارتكاب الجرائم بمعنى اخر نكون والحالة هذه امام اعمال اجرامية ترتكب بمساعدة الحاسوب والوصف الجرمي لهذه الاعمال يتصل بأنواع الجرائم التقليدية كالاحتيال والسرقة وغيرها اما النوع الثاني من الجرائم المعلوماتية فهي حين تكون تكنلوجيا المعلوماتية والاتصالات عن بعد هدف الجرائم وغايتها وبذلك نكون امام افعال جرمية جديدة ترتبط في غالبيتها بالتعرض لأمن وسلامة الانظمة المعلوماتية ولسرية البيانات والمعلومات التي يحتوي عليها ويسمى هذا النوع بالإجرام المعلوماتي في شبكة الانترنيت ويتم ذلك في حالة الدخول غير المشروع إلى هذه الانظمة والتعرض لها وللمعلومات التي تتضمنها لذا سوف يرتكز بحثنا على اساليب البحث و التحري عن الجرائم المعلوماتية عندما تكون هدفا مباشرا وغاية في ذاتها بصرف النظر عن الباعث من وراء ارتكابها .

**Résumé**

Au cours des dernières décennies, l'ordinateur est devenu un pilier des objectifs de développement dans tous les domaines de la vie, y compris diverses activités, qu'elles soient économiques, scientifiques, sociales, etc. L'utilisation régulière de l'information, que ce soit sous la forme de fonds d'information ou de méthodes, a conduit à l'émergence de ce que l'on appelle le crime d'information. C'est un résultat inévitable de tout nouveau progrès scientifique ou technique. Ce type de crime repose sur deux axes, l'un contre l'argent et l'autre contre les personnes, et son activité découle des énormes capacités de l'ordinateur. L'ordinateur en tant qu'outil de stockage a la capacité de stocker, d'organiser et d'exploiter un nombre illimité d'informations et en même temps a la capacité de les récupérer dans un court laps de temps. Afin de définir plus clairement le cadre juridique de ces crimes, il convient Distinguer entre deux types de délits ou d'attaques contre l'information : le premier est lorsque les technologies de l'information et les télécommunications ont été utilisées comme moyen de commettre des délits, en d'autres termes, nous sommes et la situation.

Ceux-ci sont en face d'actes criminels qui sont commis à l'aide d'un ordinateur, et la qualification pénale de ces actes est liée aux types de délits traditionnels tels que la fraude, le vol et autres. Quant au deuxième type de délits d'information, il S'est alors que l'informatique et les télécommunications sont le but et la finalité des crimes. Ainsi, nous sommes confrontés à de nouveaux actes criminels, dont la plupart sont liés à l'exposition à la sécurité et à la sûreté des systèmes d'information et à la confidentialité. Les données et informations qu'ils contiennent, et ce Ce type est appelé délit d'information sur Internet, et cela se produit dans le cas d'une entrée illégale dans ces systèmes et d'une exposition à ceux-ci et aux informations qu'ils contiennent.

## الفهرس


| | |
|---|---|
| **الإهداء** | |
| **كلمة شكر** | |
| **مقدمة**..... | **2-7** |
| **الفصل الأول:** | |
| **المبحث الأول: تعريف الجريمة المعلوماتية**..... | **9** |
| **المطلب الأول: تعريف الجريمة المعلوماتية**..... | **9** |
| **المطلب الثاني: خصائص الجريمة المعلوماتية**..... | **14** |
| **المبحث الثاني: مفهوم المجرم المعلوماتي**..... | **20** |
| **المطلب الأول: تعريف المجرم المعلوماتي**..... | **21** |
| **المطلب الثاني: الدوافع لارتكاب الجريمة المعلوماتية**..... | **27** |
| **الفصل الثاني: آليات التحري عن الجريمة المعلوماتية في القانون الجزائري** | |
| **المبحث الأول: الإجراءات التقليدية للتحري عن الجريمة المعلوماتية**..... | **32** |
| **المطلب الأول: معاينة الجريمة المعلوماتية**..... | **32** |
| **المطلب الثاني: التفتيش في الجريمة المعلوماتية**..... | **38** |
| **المبحث الثاني: الاجراءات المستحدثة للتحري عن الجريمة المعلوماتية**..... | **51** |
| **المطلب الأول: الاجراءات المستحدثة بموجب قانون الاجراءات الجزائية**..... | **51** |
| **المطلب الثاني: الاجراءات المستحدثة بوجوب القانون 04/09**..... | **58** |
| **الخاتمة**..... | **64** |
| **المراجع**..... | **66** |
| **الملخص**..... | **69** |
| **الفهرس**..... | **71** |