

جامعة عبد الحميد بن باديس مستغانم

المرجع: سجل رقم 07

كلية الحقوق و العلوم السياسية

قسم: القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الحماية الجنائية للمستند الالكتروني

ميدان الحقوق و العلوم السياسية

التخصص: قانون جنائي وعلوم جنائية

تحت إشراف الأستاذ(ة):

بوكر رشيدة

الشعبة: الحقوق

من إعداد الطالب:

بلعيشة علي

أعضاء لجنة المناقشة

رئيسا

بوسجة جيلالي

: الأستاذ(ة)

مشرفا مقرا

بوكر رشيدة

: الأستاذ(ة)

مناقشا

بوزيد خالد

: الأستاذ(ة)

السنة الجامعية: 2019/2018

نوقشت يوم: 2019/06/27

بسم الله الرحمن الرحيم

﴿يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات﴾

صدق الله العظيم

سورة المجادلة الآية 11.

* إهداء *

بسم الله الرحمن الرحيم

﴿ وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنون ﴾

صدق الله العظيم

والصلاة والسلام على سيد البشرية محمد (ص) وعلى اله وصحبه أجمعين

وبعد: أتقدم بإهدائي هذا:

إلى سبب وجودي في هذه الحياة أبي العزيز أطل الله في عمره

إلى التي تعبت في تربيتي وتعليمي أمي الحبيبة، إلى أحبائي إخواني وأخواتي،

إلى فلذة كبدي ابنتي سيرين في الحياة الدنيا، إلى من أعطوني الأمان والثقة

عمي وعمتي وأخوالي وخالاتي وأبنائهم الأعمام، وإلى روح عمتي المتوفاة إلى كهوف المعرفة

... و لولاء العلم... الذين كانوا لي قدوة (كل أساتذتي)

من مؤطرين ومشرفين

وخاصة أساتذتي المشرفة على مذكري.

إلى كل هؤلاء أهدي ثمرة جهدي المتواضع.

الطالب.....بلعيشة علي

* التـشكرات *

بسم الله الرحمن الرحيم

﴿ربي أوعزني أن أشكر نعمتك التي أنعمت علي وعلى والدي وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين﴾.

سورة النمل الآية 19

الحمد والشكر لله تعالى الذي أعطى كل شيء خلقه ثم هدى نحمده كثيرا طيبا مباركا

فيه على أنه وفقني وقدرني على انجاز هذا العمل المتواضع

الحمد والشكر لله تعالى الذي أعطى كل شيء خلقه ثم هدى نحمده كثيرا طيبا مباركا

فيه على أنه وفقني وقدرني على انجاز هذا العمل المتواضع

كما نتقدم بالشكر إلى الأستاذة المحترمة: "بوكر رشيدة" التي ساعدتني على إنجاز هذه

المذكرة ولقبوها تولى مهمة الإشراف علي

وبتقديمها لنا التوجيهات الدقيقة ومساعدتها لي للتغلب على العقبات

التي واجهتني كما نتقدم بالشكر الجزيل ووافر الإمتنان وأسمى عبارات التقدير

لأعضاء لجنة المناقشة لتشريفهم لنا بمناقشة هذا العمل المتواضع

ولا يفوتنا أن نشكر مدير الجامعة وكل أساتذة وكل الطاقم الإداري والمهني

إلى كل هؤلاء أسمى معاني الشكر و الاحترام والتقدير.

بلعيشة علي

قائمة المختصرات

-المختصرات باللغة العربية :

ص : الصفحة

ج ر: جريدة رسمية

ط: طبعة

ع: عدد

ص.ص: الصفحة إلى الصفحة

غ ج: غرفة جزائية

م ق : مجلة قضائية

ق إ ج : قانون الإجراءات الجزائية

ق ع : قانون العقوبات

-المختصرات باللغة الفرنسية :

P: Page

Op.cit: ouvrage preite

N: Numero.

j.s.p: juris-classeurperiodique(semaine juridique)

المقدمة

لقد ساهمت التطورات التي يعيشها مجال الاتصال في الآونة الأخيرة بروز عدة أخطار تهدد أمن وحرية الملكية الفكرية، وللمجهود الذي عرفه التسيير البدوي البطيء والمحدود الذي أصبح لا يساير مستجدات العصر، والذي أصبح كذلك غير قادر على أداء مهامه على الوجه المطلوب، جاء التسيير الإلكتروني كأحدث محطة عرفها الإنسان لتحل عدة إشكالات منها الاستفادة من الوقت بأقل جهد ممكن، كأولى أهداف من الثورة العلمية، ومن أهم هذه الإنجازات الحديثة نجد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقها للاستخدام التكنولوجي الحديث في مجال الإتصالات ونقل المعلومات إلكترونيا وهي تختلف بذلك كثيرا عن غيرها من الوسائل التقليدية للاتصال والإعلام، وإن استخدام وسائل الاتصال الإلكتروني الحديثة وخاصة في مجال المعاملات المالية الإلكترونية والتي أعطت نوعا من الثقة الكاملة لكل متعامل في المجال الإلكتروني، وإن استخدام الوسائل الإلكترونية الحديثة لا يخلو من المخاطر، فيمكن أن يستغل بعض المجرمين هذه الوسائل في ارتكاب جرائمهم بطريق الاحتيال أو المساس بخصوصيات هؤلاء المتعاملين وسرية معاملاتهم، وإن التقدم والتطور الحاصل في التكنولوجيا وظهور الشبكة العالمية والأنترنيت بكل ما حملته من تقدم وخدمات، لم يترك العالم يمر بسلام، لأنه يقدر ما كان يحدث آثار إيجابية وغير حياة ونمط المجتمعات وساهم في تطورها وتقدمها، فهو لا يتضمن الانعكاسات السلبية التي أفرزتها هذه التقنية العالمية المتمثلة في إساءة واستخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع، حيث تضر بمصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع كله، حيث أدى هذا التطور إلى ولادة أنماط وصور مستحدثة والتي سميت بالجرائم المعلوماتية.

ولقد شكل المستند الإلكتروني أهم تحوّل عرفته البشرية، فقد أصبح مستعملا في جميع الجوانب العلمية، أصبح يتخلل مجموعة من المعاملات المالية والتجارية أيضا، ورغم كل الانتقادات التي وجّهت إليه، فمن الفقهاء من ذهب إلى عدم جواز إضفاء صفة الإثبات على هذه

المحركات واعتمادها كحجة ودليل على التصرفات التي تقع بين الأطراف والبعض أخذ هذه المزايا التي تتميز بها، فهي تتضمن الحقوق وتسهل أعباء التنقل ويعتبر هذا الموضوع من المستجدات التي تمس عدة جوانب من العصر ارتبطت بمجالات حساسة يقوم عليها أي نظام في أي دولة، وظهر مع هذا التطور عدة مصطلحات تقوم على الأساس على المستندات الإلكترونية، مثل: التجارة الإلكترونية والأموال الإلكترونية والمبادلات والمعاملات الإلكترونية والعقود المبرمة عبر شبكة الأنترنت، كلها نتائج لثورة تكنولوجية تقوم بالأساس على المستندات الإلكترونية، وفي خضم هذه الثورة حلت المستندات الإلكترونية محل المستندات الورقية، مما طرح مجموعة من الإشكالات والتساؤلات التي حاول الفقه إلى جانب القضاء وضع حل لها.

- الإشكالية:

الى أي مدى إستطاع المشرع الجزائري توفير الحماية الجنائية للمستند الإلكتروني؟

- أسباب اختيار الموضوع:

يرجع سبب اختيارنا لهذا الموضوع لأسباب ذاتية وموضوعية:

- الأسباب الموضوعية:

- الأهمية التي يكتسبها المستند الإلكتروني في ظل التطور الاقتصادي والمالي الحاصل على المستوى الدولي وخطورة التعامل بالمستندات الإلكترونية في المجالات المالية وفي مختلف القطاعات والتعاملات الإلكترونية، مما نتج عنها عدة جرائم إلكترونية لدى الأفراد و الوصول إلى ما هو واقع في مجال التعاملات الإلكترونية وتقريب الحقائق إلى ذهن القارئ.

- تسليط الضوء على متانة قطاع المعلوماتية في مواجهة الجرائم المحيط به وتفعيل دور الآليات لحماية المستند الإلكتروني وذكر الحماية الجنائية المقرر لعملية الحماية.

- الأسباب الذاتية:

- اهتمام الباحث بموضوع المستند الإلكتروني والحماية الجنائية المقرر له بشكل عام وأنه يندرج ضمن التخصص.

-أهمية الموضوع:



يكتسي الموضوع باعتباره مفهوم حديث خاصة في العالم العربي، وأنه أصبح موضوع الساعة ومحل انشغال مجموعة من الباحثين وكذلك لردود الفعل المنصبة عليه، وكذلك الدور الذي يلعبه المستند الإلكتروني في الحياة اليومية وفي جميع المجالات الحيوية لما له من أهمية على المستوى الأكاديمي والتطبيقي، وتتجلى أهمية البحث أيضا في تسليط الضوء على أحد التوجهات الحديثة في مجال المعاملات، حيث تثبت مجموعة من معارك الاقتصاد الوطني العمل بهذا النوع من مستندات لملائمة التطورات الرقمية إن الحماية الجنائية للمستند الإلكتروني هو بمثابة صمام الأمن في مواجهة الأزمات المعلوماتية والتأكيد على ضرورة وجود أجهزة حكومية ووطنية ودولية خارجية إشرافية ذات خبرة تمكنها من تطبيق متطلبات الرقابة على النحو الأمثل.

- أهداف الموضوع:

تهدف دراستها إلى تبيان عدة أهداف مسطرة من قبل تسعى إلى تحقيقها ومن هذه الأهداف نشر الثقافة التأمينية الجنائية لدى الأفراد والمؤسسات التي تتعامل بالمعاملات والبيانات الإلكترونية.

- المنهج المستخدم:

إن طبيعة الموضوع تفرض علينا الأخذ بأكثر من منهج فقد تم استخدام المنهج الوصفي في عرضنا للمفاهيم العامة للموضوع ومقاربة مختلف جوانبه القانونية، وأما استخدام المنهج التحليلي الاستقرائي، وذلك من خلال الاعتماد على تقنية تحليل النصوص وتفسيرها، والتوصل إلى نتائج واستقرائها، طالما أن النص القانوني هو بداية كل دراسة قانونية لا يمكن الاستغناء عنها، وأما المنهج النقدي فاعتمدنا عليه من خلال الوقوف على أهم الثغرات التي اعترضت المستند الإلكتروني.

- خطة الدراسة:

من أجل الإحاطة بالجوانب المتعلقة بهذا الموضوع، تم تقسيم المذكرة إلى فصلين في كل فصل تناولنا مجموعة من المباحث، حيث تناولنا بالدراسة في الفصل الأول وناقشنا فيه بعد تقسيمه إلى مبحثين، مدلول المستند الإلكتروني، مفهومه وتعريفه وخصائصه والطبيعة القانونية له وتميزه عن

ما شابهه في المبحث الأول، في المبحث الثاني تطرقنا إلى النظام القانوني للمستند الإلكتروني وحجيته في الإثبات وشروط صحة المستند الإلكتروني.

وتم تقسيم الفصل إلى مبحثين، المبحث الأول تطرقنا فيه إلى الأفعال الماسة بمحتوى المستند الإلكتروني ومنها جريمة التزوير والسرقة والاتلاف والاحتيال والحماية الجنائية المقررة لكل منها، وفي الأخير ناقشنا الأفعال الماسة بسرية المستند الإلكتروني وقواعد الضبط في الجرائم المعلوماتية والاختصاص القضائي والقانون الواجب التطبيق.

وفي الأخير ختمنا دراستنا هذه بخاتمة تضمنت مجموعة من النتائج والتوصيات.

الفصل الأول

الفصل الأول: ماهية المستند الإلكتروني

إن السرعة والثقة والائتمان أساس المعاملات التي يتطلبها عصرنا الحالي، وإن جَلّ تعاملاتنا اليومية تتسم بالوضوح والتحديد من حيث مضمونها، إلى جانب توافر قدر من الأمان والثقة تجاهها، ويرجع ذلك إلى كتابة هذه المعاملات في مستندات يمكن الرجوع إليها في أي وقت إذا استدعى الأمر ذلك، ولما كان العالم اليوم قد شهد عدة تغييرات ساهم في بنائها تطور وسائل الاتصال كنمط جديد كان لزاما على الدول مسايرة هذه التطورات التي فرضت على جميع المجالات من تجارة وعالن الأموال، مما جعل هذه الدول من خلال قوانينها الوطنية أن تحاول تنظيم هذه التكنولوجيا وتقسيماتها والاستفادة من خدماتها المتنوعة والسريعة، أما الآن وعلى الرغم من التطور الكبير الذي تشهده التقنيات من خدماتها المتنوعة والسريعة، وأما الآن وعلى الرغم من التطور الكبير الذي تشهده التقنيات الحديثة، إلا أنها تقف عاجزة أحيانا أمام بعض التجاوزات التي يقوم بها بعض الأشخاص باستخدامهم وسائل احتيالية، ولفهم الطبيعة الخاصة لهذه المستندات الإلكترونية، سوف نتطرق إلى المقصود بالمستند الإلكتروني والذي يعتبر من بين ما أنتجته ثورة المعلوماتية الحديثة والتي غزت العالم اليوم، ولتعميق البحث في الموضوع سننتقل في البداية إلى دراسة ماهية المستند الإلكتروني، وذلك من خلال (المبحث الأول) وسنتناول النظام القانوني للمستند الإلكتروني وحتميته في الإثبات في (المبحث الثاني).

المبحث الأول: مدلول المستند الإلكتروني

إن عدد التعاملات الإلكترونية تختلف فيما بينها اختلافا كبيرا، فمن جهة تكون هذه التعاملات على شبكات اتصال مفتوحة للكافة دون تمييز كشبكة الأنترنت أو شبكات متعلقة يقتصر التعامل من خلالها على عدد محدود من الأفراد أو الهيئات ومثالها الشبكات الخاصة بالشركات والمؤسسات الحكومية الهيئات التي تقدم خدمات مثل: الرعاية الصحية والتأمينات، وقد أسهمت نظم جديدة في الاتصالات في زيادة أهمية وكفاءة المعاملات الإلكترونية ومثالها

الشبكات الخاصة للمعاملات (سويفت) التي بمقدورها إتمام التصرف في لحظات معدودة، وكذلك وسائل الاتصال عن بعد ونظم التبادل الإلكترونية للبيانات¹.

المطلب الأول: مفهوم المستند الإلكتروني

لقد تعددت التعاريف المتعلقة بالمستند الإلكتروني واختلفت باختلاف التشريعات التي تدخلت ونظمتها بنصوص متنوعة وخاصة بعمليات التعامل عبر أجهزة وشبكات الحاسب الآلي لهذا المستند من زوايا مختلفة مع استخدام مصطلحات مترادفة ومتنوعة².

مثل: السند الإلكتروني، المحرر الإلكتروني، الكتابة الإلكترونية، الوثيقة لمعلوماتية، السجل الإلكتروني، رسالة البيانات، وعلى الرغم من الاختلاف إلا أنها تحمل معنى واحد، وعليه لتحديد مفهوم المستند الإلكتروني سنتطرق إليه من خلال الفرع الأول إلى تعريفه وفي الفرع الثاني إلى خصائصه شروط صحته وصوره.

الفرع الأول: تعريف المستند الإلكتروني ونشأته

أولاً: تعريفه

لم يرد للمستند الإلكتروني تعريف موحد، فقد عرفته التشريعات الدولية والوطنية بالاعتماد على البيئة والوسائل المستعملة في تحريره، وهذا ما سنتناوله في الناحية القانونية له.

1/-التعريف القانوني للمستند الإلكتروني :

هو عبارة عن كتابة على دعامة إلكترونية مثبتة لواقعة قانونية يترتب عليها أثر قانوني بصفة آلية يمكن فهمها وإدراكها بمجرد النظر إليها³.

¹ - حسين شحادة الحسين، التوثيق الإلكتروني في الاعتماد المستندي، دراسة مقدمة إلى المؤتمر العلمي الثالث للقانونيين المصريين الذي عقدته الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع عن موضوع الجوانب القانونية للعمليات المصرفية، القاهرة، 12- 19 ديسمبر 2002، ص 01.

² - إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002، ص 14.

³ - إيهام خليفة، الحماية الجنائية لمحررات الإلكترونية من التزوير ، أطروحة دكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016، ص 24- 25.

هناك من يعرف المستند الإلكتروني "المستندات الإلكترونية بأنها بيانات ثبوتية يقع تخزينها ونقلها بشكل رقمي والمقصود فيها هو ذلك الشكل الإلكتروني أو الرقمي وليس الشكل الورقي اللاحق حينما يتم استخراج هذه السندات وطباعتها على الورق"¹.

ونظرا لحدثة إصطلاح المستند الإلكتروني، اختلفت التشريعات بشأن تسميته -كتابة، محرر إلكتروني، مستند، توقيع إلكتروني، وثيقة، سند أصلي، نسخة مطابقة، نشر، ختم، سجل، ملف. أ/-تعريف المستند الإلكتروني في التشريعات الدولية:

لقد نصت بعض التشريعات الدولية على تعريف المستند ، وهذا مثل قانون الأونسترال النموذجي للأمم المتحدة والتوجيه الأوروبي.

أولا: تعريف المستند الإلكتروني في قانون الأونسترال:

عرف قانون الأونسترال النموذجي والخاص بالتجارة الإلكترونية المستند الإلكتروني من خلال نص المادة الثانية (الفقرة أ) منه بأنه "المعلومات التي يتم إنشاؤها وإرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة في ذلك على سبيل المثال: تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ الورقي"². فمن خلال هذا النص، نلاحظ أن التشريع الفرنسي قد وسّع من مفهوم الكتابة في الإثبات لتشمل الكتابة الإلكترونية بغض النظر عن نوع الدعامة المستعملة في إنشائها أو المحمولة عليها أو المرسله بواسطتها، بشرط أن يكون لها دلالة واضحة ويمكن قراءتها³.

1- عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010 ص 33.

2- المادة 01 قانون الأونسترال النموذجي للتجارة الإلكترونية لسنة 1996، والصادر في جلسة رقم 25 الجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996.

3- براهيم حنان، المحررات الإلكترونية كدليل إثبات، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد التاسع، (ب.ت)، ص 138.

-تعريف القانون الفرنسي:

وفقا للقانون الصادر سنة 1988 والمتعلق ببعض الجرائم المعلوماتية بأنه المستندات التي يتم خضوعها للمعالجة الآلية، والتي يتم بالفعل صياغتها في إحدى لغات الحاسب الآلي، وبالتالي فلفظ 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 التكتيكية الجديدة¹.

-تعريف التشريع الأمريكي:

لقد عرف المشرع الأمريكي المستند الإلكتروني في القانون الموحد للتجارة الإلكترونية في نص المادة الثانية الفقرة السابعة بأنه "السجل الذي يتم إنشاؤه أو تكوينه أو إرساله أو استلامه أو تخزينه بوسائل إلكترونية، فمن خلال هذا التعريف نستخلص أن المشرع الأمريكي استعمل مصطلح السجل، بدلا من مصطلح رسالة البيانات أو المعلومات، التي هي أكثر دقة من حيث المفهوم².

ب-تعريف المستند الإلكتروني في التشريعات العربية:

نظرا لتأثر التشريعات العربية بالقانون النموذجي لليونيسترال، فقد اعترفت العديد منها بالكتابة الإلكترونية، وهذا بالرغم من اختلافها في التسمية، حيث نذكر منها على سبيل المثال:

¹ - هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ص 120.

² - صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون الخاص، جامعة تلمسان، 01، ص 45.

-التشريع الإماراتي:

عرف المشرع الإماراتي المستند الإلكتروني في المادة الأولى الفقرة الحادية عشر منه بأنه "سجل أو بيان معلوماتي يتم إنشاؤه أو تخزينه أو استخراجة أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط"¹.

وكما عرف المعلومات الإلكترونية في الفقرة الثانية من المادة الأولى بأنها "أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصوت والصوت والارقام والحروف والرموز والإشارات وغيرها"، وبذلك نجد أن المشرع الإماراتي قد عرّف المستند الإلكتروني بأنه السّجل أو البيان المعلوماتي التي يتم إنشاؤه أو إرساله أو تجزئته أو استلامه بوسيلة إلكترونية، كما وضّح المعلومات الإلكترونية والتي تشمل الكتابة الإلكترونية والصور والأرقام والأصوات والحروف وغيرها بشرط أن تكون مفهومة وتؤدي الغرض الذي وجدت من أجله في الإثبات.

-التشريع المصري:

لقد تناول المشرع المصري تعريف المستند الإلكتروني في المادة الأولى الفقر "ب" منه بأنه "رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو ستقبل كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية أو بأي وسيلة أخرى مشابهة"، كما عرف الكتابة الإلكترونية بأنها "حروف أو ارقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو بأي وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك"².

¹ - المادة 01 الفقرة الحادية عشر، المرسوم بقانون اتحادي رقم 05 لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

² - المادة الأولى الفقرة "ب" من القانون رقم 15 لسنة 2004 والخاص بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، ج.و، ع 17 الصادرة بتاريخ 2004/04/22، ص 17 وما بعدها.

-التشريع التونسي:

لقد عرّف المشرع التونسي المستند الإلكتروني على أنه "الوثيقة الإلكترونية وهي الوثيقة المتكونة من مجموعة أحرف أو أرقام أو أية إشارات رقمية أخرى بما في ذلك تلك المتبادلة عبر وسائل وتكون ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة"¹.

وقد عرف "القانون العربي النموذجي الموحد" سوء استخدام تكنولوجيا المعلومات والاتصالات في المادة الأولى منه الفقرة 18 الكتابة الإلكترونية بأنها "عملية تسجيل البيانات على وسيط إلكتروني لتخزينها"².

-التشريع السوداني:

عرف المستند الإلكتروني على أنه "التوقيع التي يتم إنشاؤه وإرساله واستقباله وتخزينه بوسيلة إلكترونية، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات يكون لها طابع منفرد ويسمح بتحديد هويته وتمييز الشخص الموقع عن غيره"³.

-التشريع الجزائري:

إن المشرع الجزائري لم ينص صراحة على تعريف المستند الإلكتروني ولم يتم بإعداد قانون خاص بالمعاملات الإلكترونية، وهذا خلافاً للتشريع المصري أو العراقي أو السوداني، وهذا ما يبين ويوضح عدم تأثره كباقي التشريعات الأخرى، ولكنه لم يعمل التطور الحاصل في الإثبات للكتابة الإلكترونية، فلقد أدخل بعض التعديلات على نصوص الإثبات والقواعد العامة للقانون المدني في نص المادة 323 مكرر و323 مكرر 01 لسنة 2005 بأنه "ينتج الإثبات بالكتابة من تسلسل الحروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما

¹- Comment, Dit Surla: Mowsal Wyer.4vlike.Com

²- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية، مصر، 2009، ص 743.

³- المادة 03 من قانون المعاملات السوداني.

كانت الوسيلة التي تتضمنها وكذا طرق إرسالها واشترط توافر شروط قانونية نص عليها في المادة 323 مكرر 01 وهي:

1- أن يتضمن تعبير عن المعاني والأفكار الإنسانية المترابطة.

2- أن يكون هذا التعبير له قيمة قانونية.

3- أن يتصف هذا المستند بالصفة الإلكترونية¹.

وعلى ضوء هذه التعريفات السابقة نجد أن كل منها قد اعتبر أن المستند الإلكتروني هو عبارة عن وسيط إلكتروني والذي هو كل شيء مادي متميز لقرص صلب أو مضغوط أو شريط ممغنط أو خلافة يصلح أن يكون محلاً لتسجيل أو تخزين معلومات فيه، معالجة بواسطة نظام المعالجة الآلية للمعطيات ويتحقق هذا من خلال توفر عناصر هي:

1- **سرية المعلومات:** يفرض قيود مصرح بها على الدخول إلى المعلومات والإفصاح عنها².

2- **صحة المعلومات:** هي الوقاية ضد تعديل وإتلاف المعلومات وتتضمن ضمان عدم خرق المعلومات وضمن صحتها.

3- **توافر المعلومات:** هي ضمان الدخول إلى المعلومات واستخدامها بشكل موثوق، وفي الوقت المناسب ويساعد أمن المعلومات وفقاً لهذه الأمور، وعلى سير عمل الخدمات الحكومية بدون عراقيل والقدرة على الحفاظ على "الأعمال كالمعتاد" مثل :

- **المحتوى content:** وهو الموضوع الرئيسي التي تدور حوله الوثيقة وأنشئت من أجله ويتفرغ منه موضوعات فرعية.

- **السياق context:** وهي البنية التي أخرجت وأنتجت الوثيقة أي السياق الإداري المحيط بالوثائق بدءاً من الإدارة المنشئة وتاريخها وعلاقتها بالوثائق الأخرى ذات الصلة.

¹ - توفيق أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني دراسة مقدمة إلى مؤتمر الأعمال المصرفية الإلكترونية، بحث منشور على شبكة الانترنت من خلال الموقع الإلكتروني <https://www.arabawifo.com> (الدليل الإلكتروني القانون العربي)، بتاريخ 05/12/2007 ص 503.

² - أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، (علم مجلة علمية محكمة)، جامعة بني سويف، مصر، العدد السادس عشر (16)، يناير 2016، ص 92-93

-البناء structure: وهي البيانات التي تساعد في تحديد ذاتية الوثيقة كالفصول وأجزاء الوثيقة والهوامش والفصول والأجزاء التي تتعلق بالبنية المنطقية للوثيقة، وهي الرموز والمعطيات التي تساعد في تشكيلة¹.

وإذا ما توافرت هذه الصفات للمستند الإلكتروني، فإنها تتحقق لها ما يلي:

- 1/-المصادقية حتى يمكن الاعتماد عليها عند اتخاذ القرارات.
- 2/- التكامل وذلك لكي يتم التأكد من ان البيانات لن تتغير بشكل مكرر.
- 3/-عدم الانكار لمنع منشئ الوثيقة من التبرؤ منها².

2-التعريف الفقهي للمستند الإلكتروني:

إختلف الفقه في إعطاء تعريف جامع للمستند الإلكتروني، حيث يعرفه البعض بأنه "المستند الذي يتضمن بيانات ذات معالجة إلكترونية، ومكتوب وموقع عليه بطريقة إلكترونية وموضوع على دعامة مادية مع إمكانية تحويل المحرر الورقي عن طريق إخراجها من المخرجات الكمبيوترية"، ويعرفه جانب آخر بأنه "معلومات إلكترونية ترسل أو تسلم بوسائل إلكترونية، أيا كانت وسائل استخراجها في المكان المستلمة فيه"³.

ولقد قام الفقه بتعريف المستند الإلكتروني بأنه "كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات أو أن يكون مشتقا من هذا النوع"⁴.

وكما ذهب بعض من الفقه إلى تعريف المحرر الإلكتروني بأنه المستند المعالج آليا عن غيره من المستندات غير معالجة آليا، وهذا الاختلاف هو ميزة تميزه عن غيره، وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد، والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام

¹- International Council Archive, 2004, P 12- 13.

²- Public Records Office, 2004, P 12- 13.

³- طمين سهيلة، الشكلية في عقود التجارة الإلكترونية، مذكرة ماجستير في القانون، فرع القانون الدولي للأعمال، مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2011، ص 68.

⁴- إيهاب فوزي السقا، مرجع سابق، ص 16.

البرامج، ويقصد بالمستندات المعالجة آليا كل المستندات التي تملك دعامة مادية يمكن أن يدون عليها شيء معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز، (قرص أو شريط ممغنط أو خلافة) ويكون محلا يصلح لأن يكون هذا الشيء قد خرج من الآلة وتم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله¹.

وبكل هذه التعاريف الفقهية نجد أن التعريف الأقرب إلى الصواب هو أن المستند الإلكتروني هو: " عبارة عن معلومات تم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة إلكترونية أو ضوئية أو رقمية أو صوتية، بشرط ان تتضمن إثبات واقعة أو تصرف قانوني معين ويحتوي على توقيع إلكتروني ينسب الواقعة أو التصرف القانوني لشخص محدد"².

ثانيا: النشأة

لقد أدى التطور التكنولوجي إلى وسائل تحرير العقود ومن بينها المستند الإلكتروني والذي ترجع جذوره إلى وضع بعض الدول قوانين منظمة له، إذ نجد من بينها المشرع الأمريكي من خلال القانون الفيدرالي المتعلق بالتوقيع الإلكتروني والتجارة الإلكترونية، وذلك في 30 يوليو من سنة 2000 رغم كون بعض الولايات قد أصدرت قوانين محلية منظمة للمستند الإلكتروني قبل ذلك الأجل ولعل من أمثلة هذه الولايات ولاية نيويورك التي اصدرت تشريعا للتوقيع والسجلات الإلكترونية في 28 سبتمبر 1999 بالإضافة إلى تشريعات أخرى من طرق البلاد ويجب أن تكون القوانين الوطنية غير متعارضة معه وهذا بالإضافة إلى تشريعات غربية وعربية التي تدخلت في شأن تنظيم المستند الإلكتروني، إذ نجد في هذا الصدد أن المشرع التونسي باعتبار أول دولة عربية تصدر هذا القانون وذلك من خلال قانون المعاملات الإلكترونية، وذلك في 11 أوت من سنة 2000 وقد تلاه المشرع الأردني بالقانون المرقم ب

¹ - أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط01، دار هومة للنشر والتوزيع، الجزائر، 2006، ص 135.

² - رياض السيد حسين أبو سعيد، توثيق المستند في التعامل الإلكتروني-دراسة تحليلية مقارنة-، مجلة دراسات الكوفة، ع 28، 2013، ص 112.

85 لسنة 2001، أما المشرع الكويتي فقد أصدر قانون التجارة الإلكتروني في 08 أبريل من سنة 2006، إلا أن المشرع المغربي لم يصدر قانون خاص بتنظيم المستند الإلكتروني، وإنما أصدر قانون متعلق بالتبادل الإلكتروني للمعطيات القانونية، وذلك في 30 نوفمبر 2007¹.

الفرع الثاني: خصائص المستند الإلكتروني وصوره

أولاً: خصائصه

إن المستند الإلكتروني في طبيعته يتصل بمجموعة مهمة من المعطيات والأنظمة التجارية والإدارية والمالية وغيرها، والتي تكون ممتدة كثيرا لتشمل الافراد والدولة معا، وهذه الطبيعة الخاصة له تعطيه خصائص مميزة وعديدة والتي سنعرضها فيما يلي:

1- القيمة القانونية:

إن احتواء المستند الإلكتروني على كتابة هامة به تضي عليه القيمة القانونية والتي تعتبر قرينة قانونية تصلح للتمسك أو الاحتجاج بها عند الضرورة، وهي تعني بإقرار حق سواء بإنشائه أم بتعديله أو بإلغائه أو إثباته².

إن المستند الإلكتروني يعد الأداة الرئيسية لتنفيذ فكرة الحكومة الإلكترونية التي تقضي باستخدام نظم المعلومات الرقمية في انجاز المعاملات الإلكترونية الإدارية وتقديم الخدمات المرفقية والتواصل مع المواطنين لمزيد من الإفصاح والشفافية ويتضمن المستند الإلكتروني تغييرا كاملا عن المعاني والأفكار الإنسانية المترابطة وهو ما يعني أن يكون هذا المحرر أداة للتفاهم وتبادل الافكار بين الافراد، وأن يكون له قيمة قانونية، يمكن التعويل عليه عند المعاملات بين الافراد والمؤسسات الحكومات، مما يخضعه للمسائلة القانونية عند المساس أو تغير ما يحمله من الحقائق.

¹ - ظهير شريف رقم 107-129، الصادر في 19 من ذي القعدة 1428، الموافق لـ 30 نوفمبر 2007)، بتنفيذ قانون رقم

53-05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

² - إيهاب قوزي السقا، مرجع سابق، ص 17.

2/- السرية:

تتميز المستندات الإلكترونية بالسرية، حيث لا يمكن لأي شخص مهما كان أن يطلع عليها لما لها من خصوصية والشخص الوحيد من له الحق في الإطلاع عليها هو المرسل أو المرسل إليه، لأنها متميزة بالتقنيات المتطورة التي توفر الامن لها، كما أن تشريعات المعاملات الإلكترونية اضفت عليها حماية لضمان الثقة فيها وذلك بأن نصت على استخدام وسائل تقنية تحفظها ، وتتمثل في أنظمة التشفير وتسليم شهادة تصديق من طريق جهات موثوقة من الدولة، تثبت أن ما على المحررات من حقوق يعود لصاحبها التوقيع عليها¹.

3/- الصفة الإلكترونية:

يحمل هذا المستند أو المحرر الصفة الإلكترونية بما يعني أن العمليات التي يمر بها المحرر مثال: كتابة أو ضغطه أو تخزينه أو استرجاعه أو نقله أو نسخة متصلة بتقنية تكنولوجيا إلكترونية، ولا يمكن استخدامه خارج هذا الوسيط الإلكتروني، بالإضافة إلى أنه يمكن أن يتم تحميل هذا المحرر ونقله من جهاز إلكتروني لآخر عن طريق دعامة إلكترونية². وبالتالي هذه الخاصية لهذا المستند تعتمد على وجود دعامة ورقية على عكس المستند التقليدي المودع على دعامة ورقية، ومن هنا نجد أنه يوجد دائما ارتباط وثيق الصلة بين المضمون في السند التقليدي والدعامة (أداة التخزين غالبا قطعة ورق)، والمدون عليها المعلومات ولا نوع من استقلال المعلومات الواردة فيه عن طريق دعامة أخرى، ويرجع ذلك إلى أن المضمون 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

¹ - إلهام بن خليفة، مرجع سابق، ص 23.

² - إيهاب فوزي السقا، مرجع سابق، ص 17.

³ - كحلول سماح، حجية الوسائل التكنولوجية في إثبات العقود التجارية، مذكرة ماستر في القانون العام للأعمال، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2015، ص 05.

4/- السرعة والائتمان في إبرام المعاملات:

إن المستند الإلكتروني هو الأداة التي من خلالها تحقق التجارة الإلكترونية أهدافها، فمن طريق هذا المستند يمكن إنجاز المعاملات وإبرام الصفقات والتصرفات القانونية بسهولة، مما يؤدي إلى توفير النفقات كما أن هذه المعاملات التجارية يتم إبرامها بوسيلة إلكترونية دون الحاجة إلى وسيط سواء كان هذا الشخص الوسيط شخصاً أو شركة، الأمر الذي يؤدي إلى تجاوز الحواجز الجغرافية بين الدول، وذلك لأن التجارة الإلكترونية تعني بتبادل البيانات الإلكترونية التي تركز على المعرفة العلمية عن بعد بواسطة الوسائط الإلكترونية المتعددة، مثل: البريد الإلكتروني، الفاكس، التلكس وغيرهم وتتميز المستندات الإلكترونية بالسرعة في إبرام العقد، إذا يستطيع الشخص الذي يتولى التعاقد عن طريق وسائل الاتصال الفوري، ويتأمن وصول إجابته إلى شخص الآخر الذي ينوي التعاقد معه في أي مكان كان، والحصول على إجابة في ثواني معدودة، وهكذا يسمح بتوفير الوقت، واختصاره بشكل كبير لاسيما في التجارة الإلكترونية وكذلك تمكن المستندات الإلكترونية، من تسليم بعض الأشياء وأداة بعض الخدمات فوراً في البيئة الافتراضية، كالحصول على خدمات معينة أو برامج كومبيوترية، وتسمح أيضاً بالوفاء فوراً أي يمكن دفع الثمن إلكترونياً ويأخذ الأساليب المعرفة للوفاء على شبكة الأنترنت، سواء عن طريق بطاقات الائتمان أم النقود الرقمية أم البطاقات الذكية، غيرها من الوسائل الوفاء¹.

ثانياً: صور المستند الإلكتروني

1/- العقود الإلكترونية:

هي عقود تتحقق بالإيجاب والقبول مثل العقود العادية التي تبرم وتوقع كتابة، غير أن الإيجاب والقبول يتحقق بوسيلة إلكترونية دون حاجة إلى مستند مكتوب².

¹ - عباس العبودي، مرجع سابق، ص 40.

² - أسامة أبو حسن، خصوصية التعاقد عبر الأنترنت، -دراسة مقدمة إلى المؤتمر الذي عقده كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر والآنترنت"، والذي بمدينة العين، في الفترة من 19-200013، ص 37.

ومثال ذلك: أن يرسل الموجب عرضه إلى الطرف الآخر بطريق البريد الإلكتروني الذي قد يكون شخصا أو هيئة اعتبارية ويقوم من يوجه إليه الإيجاب بالتوقيع عليه إلكترونيا بما يفيد القبول ويعيده إلى المرسل أو (الموجب) ثانية، ومن ثم ينعقد العقد بهذه الطريقة، وتكون له قوته القانونية، ويكون هذا القبول في رسالة مفصلة ترسل إلى صاحب الإيجاب أو أن ترسل في ذات المستند الذي يتضمن الإيجاب ويتحقق ذلك بقيام من وجّه إليه الإيجاب بالضغط على أحد الأزرار في صفحة المستند والذي يتضمن معنى القبول، وذلك عقب بيان لشروط العقد أو أن يقوم بوضع توقيع إلكتروني في خانة معينة ويقوم بإعادة المستند ثانية إلى الموجب¹.

وعرف جانب من الفقه العقد الإلكتروني بأنه "اتفاق يتلاقى فيه الإيجاب والقبول عبر شبكة دولية للاتصال عن بعد وذلك بوسيلة مسموعة أو مرئية تتيح التفاعل بين الموجب والقابل². وكما يرى أن فقهاء آخرون يرون أن هذا التعريف مهم لكونه ركّز على خصوصية هذا العقد التي تتمثل في الوسيلة التي تبرمها، إضافة إلى أنه لم يغفل صفة هامة من صفاته وهي انتمائه إلى طائفة العقود التي تبرم عن بعد³.

وهو أيضا عقد يتم انعقاده بوسيلة إلكترونية كلياً أو جزئياً سواء تمثلت الوسيلة الإلكترونية في وسيلة كهربائية أو مغناطيسية أو ضوئية أو إلكترو مغناطيسية أو وسيلة أخرى صالحة لتبادل المعلومات بين المتعاقدين ولقد عرّفه القانون رقم 08-05 المؤرخ في 84 شعبان عام 1439 الموافق ل10 ماي 2018 المتعلق بالتجارة الإلكترونية وفقا للمادة 06 منه على أنه العقد بمفهوم القانون رقم 04-02 المؤرخ في 05 جمادى الأولى 1425 الموافق لـ يونيو 2004،

¹ - أشرف توفيق شمس الدين، مرجع سابق ص 12.

² - أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، دار النهضة العربية، مصر 2007، ص 120.

³ - تامر محمد سليمان الديماطي، إثبات التعاقد الإلكتروني عبر الأنترنت، رسالة دكتوراه غير منشورة، جامعة القاهرة، 2008، ص 38.

والذي يحدد القواعد المطبقة على الممارسات التجارية، ويتم إبرامه بعد بدون الحضور الفعلي والمتزامن لأطرافه بالجوء حصريا لتقنية الاتصال الإلكتروني¹.

ولقد عرّفه المشرع المصري في م 314 ق تجارة مصري الجديد رقم 17 سنة 1999 أنه "عقد يتعهد البنك بمقتضاه بفتح الاعتماد بناءً على طلب أحد عملائه ويسمى الأمر لصالح شخص آخر يسمى المستفيد بضمان مستندات نقل بضاعة منقولة أو معدة للنقل، ويعتبر عقد الاعتماد المستندي مستقلا عقد الذي يفتح الاعتماد بسببه ويبقى المصرف أجنبيا عن هذا العقد"².

وقد عرفت المادة 2 من التوجيه الأوروبي الصادر في 1990/05/20 المتعلق بحماية المستهلك في العقود المبرمة عن بعد، ولقد عرف التعاقد عن بعد بأنه هو "عقد متعلق بالسلع والخدمات يتم بين مورد ومستهلك من خلال الإطار التنظيمي الخاص بالبيع عن بعد أو تقديم الخدمات التي ينظمها المورد، والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الإلكترونية حتى إتمام العقد، في المستند الإلكتروني"³.

وجاء تعريف معنى التعاقد الإلكتروني بأنه "التصرف القانوني الذي يتم عن بعد عن طريق وسيلة إلكترونية وذلك حتى إتمام العقد"⁴.

ويتم إبرام العقد الإلكتروني بتلاقي الإيجاب والقبول في مجلس حكمي يتم بين الحواسيب التي تكون في حوزة كل متعاقد من خلال تبادل المعلومات حول العقد ويشترط في العقد الإلكتروني ما يشترط في العقد التقليدي من أهلية التعاقد والتعبير عن التراضي بإرادة خالية من العيوب

¹ القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق ل 10 مايو سنة 2018 المتعلق بالتجارة الإلكترونية (ج.ر)، العدد 28 المؤرخة في 30 شعبان 1439 الموافق ل 16 مايو سنة 2018، ص 05.

² مازن عبد العزيز فاعول، الاعتماد المستندي والتجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط الأولى، 2006، ص 18.

³ محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، المجلة الكبرى الاسكندريةمصر، سنة 2008، ص 62.

⁴ رضا المتولى وهدان، النظام القانوني للعقد الإلكتروني والمسؤولية عن الاعتداءات الإلكترونية، دار الفكر والقانون، المنصورة، ط الأولى، 2013، ص 24.

وبتبادل الإيجاب والقبول، ويتم إبرام العقد عبر شبكة الانترنت ويعتبر العقد الإلكتروني من خلال استخدام وسائل إلكترونية، طريقة للوفاء تختلف عن طريقة الوفاء في العقود التقليدية، إذ تتم عن طريق وسائل الدفع الإلكترونية كالنقود والشبكات الإلكترونية... الخ، كما أن العقد الإلكتروني يغلب عليه الطابع التجاري فهو عقد عابر للحدود يتم بين عدة أطراف في بلدان مختلفة، وهو عقد مقترن بحق العول بسبب أن المستهلك في العقد لا يتمكن من المعاينة الفعلية لخصائص السلعة أو الخدمة.

2-/- الاعتماد المستندي:

ويتم هذا النوع من المستند الإلكتروني بهذه الطريقة عادة ما يتم بين تاجر وتاجر، بحيث يقوم أحدهما بالتصريح برغبته في استيراد بضاعة معينة من التاجر الآخر، فإنه يقوم بإبرام عقد بيع مع البائع ويتفقان فيه على دفع الثمن عن طريق الاعتماد المستندي ثم يتوجه المشتري إلى بنكه طالبا فتح اعتماد مستندي لصالح البائع محدداً فيه على دفع الثمن عن طريق الاعتماد المستندي ثم يتوجه المشتري إلى بنكه طالبا فتح اعتماد مستندي لصالح البائع محدداً فيه كافة تفاصيل عملية البيع، ويقوم البنك بعد ذلك بإبلاغ البائع بالاعتماد المستندي المفتوح لصالحه، وذلك بشكل مباشر، أو عن طريق بنك مراسل له في بلد المصدر¹.

3-/- الشيك الإلكتروني:

هو عبارة عن رسالة تحتوي على جميع البيانات التي يمكن أن نجدها بالشيك الورقي العادي، بحيث يقوم المشتري بتحرير شيك إلكتروني للبائع وإرساله له إلكترونياً عبر أي وسيلة إلكترونية كالفاكس أو البريد الإلكتروني في أغلب الأحيان، وتكون جميع التوقيعات التي يتضمنها هذا الشيك توقيعات إلكترونية أو رقمية والشيك الإلكتروني يعرفه مصطفى كمال طه ووائل أنور بندق "أنه محرر ثلاثي الأطراف معالج إلكتروني بشكل كلي أو جزئي يتضمن أمراً من شخص يسمى الساحب إلى البنك المسحوب عليه بأن يدفع مبلغاً من النقود لإن شخص ثالث يسمى المستفيد".

¹ - حسين شحادة حسين، مرجع سابق ص 120 - 122.

ويعرفه منير محمد الجنيهي وممدوح محمد الجنيهي أنه "المكافئ الإلكتروني للشيكات الورقية التقليدية التي اعتدنا التعامل بها، و هو رسالة إلكترونية موثقة ومؤمنة يرسلها مصدر الشيك إلى مستلم الشيك (حامله) ليعتمده ويقدمه للبنك الذي يعمل عبر الأنترنت ليقوم البنك بتحويل قيمة الشيك المالية إلى حساب حامل الشيك، وبعد ذلك يقوم بإلغاء الشيك فعلا، ويمكن لمستلم الشيك أن يتأكد إلكترونيا من أنه قد تم بالفعل تحويل المبلغ إلى حسابه¹.

ومن مزايا الشيك الإلكتروني أنه يعزز الثقة بين المتعاملين لاشتماله على بيانات تبعث الاطمئنان والثقة، بحيث يقوم البنك بالتحقق من بيانات الشيك، ثم القيام بعملية المقاصة، كما أنه يعد أداة وفاء تجاوزت الكثير من الأخطار والمشاكل التي افرزها التعامل بالشيك الورقي، وهذه التعريفات تظهر لنا عدة مزايا للشيك هي:

1/- يشترك كل من البائع والمشتري لدى جهة التخليص، ويتم التخليص لدى الشركة نفسها ويتم تحديد السعر الكلي.

2/- يقوم بملاً نموذج الشراء والفاتورة، حيث ترسل إلى البائع مباشرة عبر البريد الإلكتروني بعد ملئها.

3/- تقوم جهات التخليص بمراجعة الشيك والتحقق من صحة الأرصدة والتوقيعات بناء على ذلك تقوم بإخطار كل من المشتري والبائع بتمام إجراء المعاملة المالية، وهي خصم الرصيد من المشتري وإضافته إلى البائع.

4- السفتجة الإلكترونية:

" هي محرر شكلي ثلاثي الاطراف معالج إلكتروني بصورة كلية أو جزئية يتضمن أمرا صادرا من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه، بأن يدفع مبلغ من النقود لشخص ثالث يسمى المستفيد لدى الإطلاع أو في تاريخ معين"².

¹ مصطفى كمال طه ووائل أنور بندق، الاوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الطبعة الأولى، 2006.

² مصطفى كمال طه ووائل أنور بندق، مرجع سابق، ص 345.

ونستخلص من هذا التعريف أن البيانات وأطراف السفتجة الإلكترونية هي نفس السفتجة العادية والاختلاف الوحيد هو الدعامة التي تكون عليها السفتجة الإلكترونية أم الورقية ويضاف بعض البيانات بالنسبة للسفتجة الإلكترونية مثل: اسم المؤسسة المالية (المسحوب عليه) واسم الفرع الذي يوجد لديه الحساب.

أ- أنواع السفتجة الإلكترونية:

1/- السفتجة المعلوماتية الورقية:

هي السفتجة التي تصدر في نموذج مطبوع مستخرج من الحاسوب ظهرت في فرنسا في 02 جويلية 1973، من خلال الممارسات البنكية دون تنظيمها بنص قانوني، تتوفر على نفس شروط السفتجة العادية، بالإضافة إلى المعلومات البنكية الخاصة بالمسحوب عليه، أما بالنسبة لطريقة استخدامها فيتم نقلها للبنك الذي يقوم بتسجيل المعطيات على شريط ممغنط من بنك الساحب ثم إرساله للبنوك المواطنة عن طريق بنك المقاصة لفرنسا، محدد للسفاتج التي ينبغي أداؤها بالنسبة لزيائن كل بنك ويقوم البنك بإعطاء عدّاد كشف السفاتج المعلوماتية الواجب أداؤها من طرف كل مسحوب عليه، وعندما يقبل المسحوب عليه للأداء يقوم بإرساله جزء منه¹.

2/- السفتجة المعلوماتية الممغنطة:

يقوم هذا النوع من السفاتج على دعامة مغناطيسية لا ورقية، تلجأ إليها الشركات والمقاولات الكبرى في فرنسا، وتقوم هذه الشركات تسجيلها على شريط ممغنط وتسلم إلى البنك وتجمع بعد ذلك كل الأشطرة الممغنطة على الصعيد الوطني وتسلم لحاسوب المقاصة للبنك الذي يقوم بدورة بترتيب المعلومات ونقلها للبنوك، التي تتولى أمر معالجتها، فهي أداة لتحصيل الديون وهي تشبه نظام الإشعار بالإقطاء.

¹ - محمد الشافعي، الأوراق التجارية، المطبعة والوراقة الوطنية، ط02، سنة 2002، ص 27.

5/حوالة الوفاء الإلكترونية:

تطورت وسائل الوفاء، حيث أصبح بمقدور الدائن أن يوفي التزاماته بواسطة الوسائل الإلكترونية وقد أنشأت بعض الدول أنظمة وفاء وطنية، كما أصبح هناك عدة أنظمة عالمية للوفاء من أبرزها نظام شبكة السويفت Swift وهو نظام دولي يستخدم على نطاق واسع لإجراء الالتزام بالوسائل الإلكترونية، ويتم ذلك إما بتوجيه أمر من المدين إلى مصرفه بتحصيل مبلغ من حساب دائنه بناء على تفويض مسبق بواسطة إلكترونية¹

وتتم الصورة الأولى التي يطلق عليها التحويل للدائم بقيام الدائن باتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين الى المستفيد سواء كان في نفس المصرف او في مصرف اخر وسواء بدفع المبلغ مقدما إلى البنك المحول أو بتفويضه يقيد المبلغ على حسابه لدى البنك، ويمكن للدائن أن يوجه تعليمات بذلك إلى بنكه من خلال رسالة إلكترونية وعند وصولها يقوم البنك من التأكد من صحتها ومن باقي شروط التحويل مثل كفاية الرصيد ويقوم بعد ذلك بتنفيذ العملية، وأما الصورة الثانية والتي يطلق عليها التحويل المدين، فتتم بتفويض بنك المستفيد في تحصيل قيمة التحويل من الدائن أو بنكه، وفي هذا التحويل يقوم المستفيد من طلب التحويل تفويض من المحول (المدين) إلى بنكه يفوضه فيه بتحويل المبلغ إلى حساب المستفيد ويفيد القيمة على حسابه ويعد أمر التحويل مستندا إلكترونيا يمكن أن يتعرض لأفعال التزوير².

6/-السند لأمر الإلكتروني:

"هو محرر شكلي الأطراف معالج إلكترونيا بصورة كلية أو جزئية، يتضمن تعهداً من محرره يدفع مبلغ من النقود في تاريخ معين لإذن شخص آخر هو المستفيد، وهو صورة متطورة للسند لأمر التقليدي ويختلف عنه في كونه معالج إلكترونيا، بينما السند لأمر العادي يكون على

¹- فياض مالقي القضاة: مسؤولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء، دراسة مقدمة إلى المؤتمر الذي عقده

كلية الشريعة والقانون، جامعة الإمارة العربية المتحدة في موضوع القانون والكمبيوتر والأنترنت والذي عقد بفندق هيانون

العين، في الفترة من 1-5 ماي سنة 200، ص 16.

²- حسين شحادة الحسين، مرجع سابق ص 10.

دعامة ورقية ويتفق معه في كونه يتضمن تعهدا من محرر بدفع مبلغ من النقود في تاريخ معين لإذن المستفيد" واستخدامه هو أن المحرر يحزر السند في صورة ورقية ويسلمه للمستفيد والمستفيد يسلمه للمصرف وبعده تحول معلومات المستند إلى معلومات إلكترونية ممغنطة في الحاسوب.

7/- الكميالة الإلكترونية:

تعتبر الكميالة الإلكترونية صورة من صور المستند الإلكتروني، وهي من حيث الشكل لا تختلف عن الكميالة العادية، فتتضمن نفس البيانات الإلزامية التي يستلزمها قانون التجارة المغربي (المادة 159) لكنها تستلزم فضلا عن ذلك شروط أخرى¹.

1/- ضرورة صدور الكميالة الإلكترونية على نموذج مطبوع يسمح بمعالجة الكميالة والإطلاع عليها بوسائل الإطلاع الآلية والبصرية.

2/- تتضمن الكميالة الإلكترونية اسم البنك المسحوب عليه ورقم الحساب المسحوب عليه في هذا البنك.

3/- تستلزم الكميالة الإلكترونية لاستخدامها ضرورة الاتفاق المبدئي بين سائر الأطراف المتداخلة في هذه الكميالة.

8/- السجلات الطبية الإلكترونية:

إمتد استخدام السجلات الإلكترونية إلى المجال الطبي، حيث تشير الدراسات إلى تزايد استخدام "نظم الرعاية الطبية الإلكترونية"، والتي تتيح الاحتفاظ بسجلات طبية مسجلة بوسائل إلكترونية عن المرضى، وهو ما يتيح تقديم الرعاية الصحية لهم في أي مكان ومعرفة سجلهم المرضى، والذي يتحقق بمجرد الدخول على هذه السجلات والإطلاع عليها وهو ما يعرف بالرعاية الطبية المتنقلة كما تكفل هذه النظم عقد المؤتمرات والندوات وطلب المشورة الطبية من خلال السجلات الإلكترونية، الأمر الذي يؤدي إلى ارتفاع مستوى الرعاية الطبية وإلى التقليل من الأخطاء الطبية وقد أدى إلى استخدام السجلات الطبية الإلكترونية في المجال الطبي إلى تعدد

1- محمد أمين الرومي، مرجع سابق، ص 66.

الإشكاليات فيما يخص أمن هذه السجلات وخصوصية المعلومات التي تتضمنها والحق في السرية، بالإضافة إلى التوقيع الإلكتروني عليها¹.

ونجد أيضا في مجال الخدمات الصحية أن الحكومة الإلكترونية قد امتدت لتشمل استخدام المستند الإلكتروني فيتم تنظيم الرعاية الصحية فقد ظهر مايسمى بالسجلات الطبية الإلكترونية، والتي تعني بالاحتفاظ بسجلات طبية مسجلة إلكترونيا عن المرضى التي تسمح بتقديم الرعاية الطبية لهم في أي مكان من خلال الإطلاع على سجلاتهم المرضية الخاصة بهم².

9-البطاقات الإلكترونية:

وتتخذ أشكالا متعددة ووظائف مختلفة، وهي تصدر من جهات حكومية أو عن مؤسسات مالية خاصة من أجل المبادلات التجارية أو الاستفادة من بعض الخدمات ومنها: البطاقات البنكية أو المصرفية أو بطاقات إلكترونية أخرى مثل: بطاقة التعريف الوطنية البيومترية وجواز السفر الإلكتروني وبطاقة الضمان الاجتماعي، ورخصة السياقة الإلكترونية وبطاقة الوفاء، باعتبارها أداة وفاء مصرفية وبطاقة الائتمان وبطاقة الصراف الآلي، وهذا النوع من البطاقات تخضع لقانون التجارة الإلكترونية الجديد الصادر في 2018.

وبالتالي هذه البطاقات الإلكترونية تحمل مجموعة من المعلومات والبيانات التي ترتبط بمركز مالي أو قانوني معين لصاحبها، سواء كانت ظاهرة أو كانت إلكترونية، أما المعلومات الموجودة على الشريط الممغنط فهي من المستند الإلكتروني³.

¹ - توفيق أشرف شمس الدين، مرجع سابق ص 503.

² - عمار كريم كاظم+ تارمان جميل نعمة، القوة القانونية للمستند الإلكتروني، كلية القانونالعدد السابع، جامعة الكوفة، 2007، ص 27.

³ - براهيم حنان، جريمة تزوير الوثيقة الرسمية الإدارية، ذات الطبيعة المعلوماتية، أطروحة دكتوراه تخصص جنائي كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة 2015، ص 107.

المطلب الثاني: الطبيعة القانونية للمستند الإلكتروني وتميزه عن ما شابهه

إن الطبيعة القانونية للمستند الإلكتروني من النقاط التي صعب تحديدها وخاصة وأن هذا المستند لم ينظم بقانون خاص في التشريع الغربي أو العربي في وقتنا الراهن، على غرار عدة مجالات أخرى التي تغلغت في المجتمع ولما كان هذا المستند الإلكتروني من المواضيع التي تساهم في نمو وازدهار الاقتصاد على كافة أنحاء المجتمع، ولهذا فلقد تميز المستند الإلكتروني بخصائص ومميزات دفعتنا على تمييزه عن ما شابهه من حيث الإثبات والحجية وخاصة عن المستند التقليدي أو المحرر الورقي.

الفرع الأول: الطبيعة القانونية للمستند الإلكتروني

إن الاهتمام الكبير الذي حضي به المستند الإلكتروني في جلّ التشريعات العربية والغربية وباعتبار المستند ذو طبيعة معلوماتية في إبرام العقود والصفقات وإدارة المفاوضات التجارية والتي تعتبر محور التجارة في هذا العصر، ولقد ساهم المستند في تطوير التجارة وازدهارها، وهذا مما أدى بالمشرع إلى ضرورة خلق نظم حماية تتلاءم مع الطبيعة القانونية للمستند الإلكتروني، وهنا ظهرت عدة اتجاهات تتعلق بنوع هذه الطبيعة والتي اتسمت بالتباين والاختلاف.

1/- الرأي الأول: اعتبار المستند الإلكتروني يدخل ضمن النظام المعلوماتي إلى طبيعة منقولة يمكن حيازته، وبالتالي يطبق عليه قانون الذي ينظم الحيازة والقانون الذي ينص على معاقبة المساس به كسرقة والاتلاف، وبالتالي يتوجب أن يتعرض لكل من ارتكب جريمة تمس بالمستند الإلكتروني إلى العقوبات المقررة والمنصوص عليها في قانون المعلومات لكل من مس بحق من الحقوق المقررة للمنقول.

2/- الرأي الثاني: إتجه هذا الرأي إلى اعتبار البيانات الإلكترونية أو المستندات الإلكترونية لا تعدو وأن تكون مالا معنويا يتساوى في المدلول مع المال المنقول، وأنه مال به كيان مادي يمكن إدراجه وحيازته، وينهى هذا الرأي الى انه بالإمكان تطبيق النصوص المتضمنة لعقوبات التي تجرم المساس بهذا المنقول على أفعال المساس بالبيانات الإلكترونية.

3/ الرأي الثالث: لقد أقرّ هذا الاتجاه على اعتبار المستند الإلكتروني هو بمثابة من المال المنقول، لأنه لا يعقل أن نقوم بحياسة مال غير موجود، وبالتالي فإنه لا تنطبق عليه العقوبات في حالة خرق أو تلف هذه المستندات، وعليه فإن المستند الإلكتروني ذو طبيعة معلوماتية كما سبق ذكره، فإنه يسهل حفظه لأنه يتم بطريقة إلكترونية حديثة وسهلة يتيسر الإطلاع عليها بشكل يسهل الرجوع والإطلاع عليها لاحقاً ومن هنا نجد الأهمية القانونية للمستند الإلكتروني أدى بالتشريع والفقهاء والقضاء في كثير من الدول إلى التفكير ملياً في وضع صيغ تشريعية بشكل يسمح بوضع حلول لمختلف المشاكل التي تفرزها التطورات جرّاء استعمال المستند الإلكتروني، وهنا تم التّطرق إلى حقيقة المستند الإلكتروني وإلى أهميته الكبيرة في مجال الأنترنت وإن الحديث عن الطبيعة المعلوماتية للمستند الإلكتروني تحيلنا عن الحجية القانونية دون الحاجة إلى غطاء تشريعي ينظمه على وجه الخصوص عن طريق منح المستند مفهوماً موسعاً ليشمل المستند الورقي والمستند الإلكتروني، وأيضاً نجد أن الطبيعة القانونية تشمل فكرة الإدارة الإلكترونية التي يشاع تسميتها "الحكومة الإلكترونية"، إذ أنها تقتضي استخدام نظم المعلومات الرقمية في إنجاز المعاملات الإدارية وتقديم الخدمات المرفقية والتواصل مع المواطنين بمزيد من الإفصاح والشفافية.

الفرع الثاني: تميز المستند الإلكتروني عن ما شابهه

إذا أردنا معرفة تميز المستند الإلكتروني عن ما شابهه لابد من الاعتماد على مبدأ المقارنة بينه وبين المستند الورقي أو المحرر الورقي، وخاصة من حيث التعريف والحجية والإثبات ويتمثل المستند الإلكتروني مع المحرر الورقي أو التقليدي في عدة أمور، ويختلفون في أمور أخرى، حيث أن كلاً منها يحمل ملامح وخصائص يميز بها كل مستند عن غيره، وفيما يلي نوضح نقاط الاتفاق والاختلاف بين كل منها:

أولاً: أوجه الاتفاق

يتشابه المحرر الإلكتروني والمحرر الورقي (التقليدي) في أن كلاهما يحتوي على مجموعة من الرموز التي تعبر عن مجموعة مترابطة من الأفكار والمعاني الإنسانية، يدعو المشرع إليها لحمايتها¹.

1/- ويترتب الاعتداء على كلاهما وقوع ضرر يمس مصلحة عامة في المجتمع ، وتتمثل في المساس في الثقة العامة.

2/- كلاهما يحمل صفة المحرر الرسمي أو المحرر العرفي².

3/- المحرر الإلكتروني والمحرر الورقي كلاهما له حجية الإثبات وخاصة إذا اثبت فيه موظف عام أو شخص مكلف بخدمة عامة ما تمر على يده أو تلقاه من ذوي الشأن طبقاً للأوضاع القانونية وفي حدود سلطته اختصاصه.

ثانياً: أوجه الاختلاف

1/- يختلف المحرر الإلكتروني (المستند) عن المحرر التقليدي من حيث الشكل، بحيث يكتب المحرر التقليدي يكتب بطريقة يدوية وآلية في كيان مادي ملموس، ومن ثم يسهل قراءته بالعين المجردة، أما المحرر الإلكتروني فهو يعالج عن طريق المكونات المادية والمعنوية لأجهزة الحوسبة والاتصالات، ويسجل على دعامة مغناطيسية تحمل الطابع الافتراضي أو المعنوي³.

2/- يختلف المستند الإلكتروني عن المحرر التقليدي من حيث الإثبات وحجية كل منهما، حيث أن المحرر التقليدي (الورقي) يطغى على نظيره المستند الإلكتروني من حيث الإثبات، وهذا راجع إلى أن المستند الإلكتروني هو موضوع حديث حداثة قوانينه وعدم وجود قوانين كافية

¹ - إيهاب فوزي السقا، مرجع سابق، ص 18.

² - محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، سنة 2013، ص 279.

³ - نبيل صقر، مكاري نزيهة، الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية، دار الهدى، الجزائر، 2009، ص 274.

لإثباته وللتعريف به وتعزيزه بنص ينظمه كباقي المواضيع، وهذا عكس المحرر الورقي الذي تم تنظيمه بنصوص خاصة وعامة، أعطت له القوة القانونية والحجية الإثباتية للمتعاملين به.

3- 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.

4- لقد نادى الفقه أيضا بضرورة وجود قوانين خاصة بتنظيم المستند الإلكتروني بتنظيم خاص، حيث تم اكتشاف أن الكثير من الأفراد والشركات والجهات المختلفة خسرت أموالا باهظة بسبب التعامل بالوسائل الإلكترونية¹.

5- المحرر الورقي له أصل ورقي حتى وإن تم إرساله عبر أجهزة الحاسب الآلي، مثل الفاكس والبريد الإلكتروني بعد إجراء عملية المسح الضوئي له، بينما المحرر الإلكتروني مخزن ومحفوظ إلكترونيا.

6- يتميز المحرر الورقي بصفة الدوام والثبات، فهو يكون بطريقة نهائية ومن ثم يسهل كشف أي تلاعب أو تزوير 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 عون مهني متخصص في الحاسب والمعلوماتية وان التكنولوجيا الحديثة أوجدت أنظمة تقنية وقائية على درجة عالية من الثقة تحفظ وتؤمن المحررات الإلكترونية من أي تلاعب أو أي اعتداء يقع عليها².

¹ - شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، مصر، دار الجامعة الجديدة، الطبعة الأولى، السنة 2007، ص 08.

² - إلهام بن خليفة، مرجع سابق، ص 26.

المبحث الثاني: النظام القانوني للمستند الإلكتروني وحجته في الإثبات

إن الأحكام والضوابط التي تميز المستند الإلكتروني عن غيره من المستندات تقوم على عدة اعتبارات تطبع مراحل إنشائه وتوثيقه، وهذه الأحكام هي من تجعله صحيحا وقانونيا تمكن مستعمله بالدفع به وقت الضرورة ولهذه الغاية لابد من توفر شروط تضي عليه الصفة الرسمية.

المطلب الأول: النظام القانوني للمستند الإلكتروني وشروط صحته

إن خضوع المستند الإلكتروني للعديد من الأحكام والضوابط التي تميزه عن غيره من المستندات فصحته تقوم على عدة اعتبارات تطبع مراحل إنشائه وتوثيقه، وكل ذلك من أجل أن يكون المستند صحيحا، يمكن مستعمله بالدفع به وقت الضرورة، ومن ثم يجب توثيقها بشكل يسهل على اطرافه الرجوع إليه إذا اقتضى الأمر ذلك، وإن دراسة النظام القانوني للمستند الإلكتروني يجب علينا التطرق أولا إلى توثيقه وتنظيمه وفقا لما جاءت به النصوص القانونية.

الفرع الأول: تنظيم المستندات الإلكترونية.

إن مختلف التعاملات الإلكترونية وكل العقود الإلكترونية تتميز بعدم حضور كل أطرافها أثناء انعقادها في كل المجالات والمعاملات الإلكترونية بكل اختلافاتها وخصوصياتها، ففي مجال التجارة مثلا: المتعاقدان يكونان غائبين مما يخول لأصحاب النية السيئة القيام بمجموعة من التصرفات التي يطبعها الاحتيال والغش والتزوير في الخدمة موضوع التعاقد، مما استلزم معه إنشاء جهات توثيق إلكترونية سواء حكومية أو خاصة تتكلف بها النوع من الخدمات ولقد كان المشرع التونسي أول المهتمين عربيا بمجال التعاملات الإلكترونية، حيث نظم هذا المجال في القانون رقم 83 لسنة 2000، في حين لم تنظم مختلف التشريعات الأخرى التعاملات الإلكترونية إلا فيما بعد بقوانينها الخاصة وخاصة في معرفة مقدمي خدمات المصادقات الإلكترونية في تأمين وحفظ الشهادات الإلكترونية ولقد تطرق القانون المغربي من خلال المادة

21 من القانون رقم 53-05 إلى المهام التي تناط بمقدم خدمات المصادقة الإلكترونية، وذلك اثناء عرضه للشروط التي يجب أن تتوفر فيه لاكتساب صفة مقدم خدمات المصادقة، وهذه المهام تتجلى كما الآتي:

1/- يلتزم مقدم الخدمات بالتحقق من هوية الشخص الذي سلمت له شهادة إلكترونية ومطابته بالإدلاء بوثيقة هوية رسمية للتأكد من أن الشخص يتوفر على الأهلية القانونية للالتزام من جهة، وبالصفة التي يدعيها من جهة أخرى والمحافظة على مميزاته ومراع الوثائق المدلى بها لإثبات هذه الهوية وهذه الصفة.

2/- من مهامه أيضا التأكد وقت تسليم الشهادة الإلكترونية أن المعلومات التي تحتوي عليها صحيحة، وأن الموقع المشار إلى هويته يمتلك معطيات لإنشاء التوقيع الإلكتروني، تطبق معطيات التحقق من التوقيع الإلكتروني المضمن في الشهادة¹.

3/- إخبار الشخص الذي يطلب تسليمه شهادة إلكترونية كتابة بكيفيات وشروط استعمال الشهادة وكيفية المنازعة وطرق تسوية الخلافات، وتقديم هذه العناصر إلى الأشخاص الذي يستندون إلى شهادة إلكترونية، بإخبار أصحاب الشهادة المؤمنة، يستبين يوما على الأقل قبل تاريخ إنتهاء صلاحية شهادتهم، وذلك لتمكينهم من تجديدها أو إلغائها وإبرام تأمين لتغطية الأضرار الناتجة عن أخطائه المهنية وإخبارهم بإلغاء الشهادة الإلكترونية في حالة كان هناك سبب من أسباب الإلغاء.

الفرع الثاني: شروط صحة المستند الإلكتروني.

أولاً: الكتابة

الكتابة من أول طرق الإثبات المختلفة في إثبات صحة المستند الإلكتروني ووضعه في قالب قانوني، ونجد أهمية الكتابة في القوانين الحديثة، حيث أضيفت عليها حجية مطلقة، مادام التي لم ينكرها أو يدع تزويرها وتعتبر الكتابة بدقة عن الواقعة التي أدت لإثباتها، فهي دليل واضح

¹ - منشور بالجريدة الرسمية رقم 5584 بتاريخ 2007/12/06.

عند حدوث نزاع بين أطراف الاتفاق وتعطي أكبر قدر من الاطمئنان لدى المتعاقدين ويقصد بالكتابة في شكلها التقليدي بأنها "مجموعة الأحرف والأشكال والرموز والإشارات أو الأرقام المتسلسلة على أن تكون قابلة للقراءة ومترابطة وتعتبر عن فكرة معنية"¹.

أما المقصود بها في الشكل الإلكتروني حسب نص المادة 323 مكرر من التقنين المدني الجزائري: "بأنها تسلسل حروف أو أوصاف أو أرقام وأية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها"².

وهو نفس التعريف الذي نص عليه القانون المدني الفرنسي في المادة 1316 منه، وكذا التشريع المصري والعراقي، وعليه يمكن القول أن الكتابة الإلكترونية حتى يعتد بها في الإثبات يجب توفر عدة شروط تتمثل فيما يلي:

1/- أن تكون مقروءة: يجب أن تكون مقروءة ومستبينة حتى يمكن الاعتداد بها، 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 بقاءها مدة معقولة، وأخيرا يجب أن يصعب العبث بها أو التعديل فيها دون أن يترك ذلك أثراً على المحرر الذي يحتويها³.

وبالرجوع إلى قانون الأونيسترال النموذجي لعام 1996، نجد أنه أشار إلى هذا الشرط في نص المادة السادسة منه، كما أشارت التشريعات الوطنية المقارنة في هذا المجال إلى ذلك (على أن تكون الرموز).

¹ - براهيمى حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه تخصص قانون جنائي والعلوم السياسية مرجع سابق، ص 107 - 108 - 109. جامعة محمد خيضر بسكرة 2015.

² - الأمر 85/75 المؤرخ في 26/09/1975، المتضمن التقنين المدني الجزائري المعدل والمتمم بالقانون رقم 10/05 المؤرخ في 20/06/2005، ج.ر رقم 44 الصادرة بتاريخ 26/06/2005، ص 24.

³ - عابد فايد عبد الفتاح، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني، دار الجامعة الجديدة، الإسكندرية، 2014، ص 46.

2/- الكتابة الإلكترونية ثابتة ومستمرة:

يشترط في الكتابة الثبات والاستمرارية، وهما صفتان ملازمتان للمستند الورقي وهو أمر صعب التحقق بالنسبة للمستند الإلكتروني وليس مستحيل التحقق، بالرغم من أن الكتابة الإلكترونية تكون عرضة للتلف بسبب اختلاف في قوة التيار الكهربائي، أو تخريبها بسبب الفيروسات أو الاعتداء عليها بالمحو أو التعديل الكلي أو الجزئي عمدا من الغير، وعليه تمت مقابلة كل هذه المخاطر بوسائل أمنية وتقنية من أجل ضمان ثباتها واستمراريتها، ويتحقق هذا الشرط يصبح المستند الإلكتروني يعادل المستند الورقي من حيث اعتباره كدليل من أدلة الإثبات، بحيث يمكن الرجوع للمستند الإلكتروني بسهولة عند الحاجة إليه في الإثبات¹.

3/- الكتابة الإلكترونية غير قابلة للتعديل:

وإن عدم قابلية الكتابة الإلكترونية للتعديل يعني أنه لا بد من سلامة المحتوى من أي تحريف أو زيادة أو نقصان في مضمونها أي بقاء الكتابة الإلكترونية على الحالة التي تم إنشاؤها عليها أول مرة، ويتم تحقيق هذا الشرط من الناحية التقنية عن طريق برامج إلكترونية مخصصة لذلك تعمل على تحويل الكتابة الإلكترونية التي يمكن التعديل في محتواها إلى نموذج ثابت غير قابل للتعديل أو التغيير، أو بواسطة الاستعانة ببرامج إلكترونية تسمح بكشف أي تعديل أو تغيير يمس بالكتابة الإلكترونية، وتحديد البيانات المضافة أو المحذوفة وتاريخ حدوث ذلك بدقة متناهية، وحيث نص قانون الأونيسترال النموذجي في نص المادة العاشرة الفقرة الثانية على هذا الشرط، كما تضمنت التشريعات الوطنية المقارنة ذلك، حيث أشار التشريع المصري إلى هذا الشرط في نص المادة الثامنة عشر من قانون التوقيع الإلكتروني رقم 15 لسنة 2004، واشترط سلامة المستند الإلكتروني من أي تعديل أو تبديل في الكتابة الإلكترونية حتى تتمتع بالحجية في الإثبات أما التشريع العراقي، فقد نص على هذا الشرط في المادة الثانية عشر، الفقرة "ب" من قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012، كما تناول المشرع الإماراتي هذا الشرط في المادة الخامسة من القانون الاتحادي

1- عابد فايد عبد الفتاح، مرجع سبق ذكره، ص 51.

رقم 01 لسنة 2006، والمتعلق بالمعاملات والتجارة الإلكترونية في الفقرة "أ" منه، وبخصوص التشريع التونسي فقد تناول ذلك في الفصل الرابع من القانون رقم 83 لسنة 2000، والمتعلق بالمبادلات التجارية، أما بالنسبة للمشرع الجزائري فقد نص على هذا الشرط في المادة 323 مكرر 01 واشترط أن تكون الكتابة في الشكل الإلكتروني معدة ومحفوظة في ظروف تضمن سلامتها من أي تغيير أو تعديل في مضمونها، وبذلك فإذا توفرت الشروط القانونية السابقة الذكر في الكتابة الإلكترونية فإنه يمكن الاعتداد بها كدليل اثبات للتصرف القانوني وكذلك بالنسبة أيضا في مجال العقود بين الطرفين لا يجب التغيير أو التعديل أو التلاعب في البيانات أو بنود العقد مثلا، وإن أي تغيير يؤثر على التزامات الأطراف، وبالتالي على المراكز القانونية لأصحاب الحقوق، والمقصود بعدم قابلية التعديل هو عدم القدرة على التغيير في بيانات المحرر الورقي بمجرد النظر أو الاستعانة بذوي الخبرة في هذا الشأن، أما في ما يتعلق بالكتابة الإلكترونية، فإن هذا الشرط يعتمد على الدعامات المثبتة عليها المعلومات، فإذا كانت الدعامة غير دائمة، والمقصود بها المتكررة في الاستعمال كالدسك والقرص المرن والفلاش ديسك، يمكن إزالة الكتابة فيها ووضع كتابة أخرى، أما الدعامة الدائمة فهي لا تستعمل إلا مرة واحدة كالأسطوانة أو السي دي (c.d) لا يمكن محو ما كتب عليها إلا بإتلافها أو ترك أثر مادي عليها وتستعمل وسيلتي التشفير والتوثيق لمنع التلاعب والتعديل¹.

وإن بقاء المحتوى السري للمستند كما هو عند إنشائه هو ما نعنيه بحفظ المعلومات طوال مدة التقادم التي يخضع لها التصرف الملحوظ، 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 الأونيسترال في المادة 10 إلى الشروط التي يجب توافرها عند حفظ المستند الإلكتروني وهي:

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

¹ - عابد فايد عبد الفتاح، مرجع سابق، ص 65.

2- الاحتفاظ بالشكل الذي أنشأ أو استلم به أو بشكل يمكن إثباته أنه يمثل بدقة المعلومات التي أنشأت أو أستلمت.

3- الاحتفاظ بالمعلومات إن وجدت والتي تمكن من استبانة منشأ المستند الإلكتروني وجهة وصوله وتاريخ ووقت إرساله واستلامه¹.

ثانياً: التوقيع

لا يمكن الاعتماد بالمستند الإلكتروني من الناحية القانونية، إلا إذا اشتمل على توقيع من صدر عنه باعتبار أنه شرط جوهري سواء في المستند التقليدي أو الإلكتروني والذي يقصد منه مرافقة الموقع وإقراره لما هو مدون وموجود على المستند الإلكتروني، وبذلك فلا ينتج المستند الإلكتروني آثاره القانونية إذا لم يكن موضوع عليه توقيع الإلكتروني يميز هوية الموقع، ويعبر عن إقراره وموافقته لما تضمنه من بنود وشروط في إطار الضوابط التي تنص عليها التشريعات في هذا المجال و حيث نجد قانون الأونيسترال النموذجي قد نص على ذلك في المادة السابعة منه، أين اعتبر صحة المستند الإلكتروني مرتبطة بوجود توقيع إلكتروني عليه، أما التشريعات الوطنية المقارنة فقد نصت على هذا الشرط سواء في القواعد العامة للإثبات مثل التشريع الفرنسي والجزائري، أو في قوانين خاصة مثل التشريع الإماراتي والعراقي، ومن خلال ما سبق تناوله من تشريعات، مقارنة ما نصت عليه لصحة المستند الإلكتروني وتمتعه بالحجية الكاملة في الإثبات فإنه لا بد أن يتضمن توقيع من صدر عنه حتى يكون منتج لآثاره القانونية، وبالتالي فإن تخلف هذا الشرط ينفي عن الكتابة الإلكترونية صفة المستند الإلكتروني، وعليه فإن توقيع المستند الإلكتروني أمر بديهي للاحتجاج به قانوناً، ولقد عرف أيضاً قانون الأونيسترال النموذجي في المادة (2) منه أن التوقيع الإلكتروني (بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتقييم هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات².

¹ - براهيم حنان، مرجع سابق، ص 144.

² - إيهاب فوزي السقا، مرجع سابق، ص 31.

التوقيع الإلكتروني هو بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق¹.

كما عرفته المادة 07 من القانون 15-04 انه "التوقيع الإلكتروني الموصوف هو التوقيع الذي تتوفر فيه متطلبات معينة².

وكذلك يعرف التوقيع الإلكتروني بأنه جزء صغير مشفر من بيانات يضاف إلى رسالة إلكترونية، فهو جزء من الرسالة ذاتها يشفر ويرسل مع الرسالة، ليتم التوثيق من صحة الرسالة بفك التشفير وانطباق محتواه على الرسالة³.

وقد نص المشرع الجزائري على هذا الشرط في نص المادة الثانية من القانون 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع الإلكتروني والتصديق ويقوله أن التوقيع الإلكتروني (بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق)، وبالرجوع إلى نص المادة 327 من القانون المدني، نجد أن المشرع قد اعتد به شريطة أن تتوافر فيه الشروط المنصوص عليها في المادة 323 مكرر 01 من القانون المدني الجزائري التي تنص على أنه "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي اصدرها وأن تكون منظومة إنشاء التوقيع الإلكتروني محفوظ في ظروف تضمن سلامته"⁴.

¹ - الجريدة الرسمية للجمهورية الجزائرية، العدد 06، 20 ربيع الثاني عام 1436هـ/ الموافق ل 10 فبراير سنة 2018، ص 07.

² - قانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج، عدد 06 صادر في 10/02/2015.

³ - خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، المركز القومي للإصدارات القانونية، الطبعة الأولى، (د.م.ن)، 2009، ص 15.

⁴ - الأمر رقم 75-85 المتضمن القانون المدني الجزائري.

وقد عرف أيضا التوقيع الإلكتروني على أنه "وحدة قصيرة من البيانات التي تحمل علاقة رياضية من البيانات الموجودة في محتوى الوثيقة"¹

وتعرف أعمال لجنة التجارة الدولية التابعة للأمم المتحدة cnudci في قانون التجارة الإلكترونية الصادر عنها عام 1996، على أن التوقيع الإلكتروني هو عبارة عن مجموعة أرقام تمثل توقيعاً على رسالة معينة، يتحقق هذا التوقيع من خلال اتباع الإجراءات الحسابية المرتبطة بمفتاح رقمي خاص بالشخص المرسل، ومن ثمة فإنه بالضغط على هذه الأرقام الخاصة بالشخص يتكون التوقيع الإلكتروني، ويقصد بالتوقيع الإلكتروني في مشروع قانون التجارة الإلكترونية المصري بانه "حروف أو أرقام أو الرموز أو الإشارات لها طابع منفرد تسمح بتحديد شخصية صاحب التوقيع وتمييزه عن غيره"، مما يستفاد من نص المادة على أنه ينبغي أن يكون للتوقيع طابع متميز يتم من خلاله تحديد هوية الموقع وتمييزه عن الغير، وهناك صور للتوقيع الإلكتروني وأهمها التوقيع الرقمي أو الكودي والتوقيع البيومتري والتوقيع بالقلم الإلكتروني².

ثالثاً: التوثيق أو (التصديق الإلكتروني)

يقصد بالتصديق هو اللجوء إلى طرف ثالث محايد ومستقل عن الأطراف، سواء كان فرداً عادياً أو شركة أو جهة من الجهات، من أجل توثيق المعاملات الإلكترونية لأشخاص، وبهذا يتحدد وضع الموثق أو المصدق بأنه وسيط بين المتعاملين يلجأ إليه بغرض منح الثقة في محرراتهم حتى يمكنهم من استخدامها لإثبات ما تتضمنه من تصرفات قانونية، ولهذا السبب يطلق عليه البعض وكلاء الإثبات³.

¹ فيصل سعيد الغريب، التوقيع الإلكتروني وحجبه في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، 2005، ص 217.

² عبد الفتاح بيومي الحجازي، مرجع سابق، ص 16.

³ عابد فايد عبد الفتاح، مرجع سابق، ص 70 - 71.

وتلعب شهادة التوثيق الإلكتروني دوراً مهماً 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 بطلب التوقيع والتأكد من صحتها، ليتم منح هذا الشخص مفتاح تشفير خاص يتسم بالسرية، حيث يحتفظ به الموقع، ويتم تثبيت نصفه في جهاز الكمبيوتر الخاص به، والنصف الآخر في بطاقة إلكترونية، أما جهة التوثيق فتحتفظ بالمفتاح العام، حيث تقوم بإرساله بالبريد الإلكتروني إلى اشخاص الذين يتعامل معهم الموقع، وذلك لاستخدامه في فك التشفير¹.

ومن خلال هذه التعريفات نجد أن دور التصديق والهدف من وراءه هو التحقق والتأكد من الأهلية القانونية للأشخاص الموقعين وصحة وجدية الإرادة التعاقدية ونسبتها إليها وبعدها عن الغش والاحتيال وذلك بتحديد مضمون هذه الإرادة واتجاهها نحو القيام بهذا التصرف القانوني².

المطلب الثاني: حجية المستند الإلكتروني في الإثبات

إن التغلغل المتعظم والمتزايد لأنظمة الاتصال الحديثة ذات الطبيعة المعلوماتية التي يتم من خلالها المستند الإلكتروني دفع التشريع والفقهاء والقضاء في العديد من البلدان إلى التفكير ملياً في وضع صيغ تشريعية وتنظيمية جديدة تسمح بوضع حلول لمختلف المشاكل التي تفرزها هذه التطورات ويبدو جلياً أن المشكلة الحقيقية في مجال التعامل عن طريق المستند الإلكتروني هي مشكلة الإثبات ولقد ذكرنا سابقاً أن الكثير من القوانين لم تنظم وتحدد قيمته في الإثبات، لذا فقد نتج عن هذا النص التشريعي خلاف حادّ حول حجية هذا المستند في إثبات التصرفات القانونية التي تنشأ من خلاله، فقد ذهب اتجاه يعطي المستند الإلكتروني مفهوماً موسعاً، بحيث

¹ - براهيمى حنان، جريمة التزوير الوثيقة الرسمية الإدارية مرجع سابق ص 153.

² - مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، تدعيم الثقة وتأمين للتعامل عبر الانترنت، دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط سلطة عمان، 23 نوفمبر 2008، ص 18.

يشمل المستند الورقي وكذلك المستند الإلكتروني، في حين يذهب إتجاهها آخر متناقضا للاتجاه الأول، فلا يعطي المستند الإلكتروني أي قيمة قانونية إلا عن طريق التنظيم التشريعي¹. إن ما يترتب عليه عدم مواكبة القوانين، ولاسيما 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، ومن تلك البلدان نجد الجزائر مثلا².

ولقد أدى الانكباب المتزايد على أدوات الاتصال المعلوماتية في مجال المعلومات إلى الاعتماد بشكل كبير على المستندات الإلكترونية، وذلك للدور الكبير الذي أصبحت تلعبه هذه الأنواع من الوثائق ومع تزايد الاعتماد عليها يوما بعد يوم في إدارة ونفاذ الأعمال المخالفة وفي إطار سعي الدول نحو عالم الرقميات كبديل لعالم المحسوسات، يزداد الاهتمام بمدى حجية وقوة المستندات الإلكترونية من حيث الإثبات، والإثبات بمعناه القانوني هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتب في مواجهة من ينكرها آثار قانونية لمن يدعيها³.

الفرع الأول: حجية المستند الإلكتروني في الإثبات في ظل غياب النص

لقد كان الإشكال الثاني الذي واجه المستند الإلكتروني إلى جانب مشكل الإثبات هو مشكل تحديد مفهوم المستند الإلكتروني، حيث أن بعض الفقه فسّر المستند تفسيراً موسعاً يشمل المستند الإلكتروني والمستند الورقي أيضاً وإن الهدف من تحديد ماهية المستند هو الوقوف على جانب آخر من جوانب الاختلاف المتعلقة بالمستند، وهي الكتابة فيقول بعض الفقهاء أن كلمة

¹ - عمار كريم كاظم و نارمان جميل نعمة، مرجع سابق ص 173.

² - داديار حميد سليمان، دور السندات المستخرجة عن طريق الأنترنت لإثبات المسائل المدنية (دراسة تحليلية مقارنة)، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2010، ص 131-132.

³ - عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، آثار الالتزام، الجزء الثاني، دار إحياء التراث العربي، الصفحة

مستند تحمل معنيان أو بالأحرى تشمل نوعان من المستندات الإلكترونية والورقية، لأن المفهوم اللغوي للمستند لا يقتصر على نوع معين وإنما يشمل الكتابة بمفهومها التقليدي الحديث، حيث تتساوى الكتابة سواء كانت على دعامة ورقية أو دعامة إلكترونية، لأنها عبارة عن مجموعة من الحروف والرموز التي يمكننا إيجادها في المحرر الورقي والمحرر الإلكتروني معا، ولا يكون خلاف في ذلك ويرى انصار هذا الاتجاه أن تفسير كلمة مستند يمتد ليشمل المستند الورقي والإلكتروني، ذلك أن تعبير المستند لغويا لا يقتصر على نوع معين وإنما يشمل الكتابة بمفهومها التقليدي والكتابة عن طريق الوسائل الإلكترونية، فالكتابة حسب تفسير أصحاب هذا الاتجاه هي عبارة عن مجموعة الحروف والأرقام والرموز والإشارات التي تدل على معنى معين، وتكون ثابتة على دعامة قوية، وإذا كان ينظر سابقا إلى أن هذه الدعامة هي ورقية وتحتوي على بيانات معينة ويذيلها توقيعها يدويا ناتجا عن طريق الطرفين، سواء كانت مكتوبة باليد أو بواسطة ماكينة فإن هذا التطور المستمر في الوسائل الحديثة التي تتم من خلالها إجراء التصرفات القانونية يؤدي بنا إلى تغيير النظرة التقليدية لمفهوم الكتابة التي تتم يدويا، فالغرض من استلزام أن يأخذ العقد شكلا معيناً، ليس المقصود منه الدعامة الورقية بذاتها وإنما تعد الدعامة الورقية وسيلة لتثبيت المعلومات عليها، فكل ما في الأمر يجب أن تكون الكتابة مقروءة بسهولة مع إمكانية الرجوع عليها ونقلها ونسخها، لذا يجب التخلي عن المفاهيم القديمة (المستند) و(الكتابة) و(التوقيع) والأخذ بفكرة الكتابة الإلكترونية التي تحتوي مميزات تقنية تضمن سلامتها، وقد تتجاوز الضمانات التي تتمتع بها الكتابة اليدوية، فلا يوجد تلازم بين فكرة الكتابة والورق بمعناه التقليدي¹.

إلا أن هناك رأياً فقهيًا بوجود صعوبة في إضفاء طابع الإثبات على المحررات الإلكترونية، خاصة في مجال الاتصال وذلك تحت عدة مبررات تتمحور حول أن الدعامة الإلكترونية قابلة للتعديل والتبديل دون وجود أي دليل يثبت هذا التعديل، كما أن هذا النوع لا يترك أثراً مدوناً عكس الأثر الذي تتركه الدعامة الورقية، إلا أن هذا الرأي أصبح متجاوزاً، وذلك بفضل التطور

¹ - عمار كريمة كاظم و نارمان جميل نعمة، مرجع سابق، ص 182.

الذي عرفه هذا المجال، فقد ظهرت مجموعة من التطبيقات التي تدعم صحة المستند الإلكتروني، وتقوي كمسألة الضمان والإثبات وجعله بذلك يوازي عن المستند الورقي، ومن بين هذه التطبيقات التي ظهرت نجد نظام الإشعار بالتوصل الذي يسمح بالتثبت من وضع الرسالة الإلكترونية، وتمكن كذلك المرسل من معرفة تاريخ ووقت توصل المرسل إليه بالرسالة، ومن بين التطورات أيضا التي تؤيد قوة المستند الإلكتروني وتضاعف فرصة التمسك به كأداة للإثبات نجد نظام تشفير المعلومات في المستند الإلكتروني وكان لهذا النظام الفضل في الحفاظ على سرية المعلومات وعدم الإطلاع عليها إلا من طرف الأشخاص المرخص لهم بالإطلاع، وهذا ما يؤكد أن للمستند الإلكتروني مميزات تؤمن استخدامها من قبل الأطراف المتعاقدة، وتتجاوز الإجراءات التي تحمي المستند الورقي في حين يجعل رأيا آخر من الوسائل التقنية التي تضمن سلامة المستند الإلكتروني انتقادا يعترض بموجبه على المساواة بين الكتابة الإلكترونية واليدوية، إذ يرى أن الكتابة اليدوية يمكن قراءتها بسهولة وبصورة مباشرة، في حين الكتابة الإلكترونية تقتضي قراءتها فك بعض الرموز التشفيرية عند حالة تشفير الكتابة لحماية المعلومات من الانتقال، إذ أن هذه المعلومات تعد غير مقروءة إلا بعد اتخاذ إجراءات معقدة وصعبة، لذا فإن الكتابة الإلكترونية لا يسهل قراءتها بصورة مباشرة وسهلة مثل الكتابة اليدوية¹. والجدير بالذكر أن أساس الإثبات هو الحرية في جميع المعاملات التي تسمح بإثبات تصرفات قانونية بكافة الطرق، وإن تطبيق هذا المبدأ أن يعطي كل الأطراف العقد الحرية في إثبات التصرفات القانونية وإقامة الحجة على التزاماتهم وإدعاءاتهم بجميع الطرق المتاحة، ومن مميزات تطبيق هذا المبدأ هو إعطاء القاضي الحق في تقدير قيمة الدليل المستمد من الوسائل الإلكترونية، وهذا يخص العقود المدنية الإلكترونية، وهذا في إبرام العقد عن طريق الإيجاب والقبول يؤدي إلى وجود العقد وإنتاج آثاره.

1- عمار كريم كاظم و نارمان جميل نعمة، مرجع سابق، ص 42.

الفرع الثاني: حجية المستند الإلكتروني في ظل وجود نص

إن الهيكل القانوني التنظيمي المقنن يعني بفكرة المستند الإلكتروني، إذ أن القوانين المقارنة قد لجأت إلى إصدار تشريعات خاصة تنظم صور للمستند الإلكتروني كالتوقيع والسجل الإلكتروني والعقود الإلكترونية، وتتوقف حجية المستند في الإثبات على القيمة التي يمنحها المشرع له، فإذا أقر النص القانوني هذه الحجية يصبح المستند الإلكتروني مساويا للمستند الورقي من حيث القيمة القانونية، لذا فقد لجأت القوانين التي نظمت هذه الفكرة إلى الاعتراف صراحة بحجية المستند الإلكتروني مع مساواته بالمستند الورقي ويعد وعي الدول بالدور الذي تلعبه المستندات الإلكترونية نجدها لجأت لتنظيم هذا الموضوع والاعتراف به صراحةً في نصوص تنظم كيفية الاستفادة منه، وإن الوثيقة المحررة على دعامة بنفس قوة الإثبات التي تتمتع بها الوثيقة المحررة على الورق كمنظيرتها الورقية ليزيل بذلك كل الخلافات التي كانت تزعم وتتعدى بعدم جواز إضفاء صفة الثبوتية على المحررات الإلكترونية وهناك عدة تشريعات ومنها قانون التوقيع الإلكتروني والسجلات الإلكترونية لولاية نيويورك الأمريكية في نص المادة (105) منه على أن "السجل الإلكتروني يكون له ذات القوة الأثر المقرر للسجلات المحررة بغير الوسائل الإلكترونية" وفي حين نصت المادة (1/5) من قانون المعاملات الإلكترونية البحريني إلى أن (السجلات الإلكترونية ذات الحجية المقررة في الإثبات للمحركات العرفية ولا ينكر الأثر القانوني للمعلومات الواردة في السجلات الإلكترونية، من حيث صحتها وإمكان العمل بمقتضاها بمجرد ورودها كلياً أو جزئياً في شكل سجل إلكتروني أو الإشارة إليها في هذا السجل) أما المادة (4) من مشروع قانون التجارة الإلكترونية الكويتي لسنة 2006 قد جاءت شاملة لكل تطبيقات المستند الإلكتروني، إذ جاء فيها (تتمتع المعلومات التي تتخذ شكل مستند إلكتروني بذات الأثر القانوني المقرر للمستند الإلكتروني)¹.

¹ - عمار كريم كاظم و نارمان جميل نعمة، مرجع سابق، ص 192.

وبالعودة إلى المشرع المغربي فرغم أنه أقر بأن يمنح للمستند الإلكتروني نفس قوة الإثبات الممنوحة للمستند الورقي، فقد أخضع هذا المبدأ لعدة شروط تتنافى مع وجودها ميزة الإثبات في المستند الإلكتروني وهذه الشروط كالتالي:

1/-الشرط الأول: هو إمكانية التعرف بصفة قانونية على الشخص الذي صدرت منه وذلك أن تحل المعلومات الإلكترونية على هوية الشخص الذي أنشأ هذه المعلومات أو تسلمها وأن تشمل أيضا على تاريخ إرسالها وتاريخ تسلمها، وأن تكون هذه المعلومات واضحة وقابلة للقراءة وعدم استعمال أي وسائل غير مشروعة القصد منها عدم التعرف على معلومات المستند.

2/-الشرط الثاني: هو أن تكون محفوظة ومعدّة ضمن شروط تضمن تماميتها ومقتضى هذا الشرط هو أن يكون المستند الإلكتروني قابل للحفظ والتخزين والارشفة شأنه في ذلك شأن المستند التقليدي، وذلك بالطرق الفنية المعروفة وكما أن المشرع الفرنسي قد منح المحررات الناتجة عن الفاكس والتلكس والميكروفيلم، نفس القوة القانونية للمحررات التقليدية سواء كانت أصل المستند أو صورته، ولقد أكد المشرع الفرنسي على أنه في حالة تعرض سند إلكتروني وسند تقليدي يجب على القاضي أن يفاضل بينهما و أن يعتمد على الوسيلة التي أبرم بها السند وكما بيّنت المادة السادسة من القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية، حيث يتم الأخذ بسلامة الوثيقة وأخذ كذلك صفة الإثبات بموجب قانوني، وهذا ضمن شروط هي:¹.

1/- أن يكون خاصا بالموقع و يتم إنشاؤه بوسائل يمكن للموقع الاحتفاظ بها تحت مراقبة خاصة بصفة حصرية.

2/- أن يتضمن وجود إرتباطه بالوثيقة المتصلة به بكيفية تؤدي إلى كشف أي تغيير لاحق أدخل عليها ويجب أن يوضع التوقيع بواسطة آلية لإنشاء التوقيع الإلكتروني تكون صلاحيتها مثبتة بشهادة للمطابقة، وتأتي هذه الشروط كقيود لضمان صحة التوثيق إذا كان التوقيع موثوقا به، فهذا من شأنه أن يضيف على المستند الذي يحمل هذا التوقيع قوة وثقة².

¹ - مبارك الحسناوي، مجلة الفقه والقانون، العدد الخامس عشر، يناير 2014، ردمد 0615-2336، ص 134

² - المادة الثامنة من قانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

ملخص الفصل الأول:

يتضح من خلال هذا الفصل أن الإنسان واجه الكثير من المخاطر في حياته اليومية، لذلك جاءت فكرة المستند الإلكتروني لتسهيل عملية المعاملات الإلكترونية والمالية والتجارية، وهنا نجد أن فكرة المستند قد تطورت عبر الزمن وأن هيمنة عالم الإلكترونيات على اغلب مفاصل الحياة، وبروز آليات للتداول الإلكتروني في سوق الأوراق المالية والتجارية الإلكترونية، وبهذا التداول قد تحقق التواصل الإنساني والسرعة في هذه المعاملات، وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقاً للاستخدام التكنولوجي الحديث في مجال الاتصالات ونقل المعلومات، فلم يعد هناك مجال لأي دولة تريد أن تواكب العصر وتسير على خطى الدول المتقدمة، ولقد بينا في هذا الفصل ماهية المستند الإلكتروني والطبيعة القانونية له في مجال الإثبات ومدى حجيته مقارنة بالمستندات التقليدية التي كانت متداولة قديماً.

الفصل الثاني

الفصل الثاني: الأفعال الماسة بالمستند الإلكتروني

تقوم الحماية الجنائية للمستند الإلكتروني على عدة اعتبارات وأسس قانونية تقوم بحماية المستند الإلكتروني من العديد من الجرائم الماسة به، وبصحته وقوته القانونية، حيث تعددت هذه الجرائم فأصبحنا نسمع بالسرقة والاحتيال والتزوير والاتلاف، إلا أننا نجد أن معظم التشريعات خصصت قواعد غاية في الدقة، تجرم هذه الأفعال وسنبحث في هذا الجانب أخطر الجرائم التي تمس بأمن المستند الإلكتروني وذلك في المبحث الأول. وفي المبحث الثاني سنتطرق إلى الأفعال الماسة بسرية المستند الإلكتروني، وسنبحث كذلك في قواعد الضبط التي تحكم التفتيش في الجرائم المعلوماتية.

المبحث الأول: الأفعال الماسة بمحتوى المستند الإلكتروني

لا تتعدد الأفعال الماسة بالمستند الإلكتروني من جريمة لأخرى، وسنتطرق من خلال ما سيأتي في هذا المبحث إلى سرد مجموعة من الجرائم ونبين كيف أن المشرع جرّمها في نصوص بصورة صريحة في بعض الأحيان وبصورة ضمنية في نصوص أخرى، وتتنوع صور المساس بمحتوى المستند الإلكتروني وتختلف فيما بينها، غير أنه يمكن مع ذلك تأصيلها في طائفتين، الأولى هي أفعال تزوير المستند والثانية هي إتلاف هذا المستند¹.

المطلب الأول: جريمة التزوير وجريمة السرقة

سنحاول من خلال هذا المطلب دراسة جريمتي التزوير والسرقة، وسنتعرض إلى الحماية الجنائية التي أخضها المشرع للمستند الإلكتروني ضد هذه الجرائم.

¹ - صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 43.

الفرع الأول: جريمة التزوير والحماية الجنائية المقررة لها

تعتبر جرائم تزوير البيانات من أكثر الجرائم شيوعاً من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الانترنت، أو ضمن جرائم الحاسب الآلي، نظراً لأنه لا تخلو جريمة من الجرائم إلا ويكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بآخر، وتزوير البيانات يكون بالدخول على قاعدة البيانات الموجودة وتعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل.

1/-تعريف جريمة التزوير:

إن التزوير يعتبر جريمة كباقي الجرائم، فإن التزوير في المستند الإلكتروني يقوم على ركنين وهو الركن المادي والمعنوي، وبهذا عرف المشرع المغربي جريمة التزوير بأنه "تغيير الحقيقة بسوء نية تغييراً منشأه أن يسبب ضرراً من وقع المحرر بإحدى الوسائل المنصوص عليها في القانون"¹.

ولقد عرّف المشرع المصري جريمة التزوير المحررات، وهذا في المواد من 211 إلى 228 على الجرائم التي تجعل المحرر أو المستند المزور، كما أن المشرع المصري حصر طرق التزوير خاضعة للعقاب إلا أن علة هذا التجريم، والمواد التي نصت عليه لم تعرف أو لم تتعرض لتعريف جريمة تزوير المستند، مما دفع بالفقه إلى وضع تعريف يختلف فيه الكثير منهم، فمنهم من عرّفه "تغيير الحقيقة مقترناً بقصد الغش يقع في محرر بإحدى الطرق التي بينها القانون، ويكون من شأنه أن يسبب ضرراً للغير"².

وعرفه البعض الآخر بأنه "تغيير في الحقيقة بإحدى الطرق المقررة في القانون بقصد الغش في محرر صالح للإثبات ويرتب عليه القانون أثر"³.

¹ - المادة 351 من مجموعة القانون الجنائي المغربي.

² - محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 2013 ص 210.

³ - أحمد فتحي سرور، الجرائم المضرة بالمصلحة، دار النهضة العربية، 1963م، ص 307.

وفي هذا الاتجاه قد عرفه الفقه الفرنسي بأنه: " تغيير الحقيقة في وقائع اعد المحرر لإثباتها متى كان من شأنه أن يسبب ضرراً ارتكب بقصد الغش وقصد بذلك الأضرار"¹. وهذا التعريف هو للأستاذ (جارسون) الذي درج غالبية الفقه الفرنسي والمصري على اعتماده، وتضمنته أيضا المادة 286 من قانون العقوبات العراقي رقم 111 لسنة 1969². وعرف أيضا أنه: هو كشف الإزالة في المستند الإلكتروني أو المحو أو الكشط، أو الإزالة الكيميائية للبيانات الأصلية للمحرر المعلوماتي وما يؤخذ على المشرع الجزائري وبعض التشريعات العربية كالتشريع المصري أيضا أنها تعط تعريفا للتزوير وإنما يستخلص ذلك من نصوص تلك التشريعات ، إلا أن المشرع الاردني أعطى تعريفا له في نص المادة 260 من قانون العقوبات، والقانون اللبناني في مادته 453 والمشرع السوري في نص المادة 344³. فهنا فلا تقوم جريمة تزوير المستند الإلكتروني إلا بتوافر أركانها، والتي تتمثل في الركن الخاص (أولا) والاركان العامة (ثانيا)، وهذا ما سنبينه كالاتي:

أولا: الركن الخاص

يتمثل في جريمة تزوير المستند الإلكتروني في المحل الذي يقع عليه الفعل المادي لهذه الجريمة وتزوير المستند الإلكتروني المعالج، وبذلك فإن محل الجريمة ينصب عليها الفعل المكون لجريمة التزوير ويجب أن يكون مستندا إلكترونيا⁴.

ثانيا: الأركان العامة

تتمثل الأركان العامة في جريمة تزوير المستند الإلكتروني في الركن المادي والمعنوي.

¹- **Donnedieu De Viber**, Lanastion De Fait Intellectuel En Droit Françaises Ce Crime, 1974, P 277.

²- **عباس العبودي**، مرجع سابق، ص 107.

³- **طباش أمين**، الحماية الجنائية للمعاملات الإلكترونية، مذكرة ماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2013، ص 61.

⁴- **خالد علي العراقي علي إسماعيل**، مكافحة جرائم التوقيع الإلكتروني بدولة الإمارات العربية المتحدة، مجلة الفكر الشرطي، مج 22، ع 85، 2013، ص 139.

1/-الركن المادي: يتجلى الركن المادي لقيام جريمة التزوير في المستند الإلكتروني من خلال عنصرين، الأول يتمثل في تغيير الحقيقة، أي تغيير في بنود المستند عما كانت عليه ويقصد بالحقيقة "هي ما اتجهت إليه من ينتسب إليه المستند، ويكفي التغيير أن يكون جزئياً أو كلياً"¹. وهناك عدة عناصر أساسية يجب توافرها لقيام هاته الجريمة هي:

أ/-وجود محرر.

ب/-تغيير الحقيقة بإحدى الطرق المنصوص عليها قانوناً.

ج/-أن يترتب على ذلك ضرر عام أو خاص في الحاضر أو في المستقبل².
وسنبين كل عنصر من هذه العناصر على حدى:

أ/-وجود محرر: اشترط 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 حين أنه في جريمة التزوير المعلوماتي، فإن المستند المعلوماتي هو الدعامة المادية التي تم تحويل المعطيات المعالجة عليها، فيكون إما قرص مضغوط أو شريط ممغنط. ومنه 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 1-323 إلى 7-232 وتجريم المشرع الفرنسي لتزوير الوثائق المعلوماتية جاء بسبب ارتباط هذه الوثائق أو المستندات المعلوماتية بقانون الإثبات، لذلك جاءت المادة 1-441 من قانون العقوبات الفرنسي لتجريم التزوير الذي من شأنه أن يسبب ضرراً والذي يتم بأي وسيلة كانت وفي محرر أو سند للتعبير عن الرأي³.

¹ محمد أمين الرومي، مرجع سابق، ص 74.

² خشير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010، ص ص 134 - 135.

³ 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 - 47.

أما بالنسبة للمشرع الجزائري فقد ادرج 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 تشريعا، إما بتعديل نصوص التزوير التقليدي على غرار المشرع الفرنسي عند إضافته لعبارة أي سند للتعبير عن الرأي "لتعويض 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 مكرر 7، والتي تهدف لتحقيق الحماية الجنائية للنظم المعلوماتية¹.

ب/- تغيير الحقيقة: يقصد بتغيير الحقيقة هو إبدالها بما يغيرها، وبالتالي فلا يعتبر تغيير 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 إضافته 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 للتجريم².
ولذلك فإن تغيير الحقيقة في المعلومات المعالجة آليا قد يظهر على كيان مادي سواء كان ورقي أو دعامة إلكترونية كالشرائط الممغنطة والأقراص الإلكترونية، وغيرها من الدعائم المماثلة.

ج/- الضرر: الضرر هو عنصر جوهري في جريمة التزوير، إذ لا يكفي لاكتمال الركن المادي في هذه الجريمة تغيير لحقيقة في محرر، وأن يحدث هذا التغيير بإحدى الطرق التي بينها

¹ القانون رقم 66-16 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الصادر في الجريدة الرسمية، العدد 49

المؤرخة في 11-06-1966، المعدل والمتمم بالقانون رقم 16-02 المؤرخ في 19 يونيو 2016، الصادر بالجريدة الرسمية،

العدد 37، المؤرخ في 22 يونيو 2016.

² - خشير مسعود، مرجع سابق، ص 136.

القانون، ولم ينص المشرع الجزائري عند تعرضه لجريمة تزوير المحررات الرسمية على الضرر باعتباره عنصرا في جريمة التزوير، لأن موضوع الضرر من المسائل الموضوعية لا القانونية¹. لذلك يمكن القول بأن الضرر يتحقق في جريمة تزوير المستند الإلكتروني عند استعماله من طرف الجاني والاحتجاج به اتجاه الغير، بحيث يتم تعريض مصالح الآخرين للخطر، أو احتمال وقوعه إذا كان منتظر تحققه في المستقبل وفقا لمجرى الأمور العادي ونشير إلى وقت تقدير الضرر و يكون وقت حدوث تغيير الحقيقة في المستند الإلكتروني، ولذلك لا يعفى الجاني من العقاب وقيام المسؤولية الجنائية في حقه، وفي حالة انتفاء احتمال تحقق الضرر بعد حدوث التغيير، وهذا مثل إتلاف المستند الإلكتروني أو موافقة صاحب التوقيع الإلكتروني بعد تزويره على مضمون المستند الإلكتروني، وعليه فالتزوير في المستند الإلكتروني يتحقق بتغيير الحقيقة في مستند إلكتروني له صفة الحفظ أو الاستلام أو الإرسال عن طريق وسيلة إلكترونية، وله قيمة قانونية ليكون دليل إثبات لحق أو تصرف قانوني، على أن ينتج عن هذا التغيير ضرر واقعي أو محتمل الوقوع².

2-/الركن المعنوي:

ويتمثل الركن المعنوي في جريمة تزوير المستندات المعلوماتية في القصد الجنائي، على اعتبار أنها جريمة 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 ما³. وتتخذ صورة القصد الجنائي الذي يأخذ صورتين، قصد جنائي عام يقوم على ضرورة توفر على العلم والإرادة في ارتكاب جريمة ما، أما الصورة الثاني فتتمثل في القصد الجنائي الخاص الذي يتمثل باتجاه نية الجاني في استعمال المحرر فيما زور من اجله ولو لم يستعمله والتزوير

¹ - دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، الجزء 2، ديوان المطبوعات الجزائرية، قسنطينة، 2007، ص 74.

² - محمد علي سالم جاسم وعباس طالب زروقي، البطاقة الائتمانية والأساس القانوني لحمايتها من التزوير، مجلة المتحقق المحلي للعلوم القانونية والسياسية، ع2، 2015، ص 125.

³ - خشير مسعود، مرجع سابق، ص 138.

إما ماديا أو معنويا يترك أثر على المستند قد يعرف هذا الأثر بالحواس أو بواسطة الخبرة والتزوير المعنوي هو إثبات غير الحقيقة في المستند الإلكتروني مباشرة، ويكون ذلك بإثباته خاصة في المستند، وللتزوير عدة طرق تطرقت إليها مختلف التشريعات وهذا بمراعاة عدة أمور منها: وضع توقيعات مزورة وتغيير المحرر أو الكتابة أو التوقيع وكتابة إضافية أو مقحمة في السجلات أو المحررات العمومية بعد إتمام تحريرها أو اختتامها وأما المشرع المصري فوضع هو الآخر بعض طرق التزوير مثل: وضع الأختام أو بصمات مزورة، إذ تعتبر كل المحررات والأختام أو الإمضاءات أو زيادة الكلمات ووضع أسماء أو صور أشخاص آخرين تزويراً.

3/- طرق التزوير:

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

1/- طرق التزوير المادي:

يقصد بالتزوير المادي ما يترك أثراً مادياً على العنق 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 كالاتي:

- وضع إمضاءات أو أختام مزورة.
- تغيير المحررات أو الأختام أو الإمضاءات أو زيارة كلمات.
- وضع أسماء أو صور أشخاص آخرين مزورة.
- التقليد والاصطناع¹.

أما المشرع الجزائري فلقد ورد تصور التزوير في قانون العقوبات على سبيل الحصر، لذلك لا يعتبر تغيير الحقيقة تزويراً إلا إذا حصل بإحدى الطرق التي نصت عليها المواد 214 و215 بالنسبة لغير الموظف العام، ولقد حصرت المادة 214 ق.ع.ج أفعال التزوير المادي بقولها "

¹ - إيهاب فوزي السقا، مرجع سابق، ص 61.

يعاقب بالسجن المؤبد كل قاضي أو موظف أو قائم بوظيفة عمومية ارتكب تزويراً في المحررات العمومية أو الرسمية أثناء تأدية وظيفته".

- إما بوضع توقيعات مزورة.

- إما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات.

- إما بانتحال شخصية الغير أو الحلول محلها.

- وإما الكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمامها أو قفلها¹.

2/- طرق التزوير المعنوي:

بيّن المشرع المصري طرق التزوير المعنوي بنص المادة 213 عقوبات على انه يعدّ مزوراً من "غير قصد 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 أولي الشأن.

- جعل واقعة مزورة في صورة واقعة صحيحة.

- جعل واقعة غير معترف بها في صورة واقعة معترف بها².

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.

¹ - الأمر رقم 66-156 المتضمن قانون العقوبات، المؤرخ في 08 يونيو 1966 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 - إيهاب فوزي الشقا، مرجع سابق، ص 73.

-استبدال إتفاقات أو وقائع: استبدال الاتفاقات والالتزامات والمخالصات وتزييف الإقرارات والوقائع تعتبر من أشكال التزوير المنصوص عليه في المادة 216 ق.ع.ج.¹.

ويضاف 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 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 اسقاط أو تغيير الإقرارات عمداً².

وتعقياً على ما تطرقنا إليه فيما يخص التزوير المعلوماتي، فإننا نؤكد على ضرورة تدخل المشرع الجزائري لتجريم التزوير المعلوماتي الذي يقع على مستند معلوماتي كالبطاقات الإلكترونية، وذلك إما بتعديله للنصوص المبرمة 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 المغناطيسية³.

2/- الحماية الجنائية للمستند الإلكتروني من جريمة التزوير:

التزوير في المستند الإلكتروني يمثل صورة لا تقل أهمية عن التزوير في المستندات الورقية، وتتمثل هذه الأهمية من عدة أوجه:

أ-الوجه الأول: إن المستند الإلكتروني قد حل محل المستندات الورقية في الكثير من المعاملات التجارية، ومن ثم فإن المساس بمحتوى هذا المستند يؤدي إلى وقوع المتعاقدين في عيب من عيوب الإرادة، مثل: الغلط أو التدليس، الأمر الذي يؤدي إلى إثارة الكثير من المنازعات ومن ثم تهديد استقرار هذه التعاملات.

¹ - دردوس مكي، مرجع سابق، ص 73.

² - حفصي عباس، جرائم التزوير الإلكترونية (دراسة مقارنة)، دكتوراه في العلوم الإسلامية، جامعة وهران 01، أحمد بن بلة، سنة 2015، ص 33.

³ - معتوق عبد اللطيف، مرجع سابق، ص 49.

ب/-الوجه الثاني: إن الاعتماد على الطبع الورقي لأصل المستند الإلكتروني وقبوله في التعامل يؤدي إلى نتيجة مؤداها أن المساس بمحتوى المستند الإلكتروني، سيترتب عليه بالضرورة مساس بالصورة الورقية طبق الأصل لهذا المستند ولقد اختلفت خطة التشريعات المقارنة في تجريم تزوير المستند الإلكتروني إلى اتجاهين¹.

-الاتجاه الأول: يضع نصوصا عامة لتجريم هذا التزوير، ومن ثم يمتد حكم هذه النصوص ليشمل التزوير الحاصل في كافة صور هذه المستندات، مثل القانونين الفرنسي والالمانى.-
الاتجاه الثاني: فيجزم بعض الصور لتزوير المستندات الإلكترونية ومن هذه التشريعات القانون المصري².

أولاً: تجريم المستندات الإلكترونية بنصوص عامة:

1-القانون الفرنسي:

يرجع تجريم التزوير لدى المشرع الفرنسي في المستندات الإلكترونية إلى ما تقدم به أحد نواب البرلمان الفرنسي (JaquesgodFrain) في 5 أغسطس سنة 1986 في اقتراح يرمي إلى إدخال بعض التعديلات في جريمة التزوير في المحاضرات المنصوص عليها في قانون العقوبات، لتشمل أيضا تغيير الحقيقة في البيانات الإلكترونية، غير أن هذا الاقتراح لم يؤخذ به، ورأي مجلس الشيوخ في المحررات، وقد صدر القانون رقم 88-19 في 05 يناير سنة 1988 الذي انطوى على تجريم صورتين: الأولى هي تزوير المستندات المعالجة آليا أيا كان شكلها إذا كان من شأنها الإضرار بالغير (المادة 462-5) والصورة الثانية فهي الخاصة باستعمال المستندات المزورة سالفه الذكر (المادة 462-6).

¹- حسن عبد الباسط جمعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، سنة 2000، ص 63 وما بعدها.

²- أشرف توفيق شمس الدين، ص 21، ص 22.

وقد تبني هذه الوجة أيضا قانونا التجارة الإلكترونية لدوقية لكسمبورج الصادر في يونيو سنة 2000، والذي عدّل نص المادة 196 من قانون العقوبات التي تجرم التزوير، فأضاف الكتابة والتواقيع الإلكترونية إلى محل جريمة التزوير بصورتها التقليدية¹.

2/- القانون الألماني:

في هذا الإطار قرّر المشرع الألماني في مواده القانونية من قانون العقوبات الواردة في باب التزوير البيانات القانونية، حيث قرّر العقوبة التي تتحدد في الحبس لمدة تزيد عن 05 سنوات أو الغرامة، ونصت المادة 268 من قانون العقوبات على تجريم تزوير السجلات المعالجة تقنيا، ونصت الفقرة الأولى من هذه المادة في بندها الأول على تجريم فعل "كل من توصل بطريق الخداع إلى إنشاء سجل مصطنع معالج تقنيا أو قام بتغيير الحقيقة فيه"، كما عاقب في البند الثاني على استعمال هذا السجل وقد ساوى الشارع الألماني بين إنشاء سجل إلكتروني مصطنع وبين إحداث التغيير في النتيجة المؤدى إليها هذا السجل، وذلك من خلال قيام الجاني بإحداث تأثير مغل بعمل السجل، وقد نص المشرع الألماني على تجريم بعض الصور الخاصة بالمستند الإلكتروني، وذلك بعد أن وضع الإطار العام لتجريم هذه المستندات في المادة 268 سالف الذكر، ومن أهم هذه الصور: تزوير البيانات التي لها قيمة في الإثبات (المادة 269 من ق. العقوبات)².

ثانيا: تجريم بعض صور تزوير المستندات الإلكترونية

لقد اقتصر بعض التشريعات على تجريم بعض صور تزوير المستندات الإلكترونية، ومنها:

1/- القانون المصري:

لقد جرّم الشارع المصري تزوير السجلات الإلكترونية الخاصة بالأحوال المدنية، وسبق أن ذكرنا أن المشرع المصري قد ساوى في الأحوال المدنية رقم 143 لسنة 1994 بين السجلات الورقية والإلكترونية في تطبيق أحكامه، وقد اعتبر الشارع المصري البيانات المسجلة بالحاسبات

¹ - مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، سنة 2001، ص 72.

² - أشرف توفيق شمس الدين، ص 22.

الآلية بمراكز الأحوال المدنية بيانات واردة في محررات رسمية، فتتص في المادة 72 من القانون السابق على أن "في تطبيق أحكام هذا القانون وقانون العقوبات، تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية، فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية، تكون عقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات، وقد نصت المادة 74 من قانون الأحوال المدنية السالفة الذكر على أنه مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين ويعاقب بالحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد عن 500 جنيه، أو بإحدى هاتين العقوبتين كل من إطلع أو شرع في الإطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها¹.

2- القانون المغربي:

لقد نظم المشرع المغربي جريمة تزوير المستند في الفصول من 334 إلى 367 من مجموعة القانون الجنائي، وبالتالي فإن العقوبة المنصوص عليها في الفروع الخمس الأولى من الباب السادس من الجزء الأول من الكتاب الثاني من مجموعة القانون الجنائي المغربي، تختلف باختلاف صور التزوير، إذ نجد أن المشرع حدّد العقوبة الأقصى لجريمة التزوير في السجن المؤبد².

3- القانون الجزائري:

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

¹ - أشرف توفيق شمس الدين، ص 23.

² - ظهير شريف، رقم 3-44-59-1 بتاريخ 28 جمادى الثانية 1382 (26 نوفمبر 1962 بالمصادقة على مجموعة القانون الجنائي، منشور بالجريدة الرسمية، عدد 2640 مكرر بتاريخ 18 محرم 1303 (05 نوفمبر 1963)، ص 1253.

أ/- جريمة التزوير في محررات رسمية عمومية: وترتب عليها العقوبات التالية:

1/- عقوبة السجن المؤبد للقضاة أو الموظفين العموميين الذين ارتكبوا تزويراً في المحررات الرسمية أو العمومية أثناء تأدية مهامهم، وهذا وفقاً للمادتين 2 و25 ق.ع.ج.

2/- عقوبة السجن المؤقت من 10 سنوات إلى 20 سنة، وبغرامة مالية من مليون إلى 2 مليون دينار كل شخص من غير القضاة والموظفين العموميين يرتكب جريمة التزوير في محررات رسمية أو عمومية، وهذا وفقاً للمادة 216.

3/- عقوبة الحبس من سنة واحدة إلى 05 سنوات وبغرامة من 500 دج إلى 1000 دج كل شخص ليس طرفاً في العقد أدلى أمام الموظف بتقرير يعلم أنه مخالف للحقيقة وفقاً للمادة 217.

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

1/- عقوبة الحبس من سنة إلى 5 سنوات وغرامة من 500 دج إلى 2000 دج كل من ارتكب تزويراً هي محررات تجارية أو مصرفية أو شرع في ذلك وفقاً للمادة 219.

2/- عقوبة الحبس من سنة إلى 5 سنوات وغرامة من 500 دج إلى 2000 دج كل من ارتكب في محررات عرفية أو شرع في ذلك وفقاً للمادة 220.

ج/- جريمة التزوير في الوثائق الإدارية والشهادات: رتب عليها المشرع عقوبة الحبس من 06 أشهر إلى 03 سنوات وغرامة من 1500 دج إلى 15000 دج كل من قلّد أو زيّف رخصاً 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 ما نصت عليه المادة 222 ق.ع.¹

¹ - حسونة عبد الغني، جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة بحث مقدم لأعمال المنتدى الوطني حول الجريمة للمعلوماتية بين الوقاية والمكافحة كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة مابين 16 و17 نوفمبر 2015، ص 68.

4/- القانون الكندي:

ولقد كان التشريع الكندي من بين التشريعات التي حرصت على إدخال بيانات الكمبيوتر ضمن طائفة المحررات في مفهوم جريمة التزوير، والذي نص في الفصل 321 على أن المحرر "أوراق أو اي مادة أخرى مسجلة أو مدون عليها ما يمكن قراءته أو فهمه من جانب الأشخاص أو أجهزة الكمبيوتر أو أي جهاز آخر" وكل هذه العقوبات التي تطرقت إليها القوانين ترجع إلى الخطورة التي قد تشكلها عملية تداول المستند الإلكتروني مزور لماله من أضرار تلحق الأطراف المتعاملين به، تحقيقاً كذلك للأمن في التعاملات الإلكترونية التي تنشأ بواسطة المستندات الإلكترونية، وكذلك لزيادة الثقة في هذا النوع من المستندات، ومن جملة المخاطر التي تنتج عن تزوير المعطيات إهدار المال العام وسرقته دون ترك أي دليل على ذلك، وما وقع في ألمانيا في أحد المراكز الطبية، حيث قام القائمون على المركز باختلاس مبلغ 61000 دولار، وهي عبارة عن أموال مدفوعة من شركة التأمين للمركز الطبي، وحتى تتم العملية بكل نجاح قام هؤلاء الأشخاص بمحو المستندات الموجودة داخل الحاسوب الخاص بالمركز ، مما جعلها غير قابلة للتحويل¹.

الفرع الثاني: جريمة السرقة والحماية الجنائية المقرر لها

تدخل السرقة ضمن الجرائم التي تسبب ضرر لمستعمل هذا المستند، وبالتالي فلا يخرج عن باقي تصنيفات الجرائم من حيث الأركان، فلقيام جريمة السرقة لا بد من توفر ووجود ركنين، أحدهما مادي والآخر معنوي، وإن الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال، إذن إن إمكانية خضوع المستند الإلكتروني الإجرامي لجرائم السرقة وخيانة الأمانة ومدى تحقق الحماية الجزائية له وفقاً لنصوص هذه الجرائم.

1- أشرف توفيق شمس الدين، مرجع سابق ص 541.

1/-تعريف جريمة السرقة:

هي عملية اختلاس أو إخراج المال من حيازة المجني عليه إلى حيازة الجاني، وبمقتضى ذلك حرمان المجني عليه من حيازة وملكية هذا المال¹.

ولذلك تستقر الأحكام القضائية على وقوع السرقة التامة بخروج الشيء المسروق من حيازة المجني عليه إلى حيازة الجاني، وبهذا يلاحظ على أنه "المال الغير المملوك لأحد لا تقوم به جريمة السرقة، وبالتالي فإن الإستيلاء عليه لا يمثل جريمة سرقة وذلك لأن الاستيلاء على هذا المال لا يمثل اعتداء على ملكية سرقة"².

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 إلكترونياً وقد نصت المادة 350 من قانون العقوبات الجزائري على أنه (كل من اختلس شيئاً غير مملوك له يعد سارقاً) يمكن تعريف جريمة السرقة الإلكترونية على أنها (استخدام الوسائط الحاسوبية وشبكات الأنترنت لأخذ مال منقول مملوك للغير بلغ نصاباً خفية من حرز مثله، من غير شبهة ولا تأويل) ويفهم 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 ما هو مسجل عليها والجدير بالذكر على أن جريمة السرقة أو الاختلاس أو سرقة المعلومات الإلكترونية لم يكن محل إتفاق أو احتكام للقضاء الفرنسي تراجع عن هذا الرأي، وما يؤكد ذلك وهو صدور قرار محكمة النقض الفرنسية والتي قضت فيه "بوقوع جريمة السرقة من المتهم الذي قام بتصوير بعض المستندات التي تخص الغير دون موافقة هذا الأخير، بيد أن المحكمة استندت في حكمها إلى أن المتهم اختلس المستندات الأصلية في الوقت اللازم لتصورها، وليس أنه اختلس محتوى هذا المستند".

1- شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 45.

2- محمد أمين الرومي، مرجع سابق، ص 104.

ولم ينص المشرع المصري في القانون الخاص بالعقوبات الإلكترونية على جريمة سرقة المستند الإلكتروني صراحةً، ونجد أن القانون الأردني قد نظمّ الجرائم الملمة بالسرقة في الفصل الأول من الباب الحادي عشر من الكتاب الثاني من قانون العقوبات، حيث أن المشرع الأردني اعتبر السرقة هي الجريمة الأولى المنصوص عليها في قانون العقوبات تحت عنوان "الجرائم الواقعة على الأموال"، فإن المادة 399 من ذات القانون عرفت السرقة بأنها أخذ مال الغير المنقول دون رضاه¹.

ووفقاً لنص المادة فإن عناصر جريمة السرقة وأركانها تتمثل في:

1/-الركن المادي وهو محل أو فعل الأخذ.

2/-محل الجريمة وهو المال المنقول المملوك للغير.

3/-الركن المعنوي والقائم على القصد الجنائي العام المتمثل في عنصري العلم والإرادة والقصد الجنائي المتمثل في نية التمسك.

إن السارق في جريمة سرقة المستندات الإلكترونية تقاسم الإطلاع على هذه المعلومات مع مالكةا وتجب الإشارة فإن المعلومات التي يحتويها المستند الإلكتروني ليست مال، حيث أنها غير قابلة للقياس أو التحريز، ولذلك لا يجوز الخلط بين المعلومات ومالها من قيمة، حيث يمكن القول بأن المعلومة مال بالمعنى الحقيقي وبخصوص الجرائم الواقعة على المستند الإلكتروني وخاصة بالنسبة لسرقة المستند، فإنه من المتصور أن يكون أحد العاملين في مجال المعلوماتية أي الأنترنت وربما هذا يمكن أن تتصور جريمة السرقة من اشخاص خارج العاملين في مجال الأنترنت أو في الوسط الإلكتروني وهم².

1/-مستخدم الأنترنت: يعتبر هؤلاء مستخدم الأنترنت كل من يدخل موقع شبكات الأنترنت عن طريق استخدام الوسائل التقنية أو الفنية للوصول إلى المعلومات أو المستندات، وذلك عن طريق أحد الأجهزة (موديم) أو عن طريق وصلة الهاتف.

1- المواد 339-416 من القانون المشرع الأردني لجريمة السرقة

2- نهلا عبد القادر المومني، الجرائم المعلوماتية، الأردن، دار الثقافة، 2008، ص 117.

2/- عامل الاتصالات أو المتعهد بالوصول: هو من يربط المشتركين بالمواقع أو المستخدمين الآخرين بالشبكة، وتكون مسؤولية مخففة إن لم نقل منعدمة إلا إذا أخل بمسؤوليته التعاقدية سواء أمام المستخدم أو المورد كذلك.

3/- مراقب الشبكات: والذي يعتبر المسؤول عن اكتشاف المشاكل.

1- الركن المادي لجريمة السرقة:

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 ان يكون الجاني قد استولى على المال خلسةً أو عنوةً أو تسلمه بناءً على يد عارضة فغير نيته واستولى عليه، ومن ثم فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه الى الجاني، بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية¹.

ولقد اختلف 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 ومع وجود علاقة سببية بينهما، أما العنصر الآخر الشخصي فهو نية الجاني في تملك الشيء وحيازته، حيث عند تشغيل الحاسب الآلي والحصول على المعلومات أو البيانات التي يكون قد اختلسها واستحوذ عليها بطريق غير مشروع².

ولذلك أذانت محكمة (Grenoble) دائرة الجرح- المستأنفة في 15/02/1995 عامل بتهمة السرقة، كان قد أخرج من المؤسسة التي يعمل بها أوراقا سرية كان سيقوم بتصويرها ثم يعيدها للمؤسسة³.

1- طباش أمين، مرجع سابق، ص 87.

2- معتوق عبد اللطيف، مرجع سابق، ص 35.

3- محمد أمين الشوابكة، مرجع سابق، ص 156.

أما الرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة وكذلك يترتب على ذلك أن التوقيع الإلكتروني والمستند الإلكتروني، والرسالة والكتابة الإلكترونية كل هذه عبارة عن قيم منقولة أو اعتبارية ليست أشياء، بالتالي لا يمكن أن يخضع الاستيلاء عليها بدون وجه حق لجريمة السرقة¹.

2/-الركن المعنوي لجريمة السرقة:

يتخذ الركن المعنوي في جريمة السرقة في نظام المعلوماتية صورة القصد الجنائي العام والخاص، ويتحقق القصد الجنائي العام، بتوافر العلم والإرادة، فيجب أن تتجه إرادة الجاني الاستيلاء على المعلومات المسجلة إلكترونياً سواء المعلومات المخزنة داخل النظام المعلوماتي أو المعلومات المسجلة إلكترونياً، والمخزنة على دعامة خارجية مثل الأسطوانات والشرائط الممغنطة، مع علمه بأن المعلومات محل السرقة ملكاً له، فإن قام شخص بأخذ قرص ممغنط يحتوي على برامج معلوماتية أو اختلسه من صاحبه، ثم قام بتشغيله لمعرفة محتواه، ثم رده، فإن إرادة الاختلاس تنتفي لديه ويختلف القصد العام عنده².

ونلاحظ مما سبق أن التحجج بان المال المعلوماتي غير قابل للسرقة، هي حجة تجافي المنطق، ذلك أنا التسليم بها يعني تجريد المال المعلوماتي من الحماية الجنائية مما يجعله عرضة للاعتداء وبالتالي حفاظاً 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.

2/ الحماية الجنائية للمستند الإلكتروني من جريمة السرقة:

لم تكن التشريعات واضحة في مسألة تجريم المستند الإلكتروني أو اضعاف الطابع الجنائي على المستند الإلكتروني من جريمة السرقة، وذلك لصعوبة تحديد المفاهيم والطرق التي تقوم عليها هذه الأنواع من الجرائم، ومن التشريعات التي تتطرق لسرقة المستند الإلكتروني هناك

1- محمد أمين الرومي، مرجع سابق، ص 103.

2- طباش أمين، مرجع سابق، ص ص 99-100.

المشعر المصري الذي جرّم بطريقة غير مباشرة جريمة السرقة، حيث أنه جرّم سرقة المستند الذي حصل بوسيلة غير قانونية قد تكون سرقة واختلاس¹.

اتجه البعض من الفقه إلى عدم إضفاء هذه الصيغة على المستند الإلكتروني واتسدل على ذلك أن جريمة السرقة تقع على الأشياء المادية الملموسة، ولهذا اتجه هذا الرأي إلى إخراج صفة سرقة من مجال المستند الإلكتروني وهذا الرأي تم الطعن فيه، إذ من الفقهاء من ذهب عكس ذلك، أي أن اعتبار المستند الإلكتروني قيمة معنوية يجب أن يخضع للاستيلاء، ولعدم تنظيم المشعر المغربي نصوص تعاقب على جريمة السرقة في المستند الإلكتروني، فإننا نعد إلى إعمال قاعدة القياس، وذلك لما جاء في النصوص مجموعة القانون الجنائي، الأمر الذي يلزمنا أن تناول الجانب الحمائي للمستند الإلكتروني خاصة من جريمة السرقة، ولذلك سوف نقوم برصد محل المعلومات التي تستلزم الحماية وخصائصها وأنواعها، وأخيراً مدى إمكانية تطبيق نصوص جريمة السرقة على المستند الإلكتروني.

1/-المعلومات محل السرقة:

لم ينص المشعر بصفة عامة على محل هذه المعلومات التي تعتبر مجال السرقة، إلا أن الأمر تم تداركه من خلال الفقه المصري الذي عرف لنا المعلومات التي يمكن أن تكون محل للسرقة، بقوله "المعرفة هي المادة الخام ثم تأتي المعلومات وتطهيرها في أشكال مختلفة وتبرز العلاقة بين المعلومات والمعرفة في تعريف المعلومات الآلية، وهذا التعريف هو ما قررتة الأكاديمية الفرنسية"².

2/-خصائص المعلومات محل الجريمة:

لإضفاء الحماية الجنائية على المستندات الإلكترونية يجب أن تكون عبارة عن معلومات محددة بمعنى إذا لم تكن هذه المعلومات محددة، فلا تكون أمام الحماية الجنائية لهذا النوع من

¹ - المادة 23 من قانون التوقيع الإلكتروني المصري على "يعاقب الحبس والغرامة التي لا تقل عن عشرة جنيه ولا تتجاوز

إحدى هاتين العقوبتين كل من توصل بأي وسيلة من الحصول بغير حق على وسيط أو محرر إلكتروني"

² - محمد أمين الرومي، مرجع سابق، ص 110.

المستندات، ويجب أن تكون المعلومات مبتكرة وسرية، وألا تكون عامة، حيث أن في الحالة الأخيرة لا نكون أمام سرقة، فسرية المعلومات تدعو إلى الحماية الجنائية، حيث أن سرقة المعلومات وإفشائها من طرف الغير يعتبر هذا اعتداء على الحياة في حد ذاته، وتدعيما لذلك يشترط أن تكون هذه المعلومات معالجة عن طريق الوسائل الإلكترونية، كما أن البعض يشترط لإضفاء الحماية الجنائية، حيث أن سرية المعلومات وإفشائها من طرف الغير يعتبر إعتداء على الحياة في حد ذاته، وتدعيما لذلك يشترط أن تكون هذه المعلومات معالجة عن طريق الوسائل الإلكترونية، كما أن البعض يشترط لإضفاء الحماية الجنائية لهذا النوع يتوجب أن يكون المحرر الإلكتروني موقعا إلا ان الفقه المصري لا يشترط الشرط الأخير، ودليل ذلك هو اعتبار أن المستند الإلكتروني سواء كان موقعا أولا، فإنه يضاها نفس الحجية التي تنتم بما المحررات الورقية وهذه الخصائص تنقسم إلى ثلاث أنواع والتي تكون محل السرقة، وهي على التالي: المعلومات الاسمية والمعلومات الخاصة بالمصنفات الفكرية والمعلوماتية المباحة.

أ/-المعلومات الاسمية: فهي معلومات اسمية شخصية وموضوعية، تكون الأولى مرتبطة بالشخص كالاسم والسن والحالة الاجتماعية ومحل الإقامة إلى غير ذلك، وبالتالي فإن هذه المعلومات يمنع على أي كان الإطلاع عليها إلا بموافقة الشخص أو بأمر من السلطات المختصة أما المعلومات الموضوعية فهي مثلا: المقالات الصحفية والملفات الإدارية للموظفين، وهذه المعلومات تكون موجهة للغير بذاته.

ب/-معلومات خاصة بالمصنفات الفكرية: تعتبر هذه المعلومات محمية من طرف القانون ومقال ذلك حقوق المؤلف وقانون براءة الاختراع¹.

ج/-معلومات مباحة: وهي المعلومات التي لا تشكل في خرقها أو نسخها أي إشكال لأنه تعتبر مجرد بيانات عادية.

¹ - محمد أمين الرومي، مرجع سابق، ص 113.

3/- تطبيق نصوص جريمة السرقة على المستند الإلكتروني:

انقسمت الآراء الفقهية إلى اتجاهين بخصوص تطبيق نصوص جريمة السرقة المنصوص عليها في قانون العقوبات في حالة حدوث سرقة المعلومات المتضمنة داخل المستندات الإلكترونية، حيث أن الاتجاه الأول ذهب إلى إمكانية تطبيق نصوص السرقة على سرقة المعلومات المخزنة داخل الجهاز، بينما الاتجاه الآخر رفض تطبيق هذه النصوص على سرقة المستندات الإلكترونية إلا في بعض الحالات وبالتالي فإننا سندرس كل اتجاه على حدى.

أ/-الاتجاه الأول:

ذهب أنصار هذا الاتجاه وعلى رأسهم بعض الفقهاء المصريين إلى استعمال أو تطبيق نصوص جريمة السرقة على الاعتداء على المستندات الإلكترونية، الشيء الذي يشكل جريمة تضر بمصالح المستفيد من المستند الإلكتروني، حيث أنه في الواقع إذا قام شخص بدخول حاسب آلي يعود لشخص آخر وقام بالإطلاع على المستندات المخزنة فيه، وقام بنسخها بواسطة الطبع أو النسخ على (ديسك) أو (سيدي Cd)، فهذا يشكل الفعل الإجرامي في حق الشخص صاحب المستند، واستند أصحاب هذا الاتجاه على عدة حجج منها :

-إن المستندات الإلكترونية تساوي من حيث الإثبات حجية المحررات الورقية، ذلك أن المستندات الإلكترونية يمكن إدراكها بواسطة العين المجردة، وبالتالي فإن نسخ هذه المستندات بشكل سرقة، حيث يصبح الأمر موجب لتطبيق العقوبة الخاصة بجريمة السرقة، الأمر في هذا راجع إلى أن الفاعل قد قام بالتعدي على الحياة، والحيازة كما هو معلوم معقب عليها.

-كما أن الاعتداد بالسرقة لدى المشرع الفرنسي يستوجب توفر نية تملك الشيء محل الجريمة على هذا النهج صار الفقه القائم بتطبيق العقوبة المنصوص عليها في قانون العقوبات المتعلقة بالسرقة، وذهب الفقه الفرنسي إلى "إدانة سرقة المعلومات في قضية "Laquabox" حيث كان هذا الشخص يعمل موظفا في شركة فرنسية وقام بتصوير مستندات سرية ضد رغبة صاحبها¹.

¹ - محمد أمين الرومي، مرجع سابق، ص 114.

ب/-الاتجاه الثاني:

لم يتعارض هذا الاتجاه مع تطبيق نصوص القانون الجنائي على سرقة المستند الإلكتروني، إلا أنه اقتصر ذلك في بضع حالات وهي:

1/-الحالة الأولى: والتي تتمثل في سرقة دعامة إلكترونية مسجل عليها مستند إلكتروني وفي هذه الحالة يشكل الفعل جريمة سرقة تخضع لأحكام قانون العقوبات.

2/-الحالة الثانية: تتمثل في سرقة المستند الإلكتروني بواسطة نسخ البيانات المتضمنة ضمن المستند، كما أن الإطلاع على المعلومات يشكل خرق سرية المعلومات التي يعاقب عليها القانون في حالة ما إذا كانت البيانات سرية.

المطلب الثاني: جريمة الاتلاف والاحتيال

تعد جريمتي الاتلاف والاحتتيال من الجرائم المعلوماتية التي تقع على الأموال المملوكة للغير، سواء كانت منقولات أو عقارات، وقد يقع الاتلاف والاحتتيال على المكونات المادية لأنظمة المعالجة الآلية للمعلومات أو المعطيات ذاتها.

الفرع الأول: جريمة الاتلاف والحماية المقررة لها

في حقيقة الأمر ليس هناك نص يجرم إتلاف المستند الإلكتروني بشكل مباشر وإنما يمكن استنتاج ذلك عن طريق التبعية أو بشكل غير مباشر، والتي يمكن إضفاء عليها طابع الحماية من الأفعال التي تعد إتلاف للمستند بصورة غير مباشرة¹.

1-تعريف جريمة الاتلاف:

تناول كل من المشرع المصري هذه الجريمة في المادة 361 من قانون العقوبات المعدلة بالقانون رقم 97 لسنة 1992 والمشرع الجزائري في المادتين 407 و412 من قانون العقوبات، وايضا في المادة 322 فقرة 01 من قانون العقوبات الفرنسي، والمادة 719 من قانون العقوبات

¹ - اشرف توفيق شمس الدين، مرجع سابق ص 543.

السوري، فكل هذه المواد جرّمت فعل الاتلاف لكن لم تعطي تعريفاً أو معنى للاتلاف لا بصفة عامة أو بصفة خاصة فذهب الفقه وبتعريفه إلى:

- هو التأثير في مادة الشيء على نحوٍ يذهب أو يقلل من قيمته الاقتصادية عن طريق الانقاص من كفاءته للاستعمال المعدّله، فجوهر الاتلاف هو افقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله، وهو محو المعلومات أو البرامج كلياً أو تدميرها إلكترونياً أو تشويه المعلومات أو البرامج على نحو فيه اتلاف لجعلها غير صالحة.¹ وأيضاً هو أنه تعيب الشيء بما يجعله غير صالح لما أعد له مع بقاء أصله.²

والعبرة في الاتلاف في المستند الإلكتروني هو الذي يقع على المكونات المعنوية للنظام المتمثل في المعلومات المنظمة في البرنامج المعلوماتي وكما سبق القول، فإن المشرع الفرنسي نص على حماية المستند الإلكتروني في المادة 1- 2- 3 بطريقة غير مباشرة في إطار إضفاء الحماية على نظم معالجة البيانات ومن ثم تمتد الحماية إلى المستند على نحو تبعي.³

ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونياً، أو تشويهها على نحو يقع فيه الإتلاف، بما يجعله غير صالحة للاستعمال.⁴ وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوي سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض.⁵

¹ - محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2015.

² - سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجزائر الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، ب.ط، القاهرة، 2007، ص 93.

³ - المادة 3.2.1 قانون العقوبات الفرنسي.

⁴ - محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2007، ص 26.

⁵ - براهمي حنان، مرجع سابق، ص 54.

والإتلاف هو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها، سواء استيلاء على أموال أو إطلاع على معلومات، ولكن إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته¹.

ولقيام جريمة الإتلاف على المستند الإلكتروني أو على نظام المعلومات بصفة عامة، وجب أن تتوفر في جريمة الإتلاف الركن المادي للبيانات المبرمجة، وهذا التعديل يمكن أن يتخذ صورة الإضافة أو الحذف أو التغيير في البيانات ذاتها، ويقوم الإتلاف على عدة وسائل وأساليب تتنوع خطورتها من أسلوب إلى آخر، فنجد الفيروسات Vireuses التي تتميز بالتكاثر والانتشار من نظام لآخر واختنائها، مما يشكل صعوبة في اكتشافها، وتقوم بتدمير البرامج وتغيير المعلومات دون ترك، كما يمكن استعماله أو استخدامه لأغراض حماية النسخ الأصلية من خطر النسخ غير المرخص به، ومن بين الوسائل كذلك البرامج المنطقية والزمنية².

أو ما يصطلح عليه بالقبلة المعلوماتية، وهو اصطلاح يطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف، ويمكن أن نقسم القبلة المعلوماتية إلى قسمين:

1/- القنابل المنطقية: وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو في كل فترة زمنية منظمة، ويتم وضعه بشبكة معلوماتية، بهدف تحديد ظروف أو حالة محتوى النظام، بغرض تسهيل تنفيذ عمل غير مشروع³.

2/- القبلة الزمنية أو الموقوتة: وهي عبارة عن برنامج يتم إدخالها بشروط مشروعة متخفية مع برامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام وتغييرها وتعمل على مبدأ التوقيت، حيث تنفجر في وقت معين.

¹- أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، دار الجامعة الجديدة للنشر والتوزيع، ط1، مصر، 2015.

²- نهلا عبد القادر المومني، مرجع سابق، ص 132.

³- محمد أمين الرومي، مرجع سابق ص 94.

3/- استخدام برنامج الدودة: هي عبارة عن برنامج يشتغل، أي فجوات في نظام التشغيل كي ينتقل من حاسب آلي إلى آخر أو من شبكة إلى أخرى عبر المواصلات التي تربط بينهما وتتكاثر أثناء عملية انتقالها كالبكتيريا بإنتاج نسخ منها ويهدف هذا البرنامج الى شغل اكبر حيز ممكن من سعة الشبكة ومن امثلة برامج الدودة مايعرف بـ(Inter Warm) وبرنامج البرامج الدودية ضد القتل مستخدمين الذرة ب (Wank) وكل هذه البرامج كانت تساهم في انتقال العدوى بالفيروس عن طريق خرق مواقع البريد الإلكتروني والإرهاب المعلوماتي.

1/-الركن المادي لجريمة الاتلاف للمستند الإلكتروني:

ورد في علم الإجرام لقيام جريمة ما يجب توافر فيها ركنين وهما: الركن المادي والمعنوي، ويتمثل الركن المادي لجريمة الإتلاف المعلوماتي في النشاط الإجرامي وهو فعل الإتلاف وأيضا محل الجريمة والمتمثل في مال ثابت أو منقول مملوك للغير، وهذه الفروع هي كما يلي:

أ/-النشاط الإجرامي:

ويعرفه الفقه بأنه "كل فعل من شأنه يؤثر في مادة الشيء أو في قيامه بوظائفه المختلفة على نحوٍ يذهب من قيمته على النحو غير المعتاد لقيمة الشيء مع مرور الزمن مع قصد الإضرار بالغير ويعرف بأنه السلوك الإجرامي الناتج عن الإتلاف والإزالة بطريق الغش لوثيقة أو سند أو عقود أو أموال منقولة وتشتترط المادة أن تكون بواسطة موظف قاضي أو ضابط عمومي تكون قد سلمت اليه هذه الوثائق والأموال بحكم الوظيفة، أي بسببها أو لصفته".

1/-صفة الجاني:

القاضي هو الذي يصدر الأحكام وهنا بحكم وظيفة يقوم بإزالة الوظائف لغرض ما، وهما إما قضاة تابعين للنظام القضائي العادي أو الإداري، كذلك لدينا الموظف الذي يمارس مهنته بصفة دائمة أو مؤقتة ويدخل ضمن هذا الإطار كذلك الضابط العمومي.

2/-نوع الوثيقة:

هنا الإتلاف يشمل مختلف الوثائق وقد تكون المستندات أو عقود والتي تكون في حوزة الموظف، كما تشمل أموال كانت في عهده، فالمال المنقول يقصد به ذلك المال الذي يمكن

تغيير موقعه نتيجة للفعل المادي، وهنا الإتلاف العمدي 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 المزروعة والتي يرد عليها الإتلاف على هذه الأشياء كمحل للجريمة ويتمثل الركن المادي لجريمة الإتلاف في النشاط الإجرامي والذي يتمثل في التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية، عن طريق الانقاص من كفاءته للاستعمال المعدلة، فمثلا جهاز التلفاز قد يتم إتلافه عن طريق إدخال تيار كهربائي على الشدة، فيتم حرق المكونات 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 أو ما 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 الإختلاف إلى محل الجريمة، حيث يشترط أن يقع الإتلاف أو التعيب على مال منقول أو عقار، مملوك للغير والنشاط الإجرامي في جريمة الإتلاف يتخذ أربع صور كما هو منصوص عليها في المادة 361 من قانون العقوبات المصري على النحو التالي¹:

- (1)-التخريب: ويقصد به أن المال أصبح غير قابل للإصلاح، أي فقد صلاحيته للاستعمال.
- (2)-الإتلاف: ويقصد به تعيب الشيء بما يجعله غير صالح لما أعد مع بقاء أصله.
- (3)-جعل الشيء غير صالح للاستعمال: أي إعدام صلاحيته ويلحق بالتخريب.
- (4)-تعطيل الشيء: أي إعاقة عن العمل كلياً أو جزئياً.

ونجد المشرع الجزائري أيضاً لم يقيد النشاط الإجرامي في جريمة الإتلاف، بوسيلة معينة اذ هي من الجرائم ذات الطابع الحر ولهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج

¹ - سليمان أحمد فضيل، ص 93.

الحاسب الآلي خاصة وأن المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة وحيدة لقيامها¹.

3/- محل الجريمة:

إن محل جريمة الإتلاف هو مكونات الحاسوب المادية والمعنوية، ويكون محل المنقولات المادية المعلوماتية كأجهزة الحاسب الآلي وملحقاته مثل: شاشات العرض والطابعات والاسطوانات والكابلات والمفاتيح والأقراص الممغنطة وغيرها من المكونات المادية، سواء كانت تحتوي بيانات أو برامج أو مجرد أوعية خالية بشرط أن يؤدي الإتلاف أو التخريب إلى الإقلال من قيمتها الاقتصادية، أما المكونات الغير مادية ويطلق على هذه الحالة للإتلاف تدمير نظم المعلومات، ويقصد به إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة الحاسب الآلي، أي كانت شكلها، واستيلاء على نقود أو إطلاع على معلومات، ويتحقق الركن المادي في جريمة الإتلاف التقني بصورتين هما:

ب/- **الإتلاف المباشر:** هو توصل الفاعل بصورة مباشرة أو بطريقة غير مباشرة إلى جهاز الحاسوب الآلي ذاته أو بوصوله إلى لوحة المفاتيح مثلا أو وصوله إلى أحد منافذ الدخول وبوابات العبور للنظام، وهو يقدم على سلوك تقني إلكتروني ومباشر، ويتحقق الإتلاف هنا.

ج/- **الاتلاف غير المباشر:** هو الوصول الى الحاسب الآلي أو نظم المعلومات غير نافذة غير مباشرة، وهو استعمال الفاعل إحدى الا نهايات الطرفية للنظام، فيستغل وجود اتصال به لأية غاية.

2/- الركن المعنوي لجريمة إتلاف المستند الإلكتروني:

إن جريمة الإتلاف في الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام، الذي يقوم بتوافر العلم والإرادة، فيتعين أن يعلم الجاني أنه يعتدي على أموال معلوماتية مملوكة للغير وأن من شأنه فعله أن يتلف الشيء أو يعطله أو أن ينتقص من منفعته بشكل يجعله غير صالح

¹ - فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، بمقر أكاديمية الدراسات العليا بليبيا، في أكتوبر 2009، ص 10.

للاستعمال بما يؤدي إلى إلحاق الضرر به وهذه الجريمة لا تتطلب قصدا خاصا، وإنما يكفي بشأنها القصد العام بعنصره العلم والإرادة¹.

وينتفي القصد إذا اعتقد الشخص أن المال المملوك له، وبأن كان نتيجة غلط مادي كخلطه بينه وبين مال مماثل يملكه، وكذلك ينتفي القصد الجنائي لدى الشخص الذي يقوم بإدخال إحدى الأقراص الخاصة به، والتي كانت مصابة بفيروس في الجهاز الخاص بإحدى المشروعات من أجل طباعته والتي لها خصائص الطابعة ويشترط أيضا لتوافر القصد الجنائي أن تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل أو عدم الصلاحية للاستعمال، فإذا انتفت هذه الإرادة ينتفي بالتبعية القصد الجنائي ومن ثم الجريمة فالإتلاف جريمة مقصودة سواء بصورتها المادية التقليدية أو بصورتها المعنوي المستحدثة، ولا يتصور وقوع فعل الإتلاف جزائيا بغير قصد، وهذا القصد يقوم على عنصرين العلم والإرادة، العلم بالفعل ونتائجه، ثم إرادة هذا الفعل وإرادة نتائجه بغض النظر عن طبيعة وماهية السلوك أو حجم وطبيعة الضرر الناشئ عنه.

3/-الركن الشرعي: جاء في نص المادة 120 من قانون العقوبات الجزائري "يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 20.000 إلى 100.000 دج القاضي أو الموظف أو الضابط العمومي الذي يتلف أو يزيل بطريق العبث وبنية الإضرار وثائق أو سندات أو عقود أو أموال منقولة كانت في عهده وهذه الصفة قد سلمت له بسبب وظيفته"، كما نص المشرع الجزائري على جريمة الإتلاف في المادة 407 من قانون العقوبات والمقابلة للمادة 371 مكرر من قانون العقوبات المصري، والمادة 1/322 من قانون العقوبات الفرنسي، حيث جاء في نص المادة 407 من قانون العقوبات الجزائري: "كل من خرب أو أتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20.000 إلى 100.000 دج دون الإخلال بتطبيق

¹ - سليمان أحمد فضل، مرجع سابق، ص 106.

أحكام المواد من 395 إلى 104 إذا تطلب الأمر ذلك ويعاقب على الشروع في الجنحة المنصوص عليه في هذه المادة كالجنحة التامة¹.

2/ الحماية الجنائية للمستند الإلكتروني من جريمة الإتلاف:

بالرجوع إلى القانون الفرنسي الذي تناول تجريم إتلاف المستند الإلكتروني، حيث نص في المادة 3-323 بأنه إدخال البيانات عن طريق الغش، ما يمكن أن نستنتج من المادة المذكورة هو حماية المشرع الفرنسي للبيانات الموجودة بالنظام من أنه نشاط إجرامي والتي تتضمن ثلاث صور وهي: الإدخال، الحذف، والتعديل ولا يشترط أن تكون هذه الصورة مجتمعة، فقيام واحدة من هذه الصور تقوم جريمة الإتلاف للمستند الإلكتروني وفي التشريع المغربي أيضا نجد أن المشرع جرم الإتلاف بصفة عامة في فرع مشترك يضم كل من التخريب والتعيب، والإتلاف في الفرع الثامن من الباب الثامن من الجزء الأول من الكتاب الثالث، وإذا تصفحنا هذه الفصول بتمعن، نجد على أن المشرع ميّز من خلال هذه الفصول بين العقوبات باختلاف الصور الاتلاف، والتعيب والتخريب كما أن المشرع الهولندي قد ضمن قانون العقوبات الصادر في سنة 1993 نصا خاصا بإتلاف الواقع على نظام تخزين المعلومات والاتصالات، كما يتضمن القانون الإيطالي نصا خاصا بالإتلاف وتخريب الواقع على نظام المعلومات أو البرامج الداخلية فيه، كما تقع جريمة الإتلاف على الملكية، كما تتشكل في التداخل في عمليات الإنتاج أو التوظيف أو نظام المعلومات، ومن بين التشريعات العربية التي تضمن الحماية الجنائية للمعلومات من جريمة الإتلاف والتخزين في الفصل السادس من الباب الحادي عشر تحت عنوان الأضرار التي تلحق بأموال الدولة والأفراد².

¹ - الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق، ص 130.

² - نهلا عبد القادر المومني، مرجع سابق، ص 132.

الفرع الثاني: جريمة الاحتيال والحماية الجنائية للمستند الإلكتروني

غالبا ما يكون الهدف من الاحتيال المعلوماتي هو إختلاس الأموال من المؤسسات أو الشركات، سواء من طرف أحد العاملين بها أو من الغير الذي نجح في اختراقه من خلال القرصنة، وتجدر الإشارة أن أخطر أنواع الاحتيال المعلوماتي هو الاحتيال الذي يقع بهدف التحويل الإلكتروني للأموال والودائع المصرفية من خلال النظم المعلوماتية والتلاعب فيها للحصول على الأموال والخدمات بطريقة غير مشروعة، اعتداء على الغير باستخدام المستند الإلكتروني بطريقة غير مشروعة مما ينتقص من القوة الثبوتية للمستند في التعاملات المصرفية وفي الاحتجاج به في مواجهة الغير ولكن ثم مواجهة مخاطر الاحتيال باستعمال وسائل الحماية التقنية الفعالة بالاعتماد على مفتاح التشفير الطويل ذلك أن طول مفتاح التشفير يؤدي لمنع اختراقه.

1/- تعريف جريمة الاحتيال للمستند الإلكتروني:

تعددت طرق الاحتيال سواء في المعاملات التقليدية بين الأطراف او في علاقة الأطراف بالمؤسسات لتشمل بذلك التعاملات الإلكترونية، ونجد أن التشريعات المقارنة لم تعتبر الكذب ولو كان مكتوبا وسيلة احتيالية في مفهوم جريمة النصب والاحتيال إلا إذا كان مدعما بمظهر خارجي مثلا: الاستعانة بالغير لتنفيذ الطرق الاحتيالية، وذلك بقيام الغير بدور إيجابي في تأييد الكذب إذا قدموا وثائق مزورة من شأنها أن يحتال بها على المجني عليه، وأن جريمة الاحتيال بالاستعانة بالغير تقع حتى ولو لم يكن ذلك الغير موجود أثناء ارتكاب الجريمة، يكفي أنه قدم مستندات لمنفذ الجريمة، ونجد أن ما يميز النصب في مجال التعاملات الإلكترونية الاستعانة بأجهزة الكمبيوتر كوسيلة للاحتيال وكمحل له¹ ونجد العديد من التشريعات المقارنة أصبحت تعتمد نصوص خاصة للعقاب على الغش والاحتيال باستعمال الكمبيوتر أو ما شابهه، ولم تعد خاضعة للقواعد العامة إذا يمكن افتراض حالتين هما:

¹ - شيماء عبد الغني عطا الله، مرجع سابق، ص 59.

أ/- الحالة الأولى:

وفيها يستعين المتهم بجهاز الكمبيوتر للاحتيال على شخص معين، في هذه الحالة تكون الاستعانة في الاحتيال على جهاز الكمبيوتر، وذلك بقيام المتهم بنشر دعاية كاذبة بغية تحقيق أرباح من نشاطه التجاري الغير مشروع.

ب- الحالة الثانية:

يستعين فيها المتهم على جهاز الكمبيوتر للاحتيال على جهاز كمبيوتر آخر، إذا هل يمكن النصب على آلة بواسطة آلة أخرى؟ الأصل ان النصب يقع على الإنسان، المادة 336 في قانون العقوبات المصري تنص على أنه "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو اي متاع منقول، وكان ذلك باحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو احداث الأمل بحصول ربح وهمي ونجد أن الآلة تحل محل المجني عليه إذا أصبحت تثير إشكالية كبيرة، إذ نجدها تحل محل صاحبها، وهذا لا يعني إعفائه من المسؤولية، ولقد عرف المشرع الجزائري الاحتيال هو الاستيلاء على الحياة الكاملة عمدا بطريق الحيلة والخداع على مال مملوك للغير¹.

ولقد نصت المادة 372 ق.ع الجزائري على جريمة النصب والاحتيال على كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالفات أو إبراء من الالتزامات أو الحصول على أي منها أو شرع في ذلك وكان ذلك الاحتيال لسلب كل ثروة الغير أو بعضها أو الشرع 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 وهمية².

1- طباش أمين، مرجع سابق، ص 103.

2- الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري.

1/-الركن المادي لجريمة الاحتيال: هو الاستيلاء على الحيازة الكاملة لمال مملوك للغير عن طريق إحدى وسائل الاحتيال المتعددة في القانون على سبيل الحصر.

2/-الركن المعنوي لجريمة الاحتيال: 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 القول أن الاموال التي يتم تداولها في نطاق المعاملات الإلكترونية يمكن أن يثيرها النشاط الإجرامي المنصوص عليه في المادة 372 من ق.ع.ج كون التلاعب بالمعلومات او البيانات المحيطة بتلك الأموال يؤدي في النهاية إلى تسليم المال للجاني¹.

2/-الحماية الجنائية للمستند الإلكتروني لجريمة الاحتيال:

لقد تعددت الخلافات حول جواز الاحتيال على الكمبيوتر ومن بينها المشرع الياباني ممن خلال المادة 246 في الفقرة الثانية في قانون العقوبات أنه نص على ما يلي: " يعاقب على الاستعانة بمعلومات مبرمجة كاذبة أو إدخال هذا النوع من المعلومات في نظام الكمبيوتر لشخص آخر للحصول لنفسه أو للغير على ربح غير مشروع².

وقد نص المشرع المصري من خلال المادة 336 من قانون العقوبات، أما من شرع في الاحتيال ولم يتممه فيعاقب بالحبس مدة لا تتجاوز السنة ويلاحظ أن المشرع المصري عاقب مرتكب الجريمة والتي لم يتم إتمامه أنه أقر عقوبة لا تتجاوز السنة وهذا إعمالاً لمبدأ سوء نيته في ارتكاب الجريمة أو محاولة ارتكابها رغم العدول عليها في آخر المطاف، سواء بإرادته أم بإيقاف من طرف عون السلطة أو النيابة العامة إن اقتضى الحال.

1- طباس أمين، مرجع سابق، ص 114.

2-المادة 336، من قانون العقوبات المصري.

المبحث الثاني: الأفعال الماسة بسرية المستند الإلكتروني وقواعد الضبطية في الجرائم المعلوماتية

من بين المخاطر التي تهدد أمن المستند الإلكتروني، هي تلك التي تستهدف إفشاء وإذاعة ما يحتويه من معلومات قد تكون هذه المعلومات غاية في السرية لا ارتباطها بأمن الدولة أو لكنها تتعلق بأحد المشاريع الضخمة، أو الصفقات لإحدى الشركات، فيكون إفشاء سر مستنداتها الإلكترونية ضارا بمصالحها ويؤدي إلى تحقيق المنافسة الغير المشروعة.

المطلب الأول: الأفعال الماسة بسرية المستند الإلكتروني

تعدد صور الأفعال الماسة بسرية المستند والتي نصت عليها التشريعات المقارنة، فقد تأخذ هذه الأفعال صور الدخول غير المشروع على السجلات الإلكترونية، وقد تأخذ صورة نسخ محتوى المعلومات والبيانات التي يحتويها المستند أو طبعها، ونشير فيما يلي إلى خطة التشريعات المقارنة في النص على هذه الافعال، ثم نبين الأركان المشتركة لهذه الجرائم.

الفرع الأول: التشريعات المقارنة في النص على الجرائم الماسة بسرية المستند الإلكتروني

1- القانون المصري:

لم يضع المشرع المصري نصوصا متفرقة على تقرير بعض صور هذه الحماية، ومن أهمها ما نص عليه في قانون الأحوال المدنية رقم 143 لسنة 1994 السابق الإشارة إليه من ان البيانات والمعلومات المتعلقة بالأحوال المدنية، والتي تشمل عليها "السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الملحقة "سرية"، ولا يجوز الإطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نصت عليها المادة 13 في فقرتها الأولى من هذا القانون) بل إن الشارع قد اعتبر أن البيانات أو المعلومات أو الإحصائية المجمععة التي تشمل عليها السجلات والدفاتر الإلكترونية السابق ذكرها "سراً قومياً" لا يجوز الإطلاع عليه أو نشره إلا لمصلحة

قومية أو علمية وبإذن كتابي من مدير مصلحة الأحوال المدنية أو من نيوبه(المادة 13 في فقرتها الثانية).

2/- القانون الفرنسي:

عاقب المشرع الفرنسي بنص المادة 323-1 من قانون العقوبات على مجرد الدخول بطريق الخداع في كل أو جزء من نظام المعلومات أو إبقاء الاتصال به على نحو غير مشروع، وقد شدد العقوبة إذ تترتب على نشاط الجاني إلغاء أو تعديل البيانات الموجودة بالنظام أو تعديل تشغيل هذا النظام وقد شدد الشارع الفرنسي العقاب في حالة ما إذا ترتب على الدخول في النظام أو البقاء فيه أو محو تعديل البيانات التي يحتويها النظام أو ترتب عليها تعطيل النظام عن القيام بعمله، ويجب لتوافر هذا الظرف أن تتوافر علاقة السببية بين فعل الدخول غير المشروع أو البقاء في النظام وبين محو أو تعديل البيانات أو تعطيل النظام عن القيام بعمله، إما إن كان هذا المحو أو التعديل رجع إلى أسباب أخرى هي التي أدت إليه كالقوة القاهرة والحادث الفجائية، فإن صلة السببية تعد منقضية، ولا يسأل الجاني في هذه الحالة عن الظرف المشدد، ويحمي الشارع الفرنسي كذلك سرية المستند الإلكتروني من خلال المواد 226-16 إلى 226-24 من قانون العقوبات التي تجرم المساس بسرية المعلومات المخزنة¹.

2/- القانون الألماني:

تدخل المشرع الألماني بقانون 15 مايو سنة 1986 فأضاف المادة 202 (أ) إلى قانون العقوبات، التي جرم بمقتضاها فعل التجسس على المعلومات المخزنة، ويتحقق الركن المادي لهذه الجريمة بفعل الحصول على المعلومات المحفوظة أو نقلها، وذلك بطريق الدخول غير المصرح به للجاني لهذه المعلومات، ومن المستقر عليه في نظر الفقه والقضاء الألمانيين أنه يلزم لتحقيق هذه الجريمة أن تكون هذه المعلومات مخزنة بوسيلة إلكترونية مثل الكمبيوتر

¹ عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسة مقدمة إلى المؤتمر الذي عقده كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر والأنترنيت"، وذلك بفندق هيلتون العين في الفترة من 1-3 مايو سنة 2000.

وشبكات المعلومات والأرشفة الإلكترونية وقد اشترط المشرع الألماني أن تتوفر لهذه المعلومات حماية خاصة، ومثال ذلك استلزم توافر كلمة سر للولوج الى هذه المعلومات أو بطاقة خاصة¹.

5/ القانون الأمريكي:

جرّم الشارع الأمريكي الاتصال بأجهزة كمبيوتر بطريق الخداع، وذلك بموجب المادة 1030 (أ) في فقرتها الثانية، ونص على "خطر الاتصال العمدي غير المأذون به لأجهزة الكمبيوتر ذات الشأن الاتحادي. وقد أوضح المشرع الأمريكي والمقصود بعبارة "أجهزة الكمبيوتر ذات الشأن الإتحادي" من أنها جهاز كمبيوتر مقصور استعماله على مؤسسة مالية أو حكومة الولايات المتحدة أو في حالة عدم قصر استخدامه على النحو السابق فإنه يكون مستخدماً في أو بواسطة مؤسسة مالية أو حكومة الولايات المتحدة، وأن يكون التصرف المشكل للجريمة مؤثراً في عملية لهما تجري باستخدام بواسطة مؤسسة مالية أو حكومية الولايات المتحدة، وأن يكون التصرف المشكل للجريمة مؤثراً في عملية لهما تجري باستخدام هذا الكمبيوتر، أو متى تم استخدام واحد أو أكثر من أجهزة الكمبيوتر في ارتكاب الجريمة ليس جميعها موجودة في ولاية واحدة، وقدم الشارع الأمريكي صوراً مختلفة من الأفعال يجمع فيها "فعل الدخول غير المشروع" ومن أهم هذه الصور نجد:

1/-الاتصال بغير إذن بكمبيوتر، للحصول على معلومات تتعلق بالدفاع الوطني أو العلاقات الخارجية أو للحصول على معلومات في السجل المادي لمؤسسة مالية أو لمكاتب حماية المستهلك أو للتلاعب في المعلومات المخزنة على الكمبيوتر، الذي من شأنه إحداث أثر ماس لعملية التي تجريها حكومة الولاية المتحدة بهذا الكمبيوتر.

2/-الاتصال بكمبيوتر ذا شأن اتحادي دون أن يكون مرخصاً بإجراء هذا الاتصال أو بالتجاوز لهذا الترخيص، وذلك بنية سلب أو الحصول على أي شيء ذا قيمة.

3/-الدخول العمدي غير مأذون به لكمبيوتر ذو شأن اتحادي، وتمكنه بهذه الوسيلة من تغيير أو إلحاق الضرر أو محو البيانات المسجلة به، أو منع استخدام مشروع لهذا الكمبيوتر، وقد

¹- WESSELS (Johannes)/ Hettinger (Micheel):StrafrechtBesohdererteil 1/1999), 5-138.

تضمن قانون 1994 ثلاث إضافات مهمة إلى التعديل الصادر بموجب قانون 1984، الأول غير بمقتضاه ما شمله من أفعال ارتكبت على كمبيوتر ذو شأن اتحادي وأثرت على هذه الأجهزة إلى الأفعال على أجهزة كمبيوتر في داخل الولايات في مجال التجارة أو الاتصالات.

الفرع الثاني: العناصر المشتركة في جرائم المساس بسرية المستند الإلكتروني

1- الجاني:

الجاني في جرائم الاتصال غير المشروع هو من يفصل الجهاز كمبيوتر مشمول بالحماية بدون أن يكون مأذونا له بذلك ولا يكون له التوقع المعتاد لمساس فعله بالحق في الخصوصية في حال الاتصال المجري من أو إلى جهاز مشمول بالحماية ولا تتطلب الجريمة صفة خاصة في فاعلها، إذ ترتكب من أي شخص سواء أكان له صلة وظيفية في مجال أنظمة المعالجة الإلكترونية أم أنه لا تتوافر له مثل هذه الصفة¹ ويخرج عن هذا المدلول من كان يرتبط بعلاقة عقدية قائمة من مالك أو مدير جهاز كمبيوتر مشمول بالحماية تتيح له تحقيق الاتصال كليا أو جزئيا بهذا الجهاز.

2- فعل الدخول غير المشروع:

وتتحقق الجريمة بفعل الدخول، ولم تأكد التشريعات المقارنة المقصود بفعل الدخول أو الوسيلة المتبعة في ذلك الدخول، ومن ثم تقع الجريمة بأي وسيلة من الوسائل، فقد يتم الدخول باستعمال أجهزة خاصة تمكنه من كسر شفرة قاعدة البيانات أو أن يستخدم الشفرة الصحيحة الخاصة بشخص آخر مأذون له بالدخول، وتفترض الجريمة أن نظام لدخول على البيانات غير متاح للجمهور، وإنما يكون الإذن فيه مقصورا على عدد محدود من الأشخاص أو الهيئات². ويستوجب أن يتم الدخول إلى قواعد البيانات كلها أو إلى جزء فقط من نظام التشغيل، وتتحقق الصورة الأخيرة إذ تمكن الجاني من كسر شفرة بعض قواعد البيانات أو مواقع المعلومات دون

1- علي عبد القادر القهوجي، ص 51.

2- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، 2001، ص 50.

أن يتمكن من اختراق كل مواقع النظام، وقد يكون البقاء غير المشروع حقا لاحقا على دخول قد تم بموجب مشروع، ويتحقق ذلك بتجاوز شخص النطاق الزمني أو الغرض المصرح له في الاتصال بنظام المعلومات وقد ذهب رأي في الفقه إلى أن جريمة الدخول غير المشروع هي جريمة وقتية، في حين أن البقاء داخل النظام يتصف بالاستمرار وذلك أن العبرة في تحديد طبيعة الجريمة هو بتحديد مدى قابلية ركنها المادي للاستمرار، وفي تقديرنا أن هذا الرأي هو محل نظر ذلك أن العبرة في تحديد طبيعة الجريمة هو بتحديد مدى قابلية ركنها المادي للاستمرار، ولاشك في أن الدخول على نظم حفظ البيانات الإلكترونية يمكن أن يستمر فترة من الوقت بتجرد أثناءها ارتكاب الركن المادي للجريمة، ولا تقف الجريمة إلا بإنهاء الجاني دخول غير المشروع ويلاحظ في تقديرنا أنه لا يجوز الاستناد إلى تعدد صورتي التجريم في النص الفرنسي سالف الذكر والذي يجرم فعلي الدخول والبقاء لأن هذا التعدد كان لعله أخرى مفادها مواجهة صورة تجاوز الشخص الذي كان دخوله قد تم بوجه مشروع لنطاق الإذن المخول له، وهو الأمر الذي لا صلة له بطبيعة الجريمة، وقد ذهب جانب من الفقه إلى الدخول قد يكون مشروعاً إذا كان عن طريق الصدفة أو الخطأ أو السهو وأنه كان يجب على الشخص في هذه الحالة أن يقطع اتصاله وينسحب فوراً فإن بقي سري عليه نص العقاب، وينتقد البعض هذا الرأي بقولهم أن الدخول بطريق الصدفة أو الخطأ أو السهو سيتم بعدم المشروعية وإن كان القانون الجنائي لا يعاقب سوى على الدخول العمدي، وعندئذ يعاقب الجاني إذا بقي عمداً بالنظام و ذلك أن الجريمة لا تتوفر بمجرد الدخول غير المشروع، وإنما يجب أن يتصف هذا الدخول بالخداع ويعني ذلك أن احتمال السهو أو الخطأ قد لا تتوفر في حال وجود الخداع، ومن ناحية أخرى فإن الدخول المجرد من الخداع، لا يعد دخولا غير مشروع، ذلك أن سماح النظام بالدخول دون أن ينطوي هذا الدخول على أي غش أو خداع فإن الفعل يتجرد من صفة عدم المشروعية، حتى لو ثبت أن هذا السماح كان بسبب خطأ في التشغيل، ذلك أنه لا ينسب في هذه الحالة للشخص إثم، كما قد يكون الدخول مفتوحاً للكافة غير أنه يكون مقيد بقواعد

بيانات معينة دون أن يمتد إلى ملفات النظام الأمر الذي يترتب عليه عدم جواز الدخول لهذه المواقع¹.

3- استعمال طرق خداعية:

يجب أن يتحقق الاتصال غير المشروع بطرق خداعية ويفسر تعبير "طرق الخداع" تفسيراً واسعاً، فهو لا يتطلب أن يستخدم الجاني وسائل تدليسية في إحداث هذا الاتصال بل يكفي أن يتحقق دون أن يكون الجاني مأذوناً له به متى كان القصد الجنائي متوافراً لديه وقد فسر القضاء الفرنسي تعبير "الدخول بطريق الخداع" التي نص عليها المشرع الفرنسي في المادة 323-1 سائلة الذكر بأنها تشمل كل الوسائل غير المشروعة التي يتمكن بها الجاني من الدخول في نظام معالجة آلية للمعلومات، ويتحقق ذلك إذا كان حق الاطلاع على البيانات والسجلات الإلكترونية مقصوراً على أشخاص أو هيئات معينة ليس من بين الجاني، وقد يحدث في بعض الأحيان أن يكون هذا الاتصال مأذوناً به للعامة غير أنه يكون مقيداً ببعض القيود، وفي هذه الحالة لا يكون حق الدخول على البيانات مشروعاً إلا بعد استيفاء هذه القيود، ومن أمثلة هذه القيود سداد مبالغ مالية معينة نظير لدخول على موقع الكتروني معين ونسخ بعض الملفات منه، ويترتب على عدم استيفاء هذه القيود أن يصبح الاتصال الإلكتروني غير مشروع ويتوافر الخداع إذا تمكن الجاني من فك الشفرة السرية للدخول، بل ويتوافر الخداع أيضاً إذا تمكن الجاني من استخدام كلمة السر أو الشفرة الحقيقية في هذا الدخول متى لم يكن مأذوناً له بالدخول ويستوجب أن يكون الدخول على النظام قد تم مباشرة وتطبيقاً لذلك قضى القضاء الأمريكي كإدانة أحد الأشخاص بتهمة الدخول غير المشروع على السجلات المتواجدة بإحدى المحاكم الاتحادية، وتتحصل وقائع هذه القضية في أن نظام حفظ المعلومات الإلكتروني في المحاكم الاتحادية الأمريكية يجيز للعامة حق الاتصال بالسجلات الإلكترونية الخاصة بهذه المحاكم والتي تضم الأحكام والقرارات والمستندات المتعلقة بالدعاوي التي عرضت على

1- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 1992، ص 151.

المحكمة وأصدرت حكمها أو قراراتها فيها، كما تحوي أيضا تقرير إحصائية تتصل بعمل هذه المحاكم غير أن هذا النظام قد قيد حق نسخ هذه المعلومات وإنزالها على الكمبيوتر الشخصي أو طبعها بسداد مقابل نقدي عن كل صفحة وقد قام الجاني بالاتصال بسجلات محكمة مقاطعة كولومبيا، وتمكن من نسخ الملايين من الصفحات إلى جهازه كما أنه باستخدام برنامج خاص اشترطه تمكن من وضع ملفات الكترونية خفية في نظام تشغيل سجلات المحكمة الإلكترونية تسببت في عدم احتساب أي نفقات تنتج من عملية نسخ أو طبع المستندات الإلكترونية وهو ما أدى إلى إلحاق أضرار مادية جسيمة بهذا النظام.

4/- جريمة الاتصال غير المشروع تتوافر ولو يترتب ضرر بالمجني عليه:

لم تتطلب التشريعات التي جرمت فعل الاتصال الإلكتروني غير المشروع أن يترتب ضررا بالمجني عليه ويعني ذلك في حقيقة الأمر أن الجريمة تتوافر بمجرد قيام الجاني بالاتصال الكترونيا بأجهزة الكمبيوتر المخزن بها المستندات والسجلات الإلكترونية ويعني ذلك أن هذه الجريمة من جرائم السلوك المجرد التي لا تفترض بتحقق نتيجة من أي نوع، وعليه خطة هذه التشريعات هو الحق في السرية الذي يتحقق المساس به بمجرد قيام الجاني بالاتصال غير المشروع، وتطبيقا لذلك قضى القضاء الأمريكي بتوافر جريمة الاتصال بطريق الاحتيال في حق شخص تمكن من استخدام وصلة هاتف تليفوني في الاتصال غير المشروع بأجهزة الكمبيوتر الخاصة بإحدى الشركات التي تعمل في مجال التجهيزات الإلكترونية بالولايات المتحدة، وقام من خلال هذا الاتصال بالدخول على المواقع الخاصة بجامعة ليدز بإنجلترا وتمكن من فحص قوائم بأسماء الأشخاص في هذه الجامعة وشفراتهم الخاصة، وقد قضى بإدانة المتهم على الرغم مما دفع به دفاعه من أن لم يتحقق أي ضرر بالجهات التي اتصل بها الجاني، بل وأنه يحاول الحصول على مال كنتيجة لهذا الاتصال.

5- القصد الجنائي:

جرائم الدخول إلى نظام معالجة البيانات أو البقاء فيه هي جريمة عمدية فيجب أن يعلم الجاني بأنه يدخل إلى موقع لا يجوز له الدخول فيه وأن تتجه إرادته إلى ذلك، ومن ثم لا تتوافر إذا كان الدخول أو البقاء قد تم بطريق الخطأ، وتطبيقاً لذلك ينتفي القصد الجنائي إذا ثبت أن الجاني قد دخل على قواعد البيانات مصادقة وأنه كان وليد خطأ، ولم يكن فعله كاشفاً عن توافر هذا القصد ومن الأمثلة أيضاً إذا كان الدخول على النظام يتم بموجب اشتراك وكان قد سبق للشخص الدخول بوجه مشروع غير أنه قد انتهت مدة اشتراكه وكان يجهل ذلك ومن القرائن الدالة على توافر القصد هي استخدام وسائل خداعية في تحقيق الدخول أو البقاء في النظام، ويتحقق ذلك إذا كان الدخول على النظام يتطلب شفرة أو بطاقة معينة فقام الجاني بصرفه هذه البطاقة أو بكسر هذه الشفرة، وإذا توافر القصد الجنائي، فإنه لا عبرة بالبواعث التي تكون وراء قيام الجاني بفعله فيستوجب أن يكون هذا الدخول قد تم بدافع الفضول أو بغير مشروع¹.

المطلب الثاني: قواعد الضبط في الجرائم المعلوماتية

تتطلب قواعد الضبط في الجرائم المعلوماتية نفس الضوابط المعتمدة في المجالات المدنية فإنه باعتبار الشخص يتمتع بحرية فكرية وحرية في التعبير وحرية في المسكن وفي الأموال سواء المنقولة أو الثابتة فإن كل هذه الحريات والحقوق توقع على عاتق المفتش الالتزام بمجموعة من الضوابط والإجراءات سواء في مرحلة التفتيش أو في مرحلة المحاكمة وتنفيذ الحكم ويجب أن يكون التفتيش ثابتاً بطلب إذن من الجهات المختصة إلا أنه في بعض الأحيان تقع عدة استثناءات ويكون التفتيش رغم عدم قانونيته ساري المفعول، وكذلك الشأن بالنسبة للاختصاص وجانب تطبيق القانون لحل هذه الإشكالات التي تمس المستند الإلكتروني.

1- علي عبد القادر القهوجي، مرجع سابق ص 54.

الفرع الأول: القواعد المنظمة للتفتيش

في هذا الفرع سنحلل الضوابط المتعلقة بالتفتيش حيث سنتعرض في الفقرة الأولى إلى حالات التفتيش في حالة وجود إذن بذلك من طرف الجهات المختصة.

1/- تفتيش النظام بناء على إذن:

سوف نتطرق في هذه الفقرة إلى شروط إذن تفتيش المواد الإلكترونية (أولاً)، ثم إلى صعوبة تحديد محل التفتيش في الإذن (ثانياً).

أولاً: شروط إذن تفتيش في المواد الإلكترونية

وفقاً للأصل العام لا يجوز تفتيش الجهاز كما أقر ذلك التشريع الأمريكي إلا إننا قد نجد في بعض الحالات يكون التفتيش بدون إذن فما شروط ذلك:

أ- شرط خطورة الجريمة:

استقرت التشريعات بوجه عام لصحة التفتيش كون الجريمة ذات خطورة معينة، إذ نجد القانون التقليدي يستلزم أن تكون الجريمة المعاقب عليها بالحبس لمدة تزيد عن ستة أشهر، أما القانون المصري فلم يشترط درجة معينة من الجسامة عندما يتعلق الأمر بالرسائل البريدية وتسجيل المحادثات الهاتفية حيث يتعين أن يكون ذلك في جناية أو جنحة معاقب عليها لمدة تزيد عن 03 أشهر.

ب/- شرط جدية التحريات:

من المعلوم أن تكون هذه التحريات ذات جدية ويجب أن يكون مبني على دلائل كافية، وهذا ما نصت عليه قواعد الإجراءات الجنائية الأمريكية في الفقرة 41-ج إذ لا بد من توفر الدلائل

المنصوص عليها في المادة ومن أمثلة الدلائل الكافية التي يستند عليها الإذن بالتفتيش نقل الصور الفاضحة أو عناوين الانترنت وارتباطهم برقم حساب المتهم لدى مزود الخدمات¹.

ج/- شرط التحديد:

يعتبر شرط التحديد لازم لصحة الإذن بالتفتيش وذلك ما نص عليه المشرع المغربي في قانون المسطرة الجنائية في الفصل 108 الذي نص على "يمنع التقاط المكالمات أو الاتصالات المنجزة بوسائل الاتصال عن بعدها وتسجيلها أو أخذ نسخ منها وحجزها" غير أنه يمكن لقاضي التحقيق إذا اقتضته الضرورة البحث ذلك إذا أمر بالتقاط المكالمات الهاتفية وكافة الاتصالات المنجزة بواسطة رسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها².

ثانيا: صعوبة تحديد محل تفتيش في الإذن

تواجهنا مجموعة من الصعوبات في تحديد محل التفتيش في الإذن الخاص بتفتيش أجهزة الكمبيوتر مثلا ويرجع ذلك إلى العدد الكبير من الملفات التي يحملها الكمبيوتر ومما يزيد الأمر تعقيدا أن أسماء هذه المستندات لا تعمل على محتواها فقد يعتمد المتهم إلى الاعتماد على أسماء مستعارة وقد لا تحتوي على مضامين هذه الملفات كما تثار صعوبة قانونية فيما يخص جرائم الكمبيوتر وذلك عندما يشتكي صاحب الجهاز من وقوع الضرر من صاحب المستند من احد الجرائم التي تمت الإشارة إليها مثل: جريمة التزوير أو السرقة أو الإتلاف إلى غير ذلك كما هو واضح في فإن هذا المجال يدخل في مجال الالكترونيات يصعب معه تحديد التفتيش لأن الواقع العملي بالنسبة للجرائم التي تقع على المستندات سرعان ما يختفي الجاني من ساحة الجريمة أو عدم معرفتها على الإطلاق إلى أن يقع حاجز في طريق المستند يكشف حقيقة الأمر إذن فما هو مجال التفتيش؟ وما هي السلطة المختصة بإصدار إذن التفتيش؟.

1- شيماء عبد الغني عطا الله ، مرجع سابق، ص 281.

2- المادة 108 من قانون المسطرة الجنائية

- تعريف التفتيش:

يعرف التفتيش على أنه إجراء من الإجراءات التحقيق يهدف إلى جمع الأدلة، وأما الغموض عن الجريمة ونسبتها إلى متهم معين ويمكن تعريف تفتيش نظم الحاسوب والانترنت بأنه " البحث في مستودع سر المتهم عن الأشياء مادية أو معنوية تفيد كشف الحقيقة ونسبتها إليه وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني¹.

أ- مجال الإذن بالتفتيش:

يشمل الإذن بالتفتيش جميع الملفات المخزنة بواسطة جهاز يعود إلى الشخص المشترك أو المتعامل معه وكذا جميع المحتويات والبيانات المتضمنة والتي نضمها القانون الأمريكي لمدة أقل من 180 يوم حتى أن الأمر لا يستوجب صدور إذن أو توجيه إنذار المشترك وعلى هذا النحو فإن الإذن بالتفتيش لا يتقيد بنوع من المعلومات غير أن المشرع الأمريكي اشترط في هذا الإذن أن تكون الدلائل متوفرة وكافية تدل معالمها على وجود خرق للبيانات المتضمنة في المستند وتواجد جريمة ويتوجب على المعنيين بالأمر التدخل من أجل حمايتها ويمكن أن يقع التفتيش بأي مكان من ملحقات الأجهزة الإلكترونية لها علاقة بالمستندات التي وقع الإخلال بها فمثلا لو تم نسخ بعض البيانات التي كانت في حوزة شخص معين تعود ملكيتها إليه من جهازه إلى جهاز المشتبه به فإن هذا الجهاز الأخير بحالة التفتيش.

ب/- الجهة المختصة بإصدار الإذن بالتفتيش:

تحول صعوبة في تحديد الجهة المختصة بإصدار إذن التفتيش وترجع هذه الصعوبة إلى عدم ثبوت مكان معين لهذا النوع من التعاملات حيث تقضي القاعدة العامة في الكثير من الدول

1- علي عدنان القبل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة بالمكتب الجامعي الحديث (د، ب، ن) ص 39.

على سبيل المثال كندا والولايات المتحدة الأمريكية هاتين الدولتين حثا على ضرورة توافر الاختصاص للجهة القضائية التي تقوم بإجراء معين¹.

كلما تواجدت هذه البيانات محل التفتيش أو الضبط في الجهاز أو حل شبكة تتواجد في دائرة اختصاص الجهة التي تأمر بهذا الإجراء².

حيث أن الاختصاص يعود للجهة التي يعود لها محل التفتيش وقيام رجال الضبط بتفتيش أشياء لم يحددها الإذن الصادر بالتفتيش فإن ذلك يجعل التفتيش باطلا إذ أن القواعد التي يخضع لها الإذن بالتفتيش في المواد الإلكترونية مستمد من القواعد العامة وتتجلى هذه القواعد في السماح بتفتيش في الأشياء المغلقة ولو أن الإذن بالتفتيش كان صادرا بمكان تواجدها وليس بذاتها وقد اعتبر القضاء الأمريكي بصحة ذلك مثلا تفتيش الصناديق المغلقة المتواجدة في المكان الذي صدر فيه أمر التفتيش ومادام الكمبيوتر يتماثل مع الصناديق المغلقة فإن تفتيشه يعد صحيحا رغم أن الأصل في القانون الأمريكي بالنسبة لطريقة الامتثال لقاعدة عدم الاقتحام أي أن رجل الشرطة يلتزم بالقاعدة " أطرق الباب وأعلن عن نفسك" والمستفاد من هذه القاعدة طرق الباب بمرونة، وإعلان ضابط الشرطة عن نفسه أن المتهمين قد يخفوا المخدرات بسرعة وهذا الأصل يرد عليه استثناء وهو الأمر الذي يسمح للمحقق في الاقتحام ونجد المشرع المصري قد عمل على اقتحام مكان التفتيش في جميع الأحوال، ولكي يقوم المحقق بتضمين البيانات المتواجدة في الحاسب الآلي قبل أن يقوم المتهم بمسحه³.

وقد نص المشرع الأمريكي في المادة 4 من قانون الإجراءات بأن "اكتساب سماعي أو غيره لمحتوى أية اتصالات سلكية أو الكترونية أو شفوية وذلك من خلال استعمال أية جهاز سواء كان هذا الجهاز آلي أو إلكتروني أو غير ذلك" ويكمن التمييز في هذه الحالة بين أربعة أوضاع للاطلاع على محتوى المستندات والاتصالات.

1- شيماء عبد الغني، عطا الله ، مرجع سابق، ص 291.
2- المادة 4 من القانون الأمريكي الفدرالي.
3- شيماء عبد الغني، عطا الله ، مرجع سابق، ص 295.

1/- اعتراض الاتصالات ويتم ذلك أثناء تبادل الاتصالات.

2/- تفتيش الاتصالات ويتم ذلك عند نهاية الاتصالات أو وصول الرسائل الإلكترونية وقيام المكلف القضائي بفتحها والاطلاع عليها.

3/- مجرد العلم ويتم ذلك عند وصول الرسالة مفتوحة أو نهاية الاتصال في حضور رجال الضبط القضائي.

4/- اتصال بشبكة عامة وتتم هذه الحالة باتصال بشبكة عامة أي يسمح لعدد غير محدد من الأفراد الاتصال بها.

يخضع التفتيش لعدة ضوابط يجب احترامها لتكون عملية التفتيش صحيحة ولصحة هذه العملية لا بد من أخذ الإذن من الجهات المختصة، وترد على هذه القاعدة عدة استثناءات حسب الظروف المتعلقة بالجريمة وملاساتها، لأن المشرع أجاز مباشرة التفتيش دون أخذ إذن من السلطات المختصة وذلك في الحالات التالية:

1/- الحالة الأولى: وقت التفتيش

تتم عملية التفتيش في وقت معين وقد حدده المشرع المصري من ساعة السادسة صباحاً إلى الساعة التاسعة ليلاً وفقاً للمادة 69 المسطرة الجنائية التي تنص: أنه لا يمكن المشرع تفتيش المنازل أو معابنتها قبل السادسة صباحاً وبعد التاسعة ليلاً مضمون هذه الفقرة هو احترام وقت التفتيش المعين وعلاقة ذلك بالمستند الإلكتروني في المنزل، وهنا لا بد أن يتم هذا التفتيش وقت الوقت المحدد قانوناً.

2- الحالة الثانية:

إذا تعلق الأمر بجريمة خطيرة وهنا لابد من الانتقال وبشكل استعجالي ومعاينة الجريمة وذلك خشية اندثار الأدلة وان كان الوقت غير قانوني¹.

3- الحالة الثالثة: الرهن بالتفتيش

تقضي القواعد العامة بان قاضي التحقيق لا يحتاج إلى إذن من النيابة العامة بالتفتيش إذا كان صاحب الجهاز راضيا به، وهنا نقول ان محكمة النقض المصرية لما كان من المقرر أن القيود الواردة على تفتيش المنازل والحماية التي أحاط بها الشارع تسقط عنها من يكون دخوله بغير رضاء أصحابها صريحا حرا لا لبس فهو بمقتضى هذه المادة أنه إذا كان صاحب الجهاز موافقا بإرادته على تفتيش جهازه، فلا داعي لطلب الإذن بذلك، ومن خلال هذه المادة أيضا نستنتج أن دور طلب إذن بالتفتيش مجرد إجراء احتياطي في حالة رفض صاحب الجهاز تمكين قاضي التحقيق من إجراء التفتيش في الحالات التي يكون فيها التفتيش صحيح وهناك عدة أحكام وسعت نطاق التفتيش في الحالات التي يكون فيها تحت رضا صاحب الجهاز، حيث يمكن للمفتش الاطلاع على كل شيء قد يفيد في التحقيق وأي دليل يمكن أن يقوده إلى الحقيقة، وكل تفتيش نتج عنه عدم احترام النطاق المسموح به يعتبر باطلا.

4- الحالة الرابعة: حالة الضرورة

ذهب القضاء الأمريكي بجواز التفتيش دون إذن بالتفتيش وذلك في الحالات التي لا يمكن فيها الانتظار حتى يصدر الأمر بذلك وذلك لدفع ضرر محتمل الوقوع جراء التأخير في التدخل بسبب ذريعة الإذن وتتجلى كذلك في حالة خشية إتلاف دليل الجريمة، إذا كان الجهاز أو مسجل في ديسك أو أسطوانة وفي هذا ذهب المشرع المصري إلى أنه لا حاجة للاستفادة من حالة الضرورة بجواز تفتيش الأجهزة الإلكترونية الخاصة بالمتهم إذ صدر إذن بالقبض عليه.

1- الفقرة الثانية من المادة 62 من قانون المسطرة الجنائية.

5- الحالة الخامسة: حالة التلبس

تتحقق حالة التلبس طبقاً للمادة 56 من المسطرة الجنائية بجناية أو جنحة إذا ضبط الفاعل مازال مطارداً بصياح الجمهور على إثر ارتكابها، أو إذا وجد الفاعل بعد مرور وقت قصير على ارتكاب الفعل كحمل أسلحة أو أشياء يستدل معها أنه شارك في الفعل الإجرامي أو وجد عليه أثر أو علامات تثبت هذه المشاركة يعد بمثابة تلبس بجناية أو جنحة، ارتكاب جريمة داخل منزل في ظروف غير الظروف المنصوص عليها في الفقرات السابقة إذا التمس مالك أو ساكن المنزل من أنه كان الجهاز داخل المسكن، فلا يعتبر ذريعة لإقحام المنزل وتفتيشه وعلى العموم فإنه من الناحية العملية فإنه يصعب أعمال قواعد التلبس في مجال الجرائم الإلكترونية حيث يتعين أن شاهد قاضي التحقيق وهي تقع أو إذا اتبع المعني عليه مرتكبها أو تبعية العامة بالصياح اثر وقوعها أو وجد مرتكبها يعدو وقوعها بوقت قصير حاملاً الآن، أو يستدل منها على انه فاعل أو شريك فيها أو وجدت أثارا أو علامات تفيد ذلك، كما يجوز كذلك تفتيش أي جهاز وما يجعله من مستندات وذلك إذا كان ذلك من شأنه أن يسبب في خدش الأمن الوطني وإلحاق الضرر بسيادة الدولة.

6- الحالة السادسة: التفتيش من أجل الحفاظ على الأدلة

للمفتش صلاحية حيازة كل المضبوطات وتحريرها على الوجه الذي يمكن معه الرجوع إليها ولا يعين هذا الإجراء بالبطلان مثلاً وذلك في حالة إذا كان ما سيحوزه هذا المفتش يعتبر جريمة، وقد كانت هذه الحالة محل نقاش حيث أن القضاء الأمريكي لا يعتبر هذا الإجراء معقول إلا إذا كان مبرراً لذلك.

7/- الحالة السابعة: عدم مخالفة التفتيش لجريمة المسكن

لكل شخص حرمة في منزله ويجب ان لا تنتهك تحت أي مبرر وذلك انطلاقاً من عدة حقوق أولية تضمن لكل فرد الحق في أن يؤمن على نفسه وبيته وأمواله ومستنداته ضد أي تفتيش غير معقول.

الفرع الثاني: الاختصاص القضائي والقانون الواجب التطبيق

تعد هذه الإشكاليات المتعددة التي تعيب المستند الإلكتروني على وجه الخصوص والمعاملات الإلكترونية على وجه العموم تبقى من بين الإشكاليات المتعلقة بهذا الشأن حول الاختصاص القضائي وهو ما سنعالجه خلال الفقرة الأولى بينما سنخصص الفقرة الثانية للقانون الواجب التطبيق إذن فما المقصود بذلك؟.

الفقرة الأولى: الاختصاص القضائي

تقضي القواعد العامة بأن المتضرر هو الذي يقع عليه عائق الاثبات أو مما أدى إلى الضرر وعلى من يوجه له أصبح الاتهام أن يثبت العكس وإلا إذا كان متورطاً مما نسب إليه، وتبقى مهمة اللجوء إلى القضاء كما سبق الذكر على عاتق المتضرر لكن يختلف هذا الضرر المدني الذي يعتبر الأمر مفهوم فيه من حيث الجهة المختصة، إذن فما الجهة القضائية المختصة؟ يمكن تمييز في هذه الحالة بين نوعين من الاختصاص.

أولاً: الاختصاصات بمنازعات العقود الدولية الإلكترونية

إن المنازعات الخاصة بالمعاملات الدولية في المجال الإلكتروني تخضع للقاعدة العامة في الاختصاص الدولي للمحاكم، حيث يمكن رفع الدعوى أمام محكمة موطن أو محل إقامة المدعى عليه¹.

1- محمد الحسين منصور، المسؤولية الإلكترونية، مطبعة سعيد كامل، الطبعة الأولى مصر الإسكندرية، 2006، ص 347.

وإذا رجعنا إلى النصوص المنظمة للاختصاص المكاني أو المحلي لوجدنا تقرر مبدأ واحد وهو الاختصاص المكاني الذي يعهد للمحاكم التي يوجد بدائرة نفوذها موطن المدعى عليه الحقيقي أو المختار أو محل الإقامة في حالة انعدام موطن لديه¹.

وفي نفس السياق نتيجة الفصل 27 من القانون م. م التي تنظم الاختصاص المكاني يكون الاختصاص المكاني لمحكمة الوطن الحقيقي أو المختار للمدعى عليه².

وفيما يخص هذه القاعدة يمكن الخروج عنها في حالة الاتفاق بين الأطراف على تقرير الاختصاص للمحكمة الأخرى وهذا ما يطلق عليه بمبدأ الخضوع الإرادي أو الاتفاق على الاختصاص في المنازعات ذات الطابع الدولي لكن يشترط لصحة هذا الاتفاق توافق رابطة بين النزاع والقضاء المختار، أو قيام مصلحة مشروعة للأطراف من وراء هذا الاختيار المنطوي على غش، ونجد أن هذا الاتفاق يتم قبل أو بعد النزاع صراحة وذلك في جوهر العقد أو في وثيقة مستقلة أو ضمنا كرفع الدعوى أمام محكمة معينة، وعدم افتراض المدعى عليه وعلى من يدعي وجود هذا الاتفاق، عبء إثباته بالكتابة العادية أو المحررات الإلكترونية وفي حالة تعذر ما سبق ذكره يتم اللجوء إلى مكان إبرام العقد أو تنفيذه ويتحدد الإبرام بالمكان الذي علم فيه الموجب بالقبول ما لم يوجد نص يقضي خلاف ذلك، وباستثناء الأحكام السابق ذكرها نجد أن الاختصاص يعود اما للمواطن أو محل إقامة المستهلك في المنازعات الخاصة بعقود الاستهلاك وبالتالي فمصلحة المستهلك تكون خالية، وبالتالي له الاختيار أما باختيار الاختصاص لمحل إقامته أو محكمة بوطنه أو محل إقامة المدعى عليه، إذ لا يجوز الإتفاق المسبق على عدم اختصاص محكمة الموطن أو إقامة المستهلك وللمتضرر الحق في التعويض الذي لحقه من جراء العمل الغير المشروع، الذي قام به المدعى عليه والتعويض حسب المسؤولية التقصيرية ينسجم بطبيعة الضرر، الذي لحق المتضرر ويتمثل عند اختراق الجهاز المعلوماتي أو تدمير أو التعدي على الملكية الفكرية أو الحقوق الشخصية، مثلا إفساء الأضرار

1- عبد الكريم الطالب، الشرح العلمي لقانون المسطرة المدنية، المطبعة والوراقة الوطنية مراكش ط 06 افريل 2013 ص 55.

2- الفقرة الأولى من الفصل 27 من قانون المسطرة المدنية.

أو المساس بالحق في الخصوصية والمساس بسمعة المشروع أو الشخص عبر الويب والتعويض يقدر بإرجاع المتضرر إلى الحالة التي كان عليها أي إعادة التوازن الذي اختل نتيجة الضرر اللاحق وذلك على نفقة مسبب الضرر إذ يجب أن لا يتجاوز التعويض قيمة الضرر، ويجب أن لا ينقص عليها، وتقدير الضرر يقع تحديده على عاتق القاضي وذلك لما له من سلطة في الموضوع، إلا أن مهمة تقدير الضرر تسبب العديد من الإشكاليات والمتمثلة في كون الضرر الواقع يتغير ولا يتم تحديده نهائياً وقت النطق بالحكم وفي هذه الحالة أجاز القاضي المتضرر أن يطالب خلال مدة معينة أن يطالب بإعادة النظر في التقدير¹.

- الاختصاص بدعوى المسؤولية التقصيرية الإلكترونية:

تخضع المنازعات الخاصة بدعوى المسؤولية التقصيرية الإلكترونية للضابط العام الاختصاص الدولي ألا وهو محكمة موطن أو محل إقامة المدعى عليه².

ونلاحظ دائماً أن الاختصاص المكاني وفي أغلب التشريعات المقارنة تكون لموطن أو محل إقامة المدعى عليه، وهنا يمكن أن نطرح السؤال حول الاختصاص في الاشتراك في جريمة من جرائم المستند الإلكتروني وخاصة إذا كان المتهمين من مناطق مختلفة، فما هي الجهة القضائية المختصة في هذه النازلة المطروحة أمام القضاء؟ وللإجابة عن السؤال فإن العديد من الدول تأخذ بما يسمى "بنظرية استعارة الإجراء" في تحديد اختصاص قضائها³.

وبذلك فإن القضاء لا دخل له أولاً باختصاص إجراء محاكمة من إحدى الشركاء في جرائم المستندات وخاصة في جرائم التي تقع خارج دائرة نفوذ القاضي المختص إذ لا أثر للمحاكمة ضد شريك في الجرائم المعلومات الإلكترونية إذ وقعت في الخارج حيث أن القاضي ليس لديه الحق في متابعة أو محاكمة هذا الفاعل إلا أنه مع تطبيق قاعدة للمبدأ استثناء فإن الاستثناء هنا يمكن أن يعطي الاختصاص للقاضي الوطني، للبت في نازلة أو واقعة تعد معالمها أو

1- محمد الحسين منصور ، مرجع سابق، ص 344.

2- المادة 29 من قانون المرافعات المصري.

3- شيماء عبد الغني، عطا الله، مرجع سابق ص 380.

ارتباطها بشريك في الجريمة من جرائم المعاملات الإلكترونية إذا كان الجاني الأصلي في منطقة نفوذ القاضي الوطني، أن هذا الأخير يمكن أن يبيت في أمره وهذا ما تم التنصيص عليه في قانون العقوبات الفرنسي 113-5 وقد استلزم القانون الفرنسي توافر شرطين لقيام هذا الاختصاص "الأول أن يكون الفعل معاقبا عليه في القانون الفرنسي والأجنبي وان يكون قد صدر حكم نهائي أجنبي يقرر وقوع الجريمة الأصلية في الخارج" ومن خلال النص السالف الذكر يمكن توضيح اختصاص المحاكم الوطنية بالجرائم الإلكترونية التي تقع عن طريق وسائل الإعلام، وبهذا فإن القضاء الفرنسي يختص بالجرائم التي تنصب في هذا الاتجاه أي الجرائم المعلوماتية بوجه عام وفي قرار صادر عن المحكمة النقض الفرنسي والذي يقضي بأن القضاء "يختص بمحاكمة المتهم الأجنبي إذا ارتكب جريمة وقعت في الخارج ما دامت تلك الجريمة مرتبطة مع أخرى وقعت في فرنسا من جانب نفس المتهم"، والأمر هذا يتحقق في مجالات المعاملات الإلكترونية في مواقف عديدة وتدعيما لما سبق فإن اتفاقية بروكسل التي قامت من توسيع الاختصاص في القضايا المدنية، أخذه بموطن إبرام وإنشاء المستند الإلكتروني وذلك تدعيما للمستهلك والمتعامل على حد سواء في القضايا المدنية والجنائية كما أن الاتجاه الفرنسي أعطى المدعي الخيار في رفع دعواه حسب اختياره "أما أمام محكمة موطن المدعي عليه أو أمام المحكمة التي وقع الفعل الضار في ذاكرتها أو تلك التي تحقق الضرر في دائرتها"¹ ونفس الاتجاه ذهب إليه المشرع المغربي حيث أخذ بالرأي الفرنسي واستقى منه قاعدة رفع الدعوى أمام محكمة المدعى عليه قاعدة عامة، إلا أن هناك استثناء يتجلى في إقامته للدعوى باختيار المدعي في رفع دعواه أمام محكمة المدعي عليه أو وقوع الضرر.

الفترة الثانية: القانون الواجب التطبيق

يثور هذا النوع من القوانين عدة إشكالات من حيث القانون الواجب التطبيق على النازلة المطروحة وهنا تزيد في حدة هذا الإشكال، أي قضاء له صلاحية البت في المعاملات الإلكترونية بصفة عامة؟ والقانون الواجب التطبيق على المستند الإلكتروني؟ الذي هو قيد هذه

¹ - المادة 47 من القانون المدني الفرنسي.

الدراسة وبالتالي فتحدد القانون المطبق على المستند الإلكتروني يجب النظر إليه من عدة جوانب كتحديد المسؤولية العقدية الإلكترونية، وننتقل إلى المسؤولية التقصيرية الإلكترونية وفي الختام ننظر من جانب آخر إلى القانون الموضوعي الإلكتروني الدولي.

أولاً: قانون المسؤولية العقدية الإلكترونية.

المبدأ هو أن خضوع العقود والمستندات والمعاملات الإلكترونية لقانون الإرادة وبمعنى القانون الذي يختاره الأطراف، سواء كان بشكل ضمني وبما أن العالم المعلوماتي جعل العالم عبارة عن قرية صغيرة وتجاوز الحدود، ما كان من اللازم الخضوع للقانون الذي يتم الاتفاق عليه بين أطراف الشبكة من خلال الرسائل الإلكترونية المتبادلة، والملاحظ على الأطراف أنه يمكن لهم أن يقوموا بتحديد القانون الواجب التطبيق، أما عند إبرام العقد بمعنى يمكن لهم أن يتفقوا في بداية إبرام العقد على أنه إذا تم نزاع مستقبلي له علاقة بالعقد فإنهم يجدون القضاء أو المحكمة التي يرجع لها الاختصاص في البت في النزاع، كما يمكن لهم أن يتفقوا بعد إبرام العقد أو عند تنفيذه واختيار الأطراف للقانون الذي يحكم الواقعة يمكن أن يتضح ضمناً من ظروف الحال وملابسات العقد والقرائن من تحويل محكمة الاختصاص تنظر المنازعات ومكان التنفيذ، ولقاضي الموضوع سلطة استخلاص النية الضمنية للمتعاملين عن طريق التعاملات الإلكترونية دون الخضوع لرقابة النقض طالما استند في حكمه إلى أسباب (100) زائفة وهذا يرجع إلى فطنة القضاء¹.

وأهمية تحديد المحكمة المختصة بالفصل في النزاع، إذ يرتب ذلك تحديد القانون الواجب التطبيق في حالة تنازع القوانين، وهذا ما يجعلنا نؤمن بأن المحكمة المختصة هي التي تحدد القانون الواجب التطبيق ولذلك فإن تحديد المحكمة المختصة بنظر الدعوى له أهمية واضحة تتمثل في أن قاضي الدولة سوف يقوم بتحديد قاعدة الإسناد وفقاً لقانون دولته أي أن الأمر لا يقتصر على الجانب الإجرائي بل يتعداه إلى الجوانب الموضوعية التي سوف ينزلها القاضي

¹-محمد الحسين منصور، مرجع سابق، ص 53.

على موضوع الدعوى كما أن من مصلحة المدعي تقديم دعواه أمام المحكمة دولته حيث يعرف لغتها ويتابع إجراءاتها فمثلا لو حدث نزاع بين مغربي وفرنسي، وكانت المملكة المغربية هي المختصة فان القاضي هنا سيطبق القانون المغربي بطبيعة الحال لان الأمر يتعلق بالسيادة الوطنية وترجع أهمية ذلك لكون القضاء المغربي أولا له دراية بمعالم القانون الوطني ومن ناحية فالأمر يسهل على المتقاضى في رفع دعواه.

ثانيا: قانون المسؤولية الإلكترونية

فيما يخص هذه النقطة فقد أنتجت جل الانظمة القانونية، إلى الرغبة أو خضوع دعوة المسؤولية إلى الدولة التي وقع فيها الفعل الضار وهذا رأي بعض الفقهاء والمهتمين، وبما أن المستند الإلكتروني قد يتعرض إلى السرقة أو الإلتلاف أو التزوير إلى غير ذلك من الجرائم التي تمس بصحته، وتسبب ضرر للمتعاملين بهذه الطريقة، فان كان من الواجب تعويض الطرف المتضرر من هذا العمل الغير المشروع وللمحكمة أن تأمر بما تراه من تدابير ترمي إلى إصلاح الضرر فإذا كان الضرر الذي لحق الشخص بالواجب الاجتماعي، فإن المسؤولية التي تقع هي مسؤولية الجزائية إلا أن الطرف الذي قد يحصل عند رفع الدعوة أمام المحكمة الفعل الضار عند رفعها أمام المحكمة الضرر في الحالة التي يحصل فيها الضرر أكثر من دولة وإذ يمكن أن يكون الجهاز المستعمل في دولة والضرر في دولة أخرى وبالتالي فإن اختلاف يقع ما إذا رفضت الدعوة أمام محكمة الفعل تختص في أضرار التي تحققت في دولة مختلفة، كما أن الأمر يختلف لما إذا وقعت الدعوة أمام إحدى الدول التي تحققت فيها الضرر والحال هنا أن هذه المحكمة لا تختص إلا في التعويض عن الضرر الواقع في تلك الدولة " إلا بالنسبة للقضايا الجنائية حيث يتعلق الأمر بسيادة الدولة ويقتضي الأمر إيجاد مقدار من التعاون الدولي للتوسع في هذا الاختصاص"¹.

¹-شيماء عبد الغني، محمد عطا الله، مرجع سابق، ص 383.

ثالثاً: القانون الموضوعي للمستند الإلكتروني

أن مبدأ تنازع القوانين في مختلف دول العالم لا تتناسب والطبيعة القانونية للتعاملات الإلكترونية وخاصة المستند الإلكتروني موضوع هذه الدراسة، فالقاعدة العامة والمتعارف عليها أن أي دولة فإن قاعدة الاستناد تحدد قانون داخليا للدولة معينة للفصل في النزاع ذات طابع دولي لأن هذه القاعدة تدخل في تنظيم العلاقات الوطنية الداخلية، وهذا القانون يختص بالطابع الطائفي والحال هذا أن لا يهم كل الأشخاص الموجودين أو المعنيين به بل انه يخاطب أن صح القول الفئة الضئيلة والمحدودة أو المنحصرة في المجال الإلكتروني حيث أن الأمر هذا، يختص هذا النوع في القضايا أو المعاملات الإلكترونية بقضاء خاص أو ما يطلق عليه " بالقضاء الافتراضي الذي يعقد جلساته ويطبق أحكامه عبر الدوائر المعلقة للاتصالات ويتم تبادل الوثائق والمذكرات والدفاع بالبريد الإلكتروني"¹.

ويمكننا القول أن هذا النوع من القوانين يعتبر من قوانين تلقائية النشأة تابع من ضرورة وجود مجتمع الكتروني أن هذا القانون هو قانون موضوعي يحكم المعاملات التي تتصل بأكثر من دولة ويقدم الحل للمسألة، ويحل النزاع مباشرة وينظم العلاقات والروابط الإلكترونية إذ أن المعاملات الإلكترونية تتجاوز الحدود لاسيما على المستوى السياسي والاقتصادي و هذا هو المشكل الذي يواجه هذا النوع من التعاملات إذ يصعب تحديد الجهة المختصة أو القانون الواجب التطبيق ومن خلال ذلك فإن القانون الموضوعي الإلكتروني لا يعتبر قانون بالمفهوم الحقيقي، وذلك راجع إلى عدم وجود مجتمع منظم ومتربط يجمع كل المتعاملين في العالم الإلكتروني، حيث أنه يرفع فيه الصفة الإلزامية، وعدم خضوع مرتكبي أو المخلين بهذه المعاملات إلى الجزاء الذي يكفل احترامها الأمر الذي يحتم تدخل الدولة لإقامة قانون يوازي بين المتعاملين في الوسط أو المحيط الذي ينظم المجالات الإلكترونية.

1- محمد الحسين منصور، مرجع سابق، ص 356.

ملخص الفصل الثاني:

تطرقت في هذا الفصل إلى ذكر الأفعال الماسة بالمستند الإلكتروني من بحث المحتوى ومن حيث السرية وختمنا فصلنا هذا بوصف قواعد الضبط في الجرائم المعلوماتية وكل هذا يندرج تحت وصف الحماية الجنائية للمستند الإلكتروني وذكر أهم الجرائم التي تأثر سواء من حيث المحتوى أو السرية وخاصة جرائم السرقة والتزوير والإتلاف والاحتتيال والتي من شأنها أن تغير جزئياً أو كلياً محتوى المستند الإلكتروني لتضعه في دائرة أهم الجرائم المعلوماتية في هذا العصر ولنذكر بعدها قواعد الضبط في هذه الجرائم ورأي جل التشريعات منها والصيغة القانونية التي ذكرتها كل هذه التشريعات لتوفير عنصر الحماية في مجال التعامل المعلوماتي وهذا كله ضمن قواعد الضبط المحدد في مجال الحماية الجنائية للمستند الإلكتروني وهذا لا يتجسد إلا بتطبيق القانون الواجب التطبيق على هذه الأفعال.

الخلاصة

خاتمة:

من خلال هذا البحث البسيط استعرضنا فيه الحماية الجنائية للمستند الإلكتروني ويعد موضوع الحماية الجزائية للمستند الإلكتروني من المواضيع الحديثة والتي تتعلق بالإطار القانوني للتعاملات الإلكترونية ويعتبر المستند الإلكتروني هو ظاهرة حتمية فرضها التطور العلمي والتكنولوجي المعاصر والذي أفرزته العولمة الاقتصادية والإدارية وهذا مما دفع بمختلف الدول والمؤسسات بأنواعها وأهدافها لضرورة استعمال مختلف المعاملات الإلكترونية وهذا للتكيف مع مستجدات العصر وهذه التعاملات تكون وفق منظومة تشريعية وقضائية وقانونية وهذا الاعتماد الذي أدى بها إلى هذه المعاملات الإلكترونية هو نتاج ما طوي من المستند التقليدي بعد تقلص دوره وعجز أحكامه عن مواكبة التطور بالنسبة للدول التي تتطلع للرقى الصناعي والتقدم التكنولوجي، وإن هذا ما دفع بكثير من الدول إلى تطوير تشريعاتها بسن قوانين جديدة مستقلة عن القواعد التقليدية خاصة والتي كانت تعاني من نقص كبير في المعاملات الحديثة وضرورة خلق وتطوير كفاءة المحققين والقائمين بالاستدلال والتحقيق من خلال الدورات التكوينية في مجال المعلوماتية.

ولقد حاولنا في هذا البحث أن نعرف المستند الإلكتروني بوصف عناصره وفرقنا بتدوين ما يشابهه من المستندات الورقية وذلك بذكر شروط صحته في الإثبات في الجناية التي تستند إلى مبدأ حرية الإثبات وحرية القاضي الجنائي في الإقناع بالدليل الإلكتروني، وتطرقنا كذلك إلى ضوابط توثيق المستند الإلكتروني وتهدد سلامته وصحته مما يؤدي إلى ضياع الحقوق وانتهاك الحرمات الشخصية والحرية الفكرية والعملية ومن بين الجرائم التي تناولها، جريمة التزوير والسرقه والإتلاف والاحتيال وبيننا كيف أن التشريعات نظمت هذه الجرائم ويرهنها ولو ضمنا في نصوص عامة، وأفرزت لكل جريمة عقوبة اختلفت من السالبة للحرية والغرامة وفي بعض الأحيان الجمع بينهما ومما شمله هذا البحث أيضا في الأفعال الماسة بسرية المستند الإلكتروني وقواعد الضبط في الجرائم المعلوماتية وباعتبار المستند الإلكتروني مستند قائما

بالذات يستلزم إخضاعه للقواعد تتماشى مع طبيعته ولا يمكن بأي شكل من الأشكال إلى القواعد التقليدية، التي تحكم المستندات الورقية وذلك للفرق الشاسع بينهما ومما يشمل هذا البحث أيضا ضوابط التفتيش في حالة وجود إذن التفتيش و الاختصاص للمحاكم والقانون الواجب التطبيق على هذا النوع من الجرائم والتي أدت بالضرورة إلى وجود التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية وذلك نظرا لخطورة هذه الجرائم العابرة لكل الحدود العالمية وضرورة التطور المستمر في النصوص الجزائية الموضوعية والإجرائية مع التطور السريع للجريمة المعلوماتية .

وفي الأخير يبقى مجال البحث في هذا النوع من الدراسات مفتوحا على الدوام نظرا للوتيرة المتسارعة لتطور الجريمة المعلوماتية.

- التوصيات :

- الجهود المبذولة لحماية المستند من طرف المشرع وذلك من خلال:
- تعزيز مستوى الأمان والحماية على المعلومات.
- توفير آلية للتوثيق وتقييد المعلومات ومواكبة متطلبات العصر من سرعة الائتمان.
- تجريم كل الأفعال التي تمس بسلامة وصحة المستند الإلكتروني
- مكافحة الجرائم الماسة بمصادقية التعاملات الإلكترونية عموما وبالوسيلة التي تقوم عليها هذه التعاملات، أي المستند الإلكتروني على وجه الخصوص وإضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.

- النتائج :

- تسهيل عملية المعاملات الإلكترونية والمالية والتجارية وبروز آليات للتداول الإلكتروني.
- تحقق السرعة في المعاملات الإلكترونية الحديثة في سوق الأموال الإلكترونية.
- توفير عنصر الحماية في مجال التعامل المعلوماتي ضمن قواعد الضبط المحدد في مجال الحماية الجنائية للمستند الإلكتروني بتطبيق القانون الواجب على هذه الأفعال.

المراجع

المراجع:

أولا : قائمة الكتب باللغة العربية :

1. أحمد فتحي سرور، الجرائم المضرة بالمصلحة، دار النهضة العربية، 1963.
2. أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، دار النهضة العربية، مصر سنة 2007.
3. أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط1، دار هومة للنشر والتوزيع، الجزائر، 2006.
4. أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، دار الجامعة الجديدة للنشر والتوزيع، ط1، مصر، 2015.
5. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002.
6. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 1992.
7. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، سنة 2000.
8. خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، المركز القومي للإصدارات القانونية، الطبعة الأولى، (د.م.ن)، 2009.
9. خشير مسعود، الحماية الجنائية لبرامج الكمبيوتر ، دار الهدى، الجزائر، 2010.
10. داديار حميد سليمان، دور السندات المستخرجة عن طريق الأنترنت لإثبات المسائل المدنية (دراسة تحليلية مقارنة)، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2010.

11. دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، الجزء 2، ديوان المطبوعات الجزائرية، قسنطينة، 2007.
12. رضا المتولى وهدان، النظام القانوني للعقد الإلكتروني والمسؤولية عن الاعتداءات الإلكترونية، دار الفكر والقانون، المنصورة، ط الأولى، 2013.
13. سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجزائر الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، ب.ط، القاهرة، 2007.
14. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، مصر، دار الجامعة الجديدة، الطبعة الاولى، السنة 2007.
15. عابد فايد عبد الفتاح، الكتابة الإلكترونية في القانون المجني بين التطور القانوني والأمن التقني، دار الجامعة الجديدة، الإسكندرية، 2014.
16. عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2010.
17. عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، آثار الالتزام، الجزء الثاني، دار إحياء التراث العربي بيروت 1952.
18. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية، مصر، 2009.
19. عبد الكريم الطالب، الشرح العلمي لقانون المسطرة الحديثة، المطبعة والوراقة الوطنية مراكش ط 06 افريل 2013 .
20. عمار كريم كاظم و نارمان جميل نعمة، القوة القانونية للمستند الإلكتروني، كلية القانون، جامعة الكوفة، العدد السابع، سنة 2007.
21. فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، 2005.

22. مازن عبد العزيز فاعول، الاعتماد المستندي والتجارة الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط الأولى، 2006
23. محمد الحسين منصور المسؤولية الالكترونية مطبعة سعيد كامل ط 01 مصر 2006.
24. محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، الاسكندرية مصر، المجلة الكبرى، 2008.
25. محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2007.
26. محمد علي سالم جاسم وعباس طالب زروقي، البطاقة الائتمانية والأساس القانوني لحمايتها من التزوير، مجلة المتحقق المحلي للعلوم القانونية والسياسية، ص 7، ع2، 2015.
27. محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، سنة 2013.
28. محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2015.
29. محمود حسني نجيب، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 2013.
30. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، 2001.
31. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، سنة 2001.
32. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، تدعيم الثقة وتأمين للتعامل عبر الانترنت، دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط سلطة عمان، 23 نوفمبر 2008.

33. مصطفى كمال طه ووائل أنور بندق، الاوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، الطبعة الأولى، 2006.

34. نهلا عبد القادر المومني، الجرائم المعلوماتية، الأردن، دار الثقافة، 2008.

35. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 1992.

ثانيا: الكتب باللغة الأجنبية :

1. **Comment, Dit SurlaMowsal Wyer.4vlike.Com**
2. **Donnedieu De Viber**, Lanastion De Fait Intellectuel En Droit Françaises Ce Crime, 1974,
3. **International Council** Archive, 2004.
4. **Public Records** Office, 2004.
5. **WESSELS (Johannes)/ Hettinger (Micheel):StrafrechtBesohdererteil** 1/1999).

ثالثا : الأطروحات والمذكرات

1. **إلهام خليفة**، الحماية الجنائية المحررات الإلكترونية من التزوير ، أطروحة دكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016.
2. **براهيمي حنان**، جريمة التزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة الدكتوراه، تخصص جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015.
3. **تامر محمد سليمان الديماطي**، إثبات التعاقد الإلكتروني عبر الأنترنت، رسالة دكتوراه غير منشورة، جامعة القاهرة، 2008.
4. **حفصي عباس**، جرائم التزوير الإلكترونية (دراسة مقارنة)، دكتوراه في العلوم الإسلامية، جامعة وهران 01، أحمد بن بلة، سنة 2015.

5. صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون الخاص، جامعة تلمسان، 2013.
6. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
7. طباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مذكرة ماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2013.
8. طمين سهيلة، الشكلية في عقود التجارة الإلكترونية، مذكرة ماجستير في القانون، فرع القانون الدولي للأعمال، مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2011.
09. محلول سماح، حجية الوسائل التكنولوجية في إثبات العقود التجارية، مذكرة ماستر في القانون العام للأعمال، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2015.
10. 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.

ثالثا: المجالات

1. أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، (علم مجلة علمية محكمة)، جامعة بني سويف، مصر، العدد السادس عشر (16)، يناير 2016،

2. **براهيمي حنان**، المحررات الإلكترونية كدليل إثبات، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد التاسع، (ب.ت) 2015.
3. **خالد علي العراقي على إسماعيل**، مكافحة جرائم التوقيع الإلكتروني بدولة الإمارات العربية المتحدة، مجلة الفكر الشرطي، مج 22، ع 85، 2013.
4. **رياض السيد حسين أبو سعيد**، توثيق المستند في التعامل الإلكتروني-دراسة تحليلية مقارنة-، مجلة دراسات الكوفة، ع 28، 2013.
5. **مبارك الحسنوي**، مجلة الفقه والقانون، العدد الخامس عشر، ردمد 2336-0615 يناير 2014.

رابعاً: المواقع الإلكترونية

1. **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني -دراسة مقارنة-، بحث منشور على شبكة الانترنت، من خلال الموقع الإلكتروني الآتي: <https://Www.Arabawifo.Com> (الدليل الإلكتروني القانون العربي)، بتاريخ 2007/12/05.

خامساً: الملتقيات والندوات

1. **أسامة أبو حسن**، خصوصية التعاقد عبر الانترنت، -دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر والانترنت"، والذي بمدينة العين، في الفترة من 13 سنة 2000.
2. **حسونة عبد الغني**، جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة، بحث مقدم لأعمال الملتقى الوطني حول الجريمة للمعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر ما بين 16 و 17 نوفمبر 2015.

3. **حسين شحادة حسين**، التوثيق الإلكتروني في الاعتماد المستندي، دراسة قدمت إلى المؤتمر العلمي الثالث للقانونيين المصريين الذي عقدته الجمعية المصرية للاقتصاد السياسية التشريع عن موضوع الجوانب القانونية للعمليات المصرفية، القاهرة، 19-20 ديسمبر 2002.
4. **عبد القادر القهوجي**، الحماية الجنائية للبيانات المعالجة إلكترونياً، دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر والانترنت"، وذلك بفندق هيلتون العين في الفترة من 1-3 مايو سنة 2000.
5. **فشار عطا الله**، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغربي حول القانون والمعلوماتية، بمقر أكاديمية الدراسات العليا بليبيا، في أكتوبر 2009.
6. **فياض مالقي القضاة**: مسؤولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء، دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون، جامعة الإمارة العربية المتحدة في موضوع القانون والكمبيوتر والانترنت والذي عقد بفندق هيانون العين، في الفترة من 1-5 ماي سنة 2000.
- سادسا : القوانين والمراسيم
1. الأمر 85/75 المؤرخ في 26/09/1975، المتضمن التقنين المدني الجزائري المعدل والمتمم بالقانون رقم 10/05 المؤرخ في 20/06/2005، ج.ر رقم 44 الصادرة بتاريخ 2005/06/26.
2. الأمر رقم 66-156 المتضمن قانون العقوبات.

3. الأمر رقم 66-156 المتضمن قانون العقوبات، المؤرخ في 08 يونيو 1966 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.
4. الأمر رقم 75-85 المتضمن القانون المدني.
5. ظهير شريف رقم 129-107، الصادر في 19 من ذي القعدة 1428، الموافق لـ 30 نوفمبر 2007)، بتنفيذ قانون رقم 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.
6. ظهير شريف، رقم 3-44-59-1 بتاريخ 28 جمادى الثانية 1382 (26 نوفمبر 1962 بالمصادقة على مجموعة القانون الجنائي، منشور بالجريدة الرسمية، عدد 2640 مكرر بتاريخ 18 محرم 1303 (05 نوفمبر 1963).
7. العدد 06، 20 الجريدة الرسمية للجمهورية الجزائرية، ربيع الثاني عام 1436هـ/ الموافق لـ 10 فبراير سنة 2018.
8. الفقرة الثانية من المادة 62 من قانون المسطرة الجنائية.
9. قانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر. ج.ج. عدد 06 صادر في 10/02/2015.
10. القانون رقم 66-16 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الصادر في الجريدة الرسمية، العدد 49 المؤرخة في 11-06-1966، المعدل والمتمم بالقانون رقم 16-02 المؤرخ في 19 يونيو 2016، الصادر بالجريدة الرسمية، العدد 37، المؤرخ في 22 يونيو 2016.
11. القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 مايو سنة 2018 المتعلق بالتجارة الإلكترونية (ج.ر.)، العدد 28 المؤرخة في 30 شعبان 1439 الموافق لـ 16 مايو سنة 2018.
12. المادة 01 قانون الأونستيرال النموذجي للتجارة الإلكترونية لسنة 1996، والصادر في جلسة رقم 25 الجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996.

13. المادة 03 من قانون المعاملات السوداني.
14. المادة 108 من قانون المسطرة الجنائية
15. المادة 23 من قانون التوقيع الإلكتروني المصري .
16. المادة 29 من قانون المرافعات المصري.
17. المادة 336 قانون العقوبات المصري.
18. المادة 351 من مجموعة القانون الجنائي المغربي.
19. المادة 4 من القانون الأمريكي الفدرالي.
20. المادة 47 من القانون المدني الفرنسي.
21. المادة الاولى الفقرة "ب" من القانون رقم 15 لسنة 2004 والخاص بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، ج.و، ع 17 الصادرة بتاريخ 2004/04/22، ص 17 وما بعدها.
22. المادة الأولى الفقرة الحادية عشر، المرسوم بقانون اتحادي رقم 05 لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات الإماراتي.
23. المادة الثامنة من قانون 53-05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

الفهرس

الفهرس

✓ اهداء

✓ تشكرات

✓ مقدمة.....أسث

❖ الفصل الأول: ماهية المستند الإلكتروني.....5

• المبحث الأول: مدلول المستند الإلكتروني5-6

- المطلب الأول: مفهوم المستند الإلكتروني.....6

▪ الفرع الأول: تعريف المستند الإلكتروني ونشأته.....6-14

▪ الفرع الثاني: خصائص المستند الإلكتروني وصوره.....14-24

- المطلب الثاني: الطبيعة القانونية للمستند الإلكتروني وتميزه عن ما شابهه.....25

▪ الفرع الأول: الطبيعة القانونية للمستند الإلكتروني.....25-26

▪ الفرع الثاني: تميزه عن ما شابهه.....26-28

• المبحث الثاني: النظام القانوني للمستند الإلكتروني وحجيته في الإثبات.....29

- المطلب الأول: النظام القانوني للمستند الإلكتروني وشروط صحته.....29

▪ الفرع الأول: تنظيم المستندات الإلكترونية.....29-30

▪ الفرع الثاني: شروط صحة المستند الإلكتروني.....30-37

- المطلب الثاني: حجية المستند الإلكتروني في الإثبات.....37-38

▪ الفرع الأول: حجية المستند الإلكتروني في ظل غياب النص.....38-40

▪ الفرع الثاني: حجية المستند الإلكتروني في ظل وجود النص.....41-42

• ملخص الفصل الأول:.....43

❖ الفصل الثاني: الأفعال الماسة بالمستند الإلكتروني.....44

• المبحث الأول: الأفعال الماسة بمحتوى المستند الإلكتروني.....44

- المطلب الأول: جريمة التزوير وجريمة السرقة.....44

▪ الفرع الأول: جريمة التزوير والحماية الجنائية المقررة لها.....45-57

- الفرع الثاني: جريمة السرقة والحماية الجنائية المقرر لها.....65-57
- المطلب الثاني: جريمة الإلتلاف والاحتيال.....65
- الفرع الأول: جريمة الإلتلاف الحماية الجنائية المقرر لها.....65-72
- الفرع الثاني: جريمة الاحتيال الحماية الجنائية المقرر لها.....73-75
- المبحث الثاني: الأفعال الماسة بسرية المستند الإلكتروني وقواعد الضبط في الجرائم المعلوماتية.....76
- المطلب الأول: الأفعال الماسة بسرية المستند الإلكتروني.....76
- الفرع الأول: التشريعات المقارنة في النص على الجرائم الماسة بسرية المستند الإلكتروني.....76-79
- الفرع الثاني: العناصر المشتركة في جرائم المساس بسرية المستند الإلكتروني..79-83
- المطلب الثاني: قواعد الضبط في الجرائم المعلوماتية.....83
- الفرع الأول: القواعد المنظمة للتفتيش.....84
- الفرع الثاني: الاختصاص القضائي والقانون الواجب التطبيق.....91-97
- ملخص الفصل الثاني:.....98
- ❖ الخاتمة.....99-100
- ❖ المراجع101-109
- ❖ الفهرس.....110-111

ملخص المذكرة

من خلال دراسة الحماية الجنائية للمستند الإلكتروني يمكننا أن نستخلص بعض النتائج والتي تتمثل في ما يلي:

1- تناولت التشريعات المقارنة تعريف المستند الإلكتروني باعتباره أهم عنصر تقع عليه الجرائم المعلوماتية.

2- اختلاف الفقه في إعطاء تعريف جامع مانع للمستند الإلكتروني، وهذا راجع للبيئة الإلكترونية التي يتم فيها والوسائل المستعملة في إنشائه واشترطت التشريعات المقارنة لصحة المستند توفر عدة شروط قانونية فيها.

3- نصت التشريعات المقارنة على الحماية الجنائية للمستند وذلك من خلال تجريم الأفعال الماسة لمحتواه ولسريته.

4- لقد كانت الحماية الجنائية مباشرة من خلال تجريم بعض الجرائم مثل جريمة التزوير والاحتيال والإتلاف.

5- ضرورة إنشاء قواعد ضبط محددة في مجال الحماية وتطبيق قانون محدد لهذه الأفعال.

ومن هنا يتضح لنا جليا من خلال هذا العمل المتواضع أن موضوع الحماية الجنائية للمستند الإلكتروني حديث ومهم لذا يجب أن تكون هناك رزمة وجدية وحادثة في إصدار قوانين موحدة ودقيقة لتفعيل الحماية للجرائم المعلوماتية.

الكلمات المفتاحية:

1- المستند الإلكتروني 2- الحماية الجنائية 3- الجرائم المعلوماتية

4- المحرر الإلكتروني 5- الأفعال الماسة بالمستند 6- الكمبيوتر

7- قواعد الضبط في الضبط المعلوماتية 8- الشبكة المعلوماتية