وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي – برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماسترأ كاديمي في الحقوق

تخصص: قانون إعلام آلي وانترنت

الموسومة بـ

التفتيش في الجرائم المعلوماتية

إعداد الطالبتين:

✓ نواصرية ليلى

✓ سليم نصيرة

إشراف الدكتور:

*عبد الله ذوادي

لجنة المناقشة:

الإسم واللقب	الرتبة	الصفة
د/ حسين بن داود	أستاذ محاضر .أ.	رئيسا
د/ عبد الله ذوادي	أستاذ محاضر.أ.	مشرفا ومقررا
د/ عبد الحليم حاجي	أستاذ مساعد.أ.	مناقشا

السنة الجامعية 2023/2022

ملحق بالقرار رقم .... المؤرخ في .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بوا صوريه ليلى ..... الصفة: طالب، أستاذ، باحث .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 111487776 والصادرة بتاريخ 2018/10/19 .....

المسجل(ة) بكلية / معهد كلية الحقوق قسم علوم الإعلام والاتصال وعلم المكتبات

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: السفيسفة في الصراع الإعلامي .....

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2023/06/14

توقيع المعني (ة)

نظر للمصادقة على إمضاء
السيدة : .....
بطاقة هوية رقم 13 جوان 2023
عين تاغروت في : .....
رئيس المجلس الشعبي البلدي

رئيس المجلس الشعبي البلدي
ونائب الرئيس
العياشي تويري

ملحق بالقرار رقم ..... المؤرخ في .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): سليم نصيرة ..... الصفة: طالب، أستاذ، باحث .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 109328422 والصادرة بتاريخ 2018.05.24 .....

المسجل(ة) بكلية / معهد الحقوق ..... قسم قانون العلاقات الدولية .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: المقاومة في الحرب المعلوماتية .....

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2023.06.14 .....

أطلع عليه لتأكيد التوقيع
السيد: (ة) سليم نصيرة
عين وسارة في 14 جوان 2023

توقيع المعني (ة)

رئيس المجلس الشعبي البلدي
الموظف المفوض
طياري طارق


بسم الله الرحمن الرحيم

كلمة شكر

قال الإمام الشافعي رحمه الله

إن العلم بطيء اللزام، بعيد المرام لا يدرك بالسهام،

ولا يرى في المنام، ولا يورث عن الآباء والأعمام،

إنما هو شجرة، لا تصلح إلا بالغرس، ولا تغرس إلا في النفس،

ولا تسقى إلا بالدرس

أما بعد :

لا يسعنا، ونحن على أبواب التخرج إلا أن نقدم بالشكر الجزيل

إلى أساتذتنا الكرام

إلى الذين ساهموا في تكويننا طيلة السنتين

ونخص بالذكر الأستاذ المشرف

****** ذوادي عبد الله ******

لكل مجهوداته الجبارة، ونصائحه القيمة وصبره علينا

وعلى توجيهاته لنا التي أفادنا بها خلال إنجاز هذا البحث

كما نتقدم بالشكر الجزيل

إلى كل زملائنا وزميلاتنا خاصة الفوج رقم 03

إلى كل متخرجي دفعة 2023

كما نتقدم بالشكر إلى كل من ساعدنا من قريب أو بعيد لإنجاز مذكرة التخرج

لكل هؤلاء فائق الشكر وجزيل التقدير والاعتراف بالجميل .

عن الطالبتين: - سليم نصيرة.

- نواصرية ليلى .

إهداء

إلهي لاتطيب اللحظات إلا بذكرك وشكرك.... ولا تطيب الآخرة إلا بعفوك... ولا تطيب

..اللجنة إلا برؤيتك

أهدي تخرجي إلى

من كلله اللّه بالهيبة والوقار... إلى من علمني العطاء بدون انتظار... إلى من أحمل اسمه

بكل فخر واعتزاز والدي العزيز

..وإلى ملاكي في الحياة... إلى منبع الحب والحنان

...إلى من وضعت الجنة تحت أقدامها

أمي الغالية

إلى كل أقربائي وعائلتي وكل من ساهم في مساعدتنا ولو بالقليل من قريب أو وخاصة

إلى الأستاذ عبد الله ذوادي على ما قدمه لنا من نصائح و توجيهات لإكمال هذا .العمل

أدعو الله ان يوفقني على رد جميل عطائكم و مساندتكم لي.

*** نصيرة***

إهداء

*إلى أمي *

إلى أبي

إلى من نفضلهم على أنفسنا ولم لافلقد ضحوا من أجلنا،ولم
يبخلوا علينا من فضلهما في سبيل إسعادنا على الدوام

عائلتي الكريمة
والى من كانوا بمثابة العضد والسند في سبيل إنجاح حياتي
الدراسية
جميع افراد عائلاتنا
والى كل من ساعدنا من قريب أومن بعيد وخاصة *عبد الله ذوادي*
أهدي لكم بحث تخرجي هذا
داعياً المولى عزوجل أن يطيل في أعماركم ويرزقكم بالخيرات

ليلى

قائمة المختصرات:

الرمز	الكلمة
ص	الصفحة
ف	فقرة
ط	طبعة
ع	العدد.
إ ج	إجراءات جزائية
ق	قانون

مقدمة

مقدمـــــة

لقد شهد العالم اليوم ثورة كبيرة من نوع آخر في مجال الاتصال والمعلومات، نتيجة التطور الذي تجسد أساسا في انتشار أجهزة الحاسب الآلي والتي تطورت بشكل مستمر .بالإضافة إلى البرامج المتقدمة، وشبكات الاتصال التي قربت ملايين النشر بعضهم البعض وأتاحت فرصا جديدة للاطلاع على المعلومات وتبادلها، وحتى التفاوض وإبرام عقود مختلفة خصوصا عبر شبكة الانترنت، بل الأكثر من ذلك يمكن عبر هذه الأخيرة تسليم المنتجات كالبرامج، أو القطع الموسيقية، أو الصحف الإلكترونية، أو تقديم الخدمات مثل: الاستشارات القانونية أو الطبية .

وعلى الرغم من المزايا والفوائد الجمة التي تحققت وتتحقق يوم بعد يوم في كل نواحي الحياة وبفضل تقنيات ووسائل تكنولوجيات المعلومات والاتصالات، إلا أن الاستخدام المتناهي لهذه التقنيات انطوى في الوقت ذاته على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع جراء سوء استعمال هذه التقنيات واستغلالها على نحو غير مشروع ويطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات والمساس بأمن الدول واستقرارها، الشيء الذي استتبعه ظهور نمط جديد من الجرائم ازدادت مع الوقت وتعددت صورها وأشكالها يطلق عليها تسمية " الجرائم المعلوماتية "

وقد عرفت تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها والتي تتمثل في استخدام آخر ما توصل إليه العلم وتطويعه في خدمة الجريمة .

فالجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان سلبي أو ايجابي فهي أيضا معنية بالمكافحة فكان لا بد من إيجاد إطار قانوني مناسب لسد الفراغ الإجرائي ، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الالكترونية عن طريق تعديل قانون الإجراءات الجزائية لتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ،

ومنها الجريمة الإلكترونية التي أحدثت انقلابا هاما في النظريات التقليدية بما فيها نظرية الإثبات الجنائي وتحديد ما إذا كانت النصوص الجنائية التقليدية تواجه الأفعال الغير مشروعة التي ترتكب عبر شبكة الانترنت .

ومع التطور التكنولوجي للاتصالات الذي يشهده العالم الحالي والذي استفاد منه عالم الإجرام وجدت جرائم حديثة .يطلق عليها مصطلح الجرائم المعلوماتية والتي أثارت العديد من المشكلات في نطاق قانون الإجراءات الجنائي، حيث وضعت نصوص هذا القانون لتحكم الإجراءات المتعلقة بالجرائم التقليدية، التي لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الإقناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم .

أما في الجرائم المعلوماتية فيتسم إجراء التفتيش من أهم إجراءات التحقيق – فيها بالعديد من المعوقات والصعوبات، فنظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم والشبكات بمختلف أنواعها .

أهمية الموضوع:

مما لاشك فيه أن الجرائم المعلوماتية تعتبر من أحدث وأهم الجرائم في هذا الوقت، فهي تحتاج إلى قانون إجرائي وعقوبات معينة أي قانون موضوعي وتكمن أهمية الدراسة في بذل الجهد لوضع حلولا للمشكلات القانونية التي تقف في طريق إجراء التفتيش في الجرائم المعلوماتية، وإغلاق أي ثغرة موجودة في هذا المجال ووضع الحلول الملائمة لسد هذه الثغرات وذلك بوضع تشريع جزائري خاص بالإجراءات المتعلقة بالجرائم المعلوماتية . ومن هذا المنطلق فإني اخترت هذا الموضوع المهم لأنه كما ذكرنا سابقا يعتبر من الجرائم الهامة التي تحتاج إلى دقة وخبراء مختصين لإخراج هذه الأدلة الهامة أثناء التفتيش عن المعلومات الجنائية الإلكترونية .

أهداف الدراسة :

الهدف من هذه الدراسة هو تسليط الضوء على إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية ، وإبراز خصوصيتها بالنسبة للجرائم التقليدية

الدراسات السابقة:

خلال البحث اطلعنا على العديد من الدراسات السابقة، لم نصادف أي موضوع سابق يتناول التعديلات الحديثة للمشرع الجزائري بخصوص هذه الجرائم إلا في بعض جزئيات من موضوعنا نذكر منها:

1 / الدراسة الأولى: "التحقيق الجنائي في الجرائم الالكترونية"، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون ، الطالب برا هيمي جمال ، جامعة مولود معمري تيزي وزو 2018 .

كان الهدف من هذه الدراسة التعرف على طرق وآليات التحقيق في مثل هذه الجرائم ، ثم اقتراح الحلول القانونية المناسبة والممكنة لتجاوز العقبات وللاستفادة منها في المواجهة الفعالة للجرائم الالكترونية .

وأيضا كون هذه الدراسة تطبيقية لأنها تأتي في وقت تهم فيه عدة دول بما فيها الجزائر إلى إعادة النظر في قوانينها الإجرائية ، مما قد يتيح لهذا البحث توجيه أنظار المشرع في هذه الدول إلى ضرورة مسايرة تشريعات للتطور التكنولوجي واستدراك الفراغ التشريعي الملحوظ في هذا المجال .

2 / الدراسة الثانية: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جانفي 2018 .الهدف من هذه الدراسة هو تسليط الضوء على إجراءات التحقيق والتفتيش في الجرائم المعلوماتية، وإبراز خصوصيتها بالنسبة للجرائم التقليدية .

تنطلق هذه الدراسة من إشكالية محورية هل **أعطى المشرع الجزائري خصوصية إجرائية للتفتيش تتوافق مع خصوصية مسرح الجريمة المعلوماتية ؟**

وتتفرع هذه الإشكالية الرئيسية إلى جملة من التساؤلات الفرعية تتمثل فيما يلي:

1- ما ماهية إجراء التفتيش في الجرائم الإلكترونية ؟

2- هل يوجد تشريع إجرائي جزائري ينظم الجوانب الإجرائية عند ارتكاب جريمة معلوماتية؟

3- ما هي الصعوبات التي تواجهها الضبطية القضائية أثناء التفتيش في الحاسب ؟

4- ماهو سبب إحجام أكثر الضحايا في هذه الجرائم عن الإبلاغ عن هذه الجرائم ؟

واعتمدنا في دراستنا هذه على المنهج التحليلي كونه الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية على وجه الخصوص .

وللإجابة على هذا الإشكال المطروح اتبعنا المنهجية التالية، حيث قسمنا البحث إلى فصلين، الفصل لأول تناولنا فيه ماهية الجرائم الإلكترونية من خلال التطرق إلى مفهوم الجريمة الالكترونية في المبحث الأول وإجراءات البحث والتحري في الجرائم المعلوماتية في المبحث الثاني . ليصل بنا إلى الحديث عن التفتيش في الجرائم الإلكترونية في الفصل الثاني، بحيث تناولنا في المبحث الأول مفهوم التفتيش وشروطه أما المبحث الثاني تناولنا الإجراءات التحضيرية والفنية للتفتيش في الجرائم الالكترونية وآثاره.

الفصل الأول:

ماهية الجرائم الإلكترونية.

الفصل الأول: ماهية الجرائم الإلكترونية.

إن التطور الهائل في تكنولوجيا المعلومات والاتصالات والاعتماد المتزايد على التقنية والانترنت أدى إلى ظهور نوع جديد من الجرائم المستحدثة تختلف عن الجرائم التقليدية أطلق على تسميته بالجرائم الإلكترونية أو الجرائم المعلوماتية **cyber crime** نتيجة للاستخدام السيئ للتقنيات الحديثة من أجل القيام بأعمال إجرامية بسرية تامة، جعل من الانترنت بيئة مثالية لتنفيذ العديد من الجرائم المتعددة والمتنوعة يصعب حصرها .

وقد عرفت تطورا ملحوظا في عصرنا نتيجة اعتمادها على الوسائل التي أتاحتها الثورة المعلوماتية خاصة الانترنت والأجهزة الذكية ليصبح إجراما لا حدود له على مستوى العالم الافتراضي وكانت الجرائم المرتكبة باستخدام التقنية من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي .

وعليه سوف نتناول في هذا الفصل مفهوم الجريمة الالكترونية في المبحث الأول، كما سنتطرق في المبحث الثاني إلى إجراءات البحث والتحري في الجرائم الالكترونية .

المبحث الأول: مفهوم الجريمة الالكترونية.

تعتبر الجريمة المعلوماتية ظاهرة إجرامية حديثة النشأة، وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات والكمبيوتر، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، بل إن البعض ذهب إلى ترجيع عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني ومما لا شك فيه أن عدم الاتفاق على وضع تعريف شامل للجريمة المعلوماتية هو خشية حصر نطاقها داخل إطار تجريمي محدد قد يضر بها خاصة في ظل التطور المستمر للتقنية المعلوماتية والذي نلمسه كل يوم، فما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى قد ظهرت نتيجة استخدام تقنيات جديدة .[1]

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، مستغانم الجزائر، 2012، ص 98 .

وبالرغم من ذلك نجد البعض المهتمين بهذا النمط الجديد من الإجرام من الفقهاء قد بذلوا جهودا كبيرة في محاولة تعريف مناسب يتلاءم وطبيعة الجرائم المعلوماتية .

أو الجرائم الإلكترونية[1]

المطلب الأول: تعريف الجريمة الإلكترونية.

حيث أدت الحداثة التي تتميز الجرائم الالكترونية واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح موحد للدلالة عليها ، وعدم الاتفاق هذا أنجز عليه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية المستحدثة ، فالبعض من الفقهاء ينظر إليها بالمفهوم الضيق والآخر بالمفهوم الواسع ، ولهذا سنتناول تعريف الجريمة الالكترونية لغة واصطلاحا.

الفرع الأول: التعريف اللغوي للجريمة الالكترونية

اشتقت كلمة الجريمة في اللغة من الجرم وهو التعدي ، أو الذنب وجمع الكلمة اجرام وجروم وهو الجريمة ، وقد جرم يجرم واجترم واجرام فهو مجرم وجريم ، وعرفت الشريعة الإسلامية الجريمة **بأنها محظورات شرعية زجر الله عنها بحد أو تعزيز** [2]

كلمة الكترونية مشتقة من كلمة الكتروني وجمعه الكترونيات المنسوب إلى الالكتروني حيث بدأ ينشر العقل الالكتروني في كل المكاتب أو مايسمى آلة الحاسوب ، تعتمد على مادة الإلكترون لإجراء أدق العمليات الحسابية .

وعرف الكمبيوتر أو الحاسب الآلي أي جهاز الكتروني ثابت ، أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات ، أو تخزينها ، أو إرسالها ، أو استقبالها ، أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له [3].

الفرع الثاني: التعريف الاصطلاحي للجريمة الالكترونية :

[1] لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، الطبعة الأولى، دار ومكتبة الحامد للنشر والتوزيع، 2015، ص 20 – 21 .

[2] علي حسن الطوالبة ، الجريمة الالكترونية ، جامعة العلوم التطبيقية مملكة البحرين ، 2008 ، ص 46 .

[3] خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، ط2 ، دار الفكر الجامعي ، الاسكندرية 2019 ، ص 20-21 .

الجريمة عرفت بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة يقرر له القانون عقوبة أو تدابير احترازية ، أما الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت تعتمد على المعلومة بشكل رئيسي .

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الالكترونية ، فهناك عدة تسميات والمفاهيم المتقاربة وهي كالتالي :

جرائم التقنية العالمية ، الجرائم المعلوماتية ، الجرائم الرقمية ، السبير كرايم ، جريمة أصحاب الياقات البيضاء ، والجرائم المرتبطة بالكمبيوتر .

للدلالة على الأفعال التي يكون فيها الكمبيوتر هدفا للجريمة ، أما اصطلاح الجرائم المرتبطة بالكمبيوتر فيراد به تلك الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة [1]

الفرع الثالث : التعريف الفقهي للجريمة الإلكترونية

نشير بداية أنه ليس هناك اتفاق عام حول توحيد هذا المصطلح حيث أن هناك الكثير من المصطلحات التي يتم استخدامها، ويراد بها نفس المعنى وهو النظام لمعلوماتي على غرار مصطلح المعالجة الآلية للمعطيات، ومنظومة معالجة كمبيوتر، ومصطلح معالجة آلية استعمل أول مرة في فرنسا لتنظيم حماية المعلومات الاسمية عن طريق القانون 6 يناير 1976، وكان وزير المالية الفرنسي قد قام في المعجم الأبجدي تعريفا لفكرة النظام لمعلوماتي بأنه مجموعة تجهيزات وبرامج يحتوي على الأقل على الحاسب آلي يقوم بمعالجة وإرجاع البيانات وإن كان ما يؤخذ على هذا التعريف كونه قاصر وبهمل الروابط بين مختلف وسائل هذا المجموع الذي يشكل النظام .[2]

[1] رشيدة بوكر ، المرجع السابق ،ص 36 .

[2] محمد خليفة، الحماية الحنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الطبعة الأولى، دار الجامعة الجديدة الاسكندرية، ص 16، 17 .

أما اتفاقية بودابست لسنة 2001 فقد استخدمت اصطلاح منظومة كمبيوتر، واعتبرت بموجبه أنه أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة والتي يقوم واحد منها أو أكثر وفقا لبرنامج بالمعالجة الآلية للبيانات وفي ذات الوقت أن بيانات الكمبيوتر تتعلق بعمليات عرض للحقائق أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر لأداء وظيفة معينة .[1]

ومهما يكن من أمر فإن الفقه لم يشذ عن العناصر التي يتألف منها النظام لمعلوماتي وفقا لما سبق بيانه فعرف تبعا لذلك على **أنه مجموعة المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما[2].**

وذهب البعض في تعريفها على أنها: **كل سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات»**. وهي على رأي البعض الآخر كل نشاط غير مشروع موجه لنسخ أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه.

وإذا كان التعريفين السابقين يركزان على موضوع الجريمة المعلوماتية، فهناك من فضل التركيز في تعريفها على وسيلة ارتكابها، وتبعا لذلك عرفت الجريمة المعلوماتية بأنها: كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب.

وهي أيضا: نشاط إجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة أو غير مباشرة بهدف تنفيذ العمل الإجرامي المقصود.

كما أن المشرع الجزائري لم يتخلف بدوره عن تعريف الجريمة الالكترونية بأنها نتيجة التأثر بالثورة المعلوماتية التي نتج عنها أشكال جديدة من الجرائم وذلك من خلال

[1] أنظر المادة الأولى من الملحق المتعلق بالنص الكامل لاتفاقية بودابست لسنة 2001 المتعلقة بالجريمة الالكترونية

[2] شوقي يعيش تمام، محمد خليفة، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل البحث العلمي بيروت، لبنان ، ص 20 .

التعديلات الذي أدخله على قانون العقوبات بموجب القانون رقم 04 / 15 المتمم لقانون العقوبات [1] في المواد 394 إلى 394 مكرر 07 .

واستحدث القانون رقم 09 /04 المؤرخ في: 05 /8 / 2009 تسمية المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على الجريمة المعلوماتية معتبرا أن النظام ألمعلوماتي في حد ذاته من مكونات غير مادية محلا للجريمة، حيث جاء في نص المادة 02 **الفقرة** أعلى أن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية .

وعرفت الفقرة ب من نفس المادة المنظومة المعلوماتية بأنها مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة [2]

[1] القانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004 المتمم لقانون العقوبات، الجريدة الرسمية العدد 71 الصادر بتاريخ 10 نوفمبر 2004 .

[2]القانون رقم 09 –04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 بتاريخ 5 أوت 2009 .

المطلب الثاني : خصائص الجريمة الالكترونية

كثيرا ما يقع الخلط وعدم التمييز بين خصائص الجريمة المعلوماتية وصعوبات مكافحتها على الرغم من وجود حدود فاصلة بين الموضوعين، فخصائص الجريمة المعلوماتية يراد بها ما تنفرد من مميزات، والتي لا يمكن فصلها بالضرورة عنها مقارنة بباقي الجرائم العادية الأخرى، في حين أن صعوبات مكافحة الجريمة المعلوماتية تشكل مجموعة من التحديات التي لا تتعلق بالجريمة المعلوماتية لوحدها [1]، بل تشترك فيها كذلك مع بعض الجرائم الأخرى العابرة للحدود أو الجرائم المنظمة وهي ليست لصيقة بالجريمة المعلوماتية بالقدر الذي لا يمكن فصله عنها .

وعليه فإن مسألة صعوبة الإثبات أو التحقيق في الجرائم المعلوماتية ليست سمات ملازمة للجريمة المعلوماتية، بقدر ماهي إشكاليات أو تحديات مرتبطة بالجريمة المعلوماتية وسوف يأتي الحديث عنها لاحقا .

انطلاقا مما تقدم يمكن حصر خصائص الجريمة المعلوماتية على النحو التالي:

أولا : وقوع الجريمة في بيئة المعالجة الآلية للبيانات وللمعلومات .

يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع البيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها الكترونيا، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها .

وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية .

وعلى الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي الإدخال، المعالجة، الإخراج، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن النظر إلى طبيعة

[1] يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة ، الطبعة الأولى ، جامعة محمد خيضر بسكرة ، 2019 ، ص 26 .

ارتكابها إلا في وقت محدد، ففي مرحلة الإدخال ألمعلوماتي يمكن إدخال معلومات غير صحيحة، أو عدم إدخال وثائق أساسية، وفي مرحلة المعالجة الآلية للبيانات يمكن إجراء أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة .

من المفيد الإشارة أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات ومن الشائع وصف بيانات الحاسوب مثلا كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب، توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر لم يحدد موقفه، لكن من المرجع في الممارسة العملية أن تتضمن تلك البيانات والمعلومات على وسائط التخزين المادية مثل الأقراص الصلبة، وبطاقات الفلاش للتخزين وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية أو تردد الراديو .[1]

ثانيا : الصبغة العلمية العالمية للجريمة الإلكترونية.

تتصف الجريمة المعلوماتية بكونها جريمة ذات بعد عالمي أو دولي، لكن لا ينبغي أن يفهم من ذلك أنها جريمة دولية .ذلك أن هذه الأخيرة محددة على سبيل الحصر ومعرفة وفق نظام روما الأساسي في جرائم الحرب، جرائم العدوان، جريمة الإبادة البشرية، الجرائم ضد الإنسانية . ما يجعل بالضرورة التفرقة بين النوعين، فالجريمة المعلوماتية تصنف في مجال القانون الجنائي، بخلاف الجريمة الدولية التي تصنف في مجال القانون الدولي الجنائي .

والحديث عن صفة العالمية للجريمة المعلوماتية ارتبط بالتقنيات الحديثة، وما صاحبها من تطور في مجال الاتصال بحيث ألغى الحدود الجغرافية بين الدول، فتخطت بذلك

[1] يعيش تمام شوقي، ، المرجع السابق، ص 27، 28 .

الجريمة المعلوماتية حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى عدة بلدان على مستوى العالم، فالتقنيات المتصلة عالميا قد جعلت من هذه الجريمة عابرة للحدود [1].

وعليه فالطبيعة العالمية تمكن الجاني من ارتكاب الجريمة في دولة ما، وتؤثر على المجني عليه في دولة أخرى، بل أنه من الممكن أن يكون هناك ضرر محتمل في بلد ثالث وعليه تعد جرائم المعلومات شكلا جديد من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، وقد خلفت هاته الخاصية الكثير من الإشكالات القانونية في مسألة الاختصاص القضائي والتحديات التي تقترن به.

ثالثا : الجريمة الإلكترونية أقل عنفا وجهدا في التنفيذ.

لا تتطلب جرائم المعلومات عنفا لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة العنف والايذاء، كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع والكسر وغير ذلك .

وعلى هذا الأساس تتميز جرائم المعلومات بأنها من الجرائم الهادئة، أو الناعمة، حيث لا تحتاج إلى العنف، وكل ما تحتاج إليه هو عامل الخبرة، والذكاء والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في ارتكاب الأفعال غير المشروعة، فهي من الجرائم النظيفة التي تستخدم الأرقام والبيانات وليس لها أثر خارجي مادي[2].

[1] إن الجريمة المعلوماتية سلوك غير مشروع كما سبق تبيان ذلك بحيث تمس بمصالح خاصة أو عامة داخل حدود دولة معينة، مع إمكانية تجاوز هذه الحدود إلى دولة ثانية وثالثة أو أكثر من ذلك هذا ما يجعلها عابرة للحدود، في حين أن الجريمة الدولية هي كل فعل أو سلوك مخالف لقواعد القانون الدولي يتضمن اعتداء ا على القيم والمصالح الدولية يرتكبه شخص طبيعي واحد، أو مجموعة من الأشخاص سواء لحسابهم الخاص، أو لمصلحة دولة معينة، أو لمصلحة مجموعة من الدول، أو كانت بتحريض أو مساعدة منهم .....

[2] ماضي نعيمة، ناصف وردة، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص إعلام آلي وأنترنت، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، جامعة برج بوعريريج، السنة الجامعية 2021 – 2022، ص 18.

رابعا ::صعوبة اكتشاف الجريمة الالكترونية .

تتميز جرائم الحاسب الآلي بصعوبة اكتشافها كون أنه لا يتم الإبلاغ عنها لعدم اكتشافها من قبل الضحية، وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة، بل بعد وقت طويل من ارتكابها مما يساعد على عدم التعرف على مرتكبي الجرائم الالكترونية وذلك بسبب إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عن مرتكبيها خوفا من الأضرار بالمركز المالي للجهة المعتدى عليها وتجنبا للإساءة إلى السمعة وهز ثقة العملاء .

كذلك إخفاء أسلوب ارتكاب الجريمة خوفا من قيام الآخرين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة عن الجريمة وهو ما يزيد فرص المجرم لمعلوماتي في الإفلات من العقاب، حتى في حالة الضبط لا يتعاون مع جهات التحقي خوفا مما يترتب على ذلك من دعاية مضادة وضياع الثقة [1].

خامسا : صعوبة التحقيق والتحري في نطاق الجريمة الالكترونية .

ينطوي التحري والتحقيق في الجرائم الالكترونية على مشكلات وتحديات إدارية وقانونية يصعب على المحقق التقليدي التعامل معها .لأنها في بعض الأحيان قد لا تتطلب الجريمة المعلوماتية من الجاني سوى كبسة زر واحدة على لوحة المفاتيح حتى يتمكن من خلالها نقل ملايين الدولارات من مكان لآخر على سبيل المثال .حيث تتطلب جرائم الكمبيوتر إلمام خاص بتقنيات الكمبيوتر ونظم المعلوماتية سواء للتحقيق فيها أو ملاحقتهم قضائيا .

كما أن الجريمة الالكترونية تتسم بالغموض لصعوبة إثباتها أو التحقيق فيها . كما أنها تحدث هزات كبيرة في اقتصاديات الدول [2]

[1] أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص 95 .
[2] لينا محمد ألأسدي، المرجع السابق، ص 29 .

المطلب الثالث : صور الجرائم الالكترونية ومرتكبيها .

لم يوضع لجرائم الانترنيت معايير محددة من أجل تصنيفيها وذلك لتعدد هذه الجرائم وذلك تأسيسا على التطور المستمر للشبكة والخدمات التي تقدمها .

كما يتمتع محترفوا الجرائم الالكترونية بقدرة عالية من الذكاء والالمام الجيد بالتقنية العالية واكتسابهم معارف علمية وعملية، وانتمائهم الى تخصصات المتصلة بالحاسوب من الناحية الوظيفية وهذه السمات تتشابه مع سمات الياقات البيضاء[1]

ولقد صنف الباحثون والدارسون الجرائم الالكترونية ضمن فئات متعددة، وتختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني فبعض الفقهاء أسس تقسيمه على تعدد محل الاعتداء وكذا تعدد الحق المعتدي عليه فتوزع الجرائم وفق هذا التقسيم إلى :

_ جرائم تقع على الأموال وتلك التي تقع على الأشخاص وأخرى على المصلحة العامة وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقاتها بالجرائم التقليدية .

_ بينما يصنفها البعض حسب النتيجة المترتبة على السلوك الإجرامي فيقسمها إلى: جرائم ذات نتيجة وأخرى شكلية

_ هناك من يقسمها الى جرائم انترنيت وجرائم كمبيوتر .

_ ثمة تقسيم يعتمد دور الكمبيوتر في ارتكاب الجريمة حيث يلعب الكمبيوتر.

ثلاثة أدوار في ميدان ارتكاب الجرائم:

_ الأول: قد يكون الكمبيوتر هدفا للجريمة وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم ويكون الكمبيوتر هدفا

[1] محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنيت، دار الفكر والقانون، المنصورة 2013، ص.18.

للجريمة بان توجه هجمات ضد الكمبيوتر أو خدماته للمساس بالسرية أو المساس بسلامة المحتوى والتكاملية لتعطيل القدرة والكفاءة.

_ الثاني: قد يكون الكمبيوتر أداة لارتكابجرائم تقليدية كما هو في حالة استغلاله للاستيلاء على الأموال باجراء تحويلات غير شرعية، أو استخدام التقنية في عمليات التزييف والتزوير والاستيلاء على أرقام البطاقات الائتمانية وإعادة استخدامها كما يستخدم القتل والدخول إلى قواعد البيانات الصحية والعلاجية أو التأثير على عمل البرمجيات وغيرها ...

_ الثالث: قد يكون الكمبيوتر بيئة الجريمة كما في تخزين برامج القرصنة أوفي استخدامه لنشر المواد الغير قانونية أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها [1].

_ كما اعتمدت الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنيت لعام 2001(اتفاقية بودابست 2001)تقسيما تضمن أربع طوائف رئيسية لجرائم الكمبيوتر والانترنيت :

1_الجرائم التي تستهدف العناصر السرية والسلامة وديمومة توفر المعطياتوالنظم الجرائم المرتبطة بالكمبيوتر .

3_ الجرائم المرتبطة بالمحتوى (وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية).

4_ الجرائم المتعلقة بالإخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات)[2]و من خلال ما سبق يمكن تصنيف الجرائم المعلوماتية كما يلي :

الفرع الأول: الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي :

وهنا لا يكون النظام المعلوماتي هو محل الجريمة، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام ألمعلوماتي، ويكون الهدف من ورائها الربح

[1] محمود طه، المرجع السابق، ص 18.

[2]محمود أحمد طه، المرجع السابق، ص 18.

بطريق غير مشروع، الاعتداء على أموال الغير الاعتداء الأشخاص وسلامتهم وحياتهم الخاصة، أو في سمعتهم وشرفهم والاعتداء على أمن الدولة وأسرارها .

أولا: الجرائم الواقعة على أشخاص:

رغم الايجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد إلا أنها جعلت الأشخاص أكثر عرضة للانتهاك منها :

1- جريمة التهديد :يقصد به زرع الخوف في النفس بالضبط على إرادة الانسان تخويفه من أضرار ما ستلحقه أو تلحق أشخاص له بهم صلة.

- و يجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير، ولا يشترط أن يتم إلحاقا لأذى فعلا أي تنفيذ الوعيد لأنها تشكل جريمة قائمة بحد ذاتها، تخرج من إطار التهديد إلى التنفيذ الفعلي وقد يكون التهديد مصحوبا بالأمر أو بطلب القيام بفعل أو الامتناع عن فعل، أو مجرد الانتقام ولقد أصبحت الانترنيت الوسيلة المثلى لارتكاب جرائم التهديد ومن هذه الوسائلالبريد الالكتروني: عن طريق مراسلة المجني عليه بالبريد الالكتروني متضمنا تهديدا بارتكاب جريمة ضدهم وهنا يطبق النص التقليدي لجريمة التهديد وأغلب التشريعات .

- **صفحات الويب:** بقيام شخص انشاء موقع ويب خاص به ينشر عليه تهديدا لشخص آخر [1].

- **انتحال الشخصية:** وهي جريمة الألفية الجديدة وهي استخدام شخصية فرد بطريقة غير شرعية للاستفادة من ماله أو سمعته أو مكانته أو لإخفاء هوية المجرم وعليه يجب التوثيق الالكتروني كالتوقيع الرقمي وتوثيق الهوية .

[1] خالد حسن أحمد لطفي، جرائم الانترنيت بين القرصنة الالكترونية وجرائم الابتزاز الاكتروني دراسة مقارنة، دار الفكر الجامعي: الاسكندرية 2018، ص ص 28-29.

- **انتحال شخصية أحد المواقع:** وذلك عن طريق اختراق احد المواقع للسيطرة عليه ليقوم بتركيب برنامج خاص به هناك باسم الموقع المشهور .

- **جرائم السب والقذف:** للمساس بشرف الغير وسمعتهم ويكون كتابيا أو عن طريق مطبوعات أو رسوم أو عبر البريد الالكتروني أو الصوتي، أو صفحات الويب بعبارات تمس الشرف وتعتبر من أكثر الجرائم شيوعا في نطاق شبكة الانترنيت وهناك متخصصة تعمل على إبراز سلبيات الشخص المستهدف وإفشاء أسراره [1]

- المواقع الإباحية والدعارة: وفرت شبكت الانترنيت أكثر من الوسائل فعاليةو جاذبية لنشر الإباحية بشتى وسائل عرضها، من صور وفيديوهات وحوارات في متناول الجميع . وقد وجد العاملون في مجال الرذيلة والاباحية في شبكة الانترنيت وسيلة حديثة ذات كفاءة وكفاية عالية في الدعوة إلى الاعلانات الممنوعة وذلك كله في إطار التقنية التي يستخدمها الجاني في ارتكابه للجريمة وصعوبة اكتشاف هذه الجرائم وتحديد مصدرها وإقامة الدليل عليها[2].

- **التشهير وتشويه السمعة:** يقوم المجرم بنشر معلومات قد تكون سرية أو مظللة مغلوطة عن الضحية والذي قد يكون فردا أو مؤسسة تجارية أو سياسة، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين بالإضافة إلى الجرائم الخاصة بتشويه السمعة الشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من اجل تشكيك الناس في مصداقية هؤلاء الأفراد وقد يكون الهدف من ذلك الابتزاز[3].

---

[1] لينا محمد الاسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة، دار ومكتبة الحامد للنشر والتوزيع: عمان2008، ص 36.

[2] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص ص 125-126.

[3] خالد حسن أحمد لطفي، المرجع السابق، ص 31.

- **جرائم الاعتداء على حرمة الحياة الخاصة:** قد يستخدم النظام ألمعلوماتي في الاعتداء على حرمة الحياة الخاصة، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحوي على معلومات تخص شخص آخر بدون علمه وبغير إذنه أو أن يكون تجميع هذه المعلومات بموجب موافقة سابقة من صاحبها ولكن قام الشخص المكلف بحفظها باطلاع الغير عليها ودون موافقة صاحبها ويدخل في نطاقها جريمة تسجيل المحدثات الشخصية أو مراقبتها بأي وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الانترنيت بطرق غير مشروعة والتنصت على هذه المكالمات [1].

- **ثانيا: الجرائم الواقعة على الأموال:**

من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الالكترونية ومما زاد في تطور وسائل الدفع الالكتروني والامر الذي أدى إلى تطور الجريمة الالكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة [2].

وجرائم الأموال بشكل عام هي الجرائم التي تنال بالاعتداء أو التهديد بالخطر الحقوق ذات القيمة المالية، ويدخل في نطاقها كل حق ذي قيمة اقتصادية ويدخل في إطار التعامل وبالتالي يكون أحد عناصر الذمة المالية للشخص [3].

ومع هذا التطور ابتكرت طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع[4]، وهو ما هيأ فرصة لظهور قيم اقتصادية مستحدثة وعليه السطو عليها بطريق غير مشروع ومنها :

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص124.

[2] رحموني محمد، خصائص الجريمة الالكترونية ومجلات استخدامها، جامعة أحمد دراية –أدرار مجلة الحقيقة، العدد 41، تاريخ قبول المقال للنشر 2018/01/10، ص 446.

[3] لينا محمد الأسدي، المرجع السابق، ص48.

[4] خالد حسن أحمد لطفي، المرجع السابق، ص 32.

1_ جرائم الكترونية تطال بطاقات الائتمان والتحويلات المالية: لقد أضحت بطاقات الائتمان محلا للاعتداء في ظل التطور التقني، وغالبا ما يتم ذلك عن طريق معرفة المعلومات الشخصية الخاصة بالمجني عليه صاحب البطاقة [1] مما يسهل على المجرم الالكتروني الدخول إلى نظام المعلوماتية ويكون ذلك سواء بالتواجد على الشبكة أثناء إتمام عملية ما أو بإدخال بيانات إلى ذاكرة الجهاز ويكون باستخدام الاحتيال وكذلك الاحتيال بواسطة بطاقات الدفع الالكتروني .

2_ الاحتيـــال: يتم الاحتيال على الضحية من خلال تضليله بوجود مشروع يحصل من ورائه على أمول مما يدفعه إلى الانسياق وراء تغيير المجرم الالكتروني ويكون ذلك سواء بالاتصال عبر الشبكة بين الجاني الالكتروني والمجني عليه، أو من خلال استخدام المجرم الالكتروني البيانات الكاذبة التي تساعده على إيهام الكمبيوتر والاحتيال عليه بغاية الحصول على الأموال .

ب- الاحتيال بواسطة بطاقات الدفع الالكتروني: ويتم الدفع الالكتروني بواسطة بطاقة الدفع الالكتروني بتحويل مالي من المصدر وهو بنك العميل إلى رصيد متعامل آخر، كل ذلك بواسطة شبكة شبكة التسوية الالكترونية الدولية مثلا ماستر كارد، حيث يقوم المجرم بكسر كلمة السر للبطاقة الالكترونية أو خداع الصراف الآلى وبالتالي يتمكن من الحصول على السلع والخدمات وذلك بملأ نموذج الكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري .

ويمكن الاحتيال باستخدام بطاقة الائتمان من قبل صاحب البطاقة الشرعي وذلك بإساءته استخدام بيانات الائتمانية أثناء مدة صلاحيتها أو قيامه باستخدامها بعد مدة صلاحيتها أو إلغائها .

وقد يكون البنك مصدر البطاقة قد ألغاها أثناه مدة صلاحيتها بسبب سوء الاستخدام من العميل الذي يتعين عليه إعادتها إلى البنك والذي د قد يمتنع عن ذلك ويستمر في

[1] لينا محمد الأسدي، المرجع السابق، ص 49.

استعمالها باستخدام بياناتها وتعاملاته عبر الشبكة وهو ما يشكل جريمة النصب بمجرد ملأ البيانات لإقناع الغير بوجود ائتمان وهمي [1].

2 – سرقة أموال البنوك: وتكون بواسطة استخدام المجرم الالكتروني الكمبيوتر بغرض الدخول إلى الشبكة والوصول غي المشروع إلى البنوك غيرها من المؤسسات المالية بكميات بسيطة بصفة متكررة بحيث لا يلفت الانتباه وقد يتم دفعة واحدة .

1- **غسيل الأموال التي تتم عبر الانترنيت:** وهي من الجرائم المعاصرة للجريمة المنظمة ويقصد بها توظيف الأموال داخل الدولة أو خارجها في أعمال مشروعة وذلك لطمس الأصل غير المشروع لهذه الأموال وغالبا ما يتم ذلك عن طريق تسلل الأموال إلى المشروعات الاقتصادية والتأثير فيها، ويعاد استغلالها بعد ذلك على أنها من مصدر ربح مشروع [2].

ونتيجة للتطور فقد استفاد مجرموا غسيل الأموال من التقنية ومميزاتها لتحيقي أغراضهم الإجرامية، وما دفع بهمإلى استعمال الوسائل المستحدثة هي هي السرعة وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول وكما أن البطاقات الذكية والتي تشابه بطاقات البنوك تستخدم في مكائن الصرف الآلية، تساعد على تحويل الأموال بواسطة المودم أو الانترنيت مع ضمان تشفير ذلك وأمان العملية [3]، وهذا الأمر جعل عمليات غسيل الأموال عبر الوسائل التقنية وخاصة عبر شبكة الويب العالمية تتم بسرعة ودون أن تترك أي أثر في الغالب .

2- **الجرائم الواقعة على حقوق الملكية الفكرية والأدبية:** يقصد بحقوق الملكية الفكرية ذلك النوع من الحقوق الذي يرد على الأشياء المعنوية غير المحسوسة من خلق الذهن

[1] خالد حسن أحمد لطفي، المرجع السابق، ص 36.

[2] رحموني محمد، المرجع السابق، ص447.

[3] لينا محمد الأسدي، المرجع السابق، ص 77.

ونتاج الفكر فيثبت لصاحبها أبوة هذا الحق ونسبته إليه وحده ويعطيه احتكار استغلاله ماليا ويكفل له الحصول على ثمراه .

ويمكن القول أن حقوق الملكية الفكرية المتعلقة بالمعلومة الالكترونية تتسع لتشمل الحقوق المتعلقة بالمؤلف والحقوق المتعلقة ببراءة الاختراع وأخيرا الحقوق المتعلقة بالعلامات التجارية .

ويكمن الهدف الرئيسي من إقرار الحماية الجنائية لحقوق الملكية الفكرية للمعلومة الالكترونية وتشجيع الناس على ابتكار البرامج التي من شأنها المساهمة بشكل كبير في إثراء الدولوتقدمها [1].

3- **قرصنة البرمجيات:** هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل، وجريمة نسخ المؤلفات العلمية والأدبية بالطرق الالكترونية من الجرائم المستحدثة وذلك تأسيسا على أن المعلومة الادبية والفكرية ذات قيمة أدبية ومادية بالإضافة إلى براءات الاختراع التي تخول لمالكها حق معنوي وآخر مالي.

وعليه يتبين لنا أن الجرائم المرتكبة على الأموال عبر شبكة الانترنيت لا يمكن حصرها لأنها متعددة ومتشعبة كما يتبين التكييف القانوني للوقائع حسب كل حالة وذلك نظرا للفراغ القانوني الحاصل في هذا المجال، وهذا يتطلب ضرورة صدور نصوص قانونية تحصر الأفعال والممارسات اليومية خاصة أمام الإحصائيات المسجلة والمتنامية[2]

[1] محمود أحمد طه، المرجع السابق، ص77.

[2] خالد حسن أحمد لطفي، المرجع السابق، ص38.

ثالثا: الجرائم الواقعة على امن الدولة: يقوم الإرهابيون باستخدام الانترنيت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات[1].

و تتمثل هذه الجرائم في جرائم الإرهابوالتجسس والجريمة المنظمة، وهذا ما نعالجه في النقاط التالية:

1-**الإرهاب والجريمة الالكترونية:** مما لا شك فيه أن ظاهرة الإرهابأضحت عالمية حيث ظهرت الكثير من التنظيمات التي تتبنى هذا الفكر في مختلف دول العالم وبمختلف التسميات وتظهر العلاقة بين الإرهاب والجريمة الالكترونية من خلال تجنيد وتجيش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الالكتروني، كما يتم تبني العمليات الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الالكترونية بما يحقق أهدافها [2] .

2 **-التجسس والجريمة الالكترونية:** يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية وتستهدف خاصة: التجسس العسكري، التجسس السياسي والاقتصادي وذلك باستخدام التقنية المعلوماتية وتمارس من قبل دولة على جهاز آلي، وغير مسموح بالاطلاع عليها وكأن تكون من قبيل أسرار الدولة [3].

الفرع الثاني: الجرائم الالكترونية الواقعة على النظام ألمعلوماتي :

إذا كانت أشكال الجريمة الالكترونية متعددة ومتنوعة، على نحو ما نتناوله سابقا إلا أن نطاق هذا البحث لا يتسع للتعرض لكافة أنواع الجرائم الالكترونية ولذلك سوف نعرض أهم الجرائم المحتمل وقوعها ومن أهمها:

---

[1] نفس المرجع، ص 38-39.

[2] رحموني محمد، المرجع السابق، ص448.

[3] خالد حسن أحمد لطفي، المرجع نفسه، ص39.

أولا: الاعتداء على برامج النظام المعلوماتي: وهنا يستوجب الأمر أن يكون الجاني على معرفة ودراية ذات درجة عالية في مجال البرمجة وغالبا تقع هذه الجرائم على البرامج التطبيقية وبرامج التشغيل .

1- البرامج التطبيقية: يقوم الجاني بتحديد البرنامج والتلاعب فيه ويكون الهدف تعديل البرنامج لاختلاس الأموال لتحقيق الفائدة دون اثارة للشبهات عن طريق زرع برنامج فرعي في البرنامج الأصلي يسمح له بالدخول غير المشروع لنظامه المعلوماتي حيث يصعب اكتشاف هذا البرنامج لدقته وصغره.

2-برامج التشغيل: وهي البرامج المسئولة عن عمل نظام التشغيل المعلوماتي من حيث قيامها بتنظيم وضبط وترتيب التعليمات الخاصة بالنظام.

و تقوم الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية لتسهيل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي وتأخذ شكلين هما المصيدة وتصميم البرامج[1].

ثانيا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي: إن الصورة الغالبة لتحقيق غاية المجرم.

الفرع الثالث: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي .

لتحقيق غاية المجرم المعلوماتي في نطاق الشبكة تتمثل الصورة في الدخول غير المشروع إلى النظام المعلوماتي أو البقاء دون إذن، لارتكاب الجريمة فتشكل أحد أنواع جرائم الانترنت، حيث يقوم المجرم بالتلاعب بالمعلومات أو إتلافها.

- جريمة الدخول غير المصرح به .

[1] خالد حسن أحمد لطفي، المرجع السابق، ص40.

الدخول معناه في إطار المعلوماتية بصفة عامة يشمل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي . والدخول الغير المصرح به يعني توجه هجمات إلى معلومات الكمبيوتر، أو المساس بالسلامة والمحتوى والتكاملية أو تعطيل الكفاءة للأنظمة للقيام بأعمالها .[1]

3- التلاعب في المعلومات الموجودة على النظام المعلوماتي .

يكون بطريقتين: الطريقة المباشرة التلاعب يكون فيها عن طريق إدخال معلومات معرفة المسؤول عن القسم المعلوماتي، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال .

أما الطريقة الغير المباشرة التلاعب يكون فيها عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات، أو يستخدم الجاني كلمة سر أو مفتاح شفرة وإمكانية تسلل الجاني إلى المعلومات المخزنة من مسافات بعيدة.

إتلاف المعلومات في مجال المعلوماتية هو بمثابة الاعتداء على الوظائف الطبيعية للحاسب الآلي يكون بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسيب، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة، ويكون الإتلاف العمدي للبرامج والبيانات ومحوها أو تدميرها إلكترونيا أو تشويهها على نحو يجعلها غير صالحة للاستعمال .[2]

[1] خالد ممدوح إبراهيم، ، المرجع السابق، ص 242 .

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 43 – 44.

المبحث الثاني: إجراءات البحث والتحري في الجرائم المعلوماتية

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقي العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة المميزة والغالبة، ومرد ذلك هو حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الإلكترونية في شتى مجالات الحياة، فكلما أكتشف العلم شيئا حديثا وجد الاكتشاف طريقه إلى مجال الإثبات الجنائي والتدليل [1].

وقد اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب القانون رقم 09 / 04 المؤرخ في 5 غشت 2009 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ونظرا لأهمية التحقيق في هذا النوع من الجرائم قسمنا هذا المبحث إلى ثلاث مطالب تناولنا في المطلب الأول الأجهزة المكلفة بالتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية وفي المطلب الثاني الأعوان المكلفون بالتحري وجمع الأدلة وفي المطلب الثالث الوسائل المستخدمة في التحري وجمع الأدلة ومعوقاتها[2].

[1] د . عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جانفي 2018، ص 49 .

[2] المادة 02 من القانون رقم 09 – 04المرجع السابق .

المطلب الأول: الأجهزة المكلفة بالتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية

منح القانون 09 – 04 دورا إيجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم الماسة بأنظمة الاتصال والمعلوماتية وكشف مرتكبيها حيث تنص المادة الثالثة منه على وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواه[1] ونص ذات القانون في مادته الرابعة على أربعة حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الالكترونية منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة . وكذلك في حال توفر معلومات عن احتمال اعتداء على المنظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية .

وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم هذا الإجراء في نطاق إقليم دولة أخرى .[2]

[1] المادة 03 و المادة 04 من لقانون رقم 09 – 04 ، المرجع السابق .

[2] المادة 04 من قانون رقم 09 /04، المرجع نفسه.

المطلب الثاني: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة الاتصال والمعلوماتية:

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيئات بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على الكشف عن الجرائم الواقعة ضمن حدود اختصاصها الفني أو التقني والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها .

ومن أجل إشراك مزودي خدمات الانترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم التكنولوجية، يلزم القانون رقم 09 – 04 هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات الملزمين بحفظها، وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال . والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم وعناوين المواقع المطلع عليها .

ويتضمن القانون أيضا إجراءات عقابية حيث أنه ولتفادي أي تهرب من التزامات القانون رقم 09 – 04 يسلط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية عقوبة السجن من خمس إلى ستة سنوات وغرامة مالية تتراوح ما بين خمسة ملايين إلى خمسين مليون سنتيم مع معاقبة المؤسسات المخالفة بالغرامات المالية المنصوص عليها في قانون العقوبات .

الفرع الأول: جهاز الضبطية القضائية .

يعتبر أعضاء الشرطة القضائية موظفون منحهم القانون صفة الضبطية القضائية وخولهم بموجبها حقوق وفرض عليهم واجبات في إطار البحث عن الجرائم ومرتكبيها وجمع الاستدلالات عنها فيبدأ دورهم بعد وقوع الجريمة وينتهي عند فتح التحقيق القضائي أو إحالة المتهم إلى جهة الحكم وتتميز الشرطة القضائية عن الشرطة الإدارية في أن المهمة الرئيسية لهذه الأخيرة تتمثل في تنفيذ تدابير الشرطة العامة الصادرة من السلطات المختصة ومراقبة نشاط الأفراد والجماعات قبل وقوع الجريمة قصد المحافظة على الأمن العمومي ومنع أسباب الاضطرابات وإزالتها إذا وقعت فأعمال الشرطة الإدارية إجراءات وقائية ومانعة في حين أن أعمال الشرطة القضائية عبارة عن إجراءات رادعة .

الفرع الثاني: دور مقدمي الخدمات في التحري والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية.

إن تكنولوجيات الإعلام والاتصال متنوعة خاصة ما يتعلق منها بخدمات الاتصال السلكية واللاسلكية، كالهواتف النقالة والشبكات الرقمية المتمثلة في الانترنت، وهو ما يجعل عملية توصيل الخدمات المتنوعة لهذه التكنولوجيا إلى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات المنصوص عليهم[1] في القانون رقم 09 – 04 الذي يعرفهم على أنهم :

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها.[2]

[1] المادة 02 فقرة د من القانون رقم 09 – 04، المرجع السابق .

[2] عز الدين عثماني ، المرجع السابق، ص 52- 53 .

المطلب الثالث: الوسائل المستخدمة في التحري وجمع الأدلة ومعوقاتها.

عند القيام بالتحقيق في جريمة ما فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية وسهولة الوصول إلى الجاني، وحيث أن للجرائم طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج على معرفة تامة وإدراك لوسائل وقوع الجريمة وبالتالي حل لغز ما للوصول إلى الجاني وبذلك يعتمد المحقق على مجموعة من الوسائل المختلفة نذكر منها:

الفرع الأول: الوسائل المادية .

وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

- عناوين iP،والبريدالالكتروني، وبرامج المحادثة.

- **البر وكسي:** (PROXY)حيث تعمل البر وكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات وقدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة .(CASHEMEMORY)

- **برامج التتبع:** حيث تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان (iP) الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى، ومن الأمثلة على هذا البرنامج (HACKTRACER)

– نظام كشف الاختراقintrusion détectionويرمز له اختصارا بالأحرف **I D S** هذه الفئة من البرنامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الالكترونية أو الشبكة. [1]

ويتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسبة الالكترونية أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها .

– أدوات تدقيق ومراجعة العمليات الحاسوبية .

– **أدوات فحص ومراقبة الشبكات:** هذه الأدوات تستخدم في فحص بروتوكول ما وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أدوات (ARP)وظيفتها تحديد مكان الحاسبة الالكترونية فيزيائيا على الشبكة .

الفرع الثاني: الوسائل الإجرائية.

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة والغير محددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

1– افتقاد الأثر: يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق .

2– الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته .

[1] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، المرجع السابق، ص 54 .

3- الاستعانة بالذكاء الاصطناعي من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الالكترونية، وفق برامج صممت خصيصا لهذا الغرض.

- **مراقبة الاتصالات الالكترونية:** لم يعرف المشرع الجزائري على غرار العديد من المشركين عملية مراقبة الاتصالات الالكترونية، على عكس بعض التشريعات التي عرفتها مثل التشريع الأمريكي والكندي.[1]

الفرع الثالث: صعوبات ومعوقات جمع الأدلة.

من الصعوبات التي قد تواجه عملية استخلاص الدليل في الجريمة الماسة بأنظمة الاتصال والمعلوماتية مسألة نقص الخبرة لدى رجل الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية متمثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها وذلك على الأقل في البلدان العربية بشكل عام، نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاءت متأخرة عن أوروبا وكندا والولايات المتحدة، كما أن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ التكون والتشكل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقت أبطأ من وقت انتشار الجريمة، لأن الجريمة الماسة بأنظمة الاتصال والمعلوماتية – كما سبق – تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فئة إجراءات الاستدلالات والتحقيقات في الدعوى الجنائية في الجريمة الماسة بأنظمة الاتصال والمعلوماتية .

[1] فقد عرف المشرع الأمريكي مراقبة الاتصالات الالكترونية بأنها: عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو جهاز آخر، فالمادة 2510 الفقرة الرابعة من قانون الاتصالات الفدرالي الأمريكي لسنة 1968، وطبقا لقانون الاتصالات الالكترونية لسنة 1986 أصبح التعريف المذكور يتسع ليشمل الاتصالات الالكترونية الأخرى .

ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات المن وجهات التحقيق والادعاء والحكم في شأن هذه الجرائم .[1]

[1]خيرت علي محرز، خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، 2012، ص81.

الفصل الثانـي:

التفتيش في البيئة الإلكترونية

الفصل الثاني: التفتيش في البيئة الالكترونية :

تعتبر أسرار الإنسان جزء مهم من حياته اليومية، ومن هذا المنطلق يحق للفرد التمسك بعدم انتهاكها سواء كان في مسكنه أو مراسلاته أو معلومة مخزنة في حاسوبه الخاص به أو نظامه المعلوماتي ، وهذا الحق يعتبر من الحقوق الدستورية للمواطن ، لكن قد يتطلب في بعض الأحيان انتهاك هذا الحق من أجل الوصول إلى الحقيقة التي يتطلبها القانون وهذا الخرق يكون بموجب إجراء نص عليه القانون وهو التفتيش [1]وسنقسم هذا الفصل إلى مبحثين، المبحث الأول:مفهوم التفتيش وشروطه والمبحث الثاني: الإجراءات التحضيرية للتفتيش في الجرائم المعلوماتية و آثاره .

المبحث الأول: ماهية التفتيش في البيئة الالكترونية

نظرا للاختلاف بين إجراء التفتيش في المكان المادي للواقعة الإجرامية كإجراء تقليدي، وبين إجراءه في البيئة الالكترونيةالتي تتميز بكونها مكان افتراضي معنوي، فإنّ الفقه أثيرت لديه إشكالية المصطلح الذي يناسبه مقارنة بالتفتيش الذي يتلاءم فقط مع جمع الأدلة المادية في المسرح المادي للجريمة، وسوف نعرّج على رأي الفقه وهذا بعد تناول تعريف التفتيش التقليدي ، ونتطرق كذلك للمصطلح الذي استعمله المشرع الفرنسي والجزائري .

المطلب الأول :تعريف التفتيش التقليدي

بعيدا عن التفتيش في البيئة الالكترونية ، يعرف الفقه

[1] عادل عبد الله خميس المعمري،التفتيش في الجرائم المعلوماتية،جامعة عجمان للعلوم التكنولوجيا ،الامارات،المجلد22 العدد86/2013 ،ص 259 .

[1] التفتيش التقليدي بأنهّ إجراء من إجراءات التحقيق الابتدائي، فثمرته هي ضبط الأشياء المتعلقة بالجريمة، والتي تفيد في كشف الحقيقة و التي قد تُستمد منها أهم أدلة الجريمة إذ قد تكون أداة ارتكابها أو موضوعها أو متحصلاتها، فهدفه هو جمع الأدلة المادية على وقوع الجريمة ونسبتها إلى المتهم، وعلى خلاف إجراءات التحقيق الأخرى التي هدفها جمع الأدلة المادية . كالخبرة والمعاينة فإنّ التفتيش يمسّ بحرمة الحياة الخاصة ، وحرمة المسكن لذلك نجد التشريعات تقرر إبطاله في حالة عدم مراعاة الضمانات والقيود المقررة لإجرائه.

الفرع الأول: رأي الفقه حول مصطلح التفتيش في البيئة الالكترونية

مصطلح أنهّ الالكترونية في البيئة التفتيش مصطلح مجال الفقه [2]في من جانب يرى لفظ هو هذا في الأدّق والمصطلح الإلكترونية، الجريمة أدلة البحث عن لعملية صالح غير وهو البيانات في والتدقيق والتفحص والقراءة البحث يعني التفتيش لأنّ النفاذ أو الولوج بينها بهذا الموضوع من المهتمة الدولية المواثيق في الملاحظ أنّ مصطلح تقليدي ، الا التنسيق بغرض معا المصطلحين تستخدم أنّها الفضاء المعلوماتي لجرائم بودابست اتفاقية في المفاهيم تطور في الحسبان تأخذ أنّها أي والحديثة، التقليدية المفاهيم بين والتنظيم هذه المواثيق أنّ بمعنى التقليدية، بجذورها والاحتفاظ مع تحديدها الإلكتروني الوسط وهو التقليدي بالمصطلح الأخذ بين معا للتخيير الأعضاء المصطلحين للدول تضع الدولية أو المصطلح الحديث وهو الولوج.

---

[1] انظر في ذلك :محمود نجيب حسني،شرح قانون الاجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الأول،دار النهضة العربية،القاهرة،2013 ،ص592 ،و أحمد شوقي الشلقاني،مبادئي الإجراءات الجزائية في التشريع الجزائري،الجزء الاول،ديوان المطبوعات الجزائرية ، الجزائر ،1998،ص240،2241.،ومصطفى محمد موسى ، التحقيق في الجرائم الاكترونية، الطبعة الأولى،دار التجهيزات الفنية،القاهرة،2009،ص 189 ،وعلى عدنان الفيل،إجراءات التحري وجمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية،المكتب الجامعي الحديث،الإسكندرية،2012،ص 38.

[2] نبيلة هبة هروال،الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي،الاسكندرية،2007،ص 223،224 .

[1] ،إذ يُفهم من ذلك أنّ المصطلحين لهما معنى واحد.

كما يرى الفقه أيضا في مجال التفتيش في البيئة الالكترونية أنّ الأجدر إخضاعه لأحكام مستقلة تتلاءم والطبيعة الخاصة للجريمة الإلكترونية والأدلة المتوصل إليها، إنّ التفتيش التقليدي يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وغايته دوما الحصول على الدليل المادي وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي وكذا شبكة الانترنيت، فهي مجرد برامج وبيانات إلكترونية ليس لها أيّ مظهر مادي محسوس في العالم الخارجي .

ورغم ذلك فإنّ الفقه والتشريعات التي صدرت في هذا المجال أجازت بأن يرد التفتيش على هذه البيانات غيرالمحسوسة المتواجدة على مستوى أنظمة الحوسبة و شبكات الإتصال وفي الوسائط الإلكترونية كالأسطوانات والأقراص الممغنطة ومخرجات الحاسب الآلي، وعليه فهو يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط و أحكام .

الفرع الثاني :مصطلح التفتيش في البيئة الالكترونية في التشريعات المقارنة

بداية عرف المجلس الأوروبي هذا النوع من التفتيش بأنّه إجراء يسمح بجمع الأدلة المخزنة أو المسجّلة بشكل الكتروني[2] .

كما أنّ المشرع الفرنسي يُطلق على جمع الأدلة في الشكل الإلكتروني المصطلح التقليدي وهو التفتيش، ويستشف ذلك من خلال التعديل الذي أدخله على قانون

[1] هلالي عبد الله ، الجوانب الموضوعية الإجرائية لجرائم المعلومات على ضوء اتفاقية بوداباست الموقعة في2001/11/23،ص164 ، ونبيلة هبة هروال ، المرجع السابق،ص223،ص224.

[2] علي عدنان الفيل ، المرجع السابق ،ص38

الإجراءات العقابية [1] والتي جاء فيها:"يباشر التفتيش في الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة."

كما أنّ المشرع الجزائري استخدم في المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصطلح الدخول إلى منظومة معلوماتية بغرض التفتيش، بمعنى أنّ الدخول هو التفتيش طبقا لأحكام قانون الإجراءات الجزائية، ولكنّه يكون على نظام المعالجة الآلية للمعطيات أو مستخرجاتها المحمولة على وسائط إلكترونية.

لم يعرف المشرع الجزائري إجراء التفتيش إلا أنه أحاطه بجملة من الضوابط لما يترتب عنها مساس بحرية الأشخاص وحياتهم الخاصة وإنما عرف المنظومة المعلوماتية في المادة 02 من القانون رقم09_04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال[2].

وبمعنى آخر هو الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو أنظمة او شبكة الانترنت[3]

المطلب الثاني: خصائص التفتيش الإلكتروني:

[1] أضيفت هذه المادة بموجب القانون رقم:575_ 2004 المؤرخ في:2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي.

[2] المادة 02 من القانون رقم:09_04 ، المرجع السابق.

[3] أسامة بن غانم العبيدي،التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية و التدريب،الرياض، المجلد29، العدد 58،دون سنة، ص87.

من خلال التعريف الذي وضعه الفقه للتفتيش على نظم المعلوماتية يتبين أنه يتميز عن غيره من الإجراءات التي تهدف إلى إثبات الجريمة كالشهود و الخبرة و المعاينة بعدة خصائص أهمها:

_ إن التفتيش في المنظومة المعلوماتية شأنه في ذلك شأن التفتيش بشكل عام ، فيه تعرض قانوني لحرية المتهم الشخصية أو لحرمة مسكنه بغير إرادته ،وفيه اعتداء على أسراره وحياته .

_ يعتبر التفتيش وسيلة من وسائل التحري عن مختلف الأدلة المعنوية و المادية للجريمة ، يهدف إلى جمع الأدلة التي تؤدي إلى كشف الحقيقة وضبطها والوصول إلى دليل حاسم.

_ يعتبر التفتيش قيدا على حرمة وحصانة الشخص، فهو اعتداء على أسراره [1]سواء الموجودة على مستوى نظامه المعلوماتي أو جهاز حاسوبه أو حتى بريده الالكتروني وفيه مساس بقاعدة حرمة الشخص في حد ذاته أو في رسائله ، ويترتب على كون التفتيش يتضمن مساسا بحق السر أنه يخرج عن نطاقه كل إجراء يمس شيئا مكشوفا ظاهرا للعيان فلا يعد تفتيشا.

_ يسمح التفتيش أو البحث في الشبكات الإلكترونية عن الجرائم المعلوماتية ، باستخدام قواعد وأساليب تخص بتقنيات خاصة فريدة وغير مسبوقة ، فهو بعكس التفتيش في معناه التقليدي لا يتطلب في كثير من الأحيان الانتقال إلى مساكن الأشخاص الذين يشتبه أنهم ساهموا في ارتكاب الجريمة، وإنما قد يتم عن بعد أو ما يعرف بالتفتيش على

[1]رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، جامعة ورقلة، العدد،5، السنة 2012،ص161 .

الخط perquisition en ligne كما تتطلب فيمن يباشر تحقيقها أن يكون متخصصا في التحقيق الجنائي ومعالجة البيانات و المراجعات و الحسابات.[1]

_ يتميز تفتيش المنظومات المعلوماتية أن المحتوى المعلوماتي يتميز بطابعه اللامادي وتجاوزه الحدود الوطنية وسهولة إتلافه أو مسحه وتغييره في أوقات قياسية ،فهو تفتيش للفضاء الافتراضي وأوعية التخزين وللبيانات التي يحفظها جهاز الحاسوب .

_ كما يتميز التفتيش في الفضاء الرقمي بأنه عملية معقدة ومتشابكة، تقتضي من القائمين عليها أن يكون على دراية واسعة وكفاءة عالية في البحث عن المعلومة،و في معالجة المعطيات وتحليلها.

_ إن تفتيش الأنظمة المعلوماتية فيه مساس خطير بالحياة الخاصة ،كونه يتضمن وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية ،وفيه تسجيل وتجميع فوري لهذه الاتصالات وكذا القيام بعمليات التفتيش و الحجز داخل المنظومات المعلوماتية ،ولعل المثال الواضح الآثار التي يتركها متصفح الانترنت ، و التي من خلالها يمكن تجميع كم هائل عن حياته الخاصة ، من خلال صفحات الويب التي اطلع عليها، ووقت دخوله إلى الشبكة ومدة بقائه فيها و الأشخاص اللذين تواصل معهم.[1]

المطلب الثاني :ضوابط التفتيش و السلطة المختصة به :

نجد ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات التي تمس حريتهم كالتفتيش وهدف ذلك هو تحقيق الموازنة بين مصلحة

[1] رضا هميسي، المرجع السابق ،ص 162،163.

المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم وتنقسم الضوابط العامة للتفتيش إلى نوعين، ضوابط موضوعية وشكلية:

الفرع الأول :الضوابط الموضوعية لتفتيش نظم الحاسوب :

يقصد بهذه الضوابط بصفة عامة، الشروط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاثة ضوابط أساسية :السبب، المحل والسلطة المختصة للقيام به [1].

أولا :وجود سبب للتفتيش في البيئة الإلكترونية [2]

سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في من أجل الوصول إلى حقيقة الحدث ويتمثل في وقوع جريمة ما جناية أو جنحة، اتهام شخص أو أشخاص معنيين بارتكابها أو المشاركة فيها، وتوافر قرائن قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو المتهم ،في مسكنه أو بشخص غيره وهو ما ينطبق على الجريمة الإلكترونية .

ثانيا :محل التفتيش

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره ،ففي الجريمة التقليدية التفتيش ينصب على شخص المتهم أو غير المتهم، وكذلك على مسكن المتهم وما في حكمه وملحقاته [3] أو على مسكن غيره وما في حكمه

[1] ليندة بن طالب،التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية و السياسية، العدد 16،السنة 2017،ص491،490.

[2] ليندا بن طالب ، المرجع السابق ص490،491،492.

[3] قدري عبد الفتاح الشهاوي،ضوابط التفتيش في التشريع المصري و المقارن،منشاة المعارف، الاسكندرية،2005،ص 111.

وملحقاته، لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به .

ولكي يتم التفتيش على هذه الحال، ينبغي الإشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال.

ثالثا: الإذن بالتفتيش

ينص المشرع الجزائري في المادة 44 من قانون الإجراءات الجزائية أنه لا يمكن لقيام بإجراء التفتيش لا بإذن مكتوب صادر من وكيل الجمهورية او قاضي التحقيق ،وقد اشترط المشرع وجوب استضهاره قيل الدخول إلى المسكن و الشروع في تفتيشه،كما اوجب أن يتضمن الإذن بيان وصف الجرم محل البحث عن الدليل وعنوان الاماكن المراد تفتيشها و الحجز عليها،أي ان يكون مسببا والهدف من هذا الأخير هي توضيح الهدف من التفتيش ز التحقق من مدى مشروعيته،ذلك ان الإذن حسب المادة 44 السالفة الذكر إذا لم يتضمن التسبيب يقع تحت طائلة البطلان،إذ أن أشتراط المشرغ للتسبيب يتيح للقضاء تقدير صحة الأمر بالتفتيش وتقرير بطلانه غذا ثبت أن الهدف منه غاية أخرى غير المحددة بالقانون،ولا يشتط في التسبيب أن يكون مفصلا بل يكفي بيان الجرم بالإستناد إلى الدلائل المستخلصة من طرف الضبطية القضائية في تحرياتها[1]

أما المشرع الجزائري في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في قانون رقم 04 / 09 ، لا نجده يتحدث عن هذا الشرط، كل ما في الأمر أنه تحدث عن

[1] إلهام بن خليفة، التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،جامعة الشهيد حمة لخضر_ الوادي_، دون سنة،ص36.

إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى[1].

رابعا :السلطة المختصة بالتفتيش

بالرجوع إلى نص المادة 4 فقرة أ من القانون رقم:09_04 [2]التي تبين كيفيات المراقبة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في نفس المادة الفقرة الأخيرة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها المنصوص عليها بموجب المادة 13 من نفس القانون إذنا لمدة ستة أشهر قابلة للتجديد ، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها. فيما عدا هذه الحالة الخاصة وبموجب نص المادة 05 من القانون 09_04 [3]التي تنص على أنه :" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عنها في المادة 04 أعلاه الدخول بغرض التفتيش..."، إذ يتعين الرجوع إلى التدابير التي نص عليها قانون الإجراءات الجزائية في مجال التحري و التفتيش بالنسبة للجرائم الإلكترونية ، وبالضرورة في مجال الاختصاص بالنسبة لوكيل الجمهورية وقاضي التحقيق الذي يحدده المرسوم التنفيذي رقم:06_348 المؤرخ في: 2006/10/05 و المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق وباعتبارهما أيضا الجهة المؤهلة بمنح الإذن بالتفتيش وفقا

[1] ليندا بن طالب، المرجع السابق ،ص 493 .

[2] المادة 04 من القانون رقم: 09_04 المؤرخ في:05 أوت 2009 المتعلق بالوقابة من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ، الجريدة الرسمية ، العدد 47.

[3] المادة 05 ، القانون09_04 ، المرجع السابق.

للشروط المنصوص عنها بموجب نص المادة 44 من ق.إ.ج بتمديد الاختصاص لكل من وكيل الجمهورية وقاضي التحقيق في جرائم معينة من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات [1].

وعليه يمكن القول أن المشرع الجزائري حدد بوضوح الجهة القضائية المختصة سواء في مجال الإذن بوضع ترتيبات للمراقبة الإلكترونية للحيلولة دون الاعتداء على منظومة معلوماتية ، أو في مجال الدخول بغرض التفتيش ولو عن بعد لمنظومة معلوماتية أو جزء منها أو منظومة تخزين معلوماتية سواء تقع داخل الإقليم الوطني أو خارجه فكيف يتم ذلك؟

أ_ تمديد التفتيش إلى منظومة معلوماتية أو جزء منها:

نظرا لخطورة هذه الجريمة المستحدثة، وبقصد ملاحقة المجرم المعلوماتي، نص المشرع على تمديد إجراء التفتيش سواء داخل الإقليم الوطني أو خارجه [2].سنوضح هذا فيما يأتي:

1_ تمديد التفتيش داخل الإقليم الوطني:

أدى سوء استخدام الفضاء السيبراني [3]إلى بروز جرائم مستحدثة تسمى بالجرائم المعلوماتية إذ يمكن للمجرم الدخول والانتقال من منظومة معلوماتية لأخرى بما يسمح له بتغيير أو تدمير المعطيات ناهيك عن صعوبة تتبعه وإيجاد دليل ضده،لذا نص المشرع

[1] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، التواصل في الإقتصاد و الإدارة و القانون،جامعة برج باجي مختار_ عنابة_،العدد 48،ديسمبر 2016،ص87.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت،دار النهضة العربية،القاهرة،2009،ص15.

[3] يقصد بالفضاء السيبيراني:العوالم الافتراضية التي تخلقها الشبكات المعلوماتية، انظر حسين بن سعيد الغافري، المرجع السابق،ص14.

الجزائري في المادة 5 من القانون09 _04 على أنه" :يجوز للسلطات القضائية المختصة ...الدخول بغرض التفتيش ولو عن بعد إلى:

_ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

_ منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة" أ "من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها عن طريق المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطات القضائية المختصة مسبقا "... فتمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يتطلب إجراءات خاصة، فهو يتم عن بعد وبشكل سريع تماشيا مع السرعة الهائلة في نقل المعلومات وأيضا متى توفر الشك في وجود معطيات مبحوث عنها مخزنة في منظومة معلوماتية أخرى .ولكن يتم الوصول إليها عن طريق الدخول من منظومة معلوماتية أولى.

في هذا الصدد تنص المادة 5 الفقرة الأخيرة من القانون 09_04 السالف الذكر، على أنه" :يمكن السلطات 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" .[1]

2_تمديد التفتيش خارج الإقليم وشروط المساعدة القضائية:

[1] يزيد بوحليط، المرجع السابق،ص 87.

في هذا الصدد نصت المادة 15 من القانون09 _04 على انه زيادة على قواعد الاختصاص المنصوص[1] عليها في ق.إ.ج ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني."

وبذلك أقر المشرع إجراءات صارمة لملاحقة هذا النوع من الجرائم خارج الإقليم الوطني وذلك حينما وسع من نطاق التفتيش بموجب نص المادة 05 الفقرة 04 من القانون09 _04 : ..."إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل"...، غير أن المشرع الجزائري لم يترك الأمر على إطلاقه، ونظرا لمقتضيات تتعلق بالسيادة الوطنية، وضع شروطا وقيودا للمساعدة القضائية في مجال مكافحة هذا النوع من الجرائم المستحدثة .

3_ شروط المساعدة القضائية الدولية:

نصت المادة 16 من القانون 09_04 على أنه" :في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني"...، وتعرف المساعدة القضائية الدولية بأنها" :كل إجراء قضائي تقوم به دولة

[1] يزيد بوحليط، المرجع السابق ، ص89 .

من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[1]، الاستعجال والسرعة التي تتطلبها إجراءات التحقيق في مثل هذه الجرائم التي تستعمل التقنيات المتطورة في مجال الحاسوب والانترنيت ونظم الاتصالات ولضمان عدم إفلات المجرم المعلوماتي من العقاب نصت المادة 16الفقرة 02 على قبول طلبات المساعدة القضائية حتى و إن جاءت عن طريق وسائل الاتصال السريعة كالبريد الالكتروني أو الفاكس بشرط التأكد من صحتها فقط.

بناء على ما سبق وضع المشرع شروطا للمساعدة القضائية تطبيقا لنصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المادة 04 الفقرة 01 التي تنّص على أنه[2]:" تلتزم كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ إلتزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى "وهذا ما ترجمته فحوى المادة 17 من القانون 09_04 المذكور سلفا، حيث تتمثل هذه الشروط أساسا فيما يأتي: [3]

– تكون وفقا للاتفاقيات الدولية المبرمة في مجال مكافحة الجرائم المعلوماتية وما يرتبط بها كتبادل المعلومات وتسليم المجرمين والإنابات القضائية ...إلخ .

_ خضوعها لمبدأ المعاملة بالمثل الذي يؤكد سيادة الدولة.

_ توفر شروط أمن كافية للتأكد من صحة المعلومات الواردة عن طريق وسائل الاتصال الحديثة مثل :البريد الإلكتروني، والفاكس، وعموما ترك المشرع المجال مفتوحا لأي وسيلة اتصال حديثة تظهر مستقبلا .

الفرع الثاني :الضوابط الشكلية لتفتيش نظم الحاسوب الآلي

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية،دار الفكر الجامعي،الإسكندرية،2009،الطبعة الأولى،ص407.

[2] المادة 01/04 ، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 2010/12/21.

[3] يزيد بوحليط، المرجع السابق، ص89،90.

إن هذه الضوابط أو الشروط الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، بل تقيم سياجا يحمي الحقوق والحريات الفردية.وتتمثل هذه الضوابط الشكلية في: [1]

أولا :إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان على سلامة الإجراء باعتبار أن التفتيش فيه اطلاع على أسرار الغير.

فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور الشهود ، أما فيما يتعلق بتفتيش المساكن، ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية وإذا تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا، يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش [2].

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06_22 من المادة 45 منه[3]، حيث استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية

[1] أ. ليندا بن طالب، المرجع السابق، ص 493.

[2] المادة 45 من الأمر رقم 66_155 المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات قانون الجزائية المتمم بالأمر رقم 11_02 المؤرخ في:23 فبراير 2011 ، الجريدة الرسمية، العدد 212_2011،

[3] المادة 45 من القانون رقم:06_22 المؤرخ في:20 ديسمبر 2006 المعدل و المتمم للأمر رقم 66_155 المؤرخ في 8 يونيو 1966 و المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية ، العدد 2006/84.

أثناء جمع الدليل الإلكتروني، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد .كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بنظام التفتيش عن بعد، أو ما يطلق عليه الفقه الفرنسي " التفتيش على المباشر perquisition en ligne "

ثانيا :الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية [1]

يقصد بشرط الميعاد الزمني في التفتيش، أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق نطاق الإعتداء على الحرية الفردية وحرمة المسكن .إنّ القانون الجزائري يحظر تفتيش المنازل وما في حكمهما في وقت معين، وهو محدد في القانون الإجراءات الجزائية من خلال المادة 47 من الساعة الخامسة صباحا على الساعة الثامنة مساء.

وهناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد ويصح إجراء التفتيش في أي ساعة من ساعات الليل والنهار، تتمثل في:

_ رضا صريح من صاحب المنزل_ حالة النداءات من داخل المنزل_ التحقيق في جميع الجررائم المعاقب عليها في المواد 342إلى348 من قانون العقوبات.

وأن المشرع الجزائري قد أورد في قانون الإجراءات الجزائية المادة 3/64 " أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47/ 3من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر حيث أجاز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على

[1] ليندا بن طالب،المرجع السابق، ص 493.

إذن مسبق من وكيل الجمهورية المختص " ،وجاء في نص المادة 3/47 من قانون الإجراءات الجزائية[1] حيث استثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في هذه المادة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .والملاحظ المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتباره مستودع أسرارهم، إلا أن ما يبرره ويقل من خطورته الطبيعة الخاصة لهذه الجرائم خاصة الجريمة[2] الإلكترونية وطبيعة الدليل لإثباتها فهو قابل للمحو والتعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية، وما يزيد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوة الجنائية .أما بالنسبة للأماكن العامة، فإذا وجد الشخص وهو يحمل معه مكونات الحاسوب في هذه الأماكن السالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

ثالثا :محضر التفتيش في الجرائم المعلوماتية

لأن التفتيش يعتبر من أعمال التحقيق، فيستدعي ذلك إفراه في محضر يثبت فيه ما إنجر التفتيش عنه من أدلة، والقانون لم يتطلب شكلا محددا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكونا مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن

[1] المادة 3/47 المعدلة بموجب القانون رقم:06_22 المعدل و المتمم للأمر رقم:66_155 المتضمن قانون الإجراءات الجزائية.

[2] ليندا بن طالب، المرجع السابق ،ص494.

كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية.[1]

المطلب الثالث: الطبيعة القانونية للتفتيش:

للجرائم الإلكترونية إجراءات تفتيش خاصة، وذلك لخصوصية هذه الجرائم التي تمتاز بسرعة ارتكابها وتدمير أدلتها، حيث أنها تمتاز عن غيرها من الجرائم الأخرى، وتحتاج لعدة مراحل لتنفيذها.

إن وسائل تكنولوجيا المعلومات، تتكون من وسائل كهرومغناطيسية بصرية كهر وكيميائية، مادية وغير مادية، وكلمة كهرومغناطيسي تشمل كل نظام لتلقي الإشارات بواسطة الأسلاك الكهربائية والموجات اللاسلكية وكل مصدر أخر للطاقة وهذه الإجراءات بالغة الصعوبة، كون أن وسائل تكنولوجيا المعلومات تتكون من مجموعة وسائل مترابطة وغير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتبادلها، وتشمل جميع المداخل والمخارج المرتبطة بها سلكيا أو لاسلكيا، وهذه مميزات خاصة بالتقنية الحديثة، يحتاج تفتيشها إضافة إلى أشخاص متخصصين بالتعامل مع مكوناتها إلى وسائل تقنية حديثة.

المبحث الثاني: الإجراءات التحضيرية و الفنية للتفتيش في الجرائم الإلكترونية

تظهر خصوصية إجراءات التفتيش في الجرائم الإلكترونية في أنها تنقسم إلى إجراءات يجب رعايتها قبل القيام بالتفتيش، وإجراء معاصر لها، وإجراءات لاحقة لها، وتختلف هذه الإجراءات باختلاف محل التفتيش، سواء كان التفتيش منصب على وسائل

تكنولوجيا المعلومات الموجودة بحوزة شخص أو بأماكن عامة أو خاصة، داخل حدود[1] الدولة أو خارجها.

حيث سنتناول في المطلب الأول، الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية، وفي المطلب الثاني، الإجراءات الفنية للتفتيش بالجرائم الإلكترونية.

المطلب الأول: الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية

إجراءات التفتيش في الجرائم الإلكترونية بحاجة إلى إجراءات تحضيرية وهي لازمة وضرورية لنجاحه، وتكون هذه الإجراءات التحضيرية مساعدة للقائم بالتفتيش لضمان نجاحه للحصول على الأدلة المطلوبة حيث سنتناول تحديد محل التفتيش في الفرع الأول، وآلية التفتيش في الفرع الثاني.

الفرع الأول: تحديد محل التفتيش في الجرائم الإلكترونية.

تحديد محل التفتيش في الجرائم الإلكترونية، هو أول أهم الأعمال التحضيرية لإجراء التفتيش، حيث يتم تحديد وسائل تكنولوجيا المعلومات المراد تفتيشها والمستخدمة في ارتكاب الجريمة الإلكترونية، وتحديد مكانها، سواء بحوزة أشخاص أو في أماكن خاصة أو عامة، بهدف معرفة وإجراء تفتيش عليها للحصول على الأدلة المطلوبة.

تحديد وسائل تكنولوجيا المعلومات المستخدمة في ارتكاب الجريمة الإلكترونية يتم من خلال الحصول على المعلومات والبيانات الإلكترونية للأشخاص و للشبكات، والتي يتم الحصول عليها من شركات مزودي الخدمة أو شركات الاتصالات، وهذا من أهم

[1] أشرف أحمد مصطفى عموري،التفتيش في الجرائم الإلكترونية، رسالة ماجستير في القانون الجنائي،جامعة القدس فلسطين، السنة 2018، ص71،72.

الإجراءات التحضيرية التي يجب الحصول عليها، لكشف الوسائل الإلكترونية والشبكات المستخدمة في ارتكاب الجريمة الإلكترونية، وتعتبر هذه المعلومات الإلكترونية وضرورية لإجراء التفتيش.

قانون الجرائم الإلكترونية الفلسطيني عرف معلومات المشترك بالمادة الأولى بأنها " أي معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات، بما في ذلك نوع خدمة الاتصالات المستخدمة وهوية المشترك وعنوانه الجغرافي وهاتفه وأي معلومات أخرى، وهذه المعلومات تكون مخزنة لدى الجهات المختصة في الاتصالات ومزودي الخدمات، وقد ألزم قانون الجرائم الإلكترونية الفلسطيني مزود الخدمة بتزويد الجهات القضائية المختصة بجميع البيانات والمعلومات اللازمة والتي تساعد في كشف الحقيقة، وتطبيقا لهذا النص فإن مزود الخدمات ملزم بحكم القانون تزويد الجهات القضائية المختصة بجميع البيانات والمعلومات اللازمة لمعرفة وسائل تكنولوجيا المعلومات والشبكات المستخدمة في ارتكاب[1] الجريمة الإلكترونية، للوصول إلى مكانها ومعرفة فاعلها و إجراء تفتيش عليها للحصول على الأدلة المطلوبة، وكذلك ألزم المشرع السوري مقدمي الخدمات على الشبكة تقديم أي معلومات تطلبها السلطات القضائية المختصة كما ألزم القانون الفلسطيني، مزودي الخدمة بالاحتفاظ بالمعلومات الشخصية والإلكترونية للمشتركين لديه لمدة لا تقل عن ثلاثة سنوات، ولكن المشرع القطري حدد المدة بسنة واحدة فقط ،حيث سنبحث في تحديد وسائل تكنولوجيا المعلومات المستخدمة لارتكاب الجريمة الإلكترونية في الفقرة الأولى، وتحديد مكان وجودها في الفقرة الثانية.

أولا: تحديد وسائل تكنولوجيا المعلومات

[1] أشرف أحمد مصطفى عموري، المرجع السابق، ص 72

تحديد[1] وسائل تكنولوجيا المعلومات يتم من خلال المعلومات المتحصل عليها من شركات الاتصالات ومزودي الخدمات، وكذلك يتم تحديد الشبكات المستخدمة، سواء كانت داخلية أو خارجية،عرفت المادة الأولى من قانون الجرائم الإلكترونية الفلسطيني الشبكة الإلكترونية بأنها " ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات سواء كانت أجهزة حاسوب هواتف نقالة أو غيرها من الوسائل الإلكترونية التي تعمل بالتقنية الحديثة، وهذا التعريف متناغم مع التعريف الوارد في المادة 6/2 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات .

وقد ألزمت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، كل دولة بتبني الإجراءات الضرورية لتمكين السلطات من إصدار الأوامر إلى مزودي الخدمة لتسليم معلومات المشترك [2]، وبالعودة إلى المادة"31" من قانون الجرائم الإلكترونية نجد أن المشرع الفلسطيني ألزم مزودي الخدمات تزويد الجهات المختصة بجميع المعلومات اللازمة لكشف الحقيقة، ومنح النيابة العامة بالمادة 1/33 الحق في الحصول على الأجهزة والأدوات والوسائل الإلكترونية وحركة الاتصالات وبمستعمليها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.

ثانياً :تحديد مكان وجود وسائل تكنولوجيا المعلومات

تحديد مكان وجود وسائل تكنولوجيا المعلومات المستخدمة في إرتكاب الجريمة الإلكترونية، يكون إما بحوزة شخص أو الأشخاص الذين ارتكبوا تلك الجريمة تمهيدا للقيام بالتفتيش.

[1] أشرف أحمد مصطفى العموري، المرجع السابق،ص74،73.
[2] المادة 1/25 من الإتفاقية العربية لمكافحة تقنية المعلومات.المؤرخة في:2010/12/21،القاهرة.

- 1**تحديد الأشخاص:** يجب أن يتم تحديد الشخص أو الأشخاص المراد تفتيشهم بكل دقة، سواء من حيث الاسم والأوصاف والوظيفة والعمر ومحل إقامته وعمله ، وهذه المعلومات تستبعد وقوع الخطأ من تفتيش شخص آخر.

2- تحديد الأماكن: يجب على القائم بالتفتيش التعرف على الأماكن المراد تفتيشها ، ومعرفة مداخلها ومخارجها، بناءً على معاينة سرية، لتحقيق عنصر المفاجأة خوفا من التخلص من الأدلة [1].

إن آلية تحديد المكان الموجودة بداخله وسائل تكنولوجيا المعلومات المراد تفتيشها يتم عن طريق اتصال تلك الوسائل بالشبكات، سواء كان اتصالها بالشبكات سلكي أو لاسلكي، مع ضرورة معرفة إذا كان هناك أكثر من شخص أو جهة تستخدم تلك الشبكات.

الفرع الثاني :آلية التفتيش في الجرائم الإلكترونية.

إن السلطة القائمة بالتفتيش في الجرائم الإلكترونية تضع آلية للتفتيش بعد حصولها على المعلومات الضرورية واللازمة والتي من خلالها حددت وسائل تكنولوجيا المعلومات التي إرتكبت بواسطتها الجريمة الإلكترونية، سواء كانت تلك الوسائل بحوزة أشخاص، أو داخل الأماكن.

إن التفتيش في الجرائم الإلكترونية يحتاج إلى فريق متكامل يكون له دور في نجاح التفتيش والحصول على الأدلة، ويكون بعدد كاف من الأشخاص المتخصصين في وسائل

[1] إبراهيم راسخ،التحقيق الجنائي العلمي،اكاديمية شرطة دبي،الإمارات العربية المتحدة،الطبعة الاولى،1991.ص393،392.

تكنولوجيا المعلومات، ويكون تشكيله ملائم مع طبيعة الجرائم الإلكترونية، وتحديدا لمكافحة سرعة تدمير الأدلة الإلكترونية والتخلص منها.

إن إجراءات التفتيش في الجرائم الإلكترونية لا يمكن لشخص واحد القيام بها، بل بحاجة إلى تعاون عدة أشخاص لضمان نجاحه، كون إجراءات التفتيش بحاجة إلى أشخاص فنيين متخصصين في تفتيش وسائل تكنولوجيا المعلومات يسانده فريق أمني متخصص لفرض السيطرة الأمنية على المكان المراد تفتيشه لضبط مداخله ومخارجه . حيث سنتناول الفريق الفني للتفتيش بالجرائم الإلكترونية أولا، وفريق الاقتحام ثانيا [1].

أولا : الفريق الفني للتفتيش في الجرائم الإلكترونية

الفريق الفني للتفتيش بالجرائم الإلكترونية، يتكون من عدة أشخاص كل واحد منهم له دور محدد في إجراءات التفتيش، وتلك الأدوار محددة بناءً على تخطيط مسبق، وهذا التخطيط يحدد الهدف من التفتيش دور كل عضو بالفريق [2] ،يتكون الفريق الفني للتفتيش من مشرف على التفتيش، مهمته الإشراف على إجراءات التفتيش وخبراء في وسائل التكنولوجيا الحديثة[3]، وخبراء مختصين في مسرح الجريمة الإلكترونية، مهمتهم البحث والتدقيق ، وفحص جميع الغرف والمخازن والمخابئ ، وأشخاص مختصين بضبط وتحريز الأدلة، وهم ذو خبرة في التقنية الإلكترونية ، وكذلك يضم أشخاص للرسم والتصوير، مهمتهم رسم الخرائط (الكروكة) لمسرح الجريمة وتحديد مواقع الأجهزة والملفات والأشخاص والتقاط الصور الفوتوغرافية والتصوير بالفيديو[4].

[1] أشرف أحمد مصطفى عموري، المرجع السابق،ص75.
[2] محمد مصطفى موسى،ص264،245.
[3] عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت،دار الكتب القانونيةودار شتات للنشر و البرمجيات، مصر 2007،ص392.
[4] إبراهيم راسخ،التحقيق الجنائي العلمي،أكاديمية شرطة دبي، الإمارات العربية المتحدة،الطبعة الأولى، 1991 .

ثانياً :فريق الاقتحام للتفتيش في الجرائم الإ لكترونية

فريق الاقتحام للتفتيش في الجرائم الإلكترونية المتخصص، ويتم تجهيزه باختيار أعضائه من قوات مسلحة ومدربة على تأمين المكان محل التفتيش بالسرعة المطلوبة للمحافظة على الوسائل الإلكترونية من التدمير.

أجاز المشرع الفلسطيني في المادة "43" من قانون الإجراءات الجزائية، تنفيذ التفتيش باستخدام القوة إذا رفض المقيم بالمنزل أو المسؤول عن المكان السماح للقائم بالتفتيش بالدخول، ولم يشر المشرع الفلسطيني في قانون الجرائم الإلكترونية إلى آلية تنفيذ التفتيش، ولكن التفتيش في الجرائم الإلكترونية ليحقق أهدافه يجب أن يعتمد على عنصر المفاجئة والسرعة في السيطرة على المكان لتنفيذ التفتيش تماشيا مع طبيعة تلك الجرائم .

ويجب أن يتم دخول المكان محل التفتيش في الجرائم الإلكترونية عن طريق فريق الإقتحام بدون إذن صاحب البيت لتحقيق عنصر المفاجئة، ولمنع المجرم الإلكتروني من إخفاء الأدلة أو تدميرها[1] هذا الأسلوب مطابق للأسلوب الأمريكي للتفتيش بالجرائم الإلكترونية، الذي يتم عبر قيام الشرطة في إقتحام المكان بصورة سريعة ومن كافة المنافذ في وقت واحد، ويتم إبعاد الجميع عن وسائل تكنولوجيا المعلومات وإدخال الجميع إلى غرفة لا توجد بها وسائل إلكترونية وبعد ذلك يتم تقديم إذن التفتيش، والبحث عن وسائل تكنولوجيا المعلومات المطلوبة [2].

[1] أشرف أحمد مصطفى العموري،المرجع السابق ،ص76،77.

[2] عبد الفتاح بيومي حجازي،المرجع السابق ،ص384 .

ترجع طريقة تنفيذ التفتيش لتقدير القائم به، مادام التفتيش في ذاته حصل بناء على أمر قانوني [1]، والأصح أن الدخول للأماكن حتى من بابه، ولكن يجوز لمأموري الضبط القضائي بعد الحصول على إذن بالتفتيش أن يتخذوا لتنفيذه أي طؤيقة شرط أن لا يخرجوا عن القانون ويكون هدفه تحقيق الغرض منه، ويجوز الدخول خلسة إلى المكان المراد تفتيشه، و إعلام الشخص المراد تفتيشه وتفتيش ممتلكاته بعد ذلك كون أن الإعلام ربما يكون له تأثيرا عكسيا في الجرائم الإلكترونية لما يعرض التفتيش للخطر لمحاولة العبث بالدليل ومحوه [2].

للمشرف على التفتيش بالجرائم الإلكترونية، أن يصدر أوامره للقوة المرافقة التحفظ على أفراد أسرة الشخص المعني بتفتيش مسكنه ريثما ينتهي من التفتيش، وهذا ليس قبض ، وإنما من الإجراءات التحفظية لتساعده على إجراء مهمته، واذا صدر الإذن بالتفتيش لمأموري الضبط بإجراء التفتيش واستعان الضابط بزملائه لمساعدته لإجراء التفتيش، فان كل ما أجراه كل منهم من تفتيش بمفرده صحيحا لوقوعه في حدود الإذن [3].

وحسب وجهة نظرنا فإن الطرق التقليدية للدخول إلى الأماكن يحتاج إلى قرع الجرس، وعرض إذن التفتيش على الموجود بالمكان المراد تفتيشه ، وطلب الإذن منه لإجراء التفتيش، فإذا رفض يجوز إستخدام القوة لتنفيذ التفتيش، وهذا يحتاج إلى وقت، ولكن هذا الوقت يعتبر كبير في التفتيش بالجرائم الإلكترونية نظراً لخصوصيتها، وهذا الوقت كافي لأي مجرم إلكتروني بتدمير الأدلة الإلكترونية أوإخفائها، وهذا لا يتوافق مع خصوصية

[1] عبد الملك جندي،الموسوعة الجنائية،دار العلم للجميع،الطبعة الثانية، الجزء 2،3،4،دون سنة نشر، بيروت، لبنان.
[2] عمرمحمد أبو بكر بن يونس،الإجراءات الجنائية عبر الإنترنت في القانون الامريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، الطبعة الثانية،دار النهضة العربية، القاهرة،2006/2005، ص207.
[3] أشرف احمد مصطفى عموري، المرجع السابق ،ص77.

الجرائم الإلكترونية التي تحتاج إلى سرعة فائقة في الدخول إلى المكان المراد تفتيشه والسيطرة على الوسائل الإلكترونية.

المطلب الثاني :الإجراءات الفنية للتفتيش في الجرائم الإلكترونية

التفتيش التقليدي، هو الذي يهدف إلى البحث عن الأشياء المادية المتعلقة بالجريمة وتفيد في كشف الحقيقة، ولكن التفتيش في الجرائم الإلكترونية يهدف للبحث عن أشياء مادية ومعنوية لوسائل تكنولوجيا المعلومات، كون أن الأدلة الإلكترونية تحفظ وتخزن داخل تلك الوسائل[1]، لذلك سنتناول تفتيش مكونات وسائل تكنولوجيا المعلومات في الفرع الأول، ونبحث بالصعوبات والتحديات التي تواجه القائم بالتفتيش في الفرع الثاني .

الفرع الأول :تفتيش مكونات وسائل تكنولوجيا المعلومات.

تفتيش مكونات وسائل تكنولوجيا المعلومات يحتاج إلى أشخاص ذوي خبرة كونها تتكون من مكونات مادية وأخرى غير مادية، إجراء تفتيش على مكونات وسائل تكنولوجيا المعلومات، يخضع لصفة مكان وجودها، سواء بحوزة الأشخاص أو داخل الأماكن، سواء كانت منعزلة، أو متصلة بأجهزة أخرى عن طريق الشبكات الخاصة والعامة، داخل الدولة أو خارجها[2]، لذلك سنبحث بتفتيش المكونات المادية لوسائل تكنولوجيا المعلومات أولا، وتفتيش المكونات المعنوية ثانيا.

أولا : تفتيش المكونات المادية لوسائل لتكنولوجيا المعلومات.

[1] محمود محمد محود جابر،الأحكام الإجرائية للجرائم الناشئة عن استخدام العواتف النقالة، جرائم نظم الاتصالات و المعلومات،دراسة مقارنة، الكاتب الثاني،المكتب الجامعي الحديث،2018/2017،ص164.

[2] علي محمود علي حمودة، الادلة المتحصل من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى مؤتمر الجوانب القانونية و الامنية للعمليات الإلكترونية، أكاديمية شرطة دبي،الإمارات العربية المتحدة،العدد 4، المجلد الأول، 2003.

يهدف تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات التي هي عبارة عن المواد التي توجد بمكان الحادث أو الصلة به إلى البحث عن شي يتصل بجريمة إلكترونية وقعت ويفيد بكشف الحقيقة عنها وعن مرتكبيها [1].

إن تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات لا يثير أي مشكلة قانونية طالما تمت وفق الإجراءات القانونية وتطبق عليها القواعد التقليدية للتفتيش [2] ولكن مكان وجودها له أهمية، حيث يتوقف تفتيشها على طبيعة المكان الموجودة فيه، فإذا كانت بحيازة الشخص فإنها تخضع لقواعد لتفتيش الأشخاص، وإذا كانت موجودة في مكان فإن تفتيشها يخضع لقواعد تفتيش الأماكن بنفس الضمانات و الشروط.

ثانياً :تفتيش المكونات الغير مادية لوسائل لتكنولوجيا المعلومات.

إن تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، يثير صعوبات ومشاكل قانونية نظرا لطبيعتها الغير ملموسة ، ونظراً لخصوصيتها وطرق تخزينها وأماكن وجودها.

المشرع الفلسطيني أجاز في نص المادة 1/32 من قانون الجرائم الإلكترونية تفتيش وسائل تكنولوجيا المعلومات، التي عرفها في المادة الأولى على أنها تتكون من وسائل مادية و غير مادية، وقد نصت المادة 1/50 من قانون الإجراءات الجزائية الفلسطيني، على أنه لا يجوز التفتيش إلا على الأشياء الخاصة بالجريمة، ولكن المشرع البحريني كان أكثر جرأة ووضوحا عندما عرف كلمة شيء أو أشياء بالمادة 2/22 من قانون جرائم تقنية المعلومات، على أنها تشمل نظام تقنية المعلومات أو أي جزء منها، وبيانات

[1] علي عدنان الفيل، المرجع السابق،2012،ص41.
[2] هلالي عبد الله احمد،تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،دراسة مقارنة، الطبعة الثانية،دون ناشر،2008،ص73.

تقنية المعلومات، وأي من وسائط تخزين بيانات وسيلة تقنية المعلومات، أما المشرع الفرنسي أضاف كلمة المعطيات المعلوماتية إلى كلمة أشياء الواردة بالنص، لتشمل المكونات الغير مادية لوسائل تكنولوجيا المعلومات [1].

اختلف الفقهاء على إمكانية تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، منهم من أنكر إمكانية تفتيشها لطبيعتها الغير ملموسة، ومنهم من أقر إمكانية تفتيشها، حيث سنستعرض تلك الآ راء بشكل من البيان على النحو التالي:[2]

الرأي الأول :يرى (Vassilaki) ، أنه يجوز تفتيش المكونات المنطقية الإلكترونية بمختلف أشكالها مستندا إلى القوانين الإجرائية التي تنص في إذن التفتيش على ضبط "أي شيء"، وكلمة أي شيء تشمل المكونات المعنوية المحسوسة وغير المحسوسة [3]،كما تشمل المكونات المادية والغير مادية لوسائل تكنولوجيا المعلومات، والمكونات الغير مادية تفسر على أنها تشتمل على البيانات المخزنة أو المعالجة الكترونية.

إن الوصول إلى معرفة المكونات الغير مادية لوسائل تكنولوجيا المعلومات يمكن من خلال البحث في تعريف المادة، حيث تعرف المادة بأنها " كل ما شغل حيزاً مادياً في فراغ معين، وأن الحيز يمكن قياسه والتحكم فيه "و ان الكيانات المنطقية لوسائل المعلومات تأخذ حيزاً مادياً في الذاكرة ويمكن قياسها بمقياس معين ، وتأخذ شكل نبضات

[1] أشرف أحمد مصطفى عموري، المرجع السابق،ص80.

[2] أشرف أحمد مصطفى عموري ،المرجع السابق، ص80.

[3] علي عبد القادر القهوجي،الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون و الكمبيوترو الانترنت ،كلية الشريعة و القانون،جامعة الإمارات العربية المتحدة بتاريخ:03،2000/05/01 ،المجلد 2، الطبعة الثالثة،ص561.

إلكترونية تمثل الرقمين صفر أو واحد، وطبقا لذلك تعد كيان مادي تشبه التيار الكهربائي [1].

الرأي الثاني :يرى (piragff) أن كلمة" أي شيء "لا تنطبق على المكونات المنطقية الإلكترونية، ويجب مواجهة هذا القصور التشريعي بالإضافة إلى كلمة شيء كلمة المكونات المعنوية الالكترونية، كما فعل المشرع الفرنسي [2].

الرأي الثالث: يرى (Mohrenschlager) أن هدف التفتيش هو ضبط الأدلة، وأن الضبط لا يقع إلا على الأشياء المادية، ويمكن ضبط الأدلة التي تتخذ شكلا ماديا، عن طريق تصويرها أو طبعها أو نقلها على حافظة بيانات مادية.

ولكن يجب التمييز بين المعلومات والبيانات، كون أن المعلومات ليس شيئا ماديا ولا يرد عليها تفتيش، ولكن البيانات المعالجة الكترونيا هي نبضات أو ذبذبات إلكترونية قابلة للتسجيل والتخزين على وسائط معينة ويمكن نقلها ويمكن تقديرها كميا وقياسيا وهي بذلك شيء ملموس للعالم الخارجي له وجود مادي ويرد عليها التفتيش [3]، وهذه البيانات والمعلومات المخزنة في وسائط التكنولوجيا تصلح لان تكون محلا للتفتيش إذا تم تسجيلها على ورق أو على الأقراص أو أية دعامة أخرى [4].

إن تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات، هو تفتيش للفضاء الإفتراضي غير الملموس في أغلب الأحيان بما يصعب معه تحريز الأدلة إلا من خلال تجميده على شكل مادي ملموس، وهو أمر صعب إذا بقيت على صورتها المعنوية في

[1] علي عدنان الفيل، المرجع السابق، ص43.

[2] أشرف أحمد مصطفى عموري ،المرجع السابق، 81.

[3] محمود محمد محمود جابر،المرجع السابق،ص168.

[4] خالد عياد الحلبي،إجراءات التحري و التحقيق في جرائم الحاسوب و الإنترنت،الطبعة الاولى،دار الثقافة للنشر و التوزيع، عمان،2011،ص160.

شكل نبضات أو ذبذبات، أما إذا حولت إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها[1] .

الفرع الثاني :تحديات إجراءات تفتيش وسائل تكنولوجيا المعلومات

تفتيش وسائل تكنولوجيا المعلومات لا يتم بسهولة كما في الجرائم التقليدية، كون التفتيش في البيئة الإلكترونية له خصوصيته التي تخلق صعوبات للقائم به لمنعه من القيام بالتفتيش على وسائل تكنولوجيا المعلومات، وحرمانه من الوصول إلى الأدلة الإلكترونية. وبناءً على هذه الخصوصية التي تتمتع بها وسائل تكنولوجيا المعلومات تظهر صعوبات ومعوقات تواجه القائم بالتفتيش، حيث سنبحث بالمعوقات الفنية أولا ، والصعوبات الجغرافية ثانيا[2].

أولا : صعوبات فنية تقنية

القائم بالتفتيش يواجه أثناء قيامه بإجراء تفتيش على وسائل تكنولوجيا المعلومات صعوبات فنية تقنية، وتلك المعوقات يمكن أن تكون مانعا إلكترونيا لإجراء تفتيش على تلك الوسائل

عرف المشرع الفلسطيني في المادة الأولى من قانون الجرائم الإلكترونية كلمة السر بأنها "كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها، وكذلك عرف الشفرة بأنها " مفتاح أو مفاتيح سرية خاصة لشخص أو لجهة معينة

[1] خالد ممدوح إبراهيم،فن التحقيق الجنائي في الجرائم الإلكترونية،الطبعة الأولىندار الفكر الجامعي ن الإسكندرية،2010،ص200،199.

[2] أشرف أحمد مصطفى عموري، المرجع السابق ،ص 82.

تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها."

إن وسائل تكنولوجيا المعلومات، يمكن حمايتها بأرقام سرية لمنع الوصول إلى البيانات والمعلومات المخزنة داخليا، وهذه الأرقام لا يعرفها إلا صاحب تلك الوسائل أو مستخدمها، ولا يمكن إجباره على البوح[1] بها ، وقد أجاز المشرع الفلسطيني بالمادة 33 من قانون الجرائم الإلكترونية للنيابة العامة الحصول على بيانات المرور الخاصة بالمشتركين ، كون أنه لا يمكن إجراء تفتيش على وسائل تكنولوجيا المعلومات دون الكشف عن أرقام الحماية، ولكن إذا لم يتم الحصول عمليها أو لم يفصح المتهم عنها، يجوز للمفتش أن يستخدم برامج خاصة لفك الشيفرة والنفاذ إلى وسائل تكنولوجيا المعلومات واجراء تفتيش عليها .

ثانياً :صعوبات جغرافية

إضافة إلى الصعوبات الفنية التقنية لإجراء تفتيش على وسائل تكنولوجيا المعلومات، يواجه القائم بالتفتيش صعوبات أخرى جغرافية، تحتاج إلى وقت وجهد لا يقل أهمية عن الصعوبات التقنية.

وسائل تكنولوجيا المعلومات يمكن أن تكون منعزلة، ويمكن أن تكون متصلة بوسائل أخرى نهايتها في مكان أخر غير المكان المراد تفتيشه، ويخضع تفتيشها لنفس الضمانات المقررة بالقانون اتصال وسائل تكنولوجيا المعلومات ببعضها من الصعوبات الجغرافية التي تواجه القائم بالتفتيش، سواء كانت هذه الوسائل متصلة ببعضها داخل الدولة أو خارجها.

[1] يوسف أمير فرج،الجرائم المعلوماتية على شبكة الأنترنت،دار المطبوعات الجامعية ، الإسكندرية،2008،ص234.

أ_ معوقات جغرافية داخل الدولة: من الصعوبات التي تواجه القائم بالتفتيش بالجرائم الإلكترونية، وجود المعلومات والأدلة المبحوث عنها مخزنة في وسائل إلكترونية متواجدة في مكان أخر داخل حدود الدولة.

المشرع الفلسطيني، أجاز لوكيل النيابة إذا اقتضى الأمر اتخاذ إجراء من الإجراءات خارج دائرة الاختصاص الجغرافي أين بنوب عنه وكيل نيابة تلك الدائرة ، وهذا النص يسمح لقائم بالتفتيش بالجرائم الإلكترونية في حال أن الأدلة المطلوبة مخزنة خارج دائرة اختصاصه أن ينيب عنه من هو مختص بالتفتيش في المكان الآخر التي توجد به تلك الأدلة ، وهذا بحاجة إلى أذون إضافية لكل مكان تتواجد به البيانات لإجراء تفتيش عليه.

ب_ معوقات جغرافية خارج الدولة: المعوقات الجغرافية بالتفتيش بالجرائم الإلكترونية ليست داخلية فقط، وإنما يوجد معوقات خارجية كذلك تواجه القائم بالتفتيش .

أصعب المشاكل التي تواجه القائم بالتفتيش في الجرائم الإلكترونية[1] قيام المجرمين بتخزين بياناتهم في أنظمة تقنية خارج حدود الدولة، مستخدمين في ذلك شبكات الإتصال الإلكترونية لعرقلة سلطة التفتيش من جمع الأدلة، وبسبب ذلك يتعذر إجراء تفتيش على تلك الوسائل إلتزاما بمبدأ عدم الإعتداء على سيادة دولة أخرى .

المشرع الفلسطيني في قانون الجرائم الإلكترونية لم يشر إلى إمكانية تجاوز التفتيش لحدود الدولة،

التزاماً منه بمبدأ الإقليمية بعدم الإعتداء على سيادة دولة أخرى، كون التفتيش العابر للحدود لا يجوز القيام به إلا من خلال إتفاقيات ثنائية أو دولية عن طريق التعاون

[1] أشرف أحمد مصطفى عموري، المرجع السابق،ص83.

القضائي أو بعد الحصول على إذن الدولة [1]، وفي هذه الحالة فإن يد القائم بالتفتيش تبقى مقيدة .

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات أجازت في المادة"40" [2]إجراء تفتيش على وسائل تكنولوجيا المعلومات المتواجدة في دولة أخرى دون تفويض من تلك الدولة، ولكن وضعت شرطين لإجراء هذا التفتيش دون النظر إلى الموقع الجغرافي المتواجدة فيه ، **الأول** أن يكون الوصول إلى المعلومات مفتوح ومصرح به، **والثاني** وجود موافقة طواعية من الشخص الذي يملك السلطة القانونية على تلك المعلومات، وهي نفس الشر وط التي وردت في المادة 32 من الإتفاقية الأوروبية للجرائم السبيرانية، وهذه الشروط توصل إليها واضعوا الإتفاقية الأوروبية بعد مخاض عسير، كون أنهم وجدوا أ نه ليس من الممكن إعداد نظام قانوني عالمي مميز يمكن تطبيقه في المجال الإلكتروني، وتراعى الظروف الخاصة بكل حالة فردية على حدى [3].

المشرع البحريني، أجاز إمتداد الدخول والتفتيش إلى نظام تقني أخر إذا كان هناك أمارات قوية بأن البيانات المتصلة بالجريمة مخزنة عليه، وتكون قابلة للدخول إليها من النظام الأول ومتاحة على نحو مشروع، وكذلك فعل المشرع الفرنسي وأجاز لرجال الضبط القضائي أن يدخلوا إلى البيانات التي قيد التحقيق والمخزنة في النظام أو في أي نظام معلوماتي أخر مادامت متصلة بشبكة واحدة مع النظام الرئيسي وتكون متاحة.

الوضع الغالب بالتفتيش بالجرائم الإلكترونية، أن يتجاوز التفتيش المكان الذي يجري تفتيشه إلى مكان أخر، في ظل شبكة الأجهزة وربطها ببعضها سواء محليا أو إقليميا،

[1] علي عدنان الفيل، المرجع السابق،ص46.
[2] المادة 40 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.
[3] هلالي عبد الإله أحمد،اتفاقية بوداباست لمكافحة جرائم المعلوماتبة، الطبعة الأولى ،دار النهضة العربية ، القاهرة، 2011،ص 379.

كون أنه لا وجود لحدود جغرافية محددة في الجرائم الإلكترونية ولا يشترط الحصول على موافقة طرف ثالثا.[1]

المطلب الثالث: أثار التفتيش في الجرائم المعلوماتية

يهدف إجراء التفتيش إلى الحصول على الدليل لإثبات الجريمة محل التحقيق و إسنادها إلى شخص معين فإذا كانت النتائج التفتيش ايجابية وتم العثور على المعطيات المبحوث عنها فإنه يجب ضبطها وحجزها إذا كانت قابلة للحجز ،وفي حالة استحالة ذلك ،فإنه يجوز للسلطات المختصة اللجوء إلى منع الوصول اليها وسنتطرق لذلك وفقا لما يأتي :

الفرع الأول: حجز المعطيات المعلوماتية

إذا كان من المعروف في التفتيش في الجرائم العادية في أنه يتم ضبط الأشياء وحجزها التي تفيد في إثبات الجريمة وهي أشياء مادية إذ يتم جرد المنقولات ووضعها في إحراز ونقلها بينما يتم التحفظ على العقارات وتشميعها للمحافظة على آثار الجريمة فإن الأمر يختلف عنه في الجريمة المعلوماتية لأنها تتضمن أشياء مادية تتمثل في أجهزة الحاسب ولواحقها ، و الأقراص الصلبة و المرنة ،وأشرطة التخزين وأجهزة الإرسال وأشياء معنوية غير محسوسة تتمثل في البيانات و النظم والبرامج الموجودة التي تكون محل التفتيش.[2]

فبالنسبة للأشياء المادية، فلا جدال في إمكانية ضبط وحجز جميع الأشياء المفيدة في إظهار الحقيقة و الناتجة عن عملية التفتيش وإذا كانت هذه الأشياء مادية و التي يمكن

[1] أشرف أحمد مصطفى عموري،لمرجع السابق،ص 87 .

[2] رضا هميسي، المرجع السابق،ص 173،174 .

ان يكون من بينها أجهزة الحاسوب أو إحدى مكوناته المادية ويتعين جرد هذه الأشياء وتحرير محضر عنها و إرفاقه بملف الإجراءات ويتعين على القائم بالتفتيش و الحجز ان يحافظ على هذه الأجهزة بالحالة التي كانت عليها (المادة 84 من ق.إ.ج)

أما فيما يتعلق بالأشياء اللامادية او المعنوية فقد اختلف الفقهاء فيما يتعلق بحجز وضبط البيانات المعالجة و المعطيات المخزنة في الحاسوب أو النظم المعلوماتية وظهر هناك اتجاهان:[1]

الإتجاه الأول: ويرى أنصاره أنه لا يمكن إجراء الحجز وضبط الكيانات المنطقية لانتفاء الكيان المادي لها ،إلا أن هذه النظرية عفا عنها الزمن ولم تعد تساير متطلبات التفتيش عن الجريمة في المجتمع الرقمي ،ما أدى لهجرها من قبل الفقه[2] .

الاتجاه الثاني: ويرى أصحاب هذا الاتجاه أنه لا يوجد ما يمنع من حجز هذه البيانات و المعطيات المعالجة بنظام المعلوماتية أو ما يعرف بالبيانات الالكترونية و التي تتكون من المعلومات وهي لا يمكن حجزها لأنها أشياء معنوية بينما البيانات المعالجة آليا فهي ذات طابع مادي على أساس أنها ذبذبات إلكترونية و إشارات أو موجات كهرومغناطيسية يمكن أن تسجل وتخزن على وسائط معينة ويمكن قياسها .

ومهما يكن من أمر ،فإن القواعد الخاصة بالتفتيش بمفهومه التقليدي لم تعد تلبي متطلبات التحقيق في الجرائم المستحدثة التي ينبغي أن تحكمها قواعد تراعي الجوانب التقنية للمعلوماتية وتتماشى مع البيئة الرقمية التي ترتكب فيها مثل هذه الجرائم .

---

[1] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب و الأنترنت،دراسة مقارنة،عالم الكتب الحديث،إربد، الأردن2004،ص،145،147.

[2] رضا هميسي، المرجع السابق،ص 173،174.

وباستقراء موقف المشروع الجزائري نجده قد ذهب إلى تأكيد الاتجاه القائل بإمكانية تفتيش البيانات المعالجة آليا وضبطها ، فقد أجاز حجز المعطيات المخزنة داخل نظم المعلوماتي إذا كانت تفيد في كشف الجرائم أو مرتكبيها (المادة 6 فقرة 1 من القانون 09_04).

أما عن طريق حجز المعطيات المعلوماتية،طبقا للمادة 6 فتتم عن طريق نسخ المعطيات محل البحث و المعطيات الضرورية لفهمها، على دعامة تخزين الكترونية تكون قابلة للحجز ثم توضع في احراز طبقا لأحكام قانون الاجراءات الجزائية[1]، ويتم اللجوء إلى عملية النسخ عندما يكون من غير الضروري حجز كل المنظومة المعلوماتية، حيث ان المعلومة ستكون بالضرورة بالقرص الصلب للحاسوب التابع لمقدم الخدمة،و بالتالي فإن نسخها يتطلب حفظها على دعامة تخزين الكترونية مثل الأقراص المضغوطة أو المتحركة او الأقراص الصلبة الخارجية ،كما تمتد عملية النسخ إلى المعطيات اللازمة لفهم المعطيات محل التفتيش ، حيث أنه من الممكن إن هذه الأخيرة لا تقرأ مباشرة إلا بتدخل وسائل معينة ومعطيات أخرى

وبعد القيام بعملية التفتيش و الحجز وجب على السلطة التي قامت بذلك المحافظة على سلامة المعطيات في المنظومة المعلوماتية محل التفتيش وذلك باتخاذ الوسائل الفنية المطلوبة لضمان سلامة المعطيات المعلوماتية المحجوزة ، حيث أن الحجز في مثل هذه الحالات لا يعني محو المعطيات المخالفة أو إتلافها ، بل هو إجراء يهدف إلى

[1] المادة 6 الفقرة 2من القانون 09_04.

جمع أدلة الإثبات ،وإذا حجزت مع المعطبات أجهزة لا علاقة لها بالنظم المعلوماتية [1]، كأن يؤدي ذلك إلى تعديل مضمونها او محو جزء منها ،أو تعطيل جزء آخر.

الفرع الثاني: منع الوصول إلى المعطيات المعلوماتية

في بعض الأحيان يستحيل نسخ المعطيات لأسباب تقنية ،كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها ن فيتعين حينئذ على السلطة المكلفة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية و الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (المادة 7 من القانون09_04) و الهدف من هذا الإجراء الاحترازي هو الحفاظ على الأدلة في محيطها الالكتروني ، ومنع اي محاولة لطمسها او إخفاء معالمها ،وهو ما سيكون له دون شك الأثر الايجابي في نجاح إجراءات التفتيش [2].

المطلب الرابع: أثر عدم مشروعية إجراءات التفتيش

إن عدم مشروعية التفتيش من شأنه أن يوصم الدليل الناتج عنه بعدم المشروعية ،فإذا ما تمت الإجراءات الجزائية الماسة بحرمه الحياة الخاصة دون إتباع القواعد القانونية المحددة فإن ذلك يؤدي إلى بطلانها .

الفرع الاول: أسباب بطلان التفتيش

[1] المادة 6 الفقرة 3 من القانون 09_04.
[2] رضا هميسي، المرجع السابق ،ص 177,176.

لقد نظم المشرع البطلان بأسلوبين ،مرة يرتبه صراحة في حالة توافر أسبابه المحددة في القانون تحديدا دقيقا ،وهو ما يطلق عليه البطلان المطلق ، ومرة يرتبه عند مخالفة الأحكام الجوهرية وهي حالات غير محددة.

ففيما يتعلق بالإجراءات الماسة بالحياة الخاصة للأفراد نجد أن المشرع قد اقتصر في نص المادة 48 ق.إ.ج [1]على تقرير بطلان الإجراءات التي تخالف أحكام الماديتين 45و47 من ق.إ.ج، في حين أغفل الإشارة للآثار المترتبة على مخالفة أحكام [2] المواد 65مكرر 5 إلى 65 مكرر 9 المتعلقة بشروط اللجوء إلى الأساليب الخاصة بالتحري و التحقيق وهذا القصور من المشرع والفراغ القانوني يجب تداركه.

بالرجوع إلى مضمون المادتين 45و47 نلاحظ أن الإجراءات التي يترتب البطلان عليها هي:

_ استصدار الإذن المكتوب في حالة التحقيق في الجريمة المتلبس بها من وكيل الجمهورية أو قاضي التحقيق عند التفتيش في حالة الجريمة المتلبس بها ، ولاستظهاره لصاحب المسكن أو من يعينه وهذا لأن المادة 45 تحيل إلى المادة 44.

_ حضور صاحب المسكن أو من يعينه ليمثله أو تعيين شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية إذا تعذر على صاحب المسكن حضور التفتيش أو امتنع عن الحضور أو كان هاربا .

[1] نص المادة 48 من قانون الإجراءات الجزائية ، الأمر 66_155 المؤرخ في 8جوان 1966 المعدل و المتمم بالقانون 17_07 المؤرخ في:27مارس 2017:" يجب مراعاة الإجراءات التي تستوجبها المادتين 45،47 ويترتب على مخالفتها البطلان.

[2] مجادي نعيمة، الضوابط الإجرائية لتفتيش المسكن ضمانا للحق في حرمة الحياة الخاصة، مجلة البحوث في الحقوق و العلوم السايسية، المجلد03، العدد 02 سنة النشر،2018،ص79.

_ مراعاة التوقيت الزمني أي إجراء التفتيش بعد الخامسة صباحا وقبل الساعة الثامنة مساءا.[1]

إذا لم يلتزم ضابط الشرطة القضائية أو من يساعده من أعوان الشرطة القضائية بهذه الإجراءات فإن التفتيش يكون باطلا أي لا يأخذ به القاضي، وينصب هذا البطلان على النتائج المترتبة عن هذا التفتيش مثل الأشياء و المستندات التي تشكل أدلة على ارتكاب الجريمة أو إسنادها إلى شخص من الأشخاص [2].

الفرع الثاني: آثار الحكم بالبطلان

القاعدة أن يبقى العمل الإجرائي منتجا لآثاره القانونية حتى يقرر القاضي بطلانه ، وهذه القاعدة تسري أيا كان نوع البطلان سواء تعلق بالمصلحة العامة أو بالنظام العام، فإذا تقرر بطلان الإجراء فإنه لا ينتج أي أثر قانوني ويعد كأنه لم يباشر من الناحية القانونية ،وعليه بموجب المادة 2/60 من ق.إ.ج سحب الإجراءات الباطلة ،ويحظر الرجوع اليها لاستنباط عناصر أو اتهامات ضد الخصوم في المرافعات .

أما أثر الإجراء الباطل في الأعمال الإجرائية الأخرى أن الحكم ببطلان الإجراء لا أثر له على الإجراءات السابقة إذ هي مستقلة عنه فلا تتأثر بالبطلان متى تمت صحيحة في ذاتها.

أما بالنسبة للأعمال اللاحقة للإجراء الباطل فالقاعدة أن بطلان العمل الإجرائي يؤدي إلى بطلان الأعمال اللاحقة المبنية عليه، لأن ما بني على باطل فهو باطل ،فمعيار الإجراءات اللاحقة أن تكون مرتبطة بالإجراء الباطل أو أثرا مباشرا ترتب عليه، و

[1] أ، مجادي نعيمة، المرجع السابق،ص 79

[2] أحمد غامي، الحماية القانونية لحرمة المسكن، دار هومة، الجزائر،2011،ص 122.

المقصود بالارتباط هو الارتباط القانوني الذي يجعل الإجراء السابق مفترضا قانونيا لصحة الاجراء اللاحق بالإجراء السابق الباطل ومدى تأثره به من شؤون محكمة الموضوع تقدره حسب ما ينكشف لها من ظروف الدعوى و ملابساتها .

ويترتب على ما تقدم نتيجتان الأولى بطلان الاجراء السابق لا ينصرف إلى الاجراءات التالية له و المستقلة عنه، أما الآنية فتتمثل في استبعاد الأدلة المستمدة من الإجراء الباطل وذلك عملا للقاعدة السائدة التي مؤداها استبعاد الادلة المحصلة بطريق غير مشروع.[1]

[1] خليف مصطفى، الحق في الحياة الخاصة في القانون الجزائري، مذكرة لنيل شهادة الماجستير في الحقوق، الجزائر،2011،ص179.

خاتمة

خاتمة

على ضوء دراستنا لموضوع تفتيش الجريمة المعلوماتية توصلنا إلى مايلي:

يعد التفتيش في الجريمة المعلوماتية من أهم الإجراءات التقليدية التي أقرها المشرع الجزائري للتحقيق في مجال الجرائم المعلوماتية بجانب الإجراءات المستحدثة وهو من أصعب إجراءات البحث والتحري الأمر الذي يتطلب خبرة واسعة وكفاءة عالية .

المحل الذي ينصب عليه تفتيش النظم المعلوماتية ذو نطاق واسع يشمل المكونات المادية والمعنوية للحاسب الآلي فهو يتسم بطبيعة خاصة تميزه عن التفتيش بمفهومه التقليدي الذي يقتصر على الأشياء المادية الملموسة فقط .

أخضع المشرع الجزائري تفتيش النظم المعلوماتية إلى مجموعة من الضوابط الموضوعية والشكلية المقررة في قانون الإجراءات الجزائية إلا أنه نظرا لطبيعتها وخصوصية الجريمة المعلوماتية فإنه أورد بشأنها بعض الاستثناءات التي تشكل خروجا عن القواعد المألوفة في التفتيش التقليدي، يترتب على عدم مراعاة هذه الضوابط بطلان إجراء التفتيش عملا بمبدأ الشرعية الجزائية.

وقد توصلنا من خلال دراستنا إلى العديد من النتائج نذكر البعض منها:

1- التفتيش في الجرائم الإلكترونية من أدق وأخطر إجراءات التحقيق، كونه يمس خصوصية الناس بالاطلاع على أسرارهم المخزنة في وسائل تكنولوجيا المعلومات .

2- الجرائم الإلكترونية جرائم مستمرة يصعب معرفة فاعلها، ترتكب في أي مكان في هذا العالم، وتتحقق أثارها في مكان آخر، والتفتيش بتلك الجرائم بحاجة إلى نظام إجرائي خاص يراعي خصوصيتها، وبحاجة إلى أشخاص مؤهلين ومدربين تدريبا قانونيا وفنيا، للتعامل مع وسائل تكنولوجيا المعلومات والتغلب على التحديات الفنية التي يمتاز بها .

3- محل التفتيش في الجرائم الإلكترونية هو وسائل تكنولوجيا المعلومات سواء كانت بحوزة أشخاص أو داخل الأماكن، وهذه الوسائل يمكن حمايتها بأرقام سرية لمنع الوصول

إليها ويصعب اختراقها، وتحتاج إلى أجهزة ومعدات تقنية لاستخراج الأدلة، وهذا إجراء شاق وصعب ومجهول النتيجة .

4- التفتيش في الجرائم الإلكترونية يكون داخل حدود الدولة أو يمتد إلى خارجها.

5- التفتيش في الجرائم الإلكترونية بحاجة إلى تعاون ومساعدة بين الدول، كون أنه لا تستطيع دولة واحدة بمفردها مكافحة تلك الجرائم لوحدها.

6- الأدلة الإلكترونية تتكون من أدلة مادية وغير مادية، وهي أدلة حساسة بحاجة إلى معاملة لينة وإجراءات خاصة لضبطها، وكذالك تحتاج إلى أماكن مخصصة لحفظها على الحالة التي ضبط عليها.

وعليه يمكن أن نقترح التوصيات التالية:

_ ضرورة توحيد القواعدالمتعلقة بالإجراءات المتبعة في مكافحة جرائم تكنولوجيا الاعلام والاتصال في مدونة واحدة تبعا لخصوصيات هذه الجرائم وخصوصية مرتكبيها أو إدماجها في قانون الإجراءات الجزائية .

_ إن القواعد الخاصة بالتفتيش بمفهومه التقليدي لم تعد تلبي متطلبات التحقيق في الجرائم المستحدثة التي ينبغي أن تحكمها قواعد تراعي الجوانب التقنية المعلوماتية وتتماشى مع البيئة الرقمية التي ترتكب فيها مثل هذه الجرائم الأمر الذي يتوجب على المشرع تداركه .

_ تعزيز التعاون الدولي في إطار اتفاقيات دولية أو ثنائية مع تفعيل آليات المساعدة الدولية في المجال القضائي وتسليم المجرمين وذلك باحترام مبدأ المساواة بين الدول وهذا ماتقتضيه خصوصية الجرائم المعلوماتية باعتبارها جرائم عابرة للحدود وذلك لمحاصرة هذه الجرائم وملاحقة مرتكبيها وإنزال العقاب بهم .

إن موضوع هذاالبحث قد تناول مشكلة من المشكلات التي أفرزتها ثورة المعلومات والاتصالات عن بعد، حيث أنه لاشك في أن التفتيش المتعلق بالجرائم 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 و المحققين والقضاة.

ومن أهم النتائج التي يمكن أن نخلص إليها:

-إن قانون الإجراءات الجزائية الجزائري يجيز التفتيش في البيئة المعلوماتية الرقمية لضبط المعلومات على الرغم من طبيعتها المعنوية .

-كما أنه يجوز أن يصدر إذن التفتيش يكون مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعين توفر شروط تفتيش المساكن، إما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنه يكفي توافر 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 جميع الملفات الموجود 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

قائمة المصادر والمراجع

قائمة المراجع والمصادر:

أولا : ***الأوامر والقوانين :

1/ أمر رقم 66 – 155 مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية المعدل والمتمم (جريدة رسمية رقم 49 مؤرخة في 11 / 6 / 1966)

2/ أمر رقم 66 – 155 المؤرخ في 8 يوليو سنة 1966 المتضمن قانون العقوبات (جريدة رسمية رقم 49 مؤرخة في 11 / 6 / 1966)

3/ قانون رقم 09 – 04 المؤرخ في 14 شعبان 1430 الموافق ل 5أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

4/ قانون رقم 04 / 15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71 مؤرخ في: 11/10 / 2004 .

5- قانون رقم 575 -2004 المؤرخ في: 2004/06/21 المتعلق بالثقة في الإقتصاد الرقمي .

6- قانون رقم 06 -22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84/ 2006 .

7- المادة 01/04، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة 2010/12/21 .

8- مجلس أوروبا مجموعة المعاهدات الأوروبية – رقم 185 الاتفاقية المتعلقة بالجريمة الالكترونية، بودابست المؤرخة في: 2001/11/23 .

ثانيا : *** الكتب:

1- إبراهيم خالد ممدوح، إبراهيم خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، طبعة 2010، دار الفكر الجامعي، الإسكندرية.

2- إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، 2009 .

3- أحمد طه محمود، المواجهة التشريعية لجرائم الكمبيوتر والأنترنت، دار الفكر والقانون 2013 المنصورة .

4- أحمد لطفي خالد الحسن، جرائم الأنترنت بين القرصنة الالكترونية وجرائم الإبتزازالالكتروني، دراسة مقارنة، دار الفكر الجامعي، 2018 الإسكندرية .

5- أحمد هلالي عبد الله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، طبعة 2008 .

6- أحمد هلالي عبد الإله، اتفاقية بودابست لمكافحة جرائم المعلوماتية، طبعة 2011، القاهرة .

5-. الملطة أحمد خليفة، الجرائم المعلوماتية، ط2، 2006 دار الفكر الجامعي، الإسكندرية .

7- الحلبي خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، طبعة 2011، عمان .

8- الطوالبة علي حسن، التفتيش الجنائي على نظم الحاسوب والأنترنت، دراسة مقارنة، طبعة 2004، عالم الكتب الحديث إربد – الأردن .

9-الشلقاني أحمد شوقي، مبادئ الإجراءات الجزائية في التشريع الجزائري، الطبعة 1998، ديوان المطبوعات الجزائرية، الجزائر .

10- المعمري عادل عبد الله خميس، التفتيش في الجرائم المعلوماتية، طبعة 2013، جامعة عجمان للعلوم التكنولوجيا، الامارات .

11- الفيل علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، طبعة 2012، الاسكندرية .

12- الغافري حسين بن سعيد، السياسة الجنائية في مواجهة جرائم الانترنت، طبعة 2009، القاهرة .

13- الأسدي ليتا محمد، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، طبعة 2015، دار ومكتبة الحامد للنشر والتوزيع، عمان'

14- بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، طبعة2012، منشورات حلبي الحقوقية، مستغانم الجزائر.

15- بن خليفة إلهام، التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، دون طبعة، الوادي .

16- بن يونس عمر محمد أبو بكر، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، طبعة 2006/2005، القاهرة .

17- بوحليط يزيد، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري التواصل في الاقتصاد والإدارة والقانون، طبعة 2016، عنابة .

18-تمام شوقي يعيش، الجريمة المعلوماتية، طبعة 2019، جامعة محمد خيضر بسكرة، الجزائر.

19- جندي عبد الملك، الموسوعة الجنائية، دون طبعة، لبنان .

20- جابر محمود محمد محمود، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة، جرائم نظم الاتصالات والمعلومات، طبعة 2018/2017 .

21- حسني محمود نجيب، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، طبعة 2013، القاهرة .

22- حجازي عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، طبعة 2007، مصر .

23-عبد الله عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية)، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، 2007 .، الجزائر.

24- عبد الله هلالي، الجوانب الموضوعية الإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست الموقعة في 2001/11/23 .

25- غامي أحمد، الحماية القانونية لحرمة المسكن، طبعة 2011، الجزائر .

فرج يوسف أمير، الجرائم المعلوماتية على شبكة الانترنت، طبعة 2008، الاسكندرية .

26- قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005 .

27- قطب محمد علي، الجرائم المستحدثة وطرق مواجهتها، طبعة 2009، دار الفجر للنشر والتوزيع، القاهرة.

28 - علي محرز خيرت، التحقيق في جرائم الحاسب الآلي، طبعة 2012، دار الكتاب الحدي

29-سامي جلال فقي حسين، سامي جلال فقي، التفتيش في الجرام المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، 2011 .

30- راسخ ابراهيم، التحقيق الجنائي الخاص، طبعة 1991، دبي الإمارات العربية المتحدة .

31- موسى مصطفى محمد، التحقيق في الجرائم الالكترونية، طبعة 2009، القاهرة .

32- مصطفى خليف، الحق في الحياة الخاصة في القانون الجزائري، طبعة 2011، الجزائر .

33- هروال نبيلة هبة، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، طبعة 2007، الاسكندرية .

34- هلالي عبد الاله أحمد، تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات، دراسة مقارنة، طبعة أولى، دار النهضة العربية مصر، دون سنة النشر .

ثالثا : ***المقالات:

1- ضياء نعمان، الحماية التقنية للتجارة الالكترونية، مجلة قانون وأعمال، المطبعة والوراقة، مراكش، المغرب العدد 1، مارس 2011 .

2-عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جانفي 2018 .

3- محمد رحموني، خصائص الجريمة الالكترونية ومجلات استخدامها، جامعة أحمد دراية –أدرار، مجلة الحقيقة العدد 41 .

4- محمد خليفة، شوقي يعيش تمام، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل البحث العلمي بيروت، لبنان .

5- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، جامعة ورقلة، العدد 5، سنة 2012 .

6- ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية – عدد 16، جوان 2017 .

7- مجادي نعيمة، الضوابط الإجرائية لتفتيش المسكن ضمانا للحق في حرمة الحياة الخاصة، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 03، العدد 02، سنة 2018 .

8- علي محمود علي حمودة، الادلة المتحصل من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدو إلى مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي الامارات العربية المتحدة، العدد 4، 2003، المجلد الأول .

9- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، المجلد 29، العدد 58، دون سنة .

رابعا : **** مذكرات وأطروحات العلمية:

1/ أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09 – 04، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ورقلة، السنة الجامعية 2012 / 2013 .

2/ موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقال مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009 .

3- ماضي نعيمة، بن ناصف وردة، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص إعلام آلي وانترنت، جامعة برج بوعريريج، سنة 2012 – 2022 .

4- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012 / 2013 .

5-نادية غرباوي، أساليب البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قسم قانون العام، جامعة آكلي محند أولحاج، البويرة، كلية الحقوق والعلوم السياسية، قسم حقوق، 2016 / 2017 .

6- أشرف أحمد مصطفى عموري، التفتيش في الجرائم الإلكترونية، رسالة ماجستير في القانون الجنائي، جامعة القدس فلسطين، السنة 2018 .

ملاحق

ملاحق:.....

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

محكمة [redacted]

نيابة الجمهورية

رقم : 22/.321 إذن بالتفتيش و الولوج الالكتروني

نحن وكيل الجمهورية لدى محكمة [redacted]

بعد الاطلاع على المستندات التالية : طلب الإذن بالتفتيش و الولوج الالكتروني

الطلب المقدم من طرف : ضابط الشرطة القضائية لامن [redacted] .

المؤرخ في :2022/06/14 تحت رقم : 22/ 2838

في اطار قضية جنحة تسريب اجوبة امتحانات النهائية للتعليم الثانوي دورة 2022 المتبعة فيها المسماة [redacted] من مواليد : 1990/06/30 بعين ولمان ابنة [redacted] والرامي إلى الإذن بالولوج الالكتروني وتفتيش الهاتفين المشتبه فيها

والمتهمة بتسريب اجوبة امتحانات النهائية للتعليم الثانوي سنة 2022.

وبناء على التحقيق الجاري حاليا في القضية.

بعد الاطلاع على المادة 4,3 / ج و المادة 5 من قانون 09/04 المتضمن القواعد الناصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها .

- حيث انه توجد دلائل قوية متماسكة من شأنها ان تؤدي الى ضرورة تفتيش الهاتفين.

لهـــــــــــذه الأســـــــــباب

نأذن لضابط الشرطة القضائية لا[redacted] بتفتيش والالكتروني للهاتفين النقالين

-1/ الهاتف الاول : نوع SAMSUNGاسود الون يحمل الرقم 352581101396771 به شريحة موبيليس رقم [redacted]

-2/ الهاتف الثاني نوع A9 REDMIازرق اللون يحمل الرقمين 8602480539335769 86024805335777 به شريحتين الاولي موبيلس رقم 0664.22.11.21 و الثانية موبيليس رقم [redacted] و استخراج اي معطيات تفيد التحقيق .

على ان يجري التفتيش و فقا للاجراءات المنصوص عليها قانونا وتحرير محضر بذلك .

حرر بالنيابة : 2/06/14

ملاحق:.....

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة الداخلية و الجماعات المحلية
و التهيئة العمرانية
المديرية العامة للأمن الوطني
أمن ولاية سطيف
المصلحة الولائية للشرطة القضائية
فرقة مكافحة الجرائم المعلوماتية
رقم: /أو/أوس/م و ش ق/ف م ج م/22.

محضر تفتيش إلكتروني

القضية ضد:

-/ إنه في يوم الثلاثاء الموافق للرابع عشر من شهر جوان .----------
-/ سنة ألفين واثنان و عشرون 2022 .----------
-/ الساعة السابعة و النصف مساءا (19:30 سا)----------
-/ نحن ملازم أول للشرطة، بالمصلحة الولائية للشرطة القضائية، رئيس فرقة مكافحة الجريمة المعلوماتية بأمن ولاية سطيف----------
ضابط الشرطة القضائية بدائرة الاختصاص.----------
بمساعدة عون الشرطة/ التابع للفرقة .----------
=/ بناءا على نص القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها /----------
-/ تنفيذا للاذن بالتفتيش الالكتروني الحامل لرقم 321/م ع/22 المؤرخ في : 2022/06/14 الصادر عن السيد وكيل الجمهورية لدى م بخصوص قضية الحال /----------
=/ بتاريخ اليوم و الشهر و السنة المذكورين اعلاه ، قمنا بعملية الولوج بإستعمال تجهيزات و ربط الانترنت الخاصة بالمصلحة من اجل القيام بعملية التفتيش الالكتروني لكل من للهاتف النقال Redmi 9A رقم الإيمي: 860248053357769//8602480539335769 المزود بشريحتين هاتفيتين للمتعامل موبيليس و

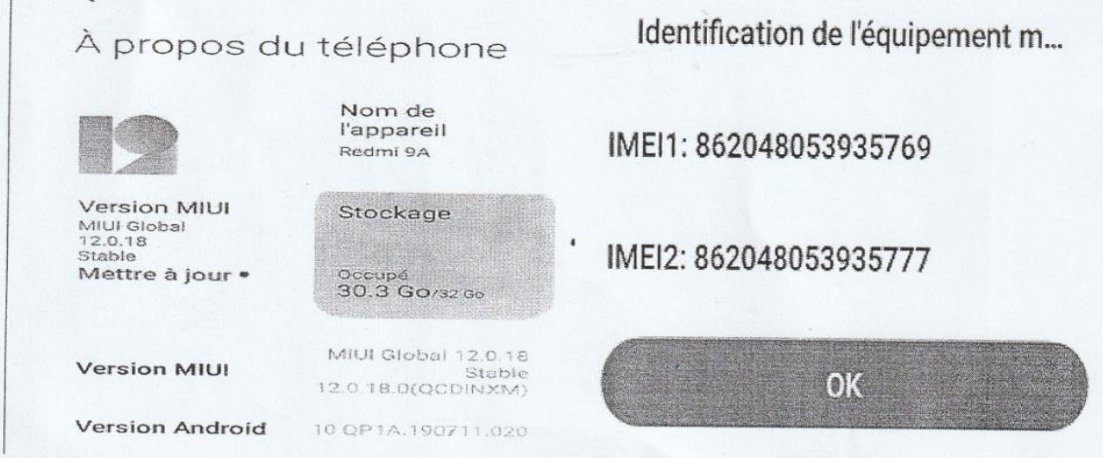
الموضوع:
محضر تفتيش الكتروني

وكذا جميع تطبيقات التواصل الاجتماعي المثبة ، 02 الهاتف النقال من نوع SAMSUNG رقم التسلسلي 352581101396771 الخاصين بالمسماة / الهدى من مواليد 1990/06/30 عين ولمان عزباء ، عاملة ، مقيمة بحبحي سطيف /----------

ضابط الشرطة القضائية

التكييف:

=/الهاتف النقال محل تحقيق من نوع Redmi 9A رقم الإيمي: 860248053357777//8602480539335769، الخاص بالمسماة /ى
المبين خصائصه ادناه /----------



ملاحق:.....

تابع/ لمحضر التفتيش الالكتروني -ص02

٢/ عملية التفتيش المقامة على الذاكرة الداخلية للهاتف النقال ،كانت ايجابية ، حيث عاينا على المسار Redmi 9A\مساحة التخزين المشتركة الداخلية\DCIM\Screenshots العديد من الصور (لقطات شاشة) لملخصات و دروس كما هو مبين في الصور ادناه /----------


Screenshot_2022-06-13-21-08-50-752_com.facebook.lite.jpg


Screenshot_2022-06-13-21-08-41-855_com.facebook.lite.jpg


Screenshot_2022-06-13-21-08-37-920_com.facebook.lite.jpg


Screenshot_2022-06-13-21-08-25-845_com.facebook.lite.jpg


Screenshot_2022-06-13-21-02-11-495_com.facebook.lite.jpg


Screenshot_2022-06-13-21-02-07-514_com.facebook.lite.jpg


Screenshot_2022-06-13-21-02-03-351_com.facebook.lite.jpg


Screenshot_2022-06-13-21-01-58-385_com.facebook.lite.jpg


Screenshot_2022-06-13-21-01-14-192_com.facebook.lite.jpg


Screenshot_2022-06-13-21-01-08-880_com.facebook.lite.jpg


Screenshot_2022-06-13-21-01-04-026_com.facebook.lite.jpg


Screenshot_2022-06-13-21-00-59-269_com.facebook.lite.jpg

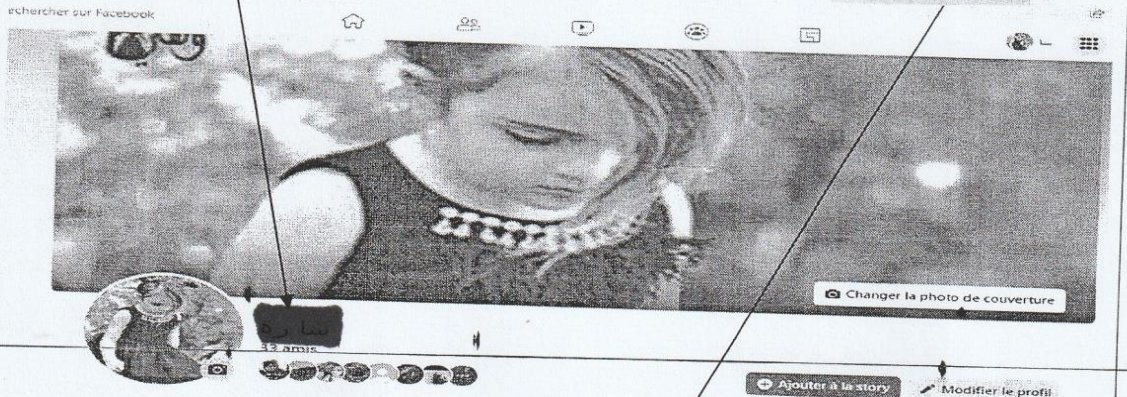

Screenshot_2022-06-13-21-00-33-810_com.facebook.lite.jpg


Screenshot_2022-06-13-20-34-48-184_com.facebook.lite.jpg

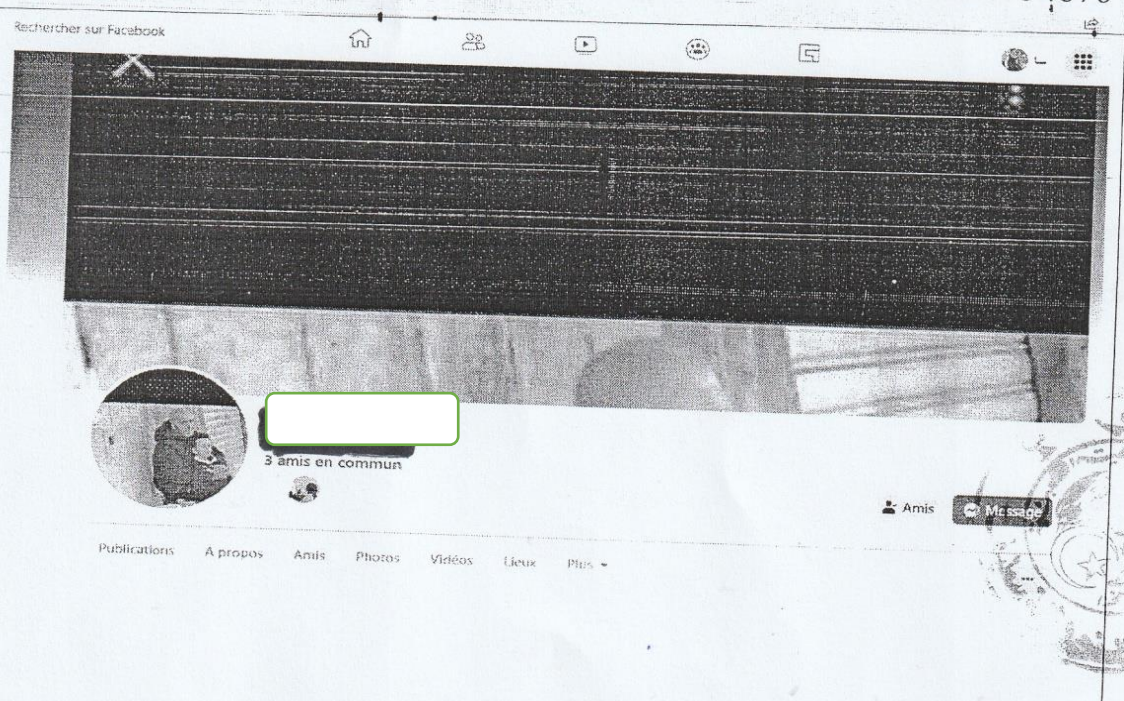

Screenshot_2022-06-13-20-34-38-243_com.facebook.lite.jpg


Screenshot_2022-06-13-20-34-30-115_com.facebook.lite.jpg

=/ المعاينة التقنية المقامة على الهاتف النقال ملك المسماة / [redacted] بينت وجود تطبيق فايسبوك مثبت مفتوح بواسطته حساب الكتروني يحمل [redacted] مرتبط بالرقم الهاتفي [redacted] كما هو مبين في الصور ادناه /----------



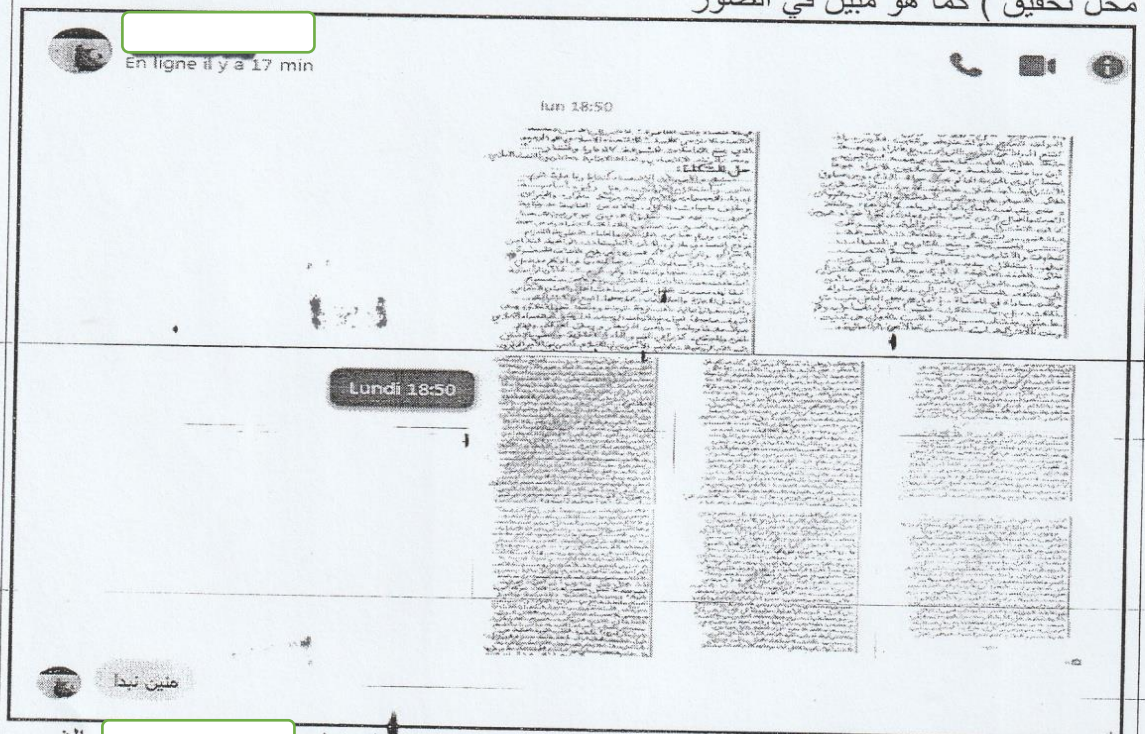
=/ من خلال المعاينة المقامة على علبة الرسائل الخاصة بالحساب السالف الذكر عاينا محادثة الكترونية مع الحساب الالكتروني الحامل لتسمية [redacted] رقم التعريفي 100064630734876 كما هو مبين في الصورة /----------



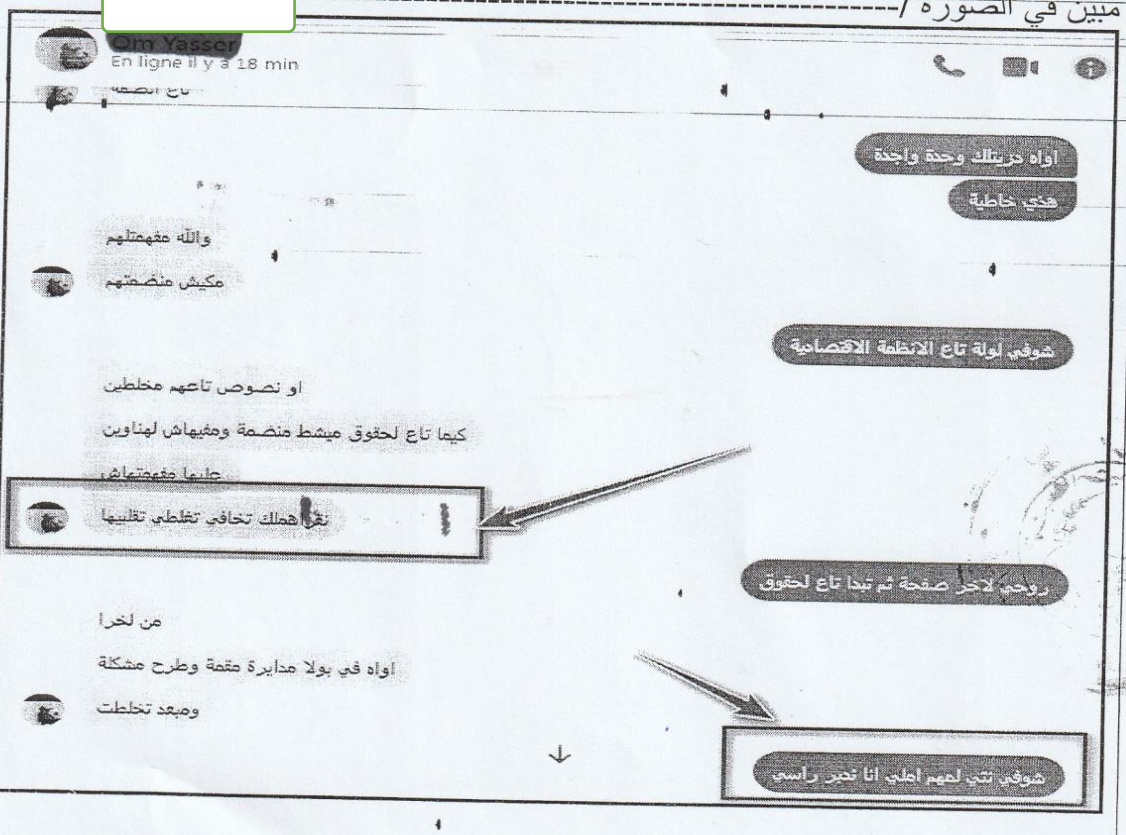
ملاحق:.....

=/ تابع لمحضر تفتيش الكتروني رقم 03

=/ المحادثة الالكترونية بين الحسابين كانت بتاريخ 2022/06/13 على الساعة 18:50 مساءا حيث بينت قيام صاحب الحساب محل تحقيق الحامل لتسمية [redacted] بإرسال لقطات شاشة لدروس و ملخصات لمادة الفلسفة (نفس الصور التي كانت مخزنة في الذاكرة الداخلية للهاتف محل تحقيق) كما هو مبين في الصور



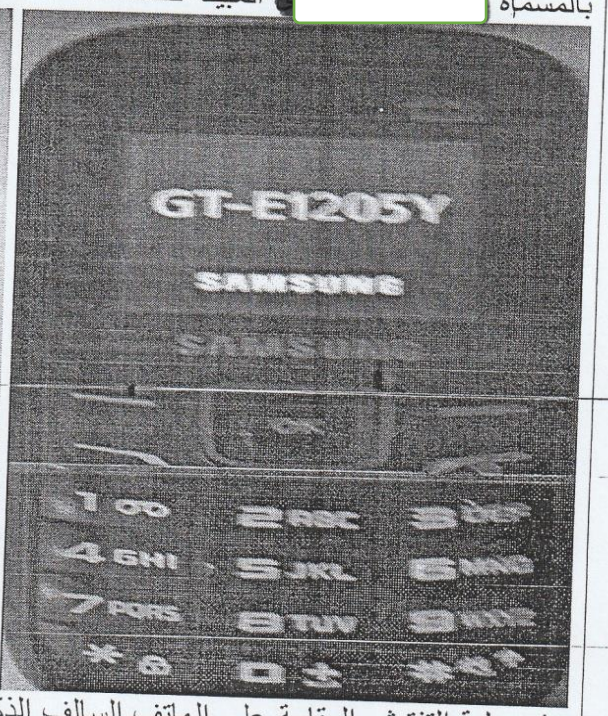
=/ نفس المحادثة بين الحسابين بينت قيام صاحب الحساب الحامل [redacted] بالشرح لصاحبة الحساب اللحامل لتسمية [redacted] حول مقالات مادة الفلسفة حيث ارسلت هذه الاخيرة رسالة جاء فيها " **نقراهملك تخافي تغلطي تقلبيها** " اين ردت عليها صاحبة الحساب محل تحقيق الحامل لتسمية [redacted] عبارة " **شوفي انتي لمهم املي وانا ندبر راسي** " كما هو مبين في الصورة /----------



ملاحق:.....

=/= تابع لمحضر تفتيش الكتروني رقم 09 =/=

02/ الهاتف النقال من نوع SAMSUNG رقم التسلسلي 352581101396771 الخاص بالمسماة [redacted] المبينة خصائصه ادناه /----------



=/ عملية التفتيش المقامة على الهاتف السالف الذكر كانت سلبية حيث لم نعاين اي شيء من شأنه افادة التحقيق /----------

=/ تم تنزيل الصور ونسخها ضمن قرص مضغوط مرفق /----------

-/ بعد الانتهاء من عملية التفتيش الإلكتروني حررنا هذا المحضر .----------

-/ إثباتا لما جاء وقعنا ووقع مساعدونا .----------

ضابط الشرطة القضائية **المساعد**

ملاحق:.....

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة العدل

س قضاء سطيف

محكمة عين ولمان

رقم:22/0322

إذن بالولـــوج والتفتـــيش

نحـــــن وكيـل الجمهوريـة لدى مجكمـــة عين ولـــمان

بعـــــد الاطلاع على المستند

الطل طرف ضابط الشرطة القضائية لامن دائرة عين ولمان

المؤرخ في :2022/06/14 رقم ://

في اطـار التحقيـق الـ الى الإذن بالولوج وتفتيش للهاتف النقال نوع

REALME رمادي اللون ملك للمسماة قمبور مريم الحامل الرقم التسلسلي

:86213505421497 به شريحة للمتعامل الاقتصادي اوريدو تحمل الرقم 0553752773

لاجل الولوج لاسترجاع اية صور او ن شانها تفيد التحقيق لاستغلاله في التحقيق

الجاري حاليا في القضية المتعلقـة جنحة تسريب اجوبة امتحانات النهائية للـ

2022

بعد الاطلاع على المادة 4،3/ج والمادة 5 من قانون 09/04 المتضمن القواعد الناصة للوقاية

من الجرائم المتصلة بتكـ ـات الاعلام والإتصال ومكافحتها.

وحـــيث انـه توجد دلائل قوية متماسكة من شانها ان تؤدي ـ مراقبة الارصدة

ة الموجودة بالهاتف النقال المستعمل من ط ، المذكـور أعلاه .

لهـــــــذه الأسبـــــاب

نـأذن ضابط الشرطة القضائية لامن دائرة عين ولمان بالولوج وتفتيش للهاتف النقال نوع

REALME رمادي اللون ملك للمسماة قمبور مريم الحامل الرقم التسلسلي

:86213505421497 به شريحة للمتعامل الاقتصادي اوريدو تحمل الرقم 0553752773

لاجل الولوج لاسترجاع اية معلومات من شانها تفيد التحقيق الـ

في القضية المتعلقـة جنحة تسريب اجـ ـت النهائية للتعليم الثانوي دورة 2022

على ان يجري التفتيش وفقا للإجراءات المنصوص عليها قانونا وتحرير محضر بذلك

حرر بعين ولمان :

وكيـــــل الجمهورية

ملاحق:.....

وزارة الداخلية و الجماعات المحلية
و التهيئة العمرانية
المديرية العامة للأمن الوطني
أمن ولاية سطيف
المصلحة الولائية للشرطة القضائية
فرقة مكافحة الجرائم المعلوماتية
رقم: /أو/أوس/م و ش ق/ف م ج م/22.

محضر تفتيش إلكتروني

نسبة ضد:

الموضوع:
محضر تفتيش الكتروني

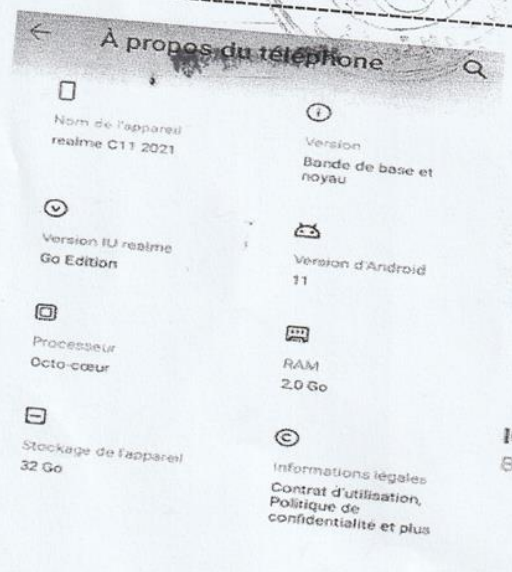
-/ إنه في يوم الثلاثاء الموافق للرابع عشر من شهر جوان .----------
-/ سنة ألفين واثنان و عشرون 2022 .----------
-/ الساعة العاشرة ليلا (22:00 سا)----------
-/ نحن رحمان عمر، ملازم أول للشرطة، بالمصلحة الولائية للشرطة القضائية، رئيس فرقة مكافحة الجريمة المعلوماتية بأمن ولاية سطيف ----------
ضابط الشرطة القضائية بدائرة الاختصاص.----------
بمساعدة عون الشرطة/ المهدي علي التابع للفرقة .----------
=/ بناءا على نص القانون رقم 04/09/ المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها /----------
-/ تنفيذا للاذن بالتفتيش الالكتروني الحامل لرقم 322/م ع/22 المؤرخ في : 2022/06/14 الصادر عن السيد وكيل الجمهورية لدى محكمة عين ولمان بخصوص قضية الحال /---------
=/ بتاريخ اليوم و الشهر و السنة المذكورين اعلاه ، قمنا بعملية الولوج باستعمال تجهيزات و ربط الانترنت الخاصة بالمصلحة من اجل القيام بعملية التفتيش الالكتروني لكل من للهاتف realmi c11 2021 رقم الإيمي: 862135054214789//862135054214797، الخاص بالمسماة /قمبور مريم من مواليد 1996/10/18 عين ولمان ابنة هاشمي و لوكية ، متزوجة و ام لطفل ، ماكثة بالبيت ، مقيمة بحي 711 مسكن عين ولمان سطيف وكذا جميع تطبيقات التواصل الاجتماعي المثبة /----------

المزود بشريحة هاتفية للمتعامل اوريدو 0553752773

ضابط الشرطة القضائية

التكييف:

=/الهاتف النقال محل تحقيق، من نوع realmi c11 2021 رقم الإيمي: 862135054214789//862135054214797، الخاص بالمسماة قمبور مريم المبين خصائصه ادناه /----------



ملاحق:.....

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

حكم

مجلس قضاء:
محكمة:
قسم الجنح

رقم الجدول: 22/02441
رقم الفهرس: 22/02279
تاريخ الحكم: 22/06/16

المثول الفوري

بالجلسة العلنية المنعقدة بمقر محكمة
بتاريخ: السادس عشر من شهر جوان سنة
النظر في قضايا الجنح
برئاسة السيد (ة): رئيسا
وبمساعدة السيد(ة): أمين ضبط
وبحضور السيد(ة): و كيل الجمهورية

النيابة ضد /

صدر الحكم الجزائي الأتي بيانه بين الأطراف التالية
السيد وكيل الجمهورية_ مدعيا باسم الحق العام.
من جهة

الطرف المدني/

1): الوكيل القضائي للخزينة العمومية غائب
الساكن : وزارة المالية عمارة احمد فرانسيس بن عكنون الجزائر

طبيعة الجرم /

جنحة تسريب مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد للمتهمة الاول +جنحة تسريب اجوبة مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد للمتهمة الثاني

ضد /

1): متهم حاضر موقوف
من مواليد:
إبن: عازب (ة)
الساكن : حي
بمساعدة الأستاذ(ة):

2): متهم حاضر موقوف
من مواليد: بـ:
إبن: متزوج (ة)
الساكن : حي 711 مسكن بلدية .
بمساعدة الأستاذ(ة):

من جهة اخرى

ملاحق:.....

بيـان وقـائع الدعـوى

حيث أن المتهمتين متابعتين من طرف نيابة محكمة
، لارتكابهما بتاريخ 2022/06/14 ومنذ زمن لم يمض عليه أمد التقادم القانوني بعد بدائرة اختصاص محكمة ، مجلس قضاء جنحة تسريب مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد للمتهمة الاولى و جنحة تسريب أجوبة مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد للمتهمة الثانية الافعال المنصوص والمعاقب عليه بنص المواد 253 مكرر 06 و 253 مكرر 07 من قانون العقوبات.
- حيث أن المتهمتين المذكورتين أعلاه أحيلا أمام قسم الجنح بموجب اجراءات المثول الفوري طبقا للمواد 339 مكرر و 339 مكرر05 و 339 مكرر06 من قانون الاجراءات الجزائية.
حيث أن وقائع القضية تتلخص في أنه بتاريخ 14/06/2022 حررت مصالح الامن الوطني بدائرة محضر تحت رقم جاء فيه أنه بالتاريخ المذكور و في اطار تأمين و مراقبة سير امتحانات شهادة البكالوريا لدورة جوان 2022بتاريخ 2022/06/14 في حدود الساعة 10:40 و على مستوى مركز الامتحان بمتوسطة الشهيد الحامل لرقم الخاص بالمترشحين الاحرار ضبطت مترشحة في محاولة الغش داخل هذا المركز خلال الفترة الصباحية خلال اجتيازها لامتحان الفلسفة و يتعلق الامر بالمسماة
و لدى سماعها صرحت انها استعملت الهاتف النقال الذي ضبط بحوزتها و حجز منها ذو المواصفات : نوع سامسونغ اللون أسود رقمه التسلسلي المزود بشريحة للمتعامل التجاري (أوريدو) تحمل رقم و سماعات الاذن في الاتصال بشقيقتها و أضافت أنها دست الهاتف النقال الاول من نوع سامسونغ داخل جيب ملابسها الداخلية أما الهاتف الثاني من نوع رادمي التي صرحت به للمراقبين التربويين و قاموا بسحبه منها عند الباب الخارجي الى غاية الانتهاء من الامتحان و بعد دخولها الى القسم و تصفحها لأسئلة مادة الفلسفة و في حدود الساعة الثامنة و النصف صباحا اتصلت بشقيقتها و لم تتمكن من سماعها لتطلب من أحد الاساتذة الحراس التوجه الى المرحاض و قبل دخولها اليه اخضعت لعملية التفتيش من قبل أحد المشرفات اين عثرت تحت طيات ثيابها على هاتف نقال من نوع سامسونغ أسود اللون رقمه التسلسلي المزود بشريحة للمتعامل التجاري (أوريدو) تحمل رقم
و سماعات أذن لاسلكية سوداء اللون كانت بصدد استعمالها للاتصال بشقيقتها لتزويدها بأجوبة مادة الفلسفة و لدى سماع شقيقتها صرحت أنه في صبيحة الوقائع تلقت اتصالا من شقيقتها و اخطرتها أنها بصدد اجتياز شهادة البكالوريا شعبة آداب و فلسفة كمترشحة حرة بأحد مراكز الامتحان بمدينة و طلبت منها تمكينها من أجوبة خاصة بمادة الفلسفة بعد اتصالها بها من داخل المركز الذي تمتحن فيه و اعطائها الاسئلة المقترحة عليها و اكدت أنها اتفقت مع شقيقتها اين تواصلت مع أختها الحامل للحساب الالكتروني عن طريق حسابها للتواصل الاجتماعي الحامل للتسمية المرتبط برقمها الهاتفي المسجل باسم و ارسلت لها مواضيعها عديدة للفلسفة المحتمل اجرائها في امتحان البكالوريا و هذا في حدود الساعة 18:30 من تاريخ 2022/06/13 و أعطتها تعليمات في كيفية املاء الدروس و أكدت لها أنها ستستعمل سماعات اذن لتلقيها و هذا كله عن طريق تقنية الماسنجر و بتاريخ الوقائع و خلال الامتحان و في حدود الساعة 08:30 اتصلت بها شقيقتها الممتحنة من هاتفها النقال على هاتفها النقال من نوع ريالمي رمادي اللون الحامل للرقم و قد أجابتها بكلمة ترحيبية فقط دون أن تسمع أي اتصال منها لينقطع هذا الاتصال و عاودت الاتصال بها لمرات عديدة لأكثر من خمس مرات على التوالي غير أنها لم ترد على اتصالاتها.
و عند قيام مصالح الامن باجراء معاينة تقنية على هاتف المسماة الهدى بينت وجود تطبيق فايسبوك مثبت مفتوح بواسطة الكتروني يحمل اسم مرتبط بالرقم
و من خلال المعاينة المقامة على علبة الرسائل السالف الذكر عاينوا محادثة الكترونية مع الحساب الالكتروني الحامل لتسمية رقم التعريفي و

رقم الجدول: 22/02441
رقم الفهرس: 22/02279

المحادثة الالكترونية بين الحسابين كانت بتاريخ 2022/06/13 على الساعة 18:30 مساء و التي بينت قيام صاحب الحساب محل التحقيق بارسال لقطات شاشة لدروس و ملخصات لمادة الفلسفة و نفس المحادثة بين الحسابين بينت قيام الحساب الحامل لتسمية بالشرح لصاحب الحساب الحامل لتسمية و نفس المحادثة و التاريخ بينت قيام صاحب الحساب الحامل لتسمية بارسال العديد من الملخصات و الدروس لصاحب الحساب الحامل لتسمية اين تشرح لها طريقة الاملاء عليها و تشرح لها الطريقة المناسبة و المعاينة المقامة على نفس المحادثة بينت قيام صاحب الحساب الحامل لتسمية تتحدث و تؤكد ضرورة استعمال السماعات و بالنسبة للهاتف النقال الثاني الخاص بالمسماة نوع سامسونغ فعملية التفتيش المقامة عليه كانت سلبية و لم يتم معاينة ما يفيد التحقيق و باستغلال كشف المكالمات بالتنسيق مع مصالح المتعامل الهاتفي أوريدو للحصول على جميع المكالمات الهاتفية التي أجريت بين المشتبه بهما و و التي بينت وجود العديد من الاتصالات كما أكدته المسماة قمبور مريم منها ثلاث اتصالات قبل بداية المتحان و خمس اتصالات خلال الامتحان

- و بتقديم المشتبه بهما و أمام السيد وكيل الجمهورية اعترفا لدى سماعهما على محضر وفقا لاجراءات المثول الفوري أين صرحت الاولى أنها تعترف بالتهمة المنسوبة اليها و المتمثلة في جنحة تسريب مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد و أكدت أنه بتاريخ الوقائع تم ضبطها من قبل الموظفين المكلفين بحراسة مركز الامتحانات بثانوية بلدية . اين تم ضبط بحوزتها هاتف نقال مزود بسماعات و أكدت انها اتفقت مع شقيقتها على تزويدها بالاجوبة الخاصة بمادة الفلسفة مسبقا و انها بعد اطلاعها على الاسئلة لا تتذكر من اتصل بالاخر و عند تبادلهما أطراف الحديث لم تسمع جيدا ما كانت تمليه عليها لتقوم بطلب الاذن للخروج الى المرحاض ليتم ضبطها من قبل الحراس و ضبط الاجهزة المستعملة بينما صرحت الثانية انها تعترف بالتهمة المنسوبة اليها و المتمثلة في جنحة تسريب أجوبة الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد و تؤكد أنها اتفقت مع شقيقتها على أن تزودها باجوبة مادة الفلسفة و انه بتاريخ الوقائع لا تتذكر من قام بالاتصال بالاخر اين قامت بتزويدها بالاجوبة (المقال) الا انها لا تعلم ان كانت تسمعها أم لا بعدها لا تعلم ان تم ضبطها أم لا و أنه فعلا المحادثات الالكترونية المكتشفة كانت بينها و بين شقيقتها أثناء الامتحان و تؤكد ذلك و قد تمت متابعتهما بالجريمة المذكورة اعلاه و جدولت القضية لجلسة 2022/06/16 ووضعت للنظر بعد حين للفصل فيها طبقا للقانون.

حيث حضرت المتهمة جلسة المحاكمة و انكرت الجرم المنسوب اليها و صرحت أنها نسيت الهاتف في جيبها.

حيث حضرت المتهمة جلسة المحاكمة و انكرت الجرم المنسوب اليها و صرحت انها لم تنقل لاختها الاجوبة.

حيث أن ممثل النيابة التمس ادانة المتهمتين بالجرم المنسوب اليهما و عقابه كل واحدة منهما بخمس سنوات حبس نافذة و 500000دج غرامة مالية نافذة مع الايداع في الحبس في الجلسة للمتهمتين.

حيث حضر دفاع المتهمتين الاستاذ نيابة عن الاستاذة جلسة المحاكمة و رافع و ذكر في مرافعته أن التسريب يتطلب أن يكون المستفيد هو الغير و ليس المنفعة الشخصية و هو ما لا يتحقق في قضية الحال و أن الهاتف الذي ضبط في حوزتها هو هاتف غير ذكي و أن المتهمتين كانتا بصدد الغش و ليس التسريب و المتهمتين يطلبان العفو مع أخذ بالاعتبار الضروف الاجتماعية لهما و التمس أساسا البراءة لانعدام ركن التسريب و في الاحتياط افادة موكلتيه بظروف التخفيف على أن تكون العقوبة موقوفة النفاذ و في الاحتياط البعيد اسعافهما بعقوبة العمل للنفع العام.

المتهم طالب جامعي متفوق في دراسته و غير مسبوق و سلوكه ممتاز و لم يكن يعلم أن ما فعله يعاقب عليه القانون و التمس اسعاف موكله بأقصى ظروف التخفيف على أن تكون العقوبة موقوفة النفاذ مع استرداد المحجوز.

حيث حضرت دفاع المتهمتين الاستاذة جلسة المحاكمة و رافعت و ذكرت في مرافعتها أن المتهمة الاولى هي التي كانت تتلقى الاتصالات و بالتالي لا يوجد تسريب و لا يوجد ما يفيد أن هذه الاتصالات كانت بغرض التسريب و المكالمات كانت خارج أوقات الامتحان و الوقائع لا تنطبق مع النصوص القانونية المتابعين بهما و تلتمس نضر المحكمة الى المتهمتين بعين الرحمة و التمست اساسا البراءة و احتياطيا اسعافهما بأقصى ظروف التخفيف فالمتهمة الاولى طالبة و تعيل والديها و الثانية متزوجة و أم لطفل عمره ثلاث سنوات.
حيث أن الكلمة الأخيرة كانت للمتهمتين اللتين التمستا العفو.
و بعد اقفال باب المرافعة وضعت القضية في النظر بعد حين للفصل فيها طبقا للقانون.

وعليــه فإن المحكـمة

بعد الاطلاع على أوراق الدعوى.
بعد الاطلاع على أحكام المواد من 328 إلى 380 من قانون الإجراءات الجزائية.
بعد الاطلاع على أحكام المادتين 253 مكرر 06 و253 مكرر 07من قانون العقوبات.
بعد الاستماع الى كل طرف بالكيفية المنصوص عليها قانونا
بعد الاستماع الى ممثل النيابة في طلباته.
بعد الاستماع الى دفاع المتهمين في مرافعتهما
بعد الاستماع الى المتهمين في كلمتهما الاخيرة.
بعد النظر في القضية وفقا للقانون.
في الدعوى العمومية :
حيث تبين لهئة المحكمة من خلال دراستها لملف الدعوى ، و المناقشات التي دارت بالجلسة، أن جنحة تسريب مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد المنسوبة للمتهمة و جنحة تسريب أجوبة مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد المنسوبة للمتهمة ثابتة في حقهما الافعال المنصوص و المعاقب عليها طبقا لنص المواد 253 مكرر 06 و 253 مكرر 07 من قانون العقوبات و ذلك بالنظر الى ما يلي :
1 ـ اعتراف المتهمتين عند سماعهما أمام الضبطية القضائية ثم أمام السيد وكيل الجمهورية بالجرم المنسوب اليهما و ما انكارهما أمام هيئة المحكمة الا محاولة منهما للتهرب من المسؤولية الجزائية ، خاصة و أنهما أكدتا أنهما أجريتا مكالمات هاتفية خلال فترة امتحان مادة الفلسفة كم أن المتهمة ضبط في حوزتها هاتف نقال و سماعات أذن .
2 ـ محضر الضبطية القضائية المذكور أعلاه الذي جاء فيه أن كشف المكالمات للمتعامل الهاتفي أوريدو يبين أن هناك 08 مكالمات الهاتفية أجريت بين المتهمتين و
بتاريخ الوقائع 03 منها قبل بداية امتحان البكالوريا (الامتحانات النهائية التعليم الثانوي) بينما 05 منهاخلال فترة الامتحانات و هو ما أكدته المتهمتين عند سماعهما أمام الضبطية القضائية ثم أمام السيد وكيل الجمهورية.
3 ـ معاينة تقنية على هاتف المسماة بينت وجود تطبيق فايسبوك مثبت مفتوح بواسطة الكتروني يحمل اسم مرتبط بالرقم و من خلال المعاينة المقامة على علبة الرسائل السالف الذكر عاينوا محادثة الكترونية مع الحساب الالكتروني الحامل لتسمية رقم التعريفي و المحادثة الالكترونية بين الحسابين كانت بتاريخ 2022/06/13 بينت قيام صاحب الحساب الحامل لتسمية بارسال العديد من الملخصات و الدروس لصاحب الحساب الحامل لتسمية اين تشرح لها طريقة الاملاء عليها و تشرح لها الطريقة المناسبة و المعاينة المقامة على نفس المحادثة بينت قيام صاحب الحساب الحامل لتسمية تتحدث و تؤكد ضرورة استعمال السماعات
حيث و الأمر كذلك و استنادا الى ما سبق بيانه أعلاه يتبين ان جنحة تسريب مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد المنسوبة للمتهمة و جنحة تسريب أجوبة مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد المنسوبة للمتهمة قائمة بركنيها المادي و المعنوي في حقهما و عليه فانه يتعين

رقم الجدول: 22/02441
رقم الفهرس: 22/02279

فهرس المحتويات

فهرس المحتويات:

العنوان	الصفحة
شكر وعرفان	
إهداء	
مقدمة	**01**
الفصل الأول: ماهية الجرائم الالكترونية	**06**
المبحث الأول: مفهوم الجريمة الالكترونية	**06**
المطلب الأول: تعريف الجريمة الالكترونية	**07**
الفرع الأول: التعريف اللغوي للجريمة الالكترونية	**07**
الفرع الثاني: التعريف الاصطلاحي للجريمة الالكترونية	**07**
الفرع الثالث : التعريف الفقه للجريمة الالكترونية	**08**
المطلب الثاني: خصائص الجريمة الالكترونية	**11**
أولا: وقوع الجريمة في بيئة المعالجة الآلية للبيانات وللمعلومات	**12**
ثانيا: الصبغة العلمية العالمية للجريمة المعلوماتية	**13**
ثالثا: الجريمة المعلوماتية أقل عنفا وجهدا في التنفيذ	**14**
رابعا: صعوبة اكتشاف الجريمة المعلوماتية	**14**
خامسا: صعوبة التحقيق والتحري في نطاق الجريمة الالكترونية	**15**
المطلب الثالث: صور الجرائم الالكترونية ومرتكبيها	**15**
الفرع الأول: الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي	**17**
الفرع الثاني: الجرائم الالكترونية الواقعة على النظام المعلوماتي	**24**
الفرع الثالث: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي	**25**
المبحث الثاني: إجراءات البحث والتحري في الجرائم المعلوماتية	**26**
المطلب الأول: الأجهزة المكلفة بالتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية	**27**
المطلب الثاني: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة	**28**

فهرس المحتويات:.....

الاتصال والمعلوماتية	**29**
الفرع الأول: جهاز الضبطية القضائية	**29**
الفرع الثاني: دور مقدمي الخدمات في التحري والتحقيق في الجرائم الماسة بأنظمة الاتصال والمعلوماتية	**30**
المطلب الثالث: الوسائل المستخدمة في التحري وجمع الأدلة ومعوقاتها	**30**
الفرع الأول: الوسائل المادية	**32**
الفرع الثاني: الوسائل الإجرائية	**32**
الفرع الثالث: صعوبات ومعوقات جمع الأدلة	**32**
الفصل الثاني: التفتيش في البيئة الالكترونية	**35**
المبحث الأول: ماهية التفتيش في البيئة الالكترونية	**35**
المطلب الأول: تعريف التفتيش التقليدي	**36**
الفرع الأول: رأي الفقه حول مصطلح التفتيش في البيئة الالكترونية	**36**
الفرع الثاني: مصطلح التفتيش في البيئة الالكترونية في التشريعات	**37**
المطلب الثاني: خصائص التفتيش الالكتروني	**39**
المطلب الثالث: الطبيعة القانونية للتفتيش	**40**
الفرع الأول: الضوابط الموضوعية لتفتيش نظم الحاسوب	**41**
الفرع الثاني: الضوابط الشكلية لتفتيش نظم الحاسوب	**47**
المبحث الثاني: الإجراءات التحضيرية والفنية للتفتيش في الجرائم الالكترونية	**51**
المطلب الأول: الإجراءات التحضيرية للتفتيش في الجرائم الإلكترونية	**51**
الفرع الأول: تحديد محل التفتيش في الجرائم الإلكترونية	**52**
الفرع الثاني: آلية التفتيش في الجرائم الإلكترونية	**55**
المطلب الثاني: الإجراءات الفنية للتفتيش في الجرائم الإلكترونية	**58**
الفرع الأول: تفتيش مكونات وسائل تكنولوجيا المعلومات	**58**
الفرع الثاني: تحديات إجراءات تفتيش وسائل تكنولوجيا المعلومات	**62**
المطلب الثالث: آثار التفتيش في الجرائم المعلوماتية	**66**

فهرس المحتويات:.....

الفرع الأول: حجز المعطيات المعلوماتية	**66**
الفرع الثاني: منع الوصول إلى المعطيات المعلوماتية	**69**
المطلب الرابع: أثر عدم مشروعية إجراءات التفتيش	**69**
الفرع الأول: أسباب بطلان التفتيش	**69**
الفرع الثاني: آثار الحكم بالبطلان	**71**
الخاتمة .	**74**
قائمة المصادر والمراجع	**78**
الملاحق : إذن بالتفتيش والولوج الإلكتروني	**86**
محضر تفتيش الكتروني	**87**
إذن بالولوج والتفتيش	**92**
حكم قضائي	**93**
فهرس المحتويات	
الملخص	

فهرس المحتويات:.....

الملخص

ملخص البحث

إن التطور الهائل في مجال تكنولوجيا المعلومات جعل الإنسان يعتمد عليها في حياته لحفظ أسراره وخصوصياته، إلا أن البعض أساء استخدام هذه التكنولوجيا في الاعتداء على المجتمع وتهديد أمنه، أين ظهر نوع جديد من الجرائم وهي الجرائم الإلكترونية.

وللكشف عن الجرائم الإلكترونية عن طريق البحث والتحري باتخاذ التفتيش كأحد الإجراءات المتبعة للوصول إلى الدليل فإنه بحاجة إلى سلطة مختصة وتقنيات لاستخراج الأدلة الإلكترونية وضبطها وحفظها من التدمير.

كما يحتاج أيضا التفتيش باعتباره إجراء صعب إلى فريق فني متخصص له دراية ومعرفة علمية قد لا تتوفر لدى رجال الشرطة والمحققين، مع ضرورة مراعاة الضمانات المقررة للتفتيش التي أقرها القانون والاتفاقيات الدولية إلا اتسم الدليل الناتج عن التفتيش بعدم المشروعية.

كون الجريمة المعلوماتية جريمة حديثة النشأة لا يكفي تطبيق الإجراءات المتبعة على الجرائم التقليدية، و عليه فالهدف من دراسة هذا الموضوع هو معرفة الإجراءات المعمول بها في تفتيش الانظمة المعلوماتية من شروط وكيفية ضبط وحجز المعطيات المتحصل عليها.

Résumé:

Le domaine des technologies de l'information connait une évolution considérable, rendant l'humain complétement dépendant d'elle dans tous les aspects de sa vie personnelle. Mais le mauvais usage de cette technologie menace désormais la stabilité et la sécurité de la société, ce qui a donné naissance à un nouveau genre de crime: La cybercriminalité.

Elucider les cybercrimes par l'investigation et la vérification comme un moyen d'apporter des preuves, requiert une autorité spécialisée et compétente et des techniques pour tirer les preuves électroniques et surtout les préserver de la destruction.

L'investigation dans la cybercriminalité est une procédure qui demande une équipe hautement qualifiée et spécialisée en connaissances scientifiques, dont ne disposent pas les agents de police et les enquêteurs.

Elle requiert d'autre part le respect de toutes les garanties de recherche et d'investigationédictées par la loi et les conventions internationales, sous peine de d'illégalité des preuves.

De ce fait, il ne suffit plus de suivre les procédures d'investigation classiques dans ce genre de crimes nouveaux, mais recourir également à d'autres conditi **الملخص**
systèmes informatiques.

Abstract :

The field of information technologies is undergoing a considerable evolution, making the human completely dependent on it in all aspects of his personal life. But the misuse of this technology threatens the stability and security of society, which has given rise to a new kind of crime: cybercrime.

To elucidate cybercrimes through investigation and verification as a means of providing evidence, requires a specialized and competent authority and techniques to draw electronic evidence and preserve it from destruction.

Investigating in cybercrime is a procedure that requires a highly qualified team specialized in scientific knowledge, which police officers and investigators do not have.

It also requires compliance with all the guarantees of research and investigation laid down by law and international conventions, under penalty of illegality of evidence.

As a result, it is no longer enough to follow traditional investigative procedures in this type of new crime, but also to resort to other search conditions in computer systems.