جامعة محمد خيضر – بسكرة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

الحماية الجزائية للمستند الإلكتروني في التشريع الجزائري

مذكرة مكملة من مقتضيات نيل شهادة الماستر في العلوم القانونية والإدارية تخصص قانون جنائي

من إعداد الطالب:

عريبي عادل

تحت إشراف الأستاذة:

شرف الدين وردة

السنة الجامعية: **2017 /2018**

إهـــــداء

إلى من علماني أن الحياة طريق كفاح نهايته النجاح

إلى من أوصاني بهما ربي برا و إحسانا والدي (أمـــي و أبـــي) حفظهما الله

إلى أختي (أمنية) و أخواتي، إلى كل أفراد عائلتي

إلى كل من عرفتني بهم الدراسة... و كانوا أنسا لي في دربي

(أصدقائي و صديقاتي)

إلى كهوف المعرفة ... و لولاء العلم ... الذين كانوا لي قدوة ...

(كل أساتذتي)

إلى كل من ساهم في إتمام دراستي من بعيد أو من قريب

إلى كل هؤلاء أهدي ثمرة جهدي المتواضع.

عادل عريبي

شكر وتقدير

الحمد وحده و الشكر له سبحانه و تعالى على نعمه التي لا تعد ولا تحصى أن تفضل علي بالتوفيق لإنجاز هذا العمل، و أصلي و أسلم على الرحمة المهداة و السراج المنير سيدنا محمد صلى الله عليه و سلم و على آله و صحبه أجمعين في العالمين.

يشرفني عظيم الشرف أن أتوجه بالشكر الجزيل و الامتنان الكثير إلى أساتذتي الفاضلة، الأستاذة (وردة شرف الدين) و التي تولت مهمة الإشراف على هذا البحث.

أشكرها على كل نصائحها القيمة و جميل صبرها وحسن تواضعها و أسأل الله العلي القدير أن يزيدها رفعة و قدرا وعلما نافعا.

كما لا يفوتني أن أخلص بالشكر إلى كل من صنع لي معروفا و كل من كان لي عونا في أحد الأيام (أصدقائي و زملائي).

كما أشكر أعضاء لجنة المناقشة على مراجعتهم لما تم عرضه و تصويبهم له بما يرونهم الأصح.

شكـــرا

مقدمـــــة

اقتحمت المعلوماتية حياتنا اليومية فيوقت قياسي وبشكل رهيب لا سيما و أن المجتمع الجزائري لم يساير هذه التكنولوجيا منذ نشأتها، ووفرت هذه التكنولوجيا في مجال الاتصالات و المعلومات الإلكترونية،إمكانية تحقق التواصل الإنساني و تقديم الكثير من الخدمات التي تهم الإنسان.

حيث أصبحت وسائل الكنولوجيا الحديثة تساهم في نقل وحفظ و استرجاع المعلومات بالصوت والصورة والكتابة بين جميع أنحاء العالم، وشملت استعمالات الإنترنت في الآونة الأخيرة مختلف نشاطات الإنسان التجارية، الأمر الذي أدى إلى انتعاش التجارة محليا ودوليا. مما أدى إلىظهور مصطلحات و مفاهيم جديدة لم تكن موجودة من قبل، فظهر مصطلح التجارة الإلكترونية أو المعاملات الإلكترونية و ظهور أيضا ما يعرف بالحكومة الإلكترونية، كل هذا أدى إلى ظهور وسائل و أساليب الكترونية تقوم في الكثير من الأحيان بأداء وظائف المستندات التقليدية.

و قد تعرضت هذه المستندات إلى اهتزاز كبير بظهور المستندات الالكترونية، والتي تجسد تنفيذ فكرة " الحكومة الالكترونية "وعلاقتها بالأفراد والهيئات العامة و الخاصة، وذلك بتقديم الخدمات ذات الطابع الشخصي أو الإداري في أسرع وقت ممكن وأقل جهد و تكلفة، وبدقة عالية.

علاوة على ذلك فلقد أفرز انتقال مجال التجارة من المجال الواقعي إلى الافتراضي أنماطا جديدة وسلوكيات متعددة غير تقليدية، وبالتالي يعتبر المستند الالكتروني وسيلة لتحقيق التجارة الدولية و الداخلية لأهدافها، حيث أن المستند الالكتروني يقوم بإنجاز المعاملات وإبرام الصفقات و التصرفات التي تقتضيها فكرة التجارة الالكترونية، وبالتالي أصبح هذا المستند ينافس المستند التقليدي في الكثير من الأعمال .

فإذا كانت هذه المستندات الإلكترونية الحديثة، تتيح إنجاز المعاملات بين الأفراد والمؤسسات، بشكل يحسن أداء الخدمة للمتعامل، فإن استعمال هذه الوسائل لا يخلو من المخاطر التي تقع عليها والتي يجب أن تكون بصدد مواجهة حقيقية لها.

أولا- أسباب اختيار الموضوع :

هناك أسباب ذاتية وأسباب موضوعية دعتنا إلى اختيار هذا الموضوع .

الأسباب الذاتية:

تتمثل في الرغبة النفسيةفي دراسة هذا الموضوع و التعمق فيه إلى جانب كونه متصل بالتخصص الدراسي.

الأسباب الموضوعية:

تتمثل في أهمية الموضوع وقيمته العلمية ذلك أن موضوع الحماية الجزائية للمستند الإلكتروني موضوع خصب لم تتناوله البحوث الوطنية بسبب حداثته حتى و ان وجدت بحوث فهي تبحث في موضوع الحماية الجزائية الموضوعية للمستند الإلكتروني دون الحماية الجزائية.

كما أن الفائدة التي ستعود من هذا البحث تكمن في كونه دراسة متخصصة في جزئية من الجريمة المعلوماتية و التي يمكن لها، إثراء المكتبة القانونية الجامعيةمن جهة ومعرفة مدى كفاية النصوصالموضوعية و الإجرائية لقانون العقوبات،وقانون الإجراءاتالجزائية في مكافحة هذه الجرائم من جهة أخرى.

ثانيا- أهمية الموضوع : يعتبر موضوع المذكرة ،ذو أهمية علمية وعملية.

من الناحية العلمية:تظهر الأهمية العلمية في موضوعنا من خلال مايقدمه من أفكار ومعلومات متنوعة،عن المستند الإلكتروني،من حيث بيان تعريفه وخصائصه وصوره وأهم الجرائم الواقعة عليه والعقوبات المقررة لها ومدى حجيته في الإثبات بالإضافة إلى توضيح خطة المشرع الجزائري في مكافحة هذا النوع من الجرائم

من الناحية العملية: تأتي أهمية دراسة هذا الموضوع نتيجة،ازدياد نسبة التعامل بهذه المستندات حيث كان لها الدور الإيجابي في تقليص التكاليف والوقت والحد من التضخم الورقي،وازدياد أهمية هذه المستندات على المستوى القانوني والاقتصادي،كان لابد على المشرع في كل دولة، وفي الجزائر على وجه الخصوص أن يتدخل من أجل تأطير الأفعال

والوقائع الماسة بهذه المستندات إلى جانب إلزام إحاطتها بضمانات وأنظمة قانونية، موضوعية واجرائية تكرس حمايتها من كل أشكال التصرفات التي تؤدي إلى المساس بها بشكل يترتب عليه زعزعة الثقة في قيمتها القانونية.

ثالثا- أهداف الدراسة:

نهدف من خلال هذه الدراسة إلى جملة من الأهداف، تتمثل في:

- بيان مفهوم المستند الالكتروني وبيان خصائصه، شروطه و تمييزه عن المستند التقليدي (الورقي).

-بيان الجرائم الواقعة على المستند الالكتروني و العقوبات المقررة لها.

- تحديد الإجراءات المتبعة للتحري والتحقيق في الجرائم الواقعة على المستند الإلكتروني، كل ذلك بغية محاولة معرفة مدى مواكبة التشريع الجزائري للقوانين المتقدمة في هذا المجال.

- التعرف على مدى قبول القاضي الجنائي للمستند الالكتروني في الإثبات، وما هي الشروط التي يجب أن تتوفر في المستند الإلكتروني حتى يتمتع بحجية في الإثبات الجنائي.

رابعا- إشكالية الموضوع:

بالرجوع إلى الدور الأساسي الذي أصبح يلعبه المستند الإلكتروني، في مجال المعاملات الإلكترونية ونظرا للقيمة القانونية والاقتصادية التي اكتسبها، فقد بات من الضروري توفير الحماية و الأمان القانوني من جهة، و يؤدي إلى أن يصبح هذا المستند دليلا في الإثبات يقف على قدم المساواة مع المستند الورقي من جهة أخرى.

ومنه فإنه يمكننا طرح الإشكالية التالية:

- إلى أي مدى وفق المشرع الجزائري في سن نظام جزائي موضوعي واجرائي، يسمح بحماية فعالة للمستند الإلكتروني؟

ويندرج تحت هذه الإشكالية الرئيسية عدة إشكالات فرعية تتمثل في:

1-ما هي أهم المميزات التي يتميز بها المستند الإلكتروني عن المستند الورقي والتي دعت إلى ضرورة توفير حماية جزائية خاصة له تختلف كل الاختلاف عن تلك الحماية المقررة للمستند الورقي ؟.

2- ما مدى كفاية النصوص لجزائية الموضوعية التقليدية في حماية المستند الإلكتروني؟.

3-ما مدى كفاية إجراءات التحري والتحقيق التقليدية في جمع الأدلة الرقمية الناتجة عن ارتكاب جرائم ماسة بالمستند الإلكتروني؟.

4- ما مدى حجية المستندات الإلكترونية في الإثبات الجنائي نظرا لطبيعتها الرقمية الخاصة؟.

خامسا- صعوبات الموضوع :

من بين الصعوبات التي واجهتنا عند معالجتنا لهذا الموضوع حداثة الموضوع خاصة في التشريع الجزائري، خاصة بعد صدور قانون التجارة الإلكترونية الجديد رقم 18-05 المؤرخ في 10 مايو 2018 والذي مازال لم يحظ بعد بالدراسات الفقهية والقانونية اللازمة، إضافة إلىقلة المراجع والكتب الجزائرية المتخصصة في هذا المجال و هو الأمر الذي جعلنا نعتمدبشكل كبير على الكتب و الرسائل الجامعية المشرقية.

سادسا- الدراسات السابقة:

توجد بعض الدراسات السابقة، والتي تناولت مواضيع مختلفة للجريمة الإلكترونية، والتي تتشابه في بعض النقاط مع بحثنا إلا أنها تختلف عنه في بعض الزوايا أيضا ومن بين هذه الدراسات نذكر:

الدراسة الأولى:

-أطروحة دكتوراه علوم، بعنوان:**جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، من إعداد الطالبة:براهمي حنان، مقدمة لكلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، حيث تطرقت الباحثة إلى مفهوم الوثيقة المعلوماتية، وارتكزت دراستها على جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية،ويلتقي بحثنا مع هذه الدراسة باعتبار المستند الإلكتروني، وثيقة معلوماتية،إلا أن دراستنا تختلف عن هذه الدراسة في أن الطالبة تحدثت عن الحماية الجزائية الموضوعية للوثيقة المعلوماتية، بينما تطرقنا في بحثنا بالإضافة إلى الحماية الجزائية الموضوعية،الحماية الجزائية الإجرائية.

الدراسة الثانية:

أطروحة دكتوراه بعنوان: **الحماية الجنائية للمحررات الإلكترونية من التزوير**، إعداد الطالبة إلهام بن خليفة، مقدمة إلى كلية الحقوق، جامعة باتنة، حيث تحدثت الطالبة عن بيان مفهوم المحررات الإلكترونية انطلاقا من تعريفات الفقه والقانون، مبينة أسباب ظهورها وخصائصها واختلافها عن المحررات الورقية. تقترب هذه الأطروحة من دراستنا في تطرقها إلى الحماية الجزائية الموضوعية والإجرائية معا،إلا أن دراستنا تختلف عنها في اقتصارها على التشريع الجزائري.

الدراسة الثالثة:

أطروحة الماجستير، بعنوان: **الحماية الجنائية للمعاملات الإلكترونية**، للطالب طعباش أمين كلية الحقوق، جامعة باتنة،حيث تناول الطالب كل مايخص جرائم المعلوماتية، ويلتقي بحثنا مع هذه الدراسة في التطرق إلى الجوانب الموضوعية الخاصة بالإجرام لمعلوماتي إلا أن دراستنا تختلف في أن الطالب تحدث عن الحماية الجزائية الموضوعية فقط ، بينما دراستنا تضمنت الحماية الموضوعية والإجرائية معا.

و العديد من المراجع الأخرى التي تناولت بعض الجزئيات المتعلقة بالموضوع.

سابعا- منهج الموضوع : للإجابة عن الإشكالية المطروحة اتبعنا **المنهج الوصفي التحليلي** وذلك من خلال وصف وتعريف المستند الإلكتروني، بيان خصائصه، ووصف الجرائم الواقعة عليه، بالإضافة إلى وصف أغلب الإجراءات المستحدثة في إطار مكافحة الجريمة المعلوماتية، والعمل على تحليل مختلف النصوص العقابية المنظمة لموضوع الدراسة.

كما استعنا على سبيل الاستئناس بالمنهج المقارن، وذلك من خلال التطرق لبعض التشريعات العقابية المقارنة على سبيل المثال لا الحصر، لإثراء موضوع البحث في بعض أفكاره، وكذلك المنهج الاستدلالي من خلال الاستدلال بالنصوص العقابية التي تم سنها في مجال البحث.

ثامنا- خطة الدراسة:

لقد تم تقسيم موضوعنا إلى مبحث تمهيدي و فصلين رئيسيين.

حيث المبحث التمهيدي خصصناه لدراسة، ماهية المستند الإلكتروني، والذي قسمناه إلى مطلبين، المطلب الأول: مفهوم المستند الإلكتروني وبيان خصائصه، أما المطلب الثاني، فتحدثنا فيه عن شروط المستند الإلكتروني وتمييزه عن المستند التقليدي.

أما الفصل الأول،فخصصناه لدراسة، الحمايةالجزائية الموضوعية للمستند الإلكتروني، والذي قسمناه إلى مبحثين، المبحث الأول،الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية التقليدية. بينما تحدثنا في المبحث الثاني عن الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية المستحدثة.

أما الفصل الثاني،فبحثنا فيه عن الحماية الجزائية الإجرائية للمستند الإلكتروني، حيث قسمناه بدوره إلى مبحثين، المبحث الأول تطرقنا فيه إلى إجراءات التحري والتحقيق في الجرائم الماسة بالمستند الإلكتروني، أما المبحث الثاني فخصصناهلدراسةإجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني.

و في نهاية بحثنا تناولنا خاتمة، عرضنا فيها لأهم النتائج التي توصلت إليها، و لأهم الاقتراحات و التوصيات.

المبحث التمهيدي
ماهية المستند الالكتروني

– إن تعاملاتنا اليومية تتسم بالوضوح والتحديد من حيث مضمونها،إلى جانب توافر قدر من الأمان والثقة تجاهها ،ويرجع ذلك إلى كتابة هذه التعاملات في مستندات يمكن الرجوع إليها في أي وقت إذا استدعى الأمر ذلك ،أما الآن وعلى الرغم من التطور الكبير الذي تشهده التقنيات، الإلكترونية ،والأمان الذي توفره هذه التقنيات ،إلا أنها تقف عاجزة ،أحيانا أمام بعض التجاوزات التي قد يقوم بها بعض الأشخاص باستخدامهم وسائل احتيالية .

ولفهم الطبيعة الخاصة للمستندات الإلكتر ونية سوف نتطرق إلى المقصود بالمستند الإلكتروني وبيان خصائصه وأنواعه في (المطلب الأول) ثم إلى شروط المستند الإلكتروني وتمييزه عن المستند التقليدي في (المطلب الثاني).

المطلب الأول

مفهوم المستند الإلكتروني وبيان خصائصه وصوره

– عرفت بعض التشريعات الحديثة المهتمة بسن قوانين خاصة بعمليات التعامل عبر

أجهزة وشبكات الحاسب الآلي المستند الإلكتروني من زويا مختلفة ،مع استخدامها مصطلحات مترادفة [1] مثل :

السند الإلكتروني ،المحرر الإلكتروني ،الكتابة الإلكترونية ،الوثيقة المعلوماتية ،السجل الإلكتروني ،رسالة البيانات ،وعلى الرغم من الاختلاف ،إلا أنها تحمل معنى واحد .

وعليه لتحديد هذه الاختلافات سوف نتطرق في (الفرع الأول) إلى تعريف المستند الإلكتروني وفي (الفرع الثاني) إلى أهم خصائصه وأخيرا (الفرع الثالث) لبعض من صوره

الفرع الأول : تعريف المستند الإلكتروني

قبل التطرق إلى تعريف المستند الإلكتروني لابد أن نعرف المستند أو المحرر في شكله التقليدي والذي هو عبارة عن مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة

[1] – إيهاب فوزي السقا ،**جريمة التزوير في المحررات الالكترونية** ، دار الجامعة الجديدة للنشر،الإسكندرية ،2002،ص14.

مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين ومنه نستنتج أن المحرر في شكله التقليدي هو عبارة عن سند يحمل كتابة ذات أثر قانوني قد تكون يدوية أو آلية يمكن فهمها وادراكها بمجرد النظر إليها[1].

أولا : التعريف الفقهي للمستند الإلكتروني

لقد عرّف الفقه المستند الإلكتروني بأنه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات أو يكون مشتقا من هذا النوع ،كما ذهب بعض من الفقه إلى تعريف المحرر الإلكتروني بأنه كل جسم منفصل ، وقد سجلت عليه معلومات معينة ،سواء كانت معدة للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أو يكون مشتقا من هذا النوع .[2]

ويختلف المستند المعالج آليا عن المستند الغير معالج آليا،وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شئ بعد والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرامج.

كذلك يقصد بالمستند المعالج آليا كل دعامة مادية يمكن أن يدون عليها شيء معنوي. ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة ،ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة وتم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله .[3]

ثانيا : التعريف القانوني للمستند الإلكتروني

عرّف قانون الأونسيترال النموذجي ،المستند الإلكتروني برسالة البيانات طبقا للمادة 2/ج على أنه 'يعني المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو

---

[1]- إلهام بن خليفة **الحماية الجنائية للمحررات الإلكترونية من التزوير** أطروحة دكتوراه في العلوم القانونية والإدارية)،تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر باتنة ،2016،ص ص24-25

[2]- إيهاب فوزي السقا، مرجع سابق ص 16

[3] - آمال قارة **الحماية الجزائية للمعلوماتية في التشريع الجزائري** ،الطبعة الأولى،دار هومة للنشر والتوزيع،الجزائر ،2006،ص135

ضوئية أو بوسائل مشابهة بما في ذلك ،على سبيل المثال لا على سبيل الحصر ،تبادل البيانات الإلكتروني أو البيانات البريد الإلكتروني أو البرق أو التلكس أو نسخ البرقي[1].

وقد عرّف أيضا قانون التجارة الأمريكي المستند الإلكتروني في المادة7/2 على انه سجل يتم إنشاؤه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر ويكون قابلا للاسترجاع بشكل يمكن فهمه[2]

يقصد أيضا بتعبير المستندات المعالجة آليا وفقا لقانون الصادر سنة1988 الفرنسي والمتعلق ببعض جرائم المعلوماتية ،أنها مستندات تم بالفعل خضوعها لمعالجة آلية ،بمعنى آخر تم بالفعل صياغتها في صورة إحدى لغات الحاسب الآلي وبالتالي فلفض المحررات المعلوماتية، هو خطوة أولى لكي يتم فيها بعده في خطوة تالية ،المعالجة الآلية وعلى هذه المستندات المعالجة آليا يقع التزوير وهذا هو مقصد المشرع ،وهنا تكمن حداثة استخدامه للتعبير الجديد وهي نقطة تحسب للمشرع الفرنسي في تفتحه على المصطلحات التكنيكية الجديدة [3]
وقد عرّف القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في المادة الأولى منه الفقرة 18الكتابة الإلكترونية بأنها عملية تسجيل البيانات على وسيط الكتروني لتخزينها [4]

كذلك عرف المشرع المصري المستند الإلكتروني في القانون رقم15 لسنة 2004، والخاص بالتوقيع الإلكتروني في مادته الأولى في الفقرة 'ب' بأنه رسالة تنشأ أو تدمج ،أو تخزن ،أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية ،أو رقمية ،أو ضوئية،أو بأية وسيلة أخرى مشابهة .

---

[1] –براهمي حنان ،**(المحررات الإلكترونية كدليل إثبات)**،مجلة المفكر،كلية الحقوق والعلوم السياسية ،جامعة بسكرة،العدد التاسع،(ب،ت)،ص138

[2]– صالح شنين ، **الحماية الجنائية للتجارة الالكترونية**،(راسة مقارنة)رسالة دكتوراه في القانون الخاص،كلية الحقوق،جامعة تلمسان،2013 ،ص 45

[3] –هدى حامد قشقو ش ،**جرائم الحاسب الإلكتروني في التشريع المقارن** ، دار النهظة العربية ، القاهرة ،ص،120

[4]– عبد الفتاح بيومي حجازي ،**مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي ال**نموذجي ، الطبعة الأولى ، دار النهضة العربية، مصر ،2009،ص،743

ويتضح لنا من هذا التعريف أن المشرع قصد بالمحرر الإلكتروني ،أنه رسالة إلكترونية مدون فيها بيانات ومعلومات يكون منشؤها أو تخزينها إلكترونيا ،كما أنها ترسل وتستقبل عبر وسيلة إلكترونية أو ما شابه ذلك .

كما تعرضت بعض التشريعات الأخرى لمفهوم المحرر الإلكتروني بمصطلحات مترادفة مثل المستند الإلكتروني أو الوثيقة الإلكترونية ففي التشريع الإماراتي، عرّف المحرر الإلكتروني في قانون التجارة الإلكترونية الخاص بإمارة دبي رقم2 لسنة2002 بأنه 'سجل أو مستند الإلكتروني يتم إنشاؤه أو تخزينه أو استخراجه أو نسخة أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر،ويكون قابلا للاسترجاع بشكل يمكن فهمه [1].

وأخيرا فإنه ما ينال من الرأي الموسع أن التشريعات المدنية والتجارية المقارنة التي أقرت بفكرة المستند الإلكتروني قد لجأت إلى إصدار تشريعات خاصة تنظم تطبيقات هذا المستند مثل السجلات،والتوقيع الإلكتروني ،واذا كان هذا الرأي صحيحا لكانت هذه التشريعات ،قد ساوت في التطبيق بين فكرتي المستند دون الحاجة إلى نصوص خاصة وهو ما لم يحدث.[2]

أما بالنسبة للمشرع الجزائري فهو لم يقم بتعريف المستند الإلكتروني ولم يقم بإعداد قانو ن خاص بالمعاملات الإلكترونية وهذا ما يبين ويوضح عدم تأثر المشرع الجزائري بباقي التشريعات الأخرى،لكنه لم يكن بمنأى عن التطور الحاصل في الإثبات بالكتابة الإلكترونية فلقد أدخل بعض التعديلات على النصوص الإثبات في القانون المدني لسنة 2005 بإضافة مواد تعرّف الكتابة الإلكترونية وحجيتها في الإثبات،وهذه المواد هي المادة323 مكرر و323مكرر 1 .[3]

---

[1]– إيهاب فوزي السقا ،مرجع سابق ،ص ص،14،15

[2]– أشرف توفيق شمس الدين ، **الحماية الجنائية للمستند الإلكتروني** (دراسة مقارنة) ،بحث منشور على شبكة الإنترنت من خلال الموقع الإلكتروني الآتي http://www,arabawifo.com (الدليل الإلكتروني للقانون العربي) بتاريخ 05/12/2017، ص،12

[3]–الأمر رقم 75–85المتضمن القانون المدني،المؤرخ في 16سبتمبر1975،المعدل والمتمم بالقانون رقم 07–05المؤرخ في13مايو2007

تنص المادة323 مكرر،ق م على أنه (ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام،وأية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها)

كما نصت المادة323 مكرر من ق م ج على أنه ' يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها وهذه الشروط هي إمكانية التأكد من هو الشخص الموقع وأن تكون منظومة إنشاء التوقيع الإلكتروني محفوظة في ظروف تضمن سلامته '

كذلك أشار في نص المادة الثانية الفقرة (ا) من القانون رقم 09-04 المؤرخ في 05 أوت سنة 2009،والمتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهاعلى أن أي جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ،كما نص في الفقرة (ج) على أن المقصود بالمعطيات المعلوماتية أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية،بما في ذلك البرامج المناسبة التي من شئنها جعل منظومة معلوماتية تؤدي وظيفتها.[1]

من خلال الفقرة (ا) والفقرة(ج) من المادة 2 من القانون رقم 09-04،نلاحظ أن المشرع الجزائري أشار إلى المستند الإلكتروني كجزء من المنظومة المعلوماتية

وعلى ضوء هذه التعريفات التشريعية نستنتج أن المستند الإلكتروني هو عبارة عن وسيط إلكتروني ،والذي هو كل شيء مادي متميز لقرص صلب أو مظغوظ أو شريط ممغنط أو خلافه ،يصلح لأن يكون محلا لتسجيل أو تخزين معلومات فيه ،معالجة بواسطة نظام المعالجة

[1]– القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل05 أوت 2009،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،(ج ر،رقم 47المؤرخة في 16 أوت 2009)،ص05

الآلية للمعطيات ،بمعنى أن المعلومات أو الكتابة الإلكترونية تنشأ عن طريق المكونات المادية والمعنوية للحاسب الآلي بواسطة هدا النظام ثم تفصل عنه .[1]

الفرع الثاني : خصائص المستند الإلكتروني: الخصائص المميزة التي يختص بها المستند الإلكتروني عديدة وهي التي سنعرضها في ما يلي :

أولا : الصفة الإلكترونية:

–يحمل هذا المستند أو المحرر الصفة الإلكترونية ،بما يعني أن العمليات التي يمر بها هدا المحرر 'مثال', كتابة أو ضغطه أو تخزينه أو استرجاعه أو نقله أو نسخه متصلة بتقنية تكنولوجية إلكترونية، ولا يمكن استخدامه خارج هدا الوسيط الإلكتروني بالإضافة إلى أنه يمكن أن يتم تحميل هذا المحرر ونقله من جهاز إلكتروني0 لأخر عن طريق دعامة إلكترونية .[2] وبالتالي تعتمد هذه الخاصية للمستند الإلكتروني على عدم وجود أي دعامة ورقية على عكس السند التقليدي المودع على دعامة ورقية ،ومن هذا الصدد نلاحظ أنه يوجد دائما ارتباط وثيق الصلة بين المضمون في السند التقليدي والدعامة (أداة التخزين غالبا قطعة ورق) المدون عليها المعلومات ولا نوع من استقلال المعلومات الواردة فيه عن أي دعامة أخرى،ويرجع ذلك إلى أن للمضمون أن لا يكون منفصلا عن هذا الوسيط ،بينما يفترض في السند الإلكتروني أن يسجل على دعامة محددة قرص صلب أو مرن ،قرص ضوئي،....الخ.[3]

ثانيا :القيمة القانونية.

يحتوي المحرر الإلكتروني على كتابة لها قيمة قانونية،أي تصلح للتمسك أو للاحتجاج بها ،وهي لا تكون كذلك إلا إذا كانت تقرر حق سواء بإنشائه أم بتعديله أو بإلغائه أو تثبته [4]. بالإضافة إلى أن المحرر الإلكتروني ،يتضمن تعبيرا عن المعاني والأفكار الإنسانية المترابطة ،وهو ما يعني أن يكون هذا المحرر أداة للتفاهم وتبادل الأفكار بين الأفراد ،وأن يكون له قيمة

---

[1]–إلهام بن خليفة ،مرجع سابق ،2016،ص ص20،21

[2] – إيهاب فوزي السقا،مرجع سابق ،ص17

[3] – كحول سماح ، **حجية الوسائل التكنولوجية في إثبات العقود التجارية** ،(مذكرة ماستر في القانون العام للأعمال)،كلية الحقوق والعلوم السياسية ،جامعة قاصدي مرباح ورقلة،2015، ص5

[4] –علي عبد القادر القهوجي،**الحماية الجنائية لبرامج الحاسب الآلي**،دار الجامعةالجديدة،الإسكندرية2010،ص144

قانونية ،يمكن التعويل عليه عند المعاملات بين الأفراد والمؤسسات والحكومات ،مما يخضعه للمسائلة القانونية عند المساس به أو تغيير ما يحمله من حقائق .[1]

ثالثا :السرعة والائتمانفي إبرام المعاملات .

تتميز المستندات الإلكترونية بالسرعة في إبرام التعاقد ،إذْ يستطيع الشخص الذي ينوي التعاقد عن طريق وسائل الاتصال الفوري ،بتأمين وصول إيجابه إلى شخص الأخر الذي ينوي التعاقد معه في أي مكان كان والحصول على إجابة في ثواني معدودة ،وهكذا يسمح بتوفير الوقت واختصاره بشكل كبير لاسيما في التجارة الإلكتروني

كذلكتمكن المستندات الإلكترو نية من تسليم بعض الأشياء وأداءبعض الخدمات فورا في البيئة الافتراضية ،كالحصول على خدمات معينة أوبرامج كومبيوترية ،وتسمح أيضا بالوفاء فورا ،أي يمكن دفع الثمن إلكترونيا بأحد الأساليب المعروفة للوفاء على شبكة الانترنت، سواء عن طريق بطاقات الائتمان أم النقود الرقمية أم البطاقات الذكية ،وغيرها من وسائل الوفاء .[2]

رابعا : السرية.

تتميز المستندات الإلكترونية بالسرية ،حيث لا يمكن لأحد ما الإطلاع عليها،إلا المُرسل أو المُرسل إليه ،لأنها مستخرجة من تقنيات متطورة توفر الأمن لها ،كما أن تشريعات المعاملات الإلكترونية أضفت عليها حماية لضمان الثقة فيها ،وذلك بأن نصت على استخدام وسائل تقنية تحفظها وتحول دون أن تمتد إليها يد العابثين عليها تتمثل في أنظمة التشفير وتسليم شهادة تصديق من طرف جهات موثوقة من الدولة ،تثبت أن ما على المحررات من حقوق يعود لصاحب التوقيع الإلكتروني عليها. [3]

---

[1] – إيهاب فوزي السقا ،مرجع سابق ،ص17

[2] – عباس العبودي ،**تحديات الإثبات بالسندات الإلكترونية ومتطلبات النضام القانوني لتجاوزها**،الطبعة الأولى،منشورات الحلبي الحقوقية ،بيروت ،2010،ص40

[3] – إلهام بن خليفة ،مرجع سابق،ص23

الفرع الثالث :صور المستند الإلكتروني

المستندات الورقية إما أن تكون مستندات رسمية وهي التي يقوم بتحريرها موظف عام مختص وفقا للأوضاع المقررة قانونا،واما أن تكون مستندات عرفية وهي التي يقوم بتحريرها الأفراد فيما بينهم وذلك لإثبات تصرف أو واقعة قانونية[1]

-هذا بالنسبة للمستندات الورقية أما المستندات الإلكترونية فصورها متعدد نذكر منها على سبيل المثال :

-العقود الإلكترونية و التي تعني :العقد الذي يتم انعقاد بوسيلة الإلكترونية كليا أو جزئيا وسواء تمثلت الوسيلة الإلكترونية في وسيلة كهربائية أو مغناطيسية أو ضوئية أو إلكترومغناطيسة أو أي وسيلة أخرى مشابهة صالحة لتبادل المعلومات بين المتعاقدين.
ولقد عرفه القانون رقم 08-05 المؤرخ في 24شعبان عام1439الموافق 10ماي2018،المتعلق بالتجارة الإلكترونية وفقا للمادة6 منه على أنه هو العقد بمفهوم القانون رقم 04-02المؤرخ في 5 جمادي الأول عام1425الموافق23 يونيو 2004 الذي يحدد القواعد المطبقة على الممارسات التجارية،ويتم إبرامه عن بعد،بدون الحضورالفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الاتصال الإلكتروني[2].

-من بين صور المستند الإلكتروني أيضا نجد الشيك الإلكتروني و التي هي عبارة عن رسالة تحتوي على جميع البيانات التي يمكن أن نجدها بالشيك الورقي العادي ، بحيث يقوم المشتري بتحرير شيك الإلكتروني للبائع و إرساله له إلكترونيا عبر أي وسيلة إليكترونية كالفاكس أو البريد الإلكتروني في أغلب الأحيان ، و تكون جميع التوقيعات التي يتضمنها هذا الشيك توقيعات الإلكترونية أو رقمية.

-كذلك من بين الصور نجد البطاقات الإلكترونية وتتخذ أشكالا متعددة ووظائف مختلفة،كما أنها قد تصدر عن جهات حكومية،أو عن مؤسسات مالية خاصة من أجل المبادلات التجارية أو الاستفادة من بعض الخدمات،ومن بينها البطاقات البنكية أو المصرفية،ومن بين الأنواع

[1] – محمد أمين الرومي،مرجع سابق،ص 38

[2] – القانون رقم 18-05المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018،المتعلق بالتجارة الإلكترونية(ج ر،العدد28)المؤرخة في 30 شعبان 1439 الموافق 16 مايو سنة 2018،ص 05

الشائعة للبطاقة الإلكترونية ،بطاقة التعريف الوطنية،جواز السفر الإلكتروني،بطاقة الضمان الاجتماعي،رخصة القيادة الإلكترونية،بالإضافة إلى بطاقة الوفاء والتي هي عبارة عن آداة وفاء تصطبغ بصبغة مصرفية وتسمح لحاملها باتخاذ الإجراءات اللازمة لخصم وتحويل مبلغ محدد من المال من حسابه لدى البنك المصدر للبطاقة لمصلحة وحساب شخص آخر[1]

كذلك من بين الصور نجد،بطاقة الائتمان وهي بطاقة خاصة يصدرها المصرف لعميله كي تمكنه من الحصول على السلع والخدمات من محلات وأماكن معينة عند تقديمه هذه البطاقة

أيضا نجد بطاقة الصراف الآلي وهي بطاقة مخصصة للقيام بالعمليات المصرفية عبر الصراف الآلي،كعمليات السحب وكشف الحساب،والعمليات الممكنة بواسطة هذا الجهاز،إذ يمكن سحب مبالغ نقدية بسقف محدد متفق عليه،بإدخال البطاقة في الفتحة الخاصة بالجهاز،وا دخال الرقم السري ليتم صرف المبلغ آليا وتسجيل المبلغ في الجانب المدين من حساب الحامل وفي هذا النطاق فلقد تضمن قانون التجارة الإلكترونية الجديد الصادر في 2018 مصطلح وسيلة الدفع الإلكترونية،والتي هي كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد،عبر منظومة إلكترونية.

وتتكون البطاقات الإلكترونية من مكونات مادية تتمثل في جسم البطاقة الذي يتميز بأبعاد معينة من حيث الطول والعرض والسمك بالإضافة إلى تموضع كل مكونات البطاقة من حيث المسافات الرأسية والأفقية بين الحروف والأرقام والصورة وشريط التوقيع والشريط الممغنط وتستخدم في صناعة هذه البطاقات طبقة بلاستيكية خاصة تغطيها لحماية المعلومات والبيانات من العوامل البيئية المحيطة والحرارة

أما المكونات المعلوماتية للبطاقة فإن الشريط الممغنط أو الشريحة الإلكترونية يحتوي على بيانات معالجة إلكترونيا تتعلق بصاحب البطاقة،حيث لايمكن إدراك هذه البيانات بصر يا ،إلا أنه من الممكن قراءتها وفقا للأصول الفنية الخاصة بها

[1]–براهمي حنان،**جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية** ،مرجع سابق،ص ص 101–102–106

وبالتالي البطاقة الإلكترونية تحمل مجموعة من المعلومات والبيانات التي ترتبط بمركز مالي أو قانوني معين لصاحبها ،سواء كانت ظاهرة أو كانت الكترونية،أما المعلومات الإلكترونية الموجودة على الشريط الممغنط فهي جزء من المستند الإلكتروني.[1]

المطلب الثاني:

شروط المستند الإلكتروني وتمييزه عن المستند التقليدي

ارتبط ظهور المحرر الإلكتروني وانتشاره ،بعدة مصطلحات الكترونية أخرى ،تستخدم عند التعامل به ،واعتبارهاكثيرا من الفقه شروطا لكي يكون للمستند الإلكتروني الحجية الكاملة في الإثبات،وامكانية مساواته بالسندات الرسمية والعرفية ،ومن أهم هذه المصطلحات ،الكتابة الإلكترونية والتوقيع والتوثيق وهي نفسها الموجودة في المستند التقليدي ،إلا أن هذا لا يعني أنهما متمثلانر غم أنهما يؤديان إلى نفس الغرض وهو الإثبات .

ومن هنا تم تقسيم هذا المطلب إلى فرعين ، الفرع الأول يتضمن(شروط المستند الإلكتروني) والفرع الثاني يتضمن ،(تمييز المستند الإلكتروني عن المستند التقليدي)

الفرع الأول :شروط المستند الإلكتروني

من شروط المستند الإلكتروني نذكر ما يلي :

أولا :الكتابة

تعتبر الكتابة من أول طرق الإثبات المختلفة في إثبات التصرفات القانونية ،ويرجع ذلك لطبيعتها من حيث تحديدها ووضوحها وامكانية بقائهاواستمرارها ،دون الارتباط بكاتبها أو موقعها ،ونظرا لانتشار الكتابة وشيوعها نجد المشرع، في القوانين الحديثة أضفى عليها حجية مطلقة ،مادام الخصم لم ينكرها أويدّع تزويرها ،ولذلك فهي لا تخضع لتقدير القاضي ،وتعتبر الكتابة بدقة عن الواقعة التي أعدتلإثباتها ،فهي تعتبر دليلا عند حدوث نزاع بين أطراف الاتفاقوتعطي قدراكبر ا من الاطمئنان لدى أصحاب الحقوق

وبالتالي تعتبر الكتابة الشرط الأساسي والأهم في المستندات الإلكترونية [1]

[1]–براهمي حنان،**جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية** ،مرجع سابق، ص ص 107–108–109

والتي تكون على شكل معادلات خوارزمية تنفّذ من خلال عمليات إدخال البيانات واخراجها من خلال شاشة الحاسب الآلي، والتي تتم من خلال تغذية الجهاز بهذه المعلومات عن طريق وحدات الإدخال والتي تتبلور في لوحة المفاتيح أو استرجاع المعلومات المخزنة في وحدة المعالجةالمركزية ،وبعد الفراغ من معالجة البيانات يتم كتابتها على أجهزة الإخراج التي تتمثل في شاشة الحاسب الآلي، أوطباعة هذه المحررات على الطابعة أو الأقراص الممغنطة أو أي وسيلة من وسائل تخزين البيانات [2]

يجب توافر مجموعة من الشروط التي توصف بالفنية أو التقنية حتى يعتد بالكتابة في المجلات القانونية نذكر مثلا:

يجب أن تكون الكتابة مقروءة ومستبينة حتى يمكن الاعتدادبها ولهذا تأثيرات قانونية خطيرة حيث أنه في حالة تخلف هذا الشرط يمكن أن يبطل التصرف القانوني ،كما يجب أن تكون الكتابة دائمة،أي يجب حفظها في شروط تضمن بقائها مدة معقولة،وأخيرا يجب أن يصعب العبث بها أو التعديل فيها دون أن يترك ذلك أثرا على المحرر الذي يحتويها .[3]

ثانيا :التوقيع:عرّف قانون الأونسترال النموذجي في المادة (2) منه ،التوقيع الإلكتروني (بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ،يجوز أن تستخدم لتقييم هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات)[4]

كذلك يعرّف التوقيع الإلكتروني بأنه 'جزء صغير مشفر من بيانات يضاف إلى رسالة إلكترونية

---

[1]– إيهاب فوزي السقا، مرجع سابق،ص 28

[2]– لورنيس محمد عبيدات ،**إثبات المحرر الإلكتروني** ،دار الثقافة ،عمان ،2009،ص،79

[3] –عابد فايد عبد الفتاح ،**الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني** ،دار الجامعة الجديدة ،الإسكندرية ،2014،ص 46

[4]– إيهاب فوزي السقا،مرجع سابق ،ص31

،فهو جزء من الرسالة ذاتها يشفر ويرسل مع الرسالة ،ليتم التوثق من صحة الرسالة ،بفك التشفير وانطباق محتواه على الرسالة [1]

وقد نص المشرع الجزائري على هذا الشرط في نص المادة الثانية من القانون 15-04،[2] الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين بقوله ،التوقيع الإلكتروني ؛(بيانات في شكل إلكتروني ،مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى ،تستعمل كوسيلة توثيق) وبالرجوع إلى نص المادة 327،[3] من القانون المدني نجد أن المشرع قد اعتد به شريطة أن تتوافر فيه الشروط المنصوص عليها في المادة 323مكرر1،من قانون المدني الجزائري ،التي تنص على أنه 'يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون منظومة، إنشاء التوقيع الإلكتروني محفوظة في ظروف تضمن سلامته'

ثالثا : التوثيق أو (التصديق):يقصد بالتصديق، اللجوء إلى طرف ثالث محايد ومستقل عن الأطراف 'سواء كان فردا عاديا أو شركة أو جهة من الجهات ' من أجل توثيق المعاملات الإلكترونية لأشخاص ، وبهذا يتحدد وضع الموثق أو المصدّق بأنه وسيط بين المتعاملين ،يلجأ إليه بغرض منح الثقة في محرراتهم حتى يمكنهم يستخدموها لإثبات ماتتضمنه من تصرفات قانونية ، ولهذا السبب يطلق عليهم .البعض ، وكلاء الإثبات .[4]

وتلعب شهادة التوثيق الإلكتروني دورا مهما في عملية التوقيع الرقمي ،حيث تؤكد صحة المفتاحين العام والخاص المستخدمين في ذلك ،حسب المعلومة الواردة بهذه الشهادة الخاصة بصاحبها ،والمنشئة من جهة محايدة ,ذلك أن منح هذه الشهادة من جهة التوثيق الإلكتروني يتطلب تقديم المعلومات الخاصة بطالب التوقيع والتأكد من صحتها ،ليتم منح هذا الشخص مفتاح تشفير خاص يتسم بالسرية ،حيث يحتفظ به الموقع ،ويتم تثبيت نصفه في جهاز

---

[1]- خالد عبد الفتاح محمد ،**التنظيم القانوني للتوقيع الإلكتروني**، المركز القومي للإصدارات القانونية ،الطبعة الأولى ،(د م ن)2009،ص 15

[2] - القانون رقم 15-04،المؤرخ في 11 ربيع الثاني عام 1436،الموافق ل01،فيفري،2015،المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين ،(ج ر ،العدد06)،ص7

[3]- الأمر رقم 85/75،المتضمن القانون المدني ،سالف الذكر.

[4]- عابد فايد عبد الفتاح ، مرجع سابق ،ص ص71،70

الكمبيوتر الخاص به ،والنصف الأخر في بطاقة إلكترونية ،أما جهة التوثيق فتحتفظ بالمفتاح العام ،حيث نقوم بإرساله بالبريد الإلكتروني إلى الأشخاص الذين يتعامل معهم الموّقع ، وذلك لاستخدامه في فك التشفير[1]

رابعا- حفظ المعلومات (سلامة المحتوى)

إن بقاء محتوى المستند كما هو عند إنشائه هو ما نعنيه بحفظ المعلومات طوال مدة التقادم التي يخضع لها التصرف المحفوظ،ولذلك يلاحظ أن عملية الحفظ لها دور هام في مجال الإثبات،ولذلك يجب حفظ المعلومات والمعطيات على دعامة إلكترونية ضد التلف والتعديل أو أي صورة من صور الهلاك

وقد أشار قانون الأونسترال في المادة10إلى الشروط التي يجب توافرها عند حفظ المستند الإلكتروني وهي:

1-تيسير الإطلاع على المعلومات الواردة به على نحو يتيح استخدامها بالرجوع إليها لاحقا

2-الاحتفاظ بالشكل الذي أنشئ أو استلم به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشأت أو استلمت

3-الاحتفاظ بالمعلومات إن وجدت والتي تمكن من استبانة منشأ المستند الإلكتروني وجهة وصوله،وتاريخ ووقت إرساله واستلامه.[2]

الفرع الثاني:تمييز المستند الإلكتروني عن المستند التقليدي:

يتماثل المحرر الإلكتروني مع المحرر التقليدي في عدة أمور،ويختلف في أمور أخرى ،حيث أن كلاّ منهما يحمل ملامح وخصائص يتميز بها عن الآخر ،وفيما يلي نوضح نقاط الاتفاق والاختلاف بين كل منهما :

أولا :أوجه الاتفاق :

[1] -براهمي حنان ،**جريمة التزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية** ،(أطروحة دكتوراه)،تخصص قانون جنائي،كلية الحقوق والعلوم السياسية،جامعة محمد خيضر ،بسكرة،2015،ص153

[2] -براهمي حنان،**المحررات الإلكترونية كدليل إثبات**،مرجع سابق،ص144

- يتشابه المحرر الإلكتروني والمحرر التقليدي (الورقي)في أن كلاهما يحتوي على مجموعة من الرموز التي تعبر عن مجموعة مترابطة من الأفكار والمعاني الإنسانية ،يدعو المشرع لحمايتها[1].

- يرتب الاعتداء على كلاهما وقوع ضرر يمس مصلحة عامة في المجتمع تتمثل في المساس بالثقة العامة ،التي تضيفها الدولة عليهما،كما يتشابه المحرر الإلكتروني والتقليدي أيضا أن كلهما قد يحمل صفة المحرر الرسمي أو المحرر العرفي [2].
- وحتى يمكن استيعاب مفهوم المحرر الإلكتروني والذي له حجية الإثبات يتعين بيان مفهوم المحرر في صورته التقليدية ،فالمحرر في صورته الورقية قد يكون ورقة رسمية أو عرفية ،فيعتبر المحرر رسميا إذا أثبت فيه موظف عام أو شخص مكلف بخدمة عامة ما، تمر على يه أو تّ لقاه من ذوي الشأن ،طبقا للأوضاع القانونية وفي حدود سلطته واختصاصه .

ثانيا:أوجه الاختلاف :

- المستند الإلكتروني مجرد ،أي ليس له كيان ملموس ،بعكس السند الورقي فالمتعامل يرى الدعامة الورقية والكتابة عليها مباشرة دون اللجوء إلى أي وسيط تقني أو واقعي ،في حين أنه بالنسبة للمستند الإلكتروني ،لا يجد أمامه سوى الدعامة الإلكترونية (مثل قرص مدمج أو غيره) ولا يستطيع الوصول إلى الكتابة المفهومة إلا عن طر يق وسيط أو أجهزة إلكترونية (كجهاز كمبيوتر) قادر على ترجمة البيانات التقنية المحفوظة إلى كتابة مفهومة للإنسان ،تظهر على شاشة الكمبيوتر أو تطبع على الورق ،وبالتالي السند الورقي قابل للقراءة مباشرة أما السند الإلكتروني فليس ذلك[3].

ويختلف المحرر الإلكتروني عن المحرر في شكله التقليدي أن المحرر التقليدي يكتب بطريقة يدوية أو آلية في كيان مادي ملموس ،ومن ثم يسهل قراءته بالعين المجردة ،أما المحرر

---

[1]– إيهاب فوزي السقا ،مرجع سابق ،ص،18

[2]– محمود نجيب حسني ، **شرح قانون العقوبات القسم الخاص** ، دار النهضة العربية ،القاهرة ،2013،ص،279

[3]– كحول سماح ، مرجع سابق ،ص ،09

الإلكتروني فهو يعالج عن طريق المكونات المادية والمعنوية لأجهزة الحوسبة والاتصالات ،ويسجل على دعامة مغناطيسية تحمل الطابع الافتراضي أو المعنوي[1].

- تحقق المستندات الإلكترونية عنصر الثقة والأمان ،حيث يصعب العبث فيها أو تغيير محتواها وذلك لأنها تعتمد على تكنولوجيا التأمين والتشفير،فهنا كشفرة سرية تستخدم في حفظ السندات بحيث لا يمكن الإطلاع عليها إلا في حالة قرصنة الشيفرة ،على عكس السندات التقليدية التي قد تتعرض للتغيير أو العبث أو السرقة وبالتالي تفتقد عنصر السرية والأمان[2].
- المحرر الورقي له أصل ورقي ،حتى وا ن تم إرساله عبر أجهزة شبكات الحاسب الآلي،مثل الفاكس والبريد الإلكتروني بعد إجراء عملية المسح الضوئي له،بينما المحرر الإلكتروني مخزن ومحفوظ إلكترونيا .
- يتميز المحرر الورقي بصفة الدوام والثبات،فهو يكون بطريقة نهائية ومن ثم يسهل كشف أي تلاعب أو تزو ير فيه بينما لا يتمتع المحرر الإلكتروني بهذه الصفة لأنه قابل للمحو أو التعديل أو التلف دون ترك أثر ملحوظ يكشف التلاعب به ،وخاصة إذا قام بذلك خبير أو مهني متخصص في الحاسب والمعلوماتية ،ويمكن أن يتم ذلك أيضا بسبب الخلل الفني أو التقني في الأجهزة المستعملة سواء أتم ذلك تلقائيا أو بفعل فاعل مثل إطلاق الفيروس على البرامج لتدمي ه غير أن هذا الكلام مبالغ فيه لأن التكنولوجيا الحديثة أوجدت أنظمة تقنية وقائية على درجة عالية من الثقة تحفظ وتؤمن المحررات الإلكترونية من أي تلاعب أو أي اعتداء يقع عليها .[3]

[1]– نبيل صقر ،مكاري نزيهة ،**الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية** دار الهدى ، الجزائر ،2009،ص،274

[2]– محمد أمين الرومي ، **المستند الإلكتروني** ، الطبعة الأولى ،دار الفكر الجامعي ، الإسكندرية ،2007،ص106

[3] – إلهام بن خليفة ،مرجع سابق ،ص26

الفصل الأول
الحماية الجزائية الموضوعية للمستند الإلكتروني

أن توجد علاقة بين نظام الحاسب الالكتروني وارتكاب بعض الجرائم هو نتيجة طبيعية للتطور التكنولوجي الحالي، سواء استخدم الحاسب الالكتروني كمحل للتحايل أو كان وسيلة للتحايل، واذا كان العصر المعلوماتي أو عصر ثورة المعلومات هو نتاج طفرة الاتصالات وطفرة تقنية المعلومات، فإن ما جاء به من أنشطة غير مشروعة، تنطوي –بلا شك– على أنشطة إجرامية تقليدية تأخذ شكلا مستحدثا.

فلقد صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، وغيرها، ... الخ. مما انجرت عنه تطور المستندات الالكترونية وأضحت جزء لا يتجزأ من هذه المعاملات، وفي إطار هذه المعاملات انتهز بعض المجرمين من أجل الاعتداء على هذه المستندات، حيث استخدموا طرق من أجل ذلك، على غرار الإتلافـو التزوير المعلوماتي. والسرقة الالكترونية بالإضافة إلى المساس بسرية المستند الالكتروني.

ولقد اختلف الفقهاء ورجال القانون في تكييف الجرائم الواقعة على المستند الإلكتروني، باعتبارها جرائم معلوماتية، فمنها من أخضعها إلى النصوص العقابية التقليدية باعتبارها جرائم عادية مثلها مثل جرائم التزوير، السرقة، النصب، خيانة الأمانة ....، ومنها من سن لها نصوص عقابية خاصة ومستحدثة نظرا للطابع الرقمي للأدلة الناتجة عن ارتكابها والتي تختلف كل الاختلاف عن الدليل المادي الناتج عن ارتكاب الجرائم التقليدية، لذلك سنتناول في هذا الفصل بالدراسة لكل من: الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية التقليدية (المبحث الأول) ثم إلى الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية المستحدثة (المبحث الثاني).

المبحث الأول

الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية التقليدية

تعتبر الجرائم المعلوماتية من الجرائم المستحدثة، وهي تستهدف قطاعات كثيرة، مما جعل من مأمورية الفقهاء فيما يخص تحديدها وتصنيفها يتميز بالصعوبة،على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة، وبالتالي لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم المعلوماتية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها[1]. وسنحاول في هذا المبحث الوقوف عن مدى كفاية النصوص العقابية التقليدية في توفير حماية جزائية فعالة للمستند الإلكتروني وذلك من خلال التطرق إلى مدى خضوع المستند الإلكتروني للنصوص العقابية لجريمة التزوير (المطلب الأول)، ثم مدى خضوع المستند الإلكتروني للنصوص العقابية لجرائم الأموال (المطلب الثاني) وأخيرا مدى خضوع المستند الإلكتروني للنصوص العقابية للجرائم الواقعة على الملكية الفكرية وذلك من خلال ما يلي:

المطلب الأول

مدى خضوع المستند الالكتروني للنصوص العقابية لجريمة التزوير:

نرى أن المساس بمحتوى المستند الإلكتروني وذلك عن طريق تزويره يكون أشد صعوبة من تزوير المستند الورقي

الفرع الأول: تعريف جريمة التزوير:سوف نتعرض في هذا الفرع إلى تعريف التزوير التقليدي ثم التزوير المعلوماتي

أولا: تعريف التزوير التقليدي

يعرف التزوير بأنه "تغيير الحقيقة في المحرر بإحدى الطرق التي حددها القانون تغييرا من شأنه أن يترتب عنه ضررا للغير وبنية استعمال هذا المحرر فيما أعد له."[2]

كما يعرف أيضا بأنه "تحريف مفتعل للحقيقة في الواقع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به يمكن أن ينتج عنه ضررا أدبيا أو ماديا أو اجتماعيا.[3]

---

[1] – صغير يوسف،**الجريمة المرتكبة عبر الانترنت** ،مذكرة ماجستير في القانون،تخصص القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية،جامعة مولود معمري،تيزي وزو،2013،ص 43

[2] – فوزية عبد الستار، **شرح قانون العقوبات، القسم الخاص**، دار النهضة العربية، القاهرة، 1990، ص.244

[3] –براهمي حنان، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**،أطروحة دكتوراه)،تخصص قانون جنائي،كلية الحقوق والعلوم السياسية،جامعة محمد خيضر بسكرة،2015 ، ص.184

وما يؤخذ على المشرع الجزائري وبعض التشريعات العربية كالتشريع المصري أيضا أنها لم تعط تعريفا للتزوير وانما يستخلص ذلك من نصوص تلك التشريعات، إلا أن المشرع الأردني أعطى تعريفا له في نص المادة 260 من قانون العقوبات، والقانون اللبناني في مادته 453 والمشرع السوري في نص المادة 440.[1]

ثانيا: تعريف التزوير المعلوماتي

التزوير في وثيقة معلوماتية هو: تغيير للحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية، وذلك بنية استعمالها.

كما عرّف بأنه "تغيير للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة.[2]

كما يعرف التزوير المعلوماتي أيضا بأنه التلاعب في المعلومات المخزنة في أجهزة الحاسبات المرتبطة بالشبكة أو اعتراض المعلومات بقصد تخزينها وتزويرها.

إذن يتضح أن التزوير المعلوماتي يتخذ مفهومين، الأول مفهوم تقليدي يبرز انطلاقا من كون النظام المعلوماتي وسيلة لارتكاب جريمة التزوير، أما الثاني فهو مفهوم حديث يتجسد انطلاقا من فكرة كون تغيير الحقيقة ينصب على معطيات موجودة و مخزنة داخل النظام المعلوماتي.[3]

الفرع الثاني: أركان جريمة تزوير مستند الكتروني والعقوبات المقررة لها

نرى أن المساس بمحتوى المستند الالكتروني وذلك عن طريق تزويره يكون أشد صعوبة من تزوير المستند الورقي، وذلك لأن المحرر الالكتروني بمجرد التوقيع عليه الكترونيا فيندمج المحرر الالكتروني والتوقيع الالكتروني ويصبحان كتلة واحدة مكونا المستند الالكتروني.[4]

---

[1]–طعباش أمين،**الحماية الجنائية للمعاملات الإلكترونية**مذكرة ماجستير في العلوم القانونية ،تخصص علم الإجرام وعلم العقاب،كلية الحقوق والعلوم السياسية ،جامعة باتنة،2013 ص.61

[2]–براهمي حنان، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، مرجع سابق، ص.189

[3] –حسونة عبد الغني، (**جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة**)،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة–كلية الحقوق والعلوم السياسية،جامعة محمد خيضر بسكرة،الجزائر،مابين 16و17،نوفمبر،2015،،ص02

[4] – محمد أمين الرومي، مرجع سابق، ص.88

أولا: الركن المادي في التزوير:

يتمثل الركن المادي في جريمة تزوير مستند معلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا، ومن هنا ولقيام هاته الجريمة لابد من توافر ثلاثة عناصر أساسية:

- وجود محرر.
- تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا.
- أن يترتب على ذلك ضرر عام أو خاص في الحاضر أو في المستقبل.[1]

و سنبين كل عنصر من هذه العناصر على حدا:

1) وجود محرر:

اشترط المشرع في جريمة التزوير التقليدية أن يقع فعل تغيير الحقيقة على محرر من المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية والشهادات، كما اشترط في المحرر أن يكون في شكل "كتابة" أو عبارات خطية، في حينأنه في جر يمة التزوير المعلوماتي فإن المستند المعلوماتي هو الدعامة المادية التي تم تحويل المعطيات المعالجة عليها فيكون إما قرص مضغوط أو شريط ممغنط.[2]

و منه المستند المعلوماتي الذي يقع عليه فعل التزوير هو كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات التي نظمها المشرع الفرنسي في الباب الثالث من القسم الثاني من الكتاب الثاني من قانون العقوبات الفرنسي في المواد من 323-1 إلى 232-7، وتجريم المشرع الفرنسي لتزوير الوثائق المعلوماتية جاء بسبب ارتباط هذه الوثائق أو المستندات المعلوماتية بقانون الإثبات، لذلك جاءت المادة 441-1 من قانون العقوبات الفرنسي لتجرم التزوير الذي من شأنه أن يسبب ضررا والذي يتم بأي وسيلة كانت وفي محرر أو سند للتعبير عن الرأي، ويشمل ذلك الأقراص الممغنطة والأسطوانات المدمجة، وأي بطاقة مغناطيسية أو وسيط يصلح لممارسة حق أو تصرف، أي أن المشرع الفرنسي اشترط أن يكون للمستند المعلوماتي قيمة في الإثبات لأي حق من الحقوق.[3]

---

[1]- خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر**، دار الهدى، الجزائر، 2010، ص ص.134، 135

[2] - معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، (مذكرة ماجستير في العلوم القانونية)،تخصص،قانون جنائي،جامعة الحاج لخضر ،باتنة،2012، ص.46

[3]- المرجع نفسه، ص.47

أما بالنسبة للمشرع الجزائري فقد أدرج النصوص الخاصة بتزوير المحررات في المواد من المادة 214 إلى المادة 229 من قانون العقوبات التي تشترط المحرر لتطبيق جريمة التزوير، وعليه فإنه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وهذا ما يستدعي حقا تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدي على غرار المشرع الفرنسي عند إضافته لعبا ر ة أي سند للتعبير عن الرأي" لتعوض فكرة المحرر التقليدية، أو بإدراج نص خاص بالتزوير المعلوماتي يخرج عن نطاق جرائم المساس بنظم المعالجة الآلية للمعطيات الذي تناولها في القسم السابع مكرر، ضمن المواد من 394 مكرر إلى 394 مكرر7 والتي تهدف لتحقيق الحماية الجنائية للنظم المعلوماتية.[1]

2) تغيير الحقيقة:

يقصد بتغيير الحقيقة هو إبدالها بما يغايرها، وبالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر أو حذف منه طالما ظل مضمون المحرر في حالته قبل الإضافة أو الحذف، ويقوم ذلك بصدد المستندات المعلوماتية في حالة حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزء من برنامج التشغيل أو برامج التطبيق، ويجب في هذه الحالة أن يكون محلا للتجريم.[2]

ولذلك فإن تغيير الحقيقة في المعلومات المعالجة آليا قد يظهر على كيان مادي سواء كان ورقي أو دعامة الكترونية كالشرائط الممغنطة و الأقراص الالكترونية وغيرها من الدعامات المماثلة، و في هذا الغرض يفرق بعض الفقهاء بين تغيير المعلومات المخزنة في الجهاز، وبين إثبات هذه المعلومات في المستندات الصادرة عن النظام المعلوماتي والتي يتحقق فيها وصف المحرر، وبالتالي تتمتع بحماية القانون لها حسب نصوص التزوير باعتبارها معدة للتداول بين الأفراد، حيث يعتبر التزوير المعلوماتي منصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه، بشرط أن تطبع على دعامة مكتوبة أو مسجلة ،أي يكون لها كيان مادي يمكن إدراكه، ولو تم تغيير الحقيقة دون طباعة فلا يمكن أن يطلق عليه تزويرا،

[1] – القانون رقم 66-156،المؤرخ في 8 يونيو 1966،المتضمن قانون العقوبات الصادر في (ج ر،العدد 49،المؤرخة في 11-06-1966)،المعدل والمتمم بالقانون رقم 16-02، المؤرخ في 19 يونيو 2016،الصادر بالجريدة الرسمية ،العدد 37،المؤرخة في 22 يونيو 2016.

[2] – خثير مسعود، مرجع سابق، ص.136.

فالتجريم وفقا للنص القانوني لا يتم إلا في حال حدوث التزوير في [1] المعلومات الخارجة من النظام المعلوماتي.

3) الضرر: الضرر هو عنصر جوهري في جريمة التزوير، إذ لا يكفي لاكتمال الركن المادي في هذه الجريمة تغيير الحقيقة في محرر، وأن يحدث هذا التغيير بإحدى الطرق التي بينها القانون.

ولم ينصالمشرع الجزائري عند تعرضه لجريمة تزوير المحررات الرسمية على الضرر باعتباره عنصرا في جريمة التزوير، لأن موضوع الضرر من المسائل الموضوعية لا القانونية.[2]

ثانيا: الركن المعنوي في التزوير

ويتمثل الركن المعنوي في جريمة تزوير المستندات المعلوماتية في القصد الجنائي، على اعتبار أن هذه الجريمة من الجرائم العمدية، وبالتالي يتخذ القصد الجنائي فيها صورة القصد العام والمتمثل في علم الجاني بفعل تغيير الحقيقة في المستند، مع إرادة إلحاق ضرر بشخص ما.[3]

أما إذا كان الجاني جاهلا بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي، و كذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة، فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل أن يكون عالما بكافة أركان الجريمة، كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة كما هو الحال بالنسبة لانتحال صفة الغير أو الاتصاف بصفه غير صحيحة فقد يقوم مبرمج بيانات بتغيير الحقيقة في المحررات ولكنه غير عالما بهذا التغيير.[4]

---

[1] –براهمي حنان**جريمة التزوير في الوثيقة الرسمية الإدار ية ذات الطبيعة المعلوماتية**،مرجع سابق، ص.205

[2]– دردوس مكي، **القانون الجنائي الخاص في التشريع الجزائري**، الجزء2 ديوان المطبوعات الجزائرية، قسنطينة، 2007، ص.74

[3]– خثير مسعود، مرجع سابق ،ص.138

[4] – معتوق عبد اللطيف،مرجع سابق، ص.49

كما لا يكفي لقيام الركن المعنوي توافر القصد لعام، إذ لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لابد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله، أي إلى الاحتجاج به على اعتبار أنه صحيح.[1]

حيث أن المشرع الفرنسي في جريمة التزوير في المستندات المعلوماتية يتطلب قصدا جنائيا خاصا يتمثل في نية الجاني إلى إحداث ضرر –سواء حقيقي أو احتمالي– للغير.[2]

ومما سبق نخلص إلى أن الركن المعنوي لجريمة التزوير في نطاق المعاملات الالكترونية هو اتجاه إرادة الجاني إلى تزوير مستندات معلوماتية مع نية مسبقة في استعمال المستندات المزورة في الغرض الذي تم تزويرها من أجله و أن يؤدي هذا الفعل إلى حصول ضرر فعلي أو احتمالي لمن ارتكب ضده فمتى توافر الركن المادي و المعنوي قامت جريمة التزوير واستحق مرتكبها العقوبة.[3]

ثالثا: طرق التزوير

إن للتزوير طرقا متعددة تختلف باختلاف المستند المعلوماتي المزور فهناك طرق التزوير المادي وهناك طرق التزوير المعنوي.

1) طرق التزوير المادي:

يقصد بالتزوير المادي، ما يترك أثرا ماديا على العبث بالمحرر وقد يتبين هذا الأثر بالحواس المجردة، وقد لا يتبين إلا بالاستعانة بالخبرة الفنية، وهو ما نص عليه المشرع المصري في المادة 211 عقوبات والتي نصت على طرق خمس للتزوير المادي، وهي كالآتي:

- وضع إمضاءات أو أختام مزورة.
- تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات.
- وضع أسماء أو صور أشخاص آخرين مزورة.
- التقليد والاصطناع.[4]

أما بالنسبة للمشرع الجزائري فلقد وردت صور التزوير في قانون العقوبات على سبيل الحصر، لذلك لا يعتبر تغيير الحقيقة تزويرا إلا إذا حصل بإحدى الطرق التي نصت عليها المواد 214

[1] –براهمي حنان،**جريمة التزوير في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، مرجع سابق،ص.266

[2] – خيثر مسعود،مرجع سابق ص.139

[3] – طعباش أمين،مرجع سابق، ص.72

[4] – إيهاب فوزي السقا،مرجع سابق ،ص.61

و215 بالنسبة لغير الموظف العام، ولقد حصرت المادة 214 ق ع أفعال التزوير المادي بقولها "يعاقب بالسجن المؤبد كل قاضي أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته:

– إما بوضع توقيعات مزورة

–واما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات

–واما بانتحال شخصية الغير أو الحلول محلها

–واما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها.[1]

2) طرق التزوير المعنوي:

بيّن المشرع المصري طرق التزوير المعنوي بنص المادة 213 عقوبات على أنه يعد مزورا من " ..غيّر بقصد التزوير موضوع السندات أو أحوالها في حالة تحريرها المختص بوظيفته، سواء كان ذلك بتغيير إقرار أولي الشأن الذي كان الغرض من تحرير تلك السندات إدراجه بها، أو بجعله واقعة غير معترف بها، في صورة واقعة معترف بها." ومن هذه المادة يتضح أن المشرع قد حصر طرق التزوير المعنوي في ثلاثة حالات:

–تغيير إقرار أولى الشأن.

– جعل واقعة مزورة في صورة واقعة صحيحة

– جعل واقعة غير معترف بها في صورة واقعة معترف بها.[2]

أما بالنسبة لطرق التزوير المعنوي في التشريع الجزائري فتتمثل في:

– استبدال الأشخاص: ويقع التزوير في هذا النوع بانتحال شخص شخصية الغير أو بإحلال شخص محل شخص آخر.

– استبدال اتفاقات أو وقائعاستبدال الاتفاقات والالتزامات والمخالصات وتزييف الإقرارات والوقائع تعتبر من أشكال التزوير المنصوص عليه في المادة 216 ق.ع.ج [3]

و يضاف إلى هذه الطرق صور التزوير المعنوي وهي الأفعال التي تناولتها بالحصر المادة 215 ق.ع.ج والمتعلقة بتزييف جوهر المحررات الرسمية أو ظروفها بطريق الغش، وكتابة

[1] – الأمر رقم 66– 156، المتضمن قانون العقوبات، سالف الذكر .

[2]– إيهاب فوزي السقا، مرجع سابق ،ص.73

[3]– دردوس مكي، مرجع سابق ،ص.73

اتفاقات خلاف التي دونت أو أمليت من قبل الأطراف، وتقرير وقائع كاذبة بصورة وقائع صحيحة، والشهادة كذبا بوقائع غير معترف بها في صورة وقائع معترف بها إسقاط أو تغيير الإقرارات عمدا.[1]

وتعقيبا على ما تطرقنا إليه فيما يخص التزوير المعلوماتي، فإننا نؤكد على ضرورة تدخل المشرع الجزائري لتجريم التزوير المعلوماتي الذي يقع على مستند معلوماتي كالبطاقات الالكترونية وذلك إما بتعديله للنصوص المجرمة للتزوير في المحررات من المواد 214 إلى 229 من قانون العقوبات، مثلما فعل المشرع الفرنسي بإضافة لعبارة: "أي سند للتعبير عن فكرة" في المادة 441-1 من قانون العقوبات الفرنسي، مما أمكن معه متابعة أعمال التزوير التي تقع على بطاقات الائتمان وغيرها من البطاقات المغناطيسية، لأن هناك فراغ تشريعي في القانون الجزائري في هذا المجال ولا يمكن تطبيق نصوص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالنظر إلى أن المستند المعلوماتي المتمثل في مخرجات الحاسب الآلي كبيانات أو معلومات مسجلة على بطاقات الكترونية أو أقراص مضغوطة هو جسم منفصل عن نظام المعالجة الآلية للمعطيات ولم تنص المواد 394 مكرر وما يليها عن حالة تغيير أو حذف معطيات منفصلة عن نظام المعالجة الآلية.[2]

رابعا: عقوبة تزوير مستند معلوماتي:

لقد نص المشرع الجزائري على تزوير المحررات بصفة عامة فجعل كل منهما مستقلة عن الأخرى، وفي هذا الإطار رتب المشرع على تزويرالمحررات الرسمية الجزاءات التالية :

أ-**جريمة التزوير في محررات رسمية أو عمومية:** رتب عليها المشرع الجزائري العقوبات التالية:

- عقوبة السجن المؤبد للقضاة أو الموظفين العموميين الذين ارتكبواتزويرا في المحررات الرسمية أو العمومية أثناء تأدية مهامهم، وهذا وفقا للمادتين214و215 ق ع
- عقوبة السجن المؤقت من 10سنوات إلى 20 سنة وبغرامة من مليون إلى 02مليون دينار كل شخص من غير القضاة والموظفين العموميين يرتكب **جريمة التزوير في محررات رسمية أو عمومية**، وهذا وفقا للمادة 216.

---

[1] – حفصي عباس، **جرائم التزوير الالكترونية** (راسة مقارنة)دكتوراه في العلوم الإسلامية، جامعة وهران1 أحمد بن بلة، 2015، ص.33.

[2] – معتوق عبد اللطيف،مرجع سابق، ص.49

- عقوبة الحبس من سنة واحدة إلى 05سنوات وبغرامة من 500 د ج إلى 1000 د ج كل شخص ليس طرفا في العقد أدلى أمام الموظف بتقرير يعلم أنه مخالف للحقيقة، وفقا للمادة217 .

ب- جريمة التزوير في محررات عرفية أو تجارية أو مصرفية: فقد رتب لها المشرع الجزائري الجزاءات التالية :

- عقوبة الحبس من سنة إلى 05سنوات وغرامة من 500د ج إلى 20000د ج كل من ارتكب تزويرا في محررات تجارية أو مصرفية أو شرع في ذلك وفقا للمادة 219
- عقوبة الحبس من سنة إلى 05سنوات وغرامة من 500 د ج إلى 2000 د ج كل من ارتكب في محررات عرفية أو شرع في ذلك وفقا للمادة 220.

ج- **جريمة التزوير في الوثائق الإدارية والشهادات:** رتب عليها المشرع عقوبة الحبس من 06 أشهر إلى 03سنوات وغرامة من 1500 د ج إلى 15000 د ج كل من قلد أو زيف رخصا أو شهادات أو كتابات أو بطاقات أو منشورات أو إيصالات أو جوازات سفر أو خدمة أو وثائق أو تصاريح أو أوامر خدمة أو من الوثائق التي تصدرها الإدارات العمومية بغرض إثبات حق أو شخصية أو صفة ،وهو مانصت عليه المادة 222 ق ع.[1]

ولم يتعرض المشرع الجزائري إلى جريمة **تزوير المستندات الإلكترونية**، لكن نستنتج من نص المادة 02 من القانون رقم 09-04 السالفة الذكر، أنه إذا ارتكبت الجرائم التقليدية المذكورة آنفا بواسطة منظومة معلوماتية تصبح جرائم تزوير مستند إلكتروني، كما أنه في المقابل أيضا استحدث المشرع الجزائري قسما خاصا في قانون العقوبات يتعلق بالأعمال الماسة بأنظمة المعالجة الآلية للمعطيات لا سيما الأعمال الخاصة بإدخال أو تعديل أو حذف معطيات في أو من هذا النظام.[2] وهو ما سنتطرق إليه في المبحث الثاني من هذا الفصل .

[1]- حسونة عبد الغني،مرجع سابق ، ص ص،08،09

[2]- المرجع نفسه،ص.01

المطلب الثاني

مدى خضوع المستند الإلكتروني للنصوص العقابية لجرائم الأموال

إذا كان الكيان المادي للمعلوماتية يخضع للنشاطالإجرامي لجرائم الأموال دون أي إشكال ،إذن سنحاول في هذا المطلب دراسة مدى إمكانية خضوع المستند الإلكتروني للنشاط الإجرامي ومدى تحقق الحماية الجزائية له وفقا للقواعد العامة المقررة لجرائم الإتلاف ،السرقة ،النصب وخيانة الأمانة .

الفرع الأول : مدى خضوع المستند الالكترونيللنشاط الإجرامي في جريمة الإتلاف

عند تحقيق المجرم المعلوماتي لغايته باختراق النظام المعلوماتي أو البقاء فيه دون إذن يدفعه ذلك البقاء في غالب الأحيان إلى الإطلاع على المعطيات أو البيانات الموجودة داخل النظام، مما قد يدفعه في النهاية لإتلاف تلك البيانات أو المكونات المعنوية لنظام المعالجة الآلية للمعطيات ،وسنتطرق في هذا الفرع إلى تعريف جريمة الإتلاف التقليدية ثم جريمة اتلاف المستند الإلكتروني للتعرف على مدى انطباق النصوص المنظمة لها على إتلاف المستندات الإلكترونية.

أولا: تعريف جريمة الإتلاف التقليدي : تعني تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كليا أو جزئيا، أما التخريب فهو توقف الشيء تماما عن أداء منفعته كليا أو جزئيا دون إتلاف مادته. أما عدم الصلاحية للاستعمال فتعني جعل الشيء لا يقوم بوظيفته على النحو الأكمل، ويعني التعطيل توقف الشيء عن القيام بوظيفته فترة مؤقتة.

يقصد به أيضا تلك الأفعال المادية التي يأتيها الجاني بغرض التخريب و هنا تخريب الوثيقة أي إزالتها أو محو آثارها عمدا بوسائل مختلفة قد تكون التمزيق ، الحذف ..... إلخ.

فالإتلاف إذن يرد على كل المال أو على جزء منه بشرط أن يكون الإتلاف في الحالة الأخيرة من شأنه أن يجعل المال غير صالح للإستعمال كما أنه لا يشترط أن يتم بوسيلة معينة بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي آخر[1]

[1]- آمال قارة،مرجع سابق ص 106

ثانيا: تعريف جريمة إتلاف مستند الكتروني

نصت العديد من التشريعات على جريمة إتلاف المستند الالكتروني أو إتلاف البرامج والمعلومات المخزنة على الحاسب الآلي.[1]

ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا، أو تشويهها على نحو يقع فيه الإتلاف بما يجعلها غير صالحة للاستعمال.[2]

وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوية سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض.[3]

وبالتالي يكون محل جريمة الإتلاف في نطاق السندات الإلكترونية هو كل من المكونات المادية والمتمثلة في الأجهزة كشاشات العرض وأجهزة الإدخال والإخراج والقرص الصلب ... إضافة إلى المكونات المعنوية والمتمثلة في البرامج والبيانات والتي تحقق المعالجة الآلية للمعطيات شرط أن تكون ملك للغير.[4]

ثالثا: أركان جريمة إتلاف سندات

1) الركن الشرعي: جاء في نص المادة 120 قانون العقوبات "يعاقب بالحبس من سنتين إلى عشر سنوات و بغرامة من 000 20إلى000 100 د.ج القاضي أو الموظف أو الضابط العمومي الذي يتلف أو يزيل بطريق العبث و بنية الإضرار وثائق أو سندات أو عقود أو أموال منقولة كانت في عهدته هذه الصفة أو سلمت له بسبب وظيفته."

كما نص المشرع الجزائري على جريمة الإتلاف في المادة407 من قانون العقوبات والمقابلة للمادة 371 مكرر من قانون العقوبات المصري والمادة 1/322 من قانون العقوبات الفرنسي. حيث جاء في نص المادة 407من قانون العقوبات الجزائري:" كل من خرب أو أتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب

---

[1]– محمد أمين الرومي، مرجع سابق، ص.89

[2]– محمد أمين الشوابكة،**جرائم الحاسوب والانترنت،** (الجريمة المعلوماتية) الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2007، ص.216

[3]–براهمي حنان، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، مرجع سابق، ص.54

[4]– طعباش أمين،مرجع سابق،ص.51

بالحبس من سنتين إلى خمس سنوات وبغرامة من 000 20 إلى 000 100 د ج دون الإخلال بتطبيق أحكام المواد من 395 إلى 404 إذا تطلب الأمر ذلك

ويعاقب على الشروع في الجنحة المنصوص عليه في هذه المادة كالجنحة التامة[1]

2- الركن المادي لجريمة الإتلاف:

السلوك الإجرامي :الإتلاف الإزالة بطريق الغش لوثيقة أو سند أو عقود أو أموال منقولة و تشترط المادة أن تكون بواسطة موظف قاضي أو ضابط عمومي تكون قد سلمت إليه هذه الوثائق والأموال بحكم الوظيفة ، أي بسببها أو لصفته.

أ- صفة الجاني:

القاضي :القاضي هو الذي يصدر الأحكام و هنا بحكم وظيفة يقوم بإزالة الوثائق لغرض ما و هما إما قضاة تابعين للنظام القضائي العادي أو الإداري كذلك لدينا الموظف : و هنا يدخل الموظف الذي يمارس مهنته بصفة دائمة أو مؤقتة المهم أن تكون هذه الوثائق أو الأموال المنقولة قد سلمت له بسبب الوظيفة التي يمارسها في تلك الفترة و يدخل ضمن هذا الإطار كذلك الضابط العمومي

ب- نوع الوثيقة : هنا الإتلاف يشمل مختلف الوثائق قد تكون المستندات أو عقود و التي تكون في حوزة الموظف كما تشمل أموال منقولة كانت في عهدته ، فالمال المنقول يقصد به ذلك المال الذي يمكن تغيير موقعه نتيجة للفعل المادي و هنا الإتلاف المعدي الذي يتم بواسطة الغش فمدلول المنقول في القانون الجنائي واسع عن القانون المدني بحيث تعبر منقولات المواشي التي يعتبرها القانون المدني عقارات بالتخصيص ، كذلك المحاصيل مزرعة و التي يرد عليها الإتلاف على هذه الأشياء كمحل للجريمة.

و يتمثل الركن المادي لجريمة الإتلاف في النشاط الإجرامي والذي يتمثل في التأثير في مادة الشيء، على نحو يذهب أو يقلل من قيمته الاقتصادية ،عن طريق الإنقاص من كفاءته للاستعمال المعد له ، فمثلا جهاز التلفاز قد يتم إتلافه عن طريق إدخال تيار كهربائي على الشدة فيتم حرق المكثفات داخل الجهاز،فبالرغم من أن الجهاز لم يتم تدميره كعنصر مادي، فهو محتفظ بهيكله وشكله ومكوناته المادية، إلا أنه يصبح غير صالح لما أعد له وهو المشاهدة

[1] - الأمر رقم 66- 156، المتضمن قانون العقوبات، سالف الذكر

وما يلاحظ أن فعل الإتلاف بصفة عامة له عدة صور ،ومن الطبيعي أن يختلف مضمون وصور الإتلاف في قانون العقوبات عن إتلاف البرامج والمعلومات ،ويرجع ذلك الاختلاف إلى محل الجريمة ، حيث يشترط أن يقع الإتلاف أو التعييب على مال منقول أو عقار، مملوك للغير

3- الركن المعنوي :جريمة الإتلاف بصفة عامة هي من الجرائم العمدية، تتطلب توفر القصد الجنائي العام لعنصريه العلم و الإرادة أي توجيه إرادة الجاني و هو مدرك كامل الإدراك إلى قيامه بالفعل أي إلى الإزالة أو إتلاف الوثائق المو ضوعة بحوزته أو تغيير مجرى الأموال المنقولة بغرض الإضرار بهلو يشترط أن يعلم الجاني أن المال الذي يقوم بإتلافه أو تعيبه مملوك للغير.[1].

وعموما فلقد اختلف الفقه بين مؤيد ومعارض لوقوع جريمة الإتلاف على المعلومات لذلك فإن الإشكالية في هذا المقام تتمثل في مدى إمكانية تطبيق النصوص التقليدية ،التي تعاقب على أفعال الهدم والتخريب الواقعة على أملاك الدولة والأفراد على إتلاف المعلومات والبرامج المعلوماتية ؟

وللإجابة على هذه الإشكالية لابد من التطرق إلى الآراء المختلفة حو ل تحديد طبيعة المعلومات

- **الرأي المؤيد لإمكانية تطبيق النصوص التقليديةلجريمة الإتلاف على جرائم المستند الإلكتروني:**

إن المشكلة تكمن في وصف المال بأنه منقول،وليس في الطبيعة المادية وغير المادية للنظام المعلوماتي بما يحتوي من معلومات وقواعد بيانات ونظم التشغيل اللازمة لها،وهذه الطبيعة المادية تمثل الجانب الأكبر من قيمة النظام كله،لذلك ،فإن جوهر الإتلاف هو إفقاد صلاحية المال المتلف من الغرض المعد له،وهو مايفقده قيمته الحقيقية.

إن البرامج والبيانات المنطقية هي مجموعة من المعلومات والأوامر لا يمكن الاستفادة منها إلا إذا وضعت في شيء مادي يمكن تعامله مع الجهاز،ومن هذا المنطلق،ذهب البعض إلى اعتبار البرنامج شيء مادي ،وبالتالي إمكانية تطبيق النصوص التقليدية،كون الأسطوانة التي يوضع فيها ،لها وجود مادي ملموس

وقد استندت هذهالآراء لتأكيد إمكانية تطبيق النصوص التقليدية،إلى العديد من الحجج:

[1]-محمد أمين الرومي ، مرجع سابق ،ص ص92-93

– إن البرنامج المعد والمعلومات المذكورة التي تشمل بطبيعتها العنصرين المادي والمعنوي،لايمكن فصل أحدهما عن الآخر،فلا يتصور أن يوجد برنامج دون وسيط مادي

– إن التطور الهائل في عالم التكنولوجيا جعل المعلومات تحتل مركزا مهما، يمكن أن تكون معها محلا للملكية، وعلى هذا الأساس يمكن اعتبارها في حكم الشيء المادي ذات القيمة الإقتصادية

على ضوء ماتقدم ،يمكن القول أن البرنامج هو عبارة عن أوامر موضوعية بشكل منطقي، فلا يمكن الإستفادة منه إلا إذا وضع في شيء مادي،إلا أنه يجب الفصل بينه وبين الوسيط المادي،لأنه يمكن الدخول إلى البرنامج واتلاف المعلومات الموجودة بداخله دون المساس بالوسيط المادي.

–الرأي المعارض لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على جرائم المستند الإلكتروني:

اعتبر هذا الرأي أن المعلومات المبرمجة آليا كالنبضات الكهربائية، تفتقر إلى الطبيعة المادية، وان هذه المعلومات ذات طبيعة معنوية، وهي تستقل من ناحية الأصل عن الوعاء المفرغة فيه من ناحية الشكل الخارجي ،ولها ذات القيمة الاقتصادية للمال المادي،وبالتالي يتعين أن تخضع لأحكامه وتعامل تماما كما يعامل، فيعطيها الحماية والحقوق ذاتها،المقرر ة للمال المادي.

وقد أكد هذا الفقه على صعوبة تطبيق النصوص التقليدية من خلال القضية التي ظهرت في أستراليا، وكانت الأولى التي يتم فيها توجيه الاتهام باستخدام برنامج خبيث لإتلاف المعلومات، وتتلخص وقائع هذه القضية في قيام طالب بالدخول إلى الكومبيوتر في معهد سوين برن للعلوم التكنولوجية، وقيامه بإدخال برنامج تمهيدي يحتوي على فيروس، مما ترتب على ذلك إتلاف جميع البيانات المسجلة على الأقراص الممغنطة، التي تم إدخالها إلى الكومبيوترات المتصلة بالنظام، فضلا عن إتلاف المكونات المادية، وقد قدم المتهم للمحاكمة بتهمتي الدخو ل غير المصرح به إلى نظام الكمبيوتر،واتلاف ممتلكات الغير، إلا أن المحكمة برأته من التهمتين، كونها انبرت أنه يمتلك حق الدخول باعتباره أحد طلاب المعهد، أما فيما يتعلق بإتلاف المعلومات، فعلى الرغم من تحقق المحكمة منه، إلا أنها استبعدت أن تكون

المعلومات محلا يمكن أن يقع عليه النشاط الإجرامي، وعلى الرغم من الخسائر،إلا أن عدم وجود نص تشريعي صريح يجرم فعله، أدى إلى تبرئته.

ويمكن القول أن الرأي المعارض قد ميز بشكل واضح بين المعلومات كمنقول معنوي، وبين أدوات الكومبيوتر وآلاته التي تخضع للنصوص التقليدية ،كونها شيئا ماديا بحتا،ومن هنا تظهر صعوبة تطبيق النصوص التقليدية.

بالإضافة إلى ذلك ،فإن العقوبات التي تفرض لا توازي قيمة الضرر، فأضرار الشركات تقدر بالملاين ،بل بالمليارات وبالتالي،فإن النصوص التقليدية عاجزة عن المساواة بين الضرر وبين العقوبة،من هنا كانت الحاجة إلى تدخل المشرع لسد هذه الثغرات[1]

إلا أن الرأي الراجع في الفقه يتجه إلى وقوع جريمة الإتلاف على البرامج والمعلومات وبالتالي وقوعها على المستند الإلكتروني وهو ما سنكتشفه في المبحث الثاني من هذا الفصل

الفرع الثاني: مدى خضوع المستند الإلكتروني للنشاط الإجرامي في جريمة السرقة وخيانة الأمانة وجريمة النصب

إذ كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال،إذن سنحاول في هذا الفرع دراسة مدى إمكانية خضوع المستند الإلكتروني للنشاط الإجرامي لجرائم السرقة والنصب وخيانة الأمانة ومدى تحقق الحماية الجزائية له وفقا لنصوص هذه الجرائم

أولا: جريمة السرقة

تتفق السرقة عبر الانترنت مع السرقة التقليدية في أوجه كثيرة إلا أن اختلافهما يكون في محل السرقة ذاته، فمحل السرقة التقليدية مال منقول مملوك للغير،أما محل السرقة عبر الانترنت فهي المعلومات والبيانات المعالجة إلكترونيا.

وقد نصت المادة 350 من قانون العقوبات الجزائري على أنه (كل من أختلس شيئا غير مملوك له يعد سارقا)

[1]– ميساء مصطفى بركات،**جرائم التعدي على المعلوماتية** (الإتلاف والتزوير)،رسالة ماجستير،كلية الحقوق والعلوم السياسية،جامعة بيروت،لبنان 2009،ص 27

يمكن تعريف جريمة السرقة الإلكترونية على أنها (استخدام الوسائط الحاسوبية وشبكات الإنترنت لأخذ مال متقوم مملوك للغير بلغ نصابا ،خفية،من حرز مثله،من غير شبهة ولا تأويل)[1]

يفهم من هذا التعريف أن السرقة في مجال المعاملات الإلكترونية لا تستهدف الشريط الممغنط أو الأسطوانة أو الذاكرة أو الأسلاك التي تنقل الشارة لأن السارق لا يستهدف سرقتها للحصول على القيمة المادية بل يسرق ماهو مسجل عليها.

1- الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية

إن البحث في مدى تحقق الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية هو مراعاة لمدى تحقق فعل الأخذ أو الاختلاس في هذه الجريمة ،ويستوي فعل الاختلاس في أن يكون الجاني قد استولى على المال خلسة أو عنوة أو تسلمه بناءا على يد عارضة فغير نيته واستولى عليه،ومن ثم فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه إلى الجاني،بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية .[2]

ولقد أختلف الفقهاء بخصوص فكرة السرقة المعلوماتية ،فالرأي المؤيد لفكرة السرقة المعلوماتية يرى أن الركن المادي للسرقة المعلوماتية وهو فعل الاختلاس يتكون من عنصرين هما العنصر الموضوعي وهو النشاط أو السلوك الإرادي المؤدي إلى النتيجة مع وجود علاقة سببية بينهما ،أما العنصر الأخر الشخصي فهو نية الجاني في تملك الشئ وحيازته ،حيث عند تشغيل الحاسب الآلي والحصول علىمعلومات أو البيانات يكون قد اختلسها واستحوذ عليها بطريق غير مشروع[3]

[1]- ضياء مصطفى عثمان ،مرجع سابق،ص 211

[2]- طعباش أمين ،مرجع سابق ،ص 87

[3]- معتوق عبد اللطيف ،مرجع سابق،ص 35

ولذلك أدانت محكمة (Grenoble) دائرة الجنح –المستأنفة في 1995/02/15،عامل بتهمة السرقة كان قد أخرج من المؤسسة التي يعمل بها أوراقا سرية كان سيقوم بتصويرها ثم يعيدها للمؤسسة [1]

أماالرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة [2]

كذلك يترتب على ذلك أن التوقيع الإلكتروني والمستند الإلكتروني، والرسالة الإلكترونية، والكتابة الإلكترونية كل هذه عبارة عن قيم منقولة أو اعتبارية ليست أشياء وبالتالي لا يمكن أن يخضع الاستيلاءعليها بدون و جه حق لجريمة السرقة[3]

2- الركن المعنوي:

يتخذ الركن المعنوي في جريمة السرقة في نطاق المعلوماتية صورة القصد الجنائي العام والخاص،ويتحقق القصد الجنائي العام ، بتوافر العلم والإرادة [4]

فيجب أن تتجه إرادة الجاني الاستيلاء على المعلومات المسجلة إلكترونيا سواء المعلومات المخزنة داخل النظام المعلوماتي أو المعلومات المسجلة إلكترونيا،والمخزنة على دعامة خارجية مثل الأسطوانات والشرائط الممغنطة،مع علمه بأن المعلومات محل السرقة ملكا له ،فإذا قام شخص بأخذ قرص ممغنط يحتوي على برامج معلوماتية واختلسه من صاحبه ،ثم قام بتشغيله لمعرفة محتواه ثم رده فإن إرادة الاختلاس، تنتفي لديه ويختلف القصد العام عنده [5]

نلاحظ مما سبق أن التحجج بأن المال المعلوماتي غير قابل للسرقة ،هي حجة تجافي المنطق ذلك أن التسليم بها يعني تجريد المال المعلوماتي من الحماية الجنائية مما يجعله عرضة للاعتداء

---

[1]– محمد أمين الشوابكة،مرجع سابق،ص156

[2]- معتوق عبد اللطيف،مرجع سابق ص 35

[3]– محمد أمين الرومي ،مرجع سابق،ص 103

[4]– محمد أمين الشوابكة ،مرجع سابق،ص 160

[5]– طعباش أمين،مرجع سابق،ص ص 99،100

وبالتالي حفاظا على المصلحة العامة والخاصة ولكي لا يفلت المجرم من العقاب يجب تطبيق القواعد العامة التي تحكم جريمة السرقة إلى أن يصدر تشريع خاص بها ،دون أن يكون في ذلك أي إخلال بالمبادئ العامة التي تحكم القانون الجنائي [1]

ثانيا: مدى تحقق الحماية الجنائية للمستند الالكتروني وفقا للقواعد العامة المقررة لجريمة خيانة الأمانة

تنص المادة 376 من قانون العقوبات الجزائري على : كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقود أو بضائع أوأوراقا مالية أو مخالصات أو أية المحررات أخ ى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو وكالة أو الرهن أو عارية الاستعمال أو لأداة عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك أضرار بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة ويعاقب عليها بالحبس من ثلاثة أشهر إلي ثلاث سنوات وبغرامة من000 20 إلى 000 100 د ج

ويجوز علاوة على ذلك أن يحكم على جانب بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 وبالمنع من الإقامة وذلك لمدة سنة على الأقل وخمس سنوات على الأكثر [2].

وتعرف خيانة الأمانة على أنها استيلاء الأمين عمدا على الحيازة الكاملة لمال سلم عليه بمقتض سند من سندات الأمانة التي نص عليها القانون [3]

والملاحظ أن المشرع الجزائري لم يتطرق لجريمة خيانة الأمانة في المجال المعلوماتي فالبرغم من استحداث هذا الأخير لنصوص تعالج المساس بالأنظمة المعالجة الآلية للمعطيات وتعالج الغش المعلوماتي بشكل مباشر وتعالج التزوير و الإتلاف مثلا إلا انه اغفل ذلك فيما يتعلق بجريمة خيانة الأمانة .

[1] –طعباش أمين،مرجع سابق ،ص ص 101،102

[2] – الأمر رقم 66–156،المتضمن قانون العقوبات ،سالف الذكر. -

[3] – علي عبد القادر القهوجي، **شرح قانون العقوبات القسم** ، الكتاب الثاني،دار المطبوعات الجامعية،الإسكندرية،1999، ص 365

والسؤال المطروح أيضا بالنسبة إلى هذه الجريمة. هل يمكن القول بخضوع المكونات المعنوية .للأنظمة المعلوماتية ومنها المستند الالكتروني للقواعد العامة التي تحكم جريمة خيانة الأمانة ؟

وفي هذا الصدد يرى جانب من الفقه أن الطبيعة المعنوية أو الغير مادية للقيم " المعلومات " في المجال المعلوماتي تثير بعض الصعوبات ،وعلى الرغم من ذلك فان هذه القيم المعنوية مثل المعلومات والبرامج تصلح لأن تكون من ذلك محلا لجريمة خيانة الأمانة إما لأنها تعتبر بمثابة بضائع ،وا ما لأنها تدخل في مفهوم المكاتيب التي ترتب إلزاما أو تحوي مخالصة .

وبالتالي نستنتج أن المعلومات التي يتم تداولها في مجال المعاملات الالكترونية تصلح لأن تكون محلا لجريمة خيانة الأمانة ، ومتى تجسدت تلك المعلومات في شكل مرئي سواء على الشاشة الحاسب الآلي أو على دعامات خارجية كالأوراق والأقراص ، فهي تعد من قبيل الأموال لها قيمة اقتصادية .

أما إذا كانت تلك المعلومات عبارة عن أفكار مجردة لم يتم تجسيدها في الواقع أي معالجتها أليا فإنه لايمكن اعتبارها من قبيل الأموال وبالتالي لايمكن أن تكون محلا لجريمة خيانة الأمانة [1]

ويتمثل الركن المادي لهذه الجريمة في الأفعال الاختلاس والاستعمال والتبديد، أما الركن المعنوي فيتطلب هذه الجريمة، القصد العام. وهو أن يعلم الجاني أن ما يستولي عليه هو مال منقول مملوك للغير.وان تتجه إرادته إلى الاستيلاء على الحيازة الكاملة للشيء والظهور عليه بمظهر المالك أو صاحب الحق عليه. أما القصد الخاص فيتمثل في نية التملك [2] .

ومن التطبيقات القضائية لجريمة خيانة الأمانة في مجال المعلوماتية قضت محكمة استئناف هولندا بثبوت جريمة خيانة الأمانة في حق محلل للبرامج بإحدى الشركات كانت طبيعة عمله التردد على عملاء الشركة لصيانة برامجهم وبحوزته أقراص ممغنطة تخص

[1]– طعباش امين ، مرجع سابق،ص ص 128 ، 129

[2]– عبد القادر القهوجي ، مرجع سابق،ص 391

الشركة تحوي برامج وبيانات معنية لازمة لعمليات الصيانة ، فقام بنسخها على أقراص تخصه بغرض إنشاء مشروع خاص به [1] .

ثالثا: مدى تحقق الحماية الجنائية للمستند الالكتروني وفقا للقواعد العامة المقررة لجريمة النصب

تنص المادة 372 قانون العقوبات الجزائري على جريمة النصب حيث أنها نصت :على كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول أو على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر و بغرامة من 000 20 دج إلى 000 100دج.

و إذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو أدونات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية فيجوز أن تصل مدة الحبس إلى عشر سنوات و الغرامة إلى 000 400 دج.

و في جميع الحالات يجوز أن يحكم علاوة على دلك عل الجاني بالحرمان من جميع الحقوق الواردة في المادة 14 أو من بعضها و بالمنع من الإقامة ودلك لمدة سنة على الأقل وخمس سنوات على الأكثر [2]

يعرف النصب على أنه الاستيلاء على الحياة الكاملة عمدا بطريق الحيلة او الخداع على مال مملوك للغير [3]

والسؤال الذي يطرح نفسه في هدا الصدد: هل من المتصور أن تقع هده الجريمة على المستند الالكتروني باعتباره من المكونات المعنوية للنظام المعلوماتي ؟ وما تجدر الإشارة إليه أن المشرع الجزائري لم يتطرق إلى النصب الواقع في مجالات المعاملات الالكترونية .

---

[1]– آمال قارة ،،مرجع سابق،ص 58

[2]– الأمر قم،66–156،المتضمن قانون العقوبات ،سالف الذكر.

[3]– طعباش أمين ،مرجع سابق، ص 103

و للإجابة على الإشكالية السابقة الذكر ظهرت عدة اتجاهات فقهية حول مدى إمكانية تطبيق القواعد العامة لجريمة النصب على النصب المعلوماتي ، حيث يرى الاتجاه الأول صلاحية المعلومات و البرامج المعالجة ألليا لأن تكون محلا أو موضوعا لجريمة النصب وفقا للقواعد العامة أما الاتجاه الثاني فيرى عكس ذلك وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة.

وذلك ما يمكن استنتاجه من نصوص المشرع الجزائري كونه لم يستحدث نصوصا تتعلق بالنصب المعلوماتي فهو يساير هذا الاتجاه التقليدي أما الاتجاه الثالث فيطبق النصوص المتعلقة بالغش في مجال البنوك و البريد والتلغراف لغرض الغش على حالات النصب المعلوماتي [1]

كما تتحقق هذه الطرق كذلك باستخدام المستندات الغير صحيحة التي يخرجها الحاسب بناء على ما وقع في برامجه أو في البيانات المخزنة من تلاعب كي يستولي على أموال لا حق له فيها[2] ويتمثل الركن المادي في هذه الجريمة في فعل الاستيلاء على الحيازة الكاملة لمال مملوك للغير عن طريق إحدى وسائل الاحتيال المتعددة في القانون على سبيل الحصر ([3])

أما الركن المعنوي في هذه الجريمة فيتطلب القصد العام وهو علم الجاني بالعناصر المتمثلة في ماديات الجريمة وانصراف إرادته إلى تحقيق هذه العناصر ويتطلب كذلك القصد الخاص وهو نية التملك .

ومما سبق يمكن القول أن الأموال التي يتم تداولها في نطاق المعاملات الالكترونية يمكن أن يشملها النشاط الإجرامي المنصوص عليه في المادة 372 من ق.ع الجزائري، كون التلاعب بالمعلومات آو البيانات المحيطة بتلك الأموال يؤذي في النهاية إلى تسليم المال للجاني [4] .

[1]– طعباش أمين ،مرجع سابق ،ص ص 107.108

[2]– آمال قارة ،مرجع سابق،ص 48

[3]– المرجع نفسه، ص 45

[4]– طعباش أمين ،مرجع سابق ص 114

وبالتالي بقيام المشرع الجزائي بالنص صراحة على خيانة الأمانة و النصب المعلوماتي يحسم الجدل القائم حول إمكانية وقوع هذه لأفعال على المستند الالكتروني .

المطلب الثالث

الحماية الجزائية للمستند الإلكتروني من خلال النصوص العقابية للجرائم الواقعة على الملكية الفكرية

نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المميزة للمال المعلوماتي، كما سبق التطرق إليه في المطلب السابق، أدى هذا إلى جدل فقهي وقضائي حول الحماية المناسبة لبرامج الحاسب الآلي، ومنها المستند الإلكتروني، فقد استقر الفكر القانونيمؤخرا على إخضاع هكذا برامج لقوانين الملكية الفكرية [1]

الفرع الأول : مدى اعتبار المستند الإلكتروني موضوع من موضوعات حق المؤلف

لقد تباينت مواقف الفقهاء بين مؤيد ومعارض فيما يخص مدى اعتبار البرنامج مصنفا فكريا ،لكن الاتجاه الذي ساد هو إخضاعها إلى قوانين حماية حق المؤلف .

لم ينص المشرع الجزائري صراحة قبل تعديل قانون حق المؤلف والحقوق المجاورة سنة 2003، على حماية البرامج المعلوماتية في إطار حق المؤلف، لكن رغم عدم التنصيص على ذلك، ذهب بعض المختصين إلى إمكانية هذه الحماية وهذا حسب نص المادة الثانية من الأمر 14/73، والمادة السابعة من الأمر 16/96،عند ذكرهما للمصنفات المشمولة بالحماية، إذ تفيدان بأن الحماية تشمل حماية المصنفات الجديدة التي لم تكن موجودة وقت صدور هذه النصوص .

وعليه فالاتجاه السائد حاليا هو الحماية وفقا للنصوص المعدلة لقوانين التأليف، وذلك بالاعترافصراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي.

وذلك مافعله المشرع الجزائري من خلال تعديله للأمر رقم 14/73، بموجب الأمر 10/97[2].

يتمتع المؤلفون بصفة عامة بحماية جنائية لحقوقهم المالية وكذا الأدبية تأتي مكملة للحماية المدنية المتمثلة في دعوى تعويض الضرر، مع إمكانية اللجوء إلى الإجراءات التحفظية

[1]- امال قارة ،مرجع سابق ص 63

[2]– المرجع نفسه،ص 77

،فالحماية الجزائية تكفل ضمان عدم التعرض مرة أخرى لحقوق المؤلف ،ويعود ذلك لطبيعتها الردعية والزجرية والتي تجعلها أكثر تأثيرا من الجزاء المدني.[1]

الفرع الثاني :مدى إمكانية حماية المستند الإلكتروني وفقا لنصوص جرائم التقليد

تعرف جريمة التقليد أو النسخ بأنها: (نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه)؛ وعرفت كذلك بأنها: القيام بعمل لا يقوم به سوى المؤلف أو يرخص به.[2]

ومادام المشرع الجزائري قد أدمج تطبيقات الحاسب الآلي ضمن قائمة المصنفات المحمية عن طريق القانون المتعلق بحقوق المؤلف، فإن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد، وقد نص المشرع الجزائري في الأمر 05/03،على جريمة التقليد والجرائم المشابهة لها .[3]

أولا: الركن المادي لجريمة التقليد

يتمثل الركن المادي لهذه الجريمة حسب نص المادة 151،من الأمر 05/03.[4]

المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 14/73،بقولها (يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

-الكشف الغير مشروع عن مصنف أو أداء فني.

-استنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة بالإضافة إلى بيع نسخ مقلدة أو تصديرها .

-تأجير مصنف أو أداء فني أو عرضه للتداول.

---

[1] راضية مشري ،**(الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف)**،مجلة التواصل في العلوم الإنسانية والإجتماعية ،العدد 34،كلية الحقوق،جامعة 8 مايو 1945،قالمة ،جوان 2013،ص142

[2] – خثير مسعود ،مرجع سابق ،ص 88

[3] - آمال قارة ،مرجع سابق ص 82

[4] – الأمر رقم 03-05،المؤرخ في 19يوليو،2003،المتعلق بحق المؤلف والحقوق المجاورة (ج ر،العدد 44،المؤرخة في 23يوليو2003)ص21.

ولا يكفي لتوافر النشاط الإجرامي في جريمة التقليد الاعتداء على حق من حقوق مؤلف البرامج أو قواعد البيانات،وانما يشترط إلى جانب ذلك عدم موافقة المؤلف على ذلك أو من يقوم مقامه

وتنتج هذه الموافقة أثرها وتحول دون قيام جريمة التقليد بالنسبة للحق أو الحقوق التي صدرت الموافقة عليها، أما التصرف في حق آخر غير الحق الذي صدرت عنه الموافقة يعتبر مرتكبا لجريمة التقليد ،ولا يجوز للجاني الاحتجاج بالموافقة السابقة.[1]

ثانيا: الركن المعنوي

لا بد من توافر العلم والإرادة لدى الجاني أثناء قيامه بأي اعتداء في صورة من الصور السابقة وبالتالي القصد المتطلب في هذه الحالة هو القصد العام وليس الخاص،فليس بالضرورة أن يقصد المعتدي ،إلحاق الضرر بمؤلف البرنامج ،وبالتالي يكفي أن يعلم الجاني أنه يعتدي على برنامج لشخص أخر وان تتجه إرادته إلى ذلك الفعل ،لقيام هذه الجريمة .

ومنه كانت العقوبات المقررة للاعتداءات على حقوق الملكية الأدبية والفنية محددة في المواد 153/156/157/158/159/من الأمر 05/03 [2]

وبالتالي رغم اعتراف المشرع الجزائري لتطبيقات الإعلام الآلي بصفة المصنف المحمي ،ورغم التعديلات الواردة في مضمون الأمر 05/03،إلا أنه أغفل نقاطا هامة لكون بعض المفاهيم التقليدية لحقوق المؤلف لا تتماشى وطبيعة المصنفات المعلوماتية

إذن كان من الأجدر في هذا الإطار أن يضع المشرع الجزائري نصا خاص بالمصنفات المشركة في مجال الإعلام الآلي كما هو الحال بالنسبة للمصنفات السمعية البصرية

لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنص بصفة أساسية على شكل البرنامج أو مضمونه الإبتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج [3]

---

[1]–راضية مشري،مرجع سابق،ص 143

[2]– الأمر رقم 03–05، المتضمن حق المؤلف والحقوق المجاورة، سالف الذكر .

[3]– آمال قارة، مرجع سابق،ص 95

حيث لا يلزم أن تكون هذه البرامج في شكل معين ،وبالتالي يمكن التعبير عنها بأية وسيلة إذا كانت مثبتة على دعامة مادية ،وقد تكون هذه الدعامة في شكل شرائط مغناطيسية ، أو شكل أقراص مغناطيسية ،أوشكل أقراص مغناطيسية مرنة ،أو أقراص صلبة أو مدمجة [1] .

لذلك لا مفر للمشرع الجزائري من ضرورة اللجو ء إلى استحداث نصوص تجريمية خاصة بتقليد المستند الإلكتروني في مجال المعلوماتية .

نستنتج أن دائرة الحماية المقررة لحقوق المؤلف والحقوق المجاورة قد تتداخل مع دائرة الحماية المقررة للمستند الإلكتروني غير أن الدراسة أظهرت الفارق بينهما فأوضحت أن عنصر الإبداع لا يعد عنصرا في المستند بخلاف المصنف ،وأن مايخرج من مدلول الأخير قد يدخل في مدلول المستند،وأن محل الحماية الجزائية للمصنف ترتكز عل حماية حق المؤلف،على أفكاره ،فإن محتوى المستند وسريته هي محل حماية المستند الإلكتروني[2] .

[1]– خثير مسعود ، مرجع سابق ،ص ص 85،86

[2]– أشرف توفيق شمس الدين،مرجع سابق ،ص 47

المبحث الثاني

الحماية الجزائية الموضوعية للمستند الإلكتروني وفقا للنصوص العقابية المستحدثة

نظرا لقصور الحماية الجزائرية الموضوعية للمستند الالكتروني بواسطة النصوص العامة التقليدية وبصفة خاصة نصوص جرائم الأموال وجرائم التزوير، وبالتالي ظهرت الحاجة إلى ضرورة سن نصوص عقابية موضو عية خاصة حديثة لمكافحة جرائم الماسة بالمستند الالكتروني.

وفي هذا الشأن تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما فلقد جرم المشرع الجزائري بعض الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي تم إدراجها في القسم السابع مكرر من قانون العقوبات هذه الجرائم محددة بموجب المواد 394 مكرر إلى 394 مكرر 7، أحكام هذه المواد تعاقب على الاختراقات الغير مصرح بها داخل نظم المعالجة الآلية للمعطيات .

وقبل التطرق إلى هذه الجرائم يجب أولا التعرف بأنظمة المعالجة الآلية للمعطيات، حيث لم يقم المشرع الجزائري بتعريفيها وهذا على غرار المشرع الفرنسي أما الفقه الفرنسي فقد عرفها كما يلي "هي كل مركب يتكون من وحدة أو مجموعة وحدات المعالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهز ة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية [1].

إن الشرط الأول الذي يلزم لتحقق الجرائم الماسة بالنظم المعلوماتية، هو وجود نظام معالجة البيانات أو نظام المعالجة الآلية للمعطيات، ونظرا لقيمة نظم المعلومات فقد جرم المشرع التعدي عليها، سواء كان ذلك بالتعييب أو التدمير، أو إعاقة عملها أو الدخول إليها على وجه غير مشروع .[2].

---

[1]– آمال قارة ،مرجع سابق،ص 102

[2]– عبد الفتاح بيومي حجازي ،**التجارة الإلكترونية وحمايتها القانونية**،دار الكتب القانونية،مصر،2007،ص22

وسنتناول في هذا المبحث جرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلال التطرق لجريمة الدخول أو البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات (المطلب الأول) جرائم الإعتداء على سلامة المعطيات (المطلب الثاني) الجرائم المنصوص عليها في قانون التوقيع والتصديق الإلكترونيين (المطلب الثالث).

المطلب الأول:

جريمة الدخول أو البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات

– نصت عليها نص المدة 394 مكرر يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000دج إلى 000 200دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك

– تضاعف العقوبة إذا أترتب على ذلك حذف أو تغير لمعطيات المنظومة .

و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6)أشهر إلى سنتين(2)والغرامة من 50.000 دج إلى000 300 ج.[1]

وبالتالي الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير مشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء الغير مشروع، أما محو أو تغير في المعطيات الموجودة في النظام أو التخريب لنظام اشتغال المنظومة .[2]

الفرع الأول: الركن المادي للجريمة الدخول أو البقاء الغير مشروع في النظام

عالج المشرع الجزائري جريمة الدخول والبقاء الغير مشروع في المادة 394 مكرر ق ع ج وعليه سوف نتطرق لفعل الدخول أولا ثم فعل البقاء

[1]– الأمر رقم 66–156،المتضمن قانون العقوبات سالف الذكر .

[2]– أمال قارة،مرجع سابق ،ص 107

أولا: فعل الدخول

– فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلومات أي الدخول المعنوي أو الالكتروني ويتحقق فعل الدخول الدخول إلى النظام متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج ، وكذالك يتحقق الدخول الغير مشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه[1]

والملاحظ أن المشرع الجزائري يعاقب بمجرد الدخول أو البقاء الغير مشروع لمدة طالت أو قصرت

وبما أن المشرع الجزائري لم يحدد وسيلة الدخول إلى النظام المعلوماتي فإنه يمكن الدخول بأي وسيلة كانت ، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها ،أو باستخدام برنامج أو شفرة خاصة ، أو عن طريق استخدام الرقم الكودي لشخص أخر أو الدخول من خلال شخص مسموح له بالدخول [2]

ثانيا: فعل البقاء

-يعرف البقاء الغير المشروع بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له لحق في السيطرة على هذا النظام [3] و يتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا انه يقرر البقاء داخل النظام وعدم قطع الاتصال، والبقاء المعاقب عليه قد يتحقق مستقلا عن الدخول إلى النظام وقد يجتمعان ويكون البقاء معاقب عليه استقلالا، حين يكون الدخول إلى النظام المعلوماتي مشروعا [4]

---

[1] -خثير مسعود ،مرجع سابق،ص ص 115-116

[2] – المرجع نفسه ،ص115 -

[3] – بومعيزة جابر ،(**الاعتداء على المعطيات الآلية في الحكومة الإلكترونية**)مجلة البحوث والدراسات القانونية والسياسية،العدد الثاني عشر،كلية – الحقوق والعلوم السياسية ،جامعة البليدة 2،(ب،ت) ص 132

[4] – طعباش أمين ،مرجع سابق،ص 38

الفرع الثاني: الركن المعنوي لجريمة الدخول أو البقاء الغير مشروع داخل النظام

–الركن المعنوي يجب تحديد ،بمعنى أن يكون المتهم على علم بالدخول أو البقاء الغير قانوني وبدون وجه حق في النظام والدخول والبقاء يشكلان جريمة عندما يرتكبان عن طريق الغش فمصطلح"عن طريق الغش يُفترض أن الدخول أو البقاء كان بإرادة الفاعل وان هذا الأخير كان على علم بارتكابه النشاط المجرم ولكن لا يهم أن يكون الفاعل أراد الإضرار أو لا بالنظام المخترق، وبالتالي الركن المعنوي في هذه الجريمة هو القصد العام. وتعد جريمتي،الدخول والبقاء في منظومة المعالجة الآلية للمعطيات من الخطر،فالجريمتين تقعن بمجرد ارتكاب فعلي الدخول أو البقاء دون أن يتطلب المشرع في ذلك نتيجة إجرامية لهذا السلوك.

والإشكالية التي تثور في هذا الصدد، متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء ؟ يذهب رأي راجع من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول داخله بعد انتهاء الوقت المحدد،أي منذ علم الجاني أنه ليس له الحق الدخول ،فإذا دخل وظل ساكنا تظل الجريمة ،جريمة الدخول إلى النظام ،أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام [1]

واذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية النظام المعالجة الآلية للمعطيات بصورة مباشرة ،إلا أنها تحقق أيضا وبصورة غير مباشرة ،حماية المعطيات أو المعلومات بذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة ،كما يمكن أن تطبق على والاستخدام غير مشروع للبطاقات الممغنطة ،إما لسرقتها أو التزوير ثم استخدامها[2]

[1]– خثير مسعود ،مرجع سابق،ص 117

[2]– أمال قارة ،مرجع سابق،ص 111

ومن أمثلة جريمة الدخول بدون إذن ، ما حكمت به محكمة جنح ولاية باتنة ،حيث قضت في إحدى أحكامها ،بإدانة متهم لدخوله الغير مشروع لأحد الأنظمة المعلوماتية التابعة لمنظمة أمريكية ،اعتبرت أن ذلك فعل مجرم طبقا للمادة 394،مكرر من قانون العقوبات [1]

ومن بين صور إتلاف المستند الإلكتروني تذكر مايلي:

للمستند الالكتروني طبيعة خاصة وذاتية تختلف عن المستند الورقي فإذا كانت جريمة إتلاف المستندات الورقية تتم عن طريق إعدام هذه الورقة المكونة للمستند وذلك سواء كان عن طريق إحراقها أو سكب مواد كاوية أو مذيبة أو أي مادة أخرى تفقد المستند الورقي بياناته وبالتالي لا يكون حجة في إثبات ما خصص من أجله. فإن المستند الالكتروني يتم إتلافه بطرق أخرى وبالتالي لا يعد مكونا لجريمة إتلاف مستند الالكتروني الصورة المنسوخة على الورق من المستند أو المحرر الالكتروني الرسمي بالرغم من حجية هذه الورقة على الكافة إذا كانت مطابقة لأصل هذا المستند ما دام المستند الالكتروني الرسمي والتوقيع الالكتروني موجودين على الدعامة الالكترونية.

و يأخذ فعل الإتلاف عدة أشكال، فقد يتمثل في استخدام أسلوب القنبلة، أو إدخال فيروس للبرنامج أو سكب أحماض أو مواد كيماوية أو ملتهبة على الجهاز مما يؤدي إلى إتلاف البرامج والمعلومات.

أ- القنبلة المعلوماتية:

أ-1- <u>استخدام برنامج القنبلة المنطقية</u> (Logic bombe)

القنبلة المنطقية هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع، ومن ذلك مثلا إدخال تعليمات في برنامج نظام التشغيل وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرنامج المراد تنفيذه.[2]

ومن الأمثلة الواقعية التي استخدمت فيها القنبلة المنطقية نسوق ما يلي:

- تمكن خبير في نظم المعلومات في الدانمارك من وضع قنبلة منطقية في نظام إحدى الحاسبات أدت إلى محو أكثر من مائة برنامج. وقد تم أيضا محو النسخ الاحتياطية عند

[1]- طعباش أمين ،مرجع سابق ،ص 67 .

[2]- محمد أمين الرومي، مرجع سابق، ص.94

تشغيلها نظرا لانتقال آثار القنبلة إليها، وتم ضبط المجرم وحكم عليه القضاء الدانماركي بالحبس لمدة سبعة أشهر.

أ-2- استخدام برنامج القنبلة الزمنية (Time bombe)

وهي عكس القنبلة المنطقية فهي تنطلق وتنفجر في زمن وتاريخ محدد من السنة، فهي مرتبطة بالزمن فيمكن إدخالها في برنامج وضبطها لكي تنفجر مثلا في يوم 2006/03/18 الساعة 3:15 بتوقيت جرينتش وذلك بغرض تحويل نقود من حساب شخص معين لآخر، أو من أجل محو وشطب كل البيانات التي يحتويها مستند الكتروني موجود على دعامة الكترونية داخل أحد أجهزة الحاسب الآلي، ومن الأمثلة الواقعية التي استخدم فيها أسلوب القنبلة الزمنية ما يلي:

في فرنسا قام خبير في نظم المعلومات بدافع الانتقام على أثر فصله من المنشأة التي كان يعمل بها بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة، وترتب على ذلك إتلاف كل البيانات المتعلقة بهذه المنشأة.

أ-3- استخدام برنامج الدودة المعلوماتية:

يقصد برنامج الدودة أو تكنيك الدودة المعلوماتية أنه تكنيك فيروسي متمثل في برنامج له القدرة على تعطيل وايقاف نظام الحاسب بصورة كاملة، فهو ينسخ نفسه عدة مرات والدودة المعلوماتية تنتشر أساسا عبر خطوط التوصيلية الالكترونية وتصدر معلومات غير صحيحة وتؤدي في النهاية إلى انغلاق النظام فيحدث الإتلاف.[1]

ومن أمثلة برامج الدودة ، قضية (Regina v. Turner) التي قام فيها المتهم باستخدام شبكة اتصالات في مدينة تورنتو بكندا للوصول إلى أقراص ممغنطة بها معلومات خاصة بشركة أمريكية، حيث قام بتشفيرها مما أدى إلى إتلاف المعلومات ولذلك اعتبرت المحكمة العليا في أونتاريو أن عملية التشفير تعد حائلا دون استخدام الأقراص الممغنطة، وبالتالي وجوب تطبيق النص الخاص بجريمة الإتلاف.[2]

---

[1]- هدى حامد قشقوش، **جرائم الحاسب الالكتروني في التشريع المقارن**، دار النهضة العربية،القاهرة، ص.104

[2]-براهمي حنان، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، مرجع سابق، ص.56

أ-4- برنامج حصان طروادة:

سميت هذه البرامج هكذا كنية بالأسطورة القديمة عندما اختفى الجنود داخل الحصان الخشبي ليدخلوا مدينة طروادة ويهزموا جيشها، هكذا فإن أحصنة طروادة هي برامج خبيثة تختفي بداخل برامج مفيدة وغرضها الأساسي هو جمع المعلومات مثل الاسم وكلمة السر ثم يبعث بهذه المعلومات لصاحبه أثناء اتصال الجهاز بالشبكة والأسوأ من ذلك أنه يسمح للهاكر بتصفح الجهاز والتحكم في الملفات تحكما كاملا، وانتشر هذا النوع من البرامج في العصور الوسطى خاصة في أربع دول أوروبية وهي إنجلترا والنرويج والسويد والدانمارك.[1]

وهو من البرامج التجسسية والتي تقوم بعمل معين، يحدده الشخص الذي يصممه أو زرعه في جهاز الضحية، يمكنه الحصول على المعلومة التي يريدها.[2]

ب- إدخال الفيروس للبرنامج:

يهدف الفيروس المعلوماتي للإتلاف الالكتروني لعناصر المنظومة المعلوماتية عن طريق التلاعب ببياناتها من خلال اقتحام المواقع وتدميرها والعبث بمحتوياتها بإزالتها أو الاستيلاء عليها بهدف تعطيلها عن العمل لأطول فترة ممكنة أو تدميرها نهائيا.[3]

يقصد بفيروسات الحاسب الآلي أنها عبارة عن برامج خبيثة (malicious program) تتسلل إلى البرمجيات بحيث تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي. وتستخدم الفيروسات في أحد الغرضين: حمائي أو تخريبي.

ب- 1- الغرض الحمائي: ويكون ذلك لحماية البيانات والبرامج من خطر النسخ غير المشروع (المرخص به)، إذ ينشط الفيروس بمجرد النسخ ويدمر نظام الحاسب الذي يعمل عليه.

ب- 2- الغرض التخريبي: ويكون ذلك بهدف الدعابة أو الابتزاز، حيث يرمي واضع الفيروس للتخريب بهدف التخريب ذاته أو بهدف الحصول على منافع شخصية.[4]

---

[1]- طعباش أمين، مرجع سابق،ص.58

[2]- ضياء مصطفى عثمان،**السرقة الإلكترونية**،الطبعة الأولى،دار النفائس، الأردن ،ص.73

[3] -فتيحة حزام، **(النظام القانوني للفيروس المعلوماتي)**،مجلة حوليات جامعة الجزائر1، العدد 31، كلية الحقوق، جامعة أمحمد بوقرة بومرداس، (ب،ت) ص.320

[4]- محمد أمين الشوابكة، مرجع سابق، ص.238

كما أن الفيروس المعلوماتي يتمتع بخصائص ينفرد بها عن غيره من البرامج المتلفة والمخربة ويظهر ذلك في أن له القدرة على الانتشار والقدرة على التخفي بالإضافة إلى القدرة التدميرية والقدرة على الاختراق.[1]

فمن خلال هذا الفيروس يمكن لشخص في أمريكا مثلا أن ينقل لآلاف الأشخاص في الجزائر فيروسات عن طريق استخدام شبكة الانترنت قد تؤدي إلى إتلاف العديد من المستندات الالكترونية ومن أهم الوسائل التي تساعد على انتقال العدوى ما يلي:

- **البريد الالكتروني:** يمكن إدخال الفيروسات إلى جهاز الحاسب الآلي المخزن على دعامته مستندات الكترونية عن طريق البريد الالكتروني ويستخدم في ذلك فيروس عيد الميلاد.[2]

ويقوم هذا الفيروس بعرض بطاقة عيد الميلاد على الشاشة، وينتقل بسرعة على الشبكة مما يؤدي إلى توقف النظام فترة من الزمن، وقد استطاع المتخصصون عزله والقضاء عليه.[3]

- **الإرهاب:** تقوم الجماعات الإرهابية المنظمة باستخدام نظم الاتصالات الحديثة في تنفيذ مخططاتها الإرهابية عن بعد، كأن تقوم بتفجير طائرة أو مطار أو منشأة عسكرية أو غير ذلك من الأماكن الإستراتيجية عن بعد.

- **الإتلاف المتعمد بواسطة العاملين بالمؤسسة:**غالبا ما يتم التخريب واتلاف البرامج والمعلومات بواسطة العاملين على جهاز الحاسب الآلي وذلك إما أن يكون بباعث الانتقام أو إثبات المهارة والكفاءة.[4] وخاصة عندما تكون الجريمة من فئة (crackers) والذين يتمتعون بمستوى مهاري عالي يسمح لهم بالدخول واقتحام الأنظمة الحاسوبية بكل سهولة واقتدار رغم احتياطات الأمن المتعددة، إذ غالبا ما تكون جرائم التحويل والنسخ والإضافة للمعلومات على البرامج وتغيير محتواها من جانب هذه الفئة ضخمة.[5]

---

[1]–فتيحة حزام،مرجع سابق ص.325

[2]– محمد أمين الرومي، مرجع سابق، ص.97

[3]–فتيحة حزام، مرجع سابق، ص.329

[4]– محمد أمين الرومي، مرجع سابق، ص.98

[5]– يعيش تمام شوقي، **(محاضرات في مقياس جرائم المعلومات)**،**(غير منشورة)**، ألقيت على طلبة السنة الثانية ماستر جنائي، خلال السداسي الثالث، كلية الحقوق بسكرة، 2018/2017، ص.10

المطلب الثاني:

جرائم الاعتداء على سلامة المعطيات

لم يورد المشرع الجزائري نص خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة بداخل النظام وربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه .

والاعتداء العمدي على سلامة المعطيات يتخذ صورتين:

- جريمة التلاعب بالمعطيات
- جريمة التعامل بمعطيات غير مشروعة.

الفرع الأول: جريمة التلاعب بالمعطيات

نصت عليها المادة 394 مكرر 1 قانون العقوبات " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3)سنوات وبغرامة من 500,000 دج إلى 000 000 4 دج كل بطريق الغش المعطيات التي يتضمنها [1]

ما يستخلص من نص المادة أن هذه الجريمة تتم عن طريق التلاعب في المعطيات الموجهة للنظام المعلوماتي عن طريق عمليات الإدخال والتعديل والإزالة لمعطيات في إطار هذا النظام المعلوماتي، حيث ينصب في هذه المرحلة نشاط الجاني على تلاعب في المعلومات المدخلة للنظام المعلوماتي دون أن يحدث تلاعب في البرامج ،ولكن البرنامج يقوم بعمله وفقا لنظامه ، وهو الأمر الذي يؤدي في النهاية إلى إخراج معلومات مزورة وغير مطابقة لحقيقة المعلومات الواجب تخزينها في النظام المعلوماتي.[2]

وبالتالي هذه المادة تحتوي على ثلاثة صور : وهي

أولا: الإدخال

وذلك بإضافة أشياء أو معطيات جديدة على المستند الالكتروني تغير محتواه [3]

---

[1]– الأمر رقم 66–156،المتضمن قانون العقوبات سالف الذكر .

[2]– حسونة عبد الغني،مرجع سابق،ص07

[3]– طعباش أمين، مرجع سابق،ص 69

ثانيا: المحو

وذلك بإزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام،أو تحطيم تلك الدعامة ،أو نقل وتخزين من المعطيات إلى المنطقة الخاصة بالذاكرة[1]

ثالثا: التعديل

وذلك بحذف شيء من المحرر وا ضافة شيء أخر ويحدث هذا الفرض كثيرا في نطاق المعاملات الالكترونية خاصة في مجال المعاملات المالية ، حيث انه في ظل انتشار التحويل الالكتروني للأموال من بنك لأخر قد يلجا المجرم إلى احتجاز أمر الدفع الموجه من البنك إلى أخر وتحريف الرسالة بحيث يتم الدفع لحسابه هو ، أو ما يقوم به الجاني من استبدال رقم القيد الخاص بأحد الأشخاص [2] .

– لقد وردت الأفعال السابقة على سبيل الحصر فهذه الجريمة لا تتحقق إلا بغيرها ، فحتى ولو وقع اعتداء على معطيات المستند الالكتروني ، فلا يخضع لنص جريمة التلاعب ، لأنها تتحقق بإدخال أو محو وتغيير المعطيات .

إذن يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام ولا يشترط توافر القصد الجنائي الخاص ، إذ يكفي إن تتجه إرادة الجاني إلى الاعتداء على المعطيات والإدخال أو التعديل أو المحو،وان يعلم الجاني بأن نشاطه ذلك يترتب عليه التلاعب في المعطيات[3] وتجدر الإشارة إلى إن الحماية الجنائية تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية أي طالما كان يحتويها ذلك النظام وكانت تكون وحدة واحدة مع عناصره ويترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها وحتى ولو لفترة قصيرة كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام،ولا يشرط أن تقع أفعال الإدخال والمحو والتعديل المعطيات بطريق مباشرة،بل يمكن أن يتحقق ذلك بطريق غير مباشرسواء عن بعد أم بو اسطة شخص ثالث[4]

---

[1]– أمال قارة ،مرجع سابق،ص122

[2]– طعباش أمين ،مرجع سابق،ص69

[3]– صالح شنين ،مرجع سابق ،ص 114

[4]– آمال قارة،مرجع سابق،ص 121

من خلال ما سبق واستنادا إلى صلاحية انطباق الأحكام التقليدية لجريمة التزوير وكذا النصوص المستحدثة الخاصة بالمساس بالمعطيات الموجودة بنظم المعالجة الآلية على جريمة التزوير المعلوماتي ، نسجل ازدواجية في الجزاءات التي يمكن توقيعها على المخالفين المثبت إدانتهم،حيث تكشف المقارنة بين هذه الجزاءات أن المشرع من خلال الأحكام التقليدية لجريمة التزوير قام بإقرار جزاءات متباينة ومتناسبة مع طبيعة التزوير ، حيث رتب جزاءات كبيرة جدا تصل إلى السجن المؤبد عندما يتعلق الأمر بتزوير محررات رسمية من قبل قضاة أو موظفين عموميين ،في المقابل خفض العقوبة إلى 06 أشهر إلى 03 سنوات عندما يتعلق الأمر بتزوير الوثائق الإدارية والشهادات، وذلك على خلاف النصوص المستحدثة والمتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات حيث وحد المشرع من خلالها الجزاءات المطبقة على كل السلوكات المشكلة للتزوير حيث رتب عقوبة الحبس من 06أشهر إلى 03 سنوات وغرامة من من 500.000 د ج إلى 000 000 4 د ج .وهو ما يجعل القاضي الجزائي عند نظره في جريمة التزوير المعلوماتي، يتأرجح في معالجته لها بين تطبيق للجزاءات المقررة في الأحكام التقليدية لجريمة التزوير أو الجزاءات المقررة للمساس بأنظمة المعالجة الآلية للمعطيات وهو ما يؤكد ضرورة أن ينص المشرع الجزائري بشكل صريح على جريمة التزوير المعلوماتي .[1]

الفرع الثاني: جريمة التعامل في معطيات غير مشروعة

نصت المادة 394 مكرر 2 يعاقب بالحبس من شهرين(2) إلى ثلاث (3)سنوات وبغرامة من 1.000.000 د ج إلى 000 000 10 د ج كل من يقوم عمدا وعن طريق الغش بما يأتي :

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم

–حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم، و الملاحظ من نص المادة أن هذه الجريمة

[1]–حسونة عبد الغني ،مرجع سابق،ص 09

تفرق بين صورتين، تعامل في معطيات صالحة لارتكاب الجريمة والصور الثانية معطيات محصلة من الجريمة المعلوماتية .[1]

أولا : الركن المادي:

1- التعامل في معطيات صالحة لارتكاب الجريمة

أ- **التصميم** :وهي تتمثل في إخراج المعطيات إلى الوجود أي القيام بخلق وايجاد معطيات صالحة لارتكاب جريمة [2]

ب- البحث: المشرع يقصد بهذه العبارة البحث في كيفية تصميم هذه المعطيات واعدادها ،وليس مجرد البحث عن هذه المعطيات .

ج- التجميع: هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة دخول غير مصرح به أو جريمة التلاعب

د- التوفير: الوضع تحت التصرف أو العرض

هـ- النشر: والمقصود بالنشر هنا هو إذاعة معطيات محل الجريمة وتمكين الغير من الاطلاع عليها .

و- الاتجار: هو تقديم المعطيات للغير بمقابل.

2- التعامل في معطيات متحصله من الجريمة :

أ-**الحيازة:**تعرف في القانون الجنائي بأنها سيطرة واقعية وارادية للحائز على المنقول تخوله مكنة الانتفاع به أوتعديل كيانه أوتحطيمه أو نقله فهي إذا سيطرة إرادية للشخص على الشئ[3]

---

[1]- الأمر رقم 66-156،المتضمن قانون العقوبات سالف الذكر

[2]- محمد خليفة ،**الحماية الجنائية لمعطيات الحاسب الألي** ،(في القانون الجزائري والمقارن) دار الجامعة الجديدة،الإسكندرية،2007،ص200

[3]- المرجع نفسه، ص ص 201.202.203.

ب-الإفشاء:لا يتطلب المشرع الجزائري حدوث نتيجة معينة من إجراء الإفشاء ويختلف الإفشاء عن الحيازة في أن هذه الأخيرة تقوم الجريمة دون تقديمها للغير على خلاف الإفشاء فهو يفترض انتقال المعطيات المتحصلة من الجريمة من حيازة شخص لأخر

ج-**النشر:** يتحقق النشر مهما كانت وسيلة النشر وسواء تم النشر بمقابل أم بدون مقابل

د- الاستعمال: ويتحقق باستخدام المعطيات المتحصلة من الجرائم المعلوماتية لأي غرض كان [1]

ثانيا: الركن المعنوي

الاعتداء العمدي على المعطيات يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، وهي جريمة عمدية فقد أضاف المشرع في هذه الجريمة لفظ عمدا إلى جانب عن طريق الغش كذلك يتطلب في هذه الجريمة قد خاصا نص عليه المشرع وهو الغش أي نية الاستخدام بغرض الإساءة ويفترض لتوافر القصد الخاص ثبوت توافر القصد العام [2]

كذالك نص المشرع الجزائري على عقوبات تكميلية إلى جانب العقوبات الأصلية المذكورة سالفا ولقد نصت المادة 394 مكرر6 وهي المصادرة واغلاق المواقع بالإضافة إلى إغلاق المحل أو المكان الاستغلال لما بالنسبة للشخص المعنوي فيعاقب بغرامة مالية تعادل خمس (5)مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي حسب ن المادة 394 مكرر 4

وبالتالي نلاحظ أن المشرع الجزائري يحمي المستند الالكتروني سواء أكان داخل النظام المعلوماتي أو خارجه فالمشرع يقصد بالمعطيات المخزنة تلك التي تكون على دعامة خارجية فا المشرع يقصد بالمعطيات المخزنة تلك التي تكون على دعامة خارجية كالأقراص أو تكون مخزنة داخل النظام ذاته في الذاكرة مثلا أما المعطيات المعالجة هي التي أصبحت من النظام أي أصبحت عبارة عن إشارة أو رموز تمثل معلومات معالجة آليا .

وللإشارة لقد نصت المادة 37 من قانون رقم 18-05المؤرخ في 10مايو 2018المتعلق بالتجارة الإلكترونية ،على أنه :دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به ،يعاقب بغرامة من 200.000 دج إلى 1.000.000 كل من يعرض

[1]- صالح شنين ،مرجع سابق،،ص118

[2]- طعباش امين،مرجع سابق، ص 47

للبيع ،أو يبيع عن طريق الاتصال الإلكتروني ،المنتجات أو الخدمات المذكورة في المادة 3 من هذا القانون .

ويمكن للقاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح بين شهر(1)إلى(6) ستة أشهر.

كما نص في المادة 38من نفس القانون على أنه دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به،يعاقب بغرامة من 500.000د ج إلى 2.000.000 د ج كل من يخالف أحكام المادة 5 من هذا القانون والتي تنص على أنه تمنع كل معاملة عن طريق الاتصالات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به ،وكذا كل المنتجات أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن الوطني[1]

لكن ما تجدر الإشارة إليه أن المشرع الجزائري اغفل استحداث نص يتعلق بالاعتداء على المستند الالكتروني في حد ذاته .

وربما يكون مرد ذلك أن المشرع الجزائري باستحداثه للنصوص التي تجرم الاعتداء على المعطيات المعالجة أليا سواء كانت داخل النظام المعلوماتي أو خارجه يكون بذلك قد تناول جانبا من جريمة الاعتداء [2]على المستند الالكتروني.

هذا بالنسبة للتشريع الجزائري إما بالنسبة للتشريعات الأوروبية فنجد أن المشرع الفرنسي اهتم بالمستندات الاليكترونية حيث انشأ هيئة عامة تسمى هيئة المعلومات والحريات العامة وحضر على الكافة جمع المعلومات أو حفظها أو نقلها أو الاطلاع عليها أو واذاعتها أو إفشائها للغير بدون الحصول على الترخيص المطلوب أما بالنسبة للوضع في تشريعات العربية نجد أن التشريع الامارتي نص ف (المادة 31) على انه يعاقب كل شخص تمكن بموجب أي سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في مستندات اليكترونية ،أو أفشى متعمدا بالحبس والغرامة التي لا تتجاوز مائة ألف درهم أو بإحدى هاتين العقوبتين [3]

وتكون العقوبة الغرامة التي لا تتجاوز مائة درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات .

---

[1] - القانون رقم 18-05 المتعلق بالتجارة الإلكترونية ، سالف الذكر،ص ص 05-09

[2] - طعباش أمين ،مرجع سابق، ص 44

[3] - محمد أمين الرومي ،مرجع سابق،ص ص 123،124

إن المستندات الالكترونية يجب أن تحاط بالسرية اللازمة والكافية وذلك من أجل عدم انتشار و اذاعة ماتحتويه من معلومات قد تكون ذات الشأن ،فقد يؤدي الدخول أو البقاء مثلا إلى المعلومات التي يحتويها المستند الالكتروني إلى تحقيق منافسة غير مشروعة بين المشروعات كذالك قد تكون هذه المستندات تحتوى على معلومات متعلقه بأمن الدولة وسلامتها لذلك تحظر معظم التشريعات المتعلقة بالمعاملات الالكترونية في القوانين المقارنة.[1] في النص على عدم الدخول أو لبقاء الغير مشروع في المعلومات التي تحتويها المستندات الإلكترونية ،ورغم أن المشرع الجزائري قد نص في هذه الجريمة على تجريمه كل من دخل أو بقى عن طريق الغش أو حذف أو غير لكل أو جزء من المنظومة المعلوماتية إلا انه غفل على النص على تقرير حماية لسرية المستندات الالكترونية بشكل صريح

الفرع الثالث :القواعد المشتركة بين كل الجرائم :

تعتبر جرائم المساس بالمعطيات من الجرائم ذات القواعد المشتركة حيث:

– نصت المادة 394 مكرر 3 من قانون العقوبات على ظرف مشدد في حالة ما إذا استهدفت جرائم المساس بأنظمة المعالجة الآلية للمعطيات الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام ، حيث تضاعف العقوبات ، ودون الإخلال بتطبيق عقوبات اشد.

– نصت المادة 394 مكرر 4 من قانون العقوبات، يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد أقصى للغرامة المقررة للشخص الطبيعي [2]

–المشاركة في الجمعية أشرار طبقا للمادة 394 مكرر 5 من قانون العقوبات وتكون مقررة لكل من شارك في المجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم الغش المعلوماتي وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقرر للجريمة ذاتها [3] .

[1]– محمد أمين الرومي ،مرجع سابق ،ص ص122،123

[2]– الأمر رقم 66–156،المتضمن قانون العقوبات سالف الذكر.

[3]– بومعيزة جابر ،مرجع سابق،ص 138

– المصادرة مع الاحتفاظ بحقوق الغير حسن النية، حيث يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع الإغلاق المواقع التي تكون محلا للجريمة، علاوة على إغلاق المحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم مالك المحل أو المكان.[1] نص المادة 394 مكرر6.

– نص المادة (394) مكرر 7: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

المطلب الثالث:

الجرائم المنصوص عليها في قانون التوقيع والتصديق الالكتروني

سعى المشرع الجزائري إلى توفير حماية جزائية موضوعية للمستند الإلكتروني من خلال العديد من النصوص العقابية المتفرقة التقليدية منها والمستحدثة كما سبق وأن عرضنا في دراستنا، ولقد عمل أيضا على توفير حماية جزائية موضوعية للمستند الإلكتروني من خلال إصدار قانون التوقيع والتصديق الإلكتروني، والذي بدورها نص من خلال على أحكام جزائية خاصة بالجرائم الماسة بالتوقيع والتصديق الإلكترونيين. وسنتناول في هذا المطلب تعريف التوقيع الإلكتروني (الفرع الأول) جرائم التوقيع الإلكتروني (الفرع الثاني).

الفرع الأول: تعريف التوقيع الالكتروني

عرفه بعض الفقهاء المصريين بأنه "كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطا ارتباطا وثيقا بالتصرف القانوني ، ويسمح بتمييز صاحبها وتحديد هويته ، ويتم دون غموض عن رضائه بهذا التصرف . [2]

ويقترن بتعاقد،أو مستند أو محرر، ويستخدمه الشخص قاصدا التوقيع على المحرر(المستند)[3]

---

[1]– احسن بوسقيعة ،**الوجيز في القانون الجزائري الخاص** ، الجزء الأول دار هومة ،الجزائر ، 2008، ص 448 .

[2]– صالح شنين ، مرجع سابق ، ص 50 .

[3]– لالوش راضية ،(**امن التوقيع الالكتروني**)، مذكرة ماجستير ،تخصص قانون دولي للأعمال ،كلية الحقوق والعلوم السياسية،جامعة مو لود معمري ،تيزي وزو،2012 ، ص 15 .

كما اعترف المشرع الجزائري المشرع الجزائري بالتوقيع الالكتروني وهذا في نص المادة 2 من القانون رقم 15-04 حيث عرفه بأنه عبارة عن بيانات في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق.

وعرفت شهادة التصديق الالكتروني بأنها. وثيقة في شكل الكتروني تثبت الصلة بين البيانات التحقق من التوقيع الالكتروني والموقع.

كذلك يتخذ التوقيع الالكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشاءه

وتتمثل أهم صور التوقيع الإلكتروني في التوقيع الرقمي، والتوقيع البيومتري، والتوقيع باستخدام القلم الالكتروني .[1]

الفرع الثاني:جرائم التوقيع الالكتروني

نص المشرع المصري على جرائم التوقيع الالكتروني في المادتين21 و23 من قانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني حيث نصت المادة 21 من هذا القانون على إن بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى جهة المرخص لها بإصدار شهادات التصديق الالكترونية سرية، ولا يجوز لمن قدمت إليه أو بحكم علمه إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من اجله

ويتضح من نص المادة 21 إن المشرع المصري يجرم إفشاء بيانات التوقيع الالكتروني وجريمة استخدام هذه البيانات في غير الغرض المخصص لها.

كذلك نصت المادة 23 من القانون 15سنة 2004 على انه " مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في قانون أخر يعاقب بالحبس وبغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز مئة ألف جنيه ، أو بإحدى هاتين العقوبتين كل من :

[1]- صالح شنين ،مرجع سابق، ص ص 63،66

– أصدر شهادة تصديق دون الحصول على ترخيص .

– اتلف أو عيب توقيعا أو وسيطا أو محرر الكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو تعديل أو بأي طريق أخر .

–استعمل توقيعا وسيطا أو محرر الكترونيا معيبا أو مزورا مع علمه ذلك .

– توصل بأي وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر الكتروني أو اخترق أو اعترضه أو عطله عن أداء وظيفته وفي حالة العود تزداد بمقدار مثل العقوبة المقررة لهذه الجرائم .

ولقد جرم المشرع الجزائري بدوره العديد من الجرائم الماسة بالتوقيع والتصديق الإلكترونيين وذلك في المواد من 66 إلى 75 من القانون رقم 15–04 السابق ذكره، والتي تتمثل في[1]:

–الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة (م66).

–إخلال مؤدي خدمات التصديق الإلكتروني بالتزامه بإعلام السلطة الاقتصادية بالتوقف عن نشاطه (م67).

– حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير (م68).

–إخلال أي شخص بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة (م69).

– إخلال مؤدي خدمات التصديق الإلكتروني بالتزامه في الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة (م70).

– إخلال مؤدي خدمات التصديق الإلكتروني بالأحكام التالية: جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة، جمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، وعدم استعمال هذه البيانات لأغراض أخرى (م71).

– أداء كل شخص لخدمات التصديق الإلكتروني للجمهور دون ترخيص أو استئناف ومواصلة مؤدي خدمات التصديق الإلكتروني نشاطه بالرغم من سحب ترخيصه (م72).

[1]– القانون رقم 04–15،المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين ،سالف الذكر.

– كشف كل شخص مكلف بالتدقيق لمعلومات سرية اطلع عليها أثناء قيامه بالتدقيق (م73).

– استعمال كل شخص لشهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها (م74).

و عليه فإن أهم الصور الأكثر عرضة للتزوير نجد التوقيع بالرقم السري وكذلك التوقيع الرقمي:

أولا: تزوير التوقيع الإلكتروني الذي يتم بالرقم السري

أكثر تطبيقات هذه الصورة وأهمها بطاقات الصرف البنكي بأنواعها المختلفة ويعد أهم صور الاستخدام غير المشروع للبطاقات البنكية كما يلي:

1– استخدام بطاقات بنكية مزيفة جزئيا أو مزيفة كليا .

2– استخدام بطاقات بنكية مسروقة .

3– استخدام بطاقات بنكية صحيحة صدرت بطريقة غير مشروعة .

قد يكون تزوير البطاقة الائتمانية ذاتها كليا أو جزئيا،حيث يتم التزوير الكلي باصطناع البطاقة بالكامل وتقليد ماعليها من كتابات وحروف وعلامات وأشرطة،أو من خلال بيانات بطاقة صحيحة يتم الحصول عليها بتصويرها فوتوغرافيا بواسطة التاجر بعيدا عن أعين العميل،وقد يكون بتغيير بعض بيانات البطاقة كنزع الشريط الممغنط الأصلي ووضع الشريط الخاص بالفاعل القائم بعملية التزوير.[1]

ثانيا: تزوير التوقيع الرقمي

التوقيع الرقمي يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات ...إلخ، حيث لا يمكن تقليدها إنما يمكن استعمالها دون علم مالكها،عن طريق الحصول على منظومة التوقيع الإلكتروني بطريق التجسس الإلكتروني أو الدخول غير المشروع، فالتوقيع بهذه الطريقة يعد سليما إلا أنه استخدم من غير صاحبه، وعليه يتم الكشف

[1]– لالوش راضية،مرجع سابق ،ص ص 145،147

عن التوقيع الرقمي المزور بإثبات أنه لم يصدر من مالك المنظومة، وانما من شخص آخر،قام بسرقتها .

ثالثا: تزوير شهادة التصديق

توجد جهات يرخص لها سواء كانت شخصية أو اعتبارية باعتماد التوقيعات الإلكترونية بشهادات مصدق عليها منهم ،وهذه الشهادات يترتب عليها آثارا قانونية تتمثل في إنشاء التزامات واثبات حقوق بالنسبة لطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما ،لذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته،كذلك هذه الشهادات تنشأ وتعالج وتسلم وتحفظ بطريق إلكتروني وأنها أصلا عبارة عن بيانات ومعلومات إلكترونية تخزن عبر وسيط إلكتروني (المستند الإلكتروني) فقد يتمكن أحدهم من اختراق هذا الوسيط ويقوم بتقليد أو تزوير أو نشر شهادة التصديق المزورة، هنا تقوم جريمة تزوير شهادة التصديق الإلكتروني.[1]

[1]- لالوش راضية،مرجع سابق،ص ص 150،151

الفصل الثاني
الحماية الجزائية الإجرائية للمستند الإلكتروني

تعد متابعة الجريمة المعلوماتية بصفة عامة و متابعة جرائم المستند الالكتروني بصفة خاصة ، من أهم التحديات التي تواجه رجال الضبطية القضائية بالنظر إلى طبيعة الجريمة المعلوماتية و هذا من حيث أنها تتعلق بمحل غير مادي بالإضافة إلى صعوبة دور الشرطة و مختلف الأجهزة الأمنية في مراقبتها و منع حدوثها و كذا التحري عن مرتكبيها .

كما أن المجرم المعلوماتي ،عادة ما يكون ذا خبرة و ذكاء و دهاء خارق قد لا يستطيع المحقق الجنائي العادي التعامل معه ، كما أن الأدلة المتحصل عليها من مسرح الجريمة تختلف عن الأدلة التقليدية .

وعليه سنتطرق في هذا الفصل إلى أهم القواعد الإجرائية التي جاء بها المشرع الجزائري لمواجهة هذه الأنماط المستجدة من الجرائم.

حيث سوف نخصص في المبحث الأول لإجراءات التحري و التحقيق في الجرائم الماسة بالمستند الالكتروني، والمبحث الثاني لإجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني.

المبحث الأول

إجراءات التحري و التحقيق في الجرائم الماسة بالمستند الالكتروني

لقد عمل المشرع الجزائري على تطوير أساليب التحري والتحقيق فيما يخص الجرائم المعلوماتية لتتلاءمع خصوصية هذه الجرائم ،وذلك من خلال تعديل قانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006،واصدار قانون رقم 09-04 المؤرخ في 5 أوت سنة 2009،والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

إن التحقيق والتحري وجمع الأدلة في الجريمة المعلوماتية له طابع خاص، مما يتوجب على السلطة المختصة بالتحري و التحقيق، الإلمام الواسع بمعطيات الحاسوب و طبيعته، ويتعين على المحقق في هذا المجال أن تتوفر فيه شروطا خاصة حتى يتمكن من التحقق على أكمل وجه ، لذا وجب أن تتم هذه الإجراءات بصورة صحيحة و قانونية لأن اللجوء إلى الطرق الغير مشرو عةيؤدي إلى بطلان هذه الإجراءات.

لذلك سنخصص هذا المبحث للحديث عن أجهزة الضبط القضائي المختصة (المطلب الأول) إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بالمستند الإلكتروني (المطلب الثاني)وأخيرا نتطرق إلى إجراءات التحري والتحقيق الحديثة في الجرائم الماسة بالمستند الإلكتروني (المطلب الثالث).

المطلب الأول :

أجهزة الضبط القضائي المختصة بمكافحة الجرائم الماسة بالمستند الالكتروني واختصاصاتها

إن التحقيق في الجريمة المعلوماتية له طابع خاص ،يختلف عن ماهو عليه الحال في الجرائم التقليدية و بالتالي سنتطرق في هذا المطلب إلى الأجهزة المختصة وقواعد الاختصاصفي مجال مكافحة جرائم الماسة بالمستند الإلكتروني.

الفرع الأول: الأجهزة المختصةبمكافحة جرائم الماسة بالمستند الإلكتروني:

لقد عزز المشرع الجزائري اختصاصات الضبطية القضائية، وذلك بموجب التعديل الأخير لقانون الإجراءات الجزائية تحت رقم 22/06 المؤرخ في 2016/12/20، بوضع أساليب وآليات جديدة للتحري والتحقيق في بعض الجرائم الواردة على سبيل الحصر،نظرا لما تحتويه من خطورة على المجتمع [1]

حيث استحدث المشرع الجزائري**الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها** بموجب القانون رقم 09-04 المتعلق بالوقاية من جرائم الاتصال و المعلومات و مكافحتها ، في المواد 13 و14 من هذا القانون .

حيث نصت المادة 14 من هذا القانون: على أن" تتولى الهيئة المذكورة في المادة 13، المهام التالية :

أ)- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكولو جيا الإعلام والاتصال ومكافحتها .

ب)- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية

ج)- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكب هذه الجرائم وتحديد مكان تواجدهم .[2]

[1]- شرف الدين وردة **(مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية،في التشريع الجزائري)** مجلة المفكر، العدد الخامس عشر، كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر بسكرة،15 جوان 2017،ص 541

[2]-ناني لحسن ،**التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية** (بين النصوص التشريعية والخصوصية التقنية)دار النشر الجامعي الجديد،تلمسان،الجزائر،2017،ص 83

وقد حدد المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر سنة 2015، تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها[1].

كما أنشئت الجزائر العديد من المراكز المتخصصة بمكافحه جرائم الانترنت وهذا على مستوى الدرك الوطني والأمن الوطني من بينها :

- **مركز الوقاية من الجرائم الإعلام وعلم الإجرام للدرك الوطني CPLCIC / GN**
- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني INCC / GN**
- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني SCLCTIC** [2]

الفرع الثاني: قواعد الاختصاص في مجال مكافحة الجرائم الماسة بالمستند الإلكتروني

فالبنسبة للإختصاص المحلي **للضبطية القضائية** في مجال جرائم الماسة بأنظمة المعالجة الآلية للمعطيات ومنها جرائم الماسة بالمستند الإلكتروني، فحسب المادة 7/16 ق ع[3]،يكون المشرع الجزائري قد منح لضباط الشرطة القضائية على اختلاف الجهات التي ينتمون إليها اختصاصا وطنيا لمباشرة صلاحياتهم في البحث والتحري، ويشترط لتمديد هذا اختصاص :

- العمل تحت إشراف النائب العام لدى المجلس القضائي المختص
- إعلام وكيل الجمهورية المختص إقليميا.

أما بالنسبة للاختصاص الإقليمي **للهيئة الوطنية المكلفة بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال**، وفيما يخص فإنه لم يحدده القانون رقم 09 -04 رغم أن

---

[1]-الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 53، الصادرة في 8 أكتوبر سنة 2015، ص 16 وما بعدها.

[2]- عز الدين عز الدين ، **(الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها)** ، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية ، كلية الحقوق والعلوم السياسية،جامعة بسكرة .16 و17نوفمبر 2015 الجزائر، 2015، ص 11

[3]- المعدلة بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006، المعدلقانون الإجراءات الجزائية، السابق الذكر.

نص المادة 18 الفقرة 2 من المرسوم الرئاسي 15-261 السابق الذكر، نصت على ضباط الشرطة المنتمين لهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته .وهذا بنصها " ..... كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية الاستعلام والأمن والدرك الوطني والأمن الوطني،يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل ، والدفاع الوطني ، والداخلية ....." والأرجح من عدم النص على النص على الاختصاص الإقليمي أن المرسوم الرئاسي 15-261 اختصاص شامل لكافة التراب الوطني

ولقد نصت المادة 36 من قانون رقم 18-05 المؤرخ في 10 مايو سنة 2018، المتعلق بالتجارة[1] وفيما يخص الجرائم الماسة بالعقد الإلكتروني باعتباره من صور السندات الإلكترونية، وكمتطلب من متطلبات التجارة الإلكترونية، على أنه: زيادة على ضباط وأعوان الشرطة القضائية المنصوص عليهم بموجب قانون الإجراءات الجزائية، يؤهل لمعاينة مخالفات أحكام هذا القانون، **الأعوان المنتمون للأسلاك الخاصة بالرقابة التابعون للإدارات المكلفة بالتجارة،** لا سيما تلك المطبقة على الممارسات التجارية وعلى شروط ممارسة الأنشطة التجارية وعلى حماية المستهلك وقمع الغش. تتم كيفيات الرقابة ومعاينة المخالفات المنصوص عليها في هذا القانون حسب نفس الأشكال المحددة في التشريع والتنظيم المعمول بهما، ويجب على المورد الإلكتروني السماح للأعوان المؤهلين لمعاينة المخالفات ،بالولوج بحرية إلى تواريخ المعاملات التجارية .

أما **بالنسبة للنيابة العامة،** الأصل يتحدد الاختصاص المحلي لها، وفقا للمادة 37 [2] من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ومحل إقامة احد الأشخاص المشتبه في مساهمتهم أو بالمكان الذي تم في دائرته القبض، وبالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى ذلك .

و نفس الشيء بالنسبة **إلى القاضي التحقيق،** ففيما يخص الاختصاص المحلي فقد نظمته المادة 40 من قانون الإجراءات الجزئية المذكورة آنفا.

---

[1] -القانون رقم 18-05 المتعلق بالتجارة الإلكترونية،سالف الذكر ،ص09

[2] - الأمر رقم 155-66 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية ،المعدل والمتمم بالأمر رقم 02-15 المؤرخ في 23 جويلية 2015،(ج ر،رقم 40،الصادرة بتاريخ 23 جويلية 2015).

وبما أن جرائم الماسة بالمستند الإلكتروني تعتبر من الجرائم المساس بأنظمة المعالجة الآلية للمعطيات، ولما كانت هذه الأخيرة قد ترتكب في مكان معين وتكون أثارها في مكان أخر فإن المشرع الجزائري بموجب المادة 37 الفقرة 2 من ق.ا.ج، المستحدثة بالمرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر سنة 2006، يتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق بالقطب الجزائي المتخصص إلى الدائرة الاختصاص المحاكم الأخرى المحددة في التنظيم[1].

ويتعين على ضباط الشرطة القضائية طبقا للمادة 40 مكر 1 من قانون الإجراءات الجزائية الجزائري أن يخبر وكيل الجمهورية لدى المحكمة الكائن لها الجريمة ويبلغونه بأصل ونسختين من إجراءات البحث. يرسل هذا الأخير فورا النسخة الثانية إلى نائب العام لدى المجلس القضائي التابعة له محكمة المختصة طبقا للمادة 40 مكرر 1 من ق.ا.ج[2].

وبموجب الأمر رقم 17-07 المعدل والمتمم لقانون الإجراءات الجزائية نصت المادة 12 منه : على أنه يحدد النائب العام التوجيهات العامة اللازمة للشرطة القضائية لتنفيذ السياسة الجزائية بدائرة اختصاص المجلس القضائي .[3]

المطلب الثاني:

إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بالمستند الالكتروني.

من خلال هذا المطلب سنتطرق إلى أهم القواعد الإجرائية التقليدية المستنبطة من الوقائع أو الأشياء (الفرع الأول)، والمستنبطة من تصريحات الأشخاص (الفرع الثاني)، والتي نص عليها المشرع الجزائري في قنون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وقانون الإجراءات الجزئية، المخصصة في البحث والتحقيق عن الجرائم الماسة بالمستند الإلكتروني

---

[1]-أنظر الجريدة الرسمية للجمهورية الجزائية الديمقراطية الشعبية، العدد 63، الصادرة في 8 أكتوبر سنة 2006، ص 29 وما بعدها.

[2]- ناني لحسن ،مرجع السابق ص ص 56، 57 .

[3]-القانون رقم 07/17،المؤرخ في 27 مارس،سنة 2017،يعدل ويتمم الأمر رقم 66-155،المؤرخ في 8 يونيو 1966والمتضمن قانون الإجراءات الجزائية،(ج ر،العدد 20)الصادرة في 29 مارس،سنة 2017.

الفرع الأول إجراءات التحري والتحقيق التقليدية المستنبطة من الوقائع أو الأشياء .

سوف نعرج في هذا الفرع الأول على أسلوب الانتقال والمعاينة ونبحث في خصوصيات التفتيش في البيئة الرقمية ونبحث في خصوصيات الحجز والضبط

أولا :الانتقال والمعاينة

عرفها مجموعة من الفقه بأنها "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة[1].

هذا بالنسبة الانتقال للمعاينة في الحالة الجرائم في صورته التقليدية، أما الانتقال والمعاينة في الجريمة المعلوماتية فيجب التمييز دائما بين حالتين أساسيتين

الحالة الأولى :المعاينة في حالة الجرائم الواقعة على المكونات المادية للحاسب الآلي كجرائم الاعتداء على الأشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومفاتيح التشغيل الأقراص وغيرها من مكونات الكومبيوتر ذات طابع المادي الملموس .

الحالة الثانية: المعاينة في الحالة الجرائم الواقعة على مكونات الغير مادية أو بواسطتها و تتمثل في تلك الجرائم الواقعة على البرامج الكمبيوتر وبياناته أو بواسطتها ، وهنا تثور الصعوبات تحول دون فعالية المعاينة من بين هاته الصعوبات نذكر :

- قلة الآثار المادية المتلفة من الجرائم التي تقع على برامج والحاسوب والشبكات
- إمكانية حدوث تغيير أو تلف أو تلفيق أو عبث بالآثار المادية أو زوال بعضها .
- نقص الدراية ومعرفة المحقق بالجوانب الفنية والتقنية لاستخدام شبكة الانترنت والحاسوب.[2]

وتكون المعاينة بعد الانتهاء من جمع المعلومات اللازمة عن الحادث حيث يبدأ المحقق بتحديد خطة العمل المناسبة وطريق العمل اللازم للتحري ، وهذا بمجرد انتهائه من رسمه

---

[1]– شرف الدين وردة،**الإثبات الجنائي بالأدلة الإلكترونية** (راسة مقارنة)أطروحة دكتوراه علوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية ،كلية الحقوق والعلوم السياسية،جامعة محمد خيضر بسكرة،2017 ص 182 .

[2]– المرجع نفسه .ص ص 183،184 .

الصورة الأولية للواقعة قصد الانتقال للمعاينة ، فعلى المحقق الأخذ بعين الاعتبار حجم ونوع الحادث لتعيين فريق التحقيق وكفاءته ، الظروف المحيطية بالحادث.[1]

واذا تمت المعاينة بعد وقوع الجريمة في المجال الإلكتروني ،فيجب مراعاة مايلي:

1) تصوير لحاسب والأجهزة الظرفية المتصلة به ،على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2) العناية بملاحظة الطريقة التي تم بها إعداد النظام .

3) ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر ،فيما بعد على المحكمة .

4) عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة .

5) التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة و فحصها ،ويرفع من عليها من البصمات ذات الصلة بالجريمة .

6) التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة ،لرفع ومضاهاة ما قد يوجد عليها من بصمات .

7) قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العالية والخبرة الفنية في مجال الحاسبات . [2]

وكذلك يختلف الانتقال والمعاينة في العالم الافتراضي عن الكيفية المتبعة لمعاينة مسرح الجريمة التقليدية .حيث يمكن لرجل الضبطية العدلية الانتقال إلى مسرح الجريمة في العالم

---

[1]– ناني لحسن ،مرجع سابق ، ص 71 .

[2]– محمد أبو العلا عقيدة ، **(التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية)**،بحث مقدم لأعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ،في 26 نيسان 2003،كلية الحقوق ،جامعة عين الشمس ،الإمارات 2003،ص 11

الافتراضي، من خلال الحاسوب الموجود في مكتبه ، أو عبر مقهى الانترنت ، أو اللجوء إلى مقر مزود الخدمة ، الذي يعتبر أحسن الأماكن الإمكانيةإجراء المعاينة.[1]

ثانيا : التفتيش

يعرف التفتيش على انه إجراء من الإجراءات التحقيق ، بهدف إلى جمع الأدلة ، وأما الغموض عن الجريمة ونسبتها إلى منهم معين

ويمكن تعريف تفتيش نظم الحاسوب والانترنت بأنه " البحث في مستودع سر المتهم عن الأشياء مادية أو معنوية تفيد كشف الحقيقة ونسبتها إلية [2]

وقد عرّف المجلس الأوروبي هذا النوعي من التفتيش، بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني[3]

ثالثا: الضبط

يعرف الضبط في البيئة الالكترونية على أنه وضع اليد على الدعائم المادية المخزنة فيها البيانات الكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت وتفيد في كشف الحقيقة عنها وعن مركبتها ، كما يعرف أيضا بأنه استخدم البرامج الهامة من اجل الولوج للبيئات المو اد ضبطها إلى جانب وضع اليد على تلك الدعائم المادية[4].

ونظرا لكون الضبط محله في مجال الجرائم الالكترونية .هو البيانات المعالجة الكترونيا .فقد ثار التساؤل حول :

- هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط. الذي يعني كمارأينا وضع اليد على شيء مادي ملموس؟

- انقسم القفة إلى اتجاهين عند الإجابة عن هذا التساؤل :

- فيرى البعض أن بيانات الحاسب لا تصلح لأن تكون محلا لضبط هذا الانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس

---

[1]– شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع السابق ص 186 .

[2]– المرجع نفسه ص 195 .

[3]– علي عدنان الفيل ،**إجرءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية** ،(راسة مقارنة)،المكتب الجامعي الحديث،(د،ب،ن) ،ص 39 .

[4]– الهام بن خليفة ،مرجع سابق ، ص 291 .

ويرى الاتجاه الثاني أن البيانات المعالجة الكترونيا ماهي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ وتخزين على وسائط مادية [1]

وتتمثل شروطالإجراء الحجز فيما يلي :

- يجب على السلطة التي تقوم بالحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.
- إذا استحال إجراء الحجز وفقا كما هو منصوص عليه في القانوني لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية .
- على السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة [2]
- تامين مسرح الجريمة الرقمية من العبث .
- ضبط الدعائم الأصلية للمعطيات وعدم الاقتصار على نسخها
- عدم ثني القرص لأنه يؤدي إلى تلفه وفقدان المعطيات المسجلة عليه .
- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة مع الإشارة إلىدرجة الحرارة المسموح بهافتتراوح ما بين4 إلى 32° م ، أما بالنسبة للرطوبة المسموح بها فتتراوح ما بين 20 إلى 80 ،وبمراعاة هذه النسب يمكن أن تصل مدة التخزين °لهذهالأقراص والأشرطة إلى ثلاثة سنوات
- عدم تعريض القرص للأتربة وذ ات الغبار والدخان
- عدم الضغط عليه بوضع أشياء تقيله عليه [3].

رابعا- إجراءات التفتيش والضبط في جرائم الماسة بالمستند الإلكتروني وفقا للتشريع الجزائري:

أ- قواعد التفتيش والضبط المتبعة في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفقا لقانون الإجراءات الجزائية:

[1]- محمد أبو العلا عقيدة ،مرجع سابق ، ص 16 .

[2]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق، ص 243

[3]- الهام بن خليفة ،مرجع سابق،ص 294

للوقوف على الأحكام المقررة للتفتيش في الجرائم المعلوماتية، لا بد من التفرقة بين قواعد التفتيش والضبط في حالة الجناية أو الجنحة المتلبس بها، وقواعد التفتيش والضبط في حال التحقيق الابتدائي، ثم على قواعد التفتيش والضبط في حال التحقيق بمعرفة قاضي التحقيق وفقا لما يلي:

أ/1- تفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالات التلبس بالجريمة[1]: ويكون ذلك وفقا للقواعد التالية:

أ- 1- 1- الحصول على إذن مسبق من قبل السلطة القضائية المختصة:

نصت المادة 44 : لا يجوز لضابط 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.

ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون.

يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها واجراء الحجز فيها، وذلك تحت طائلة البطلان.

تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون.

---

[1]- تنص المادة 41 إ ج على أنه (توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها.

كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى افتراض مساهمته في الجناية أو الجنحة.

وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية لإثباتها). أنظر: أمر رقم 66-155 مؤرخ في 8 يونيو سنة 1966يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 662.

إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا بطلان الإجراءات العارضة[1].

أ-1-2- حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

يخضع التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 3/47 إ ج، لقواعد خاصة تختلف عن القواعد العامة المقررة في البندين 1 و 2 من المادة 45 إ ج ، وتختلف هذه القواعد حسب حالتين[2]:

الحالة الأولى:إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45إ ج لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات بالشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش بمسكنه وكذلك الأمر إذا حصل التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالجريمة.

---

[1]- الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 6.

[2]- تنص المادة 45 على أنه : (تتم عمليات التفتيش التي تجرى طبقا للمادة 44 أعلاه على الوجه الآتي:

(1- إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له.واذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.

-إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش، وان تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة.

ولضابط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى أعلاه الحق في الاطلاع على الأوراق أو المستندات قبل حجزها)، أنظر: قانون رقم: 06-22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 6؛ أنظر كذلك: نجيمي جمال،قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، دار هومة، الجزائر، 2015، ص 419 وما بعدها.

الحالة الثانية: أصبح ضابط الشرطة القضائية إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبس بها أو تحقيق متعلق بإحدى أنواع الجرائم السالفة الذكر، يمكنه بموجب المادة 47مكرر المستحدثة في قانون الإجراءات الجزائية أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر وأن الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو لاحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله.

ولضابط الشرطة القضائية وحده مع الأشخاص الحاضرين عملية التفتيش الحق في الاطلاع على الأوراق أو المستندات قبل حجزها، غير أنه عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر، وتغلق الأشياء أو المستندات المحجوزة ويختم عليها إذا أمكن ذلك، فإذا تعذرت الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق ويختم عليه بختمه. ويحرر جرد الأشياء والمستندات المحجوزة (م 5/4/3/2/45 -6/45- 48 إ ج).

أ/1- 3 - ميقات التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

إذا كان قانون الإجراءات الجزائية قد وضع قاعدة عامة تحدد بدقة الميقات الذي يجوز فيه دخول المساكن وتفتيشها واجراء الحجز بها، وهو بين الساعة الخامسة صباحا والساعة الثامنة مساء المحددة في المادة 1/47 إ ج، فإنه وضع استثناء لتلك القاعدة، وهو جواز دخول المساكن وتفتيشها في أي وقت من اليوم ليلا ونهارا، دون التقيد بذلك الميقات القانوني، هذه الاستثناءات وردت في المواد 1/47، 2/47، و3/47 إ ج.

وفيما يخص بالاستثناء الوارد في المادة 3/47إ ج فالأمر يتعلق بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، أو أن

يقوم قاضي التحقيق بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك (المادة 4/47 إ ج). لأن الغرض من الإسراع في الإجراء والقيام به خارج الميقات المحافظة على الدليل نظرا للطبيعة الخاصة لهذا النوع من الجرائم التي يستفيد فيها المشتبه فيه من التطور التكنولوجي.

لا تمس هذه الأحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من المادة 45 من قانون الإجراءات الجزائية (م6/47)[1].

أ/2- التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق الابتدائي:

نصت المادة 64 إ ج أنه لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات. ويجب أن يكون هذا الرضا مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر في ذلك في المحضر مع الإشارة إلى رضاه، مع ضرورة التقيد بالأحكام المنصوص عليها في المواد 44 إلى 47 إ ج. غير أنه عندما يتعلق الأمر بتحقيق في إحدى الجرائم المنصوص عليها في المادة 3/47 إ ج فإنه تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر إ ج.

أ/3- التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق القضائي:

تنص المادة 79 إج على أنه يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات. على أن يباشر التفتيش وفقا للمادة 81 إج في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة [2].

---

[1]- الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 6-7

[2]- المرجع نفسه

أ/3-1- بالنسبة للميقات القانوني للتفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

وباستقراء المادة 82 إ ج والتي تحيل إلى المادة 47 إج الخاصة بميقات التفتيش القانوني، وفي إطار وضع الأسس القانونية الكفيلة بمحاربة بعض الظواهر الإجرامية الحديثة، كجرائم الإرهاب والمخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف، يقرر قانون الإجراءات الجزائية لقاضي التحقيق دخول المساكن وتفتيشها في أي وقت خارج الميقات القانوني المقرر في المادة 1/47 إج متى تعلق الأمر بتلك الجرائم، وله أن يأمر ضابط الشرطة القضائية المختص مكانا للقيام بتلك الإجراءات (م4/3/47 إ ج) [1].

أ/3-2- بالنسبة لحضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

باستقراء المادة 82 و83 إج الخاصة بحضور أشخاص معينين لعملية التفتيش، والتي تحيلان إلى المادة 45إ ج، يعفي قانون الإجراءات الجزائية، قاضي التحقيق من وجوب الالتزام بقاعدة الحضور المنصوص عليها في المادتين 82 و83 إ ج[2]، حيث يجرى التفتيش والضبط دون حضور هؤ لاء الأشخاص، وذلك في حالة قيامه بالتفتيش بمناسبة الجرائم المنصوص عليها في المادة 3/47 إ ج، فتنص المادة 45 فقرة أخيرة، (لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم

---

[1]- الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 6-7.

[2]- تنص المادة 81 إ ج (إذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد من 45 إلى 47...)

وتنص المادة 82 إ ج على أنه: (إذا حصل التفتيش في مسكن غير المتهم استدعي صاحب المنزل الذي يجرى تفتيشه ليكون حاضرا وقت التفتيش فإذا كان ذلك الشخص غائبا أو رفض الحضور أجري التفتيش بحضور اثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش فإن لم يوجد أحد منهم فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية.

وعلى قاضي التحقيق أن يلتزم بمقتضيات المادتين 45، 47 ولكن عليه أن يتخذ مقدما جميع الإجراءات اللازمة لضمان احترام سر المهنة، وحقوق الدفاع). أنظر في ذلك: أمر رقم 66-155 مؤرخ في 8 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية السابق ذكره، ص 620-621.

الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات المذكورة أعلاه) [1].

أ/3-3 - بالنسبة لضبط أدلة الجريمة:

تنص المادة 84إج على أنه إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها، وعلى قاضي التحقيق أن يتخذ مقدما جميع الإجراءات اللازمة لضمان احترام كتمان سر المهنة، وحقوق الدفاع، ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة.

ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق ويجوز لمن يعنيهم الأمر الحصول على نفقتهم، وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تخل دون ذلك مقتضيات التحقيق[2].

ب- قواعد تفتيش المنظومة المعلوماتية وحجز المعطيات المعلوماتية وفقا لقانون رقم 09- 04:

نص المشرع الجزائر في الفصل الثالث من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سابق الذكر، على القواعد الإجرائية المتبعة في تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية، وذلك في من خلال:

[1]-الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره،ص 6.

[2]- المرجع نفسه .

ب/1- شروط صحة تفتيش المنظومة المعلوماتية:

-نص المشرع الجزائري في المادة 5 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سابق الذكر، على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام بتفتيش المنظومة المعلوماتية في إطار قانون الإجراءات الجزائية، وهي [1]:

أ-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية،

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

- غير أنه في حال الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها حصريا بإجراءات التفتيش[2]. كذلك يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، لا سيما قانون الإجراءات الجزائية، تفتيش

---

[1]- أنظر: المادة 3و4 من قانون رقم 09-04، مؤرخ في 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 6.

[2]-المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، (ج ر،العدد،53) ص 19.

أي مكان أو هيكل أو جهاز بلغ إلى علمها أنه يحو ز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية[1].

– في الحالات سابقة الذكر، يمكن الدخول، بغرض التفتيش، ولو عن بعد إلى[2]:

أ– منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب– منظومة تخزين معلوماتية.

– في الحالة (أ) إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

– إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

– يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ب/2- حجز المعطيات المعلوماتية:

نظمه المشرع الجزائري في نص المادة 06 و 07 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سابق الذكر.

---

[1]- أنظر: المادة 30 من مرسوم رئاسي رقم 15–261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 19

[2]- أنظر: المادة 5 من قانون رقم 09–04، مؤرخ في 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 6.

وتتمثل شروط إجراء الحجز فيما يلي[1]:

– عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

– ويجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

– غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

– إذا استحال إجراء الحجز وفقا لما هو منصوص عليه فيما سبق، لأسباب تقنية، لذا يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

– على السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

– تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

[1]- أنظر: المادة 21 من مرسوم رئاسي رقم 15–261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدةالرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 6–7.

-في حال الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها حصريا بإجراءات الحجز[1].

الفرع الثاني: إجراءات التحري والتحقيق التقليدية المستنبطة من تصريحات الأشخاص.

سوف نتطرق في هذا الفرع الثاني إلى الإجراءات ذات الطبيعة الشخصية والتي غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل .

أولا: الشهادة سنتكلم عن تعريف الشهادة، واجراءاتها في مجال جرائم الماسة بالمستند الإلكتروني وذلك من خلال ما يلي:

1- تعريفها:

الشهادة هي ما يقوله احد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن واقعة بطريقة مباشرة ، فهي تحضا باهتمام القاضي إلا أنه غالبا ما يحتاج في مقام وزن الأدلة إلى من رأى الواقعة أو سمع عنها أو أدركها بحواسه ، حتى قيل أن الشهود هم عيون المحكمة وأذانها[2].

كما أن الشهادة كإجراء من الإجراءات التحقيق هي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق[3]

و يختلف الشاهد التقليدي عن الشاهد المعلوماتي ذلك أن الشاهد في الجريمة المعلوماتية هو " الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي ، والذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت

---

[1]- أنظر: المادة 21 من مرسوم رئاسي رقم 15-261 مؤرخ في 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السالف ذكره، ص 19.

[2] – احمد فتحي سرور **الوسيط في القانون الإجراءات الجنائية** ، دار النهضة ،القاهرة ،1981 ،ص 29

[3]– شرف الدين وردة،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص 245 .

مصلحة التحقيق تتطلب التنقيب عن المعلومات داخلية وتنحصر طوائف وفئات الشاهد المعلوماتي فيما يلي :

1)- مشغلو الحساب الآلي.

2)-خبراء البرمجة

3)- المحللون

4)- مهندسو الصيانة والاتصالات

5)- مديري النظام [1]

كما أن للشاهد المعلوماتي في مجال الالتزام بالإعلام في الجريمة المعلوماتية شروط تتمثل في :

- أن نكون بصدد جريمة مست بالفعل المستند الالكتروني سواء كانت جناية أو جنحة.

- أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة .

- أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية [2]

2-إجراءات الشهادة في جرائم الماسة بالمستند الإلكتروني:

اهتم المشرع الجزائ ي بدور الشاهد المعلوماتي في مساعدة السلطات العامة في مكافحة الجرائم المعلوماتية، وهذا عن طريق إلزامه بالإعلام عن المعلومات الجوهرية التي تسمح

[1]- رضا هميسي ، (**أحكام الشاهد في الجريمة المعلومات**) ،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ،كلية الحقوق والعلوم السياسية ،جامعة بسكرة ،الجزائر ما بين 16،17 نوفمبر 2015 ص04- 05.

[2]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ،ص 257

بالدخول إلى الحاسوب وجمع الأدلة المخزنة به ذلك في المادة 05 الفقرة الأخيرة من القانون09-04 [1]

كما نصت المادة 4/19 من اتفاقية بودابست لمكافحة جرائم الكمبيوتر لعام 2001 على إمكانية الاستعانة بالشاهد المعلوماتي ، بقولها يجب على كل طرف أن يتبين الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل تحويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من اجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية عن نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1و2[2]

ثانيا : الخبرة، سنتكلم عن تعريف الخبرةواجراءاتها في التشريع الجزائري وذلك وفقا لما يلي:

1- تعريفها:

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من اجل الكشف عن الدليل يفيد معرفة الحقيقية بشأن وقوع الجريمة[3]

الخبير المعلوماتي أو الرقمي هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها .

وتكون للخبرة التقنية قواعد قانونية وأخرى تقنية

أ- قواعد ما قبل التشغيل والفحص:

وتتمثل فيما يلي

- التأكد من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها
- التأكد من صلاحية وحدات النظام التشغيل
- تسجيل بيانات وحدات المكونات المحجوزة كالنوع والطراز والرقم المسلسل وغيرها [4]

---

[1]- القانون رقم 09-04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر .

[2]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص260

[3]- سعيداني نعيم ، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**،مذكرة ماجستير في العلوم القانونية ،تخصص علوم جنائية،كلية الحقوق والعلوم السياسية ،جامعة الحاج لخضر ،باتنة ،2013،ص165

[4]- الهام بن خليفة ،مرجع سابق ،ص 299

ب- قواعد التشغيل والفحص :

-عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استغلال الدليل

- عمل نسخة من كل وسائط التخزين لمضبوطة وعلى رأسها القرص الصلب لإجراء عملية الفحص المبدئي على هده النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برمجية

-إظهار الملفات المخبأة والنصوص المخفية داخل الصور

- استكمال تسجيل باقي المعطيات الوحدات من خلال قراءات الجهاز [1]

-تحديد مدى الترابط بين الدليل المادي والدليل التقني

- مرحلة تدوين النتائج إعداد التقرير

- أما الوسائل المستعان بها في الخبرة التقنية فتمثل في

* برنامج البر وكسي (proxy) وهو يعمل كوسيط بين الشبكة ومستخدمها.

*عنوان البروتوكول(Protocol)وهو اتفاق يحكم الإجراءات المستخدمة لتبادل المعلومات بين كيانين متعاونين.

* عنوانبرو توكول،الانترنت (Internet Protocol(TP)وهو المسئو ل عن تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها [2]

بالإضافة إلى برمجيات النسخ الاحتياطي الجنائي.

وبرمجيات أخرى كالبرمجياتنسخ الأقراص المدمجة ،وبرامج كشف الأجزاء المخفية الأقراص الصلبة وغيرها .....الخ[3]

2-إجراءاتالخبرة في مجال جرائم الماسة بالمستند الإلكتروني:

وتجدر الإشارة إلى أن المشرع الجزائري نظم أحكام الخبرة في المواد من 143 إلى 156 من قانون الإجراءات الجزائية [4]

---

[1]- سعيداني نعيم ،مرجع سابق ص 172

[2]- ناني لحسن ، مرجع سابق ،ص 77

[3]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ،ص 276

[4]- الأمر رقم 66-155المتضمن قانون الإجراءات الجزائية ،سالف الذكر.

كما نص المشرع الجزائري المادة 04 من المرسوم الرئاسي رقم 15- 216 المؤرخ في 8 أكتوبر سنة 2015 المحددة لتشكيلة وتنظيمه وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ولاتصال ومكافحتها، على الخبرة القضائية

كذلك يقوم المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي الجزائر العاصمة بإجراء الخبرات في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح[1]

ثالثا: الاستجواب

الاستجواب هو مساءلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه عن الجريمة التي ارتكبها ومجابهته بالأدلة وسماع ما لديه من دفوع التهمة المنسوبة إليه

والاستجواب في الجريمة المعلوماتية تحكمه ذات القواعد العامة لاستجواب المتهم في الجريمة لتقليدية

ومن بين حقوق المتهم أثناء الاستجواب، حق المتهم في الاستعانة بمحامي وحق المحامي في الاطلاع على التحقيق .

المطلب الثالث

إجراءات التحري والتحقيق الحديثة في الجرائم الماسة بالمستند الالكتروني:

إن الأنظمة المعلوماتية وفي ظل المعطيات الحديثة للمجتمعات المعاصرة تشهد انفتاحا غير مسبوق ومحدود واتاحة للمعلومة غير مشروط وهو ما جعلها مجالا مفتوحا تهدده أخطار الاعتداءات المعلوماتية بكل أشكالها [2]

مما جعل العديد من الدول تقوم بتطوير سياستها الجنائية تبعا لهذه الخصوصية وتمكن رجال الشرطة القضائية، من الكشف عن الجرائم من خلال سن إجراءات حديثة للتحري والتحقيق عن الجرائم المعلوماتية ومنها جرائم الماسة بالمستند الإلكتروني، ومنه سنتطرق في هذا المطلب إلى أهم الإجراءات التحري والتحقيق الحديثة المستنبطة من الوقائع أو الأشياء (الفرع الأول)، والإجراءات المستنبطة من تصريحات الأشخاص (الفرع الثاني)، ثم

---

[1]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص 283

[2]- ربيعي حسين، **(الأساليب التقنية الحديثة لارتكاب الجرائم المعلوماتية)** بحث مقدم لأعمال الملتقي الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة،كلية الحقوق والعلوم السياسية ،جامعة بسكرة ،الجزائر،مابين 16و17 نوفمبر 2015،ص 04

تخصص (الفرع الثالث) للحديث عن مظاهر التعاون الدولي لمكافحة جرائم الماسة بالمستند الالكتروني .

الفرع الأول: الإجراءات الحديثة المستنبطة من الوقائع أو الأشياء

تتمثل هذه الإجراءات في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بالإضافة إلجراء المراقبة الالكترونية وا جراء حفظ المعطيات المتعلقة بحركة السير .

أولا:اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور

1- تعريفه:

قد تضطر الشرطة القضائية لاستعمال كاميرات خفية أو أجهزة تصنت لكن يجب ان يكون ذلك في إطار احترام الشرعية الإجرائية حفاظا على كرامة الحياة الخاصة للإنسان كما يمكن لضابط الشرطة القضائية تصوير جسم ومكان الجريمة بشكلها العام في إطار ممارسة مهامه، لكنه يمنع من الاطلاع أو تسجيل المكالمات أو الأحاديث الخاصة إلا بإذن مسبق من طرف السلطات القضائية [1] وفقا كما نص عليه الدستور الجزائري في المادة 39

ويقصد باعتراض المراسلات بأنه إجراء يتم من خلاله رصد كل كلمة أو كل المحادثات التي تجرى بين الأشخاص وهذا الكلام أو الحوار يتم أولا التقاطه ثم تثبيته بتسجيله وبثه عند الحاجة ومن ثم يستعمل كدليل يواجه به المتهم

والمقصود بالمراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ،كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية حسب المادة 8-21 من القانون رقم 2000-3 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية [2]

أما تسجيل الأصوات والتقاط الصور فيقصد تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذالك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان واحد خاص [3]

---

[1]- ناني لحسن ،مرجع سابق ،ص 73

[1]-شرف الدين وردة ،**مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية،في التشريع الجزائري**، مرجع سابق،ص542

[3]- إلهام بن خليفة ،مرجع سابق ،ص 310

و من بين صحة شروط صحة اعترض المراسلات والتقاط الصور وتسجيل الأصوات

– أن تكون الجريمة الواقعة على المستند الإلكتروني على درجة معينة من الجسامة

– أن تكون هناك فائدة في ظهور الحقيقة

هذا بالنسبة للشروط الموضوعية أما الشروط الشكلية فتتمثل في :

– لابد من صدور أمرباعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور

– أن يسبب الأمر بالاعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور

–تحرير محضر بعملية الاعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور

– يجب أن تكون السلطة المختصة بالتحقيق الابتدائي ،سواء كان قاضي لتحقيق أو النيابة العامة وحدها دون غيرها هي من تطلع على المراسلات أو الصور

– يجب حضور بعض الأشخاص أثناء الاطلاع على المراسلات والصور تسجيل الأصوات [1]

2–إجراءات إعتراض المراسلات وتسجيل الأصوات والتقاط الصور وفقا للتشريع الجزائري

تمم قانون الإجراءات الجزائية الجزائري بالباب الثاني من الكتاب الأول بالقانون رقم 06–22 المؤرخ في 20 ديسمبر 2006 بفصل رابع بعنوان "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" ويشمل المواد من 65 مكرر 5 إلى 65 مكرر 10 حيث:

يجوز لرجال الشرطة القضائية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي[2]،القيام باعتراض المراسلات، تسجيل الأصوات والتقاط الصور لكنه قيدهم بجملة من الشروط لتكون إجراءاتهم صحيحة ومنتجة لآثارها وهي:

–أن يقوم الضباط بهذه الأعمال سعيا للكشف عن جرائم حددها المشرع في المادة 65 مكرر 5 وهي: جرائم المخدرات، الجرائم المنظمة العابرة للحدود الوطنية، الجرائم الماسة

[1]– شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية،مرجع سابق** ، ص ص 295–299

[2]– المقصود بالتحقيق الابتدائي، هو التحريات الأولية للضبطية.

بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.

ما يلاحظ أن المشرع الجزائري عدد هذه الجرائم على سبيل الحصر وقد يرجع هذا للخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة واقتصادها، أما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل.[1]

– أن يصدر الإذن إلى ضباط الشرطة القضائية –للقيام بالأعمال المحددة في المادة 65 مكرر 5، مكتوبا من وكيل الجمهورية أو قاضي التحقيق المختصين، بأن يأذنوا بما يلي:

*اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية،

* وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص،

في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة.

– ضابط الشرطة القضائية مقيد أثناء قيامه بالعمليات المحددة في المادة 65 مكرر 5، بالحفاظ على السر المهني حرصا على نجاحها من جهة وخوفا من فشلها من جهة أخرى وهذا راجع لخطورة هذه الأفعال الإجرامية التي تنفذ على مستوى من الاحتراف والسرية، واذا

[1]– شرف الدين وردة، **الإثبات الجنائي بالأدلة الإلكترونية**،المرجع السابق، ص ص 321–322

اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة.

– يجب أن يتضمن الإذن المذكور، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة سكنية أو غيرها، وتحديد به الجريمة التي تبرر اللجوء إلى هذه التدابير.[1]

– يسلم الإذن مكتوبا لمدة أقصاها أربعة (04) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

– يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات الذكورة في المادة 65 مكرر 5.

– يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

–يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات والصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف. وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية، عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض[2].

ثانيا إجراء مراقبة الاتصالات الإلكترونية

طبقا لنص المادة 03 من قانون 09-04 سابقا الذكر فقد وضع طبقا لمشرع الجزائري بين أيدي الجهات المختصة بمكافحة الجريمة المتصلة بتكنولوجيا المعلوماتية وسيلة قانونية وجديدة من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها وهو ما أطلق عليه مصطلح مراقبة الاتصالات الالكترونية .

[1]– شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ،ص 323

[2]– المرجع نفسه،ص 324

-وقد تم تعداد الحالات التي يمكن اللجوء فيها إلى هذه الوسيلة من وسائل البحث والتحري من خلال المادة 04 من ذات القانون وهي 04 حالات :

-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء إلىالمراقبة الالكترونية .

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

ولمباشرة المراقبة الالكترونية بجب الحصول على إذن مكتوب من السلطات القضائية المختصة طبقا لنص المادة 04 من القانون 09-04. [1]

- يحميالمشرع الجزائري على غرار باقي التشريعات الأخرى الحق في الخصوصية وما يتفرع عنه من حرية المراسلات وذلك عن طريق تجريمه لكل سلوك من شانه الاعتداء على حرمه الحياة الخاصة في المادة 303 مكرر من قانون العقوبات والتي جاء فيها انه يعاقب بالحبس من 06 أشهر إلى 03سنوات وبغرامة من 50.000دج إلى 300.000دج من كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأنه تقنية كانت وذلك

- بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

-ويشمل مصطلح المراسلات حتىالمراسلات البريد الالكتروني [2]

ثالثا : جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها

نظم المشرع الجزائري هذا الإجراء ضمن قانون 09 -04 السابق الذكر وجعله من التزامات مقدمي الخدمات في مساعدة السلطات حيث تنص المادة 10 على انه في إطار تطبيق أحكام هذا القانون ،يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها

[1]- ناني لحسن ،مرجع سابق ،ص ص 80،81

[2]- الهام بن خليفة ،مرجع سابق،ص 318

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذالك لمعلومات المتصلة بها ذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق [1]

الفرع الثاني :الإجراءات التحري والتحقيق الحديثة المستنبطة من تصريحات الأشخاص

سنتطرق في هذا الفرع إلىكل من إجراء التسرب واجراء الحفظ العاجل للبيانات المعلوماتية المخزنة بالإضافة إلى إجراء الأمر بإنتاج بيانات معلوماتية المخزنة بالإضافة إلي إجراء الأمر بإنتاج بيانات معلوماتية .

وقد تمإدراج هذه الإجراءات ضمن تصريحات الأشخاص بوجود شخص يتوسط بين الإجراء وبين الدليل بحيث يؤدي غياب هذا الشخص إلى انعدام الدليل [2]

أولا: التسرب

1- تعريفه:

لقد منح القانون 22/06 ضباط وأعوان الشرطة القضائية إمكانية استعمال التسرب في المواد من 65 مكرر 11 إلى 65 مكرر 18 ق ا ج كما عرف التسرب على انه قيام الضباط وأعوان الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في لارتكابهم جناية أو جنحة بإيهامهم بأنه فاعل معهم أو شريك لهم أو خاف [3]

ويعرفه البعض بأنه تقنية من تقنيات التحري و التحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخلجماعة إجرامية وهذا بهدف مراقبة أشخاص مشتبه فيهم [4]

---

[1]- قانون رقم 09-04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ،سالف الذكر .

[2]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص 329

[3]- ناني لحسن ،مرجع سابق ،ص ص 55،74

[4]- عبد الرحمان خلفي**الإجراءات الجزائية في التشريع الجزائري والمقارن**،الطبعة الثانية،دار بلقيس ،الجزائر،2016 ،ص 105

ويعرفه البعض بأنه " أكثر وسائل التحري تعقيدا وخطورة،لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة،ولكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط،ويوهمهم بأنه فاعل وشريك لهم وذلك حتى يطلع على أسرارهم من الداخل،ويجمع ما يستطيع من أدلة إثبات ،ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة "[1]

2-إجراءات التسرب في مجال جرائم الماسة بالمستند الإلكتروني:

استحدث المشرع الجزائري في قانون الإجراءات الجزائية بموجب القانون رقم: 06-22، المؤرخ في 20 ديسمبر سنة 2006، إجراء التسرب كأسلوب من أساليب التحري والتحقيق عن الجرائم الخطرة منها المعلوماتية وذلك في المواد من 65 مكرر 11 إلى 65 مكرر 18، فتعرف المادة 65 مكرر 12 التسرب على أنه (يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف). حيث تتم هذه الإجراءات وفقا للقيود والشروط المقررة في الأحكام المقررة قانونا، والتي تتمثل فيما يلي[2]:

-أن تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم الموصوفة بالإرهابية وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب، عملا بحكم المادتين 65 مكرر 5، 65 مكرر 11 من قانون الإجراءات الجزائية، والمادة 24 مكرر من قانون الوقاية من الفساد ومكافحته والمادتين 33،34 من قانون التهريب.

---

[1]-شرف الدين وردة،**مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية ،في التشريع الجزائري**،مرجع سابق،ص545

[2]- قانون رقم: 06-22، المؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966،المتضمن قانون الإجراءات الجزائية الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 9-10.

– يجب أن يتم الإذن بعملية التسرب من طرف وكيل الجمهورية أو من طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية.

– يجب أن يكون الإذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية. ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

– لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. ويعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 200.000 دج.

واذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر (10)سنوات والغرامة من 200.000 دج إلى 500.000 دج.

واذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون عقوبة الحبس من عشر (10) سنوات إلى عشرين (20)سنة والغرامة من 500.000 دج إلى 1.000.000 دج دون الإخلال، عند الاقتضاء، بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.

– إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة إجراءات التسرب للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا تتجاوز ذلك مدة أربعة (4) أشهر. وفي هذه الحالة يتعين إخبار القاضي الذي رخص بإجراء عملية التسرب تلك في اقرب الآجال، فإذا انقضت مهلة الأربعة (4) أشهر تلك دون أن

يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، أمكن لهذا القاضي أن يرخص بتمديدها لمدة أربعة (4) أشهر على الأكثر.

– يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية.

ثانيا :التحفظ العاجل على البيانات المعلوماتية المخزنة

تحدث المشرع الجزائري في الفصل الرابع من قانون رقم: 09-04، المؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، في المادتين 10 و11، على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات **بحفظ المعطيات.**

حيث نصت المادة 10، على أنه في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 **(حفظ المعطيات المتعلقة بحركة السير)**، تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير حيث نصت على أنه:مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها،

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه،

تحدد مدة حفظ المعطيات المذكورة، بسنة واحدة ابتداء من تاريخ التسجيل.[1]

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في المادة 11 من نفس القانون، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5)سنوات وبغرامة من 50.000 دج إلى 500.0 كما نص المشرع الجزائري في المادة 4 من مرسوم رئاسي رقم 15-261، المؤرخ في 8 أكتوبر سنة 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، [2]، على أنه: من بين المهام المكلفة إلى الهيئة: حفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية. إلا أنه لم يحدد المدة القصوى التي تلتزم بها الهيئة لحفظ هذه المعطيات كما فعل بالنسبة لحفظ المعطيات المتعلقة بخط السير على مستوى مقدمي خدمات الانترنت بمقتضى المادة 11 من قانون 09-04.

ثالثا :الأمر بإنتاج بيانات معلوماتية :

هو إجراء جديد للتحري والتحقيق على الجرائم المعلوماتية، لم تنص عليه معظم الدول منها الجزائر لكن تم النص عليه ضمن اتفاقية بودابست لمكافحة جرائم المعلوماتية سنة 2001 وهذا في نص المادة 18 من الاتفاقية .

كما تم النص عليه ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، وهذا في نص المادة 25 من الاتفاقية ويشير هذا الأمر إلى أن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

---

[1]-شرف الدين وردة، **الإثبات الجنائي بالأدلة الإلكترونية**، مرجع سابق، ص357

[2]-الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، السابق ذكره، ص 16.

– أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين،

– أو مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته. [1]

الفرع الثالث: مظاهر التعاون الدولي في مجال مكافحة جرائم الماسة بالمستند الالكتروني

تعددت الجهود الدولية والإقليمية في سبيل مكافحة الجريمة المعلوماتية وهذا نظرا للتهديدات الكبيرة التي أتت بها الجريمة على هاذين المستويين وفي هذا النطاق سنتطرق في هذا الفرع إلى أهم الآليات الدولية التي تكفل منع ارتكاب الجريمة المعلوماتية.

أولا : التعاون القضائي الدوليفي مواجهة الجرائم الماسة بالمستند الكتروني :

1- تعريفه: يقصد بالتعاون الدولي "سلوك بين أشخاص القانون الدولي، يتم على المستوى الثنائي، والمتعدد الأطراف يتعلق بموضوع أو أكثر من الموضوعات الدولية، قصد تحقيق هدف مشترك"

2- صور التعاون الدولي

المساعدة القضائية المتبادلة

تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم ولقد نص المشرع الجزائري في القانون 04/09 على هذا المبدأ في المادة 16 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني .

وتتخذ هذه المساعدة عدة صور منها[2]

– تبادل المعومات

–نقل الإجراءات

---

[1]–الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، الصادرة في 28 سبتمبر سنة 2014، ص 8.، أنظر كذلك: شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية** ،مرجع سابق ،ص ص 359،366

[2]– سعيداني نعيم ،مرجع سابق،ص 89

– تبادل الإنابات القضائية الدولية

–مثول الشهود والخبراء في المواد الجنائية

– ضبط ومصادر متحصلات الجريمة

– تسليم المجرمين وهو ذلك الإجراء القانوني الذي تقوم به الدولة ما لتسليم شخص موجود على إقليمها إلى دولة تطالب به لمحاكمته أو لتنفيذ العقوبة المحكوم بها أو كإجراء وقائي [1]

2–التعاون الفني الدولي في مواجهة الجرائم الماسة بالمستند الالكتروني:

نجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة بالجريمة المعلوماتية دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها وهذا كان نتيجة لظهور هذه الأنماط الجديدة من الجرائم حيث أصبحت تشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم وكذالك رجال الضبطية القضائية[2]

وفي هذا الإطار ونظرا للبعد الدولي الذي عادةما يتخذه هذا النوع من الجرائم لم تغفل المديرية العامة للأمن الوطني، الجزائري استغلال عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INERPOL) هاته الأخيرة التي تتيح مجالات للتبادل المعلوماتي الولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا[3]

ثانيا- أهم الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم المعلوماتية :

– عدم كفاية مبدأ الشرعية الجزائية لاستيعاب كل صور النشاط الإجرامي المتعلق بالجريمة المعلوماتية

– إشكالية تنازع القوانين الجناية المختصة بمكافحة الجريمة المعلوماتية

– نقص التنسيق والتوظيف الكافي الآليات الدولية والمكافحة الجريمة المعلوماتية [4]

---

[1]– شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ،ص 157

[2]– سعيداني نعيم ،مرجع سابق ، ص 92

[3]– حملاوي عبد الرحمان، **(دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية)** ،بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ،مابين 16و17 نوفمبر 2015،بسكرة، ص 09

[4]– يعيش تمام شوقي،مرجع سابق، ص16

– التجريم المزدوج والذي يقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة طالبة التسليم،وكذلك في تشريع الدولة المطلوب إليها التسليم،فلا عبرة للوصف أو التكييف القانوني الذي يطلق عل الفعل،فمثلا لو كان الفعل في تشريع الدولة الطالبة التسليم تحت مسمى جريمة توظيف الأموال،بينما كان الفعل نفسه مجرما تحت مسمى جريمة النصب والإحتيال في الدولة المطلوب منها التسليم،فإن ذلك لا يحول دون توافر شرط التجريم أو ازدواجية،حيث قد يكون هذا الشرط الذي يعتبر من أهم شروط تسليم المجرمين عقبة أمام التعاون الدولي من مجال تسليم المجرمين بالنسبة للجريمة المعلوماتية سيما وأن معظم الدول مازالت نصوصها العقابية خالية من هذا النمط الإجرامي [1]

[1]– شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ، ص 161

المبحث الثاني

إجراءات المحاكمة في الجرائم الماسة بالمستند الالكتروني

تواجه الجريمة المعلوماتية بصفة عامة العديد من المشكلات المتمثلة في تحديد القانون الواجب التطبيق والمحكمة المختصة بالنظر في تلك الجرائم.

وتبرز أهمية هذا التحديد في مجال الجرائم المعلوماتية جراء البعد الوطني الذي تتميز به هذه الجريمة، لأن غالبية الأفعال ترتكب من خارج الحدود أو أنها تمر عبر شبكة الانترنت، وهو ما يبرز مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق.[1]

والملاحظ أنه في ظل التعديلات الحديثة التي عرفتها التشريعات الجزائية وتماشيا مع التعديل الدستوري الذي تبنته الجزائر بموجب القانون رقم 16-01 المؤرخ في 2016/03/6 والذي نص في المادة 160 منه فقرة 2 على أنه يضمن القانون التقاضي على درجتين في المسائل الجزائية ويحدد كيفيات تطبيقها ، وبالتالي يظهر أن الدستور الجزائري ولأول مرة أقر استئناف الأحكام الصادرة في مواد الجنايات، وتبعه صدور القانون رقم 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم للأمر رقم 66-155المتضمن قانون الإجراءات الجزائية لتنظيم هذه المسألة باعتبارها وضعا إجرائيا جديدا أملته الظروف وفرضه العمل القضائي الذي يعتبر عنوان الحقيقة،يحتاج إلى ضمانات للوصول إليها ما دام أنه عمل بشري قابل للخطأ والصواب،مما يجعل مراجعته أمرا ضروريا لتحقيق الغاية المرجوة منه.[2]

وفي سبيل دراسة النظام القانوني والإجرائي الجديد للمحاكمة الجنائية في الجزائر، فالملاحظ أن المشرع الجزائري،قد تبنى في تعديل قانون الإجراءات الجزائية ، بموجب القانون 17-07 مبدأ التقاضي على درجتين في مواد الجنايات، فلقد نصت المادة 248 منه على أنه يوجد بمقر كل مجلس قضائي، محكمة جنايات ابتدائية ومحكمة جنايات استئنافية تختصان بالفصل في الأفعال الموصوفة جنايات وكذا الجنح والمخالفات المرتبطة بها[3] .

واستنادا إلى هذا النص فلقد تم منح الفرصة للمحكوم عليه بعرض قضيته من جديد أمام محكمة أعلى درجة من المحكمة التي أصدرت الحكم عليه لاستكمال ما يكون قد ظهر في

---

[1]- صغير يوسف،مرجع سابق ص.140

[2]- العربي شحط محمد الأمين**قراءة في الأحكام الجديدة للقضاء الجنائي في قانون الإجراءات الجزائية)** مجلة دفاتر السياسة والقانون ،العدد الثامن عشر،جامعة وهران،18 جانفي 2018،ص 214

[3]- القانون رقم 17-07المعدل والمتمم لقانون الإجراءات الجزائية،سالف الذكر.

تحقيق الدعوى الجنائية من نقص أو قصور،وتصويب ما قد تقع فيه محكمة الجنايات الابتدائية من أخطاء[1].

وسنتطرق في هذا المبحث إلى: تحديد المحكمة الجنائية المختصة (المطلب الأول)، ثم حجية المستند الإلكتروني في الإثبات الجنائي، وأخيرا تقييم الأدلة الرقمية المستخلصة من الجرائم الماسة بالمستند الإلكتروني (المطلب الثالث).

المطلب الأول:

تحديد المحكمة الجنائية المختصة:

ثار خلاف فقهي كبير حول تحديد المحكمة الجنائية المختصة في الجرائم المعلوماتية بما فيها جرائم الاعتداء على المستند الالكتروني.

وسنبين في هذا المطلب إلى موقف الفقه (الفرع الأول) من تحديد المحكمة المختصة، تحديد القانون الواجب التطبيق (الفرع الثاني)، ثم موقف المشرع الجزائري (الفرع الثالث).

الفرع الأول: موقـــــف الفقـــه

حاول الفقه حل مشكلة تنتزع الاختصاص،وانقسم إلى ثلاثة اتجاهات وهي:معيار الاختصاص المكاني،معيار القانون أكثر ملائمة ،ومعيار الضرر المرتقب

أولا: معيار الاختصاص المكاني

تعتمد أغلب التشريعات في تحديد الاختصاص المكاني، إتباع ثلاثة ضوابط، وهي مكان وقوع الجريمة أو محل إقامة المتهم أو مكان ضبط إلقاء القبض عليه، وفي حالة اجتماع أكثر من ضابط، تكون المحكمة التي ترفع إليها الدعوى أولا هي المختصة بنظر الدعوى.

وبالتالي ينعقد الاختصاص وفقا لهذا المعيار، للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكنفه بعض الصعوبات.[2]

يمثل السلوك الإجرامي والنتيجة الإجرامية شطري الجريمة المعلوماتية، ومن ثم فإن سلطات ومحاكم مكان النشاط الإجرامي ومكان النتيجة تكون مختصة، وعلى ذلك فإذا تم بث الفيروس المعلوماتي (لسلوك الإجرامي) في مكان، وتحققت النتيجة (تدمير المعلومات)

[1]– العربي شحط محمد الأمين ، مرجع سابق ص 219

[2]– الصغير يوسف،مرجع سابق،ص ص.142، 143

في مكان آخر وألقي القبض على الجاني في مكان ثالث، فإن الاختصاص ينعقد لمحاكم إحدى هذه الأماكن[1]

ثانيا: معيار القانون الأكثر ملائمة

يرى أصحاب هذا الاتجاه، بأنه نظرا للطبيعة الخاصة لجرائم المعلوماتية والأضرار الناجمة عنها التي تمتد ليشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى إلى القول بأنه يجب التوسع في تفسير قاعدة اختصاص محكمة وقوع الفعل (حصول الضرر)، ليجعل الاختصاص لمحكمة الدولة الأكثر تعرضا للضرر بشكل فعلي، مع التركيز على مبدأ التخلي أو التنازل عن الاختصاص بخلاف ذلك وان جعل الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى المعلومة من هذه الدولة أو تلك، أصبح أمرا غير كافي من الناحية القانونية لإعلان اختصاص هذه الدولة أو تلك.[2]

ثالثا: معيار الضرر المرتقب

صاحب ظهور شبكة الانترنت وجود عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديدوجهتها، وهذا العالم الافتراضي لا يخضع لأي سلطة إقليمية، وبالتالي يترتب على هذه الحالة (أ)، الضرر الذي تسببه الجريمة المعلوماتية يمكن أن يحدث في أي دولة تكون متصلة بالانترنت، وهذا هو معيار الضرر المرتقب أو الافتراضي.

الفرع الثاني: تحديد القانون الواجب التطبيق

وفقا لمبدأ الإقليمية فإن المحاكم الجزائية تختص في الدولة بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيا كانت صفة الشخص المتهم وبغض النظر عن جنسيته. فإذا ما ارتكب شخص ما جريمة معلوماتية بداخل الدولة، وتحققت نتيجتها بذات الدولة، فالقانو ن الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجني عليه.[3]

---

[1] – عبد الفتاح بيومي حجازي**مبادئ الإجراءات الجنائية ،في جرائم الكومبيوتر**،الطبعة الأولى ،دار الفكر الجامعي ،الإسكندرية،2006 ص.51، 52

[2] – صغير يوسف، مرجع سابق ص.144

[3] – المرجع نفسه، ص.141

وعملا بمبدأ العينية فإن الاختصاص يكون للمحاكم إذا وقعت جريمة من جرائم الانترنت أو المستند الالكتروني بصفة خاصة تمس بمصالح الدولة الأساسية والجوهرية وان وقعت خارج الدولة وبغض النظر عن جنسية مرتكبيها.

وعليه إن كيفت الجريمة المعلوماتية بأنها مخلة بأمن الدولة الجزائرية ووفقا لقانون العقوبات الجزائري سواء أكان الإخلال بأمن الدولة سياسيا أو عسكريا أو اقتصاديا، فإن الاختصاص هنا يعود للمحاكم الجزائري، إذ تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا ألقي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها.[1]

ووفق لمبدأ شخصية القوانين فإن الفقهاء يرون أن لهذا المبدأ وجهان أحدهما إيجابي والآخر سلبي، أما الوجه الإيجابي، فيعني بتطبيق النص الجنائي على كل من يحمل جنسية الدولة، ولو ارتكبت جريمته خارج إقليمها. أما الوجه السلبي للمبدأ، فيعني بتطبيق النص الجنائي على كل جريمة يكون المجني عليه فيها منتمية إلى جنسية الدولة ولو كان مرتكب هذه الجريمة أجنبيا وارتكبها خارج إقليم الدولة.[2]

الفرع الثالث: موقف المشـوع الجزائـــــــري

بالنسبة للاختصاص الجنائي الوطني، فإنه يتحدد وفقا للاختصاص المحلي للجهات القضائية بمكان وقوع الجريمة ومحل إقامة الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص، غير أن المشرع الجزائري مدد الاختصاص القضائي لهؤلاء بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004، والمتضمن قانون الإجراءات الجزائية.[3]

إن أهم الإشكاليات المطروحة والمتعلقة بالاختصاص القضائي في الجرائم المتصلة بتكنولوجيا المعلوماتية تتمثل أساسا في إشكالية الاختصاص المحلي في الجرائم الواقعة خارج الإقليم الوطني وكذا إشكالية الإجراءات أمام الأقطاب القضائية المختصة.

إن قواعد القانون الجنائي (شقيه الموضوعي والإجرائي) تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف، ألا وهو مبدأ الإقليمية، والأصل أن عناصر الركن المادي

---

[1] – صالح شنين، مرجع سابق ،ص.269

[2] – صغير يوسف،مرجع سابق ص.141

[3] – صالح شنين،مرجع سابق،ص269

للجريمة تكتمل في مكان واحد، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق، وبالتبعية للمحكمة المختصة بنظر الدعوى.

بيد أن الجرائم المعلوماتية يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في مكان، في حين تتحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى.[1]

لقد اكتفى المشرع الجزائري في هذا الشأن بالفقرة الثانية من نص المادة 15 من القانون 04/09 والتي تنص على: "تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج إقليم الوطني، عندما يكون مرتبكها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني."[2]

وهذه المبادرة تحسب للمشرع الجزائري، إلا أنها لم ترقى إلى المستوى المطلوب لمواجهة الجرائم المعلوماتية.

أما بالنسبة لإشكالية الإجراءات أمام الأقطاب القضائية المتخصصة، فبالرجوع إلى نص المادة 40 مكرر1 من قانون إ.ج.ج نجد أنها أبقت على العلاقة التقليدية المنظمة للعلاقة التدرجية بين وكيل الجمهورية المختص إقليميا والضبطية القضائية في مجال التحري في الجرائم المنصوص عليها في المادة 37 من نفس القانون.[3]

و ينعقد الاختصاص الداخلي،في الجرائم المعلوماتية لوكلاء الجمهورية وقضاة التحقيق وبعض المحاكم بناء على المرسوم التنفيذي 348/06المؤرخ في 2006/10/08المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق .حيث تم إنشاء أربع أقطاب :

- قطب في محكمة سيدي أمحمد
- قطب في محكمة قسنطينة
- قطب في محكمة ورقلة

[1] – ناني لحسن، مرجع سابق ،ص ص.61، 62

[2] – القانون رقم 04/09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،سالف الذكر.

[3] – ناني لحسن، مرجع سابق ،ص ص.63، 64

-قطب في محكمة وهران

حيث أن كل قطب يختص بمجموعة من الولايات وهذا على عكس الجرائم العادية في تحديد الإختصاص .

وتثار مشكلة الاختصاص القضائي المحلي بالنسبة للجرائم المعلوماتية في حالة ما إذا ارتكبت الجريمة في أكثر من نطاق اختصاص محلي داخل الإقليم الوطني للدولة، بسبب طبيعة الجريمة وشبكة المعلوماتية، فالجريمة في هذه الحالة سواء تمثلت بجريمة الدخول أو إتلاف المستند الالكتروني قد وقعت بكامل أركانها في نطاق اختصاص المحاكم الجزائرية والحل المناسب لهذه المشكلة هو تمديد الاختصاص القضائي داخل إقليم الدولة بما يتناسب وطبيعة الجريمة المرتكبة إذ يمكن تطبيق أي قاعدة من قواعد الاختصاص سواء اقترفت بمكان القبض عليه، فينعقد الاختصاص للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها. فإذا نظرت محكمة محل إقامة المتهم في قضية فتكون مختصة بالنظر فيها دون غيرها ولها أن تمدد الاختصاص بشأن اتخاذ أي إجراء من إجراءات المحاكمة، بشرط أن يكون التمديد بموجب نص قانوني.

مما جعل القانون الجزائري يمدد الاختصاص القضائي بالنسبة لبعض الجرائم التي نصت عليها المواد (37) و (329الفقرة 3) ق.إج الجزائري.[1]

وما يهمنا نحن في هذا المجال أنه من خلال ما سبق وبالرجوع إلى النصوص العقابية الموضوعية الجزائية، نلاحظ أنه بالنسبة لجريمة تزوير المحررات الإلكترونية الرسمية إذا قام بها قاضي أو موظف عمومي أثناء تأدية مهامهم،وفقا للمادتين 214 و 215 ق ع،فتكيف العقوبة على أنها جناية وتحال بذلك إلى محكمة الجنايات، في المقابل تكيف على أنها جنحة وبالتالي تحال إلى محكمة الجنح والمخالفات ،في نص المادة 394 مكرر ق ع باعتبارها تعديل في بيانات معلوماتية،وبالتالي تثار مشكلة هنا مفادها ،هل تعتبر جريمة تزوير المحرر ات الرسمية الإلكترونية جناية أو جنحة ؟

وبالتالي نسجل ازدواجية في التجريم والعقاب وهو ما يجعل القاضي الجزائي كما قلنا سابقا يتأرجع عند معالجته إلى هذه النصوص ، إلا أنه هناك مبدأ في القانون الجنائي يقضي بأنه في حالة وجود ازدواجية في التجريم والعقاب فإن القاضي الجزائي يطبق الوصف الأشد وبالتالي العقوبة الأشد.

[1] – الأمر رقم 155-66 المتضمن قانون الإجراءات الجزائية سالف الذكر .

المطلب الثاني:

حجية المستند الالكتروني في الإثبات

يعد موضوع حجية المستندات الالكترونية في الإثبات من المواضيع الحديثة التي تتعلق بالإطار القانوني للتعاملات الالكترونية التي تتم عن طريق وسائل الاتصال المتطورة باستخدام التكنولوجيا الرقمية، ولا تزال فكرة المستند الالكتروني إلى الوقت الحاضر في العديد من الدول غير واضحة المعالم.وهذا راجع للقواعد المنظمة للإثبات، حيث إنها، إما لم تعدل منذ أن وضعت بداية برغم قدم العهد بها، أو برغم من حداثتها نسبيا لم تتعرض لمدى الحجية المعترف بها لتقنيات الكتابة الحديثة في الإثبات كالفاكس والتلكس، إضافة إلى التوقيع الالكتروني.

وهذا ما يترتب عليه عدم مواكبة القوانين، ولا سيما في البلدان النامية التي تفتقر إلى هذه التقنيات ووسائل استخدامها للتطورات التكنولوجية والمعرفية الحالية وصعوبة قدرتها على استيعاب مستجدات هذا التطور وانعكاساتها على العلاقات القانونية فيها.[1] ومن تلك البلدان الجزائر مثلا.

ومنه قمت بتقسيم هذا المطلب إلى فرعين، الفرع الأول يتضمن حجية المستند الالكتروني كقاعدة عامة في الإثبات والفرع الثاني حجية المستند الالكتروني وفقا للاستثناءات الواردة على القاعدة العامة.

الفرع الأول: حجية المستند الالكتروني كقاعدة عامة في الإثبات:

نصت المادة 30 من القانون التجاري على: "يثبت كل عقد تجاري بسندات رسمية / بسندات عرفية / بفاتورة مقبولة بالرسائل / بدفاتر الطرفين / بالإثبات بالبينة أو بأية وسيلة أخرى إذا رأت المحكمة وجوب قبولها."

وفقا لنص المادة أعلاه يتبين أن المشرع الجزائري قد أخذ بمبدأ الإثبات الحر في المعاملات التجارية، وذلك نظرا للسرعة التي تقتضيها طبيعة المعاملات التجارية.

كذلك عملا بالمادة المذكورة أعلاه حتى يمكن التمسك بحرية الإثبات في الأعمال التجارية لابد أن تكتسب هذه الأعمال صفة الأعمال التجارية التي يقوم بها التاجر لمصلحة تجارية، فإذا كان العمل الذي قام به التاجر لغير صالح تجارته فإنه لا يستفيد من حرية

---

[1] – داديار حميد سليمان، **دور السندات المستخرجة عن طريق الانترنت لإثبات المسائل المدنية** (راسة تحليلية مقارنة)، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2010، ص ص.131، 132

الإثبات حتى ولو كان تاجرا. وقد يكون التصرف مختلطا، أي أن أحدطرفي التصرف تاجرا يتعاقد لأغراض تجارية والطرف الآخر غير تاجر، كالعمليات المصرفي بين العميل والبنك، في هذه الحالة يكون الإثبات حرا في مواجهة التاجر ويكون للطرف غير التاجر أن يثبت دعواه بأية طريقة من طرق الإثبات مهما كانت قيمة التصرف، وله أن يستعين بالمحررات الالكترونية.

ومن هنا فإن إثبات المعاملات والقضايا التجارية بالمحررات الالكترونية مهما بلغت قيمتها مقبول على أساس إجازة القانون لمثل هذا الأمر الذي هو حرية الإثبات في هذه المعاملات، فليس من العدل رفض مثل هذه الوسائل في المسائل التجارية.[1]

الفرع الثاني: حجية المستند الالكتروني كاستثناء على القاعدة العامة في الإثبات:

أجاز قانون الإثبات العراقي رقم 107 لسنة 1979 المعدل، أن يثبت بجميع طرق الإثبات ما كان يجب إثباته بالكتابة إذا وجد مانع مادي أو أدبي حال دون الحصول على الدليل الكتابي[2]

لقد وردت على القاعدة العامة استثناءات التي تأخذ بالمستند الالكتروني كدليل إثبات، منها مبدأ الثبوت بالكتابة وحالة وجود مانع أدبي أو مادي يحول دون الحصول على الدليل الكتابي، وحالة فقدان الدليل، فكل هذه يجوز فيها الإثبات بغير الكتابة.[3]

أولا: اعتبار المستند الالكتروني مبدأ ثبوت بالكتابة

أجاز المشرع الجزائري إثبات التصرف القانوني بالشهادة، حيث نصت المادة 335 من القانون المدني الجزائري على أنه: "يجوز الإثبات بالشهود فيما كان يجب إثباته بالكتابة إذا وجد مبدأ ثبوت بالكتابة. وكل كتابة تصدر من الخصم ويكون من شأنها أن تجعل وجود التصرف المدعى به قريب الاحتمال تعتبر مبدأ ثبوت بالكتابة.[4]

من خلال نص المادة أعلاه، يتضح وجود ثلاثة شروط للاستفادة من هذا الاستثناء.

1) وجود كتابة
2) صدور كتابة من الخصم

---

[1] -كحول سماح، مرجع سابق ،ص.15

[2] – داديار حميد سليمان، مرجع سابق،ص.159

[3] – كحول سماح، مرجع سابق ص.15

[4] -الأمر رقم 75-85المتضمن القانون المدني،سالف الذكر.

3) أن يكون من شأن الورقة الصادرة من الخصم أن تجعل التصرف المدعى به قرب الاحتمال، وهو أمر يخضع للسلطة التقديرية للقاضي.

لقد انقسم الفقه فيما يخص تطبيق هذا الاستثناء على المستندات الالكترونية إلى اتجاهين:

– الاتجاه الأول: يرى بأنه في الدول التي لا توجد بها قوانين تعترف بالحجية لهذه المستندات، فإن صدورها يعد قرينة على صدور الكتابة من المدعى عليه، حيث يمكن تكملتها بشهادة الشهود لتصبح دليل كامل.[1]

وفي هذا الإطار هناك من الفقهاء من يرى أن وجود لمعلومات على دعامات الكترونية أو استخراج صورة منها عن طريق الآلة الطابعة يمكن أن يشكل قرينة على صور الكتابة من المدعى عليه، الأمر الذي يمكن أن يضفي عليها مبدأ ثبوت بالكتابة. إلا أن هذا الرأي لا يمكن الأخذ به على إطلاقه.[2]

– أما الاتجاه الثاني: فيرى أن المستندات الالكترونية لا تعد مبدأ ثبوت بالكتابة، لأن الآلة الالكترونية لا تخرج عنها أية مستندات أو نسخ أصلية يمكن تمييزها عن النسخ المستخدمة التي يمكن تكرارها بعدد غير محدو د.

تنص المادة 325 من ق.م.ج على أنه: "إذا كان أصل الورقة الرسمية موجودا، فإن صورتها الرسمية خطية كانت أو فوتوغرافية تكون حجة بالقدر الذي تكون فيه مطابقة للأصل. وتكون الصورة مطابقة للأصل ما لم ينازع في ذلك أحد الطرفين، فإن وقع تنازع ففي هذه الحالة تراجع الصو رة على الأصل، أي أنه في حالة وجود الأصل يمكن اعتبار النسخة الالكترونية نسخة ما لم ينازع بصفة جدية وصريحة أحد الطرفين في ذلك، وفي حالة عدم وجود الأصل يمكن اعتبار السندات الالكترونية ذات حجية قانونية في الإثبات مع فارق وحيد هو إمكانية المطالبة بالمطابقة مع الأصل لأنه لا وجود ورقي له، ولأن الأصل بدوره الكتروني، وبذلك جميع السندات تعد صورا وليست أصولا."[3]

---

[1] –كحول سماح ،مرجع سابق ص.16

[2] – داديار حميد سليمان،مرجع سابق ص.165

[3] – طمين سهيلة، **الشكلية في عقود التجارة الإلكترونية**، رسالة ماجستير في القانون ،تخصص قانون دولي للأعمال ،كلية الحقوق ،مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية ،جامعة مولود معمري ،تيزي وزو ،2011،ص.91

ثانيا: قبول المستندات الالكترونية في حالة عدم إمكانية الحصول على دليل كتابي

نص المادة 336 ق.م.ج على هذه الحالات: "... يجوز الإثبات بالشهود أيضا ففيما يجب إثباته بالكتابة:

- إذا وجد مانع مادي أو أدبي يحول دون الحصول على دليل كتابي.
- إذا فقد الدائن سنده الكتابي لسبب أجنبي خارج عن إرادته."([1])

1- حالة فقدان الدليل الكتابي:

وفقا للفقه الفرنسي فإنه يمكن الاستناد إلى مثل هذا الاستثناء للاستعانة بالمحررات المستنسخة من الوسائط الالكترونية في الحالات التي يكون فيها الوسيط الالكتروني محصنا من التعديل أو التغيير أو حالات اختفاء المعلومات من على الوسيط الالكتروني واعتبار النسخة المطبوعة من الآلة لأصل لم يحفظه أطراف التصرف متى توفرت فيها شروط الأمان والديمومة دليلا كافيا للإثبات.[(2)]

2- حالة وجود مانع من الحصول على دليل كتابي:

يقصد بالمانع هنا، استحالة الحصول على دليل كتابي وقت التعاقد، سواء كانت مقصورة على شخص معين أم ترجع إلى الظروف الخاصة التي يتم فيها التعاقد، أي استحالة نسبية عارضة أو شخصية والمانع قد يكون مادي أو أدبي، أو مانع بحكم العادة.

فيما يخص عقود والمعاملات التي تتم عن طريق الوسائل الالكترونية كالمستند الالكتروني، فإنه يسهل تطبيق الاستحالة المادية، نظرا لاستخدام الوسائط الالكترونية التي يستحيل معها إبرامها بالشكل المتطلب في القواعد التقليدية، أما بالنسبة للاستحالة المعنوية، فإنها تكاد تنتفي باعتبارها عادة ما تكون عقود دولية.([3])

ثالثا: حالة الغش نحو القانون

يقصد بالغش نحو القانون أو كما يسمى بالاحتيال على القانون، تواطؤ المتعاقدين على مخالفة قاعدة قانونية تعتبر من النظام العام، واخفاء هذه المخالفة تحت ستار تصرف مشروع.

---

[1] – الأمر رقم 55-66المتضمن قانون الإجراءات الجزائية،سالف الذكر .

[2] – داديار حميد سليمان،مرجع سابق، ص.157

[3] – طمين سهيلة،مرجع سابق، ص.94

واستنادا إلى ما تقدم، يرى البعض من الفقهاء أنه إذا كان بصدد غش معلوماتي، باعتباره غشا أو تحايلا على القانون فإن قاعدة حرية الإثبات، تخول القاضي أن يستمد قناعته من أي دليل حتى ولو كان متحصلا من استخدام إحدى الوسائل الحديثة في الإثبات، ومنها السندات الالكترونية.[1]

رابعا:موقف المشرع الجزائري

بالنسبة للتشريع والقضاء الجزائري فإن المادة 212 من ق إ ج أعطت للقاضي الحرية في أن يستمد قناعته من أي دليل يطمئن إليه بما في ذلك المحررات

و نستنتج من خلال نص المادة 323 مكرر1 من القانون المدني أن المشرع الجزائري قد اعترف بالحجية القانونية الكاملة للمحررات أو المستندات الالكترونية في الإثبات، ويشترط للاعتداد بها، إمكانية تحديد هوية الشخص الذي أصدرها وأن تكون صادرة ومحفوظة في ظروف تضمن سلامتها. كما أن المشرع الجزائري قد أقر بمبدأ التعادل الوظيفي بين السندات الالكترونية والسندات التقليدية من حيث الأثر والحجية في الإثبات.[2]

وهو ما سار عليه المشرع اللبناني في نص المادة الخامسة حيث نص على أنه: "لا تفقد المعلومات أثرها القانوني أو صحتها أو قابليتها للتنفيذ لمجرد أنها جاءت في شكل رسالة بيانات."

ونصت المادة التاسعة على أنه: في أية إجراءات قانونية، لا يطبق أي حكم من أحكام قواعد الإثبات من أجل الحيلولة دون قبول رسالة بيانات كدليل إثبات، وهو ما يؤكد الاعتراف بحجية المستندات الالكترونية في الإثبات.[3]

كما ذهبت محكمة النقض المصرية إلى أنه يمكن الأخذ بالصورة الضوئية كدليل إثبات أو نفي متى اطمأنت إلى مطابقتها للأصل .

وقد نظم المشرع الجزائري المحررات كدليل من أدلة الإثبات الجزائي في المواد من 214 إلى 218 من قانون الإجراءات الجزائية ،والمبدأ أن المحررات سواء أكانت رسمية أو عرفية ليست لها حجية مطلقة في الإثبات فهي تخضع لتقدير لمبدأ الاقتناع الشخصي للقاضي

[1] – داديار حميد سليمان، مرجع سابق،ص ص.167، 168

[2] – طمين سهيلة،مرجع سابق، ص.110

[3]– محمد نصر محمد، **الدليل الالكتروني وحجيته أمام القضاء** (راسة مقارنة) الطبعة الأولى، دار الكتب العلمية، لبنان، 2013، ص.17

الجزائي،وعليه تجدر الإشارة إلى أن سلطة القاضي الجنائي في تقدير المحررات الرقمية تأخذ نفس الأحكام في حالة المحررات الورقية بصفة عامة كون أن المحررات الرقمية لم يشملها القانون بوضع خاص وما ينطبق على المحررات العادية ينطبق على المحررات الرقمية[1]

المطلب الثالث:

تقييم الأدلة الرقمية المستخلصة من الجرائم الماسة بالمستند الالكتروني

نظرا للطابع الخاص الذي تمتاز به الجريمة المعلوماتية، فقد تبين أن إثباتها تحيط به الكثير من الصعاب، ومما لا شك فيه أن إثبات هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، تختلف عن الأدلة التقليدية.[2]

ولهذا قام المشرع الجزائري بتحديد بعض التدابير التي تهدف إلى اقتفاء أثر الجريمة المعلوماتية، واستخلاص الأدلة الرقمية منها بموجب أحكام القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [3]

وسنتطرق في هذا المطلب إلى مفهوم الدليل الرقمي (الفرع الأول)، ثم تقدير الدليل الرقمي المستخلص من الجرائم الماسة بالمستند الإلكتروني أمام القضاء الجزائي (الفرع الثاني).

الفرع الأول: مفهوم الدليل الرقمي.

يعتبر مصطلح الدليل الرقمي من أهم المصطلحات المتداولة في إطار القانون الجنائي لا سيما عند الحديث عن الإثبات،حيث بدونه لا يمكن إسناد الواقعة إلى المتهم ،وعليه للوصول إلى المقصود بالدليل الرقمي سنتطرق في هذا الفرع إلى :

---

[1]– بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية** أطروحة لنيل شهادة الدكتوراه تخصص قانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2015 ص237

[2]– عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص49.

[3] – يعيش تمام شوقي، ، مرجع سابق، ص40.

أولا : تعريف الدليل الرقمي

ثانيا: أنواع الدليل الرقمي

أولا: تعريف الدليل الرقمي.

يعرف الدليل الالكتروني المستخرج من المستند الالكتروني على أنه " تلك الأدلة التي يمكن الحصول عليها من الحاسوب بإحدى وسائل الإخراج".

وهو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، ,وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور و أشكال و أصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها.

كما عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 بأنه(المعلومات ذات القيمة المحتملة و المخزنة أو المنقولة في صورة رقمية).[1]

وفي نظرة أخرى موسعة تعرف الأدلة الرقمية: (بأنها جميع أنواع البيانات المخزنة أو المرسلة من خلال تكنولوجيا المعلومات والتي تعتمد عليها نظرة إثبات ارتكاب الجريمة، بينما يعرفها دليل الشرطة للأدلة الجنائية في المملكة المتحدة " UK Police and Criminel Evidence Code" بأنها(جميع المعلومات الموجودة في الحاسوب).[2]

ومن خلال هذه التعاريف، يمكن تحديد خاصيتين للدليل الرقمي هما:

– **الخاصية الأولى:** إن الدليل الالكتروني هو عبارة عن معلومات أو بيانات الكترونية مخزنة في الحاسوب أو المنقولة بواسطته، أيا كان شكل هذا الحاسوب، سواء كان حاسوب شخصي، أو مخدم الإنترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية وغيرها.

[1] – شرف الدين وردة، **الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق،ص 06.

[2] – هارون بحرية، **(دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري)** ،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة، كلية الحقوق والعلوم السياسية ،جامعة بسكرة،الجزائر،مابين 16 و 17 نوفمبر،2015 ص02.

- **الخاصية الثانية:** القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم.[1]

ثانيا: أنواع الدليل الرقمي

1- الأدلة الورقية: وهي تلك الأدلة المطبوعة على الورق.

2- الأدلة الإلكترونية الخاصة بأجهزة الحاسوب وشبكاته [2]

وهي تلك الأدلة المتحصل عليها بواسطة الأقراص الممغنطة و الأشرطة المغناطيسية أو غيرها من الوسائط الإلكترونية ومنها وحدت الإدخال ووحدات الإخراج، المعالجة المركزية، التخزين بالإضافة إلى أجهزة المودم و الكروت أو البطاقات PCMIA Cardas والبطاقات الممغنطة[3]

كما يمكننا أن نلمس وجود أنواع أخرى للدليل الالكتروني، تضاف إلى الأنواع السابقة الذكر، والتي تتمثل في:

- التسجيلات الضوئية (شريطة الفيديو الرقمي).

-الصندوق الأسود والذي يتم تركيبه في الطائرات بأنماطها.

- كمبيوتر الجيب، ونقصد بالذكر، الكمبيوتر السفري Lap top و الكمبيوتر الدفتري Net Book.

- البريد الإلكتروني و يستعمل هذا البريد في تداول الأوراق و المستندات التي تكون مرفقة بالرسالة الإلكترونية.

- التوقيع الإلكتروني، و منها التوقيع البيومتري والتوقيع بالقلم الإلكتروني Pen-op [4]

---

[1]- شرف الدين وردة ، **الإثبات الجنائي بالأدلة الإلكترونية**،المرجع سابق، ص 07.

[2]- خالد عباد الحلبي، خالد عياد الحلبيإجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت،الطبعة الأولى،دار الثقافة ،الأردن،2011، ص 233.

[3]- شرف الدين وردة،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص ص14،13.

[4]- المرجع نفسه، ص 14.

في سنة 2007 استحدثت بمخابر الشرطة العلمية الكائن مقرها بالجزائر العاصمة ووهران و قسنطينة أقسام متخصصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة الكترونية قصد استخراج وتتبع ما من شأنه أن يفيد في التحقيق ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هاذ النوع، وأهم هاته الأجهزة المستغلة من طرف الأقسام المختصة في الأدلة الرقمية : أدوات التخزين الرقمية (أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة... الخ).[1]

و من الأمثلة عن الأدلة الرقمية نذكر، البروتوكول (TPC/IC) وهو في الواقع يضم بروتوكولين مستقلين في شبكة الانترنت هما بروتوكول TCP و بروتوكول IP حيث يعملان معا وبشكل متزامن.[2]

الفرع الثاني: تقدير الدليل الرقمي المستخلص من الجرائم الماسة بالمستند الإلكتروني أمام القضاء الجزائي

تعد مرحلة المحاكمة من أهم إجراءات الدعوى باعتبارها مرحلة حاسمة، إذ تعتبر عملية تقدير الأدلة جوهر الحكم وليس باستطاعة القاضي إدراك الدليل و الوصول إليه إلا بعد ممارسة سلطته التقديرية للأدلة محل الوقائع فتتوقف سلامة الحكم على سلامة تقدير الأدلة، ويعتبر الدليل الرقمي كباقي الأدلة يتم تقديره من طرف القاضي الجنائي، غير أنه لايستطيع هذا الأخير أن يقوم بتقدير هذا الدليل إلا إذا كانت المحكمة المرفوع أمامها الدعوى صاحبة الاختصاص بالفصل في الجريمة المعلوماتية.

أولا: شروط قبول الدليل الرقمي

حتى يتحقق الدليل اللازم للإثبات فإنه لابد من أن تتوفر فيه شروط تجعل له حجية وقيمة يثبت بها الحق.[3]

[1] – حملاوي عبد الرحمان، مرجع سابق، ص 07.

[2] – ناني لحسن، مرجع سابق، ص 77.

[3] – معتوق عبد اللطيف، مرجع سابق، ص 119.

1- شرط مشروعية الدليل الرقمي:

يشترط في الدليل الرقمي الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة [1]

ووفقا للأمانة والنزاهة ذلك أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول، لأن محل الحرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة [2] و أن لا يتحصل عليه من أدلة غير مشروعة كالإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة وهو ما ذهب إليه المشرع الجزائري، إذ عبر صراحة في نص المادة 160 من ق، إ، ج على استبعاد الأدلة الغير مشروعة و بالتالي فإن الأدلة الرقمية غير المشروعة تستبعد ولا يؤخذ بها استنادا إلى القواعد العامة [3].

2- شرط مناقشة الدليل الرقمي المستخرج من المستند الإلكتروني:

نصت المادة 212/ الفقرة 02 من ق، إ، ج، ج على أنه (ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه) [4].

و يستوي الأمر بالنسبة للأدلة الرقمية سواء كانت في شكل مخرجات ورقية أو الكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به، فيجب أن تعرض للمناقشة أثناء المحاكمة بوصفها أدلة إثبات، وللقاضي الجزائي الحرية في أن يستمد قناعته منها طالما أن لها ووقعت عليها المرافعات وناقشها أطراف الدعوى، ويترتب على هذه القاعدة شرطان أساسين هما:

أ)وجوب مناقشة الدليل الالكتروني بين أطراف الدعوى.

---

[1]- خالد عياد الحلبي، مرجع سابق، ص 238.

[2]-عائشة بن قارة مصطفى، مرجع سابق، ص 268.

[3]-بحرية هارون، مرجع سابق، ص، 13.

[4] -الأمر رقم 155-66 المتضمن قانون الإجراءات الجزائية سالف الذكر.

ب) الضوابط المتعلقة بالاقتناع القضائي: إذ أن سلطة القاضي الجزائي في تقديم الأدلة الرقمية وموازنتها وفقا لما يمليه وجدانه لا يخضع في ذلك لرقابة المحكمة العليا إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين من غير أن يكون هذا الاقتناع مخالفا لمقتضيات العقل و المنطق السليم [1].

3- شرط يقينية الأدلة الإلكترونية:

يشترط في الأدلة المستخرجة من المستند الالكتروني أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا يمكن دحض قرينة البراءة و افتراض عكسها إلا عندما يصل القاضي الجزائري لحد الجزم و اليقين [2]

فشرط اليقين في أحكام الإدانة هو شرط عام، حيث أنه سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة كالدليل الرقمي، لذلك أن يكون الدليل الرقمي غير قابل للشك، إذ أن هذا الأخير يفسر لصالح المتهم استنادا إلى قاعدة أن الأصل في الإنسان البراءة، فيكفي أن يشكك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة [3].

و القاضي لكي يصل إلى يقينية الأدلة الرقمية المجسدة. بمخرجات الكمبيوترية لابد من تطلب نوعين من المعرفة، أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه المخرجات وتفحصها وثانيهما المعرفة العقلية عن طريق التحليل و الاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها [4].

وهذا خاصة مع التحديات المحلية التي تواجه مكافحة الجريمة المعلوماتية والتي من بينها:

- زيادة عدد المشتركين في شبكة الإنترنت (أكثر من 10 ملايين مشترك بالجزائر)، انتشار تكنولوجيا الإنترنت فائق السرعة APSL. SDSL. VSAT

---

[1]- بحرية هارون، مرجع سابق، ص ص ، 13 ،14 ،15.

[2]- شرف الدين وردة ،**الإثبات الجنائي بالأدلة الإلكترونية**،مرجع سابق ص 43.

[3]- عائشة بن قارة مصطفى، مرجع سابق ،ص 277.

[4]-بحرية هارون،مرجع سابق ص ص15، 16

– التطور التكنولوجي وظهور الانترنت اللاسلكي wifi , 3G , 4G.[1]

لم يخص المشرع الجزائري نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملا بنص المادة 212،م ق إ ج ما يجعلها مقبولة نظريا .[2]

ومنه تبقى مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة،ولهذا يترك للقاضي الجنائي حرية تقدير الأدلة الجنائية وتكوين قناعته ،ويبني حكمه على أي دليل متى أطمأن إليه ولو كان مستمد من محاضر الاستدلالات .[3]

ويتأكد ذلك من خلال تناول المشرع الجزائري في القانون 04/09،طرق حديثة للاستخلاص الأدلة الرقمية منها المراقبة الإلكترونية والتفتيش المعلوماتي ثم الضبط المعلوماتي،وهي إجراءات ذات بعدين أولاها للوقاية من الجرائم المعلوماتية وثانيها لمكافحة الجريمة وذلك بضبط الأدلة الرقمية .

فبعد الإطلاع على نص المادة 6 من القانون 04/09 نجد أن المشرع الجزائري تحدث عن حجز المعطيات المفيدة في كشف الجرائم أو مرتكبيها بعد أن يتم نسخ المعطيات على دعامة تخزين وحرزها وهي شكل من أشكال الأدلة الرقمية كما سبق بيانه ،فالمشرع هنا يقصد الأدلة الرقمية [4]

و لو أنه لم يسميها إلا أنه يحرص على تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى .[5]

وأيضا بالرجوع إلى نص المادة 341 ق ع الجزائري وبالضبط في مصطلح الرسالة أو المستند هل المقصود بهما ما ورد على الشكل التقليدي أي على الكتابة المحمولة على الدعامة الورقية فقط ؟

---

[1] عزالدين عزالدين،مرجع سابق ،ص 05

[2] – بحرية هارون،مرجع سابق، ص 10

[3] – سعيداني نعيم ،مرجع سابق، ص ص 213.214

[4] – بحرية هارون،مرجع سابق ص 11

[5] – ناني لحسن،مرجع سابق، ص 116

من المعلوم بأن الرسالة قد تكون رسالة إلكترونية كما أن مصطلح المستند قد يحمل صور ومقاطع فيديو محمول على دعامة رقمية،وبما أن المشرع لم يقيد مصطلحي الرسالة والمستند بالدعامة الورقية فلماذا لا يعتد بالدليل الرقمي الذي يكون مثلا عبارة عن رسالة رقمية وجدت في البريد الإلكتروني للمتهم أو شريكه أو عبارة عن فيديو وصور تظهر جريمة الزنا وجدت في البريد الإلكتروني للمتهم وجدت في حيازته في دعائم إلكترونية مثل أقراص أو اسطوانات ممغنطة ،يضاف إلى هذا أن التطور الحاصل جعل المجتمع بصفة عامة والمجرمين بصفة خاصة يتفادون الكتابة كونها وسيلة سهلة الاكتشاف عن طريق مضاهاة الخطوط،يضاف إلى هذا أن الرسائل الورقية ناقصة الدلالة بالمقارنة مع المحررات والمستندات الإلكترونية التي تعبر عن الواقعة مثل حدوثها (فيديو رقمي) [1]

مما يعني أن المشرع الجزائري تبنى الأدلة الرقمية لكن بدون تسمية صريحة .وصفوة القول أن مبدأ قبول الأدلة الرقمية يجد له أساس في قانون الإجراءات الجزائية في باب طرق الإثبات أين ترك المجال مفتوحا لقبول أي دليل من شأنه إثبات الجريمة تطبيقا لمبدأ حرية الإثبات لذلك لم يجد المشرع حرجا لما وضع نصوص القانون 04/09 وجاءت خالية من ذكر الدليل الرقمي شأنه في ذلك شأن الأدلة العلمية الأخرى مثل ألADN....الخ [2]

[1]– بن فردية محمد ،مرجع سابق،ص281

[2]– بحرية هارون،مرجع سابق ص 11

الخاتمـــة

يعد موضوع الحماية الجزائية للمستند الإلكتروني من المواضيع الحديثة والتي تتعلق بالإطار القانوني للتعاملات الإلكترونية فلقد ساهمت المعلوماتية في تحويل المستندات الورقية إلى مستندات إلكترونية، حيث أصبح المستند الإلكتروني الأداة الأساسية لتنفيذ فكرة الحكومة الإلكترونية، والتجارة الإلكترونية.

وللإجابة عن الإشكالية المطروحة فلقد توصلنا إلى **مجموعة من النتائج:**

1- لمشرع الجزائري لم يقم بتعريف المستند الإلكتروني، لكنه لم يكن بمنأى عن التطور الحاصل في الإثبات بالكتابة الإلكترونية في القانون المدني إذ أعطى للكتابة الإلكترونية نفس الحجية التي تتمتع بها الكتابة التقليدية،و من خلال الفقرة (ا) والفقرة (ج) من المادة 2 من القانون رقم 09-04، أشار المشرع الجزائري إلى المستند الإلكتروني كجزء من المنظومة المعلوماتية، وبالتالي كل جريمة تقليدية تقع على مستند ترتكب بواسطة منظومة معلوماتية أو نظام اتصالات وفقا لهذه المادة تصبح جرائم ماسة بالمستند الإلكتروني.

2- المستند الإلكتروني هو عبارة عن وسيط إلكتروني، والذي هو كل شئ مادي متميز لقرص صلب أو مضغوط أو شريط ممغنط أو خلافه، يتضمن معلومات، معالجة إلكترونيا، ومكتوب وموقع عليها بطريقة إلكترونية، تكون قابلة للحفظ دون تلفها أو إحداث تغييرات عليها ويمكن الرجوع إليها في أي وقت مع إمكانية تحويله لمستند ورقي عن طريق إخراجه من مخرجات الكمبيوترية.

3- لا يمكن للمستند الإلكتروني أن يؤدي وظيفته مثل المستند الورقي إلا إذا توافرت فيه الشروط الفنية والتقنية والتي هي الكتابة الإلكترونية، التوقيع الإلكتروني، التوثيق أو التصديق الإلكتروني، بالإضافة إلى سلامة المحتوى.

4- تتمثل خصائص المستند الإلكتروني في أنه يتم إعداده على كيان معنوي، وأنه يؤدي إلى السرعة والائتمان في إبرام المعاملات، فضلا عن ذلك فإن المستند الإلكتروني يمتاز بالسرية وضمان الأمن القانوني، كل هذه الخصائص تجعله يتميز عن المستند التقليدي،وهذا لكونه يحمل الصفة الإلكترونية الافتراضية.

5- فيما يتعلق بالحماية الجزائية الموضوعية للمستند الإلكتروني، تبين أن قانون التجارة الإلكترونية رقم 18-05 المؤرخ في 10 مايو 2018،لم ينص على تجريم الجرائم

الواقعة على المعاملات الإلكترونية بما فيها المستند الإلكتروني، ذات الطابع الإفتراض كالتزوير الإلكتروني، جريمة الاحتيال الإلكتروني، لجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة المرتكبة بواسطة تقنية المعلومات، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكتروني...على غرار التشريعات العقابية الأخرى، بالرغم من انظمام الجزائر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252، والتي نصت في المادة 5 بالفصل الخاص بالتجريم على ضرورة أن تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقا لتشريعاتها وأنظمتها الداخلية.

وعليه تطبق في الجزائر على الجرائم الواقعة على المعاملات الإلكترونية بما فيها المستندات الإلكترونية، النصوص العقابية لقانون العقوبات والقوانين المكملة له، بالرغم من ثبوت فقهيا وقانونيا عدم كفاءة وملائمة النصوص التقليدية لمكافحة هذا النوع المستحدث من الجرائم التي جاءت لمكافحة الجرائم العاديةذات الطبيعة المادية وليست الجرائم ذات الطبيعة غير المادية، مما قد يؤدي في الكثير من القضايا إلى إفلات المجرمين من العقاب عملا بمبدأ الشرعية لعدم انطباق الجرائم المعلوماتية مع الجرائم العادية بأركانها المادية والشرعية والمعنوية. أما المواد المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 7 قانون عقوبات فجاءت لمكافحة جرائم الماسة بأنظمة المعالجة الآلية للمعطيات أي الجرائم التي تمس المعطيات الموجودة داخل المنظومة المعلوماتية وليس المعطيات الموجودة خارجا والمنفصلة علن المنظومة المعلوماتية كالأقراص المرنة والممغنطة والتي يمكن أن تقع عليها جرائم متنوعة كالتزوير والسرقة والإتلاف...

6-رغم اعتراف المشرع الجزائري لبرامج الإعلام الآلي وقواعد البيانات بصفة المصنف المحمي، إلا أنه لا يخفى علينا أن الحماية الجزائية للمستند الإلكتروني من خلال حق المؤلف، تنصب بصفة أساسية على شكل المستند أو مضمونه الإبتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج، وبالتالي فإن قانون الملكية الفكرية ولو أنه يساعد في حماية بعض جوانب المستند فهو قاصر عن تغطية كل الاعتداءات عليه.

7-خص المشرع الجزائري، التوقيع الإلكتروني بحماية جنائية خاصة وهذا من خلال إصداره للقانون رقم 15-04 المؤرخ في 01 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

8- تضمن القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، المتعلق بالتجارة الإلكترونية الجديد،بعض الجرائم التي تمس بالتجارة الإلكترونية والعقوبات المقررة لها ،لكنه لم ينص على المستند الإلكتروني بشكل صريح.

9- بالنسبة للحماية الجزائية الإجرائية للمستند الإلكتروني فالملاحظ أن المشرع الجزائري قد عمل على تطوير أساليبالتحري والتحقيق واجرائته فيما يخص مكافحة جرائم لماسة بأنظمة المعالجة الآلية للمعطيات لتتلاءم مع خصوصية هذه الجرائم وذلك من خلال،**التعديل في قانون الإجراءات الجزائية** بسن أحكام استثنائية تضاف للأحكام العامة المنظمة لكل إجراء، و**من خلال إصدار القانون رقم 09-04**، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها فظهر ما يسمى بالتفتيش والضبط والمعاينة في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وما يتميز به بأحكام خاصة واستثنائية عن التفتيش في الجرائم العادية، تفتيش المنظومات المعلوماتية، حجز المعطيات المعلوماتية. كما سن المشرع الجزائري أحكام خاصة وحديثة للتحري والتحقيق في الجرائم المعلوماتية منها جرائم الماسة بالمستند الإلكتروني كاعتراض المراسلات السلكية واللاسلكية، التسرب، مراقبة الاتصالات الإلكترونية، جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، حفظ المعطيات المتعلقة بحركة السير.

10-إن البعد الإجرائي للجرائم المعلوماتية، ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسية ،الحاجة إلى سرعة الكشف خشية ضياع الدليل، وقانونية وحجية الأدلة المستقاة من بيئة معلوماتية،وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي.

11- المستند الإلكتروني يمثل محرر له قوة إثبات قانونية والاعتراف بتلك الحجية يؤدي إلى استمرار المعاملات الإلكترونية وزيادة الثقة فيها، وحتى يتمتع المستند الإلكتروني بتلك الحجية لا بد من توفر شرط مشروعية إجراءات التحري والتحقيق في الحصول على الدليل الرقمي، ضرورة مناقشة الأدلة الرقمية المتحصل عليها من ارتكاب جرائم الماسة

بالمستند الإلكتروني بالجلسة، وأن يخضع تقييم ذلك الدليل الرقمي إلى تقدير القاضي الجزائي بأن يصل في تقديره واقتناعه به إلى درجة اليقينية .

12 – بالرغم من علمية الوسائل المستعملة في التحري والتحقيق للحصول على الدليل الرقمي المثبت لقيام جرائم ماسة بالمستند الإلكتروني، والتي تقترب إلى درجة الدقة العلمية القطعية، إلا أن تقدير هذا الدليل يخضع لاقتناع الشخصي للقاضي الجنائي مثله مثل كل الأدلة المادة المثبتة لقيام جريمة واقعة على المحررات الرسمية أو العرفية.

13–لم يخص المشرع الجزائري نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملا بنص المادة 212، م ق إ ج ما يجعلها مقبولة نظريا.

ومنه تبقى مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، ولهذا يترك للقاضي الجنائي حرية تقدير الأدلة الجنائية وتكوين قناعته، ويبني حكمه على أي دليل متى أطمأن إليه ولو كان مستمد من محاضر الاستدلالات.

وفي الأخير نقترح على المشرع الجزائري إدخال التوصيات التالية:

1–أن ينظم المشرع الجزائري حماية جنائية موضوعية كافية للمستند الإلكتروني، من خلال **النص على الجرائم الواقعة عليه والتي تتلائم مع الطبيعة غير المادي لهذه المستندات** كالتزوير الإلكتروني، جريمة الاحتيال الإلكتروني، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة المرتكبة بواسطة تقنية المعلومات، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكتروني...على غرار التشريعات العقابية الأخرى، وتنفيذا لالتزاماته الدولية من خلال مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، وذلك من خلال سن **قانون خاص بالجرائم المعلوماتية ينص ضمنه على الجرائم الواقعة على المستندات الإلكترونية**، أو **من خلال التعديل في نصوص التجريم الخاصة بالجرائم التقليدية بإضافة عبارة "أو المرتكبة بواسطة تقنية المعلومات"**، على نحو تشمل الأحكام المنظمة لها الجرائم المعلوماتية منها الجرائم الواقعة على المستند الإلكتروني، كما هو الحال بالنسبة للتشريع الألماني الذي أضاف إلى باب التزوير نصوصا خاصة بتزوير المستند الإلكتروني. أو من خلال النص على الجرائم الماسة بالمستند الإلكتروني ضمن **قانون**

التجارة الإلكترونية رقم 18- 05. مع ضرورة تشديد عقوبات الجرائم المرتكبة بواسطة تقنية المعلومات نظرا لما تخلفه مساس بالاقتصاد القومي والدفاع الوطني والنظام العام للدول

2- وضع إجراءات خاصة أكثر دقة للتحقيق والمحاكمة للجريمة المعلوماتية تختلف عن الجريمة التقليدية

3- ضرورة التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية، وذلك لان نظرا لخطورة هذه الجرائم العابرة للحدود الوطنية، ونظرا لن الدليل الرقمي قد يتواجد بإقليم دولة أخرى مما يصعب الحصول عليه وبالتالي ضياعه وافلات المجرمين من العقاب.

4- التطوير المستمر في النصوص الجزائية الموضوعيةوالإجرائية مع التطور السريع للجريمة المعلوماتية وظهور أشكال جديدة لها وسبل ارتكابها.

ويبقى مجال البحث في هذا النوع منالدراسات مفتوحا على الدوام نظرا للوتيرة المتسارعة لتطور الجريمة المعلوماتية.

"إذا اجتهد العالم فأصاب فله أجران وان اجتهد وأخطأ فله أجر"

قائمة المصادر والمراجع

أولا : المصادر

أ / القوانين والأوامر :

1- الأمر رقم 75-85 المتضمن القانون المدني،المؤرخ في 16سبتمبر1975،المعدل والمتمم بالقانون رقم 07-05المؤرخ في13مايو2007

2- القانون رقم 66-156، المؤرخ في 8 يونيو 1966،المتضمن قانون العقوبات الصادر في (ج ر،العدد 49،المؤرخة في 11-06-1966)،المعدل والمتمم بالقانون رقم 16-02، المؤرخ في 19 يونيو 2016،الصادر بالجريدة الرسمية ،العدد 37،المؤرخة في 22 يونيو 2016.

3- الأمر رقم 66-155المؤرخ في 8 يونيو سنة 1966المتضمنقانون الإجراءات الجزائية ،المعدل والمتمم بالأمر رقم 02-15 المؤرخ في 23 جويلية 2015،(ج ر،رقم 40،الصادرة بتاريخ 23 جويلية 2015).

4- القانون رقم 15-04، المؤرخ في 11 ربيع الثاني عام 1436،الموافق ل01،فيفري،2015،المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين ،(ج ر،العدد06)

5- الأمر رقم 03-05،المؤرخ في 19يوليو،2003،المتعلق بحق المؤلف والحقوق المجاورة (ج ر،العدد 44،المؤرخة في 23يوليو2003)

6- القانون رقم 04/09 المؤرخ في 05 أوت 2009،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،(ج ر،العدد 47) المؤرخة في 16 أوت 2009

7- القانون رقم 07/17،المؤرخ في 27 مارس، سنة 2017،يعدل ويتمم الأمر رقم 66-155،المؤرخ في 8 يونيو،سنة 1966والمتضمن قانون الإجراءات الجزائية (ج ر،العدد 20)الصادرة في 29 مارس،سنة 2017.

8- القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018،المتعلق بالتجارة الإلكترونية(ج ر،العدد28)المؤرخة في 30 شعبان 1439 الموافق 16 مايو سنة 2018.

ب /المراسيم :

9-المرسوم الرئاسي رقم 261-15المؤرخ في 08أكتوبر سنة 2015،يحدد تشكيلة وتنظيم وكيفيات ،سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ،(ج ر ،العدد 53)،الصادرة في 8 أكتوبر 2015

ثانيا :المراجع

أ/ الكتب:

1- أحسن بوسقيعة ،الوجيز في القانون الجزائي الخاص، الجزء الأول،دار هومة ،الجزائر2008

2- آمال قارة ،الحماية الجزائية للمعلوماتية في التشريع الجزائري،الطبعة الأولى،دار هومة للنشر والتوزيع،الجزائر 2006

3-أحمد فتحي سرورالوسيط في قانون الإجراءات الجزائية،دار النهضة،القاهرة،1981

4- إيهاب فوزي السقاجريمة التزوير في المحررات الإلكترونية،دار الجامعة الجديدة للنشر،الإسكندرية ،2002

5- دردوس مكي،القانون الجنائي الخاص في التشريع الجزائري،الجزء الثاني،ديوان المطبوعات الجامعية ،قسنطينة،2007

6- داديار حميد سليمان ،دور السندات المستخرجة عن طريق الأنترنت لإثبات المسائل المدنية،(راسة تحليلية مقارنة)،دار الكتب القانونية،دار شتات للنشر والبرمجيات،مصر2010

7-هدى حامد قشقوش،جرائم الحاسب الإلكتروني في التشريع المقارن،دار النهضة العربية،القاهرة

8- لورنيس محمد عبيدات،إثبات المحرر الإلكتروني،دار الثقافة،عمان،2009

9- محمد أمين الرومي،المستند الإلكتروني، الطبعة الأولى، دار الفكر الجامعي،الإسكندرية،2007.

10- محمد أمين الشوابكة،جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن،2007

11- محمد نصر محمد،الدليل الإلكتروني وحجيته أمام القضاء(راسة مقارنة) الطبعة الأولى،دار الكتب العلمية ، لبنان،2013.

12- محمد خليفة،الحماية الجنائية للمعطيات الحاسب الآلي،(في القانون الجزائري والمقارن) دار الجامعة الجديدة،الإسكندرية،2007

13- ناني لحسن ،التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية،(بين النصوص التشريعية والخصوصية التقنية)،النشر الجامعي الجديد،تلمسان ،الجزائر،2017

14- نبيل صقر،مكري نزيهة،الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية،دار الهدى،الجزائر،2009

15- نجيمي جمال،قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، دار هومة، الجزائر، 2015،

16- عائشة بن قارة مصطفى،حجية الدليل الإلكتروني في مجال الإثبات الجنائي،دار الجامعة الجديدة،الإسكندرية،مصر،2010

17- عبد الفتاح بيومي حجازي،التجارة الإلكترونية وحمايتها القانونية،دار الكتب القانونية،مصر2007

18- عبد الفتاح بيومي حجازي،مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي،الطبعة الأولى،دار النهضة العربية،مصر،2009

19- عبد الفتاح بيومي حجازي،مبادئ الإجراءات الجنائية في جرائم الكومبيوتر،الطبعة الأولى،دار الفكر الجامعي،الإسكندرية،2006

20- علي عدنان الفيل،إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية ،(راسة مقارنة)،المكتب الجامعي الحديث.

21- عبد الرحمان خلفي، عبد الرحمان خلفي،الإجراءات الجزائية في التشريع الجزائري والمقارن،الطبعة الثانية،دار بلقيس ،الجزائر،2016

22- عباس العبودي،تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها،الطبعة الأولى،منشورات الحلبي الحقوقية،بيروت،لبنان2010

23- علي عبد القادر القهوجي،الحماية الجنائية لبرامج الحاسب الآلي ،دار الجامعة الجديدة،الإسكندرية،2010

24- عابد فايد عبد الفتاح، الكتابة الإلكترونية في القانون المدني، بين التطور التقني والأمن التقني،دار الجامعة الجديدة، الإسكندرية، 2014

25- فوزية عبد الستار، شرح قانون العقوبات،القسم الخاص، دار النهضة العربية،القاهرة،1990

26- خثير مسعود،الحماية الجنائية لبرامج الكومبيوتر،دار الهدى،الجزائر،2010

27- خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني،المركز القومي للإصدارات القانونية،الطبعة الأولى،(د،م،ن)2009

28- خالد عياد الحلبي،إجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت،الطبعة الأولى،دار الثقافة ،الأردن،2011

29-ضياء مصطفى عثمان،السرقة الإلكترونية،الطبعة الأولى،دار النفائس،الأردن .

ب/الرسائل الجامعية :

- **أطروحات الدكتوراه:**

1- إلهام بن خليفة ،الحماية الجنائية للمحررات الإلكترونية من التزوير،أطروحة دكتوراه،في العلوم القانونية والإدارية،تخصص قانون جنائي،كلية الحقوق والعلوم السياسية،جامعة باتنة،2016

2-براهمي حنان ،جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية،أطروحة دكتوراه،تخصص قانون جنائي،كلية الحقوق والعلوم السياسية،جامعة بسكرة 2015

3- بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه تخصص قانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2015

4- حفصي عباس،جرائم التزوير الإلكترونية(راسة مقارنة)أطروحة دكتوراه في العلوم الإسلامية،جامعة أحمد بن بلة،وهران1 ،2015

5-صالح شنين، الحماية الجنائية للتجارة الإلكترونية،(راسة مقارنة)رسالة دكتوراه في القانون الخاص،كلية الحقوق،جامعة تلمسان 2013

6- شرف الدين وردة، الإثبات الجنائي بالأدلة الإلكترونية (راسة مقارنة)أطروحة دكتوراه علوم في الحقوق،تخصص قانون العقوبات والعلوم الجنائية،كلية الحقوق والعلوم السياسية،جامعة محمد خيضر ،بسكرة 2017

- **رسائل الماجستير:**

7- طعباش أمين،الحماية الجنائية للمعاملات الإلكترونية،مذكرة ماجستير في العلوم القانونية،تخصص علم الإجرام وعلم العقاب،كلية الحقوق والعلوم السياسية ،جامعة باتنة2013

8- طمين سهيلة،الشكلية في عقود التجارة الإلكترونية،رسالة ماجستير في القانون،تخصص قانون دولي للأعمال،كلية الحقوق،جامعة مولود معمري،تيزي وزو2011

9- لالوش راضية،أمن التوقيع الإلكتروني،مذكرة ماجستير ،تخصص قانون دولي للأعمال،كلية الحقوق ،جامعة مولود معمري تيزي وزو2012

10- معتوق عبد اللطيف،الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن،مذكرة ماجستير في العلوم القانونية،تخصص قانون جنائي،جامعة باتنة 2012

11- ميساء مصطفى بركات،جرائم التعدي على المعلوماتية (الإتلاف والتزوير)،رسالة ماجستير ،كلية الحقوق والعلوم السياسية،جامعة بيروت،لبنان 2009

12- سعيداني نعيم،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،مذكرة ماجستير في العلوم القانونية ،تخصص علوم جنائية،كلية الحقوق والعلوم السياسية ،جامعة الحاج لخضر ،باتنة ،2013

13- صغير يوسف،الجريمة المرتكبة عبر الانترنت ،مذكرة ماجستير في القانون ،تخصص قانون دولي للأعمال،كلية الحقوق والعلوم السياسية،جامعة مولود معمري، تيزي وزو 2013

- **مذكرات الماستر**

14-كحول سماح،حجية الوسائل التكنولوجية في إثبات العقود التجارية،مذكرة ماستر في القانون العام للأعمال،كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ، ورقلة،2015

- **ج/ المقالات**

1- العربي شحط محمد الأمين،قراءة الأحكام الجديدة للقضاء الجنائي في قانون الإجراءات الجزائية) مجلة دفاتر السياسة والقانون،العدد الثامن عشر، جامعة وهران 2، 18جانفي 2018

2- بومعيزة جابر،(الاعتداء على المعطيات الآلية في الحكومة الإلكترونية) مجلة البحوث والدراسات القانونية والسياسية،العدد الثاني عشر،كلية الحقوق والعلوم السياسية،جامعة البليدة2

3-براهمي حنان،(المحررات الإلكترونية كدليل إثبات) مجلة المفكر،العدد التاسع،كلية الحقو ق والعلوم السياسية،جامعة محمد خيضر ،بسكرة .

4-فتيحة حزام،(النظام القانوني للفيروس المعلوماتي)مجلة جامعة الجزائر1،العدد الواحد والثلاثين،كلية الحقوق،جامعة أمحمد بوقرة،بومرداس.

5-راضية مشري،(لحماية الجزائية للمصنفات الرقمية في ضل قانون حق المؤلف) مجلة التواصل في العلوم الإنسانية والاجتماعية،العدد أربعة وثلاثون،كلية الحقوق،جامعة 8 ماي1945،قالمة،جوان 2013.

6-شرف الدين وردة (مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية،في التشريع الجزائري) مجلة المفكر، العدد الخامس عشر، كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر بسكرة،15 جوان 2017.

د/ البحوث والملتقيات العلمية :

1-بحرية هارون، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة،كلية الحقوق ولعلوم السياسية،جامعة بسكرة،الجزائر،مابين 16و17 نوفمبر 2015

2-حسونة عبد الغني،جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة،كلية الحقوق والعلوم السياسية،جامعةبسكرة،الجزائر،مابين 16و17نوفمبر 2015

3-حملاوي عبد الرحمان،دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة،جامعة بسكرة،الجزائر،مابين 16و17 نوفمبر 2015 .

4-محمد أبو العلا عقيدة ،التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية،بحث مقدم لأعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية،كلية الحقوق،أكاديمية شرطة دبي،الإمارات،في 26 نيسان،2003

5-عز الدين عز الدين ،الإطار القانوني في الجرائم المعلوماتية ومكافحتها،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية،كلية الحقوق والعلوم السياسية،جامعة بسكرة ،الجزائر،مابين156و 17 نوفمبر 2015

6-رضا هميسي،أحكام الشاهد في الجريمة المعلوماتية،بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية،بين الوقاية والمكافحة،كلية الحقوق والعلوم السياسية،جامعة بسكرة،الجزائر،مابين 16و 17 نوفمبر 2015.

7-ربيعي حسين،الأساليب التقنية الحديثة لارتكاب الجرائم المعلوماتية،بحث مقدم لأعمال الملتقى الوطني،حول الجريمة المعلوماتية،بين الوقاية والمكافحة،كلية الحقوق والعلوم السياسية،جامعة بسكرة،الجزائر،مابين 16و17نوفمبر 2015.

هـ/المحاضرات :

1 - يعيش تمام شوقي،محاضرات في مقياس جرائم المعلومات،(غير منشورة)،ألقيت على طلبة السنة الثانية ماستر جنائي،خلال السداسي الثالث،كلية الحقوق والعلوم السياسية،جامعة بسكرة2018/2017

و/ مواقع الانترنت :

1- أشرف توفيق شمس الدين، **الحماية الجنائية للمستند الإلكتروني** (راسة مقارنة) ،بحث منشور على شبكة الإنترنت من خلال الموقع الإلكتروني http://www,arabawifo.com (الدليل الإلكتروني للقانون العربي)، بتاريخ 2017/12/05 على الساعة 15:00.

فهرس المحتويات

ملخـــص :

إن التطور الذي تعرفه تكنولوجيا الاتصالات في الآونة الأخيرة أدى إلى استحداث وسيلة جديدة تعرف، بالمستند الإلكتروني،خاصة بإثبات المعاملات والعقود التجارية التي تبر م عن طريق الوسائل الإلكترونية ،وأصبحت هاته الوسيلة تحتل أهمية كبيرة في مجال المعاملات الإلكترونية نظرا لأنها تقوم في كثير من الأحيان بأداء وظائف الوسائل التقليدية

وترتب عن الأهمية المتزايدة للمستندات الإلكترونية عدة مخاطر تقع عليها كالقيام بتزويرها مثلا،على نحو يهدد الثقة العامة فيها، مما جعل المشرع الجزائري،يتجه نحو ضرورة توفير حماية جزائية،موضوعية واجرائية للمستند الإلكتروني،سواء في إطار نصوص عامة في قانون العقوبات أو في إطار نصوص خاصة.

وطالما أن المشرع الوطني، مازال لم يضع قواعد قانونية تنظم المعاملات الإلكترونية، بشكل مستقل وقائم بذاته،فإن الحماية الجزائية للمستند الإلكتروني في هذا الإطار تبقى قاصرة وغير كافية .

Résumé

le développement que connais la technologie des communication a conduit a la création d'une nouvelle méthode appelle le dossier électronique relatif aux transactions et aux contrats commerciaux établîtes par les moyens électroniques .Ce moyen occupe une place tres importante dans le domaine des opérations électroniques ,parce qu'il joue ,la plupart des temps , le rôle des outils traditionnels

cette importance croissante des dossiers électroniques implique des risques ex : le fraude... . Ces risques . menacent en premier lieu la confidentialité de cette importance ,ce qui mène le législateur Algérien a prévoir une indispensable protection pénale , formelle et procédurale du dossier électronique, soit dans le cadre des textes généraux des lois . . pénaux , soit dans le cadre des textes spéciaux

tant que le législateur national n'a pas encore mis au point des normes juridiques qui ordonne les transactions électroniques d'une manière indépendante et autonome la protection pénale du dossier électronique . reste limitée et insuffisante