وزارة التعليـم العـــالـي و البحـث العلمـــي
المـــركز الجـامعـي علـي كـافـي – تندوف –
معهد الحقوق و العلوم السياسية
قسم الحقوق

# "طرق إثبات الجرائم الإلكترونية"

**مـــذكـــرة تخـــرج لنيـــل شهـادة المـــاستـر فـــي الحقـــوق**
**تخـصـص قـــانـون عـــام**

من إعداد الطلبة :
الطالب: زايدة محمد
الطالب(ة): سعدي فاطمة الزهرة

بإشراف الدكتور:
**" سعدي هارون "**

**لجنة المناقشة**

أ/- جيد محمد ، أستاذ مساعدا، "أ" المركز الجامعي علي كافي تندوف.....رئيسا

أ/- د/سعدي هارون ، أستاذ محاضر"ب" المركز الجامعي علي كافي تندوف....مشرف مقررا

أ/- أعراب سعيدة ، أستاذ مساعد "أ" المركز الجامعي علي كافي تندوف.....ممتحنا

**تاريخ المناقشة: 2022/05/29**

# شكر وتقدير

أتقدم بأخلص عبارات الشكر إلى أبي الغالي وأستاذي في نفس الوقت والذي أشرف بدوره على مذكرة تخرجنا مما زادها مكانة علمية وقيمة عاطفية بالنسبة لي.

وأخص بالشكر أمي الحبيبة وأعضاء اللجنة الموقرة على ملاحظاتهم القيمة

وأسأل الله عز وجل أن يبلغكم أسمى مراتب الدنيا وأعلى منازل الآخرة.

الطالبة / سعدي فاطمة الزهرة

# شكر وتقدير

إن الحمد و الشكر كله لله الذي وفقنا و أعاننا على إنجاز هذا العمل المتواضع.

أتقدم بخالص الشكر و التقدير و الإمتنان إلى :

الأستاذ المشرف الدكتور / سعدي هارون

على إرشاداته و نصائحه القيمة لإنجاز مذكرة التخرج و تقديم العون لنا طوال مدة الدراسة ، و الذي أفادنا و كان لنا السند و لم يبخل علينا بتقديم كل المساعدة اللازمة في إنجاز هذا العمل لنيل شهادة الماستر.

كما اتقدم بالشكر إلى كل أساتذتنا في مرحلة الدراسة بمعهد الحقوق و العلوم السياسية بالمركز الجامعي علي كافي بتنـدوف ، و كل من قدم لنا يد العون سواءا من قريب ام من بعيـد .

الطالب / زايدة محمـد

# الإهداء

أهدي هذا العمل إلى من بسمتها غايتي و تحت أقدامها جنتي

إلى من ساندتني بدعائها و من أعانتني في بحوثي

طيلة المشوار الجامعي من علمتني القراءة والكتابة لأول مرة في حياتي،

إلى نور عيني وقلبي أمي الغالية **"همال فيروز"**

إلى من علمني الحياة وأن الدنيا كفاح وسلاحها العلم والمعرفة

إلى الذي لم يبخل علي بأي شيء لمن سعى لأجل راحتي ونجاحي أبي العظيم وأستاذي المشرف القدير **"سعدي هارون"**

إلى من دعمني طيلة حياتي وكان سندا حقيقيا لي إلى خالي الغالي **"همال أمين"**

وإلى أصحاب الفضل الحقيقي أجدادي **"همال الحاج"** و المرحوم **"سعدي بشير"**

إلى أميرتي الصغيرة **"صالح بسمة"** وخلاتي وأعمامي الأعزاء **"سعدي رياض"**

و**"العربي شريف مصطفى"**

إلى كل طالب علم يسعى لكسب المعرفة وتزويد رصيده المعرفي العلمي والثقافي.

**زهرة**

# الإهـداء

إلى التي لا يمكن للكلمات أن توفي حقها

وإلى التي لا يمكن للأرقام أن تحصي فضائلها

الأم التي ربتني وأنارت دربي وأعانتني بالصلوات والدعوات.

وإلى أبي العزيز الذي عمل بكد في سبيلي وعلمني الكفاح وأوصلني إلى ما أنا عليه،

إلى أغلى شخصين في هذا الوجود "أمي وأبي" الحبيبين حفظهما الله ورعاهما.

إلى كل من لا تكفيني كل معاني الحب أهديه لها "زوجتي الغالية"

إلى حبيبي ونبر السعادة "المشاغب والمشاكس" ابني العزيز.

إلى إخواني وأخواتي

إلى كل العائلة والأصدقاء والأحباء والزملاء والزميلات ورفقاء الدرب في هذه الحياة.

إلى كل من ساهم في تدريسنا لمدة عامين من قريب أو من بعيد

إلى جميع طلبة معهد الحقوق بالمركز الجامعي تندوف

مع أمنياتنا لهم النجاح والتوفيق والسداد في حياتهم المهنية.

**محمد**

بسم الله الرحمن الرحيم

ق.ا.ج.ج : قانون الاجراءات الجزائية الجزائري .
ق.ا.ج: قانون الاجراءات الجزائية .
ت.ا و ا : تكنولوجيا الاعلام و الاتصال .
ج.ر : الجريدة الرسمية .
ط : الطبعة .
ص : الصفحة .

FBI : Federal Bureau of Investigation .
IP : Internet Protocol .
IDS : Intrusion Detection System .
A.E.C : Attestation d' Etudes Collegiales.
P : page .

# المقـــدمـــة

منذ سنة 1829 كان الفقيه دوما قد عرف الدليل بأنه " **كل ما يقنع العقل بحقيقة ما .....، نسمي " أدلة في منظور قضائي تلك الطرق التي تضبطها القوانين من اجل الكشف و إظهار الحقيقة حول وقائع محل نزاع"** [1]، و لعله من ابرز الصيغ التي أحيط بها مفهوم الدليل لرفع اللبس عن التصور الشائع و المدلول القانوني له، فإذا كانت **"الحقيقة"** هي ما ينشده كل باحث عن العدالة و الإنصاف، يجب التنبيه إلى أن الحقيقة القضائية ليست دوما بذلك الشكل البسيط الذي ينصرف لما جرى و وقع "فعلا" من أحداث، فالقضاء يسعى طبعا لإظهار الحقائق، لكن العناصر كاحترام الحقوق الأساسية كالحق في الخصوصية و بعض الحقوق و الحريات الأخرى و يلزم خضوع عملية البحث عن الدليل إلى شروط إجرائية شكلية تحدد كل من الجهة التي يخول لها البحث عن الدليل، موضوع الدليل، الإجراءات التي تخضع لها عملية جمع الأدلة و مدى قبولها و حجيتها القانونية ( النطاق الشخصي، الموضوعي، الشكلي و الأثر القانوني) و هذا حسب كل مجال طبعا، فالإثبات الجنائي يختلف عنه في المجالين المدني و الإداري .

نظرا لانتشار الجرائم ذات الطبيعة الالكترونية و فعالية الدليل الالكتروني في الإثبات أو النفي في الجرائم الكلاسيكية ( الجرائم العادية أي غير الالكترونية ) و إضافة للطبيعة الخاصة له ( الإثبات الالكتروني ) أدى ذلك لسهولة تبني التشريعات الجنائية لهذا النوع من أنظمة الإثبات خاصة في النظام التنقيبي الذي يتبنى مبدأ حرية الإثبات ولا يقيد الأطراف كثيرا في الاستعانة بكل وسيلة تقنع القاضي بمزاعمهم ( موقفهم )، لكن في ذات الحين فان الطبيعة "غير المادية" لهذا النوع من الأدلة يطرح إشكالات ، فالأخذ به يتطلب كفاءة فنية تامة في مجال المعلوماتية و التي إن توفرت لدى الخبير الذي يستعين به القضاء، فهي غير متوفرة حتما لدى القاضي ( بحكم تخصصه و تكوينه) الذي يبقى المسؤول الفعلي ابتداء و نهاية عن حكم الإدانة أو البراءة ( الإحالة أو ألا وجه للمتابعة بالنسبة لقاضي التحقيق ) ، كما أن اكبر إشكال قانوني يطرحه هذا المنهج في الثبات الجنائي ( الإثبات الالكتروني ) هو مدى توفيق المشرع و الممارسة القضائية في مراعاة أهم أمرين في معادلة المحاكمة الجنائية و هما "التصدي للجرائم و محاربة الإفلات من العقاب" لردع الجريمة و توفير السكينة العامة للمجتمع من جهة و " احترام حق المتهم في الخصوصية و عدم إفشاء أسرار اتصالاته الشخصية " كضمانة لتمتع المواطنين بحرمة حقوقهم ومن ثمة حماية المجتمع من جهة ثانية .

يبرز دور الدليل الالكتروني في كونه الوسيلة المثلى بل الوحيدة التي يستدل بها بشان الجريمة الالكترونية التي استفحلت كافة عابرة لحدود الوطن الواحد بحكم تسهيل المعلوماتية لتجاوز الحدود الجغرافية، علاوة على طبيعة الدليل الالكتروني العلمية التي تكسبه حجية عالية الحظوظ لإقناع القاضي الجزائي حتى في إثبات أو نفي الجرائم غير الالكترونية باعتباره دليل يترك لنا إمكانية التتبع و التحقق من خلال الخبرة العلمية ، فهو دليل علمي بامتياز .

يحيط المشرع الدليل الجنائي بجملة من الضمانات القانونية لتمكين القضاء من أداء عمله الرامي لردع الجريمة و احترام الحقوق للمشتبه فيهم و تجنب التعسف في حقهم، لذا يشترط ضوابط لقبول الدليل بصفة عامة و وسيلة الإثبات الالكتروني على وجه خاص باعتبارها أمر محدث و جديد في الإثبات الجزائي .

---

[1] compagnie nationale des experts de justice en informatique et techniques associées , la preuve numérique à l'épreuve du litige , colloque organisé par la première chambre de la cour d'Appel de Paris le 13/04/2010 ,p.9. disponible sur : https://www.lagbd.org/images/3/3a/Colloque_CNEJITA_13_Avril_2010.pd

***الإشكالية** ما هي الجرائم التي تثبت فيها التهم أو تنفى استنادا للدليل الالكتروني ؟ كيف يتم الحصول على الإثبات الكترونيا ؟ و كيف يبني القاضي الجزائي قناعته على أساس تقديره للدليل الالكتروني ؟

**صعوبات البحث :**

1/ صعوبات عامة : نقص كبير في المراجع ذات الصلة بالموضوع على مستوى مكتبة المركز الجامعي ، قصر المدة الممنوحة لاعداد المذكرة إعدادا جيدا .

2/ صعوبات خاصة : خلط في المفاهيم لدى بعض المؤلفين ( المراجع المعتمدة ) خاصة بين مفهومي الجريمة الالكترونية و الجريمة السبرانية و عدم التمييز بينهما بدقة ، رغم وفرة المراجع على الانترنت ( مراجع أكاديمية )، إلا أن الكثير منها يميزه الحشو و الإطناب و الابتعاد عن الدقة التي تتطلبها الدراسات القانونية، خوض بعض المؤلفين في الجوانب التقنية البحتة للمعلوماتية رغم الصفة القانونية للدراسة أو البحث ( عناوين قانونية ).

**أهداف الدراسة** سنتطرق لأهداف الدراسة الخاصة بنا ( الطالبان) و من الناحية الموضوعية طبعا لان الهدف الرئيسي و الخاص بإدارة المركز الجامعي هو " اختبار قدرة الطلبة على إعداد مذكرة لمنحهم الشهادة " و هذه غاية عامة تخص كل الطلبة.

* شرح الجرائم التي يستدل على الحقيقة فيها باستعمال الإثبات الالكتروني

*توضيح مراحل و إجراءات تجميع الأدلة الالكترونية .

* تبيان حجية الدليل الالكتروني و مدى مقبوليته في النظامين الجزائيين و خاصة أمام القضاء الجزائري .

* التأكيد على أهمية القانون في استغلال الدليل الالكتروني كدليل علمي لردع الجريمة من جهة و ضرورة احترام الحقوق الفردية خاصة الحق في خصوصية المراسلات و الاتصالات .

**المناهج المستعملة خلال الدراسة :**

لاستعراض المعلومات الضرورية لتقديم بحث أكاديمي قانوني نستعين بمناهج عدة، فقد اعتمدنا على المنهج الوصفي و الإحصائي لدى تقديمنا للأجهزة القائمة على جمع الأدلة الالكترونية و شرح هياكلها و مهامها، و لا مناص من اللجوء للمنهج التحليلي الضروري لكل دراسة قانونية جادة ، بحيث لجانا إلى تحليل النصوص القانونية و بعض الوثائق المعتمد عليها في الدراسة لاستخلاص الأفكار التي بنيت عليها الدراسة، و أخيرا لجانا للمنهج الجدلي بطريقة ضمنية لا ظاهرية ( ليس لدينا في العنونة أطروحة و نقيضها و التركيب بينهما) من خلال المقابلة بين النظام التنقيبي و النظام الاتهامي و الأخذ بما يعادل التركيب بينهما (نظام هجين).

*** الدراسات السابقة :** نذكر بعض المراجع التي إعتمدنا عليها في دراستنا منها :

**01/-** فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر(1) ، 2010- 2011

**02/-** وفاء عمران، تعامل القاضي الجزائي مع الدليل العلمي –دراسة مقارنة -، أطروحة دكتوراه، تخصص قانون العقوبات و العلوم الجنائية، جامعة قسنطينة 1، الموسم الجامعي 2019/2018.

**03/-** طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة ماجستير، تخصص قانون جنائي، كلية الحقوق، جامعة الجزائر 01، الموسم الجامعي 2012/2011.

**04/-** بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق، جامعة وهران، 2013.

05/- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي "دراسة مقارنة" ، رسالة ماجستير ، كلية الحقوق ، جامعة الإسكندرية ، 2009 .

و لمعالجة الإشكالية المطروحة أعلاه ، إرتاينا وضع الخطة التالية، اين تم تقسيم الخطة كالآتي :

**مقـــــدمـــــــة**

**الفصل الأول : المـــتابعـــة الجـــزائيـــة للجـــرائـــم الإلكتـــرونيـــة.**

**المبحث الأول: مفهـــوم الجريمـــة الإلكتـــرونيـــة.**

**المطلب الأول: مفهـــوم الجريمـــة الإلكتـــرونيـــة .**

**المطلب الثاني: صـــــور الجـــرائـــم الإلكتـــرونيـــة.**

**المبحث الثاني: طرق إثبات الجرائم الإلكترونية .**

**المطلب الأول: المعاينـــة و التفتيـــش و الشهود فـــي الجريمـــة الإلكتـــرونيـــة.**

**المطلب الثاني: الضبـــط و الخبـــرة القضائية و التسرب و التنصت و اعتراض المراسلات في الجريمـــة الإلكتـــرونيـــة.**

**الفصل الثاني : حجيـة الـدليـل الإلكتـرونـي أمام القضاء الجزائي.**

**المبحث الأول: الدليل الإلكتروني في النظام الاتهامي و النظام التنقيبي .**

**المطلب الأول: الدليل الالكتروني في النظام الاتهامي(الانجلوسكسوني).**

**المطلب الثاني: الدليل الالكتروني في النظام التنقيبي .**

**المبحث الثاني: الدليل الالكتروني في النظام القانوني الجزائري.**

**المطلب الأول: الأدوات التنفيذية و التشريعية للدليل الالكتروني في الجزائر .**

**المطلب الثاني: الدليل الالكتروني في تقدير القضاء الجزائي الجزائري.**

**الخاتمـــــــــــــــــــة.**

# الفصل الأول :

# المتابعة الجزائية للجرائم الإلكترونيــة

عصر الانترنت او عصر السموات المفتوحة أو عصر التكنولوجيا الرقمية أو المعلوماتية كل هذه الأوصاف تعبر عن مدى ضخامة القفزات العملية الهائلة التي تحققت و مدى تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة ، إلا أن هذا الوجه المشرق لتقنية المعلومات اخل في جانبه المظلم وولد معه عالم رهيب من الإجرام المعلوماتي أستغل لتحقيق مصالح و مآرب تتنوع و تتعدد .

تختلف الجريمة الإلكترونية عن التقليدية في أمور عدة، منها حداثتها وظهورها بظهور التكنولوجيا الرقمية واعتمادها على كيانات معنوية- موجات كهرومغناطيسية -في اقترافها، كما يتميز المجرم المعلوماتي عن التقليدي في كونه يتمتع بالذكاء واعتماده على الجانب الفكري في اقتراف الجريمة ، خلافا للمجرم التقليدي الذي يعتمد في ارتكاب أغلب جرائمه على القوة العضلية، إضافة إلى الإلمام بالجوانب التقنية والفنية، وأكثر من ذلك التخصص في بعض الجرائم الهامة التي لا يقترفها إلا فنيون ومتخصصون في مجال علوم الحاسوب والشبكات والبرامج ، لذلك نجد لدى المجرم المعلوماتي قدرة على إخفاء جريمته والتلاعب بالأدلة ، لذا يجب على السلطات القضائية أن تتعامل مع هذه الجرائم بما يتناسب معها من أدلة إلكترونية [1].

وتهدف إجراءات التحقيق في هذه الجرائم إلى جمع وفحص الأدلة الإلكترونية القائمة على وقوع الجريمة ونسبتها إلى فاعلها، ومن أهم هذه الإجراءات كما بينها القانون هي المعاينة ، التفتيش، الخبرة القضائية، الضبط، سماع الشهود، مراقبة المحادثات وتسجيلها، الاستجواب، المواجهة والاعتراف، إلا أن بعض هذه الإجراءات لها دور ضئيل في بيئة تكنولوجيا المعلومات، فالشهادة مثلا تقريبا لا يمكن تصور ورودها على السلوك المكون للجريمة الإلكترونية ، كون هذه الأخيرة تقتضي التلاعب في البيانات والبرامج فهي غير قابلة من حيث المبدأ لأن تشاهد من جانب الغير حتى يمكن أن يشهد به أمام القضاء شهادة مباشرة، وكما أن الاعتراف الذي يتم عن طريق الاستجواب أو السؤال أو طواعية لا يعد قضائيا كافيا ما لم يدعم بأدلة أخرى غيرها، وبالتالي سوف نقتصر الذكر على ما يصلح منها كأدلة إثبات في الجرائم الإلكترونية.
وهذا ما سوف نتناوله من خلال مبحثين على النحو التالي :الجريمة الإلكترونية (المبحث الأول)، إجراءات متابعة الجريمة الإلكترونية (المبحث الثاني) .

## المبحث الأول: الجريمة الإلكترونية .

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة نظر لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، وباعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية بخصوص تحديد ماهيتها والأفعال الإجرامية التي تدخل في نطاقها أين أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية

[1] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر(1) ، 2010- 2011 ، ص 373 .

للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عددت آراء فقهية في محالة فهم المقصود بالجريمة الإلكترونية. وقد تبنى المشرع الجزائري للدلالة على الجريمة الإلكترونية، مصطلح المساس بالأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحقيقه. ولذلك فالمشرع الجزائري لم يعرف نظام المعالجة فأوكل مهمة تعريفه لكل من الفقه والقضاء ، ولذلك ارتأينا التعرض لماهية الجريمة الإلكترونية(مفهومها و خصائصها ) في المطلب الأول و صور الجريمة الإلكترونية في المطلب الثاني :

## المطلب الأول: مفهـــــوم الجريمة الإلكتـــرونيـــة .

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

### الفرع الأول : تعريف الجريمة الإلكترونيــة

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

**أولا: تعريف الجريمة الإلكترونيــة فقها :**

إذ تعرف في نطاق فقهاء القانون بأنها سلوك يجرمه القانون و يرد عليه بعقوبة جزائية أو تدبير احترازي[2].

-ويوسع البعض مفهوم الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط بأي وجه بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب.

-كما وسع الخبير الأمريكي (Parker ) في تعريفها بأنها " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الجاني"[3].

**ثانيا: تعريف الجريمة الإلكترونيــة قانونا :**

و قد عرفته المذكرة التفسيرية في **اتفاقية بودابست** في القسم الأول منها في العنوان الأول ما يلي ذلك العنوان من المواد 2-4 و هي التي يستخدم الحاسب الآلي بها كأداة اعتداء و ليس محلا للاعتداء بذاته ، و هي جرائم الغش المعلوماتي و جرائم المحتوى و أعنى بها الجرائم

---

[1] خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية، الإسكندرية، 2008 ، ص41 .

[2] عمر محي الدين حوري،الجريمة" اسبابها -مكافحتها "دراسة مقارنة في الشريعة و القانون و العلوم الاجتماعية ،المطبعة العلمية دمشق الطبعة01 2003 ص 70

[3] محمد أمنية الشوايكة جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009ص 8

التي تستهدف شريحة معينة من الأشخاص كعرض المواد الإباحية و المواد المتعلقة بالسلوك ، مختتما بالجرائم التعدي على الملكية الفكرية و هي جرائم التعرض على المصنفات الموجودة على الانترنت [1].

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والاتصال بموجب المادة 02 من القانون 09-04 فإنه يعرفها بأنها : «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكتروني. [2]»

ويلاحظ على هذا التعريف ما يلي:

أن المشرع قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار موضوع أو محل الجريمة المساس بأنظمة المعالجة الآلية للمعطيات كأساس لتحديد الجريمة المعلوماتية ، و هي الجرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات " ، و التي تحكمها المواد من 394 مكرر إلى 394 مكرر 7 من هذا القانون، وثانيها معيار وسيلة ارتكاب الجريمة لتحديد الجريمة المعلوماتية وهو وسيلة ارتكاب الجريمة و هي المنظومة المعلوماتية أو نظام الاتصالات الالكترونية ، وثالثا معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات [3].

و هنا يمكن القول **أن الجريمة المعلوماتية حسب المشرع الجزائري تنقسم إلى طائفتين** : تضم الطائفة الأولى الجرائم التي ترتكب ضد نظام المعالجة الآلية للمعطيات و تستهدف المساس الكلي أو الجزئي بهذه المنظومة ، و هي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات تحت عنوان :"المساس بأنظمة المعالجة الآلية للمعطيات "[2].

فيما تتضمن الطائفة الثانية كل الجرائم الأخرى المنصوص عليها في قانون العقوبات أو في القوانين الخاصة التي يتم ارتكابها أو يتم تسهيل ارتكابها باستخدام منظومة معلوماتية أو أي نظام للاتصالات [2].

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

وبهذا فقد وفق المشرع برأيينا في تعريفه لأنه جمع الحالات التي تكون فيها نضم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية ولولا هذه النضم المعلوماتية وشبكات الإتصال ما كان أن نسبغ صفة المعلوماتية على هذه الجرائم.

---

[1] ناير نبيل عمر-الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية -دار الجامعة الجديدة مصر -طبعة10 / 2012 ، ص 22-23 .

[2] قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، الصادر في الجريدة الرسمية العدد 47 ، المؤرخة في 16 غشت سنة 2009 .

[3] د. عميمر عبد القادر - التحديات القانونية لإثبات الجريمة المعلوماتية - النشر الجامعي الجديد _الجزائر_ ، طبعة 2021 ، ص 18 ، 19،20 .

وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال [1].

## الفرع الثاني : خصـــــائـــــص الجريمة الإلكترونيــة

نظرا لوقوع جرائم المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للمعطيات و نظرا لأننا أمام ظاهرة إجرامية ذات طبيعة خاصة بالإضافة إلى ما تولده من خسائر فادحة تميزها عن الجرائم التقليدية ، حدد الخبراء للجريمة المعلوماتية في سياقها و ظروف إرتكابها خصائص منفردة لا تتوافر في أي من أفعال الجرائم التقليدية و تلك الخصائص نوردها كما يلي [2]:

1-الحاسب الآلي هو الأداة الرئيسية لارتكاب الجريمة المعلوماتية.

2-الجريمة المعلوماتية ترتكب ضمن نظام المعالجة الآلية للمعطيات.

3-مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي و المعلوماتية.

4-الجريمة المعلوماتية لا حدود جغرافية لها.

5-أهدافها و دوافعها عديدة ، منها الحصول على المعلومات الإلكترونية أو الاستيلاء على الأموال أو يكون هدفها الأفراد أو جهات بعينها أو تستهدف أجهزة الكمبيوتر في حد ذاتها لتخريبها أو تعطيلها على الأقل لأطول مدة ممكنة.

6-أنها جريمة هادئة لا عنف فيها يسهل إرتكابها و لا تترك أثرا لها بعد إرتكابها كونها جريمة فنية.

7-سهولة إخفاء معالم الجريمة و صعوبة تتبع مرتكبيها لما يلعبه الدور الزمني(اختلاف التوقيت بين الدول) و المكاني(إمكانية تنفيذ الجريمة عن بعد) و القانوني (أي قانون يطبق) في تشتيت جهود التحري و التنسيق الدولي.

8-أنها تحتاج إلى خبراء مختصين للتحقيق فيها و يصعب على المحقق التقليدي التعامل معها.

9-صعوبة الاحتفاظ الفني بآثارها إن وجدت.

10-كثير من هذه الجرائم لا يتم الإبلاغ عنها إما لعدم كشف الضحية لها و إما خشية من التشهير حفاظا على ثقة المتعاملين خاصة الشركات و المؤسسات الكبرى.

## المطلب الثاني: صـــور الجـــرائـــم الإلكتـــرونيـــة .

ثمة صور متعددة لجرائم المعلوماتية و قد أورد لها الفقهاء و حتى التشريعات تصنيفات متعددة و مختلفة تختلف حسب المعايير التي اعتمدوها و قد تباينوا في تصنيفاتهم حول ما يعد جريمة و ما يعد مجرد سلوك غير أخلاقي لا يرقى حد الجريمة، فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب و أخرى ترتكب بواسطته، و بعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، و آخرون يستندون

[1] بوظياف إسماهان، الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها في الجزائر، العدد 11 ، سبتمبر 2018 ، ص 352-353

[2] راجع خصائص الجرائم المعلوماتية و دوافع إرتكابها بالتفصيل د.أحمد خليفة الملط " الجرائم المعلوماتية " ، دار الفكر الجامعي الإسكندرية 2005، ص 98 و ما بعدها

إلى الباعث أو الدافع لارتكاب الجريمة ، و كمثال عن التصنيفات [1] التي أوجدت ما جاءت به **إتفاقية بودابست الأوربية لمكافحة الجريمة المعلوماتية سنة 2001** و هذا التصنيف ورد كما يلي :

**الفرع الأول : تصنيف الجرائم الإلكترونية حسب إتفاقية بودابست الاوروبية**

أولا: الجرائم التي تستهدف عناصر المعطيات و النظم و تضم الدخول غير المشروع- الإعتراض غير القانوني-تدمير المعطيات-إعتراض النظم -إساءة إستخدام الأجهزة .

ثانيا: الجرائم المرتبطة بالكمبيوتر و تضم التزوير المرتبط بالكمبيوتر -الإحتيال المرتبط بالكمبيوتر .

ثالثا : الجرائم المرتبطة بالمحتوى و تضم طائفة واحدة وفق هذه الإتفاقية و هي الجرائم المتعلقة بالأفعال الإباحية و اللاأخلاقية .

ارابعا : و هي الجرائم المرتبطة بالإخلال بحق المؤلف و الحقوق المجاورة (قرصنة البرمجيات) و نورد في هذا المطلب و باختصار تصنيفا بسيطا و شاملا [2] لمختلف صور الجريمة المعلوماتية و نظرا لكون مساحة العرض محددة و لا تكفي لعرض جميع التصنيفات الموضوعة من الفقهاء و الدارسين سنعرض باختصار أهم صور الجريمة الإلكترونية :

**1-جريمة التوصل أو الدخول غير المصرح به :** و هذا يستلزم وجود المجرم المعلوماتي داخل أحد المراكز المعلوماتية حيث أن كل ما يهمه في هذا الغرض هو الولوج إلى هذه المعلومات و الإطلاع غير المصرح به على تلك المعلومات المخزنة في ذاكرة النظام المعلوماتي و يأخذ هذا الولوج إحدى الصورتين[3] :

*الولوج المباشر أين يستطيع المجرم الإستيلاء على المعلومات المخزنة بعدة طرق و هي: 1- بإستخدام آلة طباعة لإستخراج المعلومات المكتوبة على الورق ، 2- بإستخدام شاشة النظام و الإطلاع بالقراءة على ما هو مكتوب عليها بإستخدام مكبر الصوت أو سماعات لإلتقاط المعلومات و البيانات المعالجة.

*الولوج غير المباشر عن طريق شبكات الإتصال و المعالجة عن بعد[4] و هو يأخذ الصور التالية:

---

[1] راجع مختلف التصنيفات الواردة على الجريمة المعلوماتية لدى يونس عرب ، موسوعة القانون وتقنية المعلومات ، ص 255 و ما بعدها

[2] راجع مختلف التصنيفات الواردة على الجريمة المعلوماتية لدى يونس عرب ، موسوعة القانون وتقنية المعلومات ، ص 389 .

[3] راجع خصائص الجرائم المعلوماتية و دوافع إرتكابها بالتفصيل د.أحمد خليفة الملط " الجرائم المعلوماتية " ، دار الفكر الجامعي الإسكندرية 2005، ص 224 .

[4] من الحوادث الشهيرة التي وقعت عن طريق الولوج غير المباشر (عن طريق وسائل الاتصال البعدي) و التي تتعدى الحدود الإقليمية عندما نجح أربعة تلاميذ يدرسون في إحدى مدارس نيويورك الأمريكية لا تتجاوز أعمارهم الثالثة عشر إلى الوصول إلى البيانات التي تقوم شركة الإسمنت لافارج Lafarge في كندا بتخزينها في بنك معلومات شرطة datapace الامريكية و تحقق لهم ذلك من خلال إتصالات هاتفية أجريت عن بعد من هاتف المدرسة ، وبتاريخ 1985/04/15 لاحظ موظفو الشركة ان مجهولا قد تمكن من الوصول إلى بيانات الشركو المخزنة ببنك المعلومات عن طريق الإتصال البعدي ورغم الصعوبة الشديدة لتحقق ذلك بل وحتى إستحالة حسب تقدير موظفي شركة داتابايس بوشرت إجراءات موسعة للتحقق من قبل مختصين ينتمون إلى الشركة الكندية و مكتب التحقيقات الفيدرالي FBI و امكن تتبع مصدر الاتصالات الهاتفية و تبين ان مصدرها الهاتف في إحدى المدارس الامريكية ، وللتحقق من شخصية المتسللين (الهاكرز) وافقت شركة لافارج عن القيام بدور الطعم وراقب المختصون بدهشة و إنبهار الطرق المتقدمة التي يمارسها المتسللون لتخطي أنظمة الرقابة ، و قد توصل التلاميذ إلى البرمجة الداخلية التي تتيح لهم السيطرة الكاملة

1- التقاط المعلومات المتواجدة ما بين النظام المعلوماتي و النهاية الطرفية ، 2- إلتقاط الإشعاعات الصادرة عن النظام المعلوماتي و تتم هذه الطريقة عن طريق تسجيل ثم حل شفرة النبضات الإلكترونية المبثوثة و مثال ذلك قيام شخص بإختلاس أموال عن طريق إلتقاط أمر بتحويل مرسل من بنك إلى آخر بعدما تمكن من تزييف الرسالة بأمر أدفع نفس المبلغ لحساب قام بفتحه بإسمه.

3- الولوج غير المشروع عن طريق نهاية طرفية بعدية حيث يمكن ذلك عن طريق نظام معلوماتي و معرفة كلمة السر أو مفتاح الشفرة المناسب.

**2- جريمة الإستيلاء على المعطيات و سرقة وقت الكمبيوتر:** يرصد الفقه ثلاث صور يتحقق فيها **الإستيلاء على معطيات الكمبيوتر** و هي :**أولها:-** الإلتقاط الذهني للبيانات بالنظر أو الإستماع و يتم هذا الإلتقاط بالإختزان أو الحفظ الواعي أو العرضي للمعلومات إثر مطالعتها بالبصر أن كانت قد ظهرت على شاشة الحاسوب في شكل مرئي [1]، أو بعد وصولها إلى الأذن أن تمثلت في صورة صوتية صادرة على الأجهزة **.و ثانيها -:**النسخ غير المشروع للبيانات المخزنة إلكترونيا إما عن طريق التعامل المباشر مع نظام الكمبيوتر المخزنة فيه البيانات على هيئة نبضات إلكترونية إما في الدارات المدمجة للكمبيوتر أو الدعامات كالأقراص الصلبة أو المرنة (و إما عن طريق التوصل غير المرخص به مع نظام الحاسوب عبر الإتصال عن بعد كما عرضناه فيما تقدم .**و ثالثها -:** إعتراض معطيات الكمبيوتر خلال نقلها و إلتقاطها بواسطة إحدى الطرق التي عرضنا لها فيما سبق.

أما **جريمة سرقة وقت الكمبيوتر** أو سرقة أو إغتصاب وقت الحاسوب أو جهده أو خدماته فتتم إما بالإستخدام المباشر لنظام الحاسوب دون ترخيص أو في أغراض أو قطاعات غير مرخص بالوصول إليها أو يتم بالتوصل غير المشروع عن بعد مع نظام الكمبيوتر هذا كله من أجل مصلحة شخصية دون علم الحائز الشرعي للنظام المعلوماتي بدلا من إستخدام النظام المعلوماتي لأغراض مهنية بحتة و مسموح بها[2] .و من أمثلة ذلك نذكر في هذا الخصوص واقعة إثنين من مستخدمي شركة غاز بريطانية قاما عن طريق إعلانات صغيرة ببيع رسومات صممت بواسطة النظام المعلوماتي الخاص بهذه الشركة و هو ما يساوي العمل في الظلام على حاسب آلي مملوك لرب العمل و لكن بدون علمه .

---

على النظام المعلوماتيو القيام باية اعمال غير مشروعة كإستبدال الذاكرة بأخرى و إلتقاط أية رسالة و محو البيانات كليا أو جزئيا . و قد أضافت الشركة إلى نظام تشغيل الشبكة إجراءات أمن إضافية للاستمرار في عملها و هذه الإجراءات أثارت غضب التلاميذ فعمدو إلى محو و تدمير عشرة ملايين بايت BYTES من المعلومات و التي تمثل خمس المخزون في النظام من المعلومات مما دفع رجال التحقيقات الى مداهمة المدرسة بتاريخ 1985/04/25 و إلقاء القبض على التلاميذ و بسبب صغر السن قرر المدعي العام عدم إحالتهم على المحكمة .

[1] و من أمثلتها ان ستيف جوبز(أحد الصديقين الذي أخرجا كمبيوتر APPEL إلى الوجود ) كانت مجرد مشاهدته لبعض التطبيقات أو البرامج وواجهة المستفيد (GUI) التي تستخدم الرسوم و الأيقونات بمركز أبحاث (بالو آلتو) في شركة زيروكس zerox كافية للإستيلاء و نقل التقنية و غستخدامها في نشاطه . أنظر في هذا المثال و امثلة اخرى عن جريمة الإستيلاع عن معطيات المهندس حسن طاهر داود ، جرائم نظم المعاومات ، أكاديمية نايف العربية للعلوم المانية ، الطبعة الاولى الرياض سنة 2000 .

[2] راجع مختلف التصنيفات الواردة على الجريمة المعلوماتية لدى يونس عرب ، موسوعة الفانون وتقنية المعلومات ، ص 414 .

و مثال آخر يتعلق ب 200 مستخدم قاموا بإستخدام الحاسب الآلي الخاص بمركز تصنيع و حماية الصواريخ النووية من أجل تخزين ألعاب الياناصيب و الخطابات الشخصية [1].

**3-جريمة إحتيال الكمبيوتر** [2]**:**إن صور إحتيال الكمبيوتر عديدة بل و عصية في أحيان كثيرة عن الحصر لتباينها من حيث وسائل الإعتداء التقني نفسه أو تباينها من حيث البيانات محل الإعتداء و يمكن القول بإيجاز أنها كافة الوسائل التقنية للتوصل إلى البيانات المالية أو التي تتصل بحقوق مالية و جامع هذه الوسائل و الأنشطة أن الشخص يقوم بأعمال إحتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته، و صورته كذلك في الوقت الحاضر الإحتيال عن طريق الإنترنت المتمثل بإستغلال مواقع الإنترنت لجني مبالغ الآخرين عبر مشاريع وهمية لمنتجات أو خدمات أو من خلال الوصول إلى أرقام بطاقات إئتمان الزبائن سواء بجمعها عند تلقي الموقع الوهمي لها أو التوسل للوصول إليها من مواقع أخرى .و من ثمة إستغلالها في عمليات شراء غير مشروعة، و أنشطة التلاعب بالأسهم المالية و مزادات البضائع على الإنترنت .و من الأمثلة الشهيرة لجريمة إحتيال و أثناء Michaael toumpson الكمبيوتر تتلخص في أن خبيرا في الحاسبات الإلكترونية يدعى ميخائيل طومسون عمله في بنك الكويت التجاري بعقد خاص تتحدد وظيفته فيه بتحديث النظام المعلوماتي للبنك، إستغل فرصة سفر المشرف عليه و إختار خمسة من الحسابات البنكية في خمسة فروع من فروع البنك و أدخل إلى كمبيوتر البنك برنامجا يتيح له تحويل مبالغ معينة من الحسابات و ربط عملية التحويل بتاريخ لاحق إختاره ليأتي بعد سفره من الكويت إلى بريطانيا و إنتهاء عقد عمله .و إضافة لذلك يتضمن البرنامج المزروع محو بيانات عملية التحويل هذه من ذاكرة الحاسوب بعد إتمامها.و لدى وصوله إلى بريطانيا قام بفتح حساب بنكي و طلب من بنك الكويت بواسطة التلكس تحويل أرصدته بفروع البنك الخمسة إلى حسابه في بريطانيا و تحقق له ذلك .و لدى إكتشاف أمره أحيل على المحاكمة في بريطانيا و وجهت إليه تهمة الحصول على أموال بالخداع و أصدرت المحكمة حكما عام 1983 قضى عليه بالحبس لمدة 15 شهرا.

**4-جريمة التزوير المعلوماتي** [3]**:**و هي الممارسات أو النشاطات التي تنصب على البيانات المخزنة إلكترونيا في النظام المعلوماتي و تهدف إلى التعديل غير المشروع لها بإضافة أو حذف علامات أو إشارات مصطنعة أو بيانات عكس الحقيقة و التي من شأنها أن تسبب ضررا للغير، و لا

و يقع التزوير المعلوماتي إما **ماديا** عن طريق التدخل من خلال النظام و يقع التزوير المعلوماتي إما **ماديا** عن طريق التدخل من خلال النظام المعلوماتي و ذلك بتغيير المحررات عن طريق الحذف بإزالة كلمة أو رقم أو رمز معين أو عن طريق الإضافة بزيادة رقم على مبلغ معين أو بإضافة عبارات أو بيانات غير صحيحة أو بخلق محرر لم يكن له وجود من قبل و

---

[1] د .محمد سامي الشوا ، ثورة المعلومات و إنعكاساتها على قانون المعلومات ، دار النهضة العربية 1998 ، ص 85

[2] راجع مختلف التصنيفات الواردة على الجريمة المعلوماتية لدى يونس عرب ، موسوعة القانون وتقنية المعلومات ، ص 417 , ما بعدها .

[3] كمثال عن جريمة التزوير المعلوماتي قصة مداخلة البيانات التي كانت صديقة لنادي السيارات في مدينة سكرامنتو بولابة كاليفورنيا فقد قامت هذه الفتاة بتغيير ملكية السيارات المسجلة في الكمبيوتر بحيث تصبح مسجلة باسم بعض لصوص السيارات ، ثم يقوم هؤلاء اللصوص بسرقة هذه السيارات .و كان الضحايا من اصحاب السيارات المسروقة يفاجأون عند تقدمهم للشرطة للإبلاغ بسرقة سياراتهم بأنه لايوجد في سجلات الكمبيوتر ما يثبت ملكيتهم لهذه السيارات التي يبلغون بسرقتها ، و بعد أن يقوم اللص بالتصرف في السيارة بالبيع على أنها مملوكة له تقوم هده الفتاة بإعادة السجلات لسابق عهدها حيث تعود لتظهر ملكية صاحب السيارة الأصلي لها ،فحيث أنها كانت تتقاضى مائة دولار للعملة الواحدة الى ان اعترف احد اللصوص اين قام احد رجال الشرطة السريين بالتعامل معها على انه احد لصوص السيارات فوقعت في يد العدالة .

نسبته كذبا إلى غير مصدره .و إما يقع **معنويا** و ذلك بتسجيل بيانات لم تصدر عن المتعاقدين أو أولي الشأن [1] أو إثبات وقائع كاذبة أو غير معترف بها أو إغفال معلومة أو إيرادها على وجه غير صحيح [2].

**5-جريمة إتلاف و تدمير المعطيات و النظم :**و يقصد بها هو إتلاف أو محو تعليمات البرامج أو البيانات ذاتها و لا يهدف التدمير هنا إلى مجرد الحصول على منفعة النظام المعلوماتي أيا كان شكلها) إستيلاء على نقود أو إطلاع على معلومات (و لكن يبقى ببساطة إحداث ضرر بالنظام المعلوماتي و إعاقته عن أداء وظيفته[1] .و قد تأخذ هذه الجريمة إحدى الصورتين :**أولها** إتلاف البيانات المنسوخة على الدعامات و الشرائط الممغنطة .**ثانيها** إتلاف البيانات و المعلومات الموجودة داخل النظام المعلوماتي (أو ما يطلق عليها تدمير نظم المعلوماتية).

**الفرع الثاني : تصنيف الجرائم الإلكترونية في قانون العقوبات الجزائري**

طبقا لقانون العقوبات الجزائري المعدل والمتمم و الذي إستحدث فيه المشرع قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان أنظمة المعالجة الآلية للمعطيات ، و على هذا الأساس يمكن تصنيف الجرائم الإلكترونية كالآتي ([3]):

_ الغش او الشروع فيه ، في كل جزء من المنظومة للمعالجة الآلية للمعطيات .
_حذف أو تغيير لمعطيات المنظمة . _تكوين جمعية أشرار .
_إدخال او تعديل في نظام المعطيات .
_تصميم او بحث او تجميع أو توفير او نشر أو الإتجار .
_حيازة او إفشاء أو نشر او إستعمال المعطيات .

إن أنشطة مكافحة الجرائم الإلكترونية أظهرت تحديات و مشاكل كثيرة تختلف في جوانب كثيرة عن التحديات و المشاكل التي ترتبط بالجرائم التقليدية الأخرى منها مثلا أن جرائم الكمبيوتر والانترنت لا تترك أثر ماديا وراءها بمسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية ، كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة جدا مما يستوجب ضبط هذه الجرائم و جمع الأدلة عنها والتعرف على مرتكبيها عن طريق إتباع جملة من الإجراءات ، **و هذا ما سنتطرق إليه في المبحث الثاني من خلال إجراءات ( المعاينة و التفتيش و التسرب و اعتراض المراسلات ، و كذا الضبط و الخبرة و الشهود في الجرائم الإلكترونية ).**

---

[1] و مثال هذه الحالة ان يعهد شخص بتدوين بيانات يطلب أصحاب الشأن إثباتها فيغير هو فيها الحقيقة و يكتب أشياء أخرى .

[2] كقيام محرر المحضر بإثبات اعتراف المتهم بارتكاب جريمة لم يرتكبها .

[3] أنظر المواد 394 مكرر و ما يليها من قانون رقم 15-19 مؤرخ في 18 ربيع الأول عام 1437 الموافق لـ 30 ديسمبر سنة r2015 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 و المتضمن قانون العقوبات الصادر في الجريدة الرسمية / العدد 71 رقم 03 ، و المادة 02 منه ق 04/09

## المبحث الثاني: طـــرق إثبات الجرائـم الإلكتـرونيـــة .

إن التعامل في الجريمة المعلوماتية يتطلب إجراءات لحماية الدليل ، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة الإلكترونية ، ذلك أن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها ، وتعد المعاينة والتفتيش من بين الإجراءات التي تباشرها سلطات التحقيق للوصول إلى الدليل ، كما يلعب الضبط و الخبرة دورا هاما في مجال الإثبات الجنائي للأدلة الإلكترونية خاصة في ظل تزايد تطور التكنولوجيا ، فبعد انتهاء المحقق الجنائي من إجراء التفتيش يقوم بضبط الأشياء التي يراها ضرورية، ومن ثم يأتي دور الخبير الذي يقوم بالتنقيب عن الحقيقة بناء على الأشياء المضبوطة، ثم يقدم الدليل المستنبط للقاضي الذي يمكن أن يبني حكمه بناء عليه عن طريق التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه ، وكل هذا سواء تعلق بالمجرم المعلوماتي أو التقليدي ما دام أن إجراءات الحصول على الدليل نفسها ، وهذا ما سوف .

### المطلب الأول: المعاينة و التفتيش و الشهود في الجرائم الإلكتـــرونيـــة

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية ، وذلك لندرة تخلف أثار مادية عند ارتكاب الجريمة الإلكترونية ، كما أن أطول فترة وقوع الجريمة و ارتكابيا و بين اكتشافها يكون له تأثير السلبي على الآثار الناجمة عنها سواء بسبب العبث أو المحو أو التلف لتلك الآثار[1].كما تعتبر المعاينة من أهم إجراءات التحقيق والتي يمكن من خلالها الحصول على الدليل الجنائي بحيث يجوز للنيابة العامة أن تقوم به في غيبة المتهم إذا لم يتيسر له حضوره.

باعتبار أن التفتيش من أخطر الحقوق التي منحت للمحقق لكونه يمس بالحريات التي تكفلها وتصونها الدساتير[2] كالقانون الجزائري وضع له عدة ضوابط سواء فيما يتعلق بالسلطة المختصة بمباشرته، أو التي تأذن بإجرائه، أو الأحوال التي تجوز فيها مباشرته وشروط اتخاذه، وكل هذا يمثل ضمانات الحرية الفردية أو حرمة المسكن.

#### الفرع الأول : المعـاينـــة في الجرائم الإلكترونيـة

و يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها ،مما يتطلب السرعة في الانتقال إلى مسرح الجريمة و محافظة عليه من إجراء معاينة وهذا ما تضمنته نص المادة 42 من قانون الإجراءات الجزائية الجزائري[3].

---

[1] عبد الفتاح مراد ، شرح جرائم الكمبيوتر و الانترنت ، دار الكتب و الوثائق المصرية ، 2005 ، ص 65 .

[2] من بين هذه الدساتير الدستور الجزائري، من خلال نص المادة 39 من المرسوم الرئاسي رقم( 20- 442) الموافق لـ 2020/12/30،يتعلق بإصدار التعديل الدستوري المصادق عليه في إستفتاء أول نوفمبر سنة 2020 ، الجريدة الرسمية العدد 82 ، المؤرخة في 2020/12/30 والمتضمن الدستور الجزائري المعدل والمتمم والتي تنص على، ما يلي" :تضمن الدولة عدم انتهاك حرمة الإنسان".

[3]عمرو حسين عباس،" بحث في أدلة الإثبات الجنائي والجرائم الإلكترونية "(المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من26-04/27-2008، مقر جامعة الدول العربية، ص 16 .، أنظر الموقع الإلكتروني :
www.arabip.center.com/public/events/papers/paper 2-4. pdf.
وأنظر المادة 42 من قانون رقم66-155 ، المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06-22 ، المؤرخ في2006/12/20 ، الجريدة الرسمية العدد 84 ،مؤرخة في 2006/12/24.

**أولا ـ السلطة المختصة بإجراء المعاينة لمسرح الجرائم الإلكترونيــة:**

الأصل أن انتقال المحقق لإجراء المعاينة أو لمباشرة أي إجراء آخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له، فلا يقوم به إلا إذا كانت مصلحة من ورائه، لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق[1] ، وهذا ما قضت به نص المواد 80،79،42 من قانون الإجراءات الجزائية على أن المعاينة تجرى إما من طرف قاضي التحقيق، وذلك بعد إخطار وكيل الجمهورية الذي لها لحق في مرافقته ، وكما يمكن تمديد اختصاص قاضي التحقيق إذا استدعت ضرورة الحالة إلى دوائر اختصاص محاكم مجاورة، كما يتم أيضا إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر وقوع الجريمة إلى علمهم وانتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية.

**ثانيا :شروط صحة معاينة مسرح الجرائم الإلكترونيــة:**

حتى تحقق المعاينة الغرض المرجو منها في كشف غموض الحادث ومعرفة الفاعل يجب التقييد بعدة شروط كالتالي:

**1-سرعة الانتقال إلى مكان وقوع الجريمة الإلكترونيــة** ، على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها إلى مكان الواقعة[2] .

**2-السيطرة والتحكم على مكان وقوع الجريمة الإلكترونيــة** : من خلا المحافظة على مسرح الجريمة (آثار مادية و بشرية) إلى غاية الانتهاء من إجراءات المعاينة و التحري عن الأدلة و جمعها [3].

**3-الدقة والعناية الفائقة في معاينة مسرح الجرائم الإلكترونيــة** ، وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات فيما هو مرتبط بالجريمة ، وغير ذلك من الوسائل المستخدمة في اقتراف الجريمة الالكترونية.

**4-التحفظ على مسرح الجرائم الإلكترونيــة بعد المعاينة** ، لأن الهدف من الحفاظ على آثار الجريمة بعدى انتهاء من المعاينة هو من أجل إمكانية العودة إليه كّلما أراد المحقق أو القاضي كشف غموض أو التأكد من آثار معينة. **5 -تدوين المعاينة** ، ويكون ذلك كتابيا ورسميا وتصويريا.

**الفرع الثاني : التفتيـــش في الجريمــة الإلكتـــرونيـــة**

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السر، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن [4]، ويباشر

---

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، مصر 2006، ص102 .

[2] راجع المادة 42 من قانون الإجراءات الجزائية الجزائري.

[3] المادة 50 من من قانون الإجراءات الجزائية الجزائري، أنظر أيضا خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط 1 .، دار الفكر الجامعي( الإسكندرية، 2009 ، ص158 ، ص 160

[4] المرجع نفسه ، ص180 .

التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيدا لإظهار الحقيقة [1]، و يقصد به إجراء من إجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم ، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات ، وذلك من أجل البحث عن الأفعال المرتكبة وغير المشروعة والتي تشكل جناية أو جنحة[2]، كما يرد محل التفتيش في البيئة الإلكترونية على المكونات المادية أو المعنوية للحاسب الآلي وتشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته ، فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية[3]، والتي يمكن إيجادها في مسكن المتهم أو مسكن غير المتهم[4]، والتي قد تتواجد أيضا في مكان عام، فهي بذلك تخضع للقواعد التي تحكم ذلك المكان، كما قد تتواجد هذه المكونات في حيازة شخص خارج مسكنه، فهي بذلك تخضع لقواعد تفتيش الأشخاص بوصف المكونات المادية للحاسوب أحد ملحقاته، وسواء كان الشخص الحائز المالك أو الغير، أما بالنسبة لمكونات الحاسوب المعنوية والمتمثلة في المعلومات والبيانات المعالجة آليا، فهي محل خلاف باعتبارها غير مادية[5].نص المشرع الجزائري في المادة81 من قانون الإجراءات الجزائية على عبارة - أشياء- فهذه العبارة يدخل في مضمونها الأشياء المادية والمعنوية [6] ، كما تناول قواعد تفتيش نظم الإلكترونية من خلال إجازته لسلطة التحقيق القيام بإجراءات التفتيش في منظومة إلكترونية [7]. يتم التفتيش في حالة وجود حاسب المتهم متصل بغيره من الحواسيب عبر الشبكة الإلكترونية، وفي حالة وجود حاسب متصل بحاسوب يقع في نطاق إقليم دولة أخرى وهنا يجب التمييز بين ما إذا كان حاسوب المتهم متصلا بآخر داخل إقليم الدولة ، أين تضمن المشرع الجزائري في التعديل الجديد لقانون الإجراءات الجزائية نصوص قانونية إجرائية فيما يخص بتوسيع بعض الصلاحيات في مجال التفتيش، ذلك في بعض أنواع من الجرائم من بينها الجريمة المعلوماتية، حيث يجوز لقاضي التحقيق أن يأمر ضابط الشرطة القضائية للقيام بالتفتيش أو حجز ليلا أو نهارا في أي مكان على امتداد التراب الوطني[8].

أما التفتيش في حالة وجود حاسب متصل بحاسوب يقع في نطاق إقليم دولة أخرى يتم بموجب القانون رقم09-04 لسنة 2009 من خلال تعاون السلطات

---

[1] المادة 81 من قانون الإجراءات الجزائية الجزائري رقم 66-155 المعدل و المتمم بالقانون رقم 06-22 ، المؤرخ في 2006/12/20 ، الجريدة الرسمية العدد84 المؤرخة في 2006/12/24 .

[2] علي محمود علي حمودة،" الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع1 ، دبي - الإمارات العربية المتحدة 26-28 نيسان 2003 ، ص 24 .

[3] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1 .، دار الثقافة للنشر والتوزيع، 2011، ص 158 .

[4] راجع المادة 82 و 83 من قانون الإجراءات الجزائية الجزائري رقم 66-155 المعدل و المتمم بالقانون 06-22

[5] موسى مسعود ارحومة،" الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية"، المؤتمر المغاربي الأولى حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس،29 ،28- 09 - 2009 ، ص 7 .

[6] نصت المادة 81 من قانون الإجراءات الجزائية الجزائري على أنه" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء ..."

[7] راجع المادة 03 من قانون رقم (04-09) المؤرخ في 05-08- 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات إ و إ.

[8] راجع المادة 47 من قانون الإجراءات الجزائية الجزائري المعدل و المتمم بالقانون 22/06.

الأجنبية وفقا لمبدأ المعاملة بالمثل في إطار اتفاقيات دولية في هذا الصدد [1]، و في ظل تعزيز وتبادل التعاون الدولي في إطار اتفاقيات دولية أو إقليمية أو ثنائية[2] مع تفعيل آليات المساعدة الدولية في مجال القضائي وتسليم المجرمين، وذلك باحترام مبدأ المساواة في سيادات الدول بما يفضي أنه لا مجال للدول المتقدمة في مجال المعلوماتية الرقمية أن تتحكم في أنظمة الغير والتجسس عليها بحجة ما يقتضيه إجراء التحقيق من تمديد التفتيش عن بعد بين الدول [3].

**أولا-السلطة المختصة بتفتيش النظم الإلكترونيــة:**

الأصل أن تقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق ووكيل الجمهورية، إلا أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهذا ما سنبينه تباعا.

**أ-إجراء تفتيش النظم الإلكترونيــة بمعرفة سلطة التحقيق الأصلية:**

إن المشرع المصري جعل الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة كسلطة أصلية ولقاضي التحقيق في حالات خاصة[4]، وهذا عكس ما قضى به المشرع الجزائري حيث جعل سلطة تحقيق الأصلية من اختصاص قاضي التحقيق[5] باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته[6] ، واستثناءا يجوز لوكيل الجمهورية أن يقوم ببعض إجراءات التحقيق[7]. ولا يكفي توافر صفة قاضي التحقيق لكي يقوم بإجراء التفتيش، بل لابد أن يكون مختصا سواء من ناحية الاختصاص الاقليمي أو النوعي، فيتحدد اختصاص قاضي التحقيق محليا إمَا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.كما يجوز تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وغيرها.إلى جانب الاختصاص الإقليمي لابد من توافر الاختصاص

---

[1] راجع الفقرة 3 من المادة 5 القانون رقم (09-04) المؤرخ في 05-08-2009 .

[2] لقد حدث في ألمانيا جريمة غش بيانات الحاسب الآلي، أين اتضح عند جمع إجراءات التحقيق وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا مع شبكة اتصالات في سويسرا التي تم تخزين المشروعات فيها، وقد تمكنت سلطات التحقيق الألمانية من ضبط ملفات البيانات عن طريق التماس المساعدة المتبادلة بين الدولتين، راجع علي محمود علي حمودة، مرجع نفسه، ص 26 .

[3] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر(1) ، - 2011 2010، ص 315، ص316 .

[4] هلالي عبد أللاه أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، ط 1، دار النهضة العربية، القاهرة ،1997 ، ص 133 ..

[5] يجب الإشارة إلى أن قاضي التحقيق لا يختص بالقضية إلا بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني، وذلك بعد أخذ بعين الاعتبار نص المواد 67 و 73 ، وبعد دخول القضية في حوزته يكون مختصا وله أن يقوم بكل الإجراءات راجع نص المادة 38-1 من قانون الإجراءات الجزائية الجزائري 06-02.

[6] راجع المواد 79-82 من قانون الإجراءات الجزائية .

[7] راجع المواد 56 -1 ، 59 -1 ، 117 -1 من قانون الإجراءات الجزائية .

النوعي المتمثل في نوع الجريمة التي يختص بها المحقق بالتفتيش، وبالنسبة للقانون الجزائري نجد أن قاضي التحقيق يختص بإجراء التحقيقات بما فيها التفتيش في الجنايات والجنح المتلبس بها[1].

ويبدو أنه لما كانت سلطة التحقيق الأصلية غير مطالبة بالقيام بالتفتيش بنفسها في كل الحالات إذ قد لا يكون لها وقتا كافيا، خاصة إذا تعددت الأمكنة التي يتم تفتيشها أو الأشخاص المراد تفتيشهم، ففي هذه الحالة يجوز لقاضي التحقيق ندب أحد قضاة التحقيق أو أحد ضباط الشرطة القضائية[2] .

**ب - إجراء تفتيش النظم الإلكترونيــة بمعرفة ضباط الشرطة القضائية:**يتمتع قاضي التحقيق وحده بالاختصاص الأصيل لإجراء التحقيق، ونظرا لكثرة هذه الإجراءات وتنوعها أجاز له القانون أن يندب ضباط الشرطة القضائية للقيام بها وفقا لشروط خاصة[3]، ويتحقق إجراء التفتيش نظم الإلكترونيــة بمعرفة ضابط الشرطة القضائية، في الحالات التالية [4] :

- **التفتيش بناء على إذن قضائي بإجرائه:** باعتبار أن قاضي التحقيق غير ملزم في كل الحالات بمباشرة التفتيش، فإنه يجوز له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا الإجراء و هذا ما يسمى بالإنابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصوله على إذن مسبق [5]، كما حدد المشرع الجزائري الاختصاص الإقليمي لضباط الشرطة القضائية إما بمكان وقوع الجريمة، أو بمكان إقامة المتهم، أو بمكان القبض عليه، وكما مدد اختصاصهم في حالة الاستعجال إلى كافة دائرة الاختصاص المجلس القضائي الملحقين به، ومدد بالنسبة لبعض الجرائم الخطيرة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني [6].

-**التفتيش بناء على حالة التلبس بالجريمة:**لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز لضابط الشرطة القضائية المنتدب في أحوال التلبس بالجنايات والجنح المعلوماتية تفتيش نظم الحاسب الآلي [7]، هذا ما تضمنته نص المادة 44 من قانون الإجراءات الجزائية الجزائري.

-**التفتيش بناء على موافقة المتهم:**يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر

---

[1] راجع المادة 40 من قانون الإجراءات الجزائية المعدل و المتمم بالامر رقم 20/04.

[2] هلالي عبد اللاه أحمد، مرجع نفسه، ص 138 .

[3] ومن شروط الواجب توافرها للقيام بالإنابة القضائية ما نصت عليه المواد138 ،139 ،142 من ق،إ.ج.ج ، التي تتضمن مايلي:أن تصدر الإنابة من قاضي التحقيق المختص إقليميا، وأن تصدر إلى قاضي، أو ضابط الشرطة القضائية، وأن تنصب الإنابة على إجراء أو بعض إجراءات التحقيق الابتدائي، وعليه إذا كان التفويض عاما، كانت الإنابة باطلة، ويجب أن تكون الإنابة صريحة ومكتوبة، وغيرها من شروط التي يجب مراعاتها .

[4] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، **د .ط، دار الجامعة الجديدة، الإسكندرية**، د.س.ن ، ص 428 .

[5] راجع المادة 44 من قانون الإجراءات الجزائية الجزائري و المادة 40 من الدستور الجزائري .

[6] راجع المادة 16 من قانون الإجراءات الجزائية .

[7] طارق إبراهيم الدسوقي عطية، مرجع نفسه، ص 437 .

ويذكر فيه هذه الموافقة؛ أما بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم الإلكترونيــة بناء على موافقة المتهم سواء في مصر أو في القانون المقارن، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية [1].

**ثانيا: شروط تفتيــش الجرائم الإلكترونيــة**

يعتبر التفتيش انتهاك على الحق في الخصوصية الفردية، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية، لذا عمدت الدول على إحاطته بالضمانات القانونية حتى لا يتم إساءة استخدامه وسوف نتناول في هذا الإطار ما يلي:

**01 - الشروط الموضوعية لتفتيش الجرائم الإلكترونيــة:**

يشترط أن يتوافر في التفتيش سببا له، وأن يكون محله الحاسوب بكل مكوناته المادية والمنطقية والشبكة الإلكترونية، بالإضافة إلى وجود سلطة مختصة للقيام به، وعلى ضوء ما سبق فإن القواعد الموضوعية لتفتيش نظم المعلوماتية تتمثل فيما يلي:

**أ- أسباب تفتيش النظم الإلكترونيــة :**

ترتب على إجراء التفتيش خلاف فقهي حول مدى مشروعية التفتيش في الجرائم الإلكترونية بين الذين يرون قابلية النصوص التقليدية لتطبيق هذا الإجراء في الجرائم الإلكترونية ، مع الذين يتجهون إلى وجوب استحداث نصوص تشريعية جديدة تجرم الأفعال، وأثناء غياب تشريعات جديدة فلا مجال للحديث عن سبب تفتيش الحاسب الآلي، غير أن هذه المشكلة لا يمكن أن تثير سبب التفتيش في الجرائم الإلكترونية في الدول التي تضمنت نصوص قانونية للتجريم والعقاب على مثل هذه الجرائم إلا أن المشكلة تكمن في الدول التي لم تجرم الأفعال غير المشروعة الناشئة عن أنظمة الحاسب الآلي أين قد يكون التفتيش فيها باطلا [2].

وبالتالي فقد تناول المشرع الجزائري سبب التفتيش في أكثر من نص منها المادة (44) من قانون الإجراءات الجزائية والتي نصت على ما يلي" : لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش " [3].

ولكي يعتبر التفتيش في مجال الجريمة الإلكترونية مشروعا، لابد من توافر شروط والتي نوردها فيما يلي:

-وجوب وقوع جريمة إلكترونية سواء كانت جناية أو جنحة، وبالتالي تستبعد المخالفات نظرا لقلة أهميتها باعتبارها لا تصل إلى درجة المساس بحريات الأشخاص أو انتهاك لحرمات منازلهم [4].

-اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها.

---

[1] هلالي عبد اللاه أحمد، مرجع نفسه، ص 162 .

[2] فايز محمد راجح غلاب، مرجع نفسه، ص 317- 319.

[3] المادة 44 -1 من قانون الإجراءات الجزائية المعدل و المتمم بالامر رقم 20/04.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع نفسه، ص 211. ، 210 .

-توافر أمارات قوية أو قرائن على وجود أجهزة إلكترونية تفيد في كشف الحقيقة لدى المتهم أو غيره [1].

ولذلك فلا يجرى التفتيش إلا إذا توافرت لدى قاضي التحقيق أسباب كافية مقنعة، أي تواجد أدوات أو أشياء استعملت في ارتكاب الجريمة أو متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في التفتيش عن الحقيقة سواء لدى المتهم المعلوماتي أو غيره والتي تتواجد في المكان أو عند الشخص المراد تفتيشه [2].

**ب- محل تفتيش النظم الإلكترونيــة:**

لكي يكون التفتيش صحيحا يجب أن يرد على المحل الذي قد يكون الشخص أو المكان، وهذا المحل يجب أن يكون محددا أو قابل لتحديد وجائزا قانونا[3] ، وبالتالي فالشخص الذي يقوم بتفتيش نظم الإلكترونية ، قد يكون من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، أو من مشغلي، أو مستخدمي الحاسب، أو مقدمي الخدمة، أو من مهندسي الصيانة والاتصالات، أو من مديري نظم الإلكترونية ، أما الأشخاص الذين يقوم عليهم التفتيش هم أي أشخاص آخرين يكون بحوزتهم معدات أو أجهزة إلكترونية أو أجهزة حاسب آلي محمول أو تلفونات متصلة بجهاز المودم أو مستندات، وفي كل الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به[4].

وبخصوص القانون الجزائري فهو لم يتضمن تفتيش الأشخاص كإجراء التحقيق باستثناء في بعض إجراءات التحقيق الجمركي، أين يمكن لأعوان الجمارك القيام بتفتيش الأشخاص في حالة إخفاء بضاعة مغشوشة وفقا لما نصت عليه المادة (**42**)من قانون الجمارك، وكذا نص المادة (**61**) من قانون الإجراءات الجزائية التي نصت بطريقة غير مباشرة على تفتيش الأشخاص في حالة التلبس بناء على القبض [5].

وبالنسبة لتفتيش المنازل وما في حكمها كمحل لتفتيش نظم إلكترونية، فيقصد به محل الإقامة أو المأوى والملحقات المخصصة لمنافعها والتي يستخدمها الشخص سواء بصفة دائمة أو مؤقتة متى وجدت فيه مكونات الكمبيوتر المادية أو المعنوية أو شبكات اتصال خاصة [6].

فقد تطرق المشرع الجزائري لتفتيش المنازل في نص المادتين (**82،83**)من قانون الإجراءات الجزائية، والتي تتضمن تفتيش منزل المتهم أو غير المتهم، فعلى قاضي التحقيق عند مباشرة التفتيش في هذه الحالة أن يلتزم بالشروط الواردة في

---

[1] هلالي عبد اللاه أحمد، مرجع نفسه، ص 115.

[2] طارق إبراهيم الدسوقي ، المرجع نفسه ،ص 405 .

[3] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري،" الإثبات الجنائي بالأدلة الرقمية من الناحيتين( القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العرابية للعلوم الأمنية، الرياض، 2007 ، ص19 .

[4] هلالي عبد اللاه أحمد، مرجع نفسه، ص 12.

[5] راجع المادة 42 من قانون رقم (98)المؤرخ في 22 غشت 1998 ، المتضمن قانون الجمارك المعدل والمتمم، والمادة 61 من قانون الإجراءات الجزائية .

[6] هلالي عبد اللاه أحمد، مرجع نفسه، ص 132 .

المادتين (45،47) من نفس القانون واللتان تناولتا أحكما في مجال التفتيش، حيث يوجب على ضابط الشرطة القضائية أو قاضي التحقيق مراعاة قواعد معينة وكما شملت المادتين على قواعد خاصة بكيفية التعامل مع الأوراق أو المستندات [1].

**02 - الشروط الشكلية لتفتيش الجرائم الإلكترونيــة:**

إلى جانب الضوابط الموضوعية لتفتيش نظم الحاسب الآلي، هناك ضوابط أخرى ذو طابع شكلي يجب مراعاتها والأخذ بها أثناء القيام بالتفتيش، والتي تتمثل فيما يلي:

**أ- الأشخاص المطلوب حضورهم أثناء التفتيش:**

يشترط لقيام التفتيش كضمانة حضور صاحب المكان المراد تفتيشه، حيث اعتبر غالبية الفقه أن حضور المتهم للتفتيش من الأحكام الأساسية التي يجب الالتزام بها ويترتب على مخالفتها بطلان إجراء التفتيش [2].

**ب- أسلوب تنفيذ التفتيش:**

قام القانون الأمريكي بتنظيم أسلوب تنفيذ التفتيش في نظم الحاسب الآلي، حيث يبدأ رجال الشرطة بالهجوم في الوقت نفسه وبشكل سريع على جميع منافذ المكان، باعتبار أن هذه الخطة تقلل من وقوع إصابات بين فرق رجال الشرطة، وبعد ذلك يقومون بسرعة فائقة باستبعاد الأشخاص المشتبهين فيهم على الحواسب الموجودة في المكان حتى لا يتم تغيير أو حذف أو تدمير الأدلة التي تثبت إدانتهم، حيث يوضع المتشبه فيهم في غرفة مع حراسة أمنية، وتفتيشهم في نفس الوقت مع إعلامهم أن كل أقوالهم ستأخذ بعين الاعتبار ويمكن أن يكون دليل إدانتهم، حيث يوجد مكان في المنزل يعتبر النقطة الساخنة والتي يكون فيها جهاز حاسب آلي متصل بخط هاتفي أو أكثر من ذلك.

وفي هذه الحالة يتم وضع النقطة الساخنة في فريق يتكون من خبيران فنيان أجاز لهم القاضي بالتفتيش، فالأول يسمى بالمكتشف مهمته نزع مقبس الكهرباء الخاص بسائر الأجهزة، ويقوم بالبحث عن الأقراص والمستندات وغير ذلك، والثاني يسمى بالمسجل مهمته تصوير كامل الأجهزة والأدوات المتصلة بها على الحالة التي تم ضبطها، كما يقوم أيضا بتصوير جميع الغرف الأخرى المتواجدة في المكان كضمانة لعدم إدعاء أحد المشتبه فيهم بسرقة منزله وقت التفتيش، بالإضافة إلى أجهزة الفيديو والتسجيل الصوتي التي يتم من خلالها ترقيم الأشياء المضبوطة [3].

**ج- تحديد ميعاد التفتيش:**

يعتبر ميعاد التفتيش أحد أهم الضمانات الشكلية، بحيث لا يجوز إجراؤه خارج الأوقات المحددة قانونا ما عدا في الأحوال الاستثنائية المقررة قانونا [4].

فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات

---

[1] أنظر المادة 45،47، من قانون الإجراءات الجزائية المعدل و المتمم بالامر رقم 20/04.

[2] فايز محمد راجح غلاب، مرجع نفسه، ص 334 .

[3] عبد الله حسين على محمود، سـرقة المعلومات المخـزنة فـي الحاسب الآلـي ، ط2 .، دار النهضـة ، العربية ، القاهرة ، 2001 ، ، ص 382 .

[4] فايز محمد راجح غلاب، مرجع نفسه، ص328 .

الاستثنائية التي أقرها القانون [1]، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية كاستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة[2].

**الفرع الثالث: الشهادة في الجريمة الإلكتـــرونيـــة .**

**أ- تعريف الشاهد في الجريمة المعلوماتية:** هو الشخص الفني صاحب الخبرة و المتخصص في تقنية و علوم الحاسب الآلي، و الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله، و لذلك يطلق عليه اسم الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي[3].

و يمكن القول بأن الشاهد ألمعلوماتي ينحصر في عدة طوائف و فئات هي:

1-مشغلو الحاسب الآلي: عامل تشغيل الحاسب الآلي هو ذلك الشخص المسؤول عن تشغيل الجهاز و المعدات المتصلة به. و لا بد أن تكون لديه خبرة كبيرة في مجال استخدام الكمبيوتر عن طريق استخدام هذه البيانات و كيفية إدخال البيانات ثم استخراجها. و هو يقوم بنقل البيانات من الوثائق إلى وسائط التخزين التي تجري معالجتها بواسطة الحاسب الآلي.

2-خبراء البرمجة أو مخططو البرامج: و هم الأشخاص المتخصصين في كتابة أوامر البرامج و هم فئتين: الأولى هم مخططو برامج التطبيقات و الثانية هم مخططو برامج النظم.-

3-المحللون: المحل هو الشخص الذي يحلل الخطوات و يقوم بتجميع البيانات الخاصة بنظام معين، و دراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة و استنتاج العلاقة الوظيفية بين هذه الوحدات.

4-مهندسو الصيانة و الإتصالات: و هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته و شبكات الإتصال المتعلقة به.

5-النظم: و هم الذين توكل إليهم أعمال الإدارة في النظم المعلوماتية.

ب/ التزامات الشاهد ألمعلوماتي: متى كان الشاهد ألمعلوماتي حائزا لمعلومات جوهرية تفيد سير التحقيق فإنه يكون مطالبا بأن يعلم بها سلطات التحقيق على سبيل الإلزام و إلا تعرض للعقوبات المقررة للإمتناع عن الشهادة، و ذلك في غير

[1] راجع المادة 47 من قانون الإجراءات الجزائية الجزائري المعدل و المتمم بالامر رقم 20/04 .
[2] فايز محمد راجح غلاب، مرجع نفسه، ص329 ، 330 .
[3] عبد الفتاح بيومي حجازي،المرجع نفسه، ص 33.

الأحوال التي يجيز له القانون فيها ذلك[1] و المعلومات الجوهرية التي يجب على الشاهد إفادة سلطات التحقيق بها تتركز على العناصر التالية:
1-طبع ملفات البيانات المخزنة في ذاكرة الحاسب الآلي أو الدعامات الأخرى على أن يقوم بطبعها و تسليمها إلى سلطات التحقيق.
2- الإفصاح عن كلمات المرور السرية.
3- الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة .

## المطلب الثاني: الضبط و الخبـــرة القضـــائيـــة والتسرب و التنصت و إعتراض المراسلات فـــي الجريمـة الإلكتـــرونيـــة .

من أهم طرق إثبات الجرائم الإلكترونية أيضا الضبط والخبرةو التنصت و إعتراض المراسلات التي لها دورا هاما في مجال الإثبات الجنائي للأدلة الإلكترونية خاصة في ظل تزايد تطور التكنولوجيا الرقمي، فبعد انتهاء المحقق الجنائي من إجراء التفتيش يقوم بضبط الأشياء التي يراها ضرورية، ومن ثم يأتي دور الخبير الذي يقوم بالتنقيب عن الحقيقة بناء على الأشياء المضبوطة، ثم يقدم الدليل المستنبط للقاضي الذي يمكن أن يبني حكمه بناء عليه، وهذا ما سوف نعالجه من خلال الفرعين التاليين، سنتناول في الفرع الأول الضبط في الجرائم الإلكترونية، أما في الفرع الثاني الخبرة القضائية في الجرائم الإلكترونية.

### الفرع الأول: الضبـــط في الجريمة الإلكتـــرونيـــة .

باعتبار أن النتيجة المترتبة عن إجراء التفتيش هو الضبط ، ففي هذه الحالة يجب إتباع إجراءات ضبط الأشياء والأدلة الرقمية، وهذا ما سيتم توضيحه بتعريف الضبط وطبيعته ومحله في الفرع الأول، ومدى صلاحية ضبط الأدلة في جرائم الإلكترونيـة في الفرع الثاني.

[1] تنص المادة 97 من قانون الإجراءات الجزائية على "كل شخص استدعي لسماع شهادته ملزم بالحضور و حلف اليمين و أداء الشهادة مع مراعاة الأحكام القانونية المتعلقة بالسر المهنة .." فالإلتزام المفروض على الشاهد بأداء الشهادة ليس مطلقا بل ترد عليه استثناءات، فهناك أشخاص يلزمهم القانون بعدم أداء الشهادة على وقائع معينة من المؤتمنين على الإسرار كالأطباء و المحامين فيما يتعلق بالمعلومات التي يحصلون عليها بسبب مهنتهم، وموظفو الدولة بحكم مناصبهم. أو كذلك الأزواج بسبب العلاقـة الزوجية أو الأشخاص لأسباب إنسانية الذين علاقات معينة.

و يقصد بالضبط في قانون الإجراءات وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريده من حيازته وقت ضبطه كان الضبط بمثابة إجراء تحقيق، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة، فيكون الضبط بمثابة إجراء استدلال [1].

ومن حيث محل الضبط فإنه لا يرد إلا على الأشياء المادية، لأن الأشياء المعنوية لا تصلح لأن تكون محلا لوضع اليد عليها [2]، والشرط اللازم لصحة الضبط أن يكون الشيء مفيد في كشف الحقيقة فكل ما يحقق هذا الهدف يصح ضبطه كما أن الضبط لا يرد إلا على الأشياء، أما الأشخاص فلا يصلحوا محلا للضبط، وإنما المصطلح الأصح هو القبض والقبض يختلف تماما عن ضبط الأشياء [3].

ثمة صعوبة إلى اعتبار مكونات الحاسب الآلي من الأشياء التي يمكن ضبطها وبالخصوص ضبط الشبكة الإلكترونية والمكونات المعنوية للحاسب الآلي التي تشمل محتوى أنظمة المعالجة الآلية للمعطيات، وفيما يلي نلقي الضوء على مدى قابلية كل من المكونات المادية والمعنوية والرسائل ومراقبة الاتصالات الإلكترونية لأن تكون محلا للضبط.

**أولا - ضبط المكونات المادية للحاسب الآلي:** إن ضبط المكونات المادية للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته الأساسية والثانوية لا تثير أية صعوبة، لأن الضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة[4]،ومن المكونات المادية التي تكون محلا للضبط ما يلي:

وحدة المعالجة المركزية، لوحة المفاتيح والشاشة والفأرة، والأقراص والأشرطة المغناطيسية التي يقوم البعض بتخزينها في البنوك أوفي مراكز التوثيق الحكومية الأمنية، ولوحة الدوائر الإلكترونية، وأجهزة الاتصال عبر شبكة الانترنت كأجهزة المودم [5].

حيث أنه تخضع للضبط وحدة الذاكرة الرئيسية سواء كانت لقراءة البيانات، أم كانت معدة للقراءة والكتابة معا، وضبط وحدة التحكم ووحدة المخرجات وما تشمله من وسائل، كالشاشة والطابعة، وضبط وحدات التخزين الفرعية التي تشمل على أقراص ممغنطة بنوعيها المرن FLoppy disk ، والصلب Hard disk ، والأشرطة المغناطيسية Magnetic tape ، وضبط وحدة المدخلات input unit ، بما تشمله من مفردات كلوحة المفاتيح Key board ، ونظم الإدخال المرئي Machine vision system ، نظام الفأرة Mouse system ، ونظام القراءة الضوئية للحروف نظام القراءة الضوئي Optical character Reader system **. 6**

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط1 .، دار الثقافة للنشر( والتوزيع، عمان، الأردن، 2011 ،ص 168 .

[2] عبد الله حسين على محمود، مرجع نفسه، ص 397 .

[3] نفس المرجع نفسه، ص 397 .

[4] عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط . 2، منشورات الحلبي الحقوقية، لبنان، 2007 ، ص 373 .

[5] عبد الله حسين على محمود، مرجع نفسه، ص 398 -399 .

[6] هلالي عبد اللاه أحمد، مرجع نفسه، ص198 - 199

وفيما يتعلق بضبط مكونات الحاسوب المادية في القانون الجزائري فإنه لا يوجد أي مانع من تطبيقها، مثلها مثل غيرها من الماديات التي تفي النصوص التقليدية بمواجهتها موضوعيا وإجرائيا، ومن القواعد التي تتعلق بإجراء الضبط وتطبق على المكونات المادية للحاسوب هو أن الضبط يعتبر إجراء من إجراءات التحقيق، لذا فلا يجوز ضبط الأشياء إلا وفقا للقانون، وذلك بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة [1]، فيتوجب عند إحصاء الأشياء المضبوطة التي تفيد في كشف الحقيقة وضعها في أحراز مختومة، ولا يجوز فتحها إلا بحضور المتهم مصحوبا بدفاعه [2]، كما يتوجب كذلك عدم ضبط الأوراق والمستندات التي يسلمها المتهم لمحاميه أو للخبير الاستشاري لأداء مهامه.

وباعتبار أنه لا خلاف حول ضبط مكونات الحاسب الآلي المادية ومواجهتها إجرائيا بالنصوص التقليدية، فإنه توجد بعض التشريعات تضمنت صراحة النص على تفتيش المكونات المادية[3]، ومن هذه التشريعات قانون المنافسة الكندي والقانون الإنجليزي الصادر في عام 1990 والذي يطلق عليه قانون إساءة استخدام الحاسب [4].

**ثانيا- ضبط المكونات المعنوية للحاسب الآلي:**

تكمن المشكلة في الأشياء المعنوية للحاسب الآلي التي تتضمن البرامج والبيانات، ويثور التساؤل إلى مدى صلاحيتها كمحل للضبط، حيث أن البعض من الفقهاء يتجه إلى اعتبارها لا تصلح كمحل للضبط، وهذا ما ذهب إليه الفقه الألماني لوكسمبرجي، أما البعض الآخر من الفقهاء يرو ن إمكانية تطوير النصوص التقليدية للضبط على البرامج والبيانات المخزنة، لكون الغاية من التفتيش تتحقق بضبط الأدلة المادية التي تفيد في كشف الحقيقة، ومن هذا الاتجاه الفقه الكندي الذي يرى أن غرض الضبط لم يقتصر بضبط الأشياء المادية المحسوسة، بل تطور إلى أغراض أخرى منها الحصول على المعلومات والبيانات وضبطها للوصول إلى الأدلة [5].

وقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم(**04-09**) تحت تسمية" حجز المعطيات المعلوماتية"، حيث قضت المادة 06 من نفس القانون على نسخ المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية، وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات.

أما المادة **07** من نفس القانون نصت على أنه في حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة **06** وذلك لأسباب فنية، فعلى السلطة المختصة بالتفتيش القيام بالتقنيات الواجبة للمنع من الوصول إلى محتوى المعطيات أو نسخها مع الاحتفاظ بها من طرف الأشخاص المصرح لهم بذلك كذلك نص المادة **08** تعلقت بالمعطيات التي يشكل محتواها

[1] فايز محمد راجح غلاب، مرجع نفسه، ص 342،343
[2] راجع المادة 84 من قانون الإجراءات الجزائية .
[3] فايز محمد راجح غلاب ، مرجع نفسه، ص 248 .
[4] هلالي عبد اللاه أحمد، مرجع نفسه، ص 199 .
[5] عفيفي كامل عفيفي، مرجع نفسه، ص 378 .

جريمة، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهل فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة من أجل منع الإطلاع على محتوى هذه المعطيات ؛ أما المادة 09من نفس القانون، فيتضح من خلالها أن المعلومات المتحصل عليها عن طريق المراقبة وفقا لهذا القانون، لا يجوز استخدامها إلا في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به [1].

ومن خلال مضمون هذه النصوص، نجد أن المشرع الجزائري تنبه للقصور الموجود في مصطلح ضبط الكيانات المنطقية للحاسوب، حيث استخدم مصطلح حجز وليس ضبط باعتبار أن مصطلح حجز يتلاءم مع الأشياء غير المادية [2].

## الفرع الثاني: التسرب و التنصت و اعتراض المراسلات في الجريمة الإلكتـرونيـــة

**أ/- التسرب الإلكتروني :** إن تطور الجريمة من مفهوم عشوائي تقليدي إلى مفهوم منظم و متطور ، أدى بالمشرع إلى تكريس وسائل إجرائية جديدة من أجل مكافحتها ، و من بين هذه الوسائل نجد التسرب الذي نظمه المشرع الجزائري من خلال المواد من 65 مكرر11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية المعدل بالقانون 22/06 ، و الذي عرفه المشرع في المادة 65 مكرر 12 بنصها أنه :"يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية ، تحت مسؤوليته ضابط شرطة قضائية المكلف بتنسيق العملية ، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو..." ، و يطبق الإجراء على جرائم محددة حصرا في القانون و هي جرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف و كذا جرائم الفساد ، و التي يسعى العون المتسرب من ورائها إلى الكشف عن المجرمين المتوغل معهم

**ب/ التنصت و إعتراض المراسلات :** سهلت ثورة المعلومات الاتصال بين الأفراد التي انعكس أثرها على مختلف ميادين الحياة، ومن ناحية أخرى فقد سببت الكثير من أضرار شخصية عن طريق جرائم عدة مستحدثة خصوصا انتهاك أسرار الأشخاص بواسطة الوسائل الإلكترونية، ونظرا لصلة المراسلات بالحياة الخاصة للأفراد [3] عمدت الدول على حماية هذه الأسرار الشخصية عن طريق إرساء نصوص دستورية تضمن عدم الاعتداء على خصوصية المراسلات [4]، ومن بينها الدستور الجزائري الذي تضمن منع الإطلاع على المراسلات سواء كانت بريدية أو برقية أو

[1] راجع المواد من 6-9 من قانون (04-09) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المؤرخ في 05-08-2009 .

[2] فايز محمد راجع غلاب، مرجع نفسه، ص350 .

[3] علي محمود علي حموده، مرجع نفسه، ص 3 .

[4] المرجع نفسه ، ص 32 .

هاتفية وذلك في نص المادة 39 من الدستور الجزائري التي تنص على أنه "**:سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمون** [1].

غير أن القوانين الإجرائية تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية وفقا لقواعد وشروط معينة، من أجل المحافظة على حقوق المجتمع ونظام الأمن والآداب العامة، وبناء على ذلك فهل تمتد المراسلات العادية إلى سائر المراسلات الإلكترونية المستخدمة؟ [2]وهذا ما سنبينه من خلال ضبط المراسلات الإلكترونية بالنسبة للبريد الإلكتروني، **والتنصت** والمراقبة الإلكترونية لشبكات الحاسب الآلي فيما يلي:

1-البريد الإلكتروني:

يقصد بالبريد الإلكتروني استخدام شبكات الانترنت من أجل نقل الرسائل بدلا من الطرق التقليدية، وباعتبار أن استعماله سهل أضحى من أكثر وسائل الانترنت استعمالا في الوقت الحالي.

وأهم مسائل تتعلق بالبريد الإلكتروني هو وجوب المحافظة على سريته، وهو ما أدى إلى اصطناع برامج تشفير خاصة به، حيث لا يمكن الإطلاع على رسائل الأشخاص إلا لمن يعرف الشفرة .ولقد ساعد ذلك على ظهور التوقيع الإلكتروني في تيسير عملية التراسل عبر البريد الإلكتروني [3]، فالتوقيع الإلكتروني يقوم بعملية محددة ويمنح مصداقية للوثيقة أو المحرر الإلكتروني بحيث يمكن من خلال هذا إكساب الوثيقة مصداقية لدى الغير أو الطرف الآخر مستقبل هذا المحرر أو الوثيقة [4].

وبهذا الخصوص ثار خلاف حول طبيعة الرسائل الإلكترونية واختلافها على الرسائل الورقية حيث يعتبرها البعض عبارة عن موجات كهرومغناطيسية وذبذبات إلكترونية تختلف تماما على المستندات المادية الورقية، والبعض الآخر يعتبرها مستند تقليدي، فالمستند أصبح مفهومه الذي يتفق مع ثورة الاتصالات عن بعد بأنه كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو كتابة إلكترونية.وقد أسفر الخلاف الحاصل حول طبيعة الرسائل الإلكترونية ومفهوم المستند، إلى تضارب بعض الأحكام التي تجرم فعل الإطلاع عليها من طرف الغير من عدمه وفقا لما تضمنته النصوص التقليدية [5].

وبالرجوع إلى النصوص القانونية يلاحظ بأن القانون الجزائري استحدث مصطلحات تقنية جديدة في نصوص قانونية جديدة تتلاءم مع ضبط الرسائل الإلكترونية في العديد من الجرائم في حالة التلبس أو التحقيق الابتدائي، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذه النصوص خصت عن النصوص التقليدية بجوانب

---

[1] المادة 39 من قانون رقم 08- 19 المؤرخ في 15 نوفمبر 2008 ، المتضمن الدستور الجزائري المعدل والمتمم

[2] فايز محمد راجح غلاب، مرجع نفسه، ص 351 .

[3] علي محمود علي حموده، مرجع نفسه، ص33 .

[4] مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الانترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2011 ، ص196 .

[5] فايز محمد راجح غلاب، مرجع نفسه، ص352 .

تقنية تجيز بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور [1].

وهذا ما يتضح من خلال نص المادة(**65 مكرر** 5) من قانون الإجراءات الجزائية ، حيث قضت هذه المادة على أنه في حالة الضرورة لإجراء أساليب تحريات خاصة في بعض من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية، أو وضع ترتيبات تقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة أو التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص، وتتم هذه العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، أما في حالة فتح تحقيق قضائي تتم العمليات بناء على إذن من قاضي التحقيق وتحت رقابته المباشرة [2].

وكما نصت المادة (**03**) من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على ما يلي" :مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية في هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"[3] .

**2-التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:**

يقصد بمراقبة المحادثات الهاتفية وتسجيلها بأنها إجراء من إجراءات التحقيق، تباشرها السلطة المختصة للبحث عن أدلة إثبات الجريمة ضد شخص نسبت إليه ارتكابها أو لديه أدلة تتعلق بها، وكانت هذه الجريمة على درجة من الخطورة لاتخاذ مثل هذا الإجراء الاستثنائي [4].

فقد أجازت بعض التشريعات التنصت والمراقبة الإلكترونية، منها التشريع الفرنسي والذي أجاز على اعتراض الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات، وكما أجاز التشريع الهولندي لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسب الآلي إذا كان الهدف منها ضبط الجرائم الخطيرة، وكذا إمكانية مراقبة التلكس والفكس ونقل البيانات [5].

أما بالنسبة للقانون الجزائري فقد استحدث في ديسمبر سنة 2006 نصوص قانونية تتعلق **باعتراض المراسلات وتسجيل الأصوات والتقاط الصور**، والتي

---

[1] المواد من 65 مكرر -65 ( مكرر 10 من الباب الثاني من الكتاب الأول في الفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" من القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006، يتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم

[2] المادة 65 مكرر 5 قانون الإجراءات الجزائي المعدل و المتمم بالقانون رقم 02/06.

[3] المادة 03 من قانون رقم(04-09) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام لسنة 2009

[4] علي محمود علي حموده، مرجع نفسه، ص 34 .

[5] مرجع نفسه ، ص34 .، 35 .

تضمنت عدة أحكام منصوص عليها من المواد( **65 مكرر 5 إلى 65 مكرر 10**) والتي نذكرها كالتالي:

-قيام العمليات المذكورة في نص المادة( **65 مكرر 5** ) بشرط عدم المساس بالسر المهني بالنسبة لأماكن التي يشغلها أشخاص ملزمون بالمحافظة على أسرار الآخرين.

-وفي حالة اكتشاف جرائم أخرى بصورة عارضة، فلا يكون هذا سببا في بطلان الإجراءات.

-يجب أن يتعلق الإذن بجميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها

والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

-يجب أن يكون الإذن مكتوبا وسليم لمدة أقصاها ( 04 ) أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري والتحقيق.

-يجوز لوكيل الجمهورية أو لقاضي التحقيق أو لضابط الشرطة القضائية المأذون له، تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للقيام بالجوانب التقنية للعمليات المشار إليها في المادة( **65 مكرر5** ) .

-تحرير محضر من طرف السلطات المختصة بالبحث والتحري عن كل عملية اعتراض أو تسجيل للمراسلات ، وكذلك عمليات وضع الترتيبات التقنية وعملية التقاط والتثبيت والتسجيل الصوتي والسمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية ونهاية العمليات و هذا ما نصت عليه المواد 65 مكرر 11 إلى المادة 65 مكرر 18 من قانون 22/06 المتضمن ق إ ج ج و المادة 25 من ق . ع

-يوصف أو ينسخ ويودع المراسلات أو الصور أو المحادثات المسجلة في إظهار الحقيقة من طرف ضباط الشرطة القضائية المناب له ذلك، وكذلك نسخ وترجمة المكالمات الأجنبية بمساعدة مترجم يسخر لهذا الغرض [1].

غير أن هذه الأحكام لم تتضمن صراحة الرقابة على الاتصالات الإلكترونية، ومن أجل ذلك فقد شمل المشرع الجزائري فصل ثاني خاص بمراقبة الاتصالات الإلكترونية في القانون رقم (**09-04**) لسنة **2009** المتعلق بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وقد تعلقت بنوعين من الرقابة، رقابة وقائية هدفها الوقاية من الجرائم الخطيرة المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ أما الثانية فهي رقابة ضبطية قضائية تتضمن حالتين:

-الحالة الأولى، عندما يقتضي الأمر التحري والتحقيق في ذلك لاستصعاب القيام بذلك بالطرق العادية

دون اللجوء إلى المراقبة.

-الحالة الثانية، وذلك في ظل متطلبات التبادل والمساعدة القضائية بين الدول [2].

---

[1] المواد من 65 مكرر5 65 مكرر 10 من ق.إ.ج.ج.

[2] المادة 04 من القانون رقم (04-09) المؤرخ في 05 -08-2009

## الفرع الثالث: الخبـــــــرة القضـــــائيـــة في الجريمة الإلكتـــرونيـــة .

تقدم الخبرة عونا كبيرا للقضاء ولجميع جهات المختصة بالدعوى الجنائية من خلال أداء مهمتها التي بدونها يستحيل الوصول إلى رأي بشأن المسائل الفنية، والتي من خلالها يمكن التوصل إلى ظهور الحقيقة المبنية على حقائق علمية فنية والذي يعتبر العنصر المميز لها عن غيرها من إجراءات الإثبات[1] ، **و الأساس القانوني للخبرة القضائية في الجريمة الإلكترونية المواد من 143 إلى المادة 156 من قانون الإجراءات الجزائية المعدل و المتمم بالقانون 02/06 ، و المادة 03 ، و المادة 05 من قانون رقم 05/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال .**

وفي هذا المجال نتطرق إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية في الجريمة الإلكترونيـة كفرع أول و القواعد الفنية التي تحكمها كفرع ثاني، وكذا مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة كفرع ثالث.

### أولا : القواعد القانونية التي تحكم الخبرة القضائية في الجرائم الإلكترونيـة

تظهر أهمية الخبرة في مجال الجريمة المعلوماتية لتعلقها الوثيق بالحاسبات وشبكات الاتصال المرتبطة بالتخصصات العلمية والفنية الدقيقة، ومع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها، بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم [2] .

وتعد الخبرة إجراء من إجراءات جمع الأدلة بعد إحاطة الموضوع بمعلومات فنية تسمح باستنتاج والوصول إلى الدليل، فالخبرة تعتبر وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الأدلة أو تحديد مدلولها من خلال الاستعانة بالمعلومات العلمية، حيث يستند القاضي إلى الخبرة لاتخاذ القرار المناسب .

أما الخبير فهو كل شخص تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة [3].

**أ- تعيين الخبير المعلوماتي:**

إن أهم صعوبة تواجه الخبرة هي تكوين الخبير المناسب للاستعانة به، باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصة بتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية [4]، فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال الجريمة المعلوماتية بشكل خاص أن يتمتع بشروط خاصة، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادة ودراسات عليا في فرع التخصص، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفة من أجل مواكبة كل جديد

---

[1] أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة الماجستير في العلوم الجنائية، كلية 247.، الحقوق، جامعة القاهرة، 2007 ، ص256 .

[2] عبد الله حسين على محمود، مرجع نفسه، ص392 .

[3] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع نفسه، ص24 .

[4] عمر محمد أبو بكر بن يونس، مرجع نفسه، ص 1034 .

يطرأ على تخصصه لأداء مهمته [1]، فيتطلب من الخبير أن يكون ملما بالجوانب الفنية والتقنية، ومنها ما يلي:
-المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور وأكواد التشفير...الخ.
-طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة لذلك.
-المواضيع الرقمية المحتمل تواجد فيها أدلة الإثبات والصور أو الأشكال التي تتخذها.
-الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة.
-الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب على ذلك إتلافها.
-التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها [2].

وعليه فإن اختيار الخبير في مجال الجريمة المعلوماتية يتحدد بنوعية الجريمة المرتكبة، نظرا لأن الحاسبات وشبكة الاتصال ذات نماذج متعددة، وبالتالي لا يوجد خبير لديه معرفة متعمقة مع كافة أنواع الحاسبات وبرمجياتها وشبكاتها، كما أنه ليس هناك خبير قادر على التعامل مع أنواع الجرائم التي تكون هذه الوسائل الإلكترونية محلا لارتكابها أو أداة لها [3].

فقد يكون الخبير سببا لفقدان الأدلة لعدم التخصص الدقيق في المسألة التي تطلب ضرورة الخبرة وقد تحتاج إلى أكثر من خبير[4]، فيجب أن يكون الخبراء في مجال الأدلة الرقمية على وعي تام لأن أي خطأ في التفسير يؤدي إلى إتلاف أو محو الدليل الرقمي كحالة الخطأ في طريقة الحصول على الدليل الرقمي أو عدم تحريز الأدلة [5]، كما قد يتم إتلاف الأدلة بسبب خطأ الخبراء والجهة المجني عليها [6].

**ب-أنواع الخبرة في المجال المعلوماتي:**

**1-الخبرة الخاصة:**

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع نفسه، ص 26 .

[2] عبد الله حسين على محمود، مرجع نفسه، ص394-395.

[3] نفس المرجع نفسه ، ص 392

[4] عبد الله حسين على محمود، مرجع نفسه، ص 392

[5] Compagnie national des experts de justice en information et techniques Associées, la preuve numérique à l'épreuve du litige, les acteurs du litige face à la preuve numérique(l'information numérique fait la preuve), Colloque du 13 avril 2010 à la première chambre dela cour d'appel de paris ; p.28
أنظر الرابط الإلكتروني :
http://www.cnejita.org/dac/collague 20100513 Actes.PDF

[6] ومثال من اشتراك الخطأ بين الخبراء والمجني عليه، ما وقع في إحدى جرائم المعلوماتية حيث قام أحد الأشخاص في إحدى الشركات بوضع قنبلة منطقية بنظام الحاسب الآلي، وقد تم التأكد أن الشركة قبل إبلاغ السلطات المختصة قامت باستدعاء خبير للتحقق من صحة وجود القنبلة وإبطالها، وقد اكتشف الخبير القنبلة وقام بإزالة البرنامج الموضوع لها، وعندما تولت الشرطة التحقيق وجدت أن إزالة القنبلة أدى إلى إتلاف أدلة وجودها، راجع فايز محمد راجح غلاب، مرجع نفسه، ص363 .

تعتبر الخبرة الفردية من أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت فالمؤسسات الكبرى المتخصصة في هذا مجال تعمل جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الحاسب الآلي والانترنت، فهناك من الدول تقوم بمحاولة التعرف على قراصنة الذين تحولوا مع مرور الزمن إلى رموز وطنية من جراء تحركاتهم عبر الشبكة الإلكترونية [1].

**2-الجهات التعليمية:**

يمكن مواجهة الجريمة الإلكترونيــة عن طريق المؤسسات التعليمية والتي تهدف بدورها إلى تطوير العلم والقضاء المشكلات التي تواجه الإنسانية، حيث يتم تدعيمها ماديا ومعنويا حتى تكون أفضل سبيل للمواجهة، وأنشأت العديد من المؤسسات التعليمية منها دراسات الكمبيوتر في جامعة ستافرورد ومعهد التكنولوجيا في ماساشوستس والذي وَفر خبراء على درجة عالية من التفوق[2].

**3-جهات الضبط القضائي:**

قامت بعض الدول وأهمها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصة للخبرة في إجراء الخبرة على الانترنت، العابر نشاطها الإطار الدولي في هذا المجال المتمثل في منظمة الأنتربول.

حيث أن آخر نشاط مؤسسي في هذا الإطار هو الفرع الجديد الذي تأسس في المباحث الفيدرالية أطلق عليه المعمل الإقليمي الشرعي للحاسوب، وأصبح مقر خبرة عامة متعددة النواحي FBI الأمريكية القضائية هدفه مكافحة التصعيد الخطير في الجرائم المعلوماتية من خلال التصنيف والتحليل للدليل الرقمي، وأهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها [3].

**ج- مجالات الخبرة في الجرائم الإلكترونيــة:**

أفرز التطور الهائل في مجال تكنولوجيا المعلومات على العديد من الأنشطة المستحدثة، منها العمليات المصرفية الإلكترونية، الإدارة الإلكترونية والتجارة الإلكترونية، مما يقتضي تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها، من بين هذه الجرائم:

-الغش أثناء نقل البيانات أو بثها.

-التلاعب في البيانات أو في البرامج سواء الأساسية منها أو برامج التطبيقات [4].

## ثانيا : القواعد الفنية التي تحكم الخبرة القضائية في الجرائم الإلكترونيــة

تتمثل القواعد الفنية للخبرة أساسا في الوسائل الفنية التي يستعين بها الخبير المعلوماتي من أجل إظهار الحقيقة وتقدير عمله ودوره في العمل على حفظ الأدلة الناجمة عن الخبرة التقنية، والتي سنتناولها فيما يلي:

**1- وسائل الخبير في اكتشاف الدليل الإلكتروني:** نتناول في هذا الإطار الوسائل المادية والإجرائية كالتالي:

---

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس ، 2004 ، ص 1035 .

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع نفسه، ص299 .

[3] عمر محمد أبو بكر بن يونس، مرجع نفسه، ص1038 .،103

[4] علي محمود علي حموده، مرجع نفسه، ص30 .

**أ- الوسائل المادية:**

وهي الأدوات الفنية للنظم المعلوماتية التي يمكن أن تستخدم في ارتكاب الجرائم، وأهمها ما يلي:

**البريد الإلكتروني وبرامج المحادثة،** ويقصد بعنوان الانترنت **IP أ-عنوان برتوكول الانترنت** المسؤول عن تراسل كم من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ويشبه عنوان البريد العادي حيث يسمح للشبكات بنقل الرسالة وهو يوجد بكل جهاز إلكتروني مرتبط بالانترنت ويتكون من أربعة أجزاء وهي المنطقة الجغرافية، مزود الخدمة، الحاسبات الآلية المرتبطة، والرابع يقوم بتعيين الحاسب الآلي الذي تم الاتصال به [1].

وتوجد أكثر من طريقة يمكن من خلالها معرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر ، مثل ما يستخدم في حالة العمل على نظام تشغيل Windows حيث يتم كتابة WINPCFG، في أمر التشغيل فيظهر مربع حوار فيه عنوان **IP** على أنه عنوان الانترنت، وقد يتغير في كل اتصال شبكة الانترنت.

أما في حالة استخدام برامج المحادثات كأداة للجريمة، فإنه يجب تحديد هوية المتصل حتى ولو لم يدون معلوماته في خانة المرسل، وذلك بشرط أن تكون المعلومات التي وضعها أثناء إعداد بريد إلكتروني صحيحة.

**ب- البروكسي Proxy :** يعمل البروكسي كوسيط بين الشبكة ومستخدميها المستخدم البحث عن صفحة ما ضمن ذاكرة Cache المحلية والمتوفرة ، لذلك يتحقق البروكسي في حالة تنزيل الصفحة من قبل، وبالتالي يقوم بإرسالها إلى المستخدم دون حاجة الرجوع إلى الشبكة العالمية، أما إذا لم يتم تنزيلها فيتم إرسال طلب إلى الشبكة العالمية، وفي هذه الحالة يقوم البروكسي كمزود زبون ويستخدم أحد عناوين **IP** ، كما يمكن لمزود البروكسي أن يحتفظ بتلك العمليات خاصة ، لإجراء الإثبات بواسطة فحص تلك العمليات المحفوظة به [2].

**ج -نظام كشف الاختراق** ، يرمز له بأحرف **IDS** وهذه البرامج تقوم بمراقبة وتحليل بعض العمليات التي تحدث على أجهزة الحاسب الآلي أو الشبكة، من أجل البحث عن إشارات تفيد وجود مشكلة في الحاسوب أو الشبكة، وذلك من خلال تحليل مجموعة من البيانات أثناء انتقالها عبر الشبكة ببعض ملفات التشغيل التي تختص بتسجيل الأحداث فور وقوعها في الحاسب الآلي أو الشبكة، ومقارنة النتائج بمجموعة الاعتداءات الواقعة على الأنظمة المعلوماتية والتي يطلق عليها مصطلح التوقيع، بالتالي إذا تم اكتشاف النظام لوجود توقيع من التوقيعات يقوم بإنذار مدير النظام بطرق عديدة وفورية، حيث يقوم نظام كشف الاختراق بتسجيل البيانات محل الاعتداء في سجلات الحاسوب الخاصة لهذا الغرض.

**ب- الوسائل الإجرائية:** من بين الوسائل الإجرائية نجد ما يلي:

**أ-اختفاء الأثر،** إن المسجلات التي يتم نشرها في المواقع الخاصة بالمخترقين تشير دائما بنصائح مختلفة من بينها قم بمسح آثارك Cover your trachs ، وفي حالة عدم مسح المخترق لأثاره يقبض عليه، حيث يتقصى على الأثر بطرق عديدة سواء بواسطة البريد الإلكتروني الذي تم استقباله أو بتتبع أثر الجهاز الذي تم استخدامه للقيام بالاختراق،

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع نفسه، ص3

[2] نفس المرجع نفسه ، ص305

وحتى لو تمت عملية الاختراق بشكل صحيح وسليم إلا أنه يمكن القبض عليه كونه لم يقم بمسح أثاره.

**ب- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته،** من المفروض على المحقق في حالة إجرائه للتحقيق في جريمة الإلكترونية ما، أن يقوم بالإطلاع على النظام المعلوماتي ومكوناته من شبكات وبرامج، وعملياته كقاعدة المعطيات وإدارتها ومعرفة النظام والمستفيدين والإجراءات منها إجراء أمن العاملين، وكذلك عليه الإطلاع على أسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية كمراقبة المستفيدين والبرامج وتسجيل الوقائع.

**ج-الاستعانة بالذكاء الصناعي**:من الممكن الاستعانة بالذكاء الصناعي في جمع الحقائق والأسباب والفرضيات، التي يستخلص منها النتائج عن طريق معاملات حسابية يتم تحليلها بالحاسب الآلي وفقا لبرامج صممت لأجل ذلك، حيث أن تقنيات الحاسب الآلي أثبتت نجاحها وتمكنها من جمع أدلة جنائية وتحليلها واستنتاج الحقائق منها [1].

**ثالثا - عمل الخبير وأساليبه:**

تقتصر مهمة الخبير على التحقيق في الدعوى وإبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية [2] وعليه، لجمع الأدلة حول الجرائم السالفة الذكر بمعرفة الخبير المعلوماتي، يجب مراعاة القواعد الفنية المتعارف عليها في مجال الخبرة المعلوماتية ، وبالتالي يمكن للخبير إتباع الخطوات التالية في عمله:

**1-مرحلة ما قبل التشغيل والفحص:**يجب على الخبير أن يقوم بوضع نسخة أو نسخ مطابقة للأصل لوسائط التخزين المضبوطة كالقرص الصلب للقيام بعملية الفحص المبدئي وحماية الأصل من الفقدان أو التلف، وعليه التأكد من صلاحية النظام للتشغيل ومدى مطابقة محتوى الأحراز المضبوطة أثناء التحقيق بما هو مدون عليها كما يقوم بتسجيل محتوى البيانات المضبوطة كالطرز والنوع...الخ [3].

**2-مرحلة التشغيل والفحص:**يقوم الخبير في هذه المرحلة باستكمال تسجيل البيانات التي لم يتم ضبطها من خلال قراءة جهاز الحاسب الآلي، ويحدد أنواع البرمجيات كبرامج النظام، برامج التطبيقات و أي من البرامج له علاقة بموضوع الجريمة التي تحقق المعالجة فيها الصور في جرائم التزييف أو التعديل أو التلاعب...الخ مع إبراز إذا كانت مستندات أو معلومات لها دلالة بموضوع الجريمة كبصمات الأصابع في جرائم التزوير ووجود رسائل تهديد في جرائم القتل وغيرها، وكذلك ينبغي عليه اكتشاف المستندات أو النصوص المخبأة داخل الصور، وأن يقوم بتحويل الدليل الرقمي إلى مكونات مادية بواسطة طباعة الملفات أو تصوير محتواها أو وضعها وعاء حسب نوع البيانات المكونة، ويجب أن يقوم باسترجاع الملفات التي تم محوها على الأصل عن طريق استخدام أحد برامج استعادة البيانات بالنسبة للملفات والسجلات المعطلة أو التالفة وذلك باستخدام

[1] المرجع نفسه ، ص308 .

[2] محمد حسين منصور، الإثبات التقليدي والإلكتروني، د .ط.، دار الفكر الجامعي، الإسكندرية، 2006 ، ص . 254

[3] المرجع نفسه ، ص 254

برنامجEassy Recover 4 all Professional والعمل على تخزين السجلات أو البيانات والقيام بنسخ طبق الأصل من الأقراص أو الأسطوانات لفحصها [1].

**3- مرحلة تحديد مدى ترابط الدليل المادي والدليل الرقمي:**يتم في هذه الخطوة فحص الدليل المادي المضبوط مع الدليل المستخرج من جهاز الحاسب الآلي والربط بينها ليصبح الدليل موثوق ويقيني حتى يتسنى قبوله أمام المحكمة.

**4- تدوين النتائج وإعداد تقريره:**يقوم الخبير بتقديم تقرير موقعا منه لما توصل إليه من نتائج من بداية إجرائه للخبرة، وغالبا ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة وغيرها، ويقدم الملف إلى جهة التحقيق أو جهة الحكم[2] .

ومن هنا فعلى الخبير الفني أن يستخدم الأساليب العلمية المتخصص فيها من أجل الوصول إلى الحقيقة، وهناك أسلوبين لعمل الخبير التقني:

الأول: القيام بتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها مثل التهديد أو النصب أو جرائم النسخ أو دعارة الأطفال، ثم القيام بتحليل رقمي لها من أجل معرفة كيفية برمجتها وتحديد عناصر حركتها وطريقة الوصول إلى معرفتها، ومن ثم الوصول إلى معرفة بروتوكول الانترنت **IP** الذي نسب أو ارتبط بجهاز الكمبيوتر الذي صدر عنه هذه المواقع.

الثاني: تجميع وتحصيل مجموعة المواقع التي لا يمثل موضوعها جريمة بحد ذاتها، وإنما يؤدي متابعة موضوعها إلى ارتكاب الجرائم مثل المواقع التي تقوم بالمساعدة للتعرف على جرعات المخدرات أو المؤثرات العقلية أو كيفية إعداد القنابل وتخزينها [3].

**رابعا-دور الخبير التقني في حفظ الأدلة الإلكترونية:**

يتطلب لحفظ الأدلة داخل جهاز الحاسوب معرفة دقيقة لصحة البيانات الواردة في الحاسب الآلي وهذا ما يستلزم من الخبير التقني ضرورة الكشف بداية على نطاق محتوى صحة حركة الحاسب الآلي من وجود شك في صحة الأدلة المستفادة، خاصة حالة وجود الخلل أو العطب مثل الفيروس.

ومثل هذا الاتجاه نجد التشريع الإنجليزي، حيث تتم عملية حفظ الأدلة داخل جهاز الحاسوب بأساليب عديدة منها استخدام الحفظ العادي وأهمها القيام بعمليات حجز الحاسوب على الدليل الموضوع فيه، ذلك أن الدليل الرقمي هو ملف يحتوي على معطيات رقمية تبين مظهرا معلوماتيا محددا غير قابل للتحويل إلا بقيام تعديلات أو تغييرات رقمية على البيانات المذكورة.

فعملية حفظ الأدلة الرقمية تتطلب من الخبير التقني القيام بمعرفة موقع الانترنت أو المعلومات التي تشكل الجريمة، كجرائم السب والقذف في غرف المناقشة أين يتم العودة إلى ذاكرة الخادم ليقوم بربط الغرف حتى يتم التوصل إلى تحديد موضوع السب والقذف وتاريخه، أما في حالة كون الجريمة من جرائم النشر عبر الانترنت، فيتم اللجوء مباشرة إلى ذاكرة الحاسب الآلي المستخدم، وبالتالي تستدعي عمليات حفظ الأدلة من الخبير أن يقوم باستخدام البرمجيات للقيام بحفظ الأدلة الرقمية كما أنه ملزم أن يقوم بعرض الأدلة على المحكمة أو جهات التحقيق [4].

---

[1] المرجع نفسه ، ص 255

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع نفسه، ص35، ص36 .

[3] عمر محمد أبو بكر بن يونس، مرجع نفسه، ص 1043 ، ص1044 .

[4] مرجع نفسه، ص1045 .

وعليه في الأخير يمكن القول أن الجرائم المعلوماتية هي جرائم ذو طبيعة غير مادية، هذا ما أدى بإجراءات التحقيق الجنائي فيها لا تزال محل خلاف فقهي وقضائي، وبالأخص إجراءات التفتيش والضبط عن بعد، والمعاينة وكذا غياب وجود الخبير المعلوماتي المتخصص في المجال الرقمي وغيرها من إجراءات التي تثير العديد من المشكلات التي تعيق التحقيق، باعتبار أن الدليل المراد استنباطه يكون خفيا غير مرئي وأكثر من ذلك فقدان الدليل لأثاره سواء بالتلاعب أو التغيير أو الحذف، لكون الجريمة المعلوماتية مجهولة لا تصل إلى علم سلطات التحقيق والاستدلال، وهذا راجع إلى عدم اكتساب المهارة والمعرفة وعدم الخضوع للتدريبات التي تسمح للقضاة وضباط الشرطة القضائية بمواجهة تقنيات الحاسب الإلكتروني المتطورة، وكذا عدم استعانتهم بخبراء مختصين في مجال التحقيق، وهذا ما ينعكس سلبا على نفسية المحقق والمجتمع وإيجابا على نفسية الجاني، كونه على ثقة بأن السلطات التحقيق المختصة غير قادرة على إيجاد الدليل ضده وهذا ما يشجعه أكثر على ارتكاب جرائم كثيرة وخطيرة، لذا فإن متابعة إجراءات التحقيق في مجال الجريمة المعلوماتية، تحتاج إلى الأمن المعلوماتي ولرجال الضبط القضائي والقضاة المتمكنون في الأمور الفنية، والتي لن يتسنى تحقيقها إلا عن طريق التدريب والتأهيل في المجال التقني المعلوماتي.

وكل هذه الأمور لا تؤدي إلى الكشف عن الحقيقة إلا بالحصول على الدليل الإلكتروني الرقمي، الذي يقوم عليه الإثبات الجنائي في الجرائم المعلوماتية للوصول إلى الحقيقة المطلقة، **وبالتالي من المهم جدا التعرض إلى الدليل الرقمي والذي لنَا الحديث عنه في الفصل الثاني كما سيأتي.**

# الفصل الثاني :

# حجية الدليل الإلكتروني أمام القضاء الجزائي

جاء ضمن القرار الذي أصدرته غرفة الاستئناف لمحكمة الجنايات الدولية " يجب أن تستند أحكام و قرارات القضاء على وقائع مثبتة بالأدلة "[1] ، كما أن كل المواثيق و الصكوك الحقوقية الدولية ( ابتداء من الإعلان العالمي لحقوق الإنسان) أكدت على احترام حقوق الدفاع و المبادئ القانونية المتفرعة عنه كقرينة البراءة و حق المتهم في محاكمة عادلة ، و من البديهي ألا يمكن أن تحترم هده المبادئ الحقوقية الأساسية بإصدار الأحكام بالشبهة و الشك و عدم تحري اليقين الذي لا يقوم إلا بوجود الدليل أو الأدلة الدامغة التي لا يمكن ردها . بما أن طبيعة السلوك المادي للجرائم تغير ( في ما يتعلق بالجريمة الالكترونية) ، فمن الطبيعي آن إثبات هدا النوع من الجرائم يستدعي إثباتا من ذات الطبيعة ، أي أن إقامة الدليل على السلوك الذي أتاه المتهم ( الركن المادي) يرتبط حتما بنوع أو طبيعة هدا السلوك . طرحت مسالة شرعية أو مدى مقبولية نوعية الدليل أو بالأحرى طبيعته لما يكون الكترونيا باعتبار الأمر جديد ( في بداية عهد ظهور الجرائم الالكترونية . و بما أن المعروف لدينا أن هناك فلسفتين أو مدرستين في الإجراءات الجزائية و هما النظام ألاتهامي و النظام ألتنقيبي ، وجب التطرق لتقدير القضاء للدليل الالكتروني في كل منهما على حدا ، و الأهم منه توضيح ما اخذ به المشرع الجزائري و التزم به القضاء الجزائري الجزائي في هدا الشأن[2].

قسمت الأدلة الالكترونية بطرق مختلفة ( حسب المعيار المختار) ، و لعل ابرز تقسيم ذلك الذي صنفها إلى "أدلة لم تعد للإثبات " ( في الأصل) و أخرى " معدة للإثبات" ، كما قدمت في أشكال و صور مختلفة كالصور الرقمية ، التسجيلات الصوتية و النصوص المكتوبة [3] ، لكن أحسن تصنيف و الذي نرى فيه أكثر وجاهة و تبصرا لتفادي الوقوع في خطيئة الربط الحتمي بين الجريمة الالكترونية و الدليل الالكتروني لان هذا الأخير أوسع نطاقا و اشمل مجالا ، ذلك انه يستدل به في الجرائم الالكترونية بديهيا ، و لكن قد نلجأ إليه في الجرائم الأخرى ( الكلاسيكية ) كالسرقة ، القتل ، الاختلاس أو الفساد و غيرها من الأفعال المجرمة و التي ليست من الجرائم الالكترونية ، و عليه نحن أمام أدلة الكترونية خاصة بالجرائم ذات نفس الطبيعة ( الالكترونية) و أدلة الكترونية للجرائم الأخرى .

## المبحث الأول الدليل الالكتروني في النظام الاتهامي و النظام التنقيبي

كنا نجد دوما في ظل الفقه "التقليدي" وضع النظامين بصورة تقابلية ، و كان على المشرع أن يختار احدهما نظرا للاختلاف بينهما الذي قد يصل لحد التعارض

**1 قرار غرفة الاستئناف لمحكمة الجنايات الدولية بخصوص رفض دفاع "دومينيك اونغوان" لأحكام الغرفة التمهيدية للمحكمة ، الوثيقة icc-02/04-179الصادر بتاريخ 2009/02/23**

**2** بخلاف ما يعتقد خطا لدى البعض ، تجاوزنا دلك العهد الذي كان المشرع الجزائري يأخذ بالاتجاه التنقيبي فقط ، الأمر أصبح أكثر انفتاحا ، فللمشرع أن يتبنى ما شاء من المبادئ و الأدوات القانونية من هدا المذهب أو داك ، فهو غير ملزم بان يكون حبيس النظام اللاتيني أو الانجلوسكسوني .

[3] تقرير صادر عن مركز هردو لدعم التعبير الرقمي ، الجريمة الالكترونية و حجية الدليل الرقمي في الإثبات الجنائي ، القاهرة ، 2014 ، ص25.

القطري في عدة قواعد إجرائية ،فبينما يضع النظام الاتهامي الانجلوسكسوني أطراف النزاع ( المدعي المدني أي الضحية من جهة و المتهم من جانب آخر ) في وضع الصراع ، نجد النظام اللاتيني ألتنقيبي يجعل من المحاكمة صراعا بين المجتمع و المتهم ، و عليه فان هدا الأخير يهتم بأقل درجة بحقوق الدفاع و يجعل القاضي في موقع أكثر ايجابية للبحث عن الدليل ، و لهدا تبنى مبدأ حرية الإثبات ( مع قيود استثنائية) ، في حين قيد النظام الاتهامي طرق و مقبولية الأدلة الجنائية كقاعدة عامة ( في ظل استثناءات لإطلاق يد القاضي في الإثبات) .

و بما أن موضوعنا يتعلق بالدليل الالكتروني ، وجب تعريفه قبل أن نتوغل في دهاليز الاختلافات بين الأنظمة القانونية يمكن التمهيد بما جاء به

يمكننا أن نورد جملة من التعريفات التي صاغها رجال القانون لتحديد "الدليل الالكتروني" في الاصطلاح القانوني ، عرفه الدكتور اشرف عبد القادر قنديل ب " معلومات مخزنة في أجهزة الحاسوب و ملحقاتها أو متنقلة عبر شبكات الاتصال( مثل البريد الالكتروني [1] ، و التي يتم تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة بهدف إثبات وقوع الجريمة و إسنادها لمرتكبيها "[2] ، و عرف أيضا بأنه " الدليل الذي يجد أساسا له في العالم الافتراضي و يقود للجريمة "[3].كما يمكن تعريفه بأنه "الدليل المشتق من /أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة وأدوات الحاسب الآلي، أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا باستخدام برامج وتطبيقات خاصة أو تفسيرها في شكل نصوص مكتوبة ، أو رسومات أو صور أو شكاتِل وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها مما يضفي عليه طابع وسيلة إثبات جنائي"[4].

## المطلب الأول الدليل الالكتروني في النظام الاتهامي ( الانجلوسكسوني)

تأخذ التشريعات التي يغلب عليها النظام التهامي مبدئيا ( بريطانيا ، الولايات المتحدة ، كندا ، استراليا و باقي دول الكومنولث[5] بالإثبات المقيد ، أي خضوع الأدلة التي يعتد بها القاضي الجنائي لصور و إجراءات محددة على سبيل الحصر لا يمكن الخروج عنها ،و من بين الأشكال المستبعدة للدليل "الشهادة المسموعة" ( أي شهادة من

[1] عرف التشريع الفرعي الجزائري مصطلح " البريد الالكتروني" ب "خدمة تبادل رسائل الكترونية بين مستعملين " المرسوم التنفيذي 257/98 يضبط شروط و كيفيات إقامة خدمات الانترنت و استغلالها الصادر في 1998/08/25 يتمم بعض الأحكام التنظيمية للمرسوم التنفيذي 75-98 يتضمن قانون البريد و المواصلات مؤرخ في 1975/12/30.

[2] د/ اشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الالكترونية ، دار الجامعة الجديدة للنشر ، مصر، 2015 ، ص125

[3] د/ عمر محمد بن يونس ، الإجراءات الجنائية عبر الانترنت ، المرشد الفدرالي الامريكي لتفتيش و ضبط الحواسيب وصولا للدليل الالكتروني في التحقيقات الجنائية ، دون ناشر ، و.م.ا ، 2008 ،ص969.

[4] بوزيد ايغليس ، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي "دراسة تحليلية مقارنة بين القانون الجزائري و القانون المصري و بعض القوانين العربية "، دار الهدى ، الجزائر ، 2010،ص113. و انظر أيضا بلجرف سامية ، سلطة القاضي الجزائي في قبول و تقدير الدليل الرقمي ، مجلة الدراسات القانونية المقارنة ، المجلد 07 ، العدد 01 ، سنة 2021 ،ص281.

[5] منظمة دولية حكومية تتكون من 54 دولة تشترك تقريبا جميعها في كونها مستعمرات بريطانية سابقة .

سمع الواقعة و لم يشهدها عيانا ) و نظرا للتقارب بين الدليل الالكتروني و الشهادة المسموعة ، أثيرت إشكالية مقبولية الدليل الالكتروني لدى القضاء الجنائي في ظل النظام الاتهامي ، لكن اعتبر الإثبات الالكتروني كأحد الاستثناءات عن قاعدة استبعاد الشهادة المسموعة[1] .

**الفرع الأول الدليل الالكتروني في ظل الإثبات المقيد**

يعتبر الدليل الالكتروني في النظام القانوني الانجلوسكسوني من قبيل "الشهادة المباشرة" و على أساس انه استثناء عن "قاعدة شهادة السماع" كما أسلفنا ، و قد تبنى المشرع الأمريكي قاعدة في مجال "الإثبات الجنائي" تسمى **قاعدة الدليل الأفضل** الذي نصت عليه المادة 1002 من قانون الإثبات الأمريكي ، و مقتضاه انه ينبغي لأطراف الدعوى الجنائية أن يقدموا الأصل لا الصورة التي لا تقبل إلا بتوفر الأصل في الأدلة الكتابية أو التسجيلية ، إلا إذا نص قانون خاص على خلاف دلك . بظهور الدعائم الالكترونية ، وجد القضاء ( في النظام الانجلوسكسوني طبعا) نفسه أمام عائق لتطبيق هده القاعدة مع الدليل الالكتروني الذي وفق المفهوم التقليدي للمستند القانوني لا يعدو أن يكون إلا نسخة و ليس الأصل ، فأصبح المشرع مضطرا لتبني ما يمكن من الملاءمة الضرورية لقبول هدا المنهج الجديد في الإثبات [2].

وسع التشريع الأمريكي في نطاق مفهوم الكتابة و التسجيلات بضم الحروف ، الكلمات أو الأرقام أو ما يعادلها من الرموز الاصطلاحية ، و هكذا أصبح تقدير الصورة "الافتراضية" ( الكهرومغناطيسية) كصورة أصلية للمحرر و بالتالي عدم تعارض الدليل الالكتروني مع مبدأ " الدليل الأفضل" . بالنسبة للتشريع البريطاني ، تبنى مقبولية الصور المطابقة للأصل للمحررات أو جزء منها كدليل يحل محل المحرر الأصلي من خلال ما نصت عليه المادة 27 من قانون العدالة الجنائية لسنة 1988 [3].

**الفرع الثاني شروط قبول الدليل الالكتروني في النظام الاتهامي**

باعتبار هدا النظام يتبنى قواعد صارمة في قبول طرق و وسائل الإثبات الجنائي ، لم يدع خروجه عن الأصل العام "عدم قبول الشهادة الصوتية" دون ضوابط و شروط ، حيث اخضع المشرع البريطاني قبول الدليل الالكتروني لشروط نصت عليها المادة 69 من قانون الشرطة و الإثبات الجنائي لسنة 1984 ، يمكن أن نحصرها فيما يلي:

ا/ غياب مسوغات تدعو لاعتبار المستند الالكتروني لا يتوفر على الدقة بفعل الاستخدام غير الطبيعي أو الخاطئ للحاسوب .

[1] د/ اشرف عبد القادر قنديل ، مرجع نفسه ، ص201

[2] المرجع نفسه ، ص203.

[3] المادة 27 من قانون العدالة الجنائية البريطاني لسنة 1988.

ب/ سلامة اشتغال الحاسوب في كل المراحل ، و في حالة المخالفة ، عدم تأثير الجزء المعطل عن استخراج المستند أو دقة محتواه.

ج/ استجابة المستند لكل شروط القواعد الجوهرية للمحاكمة [1].

إلى جانب الشروط التي نص عليها القانون ( الإثبات الجنائي لسنة 1984) الواجب توفرها في الدليل الالكتروني ، نص أيضا على معايير التقدير و التقييم لصحة المستند المستخلص من الحاسوب [2].

نصت المادة 29 من قانون الإثبات الكندي بدورها على شروط قبول القضاء للمحرر الرقمي ، و التي يمكن تلخيصها في :

ا/ أن يكون الدليل صورة حقيقية من المدخل الأصلي .
ب/ أن تتضمن النسخة المقدمة للقضاء وصفا كاملا لنظام حفظ السجلات السائد في المؤسسات المالية[3].

## المطلب الثاني : الدليل الالكتروني في النظام التنقيبي

يتميز النظام التنقيبي في الإجراءات الجزائية بحرية الإثبات ( مقارنة بالنظام الاتهامي ) ، و يدعى أيضا ب"نظام الأدلة الاقناعية" ، بحيث يكون للقاضي سلطة أوسع في تقديره و مدى قبوله للدليل . و من أهم التشريعات التي يغلب على نظامها الإجرائي المذهب التنقيبي كل من الجزائر [4] ، مصر و فرنسا . غير أن كلامنا لا يفيد حتما خلو القواعد الإجرائية في هده الأنظمة ( تشريعات الدول المشار إليها) من مظاهر النظام الاتهامي . و على القاضي الخاضع لقواعد الإجراءات التنقيبية أن يبادر للبحث عن الدليل وعدم الاكتفاء بفحص وسائل الإثبات التي يقدمها الأطراف ( نيابة عمومية أو المتهم) ، كالأمر بتفتيش الحاسوب[5].

### الفرع الأول الدليل الالكتروني في ظل "حرية الإثبات"

تبنت المواد 212 من قانون الإجراءات الجزائية الجزائري ، 291 من ق.ا.ج مصري و المادة 342 من ق.ا.ج فرنسي على مبدأ حرية الإثبات في المادة الجزائية و التأكيد على مبدأ " القناعة الشخصية للقاضي" ، و التي لا يمكن تصور تكونها إلا بإقامة

[1] المادة 69 من قانون الشرطة و الإثبات البريطاني لسنة 1984 .
[2] رغم أن كيفية استخلاص المستند من الحاسوب هي من صميم عمل الخبير في الإعلام الآلي ، و رغم أهمية الخبرة في عمل تقني كهذا ، أبى المشرع البريطاني إلا أن يضع ضوابط مرشدة للقاضي الذي يبقى المسؤول الأول عن عدالة الحكم و كذلك كضمانة للمتقاضين لرقابة قبلية للخبرة و عدم إخلالها بواجب العدالة و الإنصاف .
[3] عبد العالي هلالي عبد الإله احمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، الطبعة الأولى ، دار النهضة العربية ، مصر ن 1997 ،ص55.

[4] الفقرة الأولى من المادة 212 من قانون الإجراءات الجزائية الجزائري .
[5] عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة للنشر ، مصر،2010 ،ص194 . وانظر أيضا بن فردية محمد ، الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائي ( دراسة مقارنة ) ، Revue académique de la recherche juridique , vol, n°1,p.282. 5.

الأدلة اليقينية ، خاصة إذا كان الدليل للإدانة ( أي مقدم الدليل هو النيابة العمومية) طبقا لقاعدة " تفسير الشك لمصلحة المتهم"[1].

يتناول الفقه الفرنسي حجية المستند المستخرج من الحاسوب في الإثبات الجنائي ضمن ما يعرف ب "الأدلة العلمية " سواء تعلق الأمر ببيانات كتابية آو صور ، و عليه اعتبر بان للتسجيلات الممغنطة قيمة الأدلة المفترض فيها الوثوق و بالتالي مقبولة للإثبات أمام المحاكم الجزائية ( جنح و مخالفات ، جنايات و أقطاب جزائية ) .
رغم إجماع التشريعات التي يغلب عليها النظام التنقيبي على قبول الإثبات بالمستند الرقمي ( الالكتروني ) نظرا لما يميزه من عناصر موضوعية علمية تساعد القاضي في الاقتناع بما يحتويه من معطيات بتبرئة المتهم أو بإقامة دليل إدانته ( حسب الحالة )، إلا أنها تختلف في أساليب تقديم المحرر الرقمي أمام الهيئة القضائية الجزائية المختصة[2].
يكون للقاضي الذي ينظر في الدعوى العمومية تقديره للدليل ، فهو عمل يأتي بعد دور الخبير الذي يقدم رأيه فيه ، و مع دلك يبقى القاضي هو الذي يتحمل مسؤولية إقامة العدل و إصدار حكم منصف ، فتقديره و بناء قناعته بناء على الدليل الرقمي الموضوع بين يديه هو المرحلة الفاصلة و الأهم لما سيرتب من نتائج ( تبرئة أو إدانة )، و مهما كانت القيمة العلمية للدليل الالكتروني تبدو قاطعة [3]، لا يعني دلك أن القاضي مجبر على تأييد ما تقول به الخبرة دون أن يتعمق في جمع معطيات تتصل بملابسات و حيثيات و بيئة هده المستندات الالكترونية و ظروف استخراجها و جمعها ، لان صدقها ليس أمرا مسلما به و إلا ما حاجتنا للقاضي ؟[4].

**الفرع الثاني ضوابط اقتناع القاضي بالدليل الالكتروني**

لا يعني مبدأ " حرية الإثبات" في النظام التنقيبي ترك مسالة قبول الدليل على عواهنها ، بل اتساع نطاق السلطة التقديرية للقاضي في ظل هدا النظام مقارنة بالنظام الاتهامي ، حيث يبقى القاضي خاضعا للقانون رغم استقلاله عن السلطتين التنفيذية و التشريعية ( المفترض ) ، و هدا ما نص عليه الدستور الجزائري بمقتضى نص المادة 163 في فقرتها الثانية " القاضي مستقل ، لا يخضع إلا للقانون " ، كما اخضع المؤسس الدستوري عمل القاضي لضمانة تمكن جهات الاستئناف و خاصة قاضي النقض (باعتباره قاضي قانون) من ممارسة رقابة " مدى قانونية الحكم أو الأمر أو القرار

[1] O.Nober , L'encadrement du raisonnement du juge des faits au sein du procès pénal ,mémoire de maitrise en Droit ,université Laval ,Canada ,2017,p.30.
[2] A.E.C Tamano ,l'admissibilité de la preuve électronique devant les tribunaux ,p.47 : https ://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_fr.pdf.
[3] د/ جميل عبد الله ، حجية مخرجات الكمبيوتر في المواد الجنائية ، دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية .و انظر أيضا الحسن الطيب عبد السلام الحضيري ، الإثبات الجنائي بالوسائل العلمية الحديثة ( دراسة مقارنة بين القانون الجنائي الليبي والفقه المعاصر ) ، رسالة ماجستير ،جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج ،اندونيسيا ، فيفري 2016 ، ص.127 .
[4] - د/ جميل عبد الباقي الصغير ، الانترنت و القانون الجنائي ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، الطبعة الأولى ، دار النهضة العربية ، مصر،2001 ،ص.23.

القضائي " من خلال مبدأ دستوري أيضا ، و هو خضوع الأحكام و الأوامر و القرارات القضائية للتسبيب ، أي على القاضي آن يعلل موقفه [1] .
يمكن أن نوجز ضوابط بناء موقف القاضي على الدليل الالكتروني في ما يأتي :

**أولا – الضوابط العامة**

**ا/أن تكون النتائج المستخلصة من الدليل الالكتروني تتفق مع المنطق السليم و مع القانون**

فلا يمكن للقاضي قبول محرر رقمي يخرق النواميس و القوانين الطبيعية المعروفة أو يستند لخرافات و هرطقة لا تحترم صحيح العلم ، إضافة لشرط عدم تعارض محتوى الدليل مع المبادئ القانونية الجوهرية التي يتبناها النظام القانوني للبلد ، و هدا ما ثبت عن غرفة الجنح و المخالفات بالمحكمة العليا[2].

**ب/ أن تكون مجمل الأدلة متساندة :**

و معنى تساند مجموع أو مجمل الأدلة هو أن تكون تخدم بعضها بعضا و تؤيده ، لا أن يهدم جزؤها كلها أو قليلها كثيرها ، إذ يقع على القاضي تقديرها ( تقدير ما تثبته) مجتمعة لا منفردة[3].

**ج/ أن يكون الدليل قد تمت مناقشته خلال إحدى الجلسات على الأقل**:

لا يمكن للقاضي أن يؤسس منطوق حكمه مستندا لوسيلة إثبات لم تتعرض للمناقشة من أطراف الدعوى الجزائية تماما ، و هو ما يعرف في الاصطلاح القانوني " مبدأ وضعية الدليل " و هو احد ضمانات مبدأ "**الوجاهية**" و مبدأ " **احترام حقوق الدفاع**" الضروريان لإقامة محاكمة عادلة لا تخل بحقوق المتقاضين .
كرست الغرفة الجزائية الثانية للمحكمة العليا بالجزائر المبدأ من خلال ما ضمنته لأحد قراراتها ، حيث أكدت على " يتعين على قضاة المجلس أن يبينوا في قراراتهم أدلة الإثبات التي أدت إلى اقتناعهم ، و أن هده الأدلة قد تمت مناقشتها حضوريا و إلا ترتب عن دلك النقض "، إلى جانب قرار آخر عن نفس الهيئة جاء فيه " من المقرر قانونا انه لا يسوغ لقضاة الاستئناف أن يبنوا قضاءهم بالإدانة إلا على الأدلة المقدمة لهم أثناء المرافعات و التي حصلت المناقشة فيها حضوريا أمامهم "[4].

**د/ خضوع الدليل للقانون الساري وقت إعداده**

تنص المادة 08 من القانون المدني الجزائري على " **تخضع الأدلة المعدة مقدما للنصوص المعمول بها في الوقت الذي اعد فيه الدليل ، أو في الوقت الذي كان ينبغي فيه إعداده** " [5]، و تعتبر هذه القاعدة إحدى صور الخروج عن مبدأ " **القانون الأصلح للمتهم**" .

---

[1] المادة 169 من الدستور الجزائري 2020 .
[2] قرار صادر عن غرفة المخالفات و الجنح للمحكمة العليا في الملف رقم 37941 بتاريخ 1987/05/07.
[3] خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت ، الطبعة الأولى ، دار الثقافة للنشر و التوزيع ، الأردن ،2011 ، ص352.
[4] المجلة القضائية للمحكمة العليا ، العدد الرابع ،سنة 1990 ، ص214.
[5] القانون 05-10 مؤرخ في 20 جوان 2005 يعدل و يتمم القانون المدني الجزائري .

إن وجود النص ضمن القانون المدني لا يعني عدم سريانه على المواد الجزائية لأنه جاء ضمن قواعد قانونية تعتبر الشريعة العامة للإجراءات في المنظومة التشريعية الجزائرية ، و ما دام لم يرد ما يناقض هذه القاعدة ضمن قانون الإجراءات الجزائية أو قانون العقوبات ، فإنها تبقى صالحة بالنسبة للأدلة في الإثبات الجنائي و المدني على حد سواء .

نصت المادة 302 من قانون الإجراءات الجنائية المصري على " **و مع ذلك لا يجوز له ( المقصود هو القاضي) أن يبني حكمه على دليل لم يطرح أمامه في الجلسة** " ، و قد كان لمحكمة النقض المصرية عدة قرارات أكدت فيها على المبدأ ( ضرورة أن يكون محل نقاش في الجلسات ) في مناسبات عديدة[1]. و حتى يتوفر شرط وضعية الدليل يجب أن يتحقق :

ا/ تمكين أطراف الدعوى من الدليل ( محتواه و ليس الدليل نفسه ) لإمكانية الرد عليه .

ب/ أن يكون للدليل أصل في ملف الدعوى ( الدليل ذاته ) و الشرط ضروري لتمكين جهة النقض من التعقيب على قانونية المستند[2].

**ثانيا- الضوابط الخاصة بالدليل الالكتروني**

إضافة لما ينبغي أن يتوفر في الدليل ضمن نظام الإثبات الحر ، يجب أن يكون المستند الالكتروني متوفرا على بعض العناصر الضرورية كي يستدل به القضاء للفصل في الدعوى ، لذلك يقع على "خبراء" الإعلام الآلي احترام بعض المبادئ و القواعد القانونية لدى استحضارهم المخرج البياني للحق المدعى به:

ا/ احترام قواعد حفظ البيانات أو المعلومات ( التشريع الألماني و اليوناني ).

ب/ الاحترام التام و المراعاة الشديدة لخصوصية المراسلات ( التشريع الجزائري [3]، الفرنسي و لوكسمبورغ ).

ج/ استعمال أجهزة متطورة و نظام تشفيري حديث ( التشريع الايطالي ).

د/ الحصول على عقد توثيقي للنسخة الأصلية ( لدى موثق و شهادة شخصين على الأقل ، التشريع الاسباني و الروماني )[4].

---

[1] قرار صادر عن محكمة النقض المصرية رقم 360 بتاريخ 1976/06/06 و قرار أخر صادر عن ذات الهيئة رقم 929 بتاريخ 1992/10/13.

[2] مأمون محمد سلامة ،الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية ،مصر ، 2000 ، ص182.

[3] الفقرة 2 من المادة 47 من الدستور الجزائري و المادتان 65 مكرر 5 و 65 مكرر 7 من قانون الإجراءات الجزائية الجزائري .

[4] A.E.C Tamano , op cit , p.58.

## المبحث الثاني الدليل الالكتروني في النظام القانوني الجزائري

حتى و إن كان المشرع الجزائري يأخذ بالنظام التنقيبي كأصل عام في الإجراءات الجزائية ( قاضي التحقيق مثلا ) ، إلا أن هدا لا يمنع من الأخذ ببعض القواعد الإجرائية من النظام الاتهامي لدى الضرورة ، و لعل ابرز مثال ما جاءت به المادة الأولى من قانون الإجراءات الجزائي الجزائري التي منحت للضحية حق تحريك الدعوى العمومية[1] ( في النظام التنقيبي الصرف ينحصر حق التحريك في يد النيابة العمومية فقط ) ، و في ضوء ما سبق ، يمكن القول بان المشرع الجزائري و رغم تأثره الشديد بالنظام التنقيبي ، إلا انه يأخذ بنظام **"مختلط "** ، لهدا وجب التطرق لقيمة و مقبولية الدليل الالكتروني في التشريع الجزائري رغم تسليطنا الضوء على الأمر في كلا النظامين .

بما أن المشرع الجزائري اخذ بوسيلة ارتكاب الجريمة ( أنظمة المعالجة الآلية للمعطيات ) كمعيار لتحديد الاصطلاح القانوني ل"الجريمة الالكترونية "[2]، سيكون من المسلمات اعتماد القضاء الجنائي الجزائري على الدليل الالكتروني ( تواؤم طبيعة الدليل مع طبيعة الجرم ) لإثبات الإدانة أو التدليل على البراءة .

و للتطرق بصفة واضحة و دقيقة لمكانة الإثبات الالكتروني ضمن منظومتنا القانونية و القضائية ، لا مناص من استعراض النصوص القانونية التي تضمنت الموضوع قبل تقديم ملامح أو مظاهر الممارسة القضائية الجزائرية في ذات الصدد .

### المطلب الأول : الأدوات التنفيذية و التشريعية للدليل الالكتروني في الجزائر

يقتضي مبدأ الشرعية و كل مبادئ الحقوق التي لقيت تعاقدا اجتماعيا بمقتضى الدستور الجزائري إلا توكل مهمة الضبط القضائي إلا لمن تتوفر فيهم الشروط القانونية الضرورية لسلامة العملية التي تراعي حق المجتمع ( من خلال النيابة العمومية ) في ردع الجريمة لتوفير الأمن و السكينة العموميين لاستقرار حياة الجماعة من جهة و حق المتهم في الدفاع عن نفسه لإثبات براءته على اعتبار أن الخطأ وارد في أي عمل بشري ، اقتدى المشرع الجزائري بغيره في هذا المجال موكلا مهمة الضبط للقضائي لأجهزة و أعوان و ضباط مختصون ، لا يباشرون أعمالهم إلا باستيفاء الشرط القانونية لذلك[3].

بما أن الجريمة الالكترونية هي إحدى الجرائم التي تناولتها نصوص قانون العقوبات و بعض القوانين الخاصة ( مذكورة في هذه المذكرة ) ، فان سياق التطرق للدليل الالكتروني لن ينقلنا خارج هذه الأدوات " التشريعية" و الأحكام و الأوامر و

[1] الفقرة 2 من نص المادة الأولى من قانون الإجراءات الجزائية الجزائري .

[2] المادة 02 من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] المواد من 12 إلى غاية 28 من الأمر 66-155 المتضمن قانون الإجراءات الجزائية الجزائري .

القرارات القضائية الصادرة عن الجهات القضائية الجزائرية في مختلف مستوياتها ، سواء تلك التي تمثل مظاهر " مبدأ التقاضي على درجتين" [1]،أو محكمة الجنايات ، أو الاجتهاد القضائي الصادر عن جهة النقض[2].

## الفرع الأول الأدوات التنفيذية و التشريعية الجزائية للأدلة الالكترونية في الجزائر

يمكن للمتهم أن يقدم مستندا ذو طبيعة افتراضية لإثبات براءته من التهمة الجنائية الموجهة له احتراما لمبدأ " احترام حقوق الدفاع" و هو ما اقره الدستور الجزائري في(مادته 175)[3]، إذ تنص على **" الحق في الدفاع معترف به "** ، لكن محور اهتمامنا في هذا المقام يتعلق بالهيئات الحكومية الرسمية المكلفة بجمع الأدلة الالكترونية لإدانة أو تبرئة المتهم ، فمن غير المعقول أن توكل مهمة خطيرة على منظومة الحقوق في المجتمع و على النظام العام لغير الجهات المختصة و المكونة تكوينا يجمع بين المعرفة التقنية للإعلام الآلي واليات الاتصال و كذلك الدراية القانونية في ذات الوقت .

### أولا – الهيئات المختصة بجمع الأدلة الالكترونية في جهاز الشرطة الوطنية :

في إطار تنفيذ الدولة الجزائرية لالتزاماتها التعاقدية الدولية بمقتضى تصديقها على اتفاقية "بودابست" [4]، بادرت المديرية العامة للأمن الوطني بإنشاء وحدة مختصة في مجال مكافحة الجريمة الالكترونية . منذ مطلع عام 2003 بدأت السلطات الأمنية الشرطية في الجزائر عمل تنسيقي مع الدول الأوروبية ، و كانت البداية بإرسال أكثر عدد من ضباط الشرطة للتكوين في مجال التحقيق الجنائي المتعلق بالجرائم الالكترونية ، أعقبتها عملية إشراف فرنسي على تكوين 22 ضابط جزائري سنة 2005[5].

اهتمت المديرية العامة للأمن الوطني الجزائري بتكوين الضباط و أعوانهم في مجال مكافحة الجريمة الالكترونية ، و بطبيعة الحال كان التكوين يضم تعلم قدرات و كفاءات التحري الجنائي و بالتالي كيفية جمع الأدلة و وسائل الإثبات المتعلقة بهذا الصنف من الأفعال المجرمة ، كما عمدت المديرية لإحداث إعادة هيكلة لجهاز الشرطة أسفرت عن إنشاء مصالح مختصة بمكافحة الجريمة الالكترونية .

**ا- على الصعيد الجهوي:** تكوين مخابر مجهزة بالوسائل التكنولوجية المساعدة في الإثبات الجنائي في العاصمة ، قسنطينة و وهران بها أقسام خاصة بالبحث الجنائي الرقمي تختص بالتحري و البحث في الجرائم الرقمية و استخراج الأدلة الالكترونية لاستعمالها في المتابعة الجزائية لهذه الجرائم[6].

---

[1] أقسام الجنح و المخالفات على مستوى المحاكم الابتدائية و الغرف على مستوى المجالس القضائية .

[2] المحكمة العليا طبقا لنص الفقرة 3 من المادة 179 من الدستور الجزائري (2020).

[3] المادة 175 من الدستور الجزائري (2020) .

[4] أول معاهدة دولية تهدف للتصدي للجرائم الالكترونية سواء للحاسوب المعزول أو الانترنت عن طريق خلق انسجام و توحيد ( على الأقل تقريب ) المعايير بين التشريعات الوطنية .

[5] بوخبزة عائشة ، مرجع نفسه ،ص246 ، ص247.

[6] https://www.algeriepolice.dz

**ب – على مستوى المحلي (الولايات)** :استحداث 23 خلية عمل ميداني ( عملياتي ) في يناير من سنة 2010 على صعيد مصالح الشرطة القضائية للولايات :08 خلايا بالوسط ، 08 بالشرق ، 06 لولايات الغرب و خلية واحدة بالجنوب الكبير[1] .

**ثانيا- الأجهزة المكلفة بالأدلة الالكترونية على مستوى الدرك الوطني**

على غرار قطاع الشرطة الوطنية ، بادر جهاز الدرك الوطني- باعتباره جهازا امنيا تابع لوزارة الدفاع و يتعامل مع امن الأشخاص و الممتلكات في ذات الوقت – إلى تطوير هياكله و أدواته في التعاطي مع الجرائم الالكترونية قصد تبني منهجية أكثر نجاعة و فاعلية ، و في هذا الصدد أنشأت القيادة العامة للدرك الوطني مصالح مختصة للنظر في هذه الجرائم و بالضرورة هي المنوط بها جمع الأدلة حولها .

**ا- المصلحة المركزية للتحريات الجنائية ( service central des investigations criminelles) :** جهاز له اختصاص وطني في مكافحة الجرائم المنظمة ، الجرائم الاقتصادية الكبرى و الجرائم الالكترونية .

**ب- المصالح الجهوية للشرطة القضائية:** تسند لها مهام التنسيق بين مختلف وحدات الشرطة القضائية التابعة للدرك الوطني ( على مستوى كل الكتيبات ) إضافة إلى تقديم الدعم اللوجيستيكي و التقني لها في مجال التحري و البحث عن الأدلة الجنائية .

**ج- فصائل الأبحاث :**وهي وحدات موجودة سابقا في جهاز الدرك الوطني ، غير أنها عرفت إعادة هيكلة لتطويرها و تمكينها من التأقلم مع التطور في أساليب الإجرام ، من خلال استحداث أفواج مختصة في التصدي للجرائم الاقتصادية الكبرى و جرائم الانترنت[2].

**د- المعهد الوطني للأدلة الجنائية و علم الإجرام:** جهاز امني تابع لوزارة الدفاع الوطني ، يشرف عليه قائد الدرك الوطني بتفويض من وزير الدفاع ، يضطلع بمهام تقديم الخبرات العلمية التقنية في مجال البحث و التحقيق الجنائي بناء على طلب القاضي المختص [3]، كما كلف بإنشاء بنك معلومات ( قاعدة بيانات ) ، ز انجاز أبحاث في مجال التحقيق الجنائي خاصة ما تعلق منها بالتكنولوجيا الدقيقة .

**ثالثا – الهيئة الوطنية للوقاية من جرائم الإعلام و الاتصال** :أنشا القانون 09-04 من خلال مادته 15 جهازا يختص بالوقاية من الجرائم الالكترونية و مكافحتها ، حددت المادة 14 من ذات القانون على صلاحيات هذا الجهاز بنصها "تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام التالية :

---

[1] ارزقي سي حاج محند ، الإثبات الالكتروني في المادة الجزائية ، مداخلة ضمن ندوة "وسائل الإثبات الحديثة" ، مركز البحوث القانونية و القضائية ، 2015/02/05 .

[2] التعليمة رقم 2007-223-04 الصادرة عن ديوان قيادة الدرك الوطني الجزائري بتاريخ 2007/07/21.

[3]المرسوم الرئاسي 183/04 المؤرخ في 2004/06/26 المتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك و تحديد قانونه الأساسي ، ج.ر عدد41 الصادرة في 2004/06/27 المعدل و المتمم بمقتضى المرسوم الرئاسي 118/09 الصادر في 2009/04/14 ، ج .ر عدد 24 الصادرة في 2009/04/22.

ا- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بشبكة الإعلام و الاتصال و مكافحتها[1].
ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية .
ج- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم[2].

فالهيئة الوطنية منوط بها دور التنسيق مع الجهات القضائية و الأمنية الدولية في إطار تنفيذ اتفاقيات التعاون الدولي [3]باعتبار الجريمة الالكترونية "عابرة للحدود بامتياز" بطبيعتها لأنها غير محصورة بعامل الجغرافيا خاصة بفعل الشبكة المعلوماتية العنكبوتية.

نص الفصل الخامس من القانون 09-04 -المتضمن القواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال – على إنشاء هيئة وطنية للوقاية من الجرائم المعلوماتية (الالكترونية) ، نصت المادة 14 من القانون 09-04 على مهام هذه الهيئة الوطنية إلى جانب ذكر اختصاصاتها ضمن نص المرسوم الرئاسي 261/15- المحدد لتشكيلة و تنظيم و كيفيات تسيير هذا الجهاز – المعدل و المتمم بمقتضى المرسوم الرئاسي 172/19 المعدل للمرسوم السابق بالإلغاء ( تعديل جوهري بنقل الوصاية عن الجهاز من وزارة العدل في المرسوم الأول إلى وزارة الدفاع في الثاني ، و هو أمر ينقص من الطبيعة القانونية البحتة للهيئة و يضفي عليها صبغة أمنية صرفة)[4].

من بين الأدوات التنفيذية للهيئة الوطنية للوقاية من الجرائم الالكترونية "مديرية تقنية " اسند لها من ضمن الأدوار مهمة تقديم الخبرات القضائية ( بطلب من القاضي الجزائي المختص ) في مجال الجرائم الالكترونية ، تفتيش نظم المعالجة للمعطيات ، اعتراض المراسلات السلكية و اللاسلكية و حجز المعطيات ذات المحتوى المجرم بمقتضى التشريع الوطني [5].

**خامسا – المكتب المركزي الوطني لانتربول الجزائر**

---

[1] عرفت الفقرة 9 من المادة 08 من القانون 2000-03 –يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية ، الصادر في 2000/08/05 ، ج.ر عدد 48 الصادرة في 2000/08/06- شبكة المواصلات السلكية و اللاسلكية ب" كل منشاة أو مجموعة منشات تضمن إما التراسل و إما تراسل و إرسال إشارات المواصلات السلكية و اللاسلكية و كذا تبادل معلومات التحكم و التسيير المشتركة ما بين النقاط الطرفية لهذه الشبكة ".

[2] المادة 13 من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

[3] بوخبزة عائشة ، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماجستير ، تخصص قانون جنائي ، كلية الحقوق ، جامعة وهران ، 2013 ، ص255

[4] المرسوم الرئاسي 261/15 مؤرخ في 2015/10/08 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج.ر. عدد 53 الصادرة في 2015/10/08 المعدل ب المرسوم الرئاسي 172/19 الصادر في 2019/06/06 ، ج.ر.عدد 37 المؤرخة في 2019/06/09.

[5] الفقرة 02 من المادة 12 من المرسوم الرئاسي 172/19.

يعد الحقل الأمني من أكثر المجالات خصوبة لإعمال التعاون الدولي ، خاصة بالنسبة للجرائم العابرة لحدود الدولة الواحدة ، و لما كانت الجرائم الالكترونية من أكثر الأفعال المجرمة التي يسهل على مرتكبيها ضم أكثر من عنصر وطني ( توفرها على مقومات الجريمة الدولية بفعل صعوبة حصرها في نطاق جغرافي لدولة بعينها ) ، و لتحقيق هذا النوع من التعاون تم إنشاء المنظمة الدولية الحكومية **" الانتربول"** سنة 1963 و هي سنة انضمام الجزائر لها ( في أوت 1963) .

يعمل المكتب المركزي الوطني لانتربول الجزائري تحت إشراف مديرية الشرطة القضائية التابعة مباشرة للمديرية العامة للأمن الوطني ، ومن ابرز اختصاصاته إدارة مكافحة الجريمة المنظمة ، و التي تعتبر الجرائم الالكترونية أهم أشكالها في ظل تطور الأداة المعلوماتية ، ففضلا عن ملاحقة العصابات الإجرامية ، يلعب المركز دورا رئيسيا في تجميع المعلومات العملياتية و تقديم المساعدة التقنية[1].

**الفرع الثاني الدليل الالكتروني في النصوص التشريعية الجزائرية**

تنص المادة 167 من الدستور الجزائري على مبدأ الشرعية صراحة ، و هو المبدأ الذي تضمنه نص المادة الأولى من قانون العقوبات في فحواه ، بحيث لا يمكن أن يتعرض أي شخص لمتابعات أو عقوبات جزائية ما لم يقع فعله تحت طائلة نصوص قانونية سارية المفعول على الإقليم الجزائري سواء بمقتضى قانون العقوبات ، قانون الإجراءات الجزائية ، أو أي نص تشريعي أو تنظيمي يجرم الفعل المنسوب للمتهم[2].
نجد الركن الشرعي للجريمة الالكترونية ( باعتبار الركنين المادي و المعنوي سبق لنا التطرق لهما ) في نص المواد من المادة 394 مكرر إلى المادة 394 مكرر7 من قانون العقوبات الجزائري .
تضمنت مختلف الفئات النصية التشريعية السارية المفعول على إقليم الدولة الجزائرية و مواطنيها قواعد مرتبطة بالحماية الجزائية من الجرائم الالكترونية ، و بالتالي علاقتها بالدليل الالكتروني .

**أولا- الدستور الجزائري**

كفلت الدساتير الجزائرية القدر اللازم من سقف الحقوق الأساسية الفردية منذ دستور 1989 إلى غاية دستور 2020 [3]( لا يتسع المقام لانتقاد دستوري 1963 و 1976 ، فيكفي أنها كانت في ظل أحادية حزبية لا تقبل أي رأي معارض) ، فقد نصت المادة 47 من دستور 2020 على حق الأشخاص في الحماية القانونية الخاصة و في سرية المراسلات و الاتصالات و معالجة المعطيات ذات الطابع الشخصي ، فهذه القواعد الدستورية تحقق موازنة مهمة بين الحق في الحماية ( الضحايا) من جهة و ضمانات

[1] د/ عائشة عبد الحميد ، النظام القانوني للمنظمة الدولية للشرطة الجنائية ( الانتربول) و دورها في مجال التعاون الدولي الشرطي ، المجلة الأكاديمية للأبحاث و النشر العلمي ،الإصدار11 ، تاريخ 2020/03/05 ،ص11 ، ISSN2706-6495.

[2] المادة 163 من الدستور الجزائري و المادة الأولى من قانون العقوبات الجزائري .

[3] المادة 35 من الدستور الجزائري .

تضبط سلوك السلطات القضائية لدى الضبط القضائي لحماية حقوق المتهم الذي يظل بريئا ما لم يصدر في حقه حكم نهائي بات بمقتضى محاكمة عادلة [1]، و عليه فهي ضوابط للإجراءات التي تسعى للحصول على الدليل " الالكتروني" ( في حالتنا هذه).

**ثانيا – الاتفاقيات الدولية:**تعتبر القواعد القانونية التي تتضمنها الاتفاقيات الدولية التي ارتضتها دولة ما عن طريق التوقيع ، تبادل الوثائق ( رضا أولي ) ، التصديق ، الانضمام ، الموافقة أو القبول [2]ملزمة لقضاء تلك الدولة لأنها أصبحت التزامات دولية ، فيحتج بها الخصوم إزاء بعضهم و اتجاه القضاء و يثيرها القاضي الجنائي من تلقاء نفسه باعتباره يلعب دورا ايجابيا من خلال إثارة كل الحجج المبنية على قواعد قانونية متى اتضح له ذلك ( سبق لنا الإشارة لدور القاضي الجنائي الايجابي خاصة في النظام التنقيبي ) ، تحتل الاتفاقيات الدولية التي ترتضيها الدولة الجزائرية من خلال إحدى الطرق التي حددتها المادة 13 من اتفاقية **فيينا** لقانون المعاهدات المرتبة الثانية في مصادر التشريع الملزم للقاضي الجزائري بعد الدستور و قبل سائر فئات النصوص .

بما أن فكرة السيدة تمثل حجر الزاوية للدولة ( من أهم الأركان المعنوية إلى جانب الاستقلال و الشخصية المعنوية ) ، فان التعاون الدولي الحقوقي و الأمني قد يجد أحيانا إشكالات تتعلق بسيادة الدول التي يفترض أن تتساوى بغض النظر عن قوة كل منها ، فلا يحق حتى للأمم المتحدة التدخل في الشؤون الداخلية للدولة دون إذن منها[3]، لذلك اعتمدت بعض الإجراءات في التحقيقات الجنائية حول الجرائم الالكترونية قصد التذليل من صعوبات و عقبات إفرازات تطبيق مبدأ السيادة ، و منها الإنابة الخارجية و التحقيق عن بعد [4].

**ا- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ( اتفاقية باليرمو)**

وقعت الجزائر على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية أو ما يعرف باتفاقية **"باليرمو"**[5] في 2000/01/12 و صادقت عليها بتاريخ 2002/10/07 ( الاتفاقية ملحقة ب 3 بروتوكولات )[6] .

بتاريخ 18 أوت من سنة 2015 بادر مؤتمر الأطراف ( انشأته المادة 32 من نص الاتفاقية )

من خلال الفريق العامل المعني بالتعاون الدولي[7] إلى إصدار وثيقة عمل تتضمن "جمع و تبادل الأدلة الاثباتية الالكترونية" ، قدمته الأمانة العامة لمؤتمر أطراف الاتفاقية كدليل أو

---

[1] المادة 41 من الدستور الجزائري .

[2] المادة 11 من اتفاقية فيينا لقانون المعاهدات (وسائل التعبير عن رضا الدولة ) ، العرض للتوقيع في 23 /05/ 1969 ، دخول حيز النفاذ في 27/ 01/ 1980.

[3] الفقرة 7 من المادة 02 من ميثاق منظمة الأمم المتحدة .

[4] د/ عادل يحيى قرني ، التحقيق و المحاكمة الجنائية عن بعد ، دار النهضة العربية ، الطبعة الأولى ، مصر ، 2006 ، ص16.

[5] اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، تاريخ الاعتماد و العرض للتوقيع و التصديق 2000/10/15 ، دخول حيز النفاذ 2003/09/29 طبقا لمادتها 38 ، عدد الأطراف 190 منذ 2018/08/26 .

[6]https ://treaties.un.org/pages/ViewDetails.aspx ?src=IND&mtdsg_no=XVIII-12&chapter=18&clang=_fr.

[7] المادة 13 من اتفاقية "باليرمو".

نموذج في القواعد الموضوعية و الإجرائية لكل ما يتعلق ب" الدليل الالكتروني" خاصة ما ارتبط منها بالتعاون و التنسيق الدولي في سبيل ضبط الجرائم المنظمة الدولية ( العابرة للحدود الجغرافية ) ، و نظرا للأهمية البالغة لهذه الوثيقة ، قدرنا أنها ستكون مفيدة كملحق للمذكرة لما فيها من الوجاهة و الدقة و التفصيل في القواعد القانونية في مجال الإثبات الجزائي عن طريق مستندات رقمية[1].

**ب- اتفاقية بودابست**

و هي أول اتفاقية دولية متعددة الأطراف لمكافحة الجريمة الالكترونية ، وضعت للتوقيع و التصديق بتاريخ 2001/11/23 ، لكنها لم تدخل حيز النفاذ إلا في 2004/07/01 أي بعد مصادقة 3 دول من المجلس الأوروبي . سبب اهتمامنا بهذه الأداة التشريعية الدولية رغم أنها لا تعني الجزائر بصفة مباشرة - لأنها ليست معنية بها ، فلا هي من المصدقين ، ولا حتى من الدول الموقعة عليها- هو التأثر الشديد للمشرع الجزائري بفحوى هذه الاتفاقية ، و هذا أمر طبيعي بما أنها كانت رائدة في التشريع الجنائي الالكتروني .

نصت المادتان 16 و 17 من اتفاقية بودابست على تجميع و تخزين البيانات المعلوماتية ، أما المادة 19 فقد وضعت أحكام التفتيش الالكتروني ، بينما نجد نص المادة 31 من الاتفاقية يتعلق بالدليل الالكتروني مباشرة ، أما المادة 21 ، فلقد أكدت على التعاون الدولي[2].

**ج- مؤتمر "ريوديجانيرو" للجمعية الدولية لقانون العقوبات**

انعقد المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات بمدينة **ريو** البرازيلية في 1994/09/04 بغاية محاولة إرساء بعض المبادئ القانونية التي تؤطر مكافحة الجرائم الالكترونية التي أخذت منحنى تصاعديا و كان المجتمع الدولي حديث العهد بتلك الآفة آنذاك .

خرج المؤتمرون بعد انتهاء أشغال الدورة ببعض التوصيات التي يرجى من الدول الأطراف في الجمعية الدولية ( الجزائر عضو) إدراجها ضمن قوانينها الجنائية ، منها ما جاء في التوصية رقم 12 و هو اشتراط الحصول على إذن قضائي مسبق قبل استقاء أي **دليل** يمس بخصوصية المتهم أو بسرية اتصالاته ، و أوصى المؤتمر من خلال التوصية 18 على إبطال الأدلة التي يحصل عليها بطرق تمس بالحقوق الأساسية للمتهم و عدم منحها أي اعتبار في كل مجريات و مراحل المتابعة[3].

**د- الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية**

---

[1] مؤتمر الدول الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، الفريق العامل المعني بالتعاون الدولي ، ورقة معلومات أساسية ، " جمع و تبادل الأدلة الاثباتية الالكترونية " ، الوثيقة CTOC/cop/wG3/2015/2 الصادرة في 2015/08/18 .

[2] اتفاقية مكافحة الجريمة الالكترونية "بودابست" ، توقيع 2001/11/23 ، حيز النفاذ 2004/07/01 .

[3] طرشي نورة ، مكافحة الجريمة المعلوماتية ، مذكرة ماجستير ، تخصص قانون جنائي ، كلية الحقوق ، جامعة الجزائر 01 ، الموسم الجامعي 2012/2011 ، ص110،109.

رغم عدم انضمام الجزائر للمنظمة العالمية للتجارة ( في وضعية تفاوض حول شروط و إجراءات الانضمام )[1]، إلا أن هذا لم يمنع من تأثر المشرع الجزائري لدى سنه للقانون 18-05 يتعلق بالتجارة الالكترونية باتفاقية التريبس و التي ورثتها المنظمة العالمية للتجارة عن منظمة الجات ( سابقا حيث حازت الجزائر على صفة مراقب بعد إعلان مراكش في سنة 1995)[2].

أحالت اتفاقية التريبس في أحكامها الواردة ضمن المواد من 1 إلى 21 إلى أحكام معاهدة "برن"[3] التي تنص الفقرة الثانية من مادتها 15 على قواعد الإثبات أمام القضاء ، وحتى و إن كان المعني هو الإثبات للحصول عن التعويض المدني ، لكن قد نلجأ للإثبات الجنائي القطعي الذي نستعمله أمام القاضي المدني لاحقا أو في الدعوى المدنية بالتبعية طبقا لمبدأ **" الجنائي يوقف ( يرجئ ) المدني "**[4].

لكن علينا أن نسجل الاختلاف بين حجية الإثبات الالكتروني في المسائل المدنية ( التوقيع الالكتروني ) عنه في القضايا ذات الطابع الجنائي ، فإذا كان الإثبات في المدني خاضعا لقواعد شكلية صارمة و محددة بدقة ، فانه أكثر حرية في الجنائي و للقاضي سلطة تقديرية واسعة في تقييم الدليل ، غير أن وجود نظام تقني لتسجيل الدخول على شبكة الانترنت يمكننا من التعرف على هوية الأشخاص الذين تورطوا في الجرم الالكتروني بما يشبه نظام التوقيع في المبادلات المدنية ( خاص بجرائم الانترنت فقط)[5] .

**ه- القانون العربي النموذجي لمكافحة الجرائم المعلوماتية**

بصفة الجزائر عضو في جامعة الدول العربية ، فهي معنية بهذا التشريع الذي أفضت إليه أعمال مجلسي الوزراء العرب في كلا من قطاعي العدل و الداخلية بشان مكافحة الجرائم الالكترونية في أعقاب شهر ماي من سنة 2003[6].

جاء في نص الفقرة الثانية من المادة 04 من القانون العربي النموذجي لمكافحة الجرائم الالكترونية ترتيبا يتعلق بالإثبات من خلال المحرر الالكتروني الذي يكون محل تزوير مع توفر القصد الجنائي أي العلم بالتزوير و نية استعماله للإثبات(التزوير الالكتروني)[7].

**ثالثا – التشريع العادي ( القوانين الوطنية )**

تناولت النصوص التشريعية العقابية و الخاصة بقطاع الاتصالات تنظيم أحكام الجرائم الالكترونية ( قانون العقوبات ، قانون البريد و الاتصالات اللاسلكية ، القانون 09-04 أي الخاص بالوقاية من جرائم الإعلام و مكافحتها و غيرها ) ، لكن قليلة هي

---

[1] ا/ عبيدة سليمة ، مسار انضمام الجزائر للمنظمة العالمية للتجارة ، مجلة الاقتصاد الجديد ، العدد 08 ، ماي 2013 ، ص330.

[2] مجلة الفكر البرلماني ، مجلس الأمة الجزائري ، جويلية 2008 ، ص159.

[3] اتفاقية برن لحماية المصنفات الفكرية و الفنية ، الإبرام 1886 ، بعد تعديلات متتالية ، اعتماد أخر نسخة في سبتمبر 1979 بباريس .و انظر أيضا علي حسن طوالبة ، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي ، ص15.

[4] المادة 339 من القانون المدني الجزائري و المادة 03 من قانون التحقيق الجنائي الفرنسي .

[5] http ://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim-tech-info-pdf.

[6] د/ عمر فاروق الحسيني ، تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي ، مجلة المحاماة ، السنة 12 ، عدد نوفمبر/ديسمبر ، 1989 ،ص385.

[7] المادة 04 من القانون العربي النموذجي لمكافحة جرائم الكمبيوتر و الانترنت .

الأحكام أو التدابير المتعلقة بالدليل الرقمي على وجه الخصوص ، ربما يرجع تفسير ذلك لفلسفة التشريع الجنائي الجزائري ( مبدأ حرية الإثبات الجنائي) .
وضع قانون الإجراءات الجزائية الجزائري المبدأ العام للإثبات من خلال نص المادة 212 منه ، بينما استحدث القانون 04-05 المعدل و المتمم لقانون العقوبات الجزائري أحكاما تتعلق بالمعالجة الآلية للمعطيات من خلال المواد من 394 مكرر إلى غاية 394 مكرر7 من قانون العقوبات الجزائري[1].

ألحقت التعديلات التي سنها المشرع الجزائري بمقتضى القانون 06-22 تغييرا إجرائيا في أساليب التحري عن بعض الجرائم وبالتالي في طرق حيازة الدليل ، ومنها تسجيل الأصوات و اعتراض المراسلات دون علم المشتبه به ، حيث نصت المادة 65 مكرر10 من قانون الإجراءات الجزائية الجزائري و المستحدثة بمقتضى القانون المذكور أعلاه صراحة على " .....المراسلات و الصور أو المحادثات .....في إظهار الحقيقة ....." ، فإذا كانت هذه المادة ليست خاصة بالثبات الالكتروني حصرا ، غير أنها مرتبطة به مباشرة[2].

تناول قانون 18-04 يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ضمن نص المادة 60 تحويل الأموال عن طريق الحوالة الالكترونية ، فيمكن عن طريق الدليل الالكتروني لتحويل مالي ما أن يستخدم في إثبات ذو طبيعة جنائية عن التدليل عن جرم ليس بالضرورة من ذات الطبيعة ( جريمة فساد أو اختلاس أموال عامة أو غيرها من الجرائم المالية )[3].

أما القانون 09-04 ، فقد تناول أحكاما ترتبط بصفة مباشرة بالإثبات عن طريق المستند الالكتروني في المتابعات الجنائية للجرائم الالكترونية من خلال مواده 10ن 11 و 12 ، حيث فرض المشرع بمقتضاه على مزودي خدمات الاتصالات الالكترونية التعاون مع مصالح الأمن في مجال تسهيل الوصول للدليل عن ارتكاب الجرم بحفظ المعطيات و البيانات الرقمية و السهر على سلامتها و وضعها في متناول القضاء متى طلب ذلك[4].

## المطلب الثاني الدليل الالكتروني في تقدير القضاء الجزائي الجزائري

تنظر الهيئة الجزائية المختصة ، سواء قسم الجنح و المخالفات ، النيابة العمومية ، قاضي التحقيق ، غرفة الاتهام ، محكمة الجنايات[5] أو حتى إحدى الغرف الجزائية للمحكمة العليا في مشروعية و مدى صحة وسيلة الكترونية لإثبات ارتكاب جرم ما أو نفيه ( حسب الحالة ) ، يكون الدليل محل نقاش من الأطراف للتمحيص في صحته حتى ينال القبول القانوني و يلج قناعة و ضمير القاضي ليحكم به وفقا لما يقتضيه القانون و ما

[1] القانون 04-15 المؤرخ في 2004/11/10 ، ج.ر عدد 71 ، يعدل و يتمم الأمر 156/66 المتضمن قانون العقوبات .
[2] القانون 06-22 ، مؤرخ في 2006/12/20 ،ج.ر 84 ، الصادرة في 2006/12/24.و انظر أيضا د/ شيخ ناجية ، أساليب البحث و التحري المستحدثة في القانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري ، المجلة النقدية للقانون و العلوم السياسية ، السنة 08 ، العدد01 ،ص279.
[3] القانون 18-04 مؤرخ في 2018/05/10 يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، ج.ر عدد 27 الصادرة في 2018/05/13.
[4] د/ بوضياف اسمهان ، الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، العدد11 ، سبتمبر 2018 ،ص366.
[5] المادة 258 من ق.ا.ج.جزائري .

يملي عليه ضميره المهني و ما يفرضه المنطق السليم و الحقائق العلمية المؤكدة لتحقيق العدل و إحقاق الحقوق و تحمل الالتزامات[1].

باعتبار أن المشرع الجزائري يأخذ مبدئيا بحرية الإثبات مع التأثر نسبيا بنظام الإثبات المقيد ( نظام مختلط ) شانه في ذلك شان المشرع الياباني الذي اخذ بهذا الاتجاه ، حيث تخضع الأدلة الجنائية الالكترونية للسلطة التقديرية للقاضي على النحو التالي اعتبار المستندات الكهرومغناطيسية وسائل إثبات مقبولة جنائيا بشرط قابليتها للتحويل إلى محتوى مرئي أو منسوخ و استبعادها في الحالة المخالفة[2].

**الفرع الأول الاختصاص القضائي للنظر في الدليل الالكتروني**

ينعقد الاختصاص القضائي الجزائي محليا ( لان الاختصاص النوعي مفروغ من أمره مادمنا بصدد متابعة جزائية ) بشكل عام وفقا للقواعد التي وضعها المشرع الجزائري ضمن نص المادتين 37 و 40 من قانون الإجراءات الجزائية و المتمثلة في المعايير الثلاثة مكان وقوع الجريمة ، مكان إقامة احد المشتبه فيهم أو مكان القبض عليه ، و بما أن الدليل الالكتروني قد يستعمل للإثبات أو النفي في أي جريمة كما اشرنا له ، فان هذا الاختصاص يسري عليه .

بما أن التجربة الجنائية أثبتت ارتباط الإثبات الالكتروني بالجرائم الالكترونية بشكل شبه مطلق ، حري بنا التطرق على الاختصاص القضائي بالجرائم الالكترونية ، إذ أشارت الفقرة 2 من المادة 37 من قانون الإجراءات الجزائية إلى إمكانية تمديد الاختصاص القضائي لوكيل الجمهورية في جرائم محددة حصرا عن طريق التنظيم ، و من الجرائم المعنية نجد تلك الماسة بأنظمة المعالجة الآلية للمعطيات ( من الجرائم الالكترونية و ذكرها القانون 09-04)[3].أكدت بعض المؤتمرات الدولية على الأهمية البالغة لإنشاء جهات قضائية جزائية مختصة حسب طبيعة و خطورة الجرائم كمؤتمر "روما "لسنة 1958 ، مؤتمر" نيس "المنعقد في فرنسا 1972 و مؤتمر "ريوديجانيرو" لسنة 1978 ، و هو ما ترجمه القانون 04-14 الذي أقحم المادتين المشار لهما أعلاه ( 37 و 40 ) ضمن قانون الإجراءات الجزائية[4].

أنشئت أقطاب جزائية بمقتضى التنظيم ( المرسوم التنفيذي 348/06 ) طبقا لمقتضيات المادة 40 من قانون الإجراءات الجزائية تختص بالنظر في بعض الجرائم منها الجرائم الالكترونية ، و هو خيار انتهجته السلطة الجزائرية لتأسيس قضاء مختص من جهة و تخفيف الأعباء المالية الضخمة التي تكلفها أكثر في حالة التركيز على ازدواجية التخصص ( القضاة و الهيئات ) التي أوصت بها المؤتمرات المذكورة ، فهو

[1] د/ لورنس سعيد الحوامدة ، حجية الأدلة الرقمية في الإثبات الجنائي دراسة تحليلية مقارنة ، مجلة البحوث الفقهية و القانونية ، العدد36 ، أكتوبر 2021 ، ص925.

[2] د/ عبد الفتاح بيومي حجازي ، الإثبات في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، مصر ، 2004 ، ص46.

[3] المرسوم التنفيذي 348/06 المتضمن تمديد الاختصاص المحلي لبعض المحاكم وكلاء الجمهورية و قضاة التحقيق ، الصادر في 2006/10/05، ج.ر. عدد 63 .

[4] القانون 14-04 المؤرخ في 2004/11/10 المعدل و المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية الجزائري .

خيار توفيقي بين الفعالية و المرونة من جهة و الاقتصاد و تخفيف العبء عن الخزينة من جانب ثاني[1].

**الفرع الثاني سلطة القاضي الجزائي الجزائري في الأخذ الدليل الالكتروني**

يتفق الفقه على السلطة التقديرية الواسعة للقاضي الجزائي في تقدير الأدلة بشكل عام و الدليل الالكتروني على وجه الخصوص ، غير أن مراعاة بعض الضوابط القانونية يفرضه المنطق القانوني و متطلبات العدالة و الإنصاف و التوفيق بين مبدئي " محاربة الإفلات من العقاب " من جهة و " احترام حقوق الدفاع " من جانب آخر ، فرغم عدم تحديد المشرع لهذه الضوابط حصرا ، أرست المنظومة القانونية الجزائية في كل الدول شروطا عامة لمقبولية الدليل الرقمي ، و النظام القانوني الجزائي الجزائري لم يشذ عن القاعدة ، يمكن إيجازها في :

ا- وجود نسخة أصلية للدليل الالكتروني المقدم ضمن مستندات الدعوى بغرض إمكانية التأكد لدى الضرورة من صحة المستند[2].

ب- أن يكون الدليل الالكتروني قد قدم ضمن ملف الدعوى[3].

ج- أن يكون الدليل محل مناقشة أثناء جلسات المحاكمة[4].

د- أن يكون يقينيا إذا ما كان للإدانة ، لان الشك يفسر لمصلحة المتهم[5].

ه- أن يتم الحصول عليه بطريقة مشروعة وفقا لمبدأ " الشرعية الجنائية" الذي يستند إليه كل النظام القانوني الجزائي[6].

يفرض منطق النظام التنقيبي ( الغالب على المنظومة الإجرائية الجزائية الجزائرية ) دور فعال للقاضي الذي ينبغي عليه البحث الحثيث عن الحقيقة أينما كانت سواء تعلقت بإثبات التهمة أو بنفيها بخلاف القاضي المدني ( سلبية القاضي المدني) و بشكل ابرز من دور القاضي الجزائي في النظام الاتهامي ، خاصة في التحقيق النهائي ( التحقيق الذي يجريه قاضي الحكم أثناء الجلسة ) أو إعادة التحقيق أمام قاضي التحقيق رغم صدور **" ألا وجه للمتابعة "** في حالة ظهور دليل الكتروني جديد[7]. فالقاضي أمام التزام قانوني و أخلاقي ( نص الدستور على ضمير القاضي) بإعمال كل قدراته الذهنية لتمحيص عناصر الدليل الالكتروني تحليلا نقدا و تركيبا و فحصا و تقليبا على كل الأوجه الممكنة لبناء قناعته الشخصية[8].

---

[1] ا.د/ عمار بوضياف ، النظام القضائي الجزائري ، دار ريحانة ، الجزائر ، 2003 ،ص229

[2] قرار صادر عن الغرفة الجزائية الثانية بالمحكمة العليا ، قضية رقم 25814 ، صادر بتاريخ 1982/01/05.

[3] المادة 212 من قانون الإجراءات الجزائية الجزائري .

[4] غلاي محمد ، احترام أصل البراءة مطلب من متطلبات دولة القانون ، دار بلقيس ، الجزائر ، 2012 ،ص90.

[5] المادة 163 من قانون العقوبات الجزائري .

[6] المادة الأولى من قانون العقوبات الجزائري .

[7] المادة 75 من قانون الإجراءات الجزائية الجزائري .

[8] عبد الحكيم فودة ، حجية الدليل الفني في المواد الجنائية و المدنية ، دار الفكر الجامعي ، الطبعة الأولى ، مصر ، 1996 ، ص24. و انظر أيضا وفاء عمران ، تعامل القاضي الجزائي مع الدليل العلمي –دراسة مقارنة - ، أطروحة دكتوراه ، تخصص قانون العقوبات و العلوم الجنائية ، جامعة قسنطينة 1 ، الموسم الجامعي 2019/2018 ،ص96.

حدد المشرع الجزائري قواعد ندب الخبرة الفنية في القضايا الجزائية ضمن المواد من 143 إلى غاية 153 من قانون الإجراءات الجزائية الجزائري ، إذ حددت المادة 146 ق.ا.ج.ج نطاق الخبرة **" عدم تجاوز حدود الجوانب التقنية البحتة "** ، فالخبير يقدم أطروحة فنية تحتاج أن تقترن بنظرة أو رأي قانوني يدركه القاضي حتى يتوصل لقناعته في إصدار الحكم ، فالقول بان القاضي هو وحده من يتحمل مسؤولية حكمه و ليس الخبير ( للقاضي أن يستعين بخبرة ثانية ) لا يجعله في حل من أي رقابة لأنه تحت طائلة تعقيب محكمة النقض ( المحكمة العليا ) لان مسالة تقدير الدليل لها أوجه قانونية و ليست مسالة واقع فقط[1]، و تظهر رقابة المحكمة العليا على الدليل في القضايا الجزائية عموما و بالتالي على الدليل الالكتروني في القضايا الجنائية من خلال :

ا- الرقابة على فحوى و مضمون و مالأت ( نتائج ) الدليل الرقمي .

ب- رقابتها على الانسجام و خلو الأدلة من التناقض الذي يؤذي إلى إعدام أثرها.

ج- رقابتها على الإسناد ، بمعنى أن تعقب على معاينتها لأخطاء في أن ينسب القاضي شهادة لطرف ما يتضح انه لم يقدمها .

د- الرقابة على سلامة منطق و الأساس العلمي للأدلة الالكترونية[2].

[1] عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي "دراسة مقارنة" ، رسالة ماجستير ، كلية الحقوق ، جامعة الإسكندرية ، 2009 ، ص183.

[2] د/ عميمر عبد القادر ، مرجع نفسه ،ص135-136.

# الخـــــاتمـــــة

## خـــاتمـــــة :

طبقا لما ينص عليه الدستور الجزائري الحالي ( 2020) و كذا ما نصت عليه الدساتير السابقة ( 1989 ، 1996 و 2016) ، فان الحق في الخصوصية و خاصة سرية المراسلات و الاتصالات الشخصية مكفول لكل مواطن ، و هذا ما أكدته المواثيق و العهود الدولية التي صادقت عليها و انضمت إليها الدولة الجزائرية ( رغم أن الحقوق الأساسية معتبرة من القواعد الآمرة بمقتضى اتفاقية فيينا لقانون المعاهدات ) ومنها الاتفاقية الإفريقية حول الأمن السيبراني و حماية المعطيات ذات الطابع الشخصي أو ما يعرف باتفاقية "مالابو" لسنة 2014 التي أكدت ديباجة و مواد على ضرورة احترام هذا الحق الأساسي للأفراد ، فمجال الإثبات عن طريق استغلال الأدلة الالكترونية مجال ثري و خصب للتقاطعات بين التقنية من جانب و القانون من جانب أخر لتمكين القضاء من حل المتراجحة العويصة بين الحصول على تفوق ( سبق) تقني على المجرمين و احترام حقوق الأبرياء و عدم انتهاك نطاق خصوصيتهم الذي لا ينفصل عن كرامتهم و شرفهم ، مع التذكير دوما بقرينة البراءة التي يتمتع بها المشتبه فيهم ما لم يدانوا بحكم نهائي بات .

فإذا كنا نحقق من مكاسب التطور التكنولوجيا قدرا من الرفاهية و سهولة الأداء الإداري و التواصل المتدفق و غيرها من مظاهر الرفاهية ، وجب الانتباه للمخاطر التي تقابل كل هذا ، و منها ما يسمى " مجتمع الرقابة" أو المجتمع المراقب و الذي تكون فيه بعض الحقوق في خطر حقيقي خاصة الحق في الخصوصية ، فاستفحال الجرائم و خاصة الالكترونية منها و ضرورة التصدي لها و مكافحة آفة الإفلات من العقاب لا ينبغي أن يؤثر على قدسية و جلل هذا الحق الأصيل لأنه مرتبط بشعور الإنسان بالأمن و التمتع بالعزة و الستر و حقه في عدم البوح بما يخصه دون عامة الناس و الاحتفاظ بنطاقه الخاص و بالتالي على المجتمع من خلال المشرع أن يحيط هذا النطاق الذاتي جدا بكل الأدوات القانونية الضرورية لصونه ، و ألا نجعل من التصدي للجريمة ذريعة استباحة إلا في الحدود الضرورية للوصول للحقيقة حول الجرم و بضوابط صارمة جدا .

من خلال هذه الدراسة يمكن نورد بعض النقاط المستخلصة و التي تهمنا أكثر من غيرها فيما يلي

1- ارتكاب الجريمة أصبح الآن أسهل و اقرب لنا مما نظن ، لان أهم أدوات الجريمة الالكترونية الحاسوب او الهاتف الذكي الذي تكاد الأيدي لا تبارحه ، فحذاري مما نكتب أو نعلق به على صفحات شبكات التواصل ، فرب تغريده تشهير ، ورب تعليق قد يوصف بالقذف ، و المتابعات على أساس الإساءة لرموز الدولة عبر هذه الشبكات كثيرة أمام القضاء الجزائري .

2- لا يجب ربط الدليل الالكتروني حتما بالجريمة الالكترونية ، فهو أوسع منها نطاقا ، لأنه يصلح للإثبات في الجرائم غير الالكترونية أيضا .

3- التمييز بين الإثبات في الجرائم المرتبطة بالحاسوب غير الموصول بالشبكة و تلك المتعلقة بجرائم الانترنت لأنها تختلف من عدة مناح ، خاصة النطاق الإقليمي المعقد في جرائم الانترنت و قد تتضارب بشأنها القواعد القانونية لتنازع الاختصاصات القضائية .

4- عدم وجود قضاء جزائي جزائري مختص بالنظر في الجرائم الالكترونية (لوحدها ، فالأقطاب الجزائية ليست مختصة في الجريمة الالكترونية ) التي تتطلب تكوينا خاصا للقاضي ، فرغم وجود الخبراء في مجال المعلوماتية غير أن القاضي هو من يصدر الحكم و يتحمل مسؤوليته .

5- التعاون القضائي من خلال الاتفاقيات المتعددة الأطراف و الثنائية حيوي لردع الجرائم الالكترونية لأنها عابرة للحدود الوطنية .

و على ضوء ما تقدم في هذه المذكرة ، و خاصة ما تم التوصل إليه من نتائج ، يمكن اقتراح بعض التوصيات على النحو الأتي

1- ضرورة مواكبة التشريع الجزائي لوتيرة تطور أساليب الجرائم الالكترونية و لو بوضع قواعد عامة و ترك بعض التفاصيل للتنظيم ، و مساهمة بعض القوانين الخاصة في تضمن قواعد عقابية تعزز قانون العقوبات لتحقيق مرونة و سرعة اكبر.

2- الأخذ بمبدأ حرية الإثبات بالشكل الأمثل و عدم تقييد الدليل الالكتروني إلا في حدود ما ينتهك حقوق المتهم الأساسية و حقوق الغير ( لأنه بطبيعته دليل علمي فهو موثوق لحد كبير ).

3- تكوين قضاة مختصون تكوينا كافيا في مجال المعلوماتية ، فرغم وجود الخبير ، يبقى التقدير الذي يبنى على أساسه الحكم للقاضي ( اعتماد القاضي كليا على تقرير الخبير دون فهم و مناقشة ينتقص من هيبة القضاء ).

4- تحديد المعايير القانونية للدليل الالكتروني و تمييزها عن تلك المتعلقة بمسائل الواقع بشكل واضح يجعل مسوغات الطعن بالنقض لتعقيب المحكمة العليا عن حكم القاضي أكثر وضوحا .

5- الاهتمام بالضبط الإداري و تكوين خبراء الأمن المعلوماتي لتلافي ارتكاب الجريمة من الأساس مصداقا للحكمة " الوقاية خير من العلاج"

و السلام ، تم الختم بفضل الله و حمده .

Distr.: General
18 November 2015
Arabic
Original: English

# مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

## تقرير عن اجتماع الفريق العامل المعني بالتعاون الدولي، المعقود في فيينا يومي ٢٧ و٢٨ تشرين الأول/أكتوبر ٢٠١٥

### أولاً- مقدِّمة

١- قرَّر مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية، في مقرَّره ٢/٢، أن ينشئ فريقاً عاملاً مفتوح العضوية لكي يعقد مناقشات مواضيعية حول المسائل العملية المتعلقة بتسليم المطلوبين والمساعدة القانونية المتبادلة والتعاون الدولي لأغراض المصادرة. وقرَّر المؤتمر في مقرَّره ٢/٣ أن يكون الفريق العامل المفتوح العضوية المعني بالتعاون الدولي عنصراً ثابتاً من عناصر المؤتمر. وعقد الفريق العامل المعني بالتعاون الدولي، الذي أنشئ بموجب ذلك المقرَّر، اجتماعاً في فيينا يومي ٢٧ و٢٨ تشرين الأول/أكتوبر ٢٠١٥.

### ثانياً- التوصيات

٢- وضع الفريق العامل التوصيات التالية:

(أ) ينبغي أن تواصل الأمانة إعداد مواد تدريبية بشأن جمع وتبادل الأدلة الإثباتية الإلكترونية، بموجب اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية، لمواصلة استخدامها في أنشطة المساعدة التقنية؛

(ب) ينبغي أن تواصل الأمانة تعميم موضوع الأدلة الإثباتية الإلكترونية على ما هو قائم من أدوات التعاون الجنائي الدولي وما سيُعَدُّ منها لاحقاً، وأن تطلب من الدول تقديم معلومات ومواد ذات صلة لإدراجها في بوَّابة إدارة المعارف المعروفة باسم "بوَّابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة" (شيرلوك)؛



الرجاء إعادة الاستعمال

(ج) ينبغي أن تعزِّز الدول الأعضاء كفاءة آليات التعاون في مجال إنفاذ القانون بوسائل منها استحداث نظم فعَّالة لتبادل المعلومات، وإنشاء قنوات اتصال بين السلطات المختصة فيها، وعقد ترتيبات لتعزيز المساعدة التنفيذية إذا لزم الأمر؛

(د) ينبغي أن تنظر الدول الأعضاء في استكشاف السبل والوسائل الكفيلة بتعزيز التعاون الدولي على نحو يشمل، فيما يشمل، استخدامَ الأدلة الإثباتية الإلكترونية؛ وحفظَ هذه الأدلة؛ وعلى وجه الخصوص استكشافَ السبل الممكنة للتعجيل بعمليات المساعدة القانونية المتبادلة الرسمية؛

(هـ) ينبغي أن تنظر الدول الأعضاء، في الحالات المناسبة، في تشجيع الممارسين على التشاور بصفة غير رسمية قبل تقديم طلب رسمي بشأن تسليم المطلوبين أو التماس المساعدة القانونية المتبادلة؛ وتحقيقاً لذلك، ينبغي للدول الأطراف أن تشجِّع المبادرات الرامية إلى إتاحة إرشادات واضحة عن إجراءاتها ومتطلباتها المتعلقة بتقديم تلك الطلبات؛

(و) ينبغي أن تنظر الدول الأعضاء في دعم جهود المساعدة التقنية، بما فيها تلك التي يضطلع بها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب)، الرامية إلى وضع برامج تدريبية لتحسين قدرات موظفي إنفاذ القانون المحليين، ومن ضمنهم أولئك المخوَّلون القيام بمهام ضباط الاتصال، وقدرات قضاة الاتصال، وتعزيز معارفهم بشأن مواضيع منها الصكوك الدولية المنطبقة والنظم القانونية المحلية للبلدان المضيفة وقوانين إجراءاتها الجنائية، بما في ذلك شروط مقبولية الأدلة الإثباتية في المحاكم؛

(ز) ينبغي أن تواصل الأمانة تطوير أدوات التعاون الدولي في المسائل الجنائية، بما في ذلك وضع الصيغة النهائية لأداة كتابة طلبات المساعدة القانونية المتبادلة المنقَّحة، وأن تقدِّم تقريراً إلى مؤتمر الأطراف في اتفاقية الجريمة المنظَّمة في دورته الثامنة عن المرحلة التجريبية لاختبار استخدام هذه الأداة في الممارسة العملية كمادة تدريبية؛

(ح) ينبغي أن تواصل الأمانة عملها، بما في ذلك من خلال وسائل عدَّة منها البوَّابة الإلكترونية لإدارة المعارف "شيرلوك"، على جمع وتعميم القوانين الوطنية والإرشادات والمبادئ التوجيهية ذات الصلة التي يمكن أن تساعد السلطات المركزية والممارسين في إعداد طلبات المساعدة القانونية المتبادلة وتقديمها بسرعة؛

(ط) ينبغي، من أجل تعزيز الاتصال المباشر بين السلطات المركزية، أن تعدِّل الأمانةُ دليلَ السلطات الوطنية المختصة بموجب المواد ٦ و٧ و١٧ من اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدِّرات والمؤثِّرات العقلية لعام ١٩٨٨ والسلطات الوطنية

المختصة بموجب اتفاقية مكافحة الجريمة المنظَّمة عبر الوطنية بتقسيم الدليل إلى جزأين، أحدهما يتضمَّن معلومات عن السلطات المركزية المعيَّنة بمقتضى مختلف الأحكام التعاهدية ذات الصلة بالمساعدة القانونية المتبادلة، بما في ذلك بيانات الاتصال، واللغات المقبولة والأشكال المقبولة لإحالة الطلبات، ويتضمَّن الآخر معلومات عن سائر السلطات المختصَّة و/أو السلطات التنفيذية، حسب الاقتضاء، وعن القنوات وسُبل التعاون غير الرسمي؛

(ي) ينبغي أن تدعو الأمانةُ الدول الأطراف إلى تحديث شرط الإشعار بموجب الفقرة الفرعية ٥ (أ) من المادة ١٦ من اتفاقية الجريمة المنظَّمة والنظر في إتاحة هذه المعلومات المحدَّثة على نطاق واسع؛

(ك) ينبغي، بالنظر إلى عدم قبول بعض تقارير الأطراف باتفاقية الجريمة المنظَّمة كأساس للمساعدة القانونية بموجب الفقرة ٧ من المادة ١٨ من الاتفاقية، أن تتَّخذ الدول الأطرافُ خطواتٍ في سبيل تعزيز استخدام اتفاقية الجريمة المنظَّمة كأساس قانوني للمساعدة القانونية المتبادلة، مع مراعاة قيمتها المضافة باعتبارها أداةً تيسِّر التعاون الدولي بشأن نطاق واسع من الجرائم وعلى أوسع مدى ممكن؛ وينبغي للدول الأطراف أيضاً أن تكفل امتثال قوانينها وممارساتها الداخلية للمادة ١٨ من الاتفاقية؛

(ل) ينبغي أن تنظر الدول الأعضاء، بمساعدةٍ من الأمانة ورهناً بتوافر موارد من خارج الميزانية، في إمكانية استحداث شبكة عالمية، من خلال بيئة افتراضية، لغرض إنشاء وتعزيز سبل الاتصال المباشر بين السلطات المركزية؛

(م) ينبغي أن تباشر الأمانة تحديث واستكمال وإقرار مشروع تقرير الفريق العامل غير الرسمي من الخبراء المعني بالتحرِّيات المشتركة، بما في ذلك استنتاجاته وتوصياته، وهو المشروع الذي أُطلع عليه مؤتمر الأطراف في دورته الرابعة ضمن ورقة الاجتماع CTOC/COP/2008/CRP.5؛

(ن) تُدعَى الدول الأطراف إلى أن تنظر في أن تضمَّ إلى وفودها المشاركة في دورات الفريق العامل المقبلة ممارسين مكلَّفين بمسائل متَّصلة بأحكام التعاون الدولي المنصوص عليها في الاتفاقية وإلى تشجيعهم على المشاركة بنشاط في اجتماعات الفريق العامل؛

(س) ينبغي أن تنظر الدول الأطراف، بالتنسيق مع الأمانة، في تحديد مواعيد اجتماعات الفريق العامل المقبلة على نحو معيَّن (كأن تعقُبَ اجتماعاتٍ أخرى ذات صلة) يُيَسِّر مشاركة الممارسين واستخدام موارد الحكومة والمؤتمر على أفضل وجه ممكن.

## ثالثاً- موجز المداولات

### ألف- جمع وتبادل الأدلة الإثباتية الإلكترونية

٣- نظر الفريق العامل، أثناء جلسته الأولى المعقودة في ٢٧ تشرين الأول/أكتوبر ٢٠١٥، في البند ٢ من جدول الأعمال، وهو البند المعنون "جمع وتبادل الأدلة الإثباتية الإلكترونية". وترأس الرئيس هذه الجلسة، وأدار المناظر ديفيد ورنر (الولايات المتحدة الأمريكية) مناقشات هذه الجلسة.

٤- وأشير إلى استخدام مصطلحي "الأدلة الرقمية" و"الأدلة الإلكترونية"، وبيَّن بعض المتكلِّمين أنَّ كلا المصطلحين مستخدمان في ولاياتهم القضائية. وأشار بعض المتكلِّمين إلى خبراتهم الوطنية في مجال جمع وتبادل الأدلة الإلكترونية، وذكروا، في جملة أمور، قوانينهم القائمة أو عمليات التحديث التي تجرى عليها، وكيف أنَّ تلك القوانين تنظِّم، على سبيل المثال، عمليات اعتراض الاتصالات.

٥- وسلَّط متكلِّمون آخرون الضوء على الطابع عبر الوطني للجريمة السيبرانية والتحدِّيات ذات الصلة التي تفرضها على مسألة السيادة الوطنية ومسألة تحديد أنسب ولاية قضائية جنائية. وأشير إلى أن تعقُّد المسائل القانونية والتنفيذية المرتبطة بالجريمة السيبرانية يتطلَّب استحداث وسائل إضافية لتحسين قدرة أجهزة إنفاذ القانون والسلطات القضائية لدى الدول الأعضاء، وكذلك تقديم مساعدة تقنية دعماً لاختصاص أجهزة إنفاذ القانون في التصدِّي للجرائم السيبرانية.

٦- وناقش المتكلِّمون تجارب دولهم في مجال طلب معلومات من مقدِّمي خدمات الإنترنت أو طلب حفظ البيانات لديهم، والمتطلبات الإجرائية والقانونية اللازمة لذلك. وبرز تحدٍّ خاص تمثَّل في كيفية تقديم ذلك النوع من الطلبات إلى مقدِّم خدمات إنترنت أجنبي يعمل في الولاية القضائية لدولة ما، أو عندما تكون البيانات مخزَّنةً في خادوم موجود في ولاية قضائية أخرى. ونوقشت مسألة المستوى الرسمي اللازم لطلبات المساعدة القانونية المتبادلة من هذا النوع، كما نوقشت مسألة أهمية نقاط الاتصال المتاحة على مدار الساعة طوال أيام الأسبوع في التعجيل بتنفيذ الطلبات. وأشار أحد المتكلِّمين إلى ضرورة أن تعزِّز السلطات المركزية عمليات توعية القضاة بالإجراءات السليمة لطلب معلومات من ولاية قضائية أخرى.

٧- وشدَّد بعض المتكلِّمين على أنَّ المسائل المتعلقة بجمع وتبادل الأدلة الإلكترونية لا تتعلق فقط بالجريمة السيبرانية، بل تتعلق أيضاً بأشكال أخرى من الجرائم مثل التزييف والاتجار بأدوية مغشوشة وتمويل الإرهاب والاتجار بالأشخاص وإيذاء الأطفال عبر شبكة

الإنترنت. وأشار أحد المتكلِّمين إلى ضرورة تفسير المادة ١٨ من اتفاقية مكافحة الجريمة المنظَّمة، المتعلقة بالمساعدة القانونية المتبادلة، بمعناها الواسع لتشمل طلبات المساعدة القانونية المتبادلة التي تنطوي على استخدام أدلة إثباتية إلكترونية أو مناولتها.

٨- ورأى بعض المتكلِّمين أنَّ من الضروري وضع صك قانوني عالمي في إطار الأمم المتحدة للتمكُّن من مكافحة الجريمة السيبرانية بفعالية، وأنه ينبغي لذلك الصك أن يتناول مجالات منها التعاون الدولي الفعَّال وقانون الإجراءات الجنائية. ورأى بعض المتكلِّمين الآخرين أنه ينبغي للدول بدلاً من وضع صك جديد أن تركِّز على التنفيذ الفعلي للصكوك القائمة، ولا سيما اتفاقية الجريمة المنظَّمة، وعلى تحديد احتياجاتها الوطنية من المساعدة التقنية. وناقش بعض المتكلِّمين أيضاً منافعَ توسيع نطاق استخدام اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وأعرب بعض المتكلِّمين عن تطلُّعهم إلى مواصلة عمل فريق الخبراء المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية وإلى النظر في إمكانية التوسُّع في الدراسة الشاملة التي يجريها المكتب عن الجريمة السيبرانية. وأكَّد متكلِّمون آخرون أنَّ فريق الخبراء هو المحفل المناسب لمناقشة مزايا النظر في الحاجة إلى صك قانوني عالمي جديد لمكافحة الجرائم السيبرانية قياساً على مواصلة الاعتماد على اتفاقية الجريمة المنظَّمة والصكوك الإقليمية المنطبقة.

٩- وأشار بعض المتكلِّمين إلى أنَّ جمع معلومات بشأن حالة تطبيق الاتفاقية في التشريعات الوطنية وتحديد الاحتياجات من المساعدة التقنية على نحو صحيح يتطلَّبان وضع آلية لاستعراض اتفاقية الجريمة المنظَّمة. وأشار متكلِّمون آخرون إلى أنَّ الفريق العامل المعني بالتعاون الدولي ليس المحفل المناسب لحسم مسألة آلية الاستعراض.

## باء- تحقيق أقصى قدر من الكفاءة، بطرائق منها استخدام ضباط الاتصال وآليات التبادل الخاصة بأجهزة الشرطة

١٠- نظر الفريق العامل، في جلستيه الأولى والثانية المعقودتين في ٢٧ تشرين الأول/أكتوبر ٢٠١٥، في البند ٣ من جدول الأعمال، وهو البند المعنون "تحقيق أقصى قدر من الكفاءة، بطرائق منها استخدام ضباط الاتصال وآليات التبادل الخاصة بأجهزة الشرطة". وأدار المناقشةَ في إطار هذا البند من جدول الأعمال المناظران ريكاردو أندرادي سادي (البرازيل) وسيزار موريسيو رودريغيس زاراتي (كولومبيا).

١١- وتبادل المتكلِّمون معلومات عن تجاربهم المتعلقة باستخدام ضبَّاط الاتصال وقضاة الاتصال المنتدَبين للعمل لدى أجهزة أجنبية لإنفاذ القانون أو لدى منظمات حكومية دولية،

مثل المنظمة الدولية للشرطة الجنائية (الإنتربول) ومكتب الشرطة الأوروبي (يوروبول) والمركز الأوروبي للجريمة السيبرانية، ومعلومات عن تجارب ناجحة في مجال التعاون الدولي. وشملت تلك التجارب الناجحة في مجال التعاون الدولي حالات اضطلع فيها ضبَّاط اتصال أو قضاة اتصال بدور هام في إجراء تحقيقات فعَّالة عبر الحدود، بسبل منها تيسير إعداد طلبات المساعدة القانونية المتبادلة المقدَّمة إلى دولهم، وتقديم معلومات بشأن ما يلزم إدراجه في طلبات تسليم المطلوبين وإجراءات التسليم. وأشير أيضاً إلى أنَّ ضابط الاتصال الذي يعمل في بلد ما يمكنه أن ييسِّر التعاون مع بلدان أخرى في المنطقة، وأنَّ فعالية استخدام ضباط الاتصال أو قضاة الاتصال تتعزَّز بالتدريب المتخصِّص على كيفية استخدام اتفاقية الجريمة المنظَّمة والصكوك الدولية المنطبقة الأخرى، والنظام القانوني للبلد المضيف وقوانينه الوطنية. وشُدِّد على أنَّ الشرط اللازم للنجاح في عملية انتداب ضبَّاط الاتصال أو قضاة الاتصال للعمل في ولايات قضائية أجنبية أو لدى منظمات حكومية دولية هو وجود ولايات واضحة ومحدَّدة بدقة بشأن دورهم ومهامهم. وسلَّط متكلِّم الضوء على أهمية مساهمة ضباط الاتصال أو قضاة الاتصال، ولكنه أشار أيضاً إلى الحاجة إلى ضمان تدخُّل القضاء أو الادِّعاء العام في الإجراءات المتَّخذة في ذلك الشأن. وأشار أحد المتكلِّمين إلى أهمية وضع آليات تنسيق داخلية من أجل مكافحة غسل الأموال والجرائم الأخرى، وعَرَضَ الخبرةَ التي اكتسبتها حكومته في ذلك الصدد.

١٢- وناقش المتكلِّمون مسألة جدوى التعاون بين أجهزة الشرطة ومسألة مقبولية الأدلة التي تجمع من خلال التعاون الدولي. كما ناقش المتكلِّمون أهمية أن تكون السلطات المحلية على علم بالمتطلبات القانونية والمقتضيات الإجرائية المتعلقة بجمع واستخدام مختلف أنواع الأدلة، فتحدِّد، على سبيل المثال، الحالات التي يمكن فيها الحصول على تلك الأدلة من خلال التعاون غير الرسمي فيما بين أجهزة الشرطة أو الحالات التي يجب فيها استخدام قنوات اتصال أكثر اتِّساماً بالطابع الرسمي. وشدَّد بعض المتكلِّمين أيضاً على فائدة التكنولوجيات المتاحة في تيسير التعاون الدولي.

## جيم- معلومات محدَّثة من الأمانة عن أدواتها ذات الصلة بالتعاون الدولي، بما في ذلك فيما يخصُّ جمع المعلومات عن تنفيذ الأحكام المتعلقة بالتعاون الدولي من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية

١٣- نظر الفريق العامل، أثناء جلسته الثانية المعقودة في ٢٧ تشرين الأول/أكتوبر ٢٠١٥، في البند ٤ من جدول الأعمال، وهو البند المُعنون "معلومات محدَّثة من الأمانة عن أدواتها ذات الصلة بالتعاون الدولي، بما في ذلك فيما يخصُّ جمع المعلومات عن تنفيذ الأحكام المتعلقة بالتعاون الدولي من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية". وقدَّم ممثِّلون للأمانة عروضاً يَسَّرت النقاشَ بشأن هذا البند من جدول الأعمال.

١٤- وناقش المتكلِّمون جدوى شتَّى الأدوات التي استحدثتها الأمانةُ ومنظماتٌ حكومية دولية أخرى من أجل تيسير التعاون الدولي؛ ومنها مثلاً أداة كتابة طلبات المساعدة القانونية المتبادلة التي استحدثها المكتب ومبادرة الإنتربول المتعلقة بالمعالجة الإلكترونية لمسائل تسليم المطلوبين. ولوحظ أنَّ من الضروري توفير استمارات موحَّدة تخصُّ طلبات المساعدة القانونية المتبادلة، وأنَّ من المهم مع ذلك أن تكون الدول على دراية بما لدى الدول المتلقِّية للطلبات من معايير خاصة بشأن الحصول على أنواع معيَّنة من الأدلة الإثباتية.

١٥- ودعا أحد المتكلِّمين إلى الإكثار من استخدام أشكال جديدة من التكنولوجيا، بما في ذلك، حيثما يكون مناسباً، المنصَّات الحاسوبية، على الصعيد الثنائي والإقليمي والدولي لتعزيز التعاون الدولي على النحو المنصوص عليه في اتفاقية الجريمة المنظَّمة، ولا سيما في المادتين ١٦ و١٨. وأشار أحد المتكلِّمين في هذا الصدد إلى مسألة أمن الاتصالات (التشفير) ومتطلبات التوثيق.

١٦- وناقش الفريق العامل دليل السلطات الوطنية الذي أَعدَّه المكتب بموجب اتفاقية عام ١٩٨٨ واتفاقية الجريمة المنظَّمة، حيث دار نقاش بين المتكلِّمين بشأن ما إذا كان من المفيد بقدر أكبر تقسيم الدليل إلى جزأين، يتضمَّن أحدهما معلومات عن السلطات المركزية المعيَّنة بمقتضى مختلف الأحكام التعاهدية ذات الصلة بالمساعدة القانونية المتبادلة، ويتضمَّن الآخر معلومات عن سائر السلطات المختصة وعن القنوات وسُبل التعاون غير الرسمي. وأعرب الكثير من المتكلِّمين عن تأييد الاقتراح المتمثِّل في إنشاء مكوِّنين منفصلين على النحو المبيَّن أعلاه تجنُّباً للالتباس وتيسيراً للتعاون الرسمي وغير الرسمي على حدٍّ سواء.

## دال- استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية كأساس قانوني للتعاون الدولي على مكافحة جميع أشكال الجريمة المنظَّمة عبر الوطنية

١٧- نظر الفريق العامل، أثناء جلسته الثالثة المعقودة في ٢٨ تشرين الأول/أكتوبر ٢٠١٥، في البند ٥ من جدول الأعمال، وهو البند المعنون "استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية كأساس قانوني للتعاون الدولي على مكافحة جميع أشكال الجريمة المنظَّمة عبر الوطنية". وتولَّت المناظِرةُ دانا ماريا رومان (رومانيا) مهمةَ تسيير مناقشة هذا البند من جدول الأعمال.

١٨- وتبادل المتكلِّمون تجاربهم في مجال استخدام اتفاقية الجريمة المنظَّمة كأساس قانوني للتعاون في عدَّة مجالات، منها المساعدة القانونية المتبادلة، وتسليم المطلوبين، ومصادرة عائدات الجريمة، ونقل الأشخاص المحكوم عليهم، وأساليب التحرِّي الخاصة، والتحقيقات المشتركة. وأشار المتكلِّمون إلى استخدام الاتفاقية من أجل التعامل مع أشكال الجريمة التقليدية والجديدة والمستجدَّة على حدٍّ سواء، بما في ذلك الاتجار بالمخدِّرات والفساد والجرائم السيبرانية وجرائم الحياة البرية والاتجار بالممتلكات الثقافية. وشدد المتكلِّمون في ذلك الصدد على القيمة المضافة للاتفاقية، وما تنطوي عليه من قدرة هائلة على استخدامها كأساس قانوني للتعاون الدولي، وأشاروا بصورة خاصة إلى أحكام معيَّنة من الاتفاقية تهدف إلى النهوض بهذا الاستخدام (مثل الفقرتين ٣ و٦ من المادة ١٦؛ والفقرتين ٣ و٧ من المادة ١٨). ولوحظ أنه يمكن تفادي التعارض المحتمل بين الولايات القضائية أو انتهاك قاعدة عدم جواز المحاكمة مرتين على نفس الجرم باستخدام الاتفاقية الأوروبية المتعلقة بنقل الدعاوى الجنائية عندما يسمح التشريع الوطني بذلك. وعُرضت أيضاً أدلة على الفريق العامل، من خلال حالات وإحصاءات محدَّدة، بشأن زيادة استخدام الاتفاقية كأساس قانوني لتعزيز التعاون الدولي في قضايا الجرائم السيبرانية وفيما يتعلق بجرائم أخرى مثل الفساد.

١٩- وناقش الفريق العامل كذلك "التفاعل" بين اتفاقية الجريمة المنظَّمة وغيرها من المعاهدات الثنائية أو المتعدِّدة الأطراف المستخدمة كأُسس قانونية للتعاون الدولي. وأُشير إلى أنَّ هناك دولاً لا تقبل بالاتفاقية كأساس قانوني لتسليم المطلوبين وأنَّ المعاهدات الثنائية والإقليمية والمتعدِّدة الأطراف والمعاملة بالمثل يمكن أن يكون لها علاقة تكاملية في تعزيز التعاون الدولي وتسهيله. وقدَّم المتكلِّمون أمثلةً على حالات يستند فيها اختيار الصك القانوني المنطبق إلى معايير معيَّنة، مثل تيسير التعاون الدولي وفعاليته. كما قدَّم المتكلِّمون أمثلةً على تشريعات وطنية وممارسات وطنية تتيح، في حالات معيَّنة، استخدام اتفاقية الجريمة المنظَّمة لأغراض تسليم المطلوبين.

٢٠- وناقش الفريق العامل المادة ١٨ من الاتفاقية، بشأن المساعدة القانونية المتبادلة. وأشار أحد المتكلِّمين إلى رفض النظراء الأجانب في بعض المشاورات مع بلده استخدامَ الاتفاقية كأساس قانوني للمساعدة القانونية المتبادلة وتفضيلهم التفاوضَ بشأن معاهدات ثنائية معرباً عن قلقه من أن تؤدِّي هذه الممارسة إلى صعوبات كبيرة نظراً لأنَّ عملية التفاوض بشأن معاهدات ثنائية هي عملية شاقة تتطلَّب مواردَ ضخمةً بل ونظراً أيضاً لاختلاف المعايير التي يمكن أن تنشأ عن ذلك فيما يخصُّ ممارسات التعاون الدولي. واتَّفق بعض المتكلِّمين على أنَّ عدم امتثال بعض الدول الأطراف للمادة ١٨ يشكِّل مصدر قلق. وركَّز الفريق العامل على الفقرة ٣٠ من المادة ١٨، حيث طرحت وفودٌ تفسيرات مختلفة فيما يتعلق بمعنى "اتفاقات أو ترتيبات ثنائية أو متعدِّدة الأطراف". وبصرف النظر عن التفسيرات المختلفة، لوحظ أنه لا ينبغي تفسير الفقرة ٣٠ من المادة ١٨ على أنها تقوِّض التزام الدول الأطراف بأن يُقدِّم بعضها لبعض أكبر قدر ممكن من المساعدة القانونية المتبادلة؛ وإنها ينبغي التعامل مع تلك الفقرة على أنها حكم تكميلي، يُقرأ بالاقتران مع الفقرة ٧ من المادة ١٨.

٢١- وأُشير إلى أنَّ لدى بعض الدول معلومات وافية عن استخدامها للاتفاقية كأساس قانوني للتعاون الدولي؛ غير أنَّ الأمانة أفادت بأنه ليس لديها أي إحصاءات محدَّدة عن هذا الموضوع، إذ لم تُجرَ هيكلة تقديم التقارير منذ عام ٢٠٠٨. وأُشير أيضاً إلى المناقشات الجارية في الاجتماع الحكومي الدولي المفتوح العضوية المعني باستكشاف جميع الخيارات المتعلقة بوضع آلية مناسبة وفعَّالة لاستعراض تنفيذ اتفاقية مكافحة الجريمة المنظَّمة والبروتوكولات الملحقة بها.

## هاء- مسائل أخرى

٢٢- نظر الفريق العامل، أثناء جلسته الثالثة المعقودة في ٢٨ تشرين الأول/أكتوبر ٢٠١٥، في البند ٦ من جدول الأعمال، وهو البند المعنون "مسائل أخرى". ولاحظ الرئيس أنَّ الأمانة سوف تيسِّر الإبلاغ عن النقاط البارزة المنبثقة من مداولات الفريق العامل، فضلاً عن توصياته، أثناء اجتماع الخبراء الحكومي الدولي الرابع المفتوح المشاركة لتعزيز التعاون الدولي في إطار اتفاقية الأمم المتحدة لمكافحة الفساد، المُزمع عقده في سانت بطرسبرغ، الاتحاد الروسي، يومي ٢ و٣ تشرين الثاني/نوفمبر ٢٠١٥، بالتوازي مع انعقاد الدورة السادسة لمؤتمر الدول الأطراف في اتفاقية الأمم المتحدة لمكافحة الفساد. وأشير إلى أنَّ الغرض من هذا الإبلاغ هو مواصلة تعزيز الترابط وتبادل المعلومات بين هاتين الهيئتين المتخصِّصتين.

# رابعاً- تنظيم الاجتماع

## ألف- افتتاح الاجتماع

٢٣- اجتمع الفريق العامل يومي ٢٧ و٢٨ تشرين الأول/أكتوبر ٢٠١٥، وعقد ما مجموعه أربع جلسات.

٢٤- وترأس الجلسات توماس بوروز (الولايات المتحدة).

## باء- الكلمات

٢٥- في إطار البنود ٢ إلى ٧ من جدول الأعمال أدلى بكلمات ممثِّلو الدول التالية الأطراف في الاتفاقية: الاتحاد الروسي، الأرجنتين، إسبانيا، أفغانستان، إكوادور، إيطاليا، باكستان، البرازيل، البرتغال، بيرو، الجمهورية التشيكية، جنوب أفريقيا، رومانيا، الصين، عُمان، غانا، غواتيمالا، فرنسا، كندا، كوبا، كوستاريكا، كولومبيا، كينيا، مصر، المغرب، المكسيك، الهند، هولندا، الولايات المتحدة الأمريكية.

٢٦- وأدلى بكلمة أيضاً المراقبان عن اليابان وجمهورية كوريا، الدولتين الموقِّعتين على الاتفاقية.

٢٧- وقدَّم ممثِّلون للأمانة عروضاً في إطار البنود ٢ و٣ و٤ و٥ من جدول الأعمال.

## جيم- إقرار جدول الأعمال وتنظيم الأعمال

٢٨- أَقرَّ الفريق العامل، أثناء جلسته الأولى المعقودة في ٢٧ تشرين الأول/أكتوبر ٢٠١٥، بتوافق الآراء جدول أعماله المؤقَّت وتنظيم الأعمال. وفيما يلي نصُّ جدول الأعمال:

١- المسائل التنظيمية:

(أ) افتتاح الاجتماع؛

(ب) إقرار جدول الأعمال وتنظيم الأعمال.

٢- جمع وتبادل الأدلة الإثباتية الإلكترونية.

٣- تحقيق أقصى قدر من الكفاءة، بطرائق منها استخدام ضباط الاتصال وآليات التبادل الخاصة بأجهزة الشرطة.

٤- معلومات محدَّثة من الأمانة عن أدواتها ذات الصلة بالتعاون الدولي، بما في ذلك فيما يخصُّ جمع المعلومات عن تنفيذ الأحكام المتعلقة بالتعاون الدولي من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية.

٥- استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية كأساس قانوني للتعاون الدولي على مكافحة جميع أشكال الجريمة المنظَّمة عبر الوطنية.

٦- مسائل أخرى.

٧- اعتماد التقرير.

## دال- الحضور

٢٩- حضر الاجتماعَ ممثِّلو الدول التالية الأطراف في الاتفاقية: الاتحاد الروسي، الأرجنتين، إسبانيا، أفغانستان، إكوادور، الإمارات العربية المتحدة، إندونيسيا، أنغولا، أوروغواي، آيرلندا، إيطاليا، باكستان، البحرين، البرازيل، البرتغال، بنما، بولندا، بوليفيا (دولة-المتعدِّدة القوميات)، بيرو، تايلند، تركيا، تونس، الجزائر، الجمهورية التشيكية، الجمهورية الدومينيكية، جنوب أفريقيا، رومانيا، سان مارينو، السلفادور، سلوفاكيا، السودان، السويد، سويسرا، شيلي، الصين، العراق، عُمان، غانا، غواتيمالا، فرنسا، الفلبين، فنزويلا (جمهورية-البوليفارية)، فنلندا، قبرص، قطر، الكرسي الرسولي، كرواتيا، كندا، كوبا، كوستاريكا، كولومبيا، كينيا، لبنان، مدغشقر، المغرب، المكسيك، المملكة العربية السعودية، ميانمار، النرويج، النمسا، نيجيريا، الهند، هنغاريا، هولندا، الولايات المتحدة الأمريكية، اليمن.

٣٠- وحضر الاجتماعَ ممثلٌ للاتحاد الأوروبي، وهو منظمة تكامل اقتصادي إقليمية طرف في الاتفاقية.

٣١- وحضر الاجتماعَ بصفة مراقب ممثلون لليابان وجمهورية كوريا، الدولتين الموقِّعتين على الاتفاقية.

٣٢- وحضر الاجتماعَ بصفة مراقب ممثلٌ للوكالة المتخصِّصة التالية التابعة لمنظومةِ الأممِ المتحدة: منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو).

٣٣- وحضر الاجتماعَ بصفة مراقب ممثِّلو المنظمات الحكومية الدولية التالية: المنظمة الاستشارية القانونية الآسيوية-الأفريقية، والشبكة القضائية الأوروبية، ومكتب الشرطة

الأوروبي، وجامعة الدول العربية، ومنظمة الأمن والتعاون في أوروبا، ومنظمة التعاون والتنمية في الميدان الاقتصادي.

٣٤- وترد في الوثيقة CTOC/COP/WG.3/2015/INF/1/Rev.1 قائمة بأسماء المشاركين.

## هاء- الوثائق

٣٥- عُرضت على الاجتماع الوثائقُ التالية:

(أ) جدول الأعمال المؤقَّت وشروحه (CTOC/COP/WG.3/2015/1)؛

(ب) ورقة معلومات أساسية من إعداد الأمانة عن جمع وتبادل الأدلة الإثباتية الإلكترونية (CTOC/COP/WG.3/2015/2)؛

(ج) ورقة معلومات أساسية من إعداد الأمانة عن استخدام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية كأساس قانوني للتعاون الدولي على مكافحة الجريمة المنظَّمة عبر الوطنية (CTOC/COP/WG.3/2015/3).

## خامساً- اعتماد التقرير

٣٦- في ٢٨ تشرين الأول/أكتوبر ٢٠١٥ اعتمد الفريقُ العامل هذا التقريرَ عن اجتماعه.

# قائمـــة المـــراجـــع

## قائمة المصادر والمراجع:

### أولا / الكتب :

#### أ- العامة:


**01/-** الدكتور. عادل يحيى قرني ، التحقيق و المحاكمة الجنائية عن بعد ، دار النهضة العربية ، الطبعة الأولى ، مصر ، 2006.

**02/-** عبد الحكيم فودة ، حجية الدليل الفني في المواد الجنائية و المدنية ، دار الفكر الجامعي ، الطبعة الأولى ، مصر ، 1996.

**05/-**عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة ، منشورات الحلبي الحقوقية، الطبعة الثانية ، بيروت لبنان، 2003.

**03/-** الدكتور.عمار بوضياف ، النظام القضائي الجزائري ، دار ريحانة ، الطبعة الأولى ، الجزائر ، 2003 .

**04/-**عمر محي الدين حوري ، الجريمة" أسبابها و مكافحتها "دراسة مقارنة في الشريعة و القانون و العلوم الاجتماعية ، المطبعة العلمية ، الطبعة الأولى ، سوريا، 2003 .

**07/-** مأمون محمد سلامة ،الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية للنشر و التوزيع ، الجزء الأول ، الطبعة الأولى ، مصر ، 2008.

**06/-** الدكتور .محمد سامي الشوا ، ثورة المعلومات و انعكاساتها على قانون المعلومات ، دار النهضة العربية للنشر و التوزيع ، الطبعة الأولى ، مصر ، 1994.


#### ب- المتخصصة:


**01/-** الدكتور . أحمد خليفة الملط " الجرائم المعلوماتية " ، دار الفكر الجامعي ، الطبعة الثانية ، مصر، 2006 .

**02/-** الدكتور. اشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الالكترونية ، دار الجامعة الجديدة للنشر ،الطبعة الأولى ، مصر، 2015 .

**03/-** الدكتور.جميل عبد الباقي الصغير ، الانترنت و القانون الجنائي ، الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، دار النهضة العربية ، الطبعة الأولى ، مصر،2001 .

**04/-** الدكتور. جميل عبد الله ، حجية مخرجات الكمبيوتر في المواد الجنائية ، دراسة مقارنة ، دار النهضة العربية ، الطبعة الأولى ، مصر ، 2016 .

**05/-** حسن طاهر داود ، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم ألمانية ، الطبعة الأولى ، السعودية ، 2000 .

**06/-** خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، دار الثقافة للنشر والتوزيع ، الطبعة الأولى ، الأردن، 2011 .

**07/-** خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية ، الطبعة الأولى ، مصر ،2009 .

**08/-** خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الأولى ، دار الفكر الجامعي ، مصر ، 2009 .

09/- طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة ، الطبعة الأولى ، مصر، 2010 .
10/- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة للنشر ، دون طبعة ، مصر،2010.
11/- عبد العالي هلالي عبد الإله احمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية ، الطبعة الأولى ، مصر 1997.
12/- الدكتور. عبد الفتاح بيومي حجازي ، الإثبات في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، الطبعة الأولى ، مصر ، 2004.
13/- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية ، بدون طبعة ، مصر،2007 .
14/- عبد الفتاح مراد ، شرح جرائم الكمبيوتر و الانترنت ، دار الكتب و الوثائق المصرية ، الطبعة الأولى ، مصر، 1900 .
15/- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي ، دار النهضة العربية ، الطبعة الثانية ، مصر ،2001 .
16/- الدكتور عمر محمد بن يونس ، الإجراءات الجنائية عبر الانترنت ، المرشد الفدرالي الامريكي لتفتيش و ضبط الحواسيب وصولا للدليل الالكتروني في التحقيقات الجنائية ، دون ناشر ، و.م.ا ، 2008.
17/- الدكتور. عميمر عبد القادر - التحديات القانونية لإثبات الجريمة المعلوماتية - النشر الجامعي الجديد _الجزائر_ ، طبعة 2021 .
18/- محمد أمنية الشوايكة جرائم الحاسوب والأنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع ، الطبعة الأولى ، مصر ، 2009 .
19/- ناير نبيل عمر-الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية -دار الجامعة الجديدة ، الطبعة الأولى ، مصر ، 2012 .
20/- نبيلة هبه هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دار الفكر الجامعي ، بدون طبعة ، مصر ، 2007 .
21/- هشام محمد رستم : الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، الطبعة الأولى ، مصر ، 1994 .
22/- هلالي عبد ألاله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، دار النهضة العربية، الطبعة الأولى ، مصر ،1997 .
23/- يونس عرب ، موسوعة القانون و تقنية المعلومات-دليل أمن المعلومات و الخصوصية الجزء الأول -جرائم الكمبيوتر و الانترنت ، منشورات اتحاد المصارف العربية ، الطبعة الأولى، الأردن، 2002 .

## ثانيا / الدراسات و البحوث الأكاديمية :

### أ- أطروحة دكتوراه :

01/- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر(1) ، 2010- 2011

02/- محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس، 2004 .
03/- مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الانترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة،2011 .
04/- وفاء عمران ، تعامل القاضي الجزائي مع الدليل العلمي –دراسة مقارنة - ، أطروحة دكتوراه ، تخصص قانون العقوبات و العلوم الجنائية ، جامعة قسنطينة 1 ، الموسم الجامعي 2019/2018.

أ- رسالة ماجيستير :

01/- أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة،2007 .
02/- الحسن الطيب عبد السلام الحضيري ، الإثبات الجنائي بالوسائل العلمية الحديثة ( دراسة مقارنة بين القانون الجنائي الليبي والفقه المعاصر ) ، رسالة ماجستير ،جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج ،اندونيسيا ، فيفري 2016.
03/- بوخبزة عائشة ، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماجستير ، تخصص قانون جنائي ، كلية الحقوق ، جامعة وهران ، 2013.
04/- طرشي نورة ، مكافحة الجريمة المعلوماتية ، مذكرة ماجستير ، تخصص قانون جنائي ، كلية الحقوق ، جامعة الجزائر 01 ، الموسم الجامعي 2012/2011.
05/- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي "دراسة مقارنة" ، رسالة ماجستير ، كلية الحقوق ، جامعة الإسكندرية ، 2009 .

ثالثا / المقالات :

01/- أستاذ عبيدة سليمة ، مسار انضمام الجزائر للمنظمة العالمية للتجارة ، مجلة الاقتصاد الجديد ، العدد 08 ، ماي 2013.
02/- بن فردية محمد ، الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائي ( دراسة مقارنة ) ، Revue académique de la recherche juridique , vol, 5 ,n°1
03/- الدكتورة . بوضياف اسمهان ، الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، العدد11 ، سبتمبر 2018.
04/- جاسم خريبط خلف ،" الضبط القضائي في جرائم الانترنت"، مجلة جامعة ذي قار، العدد4 ، البصرة،2009 .
05/- الدكتور.عائشة عبد الحميد ، النظام القانوني للمنظمة الدولية للشرطة الجنائية ( الانتربول) و دورها في مجال التعاون الدولي الشرطي ، المجلة الأكاديمية للأبحاث و النشر العلمي ،الإصدار11 ، تاريخ 2020/03/05 ، ISSN2706-6495
06/-عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية ، المجلة الكبرى ، 2008 ، Collation: 308 ، ISBN: 9775237750 .

07/-غلاي محمد ، احترام أصل البراءة مطلب من متطلبات دولة القانون ، دار بلقيس ، المجلة الوطنية ، الجزائر ، 2012 ، متوفرة على الرابط التالي :
http://dspace.univ-tlemcen.dz/handle/112/252
08/- الدكتور. عمر فاروق الحسيني ، تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي ، مجلة المحاماة ، السنة 12 ، عدد نوفمبر/ديسمبر ، 1989.
09/-الدكتور. لورنس سعيد الحوامدة ، حجية الأدلة الرقمية في الإثبات الجنائي دراسة تحليلية مقارنة ، مجلة البحوث الفقهية و القانونية ، العدد36 ، أكتوبر 2021.
10/- مجلة الفكر البرلماني ، مجلس الأمة الجزائري ، جويلية ، 2008.
11/- محمد عادل ريان ، جرائم الحاسب الآلي و أمن البيانات ، العربي ، (440)، متوفر على الرابط التالي : www.anaharonline.com
12/- محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي،مجلة العلوم الإنسانية ، العدد 3 ، 2021 ، على الرابط التالي :
http://revue.umc.edu.dz/index.php/h/article/view/3737ذ

**رابعا / الندوات و أيام الدراسية :**

01/- ارزقي سي حاج محند ، الإثبات الالكتروني في المادة الجزائية ، مداخلة ضمن ندوة "وسائل الإثبات الحديثة" ، مركز البحوث القانونية و القضائية ، 2015/02/05.
02/- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري،" الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العرابية للعلوم الأمنية، الرياض،2007 .
03/- علي محمود علي حمودة،" الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع1 ، دبي - الإمارات العربية المتحدة 26-28 نيسان2003 .
04/- عمرو حسين عباس،" بحث في أدلة الإثبات الجنائي والجرائم الإلكترونية " (المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من26-04/27-2008، مقر جامعة الدول العربية .
05/- موسى مسعود ارحومة،" الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية"، المؤتمر المغاربي الأولى حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس،29 ،28- 09 - 2009 .

**خامسا / التقارير:**

01/- تقرير صادر عن مركز هردو لدعم التعبير الرقمي ، الجريمة الالكترونية و حجية الدليل الرقمي في الإثبات الجنائي ، القاهرة ، 2014 .
02/- مؤتمر الدول الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، الفريق العامل المعني بالتعاون الدولي ، ورقة معلومات أساسية ، " جمع و

تبادل الأدلة الاثباتية الالكترونية " ، الوثيقة CTOC/cop/wG3/2015/2 الصادرة في 2015/08/18.

**سادسا / القرارات:**

**03/-** قرار غرفة الاستئناف لمحكمة الجنايات الدولية الصادر بتاريخ 2009/02/23 بخصوص رفض دفاع "دومينيك اونغوان" لأحكام الغرفة التمهيدية للمحكمة ، الوثيقة ICC-02/04-179 .

**04/-** قرار صادر عن غرفة المخالفات و الجنح للمحكمة العليا في الملف رقم 37941 بتاريخ 1987/05/07.

**05/-** قرار صادر عن محكمة النقض المصرية رقم 360 بتاريخ 1976/06/06 و قرار أخر صادر عن ذات الهيئة رقم 929 بتاريخ 1992/10/13.

**06/-** قرار صادر عن الغرفة الجزائية الثانية بالمحكمة العليا ، قضية رقم 25814 ، صادر بتاريخ 1982/01/05.

**سابعا / النصوص القانونية :**

**01/-** الدستور الجزائري 2020 ، الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق لـ30 ديسمبر سنة 2020 في الجرية الرسمية العدد 82

**02/-** قانون رقم( 08- 19) ،المؤرخ في 2008/11/15 ، الجريدة الرسمية العدد 63 ، المؤرخة في-11-2008 16 والمتضمن الدستور الجزائري المعدل والمتمم .

**03/-** قانون رقم 15-19 مؤرخ في 18 ربيع الأول عام 1437 الموافق لـ 30 ديسمبر سنة 2015 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 و المتضمن قانون العقوبات الصادر في الجريدة الرسمية / العدد 71 رقم 03 .

**04/-** قانون رقم66-155 ، المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06-22 ، المؤرخ في2006/12/20 ، الجريدة الرسمية العدد 84 ،مؤرخة في 2006/12/24.

**05/-** القانون 05-10 مؤرخ في 20 جوان 2005 يعدل و يتمم القانون المدني الجزائري .

**06/-** القانون 06-22 ، مؤرخ في 2006/12/20 ،ج.ر 84 ، الصادرة في 2006/12/24.و انظر أيضا د/ شيخ ناجية ، أساليب البحث و التحري المستحدثة في القانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري ، المجلة النقدية للقانون و العلوم السياسية ، السنة 08 ، العدد01.

**07/-** القانون 14-04 المؤرخ في 2004/11/10 المعدل و المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية الجزائري الجريدة الرسمية رقم 71 بتاريخ 2004/10/10.

**08/-** قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، الصادر في الجريدة الرسمية العدد 37 ، المؤرخة في 16 غشت سنة 2009 .
**09/-** القانون 2000-03 –يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية ، الصادر في 2000/08/05 ، ج.ر عدد 48 الصادرة في 2000/08/06-
شبكة المواصلات السلكية و اللاسلكية .
**10/-** القانون 18-04 مؤرخ في 2018/05/10 يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، ج.ر عدد 27 الصادرة في 2018/05/13.
**11/-** المرسوم الرئاسي 183/04 المؤرخ في 2004/06/26 المتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك و تحديد قانونه الأساسي ، ج.ر عدد41 الصادرة في 2004/06/27 المعدل و المتمم بمقتضى المرسوم الرئاسي 118/09 الصادر في 2009/04/14 ، ج .ر عدد 24 الصادرة في 2009/04/22.
**12/-** المرسوم الرئاسي 261/15 مؤرخ في 2015/10/08 يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج.ر. عدد 53 الصادرة في 2015/10/08 .المعدل ب المرسوم الرئاسي 172/19 الصادر في 2019/06/06 ، ج.ر.عدد 37 المؤرخة في 2019/06/09.
**13/-** المرسوم التنفيذي 257/98 يضبط شروط و كيفيات إقامة خدمات الانترنت و استغلالها الصادر في 1998/08/25 يتمم بعض الأحكام التنظيمية للمرسوم التنفيذي 75-98 يتضمن قانون البريد و المواصلات مؤرخ في 1975/12/30.
**14/-** المرسوم التنفيذي 348/06 المتضمن تمديد الاختصاص المحلي لبعض المحاكم وكلاء الجمهورية و قضاة التحقيق ، الصادر في 2006/10/05، ج.ر. عدد 63 .

## ثامنا / الإتفاقيات :

**01/-** إتفاقية فيينا لقانون المعاهدات (وسائل التعبير عن رضا الدولة ) ، العرض للتوقيع في 23 /05/ 1969 ، دخول حيز النفاذ في 01/27/ 1980
**02/-** اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، تاريخ الاعتماد و العرض للتوقيع و التصديق 2000/10/15 ، دخول حيز النفاذ 2003/09/29 طبقا لمادتها 38 ، عدد الأطراف 190 منذ 2018/08/26 .
**03/-** اتفاقية مكافحة الجريمة الالكترونية "بودابست" ، توقيع 2001/11/23 ، حيز النفاذ 2004/07/01 .
**04/-** اتفاقية برن لحماية المصنفات الفكرية و الفنية ، الإبرام 1886 ، بعد تعديلات متتالية ، اعتماد أخر نسخة في سبتمبر 1979 بباريس .و انظر أيضا علي حسن طوالبة ، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي .

## سابعا /إجتهادات قضائية :

**01/-** المجلة القضائية للمحكمة العليا ، العدد الرابع ،سنة 1990.

**ثامنا / المراجع الإلكترونية :**

**01/-** www.arabip.center.com/public/events/papers/paper 2-4. pdf.

**02/-** علي حسن الطوالبه،" مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة بحث منشور على شبكة الانترنت على موقع التالي:
www.policeme.gouvbh/reports/2011/April/13-14-2011/634383168746341670.pdf. (le 06-05-2022 à 17:00 h)
http://www.cnejita.org/dac/collague 20100513 Actes.PDF(le 09-05-2022 à 14:30 h)

**03/**https ://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_ aeec_fr.pdf. (le 12-05-2022 à 18:00 h)

**04/-**http ://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim-tech-info-pdf. (le 13-05-2022 à 22:00 h)

**05/**https ://treaties.un.org/pages/ViewDetails.aspx ?src=IND&mtdsg_no=XVIII-12&chapter=18&clang=_fr. (le 14-05-2022 à 09:00 h)

**06/-** https://www.algeriepolice.dz(le 16-05-2022 à 16:30 h)

**تاسعا/ المراجع باللغة الفرنسية :**

**أ- رسالة ماجيستير:**

**01/-** O.Nober , L'encadrement du raisonnement du juge des faits au sein du procès pénal ,mémoire de maitrise en Droit ,université Laval ,Canada ,2017.

**أ- تقارير:**

**02/-** A.E.C Tamano ,l'admissibilité de la preuve électronique devant les tribunaux .

**03/-**compagnie nationale des experts de justice en informatique et techniques associées , la preuve numérique à l'épreuve du litige , colloque organisé par la première chambre de la cour d'Appel de Paris le 13/04/2010 ,p.9. disponible sur :
https://www.lagbd.org/images/3/3a/Colloque_CNEJITA_13_Avril_2010.pd

.

# الفهـــــرس

**الفهـــرس :**

---

**الشكر و التقدير**

**الإهـــداء**

**قائمة المختصرات..... أ**

**مقـــدمة.....3،4،5،6**

**الفصل الأول : المتابعة الجزائية للجرائـــــم الإلكترونيـــــــة. ..... 7**

**المبحث الأول: الجريمة الإلكتـــرونيـــة . ..... 9**

**المطلب الأول: مفهـــــوم الجريمة الإلكتـــرونيـــة . ..... 9**

**الفرع الأول : تعريف الجريمة الإلكترونيـة ..... 10**

أولا: تعريف الجريمة الإلكترونيـة فقها :..... 10

ثانيا: تعريف الجريمة الإلكترونيـة قانونا :..... .10

**الفرع الثاني : خصـــائـــص الجريمة الإلكترونيـة ..... 12**

**المطلب الثاني: صـــور الجـــرائـــم الإلكتـــرونيـــة . ..... 13**

**الفرع الأول : تصنيف الجرائم الإلكترونية حسب إتفاقية بودابست الاوروبية . 13**

1-جريمة التوصل أو الدخول غير المصرح به:..... 14

2- جريمة الإستيلاء على المعطيات و سرقة وقت الكمبيوتر.....15

3-جريمة إحتيال الكمبيوتر..... 16

4-جريمة التزوير المعلوماتي..... 17

5-جريمة إتلاف و تدمير المعطيات و النظم ..... 18

**الفرع الثاني : تصنيف الجرائم الإلكترونية في قانون العقوبات الجزائري ..... 18**

**المبحث الثاني: طرق إثبات الجرائم الإلكترونية ..... 19**

**المطلب الأول: المعاينة و التفتيش و الشهادة في الجرائم الإلكتـــرونيـــة ..... 20**

**الفرع الأول : المعـاينـــة في الجرائم الإلكترونيـة ..... 21**

أولا - السلطة المختصة بإجراء المعاينة لمسرح الجرائم الإلكترونيـة : ..... 21

ثانيا :شروط صحة معاينة مسرح الجرائم الإلكترونيـة: ..... 22

**الفرع الثاني : التفتيـــش في الجريمـة الإلكتـــرونيـــة ..... 22**

**الفهـــرس :**

أولا-السلطة المختصة بتفتيش النظم الإلكترونيــة: ..... 24
ثانيا: شروط تفتيــش الجرائم الإلكترونيــة ..... 27
**الفرع الثالث : الشهادة في الجريمــة الإلكتـــرونيـــة** ..... 27
**المطلب الثاني: الضبـــط و الخبـــرة القضـــائيـــة و التسرب و النتصت و إعتراض المراسلات فـــي الجريمـة الإلكتـــرونيـــة ..... 34**
**الفرع الأول: الضبـــط في الجريمة الإلكتـــرونيـــة ..... 34**
أولا - ضبط المكونات المادية للحاسب الآلي ..... 35
ثانيا- ضبط المكونات المعنوية للحاسب الآلي ..... 36
**الفرع الثاني : التسرب و التنصت و إعتراض المراسلات في الجريمة الالكترونية.....38**
**الفرع الثالث: الخبـــــرة القضـــائيـــة في الجريمة الإلكتـــرونيـــة .. 43**
أولا : القواعد القانونية التي تحكم الخبرة القضائية في الجرائم الإلكترونيــة .... 43
ثانيا : القواعد الفنية التي تحكم الخبرة القضائية في الجرائم الإلكترونيــة ..... 47
ثالثا - عمل الخبير وأساليبه: ..... 49
رابعا-دور الخبير التقني في حفظ الأدلة الإلكترونية ..... 50
**الفصل الثاني : حجية الدليل الإلكتروني أمام القضاء الجزائي.....54**
**المبحث الأول الدليل الالكتروني في النظام الاتهامي و النظام التنقيبي ..... 55**
**المطلب الأول الدليل الالكتروني في النظام الاتهامي ( الانجلوسكسوني) ..... 56**
**الفرع الأول الدليل الالكتروني في ظل الإثبات المقيد ..... 57**
**الفرع الثاني شروط قبول الدليل الالكتروني في النظام الاتهامي ..... 58**
**المطلب الثاني : الدليل الالكتروني في النظام التنقيبي ..... 59**
**الفرع الأول الدليل الالكتروني في ظل "حرية الإثبات" ..... 59**
**الفرع الثاني ضوابط اقتناع القاضي بالدليل الالكتروني ..... 60**
أولا – الضوابط العامة ..... 61
ثانيا- الضوابط الخاصة بالدليل الالكتروني ..... 63
**المبحث الثاني الدليل الالكتروني في النظام القانوني الجزائري ..... 64**

**الفهـــرس :**

**المطلب الأول الدليل الأدوات التنفيذية و التشريعية للدليل الالكتروني في الجزائر ..... 64**

**الفرع الأول الأدوات التنفيذية و التشريعية الجزائية للأدلة الالكترونية في الجزائر ..... 65**

أولا – الهيئات المختصة بجمع الأدلة الالكترونية في جهاز الشرطة الوطنية. .....66

ثانيا- الأجهزة المكلفة بالأدلة الالكترونية على مستوى الدرك الوطني....67

ثالثا – الهيئة الوطنية للوقاية من جرائم الإعلام و الاتصال.....68

رابعا – المكتب المركزي الوطني لانتربول الجزائر.....69

**الفرع الثاني الدليل الالكتروني في النصوص التشريعية الجزائرية.....**70

أولا- الدستور الجزائري.....70

ثانيا – الاتفاقيات الدولية.....71

ثالثا – التشريع العادي ( القوانين الوطنية ).....75

**المطلب الثاني الدليل الالكتروني في تقدير القضاء الجزائي الجزائري**.....76

**الفرع الأول الاختصاص القضائي للنظر في الدليل الالكتروني**.....77

**الفرع الثاني سلطة القاضي الجزائي الجزائري في الأخذ الدليل الالكتروني**...78

**الخاتمة ..... 82**

**الملحق (مؤتمر الأطراف في إتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية )**

**قائمة المراجع ..... 86**

**الفهرس ..... 97**