جامعة مولود معمري – تيزي وزو

كلية الحقوق والعلوم السياسية

مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية

حماية وتامين المحررات الالكترونية بين التشريعات الوطنية والدولية

أطروحة لنيل درجة الدكتوراه في القانون

تخصص: قانون

من إعداد الطالب :

بلقاسم عبد الله

تحت إشراف الأستاذة:

أ.د إقلولي/ ولد رابح صافية

لجنة المناقشة:

- صبايحي ربيعة ، أستاذة، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....رئيسا
- إقلولي/ ولد رابح صافية ، أستاذة، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....مشرفة ومقررة
- حساين سامية ، أستاذة، كلية الحقوق، جامعة أمحمد بوقرة، بومرداس.....ممتحنا
- حابت أمال ، أستاذة محاضرة "أ"، كلية الحقوق، جامعة مولود معمري، تيزي وزو.....ممتحنا
- أعمروش أحسن ، أستاذ محاضر "أ"، كلية الحقوق، جامعة جيلالي بونعامة، خميس مليانة...ممتحنا
- حمادي أمال ، أستاذة محاضرة "أ"، كلية الحقوق، جامعة سعد دحلب ، البليدة.....ممتحنا

تاريخ المناقشة:2022/03/10

قائمة أهم المختصرات

أولا: باللغة العربية

ص.ص : من الصفحة إلى الصفحة .

ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية.

ق.إ.ج.ج : قانون الإجراءات الجزائية الجزائري.

ق.ع.ج : قانون العقوبات الجزائري .

ق.ع.م : قانون العقوبات المصري.

ثانيا: باللغة الأجنبية:

Art : Article.

CD : Compact Disc.

C.P.F : Code pénal français

C.P.P.F : Code de procédure pénale français.

C.C.E : Conseil des communautés européennes.

éd : édition.

IP : Internet Protocol.

J.O.R.F : Journal officiel de la république française**.**

Op.cit : Référence Précédemment Cité.

TCP : Transmission Control Protocol.

Tic : Technologies de l'Information et de la Communication.

شكر وتقدير

أتقدم بخالص الشكر والتقدير إلى المشرفة الأستاذة الدكتورة إقلولي/أولد رابح صافية على ما بذلته من جهد مخلص، فقد كانت لتوجيهاتها ونصائحها الأثر في أن تكون هذه الأطروحة بهذه الصورة.

ولا أنسى أن أشكر أعضاء لجنة المناقشة، لتكرمهم بالموافقة على مناقشة هذه الأطروحة.

مقدمة

مقدمة

تعد الثورة التي يشهدها العالم في الوقت الراهن نهضة علمية جديدة في مجال الاتصالات والفضائيات والحاسبات الآلية وتبادل المعلومات عبر شبكة الانترنت، حتى عرف بعصر التكنولوجيا والاتصال عن بعد، بحيث شهد أنماطا جديدة وأشكالا متعددة غير تقليدية في مجال الاتصالات حتى باتت المعلومات تنتقل عبر وسائل الكترونية، وأصبحنا نتعامل مع ما يعرف بالعالم غير الورقي واستبدلت الأوراق أو المحررات الورقية بدعامات غير ورقية، فأصبح الملايين من الأشخاص حول العالم يقومون بإبرام تصرفاتهم القانونية عبر وسائل الاتصال الحديثة، بوصفها اتصالات سريعة وفعالة، أو بعبارة أدق لا وجود لهما بنفس الصورة المتعارف عليها في التعاملات القانونية في صورتها التقليدية، بالتالي أصبحت تمثل واقعا افتراضيا في كافة المجالات، مما منح نمطا جديدا للكتابة والتوقيع اللذان أصبحا يتمان بطريقة إلكترونية سيما أن لهما شروط وخصائص مميزة تفصلهم عن تلك التي تأخذ في الشكل المادي الملموس، فلهذا لم يعد ضروريا أن يتخذ المحرر شكلا ورقيا، وإنما ظهرت أنواع جديدة من المحررات تعتمد أساسا على دعامات غير ورقية، وهو ما يعرف واصطلح على تسميته بالمحررات الإلكترونية، مما استدعى ضرورة إدخال مثل هذه الوسائل في النظام القانوني للدول والاعتراف بها كوسيلة لإبرام التصرفات القانونية والاستناد لها كأدلة إثبات.

تعتبر المحررات الالكترونية عماد أغلب المعاملات والتصرفات القانونية الحديثة، حتى أنها أصبحت حديثا واقعا مفروضا، خاصة مع استخدام المعلوماتية ووسائل الاتصال الحديثة مما أدى إلى ظهور ما يسمى بالجريمة المعلوماتية القائم على أغراض إجرامية خطيرة، واستدعى ذلك وجوب توفير قدر من الحماية والأمن والثقة لأطراف المعاملات الالكترونية، إلى جانب الحفاظ على السرية والخصوصية للمعطيات والمعلومات التي تحملها مراسلاتهم.

على الرغم من الايجابيات التي حملتها المحررات الالكترونية، إلا أنها لا تخلو من بعض السلبيات والمخاطر التي تستهدف جهود عمل المؤسسات والأفراد التي توجهت نحو النموذج

الالكتروني في المعاملات، وتحول دون خلق بيئة آمنة موثوقة لكافة المتعاملين، خاصة مع تنامي الجرائم الالكترونية الواقعة عليها، وهذه الأسباب كفيلة بالبحث عن الحلول القانونية والتقنية الكفيلة بتأمين المحرر الإلكتروني، وذلك بالدفع باتجاه إيجاد بيئة تشريعية جديدة تقوم على تطوير القواعد القانونية التقليدية حتى تتلاءم مع هذه التطورات، أو باستحداث قواعد قانونية جديدة تكفل الحماية القانونية للمتعاملين بالوسائط الالكترونية، كتصد لها من كل أشكال التجاوزات التي قد تحول دون ترقية استعمال هذه الآليات والحد من مساهمتها في تسهيل المبادلات، فوضع المعايير والوسائل التكنولوجية اللازمة للمحررات الالكترونية لتلافي حدوثها وتنظيمها بصورة محكمة، يشجع المعاملات المدنية والتجارية الوطنية منها والدولية، كما تعمل على الحد من النفقات التي تتطلبها التعاملات التقليدية الورقية التي تأخذ الكثير من الوقت والجهد من خلال المعاملات الالكترونية المتميزة بالسرعة.

لاعتبار المحررات الإلكترونية وسيلة إثبات حديثة والاعتراف بها كقوة إثبات كاملة، لابد من إضفاء الحجية القانونية لها وجعلها معادلة في حجيتها للمحررات الورقية بنوعيها العرفية والرسمية طالما أنها ستؤدي ذات الغرض وتحقق نفس الدرجة والثقة والأمان، فالمساواة بين المحررات الورقية والمحررات الإلكترونية يؤدي إلى نشوب نزاع بين أطراف العلاقة القانونية، بالتالي لا بد من إيجاد آليات قانونية لضمان الأمن القانوني للمحررات الإلكترونية، خاصة فيما يتعلق بسلامتها من حيث مضمونها ودقة نسبتها إلى من صدرت منه وكيفية حفظها عبر وسائل الاتصال الحديثة، من حيث مضمون البيانات والمعلومات الواردة فيه دون تعرضها لأي نسخ أو تعديل غير مشروع للبيانات والمعلومات التي يتضمنها، بالإضافة إلى حفظها من التلف والزوال سواء بفعل الإنسان أو بفعل الزمن عن طريق إيجاد أنظمة خاصة لتخزينها وأرشفتها، وإمكانية استرجاعها والرجوع إليها وفي أي وقت، وهذا بالشكل الذي تم إنشائها دون تلف أو تعديل في البيانات المدونة عليها وذلك حتى يمكن الاحتجاج بهذه المحررات الإلكترونية المحفوظة.

تحظى المحررات الإلكترونية بالكثير من المزايا والتي من خلالها عرف ازديادا وانتشارا واسعا في الاستخدام فهو يمتد ليشمل الدولة والأفراد على حد سواء، فحماية هذه الأخيرة مكن التجارة الإلكترونية من تحقيق أهدافها التي تتطلب أساسا السرعة والائتمان في إنجازها، بالإضافة إلى تكفلها بضمان تحقيق الاستقرار والأمان في المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام والتي تصدرها هذه الجهات الحكومية. ففي ضل تعاظم استخدام المحررات الإلكترونية في أغلب التعاملات الإلكترونية وكمظهر من مظاهر إساءة استخدام تقنية المعلومات والاتصالات ظهرت الجرائم الإلكترونية التي تختلف طبيعة ومضمونا عن الجرائم التقليدية مما جعل النظم والقوانين الحالية غير كافية لمواجهة هذه الجرائم سواء في مجالات التجريم أو العقاب أو الوقاية، في ضل الاستفادة من تقنية المعلومات وبين إساءة استخدامها.

يصعب تحديد الجرائم الالكترونية وتصنيفها وذلك نظرا لتعقيد إجراءات الادعاء فيها أمام القضاء، مما ساعد مرتكبو الجرائم الإلكترونية في استغلال ذلك في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة بل تجاوزت حدود الدول وهي جرائم مبتكرة ومستحدثة لم يكن لها مجال ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية فالجريمة الالكترونية بطبيعتها جريمة معقدة لأن أداتها جهاز الحاسب الآلي وملحقاته العديدة ولغاته وبرامجه التي لا يفهمها إلى القلة من الخبراء والمختصين، بالتالي كان لا بد من إعادة النظر في الكثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة استيعاب هذه الظاهرة الإجرامية الجديدة، مما يستوجب تطوير البنية التشريعية الجنائية الوطنية بشكل يضمن احترام مبدأ شرعية الجرائم والعقوبات من جهة، ومبدأ الشرعية الإجرائية من جهة أخرى، خاصة حول تكييف الجرائم الماسة بالمحررات الإلكترونية، من حيث مدى إخضاعها إلى النصوص التقليدية، أو استحداث نصوص عقابية خاصة، بالنظر إلى الطبيعة الخاصة التي تتميز بها جرائم المحررات الإلكترونية، لأن هذا النوع المستحدث من الإجرام نشاطه من التطور الذي عرفته وسائل الاتصال الحديثة، وخاصة ظهور وانتشار جهاز الحاسب الآلي وشبكة الإنترنت والذي ساعد كثيرا في سهولة الولوج إلى البيانات والمعلومات التي يتضمنها

نظام الحاسب الآلي، والذي من خلاله أتاح عن طريق ربطه بشبكة الإنترنت الدخول إلى العديد من المواقع الإلكترونية، مما أحدث نموا هائلا في حجم المعلومات المتاحة، لكن بالمقابل قد تكون هذه الوسائل المتاحة عرضة لإساءة استعمالها واستغلالها واستخدامها، على نحو غير مشروع من قبل بعض المجرمين مسببة أضرارا للمصالح المشروعة، بحيث أضحت أداة تستخدم في ارتكاب الجرائم الإلكترونية، فجرائم المساس بالمحررات الإلكترونية تواجه تحديات قانونية تستلزم التنظيم القانوني لها، وذلك للتصدي لمثل هذه الأساليب المستحدثة والمستخدمة في التعدي والمساس بها.

فتطبيق القانون الجنائي الإجرائي على جرائم المحررات الإلكترونية يمكن أن يثير صعوبات إجرائية، تكمن أساسا حول تطبيق الإجراءات التقليدية، سيما وأنها تتعلق ببيانات معالجة إلكترونية وكيانات غير ملموسة، فالأساليب المستحدثة المستخدمة في إثبات الجرائم الماسة بالمحررات الإلكترونية وتحديد هوية مرتكبيها تعتبر ذات فاعلية في التحقيق الجنائي، بالتالي أصبحت واقعا مفروضا، فازدياد استخدام المعلوماتية ووسائل الاتصال الحديثة أدى إلى تعرض المحررات الالكترونية إلى مخاطر جسيمة بفعل هذا النوع المستحدث من الجرائم، بالتالي يفرض الواقع العملي على الدول تبني سياسة جنائية جديدة تتواءم مع هذا النمط المستحدث من الإجرام، عن طريق إما إدخال تعديلات جزئية في التشريعات الجنائية القائمة بما يكفل توفير الحماية لها وذلك بتحديث وتطويع النصوص التشريعية بالكيفية التي تكفل هذه الحماية، أو عن طريق سن تشريعات خاصة، تقوم على هدف محدد وهو مواجهته مواجهة موضوعية إجرائية، سعيا منها لإضفاء نوع من الأمان والثقة في التعامل بهذا النوع المستحدث من المحررات، فوضع الثقة في الوسائل التقنية يجعل من الصعب بلوغ هذا الهدف، فالخصائص التي تتميز بها جرائم المحررات الإلكترونية تعد عائقا حقيقيا أمام جهات التحقيق في التوصل إلى ضبط الدليل الإلكتروني وإثبات هذا النوع من الجرائم، وذلك في كونها جريمة لا تتقيد بمكان وزمان محددين، بالإضافة إلى السرعة في تنفيذها وإتلاف الأدلة وسهولة إخفاء وطمس معالم الجريمة وآثارها، خاصة الأدلة التي تدل على مرتكبيها من

حيث أنهم في الغالب أشخاص ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي.

يعد الدليل الإلكتروني في وقتنا الحاضر من الأدلة التي يعتد بها في الإثبات الجنائي، فقد حظي باهتمام كبير من قبل فقهاء القانون وذلك باعتباره الدليل الأفضل لإثبات هذا النوع المستحدث من الجرائم خاصة جرائم المحررات الإلكترونية، لأنه من طبيعة الوسط الذي ارتكبت فيه الجريمة، فالأدلة الجنائية الالكترونية تشمل جميع البيانات الرقمية التي يمكن استخدامها في أي مرحلة من مراحل الدعوى الجنائية لإثبات حقيقة أن هناك جريمة قد ارتكبت.

من خلال موضوع البحث سنحاول الإجابة على الإشكالية والتي مفادها: **ما مدى فاعلية الآليات القانونية التي اعتمدتها التشريعات الوطنية والمواثيق الدولية في ضمان الأمن القانوني للمحررات الإلكترونية ؟.**

للإجابة على الإشكالية ومن خلال ما سبق سنخصص **(الباب الأول)** للمحررات الإلكترونية محل الحماية من خلال بيان الطبيعة الخاصة للمحررات الإلكترونية من حيث ماهيتها،عناصرها،أهميتها، تطبيقاتها ومن حيث تأمين سلامتها، لنتناول في **(الباب الثاني)** الحماية الجنائية الموضوعية والإجرائية لها، ونظرا للطبيعة الخاصة التي تتميز بها المحررات الإلكترونية فقد اعتمدنا على المنهج الوصفي في تبيان الطبيعة الخاصة للمحررات الإلكترونية، وكذا الاعتماد على المنهج التحليلي من خلال تحليل النصوص القانونية والتنظيمية التي جاءت بها التشريعات التي عالجت هذا النوع المستحدث من المحررات سواء التي قامت بتعديل التشريعات القائمة لتتلاءم مع حجيتها في الإثبات والاعتراف بها ومساواتها بالمحررات التقليدية عن طريق تكريس مبدأ التعادل الوظيفي، أو التي وضعت نصوص خاصة عن طريق وضع نظام قانوني يتصدى لكل العوائق التشريعية والتقنية في ضمان سلامة المحرر الالكتروني، وفي حمايته جنائيا سواء حماية جنائية موضوعية أو حماية جنائية إجرائية.

الباب الأول

المحرر الإلكتروني محل الحماية

الباب الأول
المحرر الإلكتروني محل الحماية

يشهد العالم في الوقت الحاضر تطورا كبيرا في شتى مجالات الحياة، ومع التطور التكنولوجي في وسائل الاتصال الحديث أوجد العلم ما يسمى بالرسائل والبيانات والمعلومات المتبادلة الكترونيا والتي بدأت بالفاكس والتلكس، إلى غاية ظهور الحاسوب وشبكة الانترنت والتي أصبحت أغلب هذه المراسلات والتعاقدات تتم عن طريق هذه الشبكة، وهو ما يعرف بالمحررات الالكترونية والتي فرضت نفسها في المعاملات الالكترونية في الوقت الحاضر، بالإضافة إلى تمتعها بثقة المتعاملين بها نظرا أنه يمكن الرجوع إليها في أي وقت وفي أي مكان بدون مشقة أو عناء، وذلك لسهولة الاطلاع عليها عن طريق أجهزة ووسائل الاتصال الحديثة خاصة جهاز الحاسب الآلي وشبكة الانترنت، ونسبتها إلى موقعها من خلال التوقيع الالكتروني حتى أصبحت لها تأثير واضح على طبيعة المعاملات، فالمحرر الالكتروني يحتوي على كتابة لها قيمة قانونية تصلح للتمسك أو للاحتجاج بها، لكن هذه الكتابة لا بد من اقترانها بالتوقيع الإلكتروني حتى يعتد بها في الإثبات، والذي يعني وجود تكامل بين البيانات المتعلقة بالتوقيع الإلكتروني فأي تغيير أو تعديل يمس المحرر الإلكتروني بعد توقيعه يعد قابلا للكشف، فلا بد من سلامة المعلومات والبيانات الواردة فيه دون أن يلحقها أي تغيير في شكلها الأصلي الذي نشأت به، ويتم الاحتفاظ بها عن طريق حفظها وتخزينها بحيث يمكن استخدامها والرجوع إليها عند الحاجة، وتختلف الكتابة باختلاف الجهة التي تقوم بتحرير المحرر الإلكتروني، فهناك محررات رسمية والتي تصدر عن موظف عام أو شخص مكلف بخدمة عامة وأخرى عرفية وهي التي يتم تحريرها بمعرفة أطرافها وهي على نوعين محررات معدة للإثبات وهي معدة مسبقا لتكون أدلة إثبات فيما قد يثور بينهم من نزاع، ومحررات غير معدة للإثبات أي لم يقصد حين تحريرها استعمالها في الإثبات.

تتميز المحررات الالكترونية كثيرا وتختلف اختلافا جوهريا عن المحررات الورقية التقليدية، سواء من حيث الوسائط أو الدعائم التي تنظم هذه المحررات، أو من حيث إنشائها

تبادلها تخزينها وتوقيعها، حتى أصبحت حقيقة قائمة يستحيل تجاهلها في إبرام التصرفات القانونية مما أحدث فجوة بين الواقع الملموس والقواعد المنظمة لأدلة الإثبات في القانون المدني التي لا تعرف سوى المحررات الورقية، مما أدى بأغلب التشريعات المقارنة إلى الإقرار بصحة المحررات المدونة على الوسائط الإلكترونية ومنحها حجية في الإثبات مساوية لتلك الحجية المقررة للمحررات المدونة على الورق، ولكي يتمتع المحرر الالكتروني بهذه الحجية وإمكانية مساواته بالمحرر الورقي، لابد من أن يتوفر على شروط أساسية حددتها كل من التشريعات الوطنية والدولية، كشرط أن يكون قابلا للقراءة والإدراك بمعنى أي شخص بإمكانه قراءة مضمونه، ويكون المضمون مفهوما للجميع ولا يكون فيه أي تغيير حتى بعد فترة زمنية معتبرة، وأن تكون الدعامة التي يتم بها كتابة المحررات الالكترونية موجودة ومحفوظة بشكل جيد وصالحة للقراءة، فالمحرر الإلكتروني من حيث وظيفته يمكن اعتباره حجة في الإثبات لقيامه بنفس وظائف المحرر التقليدي، وهي تحديد هوية الموقع وإظهار موافقته على الالتزام بمضمون المحرر الذي قام بتوقيعه، وقابلية المحرر الإلكتروني للاحتفاظ به بشكله الأصلي الذي نشأ به والمتفق عليه بين أطراف العلاقة، وحتى يتحقق هذا لا بد من ضمان سلامته بأعلى درجات الثقة والأمان، فلا بد من أن تتم كتابة المحرر الالكتروني والتوقيع عليه باستعمال وسائل ونظم من شأنها الحفاظ على سلامته، والتي تعتبر ضوابط تقنية وقانونية يفترض على التشريعات المقارنة تبنيها وتنظيم جزئياتها، وذلك لتوفير حماية قانونية لهذا النوع المستجد من المحررات، كأنظمة التشفير والتصديق الالكتروني، بالتالي سنتناول أولا الطبيعة الخاصة للمحررات الإلكترونية من خلال تحديد ماهيتها وعناصرها في **(الفصل الأول)**، لنتناول ضمان سلامة المحررات الإلكترونية من حيث حفظها و ضمان الأمن القانوني لها **(الفصل الثاني)**.

الفصل الأول

الطبيعة الخاصة للمحررات الإلكترونية

أدى التقدم التكنولوجي وثورة المعلومات والاتصالات خاصة مع ظهور الانترنت إلى إحداث تطور في النصوص والمصطلحات القانونية المختلفة، سواء أكانت في نطاق القانون المدني أو التجاري أو في قوانين أخرى، مما أدى إلى تغيير في المفاهيم الأساسية للآليات المستحدثة في وسائل الاتصال الحديثة التي نتجت عنها ما يسمى بالمحررات الإلكترونية، فهذه المحررات امتدت لتشمل جميع فروع القانون، وفي إطار ذلك سارعت بعض التشريعات إلى استيعاب هذه الوسائل التكنولوجية الحديثة ومرجعيتها الأولية كانت قوانين الأونسترال النموذجي للتجارة الإلكترونية ثم تلاه بعد ذلك القانون النموذجي للتوقيع الإلكتروني، حيث أصدرت لجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة قانون الأونسترال النموذجي ودعت الدول إلى تنظيم قوانينها الداخلية لمثل هذه الوسائل، وضمن هذا التوجه حاولت العديد من التشريعات الوطنية والدولية ضبط ومعالجة المسائل القانونية التي أثارتها هذه المسائل، ونظرا لحداثة مصطلح المحررات الالكترونية فإن أغلب التشريعات المقارنة رغم اختلافها من حيث التسمية ومن حيث سياق التعريف، إلا أنها تتفق من حيث تحديد المعنى والمضمون والهدف الذي تسعى إليه، ورغم اختلاف الفقه حول هذه التسميات إلا أن الدلالة والمعنى المقصود هو واحد طالما كان المقصود بالمحرر الإلكتروني هو الشكل الرقمي أو الإلكتروني، إذ أن أغلبها اعترفت بالمحررات الالكترونية وذلك لإثبات التصرفات القانونية التي تتم عبر وسائل الاتصال الحديثة، مهما كانت طريق إنشائها، ما دام أن المحرر تتوافر فيه الشروط التي تمنح له السرية والأمن القانوني، فاعتمدت أغلبها على مبدأ مهم وهو مبدأ التكافؤ الوظيفي، والذي كان مفاده ضرورة النظر إلى المحررات الإلكترونية على قدم المساواة مع المحررات الورقية من ناحية حجيتها في الإثبات وعدم التمييز بينها رغم اختلاف الدعامات التي تدون عليها، لكن بالمقابل وضعت حدودا وشروطا لهذا الاعتراف، وذلك عن طريق توفير ضمانات معينة في المحرر الإلكتروني مشابهة لما توفره الدعامة الورقية من درجات الأمان، والتي من شأنها النهوض بها إلى مستوى المحرر الورقي، بحيث أصبحت أهم وسيلة لإثبات التصرفات التي تتم بوسائل

التكنولوجيا الحديثة، وهذا يحيلنا إلى أهمية المحررات الإلكترونية بحيث تعتبر وسيلة تطبيق ما يسمى حاليا بالإدارة الإلكترونية الرامية إلى تيسير التعامل مع الأجهزة الحكومية والقضاء على البيروقراطية الإدارية، كما أنها إحدى التطبيقات التي تقوم عليها التجارة الإلكترونية، بالإضافة إلى اعتبارها عماد الأعمال المصرفية الحديثة، إلى غير ذلك من الأهمية والدور الوظيفي لها في أغلب المعاملات سواء على صعيد الدولة الواحدة أم على الصعيد الدولي، ولفهم الطبيعة الخاصة للمحررات الالكترونية سنحاول التطرق إلى تحديد ماهية المحررات الإلكترونية وهذا في **(المبحث الأول)**، ثم بعد ذلك نتناول عناصر المحررات الإلكترونية في **(المبحث الثاني)**.

المبحث الأول

ماهية المحرر الالكتروني

لم تعد فكرة المحرر الالكتروني التي ارتبطت في أذهاننا بالورقة المكتوبة تقتصر على مفهومها التقليدي السائد، بل حتى أنه لا يوجد في الأصل اللغوي لهذه الكلمة ما يقصر معناها على ما هو مكتوب على نوع معين من الدعامات سواء أكانت ورقا أم غير ذلك، ومن ثم نستطيع أن نقول أن كلمة محرر بهذا المعنى تشمل المحرر الورقي والإلكتروني على حد سواء[1]، فهي محررات فرضت نفسها لما لها من تأثير واضح على طبيعة المعاملات التي تتم عن طريق وسائل الاتصال الحديثة، أما الاختلاف الجوهري والأساسي بين المحرر الالكتروني والمحرر الورقي فهو يكمن في الدعامة التي يكون عليها كل واحد منهم ، فالمحرر الورقي دعامته ورق ملموس على خلاف المحرر الالكتروني والذي ترجع دعامته إلى برامج الكمبيوتر أو أية وسائط تقنية .

فلتحديد ماهية المحرر الالكتروني لابد من تحديد مفهومه وذلك بالرجوع إلى تعريف الفقه من جهة والتشريعات الدولية والوطنية من جهة أخرى، وتحديد أهميتها ومجالات تطبيقها والذي سنتناوله بشيء من التفصيل في **(المطلب الأول)**، ثم تحديد أنواع المحررات الإلكترونية في **(المطلب الثاني)**.

[1] ـ سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دار الكتب القانونية، مصر، 2008، ص.497. محمد السعيد رشدي، التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، منشأة المعارف، الإسكندرية، 2008، ص.16.

المطلب الأول

مفهوم المحرر الالكتروني

أثار المحرر الالكتروني خلافا حول تسميته وسياق تعريفه، إلا أنها بالمقابل توافقت في المضمون والغاية التي تسعى إليه، ومما تجدر الإشارة إليه بأنه هناك نوع من المخرجات المعلوماتية التي تتفق مع المحررات التقليدية، مثال ذلك المخرجات الورقية التي تأخذ شكل فواتير أو شيكات أو تقارير تنتج من النظام المعلوماتي في صورة محررات تقليدية، ونوع آخر من المخرجات المعلوماتية التي يطلق عليها بعضهم اسم المخرجات اللاورقية أو الالكترونية، وتعتبر أوعية للمعلومات كالأشرطة والاسطوانات والأقراص الممغنطة والمصغرات الفيلمية، إلى غير ذلك من الأشكال غير التقليدية للتكنولوجيا التي تتوافر عن طريق الوصول المباشر، حيث يقوم المستخدم بإدخال البيانات منها ويحصل على المخرجات في نفس الوقت، ويتم من خلالها التعامل مع النظام المعلوماتي[1]، وتبعا لذلك فقد أقرت أغلب التشريعات مبدأ المساواة بين المحررات الإلكترونية ونظيرتها الورقية، من حيث الآثار القانونية وحجيتها في الإثبات متى استوفت الشروط القانونية والضوابط الفنية، التي تكفل التعامل بهذا النوع المستحدث بكل ثقة وأمان، سيما أن توفير الاطمئنان اللازم للتعاملات الإلكترونية عن طريق حماية وتأمين المحررات الإلكترونية تمكن من إنجاح فكرة التجارة الإلكترونية، بكل ما تقتضيها من إنجاز للمعاملات وإبرام للتصرفات بكل سرعة وائتمان، كما تمكن أيضا من تجسيد تنفيذ فكرة الحكومة الالكترونية والتي تعتمد أساسا على تقديم الخدمات ذات الطابع الإداري بكل سرعة وبأقل جهد وتكلفة ممكنة، بالتالي من خلال هذا المطلب سنتعرض أولا إلى تعريف المحرر الإلكتروني في **(الفرع الأول)**، لنتناول بعد ذلك أهميتها وتطبيقاتها في **(الفرع الثاني)**.

[1] ـ هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1999، ص.16.

الفرع الأول

تعريف المحرر الإلكتروني

وضع الفقه القانوني عدة تعاريف للمحرر الإلكتروني، تضمنت أغلبها الاعتبارات الأساسية لتعريف أي محرر مع مراعاة خصوصيته كونه يبرم عن طريق شبكة الإنترنت، ونظرا لكثرة التعاملات الإلكترونية في الآونة الأخيرة وما أثارته من إشكالات قانونية، فقد حظيت باهتمام تشريعي حيث أصدرت بعض الدول تشريعات قانونية لمعالجة ذلك، وقد ارتأينا أن نتناول التعريف الفقهي للمحررات الالكترونية **(أولا)**، ثم التعريف القانوني لها**(ثانيا)** وذلك على النحو التالي :

أولا: التعريف الفقهي للمحرر الالكتروني

عرف جانب من الفقه المحرر الالكتروني بأنه **:" تلك المعلومات الالكترونية التي ترسل أو تسلم بوسائل إلكترونية أيا كانت وسيلة استخراجها في المكان المستلمة فيه"**[1] .

يؤخذ على هذا التعريف أنه ينطبق على الرسالة الالكترونية، وليس على المحرر الالكتروني، فالرسالة الالكترونية تشكل جزء من المحرر الالكتروني، بالإضافة إلى التوقيع فيجب ذكر الشخص الذي قام بالتوقيع عليها وبيان العناصر الأخرى التي تتكون منها المحررات الالكترونية عامة، لذا فلا يصح أن نعرف الكل بذكر فقط أحد أجزائه.

عرفه جانب آخر من الفقه بأنه **:" كل ما هو مكتوب على نوع معين من الدعامات[2] سواء كان ورقيا أم غير ذلك من الوسائل الالكترونية، يمكن أن يدون عليها شيء معنوي، ويقصد**

[1] - مشار إليه لدى: لورنس محمد عبيدات، إثبات المحرر الالكتروني، دار الثقافة ، ط2،عمان، 2005، ص. 78.

[2]- تختلف الدعامة في المحررات الالكترونية بحسب الوسيط الموجود عليه المحرر الالكتروني، فإذا كان المحرر الالكتروني موجودا على قرص مرن، فإن الدعامة هنا تكون عبارة عن قطعة مرنة من البلاستيك الرقيق مغطاة بمادة سريعة ممغنطة، ويتم الكتابة على القرص المرن بطريقة مغناطيسية ، وإذا كان المحرر الالكتروني موجودا على قرص ضوئي، فان الدعامة تكون عبارة عن مادة من البلاستيك مغطاة بطبقة من مواد خاصة ،يمكن كتابة وقراءة البيانات عليها بأشعة الليزر، أما إذا كان المحرر الالكتروني موجودا على القرص الصلب الخاص بالحاسب الآلي، فإن الدعامة هنا هي بمثابة قرص معدني رقيق مغطى بمادة قابلة للمغنطة، وفي هذه الحالة يتم الكتابة عليه في شكل ممغنط: للمزيد راجع في ذلك: سامح عبد الواحد التهامي ، مرجع سابق، ص.512. سامي جلال الفقي، الأدلة

بالمحرر في مجال المعلوماتية كل شيء مادي متميز (قرص، أو شريط ممغنط) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة ، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة وتم تصنيفه أو تخزينه أو أنه ما زال بداخلها انتظارا لاستخراجه أو تعديله[1].

يلاحظ أن هذا التعريف لم يقدم تعريفا للمحررات الالكترونية وإنما عرف الدعامة المادية التي يتم عليها تخزين أو حفظ الكتابة الالكترونية ذاتها، فهذا الجانب الفقهي استند في تعريفه إلى الطبيعة المادية للمحررات الالكترونية، وبالتالي هذا التعريف نراه من جانبنا ناقص من حيث دلالته.

عرفه جانب آخر من الفقه بأنه **: " البيانات المخزنة على أي وسيط أو في جهاز كمبيوتر أو أي جهاز مماثل، ويمكن أن تقرأ أو تفهم من طرف أي من هذه الوسائل أو من طرف شخص ،ويشار أيضا إلى التمثيل الافتراضي أو طباعة البيانات"**[2].

كما عرفه آخرون بأنه: **"عبارة عن رسالة إلكترونية موثقة وموقعة ترسل من مصدر المحرر إلى مستلم المحرر ليعتمد، ويتم تقديمه إلى الجهة المعتمدة عبر الانترنت"**[3].

يلاحظ أن هذا التعريف قدم تعريفا موسعا للمحرر الالكتروني بحيث أنه لم يحصره بشبكة الانترنت، لكنه لم يحدد الوسيلة الالكترونية التي يتم استخراج أو إرسال أو تسلم تلك الرسائل.

المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، القاهرة، 2001، ص.61.عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، ص27. عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، بيروت، 2010، ص.40.

[1] - عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية،2004، ص.151.

[2] - « ***document électronique» Données mises en mémoire sur quelque support que ce soit par un ordinateur ou un dispositif semblable et qui peuvent être lues ou comprises par un de ces moyens ou par une personne. Est également visée la représentation virtuelle ou imprimée de ces données***».
« Données » Toute forme de représentation d'informations ou de concepts, SEDALLIAN Valérie, Preuve et signature électronique, article disponible sur le site : www.juriscom.net/chr/2/fr20000509.htm.

[3] - مشار إليه لدى: فضالة حسن موسى، التنظيم القانوني للإثبات الالكتروني، دار السنهوري، بيروت، 2016، ص.26 .

يمكن من خلال هذه التعريفات الفقهية أن نقول بأن المحررات الالكترونية هي كل بيان على شكل كتابة، أو صورة أو صوت يتم إنشاؤه أو إرساله أو تسلمه أو خزنه، أو تجهيزه بوسائط إلكترونية والتي هي وسائط الإعلان والتعاقد والوفاء بالالتزامات التي تعتمد على وسائل إلكترونية صوتية، ضوئية، أو أية وسيلة مشابهة بما في ذلك الحاسب الآلي والبرق والتلكس والنسخ البرقي والفاكس، والهاتف، وتعطي دلالة قابلة للإدراك على مضمونها وأي شخص قام بالتوقيع عليها وتكون مثبتة على دعامة غير ورقية.

ثانيا: تعريف المحرر الالكتروني في المواثيق الدولية و التشريعات الوطنية

أثارت التشريعات المتعلقة بالمحرر الالكتروني ولا تزال تثير إشكالات عديدة، بالرغم من إقرار عدد منها منذ سنوات في كثير من الدول، فالمناقشات في هذا الموضوع لا تزال تغني البحث وتسهم في توضيح كيفية تطبيق النصوص والممارسات والآليات التقنية لا سيما بعد اختبارها، كما تسهم في تعديلها وتطورها في أحيان كثيرة، فأصبحت المراسلات والتعاقدات تتم في الغالب عن طريق شبكة الانترنت، بحيث أنها لا تتماشى إطلاقا مع متطلبات العصر الالكتروني الحديث، وتولت مجموعة من التشريعات الدولية والوطنية تحديد معنى المحرر الالكتروني مراعية البيئة والوسائل التي يحرر بها.

1 ـ التعريف الوارد في المواثيق الدولية:

برزت الحاجة أمام التطور التكنولوجي في وسائل الاتصال الحديثة لدى العديد من الدول لمجارات هذه التطورات في تشريعها، إلى ظهور جهود تشريعية دولية لقبول هذه الوسائل الحديثة في قواعد الإثبات، بالتالي وضعت أحكاما قانونية تنظم بها المعاملات الالكترونية بصورة عامة و المحررات الالكترونية بصورة خاصة، ويظهر ذلك أساسا من خلال إصدار قانون الأونسترال النموذجي بشأن التجارة الالكترونية والقانون النموذجي بشأن التوقيعات الالكترونية الصادران عن لجنة الأمم المتحدة للقانون التجاري الدولي، واللذان وضعا الإطار الرئيسي للدول من أجل إصدار قوانين تعطي المحررات الالكترونية الحجية الكاملة في الإثبات وإمكانية مساواتها بالمحررات التقليدية.

أ ـ تعريف المحرر الالكتروني في القانون النموذجي للأمم المتحدة بشأن التجارة الإلكترونية:

عرفه قانون الأونسترال الخاص بالتجارة الالكترونية الذي أعدته لجنة القانون التجاري الدولي التابعة للأمم المتحدة لسنة 1996، في المادة 02 منه تحت مسمى رسالة البيانات بأنه: **"المعلومات التي يتم إنشائها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني ، أو البرق ، أو التلكس أو النسخ البرقي"**[1] .

نص أيضا في المادة 1/11منه على أن هذه الوسائل هي وسيلة تعبير عن العرض والقبول، إذ نصت في سياق تكوين العقود وما لم يتفق الطرفان على غير ذلك يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند استخدام رسالة بيانات في تكوين العقد لا يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك الغرض[2].

اعتبر رسالة البيانات عبارة عن معلومات لكونها تحمل معنى معين، كما أنه استخدم مصطلح رسالة البيانات وذلك لاختلاف البيئة التي يتم تداول هذا المحرر فيها ، فهي بيئة غير ورقية تعتمد على وسائل الكترونية أو ضوئية أو وسائل مشابهة، حيث لم يتم حصر هذه الأشكال حتى يتم استيعاب كل وسيلة جديدة قد تفرزها التكنولوجيا.

ب ـ تعريف منظمة المواصفات العالمية للمحرر الالكتروني (IS0) :

أكدت منظمة المواصفات العالمية **(ISO)** بخصوص المواصفات الخاصة بالمحررات أن المحرر هو:**"مجموعة المعلومات والبيانات المدونة على دعامة مادية...بالشكل الذي يسهل قراءته"**.[3]

---

[1] - المادة 2/أ من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 12ديسمبر2001، متوفر عبر الموقع المنشور باللغتين العربية والانجليزية على الموقع:

http://www.uncitral.org.stabl/ml-elecsig-a.pdf

[2] - المادة 1/11 من قانون الأونسترال السالف الذكر.

[3] - « International Organization for Standardization» وهي اتحاد عالمي مقره في جنيف ويضم في عضويته أكثر من 90 هيئة تقيس وطنية، جاء اختصارها (ISO) اعتمادا على الكلمة اليونانية (ISOS) ، فهي سلسلة من المواصفات والمقاييس المعتمدة عالميا

2 ـ تعريف المحرر الالكتروني في التشريعات الوطنية:

خضع تعريف المحرر الالكتروني في التشريعات الوطنية المختلفة إلى محاولة تعديل بعض المفاهيم في نظمها القانونية المختلفة في ضل تقنية المعلومات وتحدياتها، على اعتبار أن المفاهيم القائمة في نطاق هذه التشريعات عموما تتعامل مع مفاهيم ذات مدلول مادي من كتابة وتوقيع، فلم يكن أمام هذه التشريعات إلا أن تتدخل لتعديل هذه المفاهيم بشكل يجعلها تستوعب هذا النوع من المحررات، و يعد التشريع الفرنسي من المناهج التي اعتبرت نموذجا في بيان معنى المحرر الالكتروني مقارنة بالنماذج الأخرى الغربية، على غرار التشريعات العربية التي لم يرد للمحرر الإلكتروني تعريف واحد وموحد في قوانينها، ولكن وردت تعريفات متشابهة مرتكزة في غالبيتها على التعريف الذي ورد في القانون النموذجي الأونسترال، واستجابة منها للواقع الإلكتروني والتكنولوجي أصدرت مجموعة تشريعات تواكب هذه التطورات فاعترفت بالمحرر الإلكتروني كدليل للإثبات وحاولت تقديم تعريف للمحرر الإلكتروني ومن بينها: التشريع المصري والأردني والتونسي التي تعتبر أيضا السباقة في تنظيم التعامل بهذا المحرر وبيان معناه.

أ ـ القانون الفرنسي :

أجرى المشرع الفرنسي تعديلات على التقنين المدني حتى يمكنه استيعاب المحرر الالكتروني في نصوصه، فقد عدل المادة 1316 من هذا القانون والتي تتضمن تعريف الكتابة على نحو يشمل كل تدوين للحروف أو العلامات أو الأرقام أو أي إشارات أو رموز أخرى ذات دلالة تعبيرية مفهومة لآخرين أيا كان نوع الوسيط أو الدعامة التي تقع عليه ، وأيا كانت طريقة نقلها.

وتستخدم في توكيد جودة العمليات والنشاطات في المؤسسات، ويرمز الرقم 9000 لسلطة المواصفات التي تختص بإدارة الجودة في المؤسسات المختلفة، والتي قد تكون مصنع، أو بنك، أو مستشفى، أو مدرسة، أو عيادة طبيب أو أي شيء آخر، هذه المواصفات تقدم الشهادة على ممارستك لنظام إدارة الجودة والذي يطبق على العمليات والأنشطة المختلفة في المؤسسة، وليس على المنتج أو الخدمة نفسها، مشار إليه لدى: صفاء فتوح جمعة، العقد الإداري الإلكتروني، دار الفكر والقانون، المنصورة، 2014، ص.127.

نص في المادة **1316** فقرة **3** (مدني معدلة) " **أن الكتابة على دعامة إلكترونية لها نفس القوة في الإثبات المقررة للكتابة على دعامة ورقية** "، كذلك المادة **1316** فقرة **1** مدني معدلة من نفس القانون[1]، حيث نصت على أن " **الكتابة الإلكترونية مقبولة في الإثبات كدليل كتابي على الورق، شرط أن تكون منسوبة إلى صاحبها ودالة على شخصيته**"[2].

أعطى المشرع الفرنسي لمفهوم المحرر الالكتروني تعريفا موسعا بحيث أنه لم يحصر الكتابة في دعامة معينة أو في شكل إرسالها، بمعنى أنه لم يميز بين أنواع الكتابة على أساس الدعامة التي تقوم عليها.

ب ـ القانون الأردني:

عرف المحرر الالكتروني في قانون المعاملات الالكترونية الأردني 15لسنة 2015 من خلال المادة الثانية منه على أنه: **"المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بأي وسيلة إلكترونية ومنها البريد الإلكتروني أو الرسائل القصيرة أو أي تبادل للمعلومات إلكترونيا"**[3].

نلاحظ أن المشرع الأردني قد اخذ بنفس التعريف الذي قدمه القانون النموذجي للتجارة الالكترونية (الأونسترال) مع تغيير لبعض الألفاظ، فاستخدم مصطلح رسالة المعلومات بدلا من مصطلح رسالة البيانات.

---

[1]- Article 01 de la loi n°2000-230 du 13mars 2000 du 14 mars 2000 : « **l'écrit sous forme électronique est. admis en preuve au même titre que l'écrit sur support papier , sous réserve que puisse être dument identifiée la personne dont 'il émane et qu'il soit établie et conserve dans des condition de nature à en garantir l'intégrité** » , sur le site : https://www.legifrance.gouv.fr/

[2] -Article 03 de la loi n°2000 -230 du 13mars 2000 du 14 mars 2000 : « **l'écrit sur support électronique a la même force probante que l'écrit sur support papier** ».

[3] ـ المادة 02 من قانون المعاملات الإلكترونية الأردني رقم15 لسنة 2015 على الموقع: http://www.cbj.gov.jo/

ج ـ القانون المصري:

عرف المشرع المصري المحرر الالكتروني في القانون 15- 04 الخاص بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات في المادة الأولى منه فقرة ب بأنه: **" كل رسالة بيانات تتضمن معلومات تنشا أو تدمج أو تخزن أو ترسل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى مشابهة"**[1]، كما بين في المادة 15 منه أن المحرر الالكتروني الرسمي هو المحرر الصادر عن جهة إدارية ويحمل توقيعا الكترونيا من الموظف المختص.

يلاحظ أن تعريف المشرع المصري لرسالة البيانات هو نفس تعريف المحرر الإلكتروني، الذي ورد في قانون الأونسترال النموذجي، وما نلاحظه أنه هناك قصور من ناحية تعبير رسالة البيانات عن الإلمام بصور المستند الإلكتروني، حيث أنه بتعبير المشرع أن المحرر الإلكتروني هو"رسالة البيانات" للدلالة على هوية الموقع على المحرر والرضاء بمضمونه نتيجة المراسلات المتبادلة بين طرفي العلاقة[2].

د ـ القانون التونسي:

عرف المشرع التونسي المحرر الإلكتروني من خلال المادة 453 (مكرر) من القانون المدني بنصه على أنه: **" يقصد بالمحرر الإلكتروني الوثيقة المكونة من مجموعة أحرف أو أرقام أو أية إشارات أخرى رقمية، بما في ذلك المتبادلة على حامل الكتروني يؤمن قراءتها والرجوع إليها عند الحاجة"**[3].

---

[1]- المادة الأولى الفقرة (ب) من قانون رقم 15- 2004 خاص بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ، متوفر على موقع:www.mcit.gov.eg/Ar/Media_Center

[2]- سمير حامد عبد العزيز الجمال، مدى حجية المحرر الإلكتروني في الإثبات في المسائل المدنية و التجارية في ضوء قواعد الإثبات النافذة ، دار النهضة العربية، القاهرة، 2004 ، ص.95.

[3] ـ المادة 453 من القانون المدني التونسي على موقع: http://www.legislation.tn/

اعتمد المشرع التونسي تعريفا يستند إلى العناصر المميزة للوثيقة الإلكترونية ، وتبنى تعريفا موسعا تاركا المجال مفتوحا ليشمل كل وسائل الاتصال التي سوف تظهر مستقبلا.

د ـ موقف المشرع الجزائري:

لم يعرف المشرع الجزائري المحرر الإلكتروني، ولم ينص صراحة على أي تعريف خاص ومحدد سواء بقانون خاص بالمعاملات الالكترونية أو في القوانين العامة الأخرى على خلاف التشريعات الأخرى كالمشرع المصري والأردني والتونسي، سيما أن التعاملات الإلكترونية أصبحت جزء مهم من حياة والأفراد والدولة، فعدم وجود تنظيم دقيق ومفصل يهدد استقرار المعاملات الالكترونية، بالمقابل كرس مبدأ التعادل الوظيفي بين المحررات الورقية والمحررات الالكترونية ، عن طريق المعادلة في حجية الإثبات بالكتابة مهما كان شكلها ومهما كانت الدعامة التي تحملها سواء كانت دعامة ورقية أو دعامة إلكترونية وذلك بنصه في المادة 323 مكرر من القانون المدني على أنه: **" ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها ، وكذا طرق إرسالها".**

نجد من خلال النصوص السابقة أن أغلب التشريعات اعتمدت في تعريفها للمحرر الالكتروني على استعمال مصطلح رسالة البيانات، والذي هو معتمد في قانون الأونسترال الذي يعتبر دليل استرشادي للدول، كما يمكننا القول أيضا أن جل التعريفات التشريعية السابقة بما فيها التشريعات الغربية والعربية قد شابها القصور نظرا لتركيزها على احد عنصري المحررات الالكترونية وهو الكتابة الالكترونية، دون أن تتضمن أية إشارة إلى العنصر الآخر وهو التوقيع الإلكتروني، كما أنها لم تبين الشروط اللازم توافرها في هذه المحررات، وكل هذا من شأنه أن يوسع في نطاق تعريف المحررات الالكترونية وبالتالي السماح لاستيعاب بيانات ومعلومات إلكترونية قد تكون غير موقعة إلكترونيا أو غير مستوفية لشروط هذه المحررات هذا من جهة، ومن جهة أخرى نلاحظ أن أغلب التشريعات الوطنية وإن اختلفت في سياق تعريفها للمحرر الالكتروني إلا أنها توافقت في المضمون.

يمكننا بناءا على ما سبق أن نعرف المحرر الالكتروني بأنه اصطلاح حديث يطل على كل الرسائل والبيانات الالكترونية التي تستخرج من وسائل الاتصال العلمية الحديثة كالتلكس والفاكس والحاسب الآلي والانترنت، التي أثبت العلم كفاءة هذه الوسائل فهي وسائل حديثة في الإثبات تترك أثرا ماديا مكتوبا على ورق خاص كما في التلكس أو يستنسخ المحرر طبقا لأصله كما في الفاكس وهذا الأثر المادي يصلح لإثبات مختلف التصرفات القانونية.

الفرع الثاني

أهمية المحررات الالكترونية وتطبيقاتها

ترجع أهمية المحررات الإلكترونية إلى التطورات التي فرضت نفسها على جميع الجوانب العملية من معاملات مالية وتجارية وحكومية، حيث أصبحت هذه النظم تعتمد في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لما تتميز به من سرعة وثقة وائتمان، والذي يعتبر أساس المعاملات التي يتطلبها عصرنا الحالي، ونظرا لوعي الدول بالدور الذي تلعبه المحررات الإلكترونية من حيث التزايد المستمر في الاستخدام والمكانة التي احتلتها كوسيلة إثبات التصرفات والمعاملات الإلكترونية، لجأت هذه الدول إلى تخصيص جانبا من اهتماماتها لتنظيم هذا الموضوع والاعتراف به صراحة في نصوص تنظم كيفية الاستفادة منه والاعتماد عليه، وذلك بمنحها قيمة قانونية عن طريق النص على مبدأ المساواة بين المحررات الإلكترونية والمحررات التقليدية من حيث الحجية، بحيث يكون لها نفس الأثر والقوة المقررة للمحررات التقليدية وبالتالي الاحتجاج بها في أي نزاع أو خلاف يثور بشأنها، بالتالي فإن أهم ما يستنتج من هذا المبدأ هو أن القاضي لا يفرق بين المحرر الورقي والمحرر الالكتروني ولا يرجح بين الحجج اعتمادا على شكلها أو وسيلة حفظها، وإنما المعيار الوحيد الذي يجب على القاضي الاعتداد به هو معيار المصداقية **(أولا).**

يتصل المحرر الإلكتروني من ناحية أخرى بطائفة مهمة من النظم الإدارية والتجارية والمالية التي تمتد لتشمل الدولة والأفراد على حد سواء، فالمحرر الالكتروني هو أحد الأدوات المهمة في تنفيذ فكرة الحكومة الالكترونية التي تقدم خدماتها إلى الأفراد والهيئات العامة

والخاصة، كما يعتبر أيضا الوسيلة التي من خلالها تحقق التجارة الدولية أهدافها، فمن خلال هذا المحرر وحده يمكن إنجاز المعاملات وإبرام التصرفات والصفقات التي تقتضيها فكرة التجارة الالكترونية، والذي أفضي إلى سهولة المعاملات التجارية وسرعة إنجازها وإلى توفير النفقات **(ثانيا)**.

أولا: أهمية تكريس مبدأ المساواة بين المحرر الإلكتروني والمحرر الورقي

تكمن أهمية تكريس مبدأ المساواة بين المحرر الالكتروني والمحرر الورقي في أنه يتماثل مع المحرر التقليدي من حيث الوظيفة التي يؤديها ومجالات استعماله، غير أن المحرر الالكتروني له الكثير من المزايا التي تكفل له انتشارا واسعا وتزايدا مستمرا في الاستخدام[1]، و تأتي أهمية هذا المبدأ في أنه يضفي على المحرر الالكتروني حجية في الإثبات باعتباره دليلا كتابيا كاملا يفرض نفسه على القاضي شأنه في ذلك شأن المحرر الورقي، ما لم يعد مسموحا رفض المحرر الالكتروني كدليل كتابي لمجرد أنه مدون على دعامة إلكترونية أو لكونه موقعا الكترونيا وليس بخط اليد.[2]

1 - مبدأ المساواة بين المحرر الالكتروني والتقليدي:

أحدث التطور التقني والفني في وسائل الاتصال الحديثة أثرا كبيرا على أدلة الإثبات الكتابية، فالمحررات الإلكترونية في ميدان المعاملات الإلكترونية أصبحت لها مكانة ضمن وسائل الإثبات فهي تحقق نفس الوظائف التي تحققها نظيرتها الورقية، بالتالي الاعتراف بمعادلتها للمحررات الورقية من حيث الحجية، إلا أن صعوبة المساواة بين المحرر الالكتروني والمحرر ذو الدعامة الورقية تكمن في توافر خصائص المحرر الورقي في المحرر الالكتروني، فالمحرر الالكتروني لا يستوفي الشروط اللازمة لاعتباره دليلا كتابيا كاملا في الإثبات، إذ أن التوقيع الالكتروني وإن كان يمكنه القيام بوظيفة التوقيع التقليدي ذاته إلا أنه لا يستوفي الشكل الذي

[1] - عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض، 2012، ص.78.

[2] - محسن إبراهيم البيه، دور المحررات الإلكترونية في الإثبات في القانون المصري، ص.97، بحث منشور على موقع:
http://law77.blogspot.com/

يتطلبه القانون، ومن ثم تبدوا إمكانية مساواة المحرر الالكتروني بالمحرر العرفي التقليدي في الإثبات محل شك في ظل قواعد الإثبات الحالية[1]، واختلفت آراء الفقه وأحكام القضاء حول إعطاء المحرر الالكتروني قيمة قانونية كالمحررات التقليدية، وبالرغم من المحاولات الفقهية العديدة في إصباغ الحجية القانونية على المحررات الالكترونية وفقا للقوانين التقليدية، إلا أن التدخل التشريعي ظل هو الطريق الراجح الذي من خلاله يمكن تلافي أمرين:

1- التوسع في التفسير الذي يتعارض مع الشرعية الجنائية.

2- إن ترك المعالجة التشريعية يتناقض وما يجب أن يقوم به التشريع في مواكبة التطور في مجال المعاملات التجارية الالكترونية[2].

توالت العديد من الجهود التشريعية سواء على المستوى الدولي أو على المستوى الوطني، على إيجاد ووضع أنظمة قانونية تواكب تلك التطورات الحاصلة والتي ارتكزت أساسا حول إضفاء الصبغة القانونية على المعاملات الالكترونية، وإجازة إثباتها من خلال آليات حديثة سميت بالمحررات الالكترونية، والتي تم اعتبارها بديلا قانونيا للمحررات الورقية تتساوى معها من ناحية الآثار والحجية في الإثبات، الأمر الذي أدى وبشكل مطرد إلى تزايد الاعتداد بحجية المحررات الإلكترونية في الإثبات.

أ ـ قانون الأونسترال بشأن التجارة الإلكترونية :

جاء القانون النموذجي والذي تم وضعه بمعرفة لجنة الأمم المتحدة للقانون التجاري الدولي في 17 ديسمبر 1996 ما نصه بالمادة 11 منه على أنه: **" وفي سياق تكوين العقود ، وما لم يتفق الطرفان على غير ذلك يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند استخدام رسالة البيانات في تكوين العقد، ولا يقيد المحرر صحته أو قابليته للتنفيذ لمجرد استخدام رسالة البيانات لذلك الغرض"[3].**

[1] ـ ماجد محمد سليمان أبا الخليل، ، العقد الالكتروني، مكتبة الرشد، الرياض،2009، ص.103.

[2] ـ حسن عبد الباسط جميعي، مرجع سابق، ص.81.

[3] ـ المادة 11 من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 متوفر على موقع:
https://www.uncitral.org/pdf/arabic/texts/electcom/ml-ecomm-a_ebook.pdf

أضافت المادة 12 منه نصا آخر على أنه: " **في العلاقة بين منشئ رسالة البيانات المرسل إليه لا يفقد التعبير عن الإرادة أو غيره من أوجه التعبير مفعوله القانوني أو صحته أو قابليته لمجرد أنه على شكل رسالة بيانات**"[1].

ساوى أيضا هذا القانون فيما بين الكتابة التقليدية والكتابة الالكترونية فنص في المادة 1/06 على أنه: " **عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا**"[2].

ب ـ المشروع الأوروبي الموحد للتجارة الإلكترونية:

أخذ المشروع الأوروبي الموحد للتجارة الالكترونية بنهج القانون النموذجي للتجارة الالكترونية والذي أعدته لجنة الأمم المتحدة الأونسترال، كما أخذ في اعتباره وضع إطار عام لقانون يسمح بالتنسيق بين مجموعة الدول الأوروبية على اختلاف أنظمتها القانونية، فنص في المادة التاسعة منه للاعتراف بقبول المحررات الالكترونية وتحديد حجيتها في الإثبات، وذلك من خلال الأخذ بمبدأ المساواة بين المحرر الالكتروني والأدلة الكتابية، وهو ما يعرف بمبدأ المساواة الوظيفية في الإثبات للقيام بذات الدور دونما اعتبار لشكل أو وسيلة الإثبات[3].

ج ـ القانون الفرنسي :

نص المشرع الفرنسي في المادة 1316 من التقنين المدني على أن الدليل الكتابي أو المكتوب هو: " **عبارة عن مجموعة من الحروف أو الأشكال أو الأرقام أو من إشارات أو رموز لها مدلول أيا كانت الدعامة المثبتة عليها**"[4].

[1] ـ المادة 12 من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996.

[2] ـ المادة 01/6 من قانون الأونسترال بشأن التجارة الإلكترونية لسنة 1996 .

[3]- مشار إليه لدى : حسن عبد الباسط جميعي، مرجع سابق، ص.84.

[4] - Art.1316 C.C.F. dispose que **:«** ***La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*** **»** .

أقر المشرع الفرنسي في هذه المادة بالمساواة بين المحررات أيا كانت الدعامة التي يدون عليها وأيا كانت طريقة الكتابة أو رموزها، بالتالي فإنه يمكن القول بأن المشرع الفرنسي أخذ بالمفهوم الوظيفي للمحرر وذلك بإقراره قوة ثبوتية مساوية للقوة الثبوتية للمحررات الكتابية، أيا كانت دعامتها سواء في ذلك الورق أو الدعامة الإلكترونية، فلم تعد الكتابة قاصرة على الكتابة كوسيلة إثبات وإنما تشمل الكتابة كشرط لصحة التصرف وذلك بالنظر إلى عمومية نص المادة 1/1316 والذي يعتبر أكثر وضوحا فيما يخص ما تتضمنه من تعريف للكتابة، مما يعطي لها معنى كامل دون تخصيص لها[1].

نص المشرع الفرنسي كذلك على الأخذ بالمفهوم الوظيفي سواء للكتابة أو التوقيع الالكتروني حيث نص في نفس المادة 1316 من التقنين المدني على أنه: **" يعتد بالكتابة المتخذة شكل الكتروني كدليل شأنها شأن الكتابة على دعامة ورقية، بشرط أن يكون في الإمكان بالضرورة تعيين الشخص الذي صدرت منه، وأن تعد وتحفظ في ظروف من طبيعتها ضمان سلامتها"**[2].

أقر المشرع الفرنسي أيضا بالحجية الكاملة للكتابة الالكترونية مثلها في ذلك مثل الكتابة التقليدية فنص المادة 1316-3 من نفس القانون على أنه**: " يكون للكتابة على دعامة الكترونية نفس القوة في الإثبات التي للكتابة على الورق"**[3] .

بدأ القضاء الفرنسي في قبول المحررات الالكترونية كأدلة كاملة في الإثبات، ويظهر ذلك في العديد من أحكام القضاء الفرنسي والتي نذكر مثالا لها ، الحكم الصادر في الثاني من جانفي 1998 والذي ورد في حيثياته أن: **"... المحررات يمكن تدوينها وحفظها على أي وسيط... بما في ذلك الوسائط الالكترونية، طالما أن المحررات تبدو ظاهرة الصحة ومكتملة العناصر**

[1] - OLIVIER D'AUZON, Le droit du commerce électronique ,Edition du puits fleuri, Paris, 2004, p76.

[2] - Art. 1316-1 du C.C.F. dispose que : ***« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*** .

[3] - Art. 1316-3 du C.C.F. dispose que: ***« L'écrit sur support électronique a la même force probante que l'écrit sur support papier ».***

خصوصا في شأن انتسابها لأطرافها، وطالما لم يذكر المدعي عليه"، وعلى الرغم من وجود اتجاه في القانون الفرنسي والقضاء يؤيد إعطاء المحررات الالكترونية الحجية القانونية في الإثبات، إلا أنه لا يمكن القول بأنه توجد نظرية عامة تحكم تلك المسألة يسير على خطاها القضاء، ويكون من شأن ترك تلك المسألة لتقدير القضاء ما لا يتفق والثقة التي يجب توفيرها لتلك المحررات الالكترونية وعدم الاعتداد بها في مجال إثبات التصرفات[1].

اتجهت كذلك محكمة النقض الفرنسية في بعض أحكامها إلى إعطاء المحررات الالكترونية حجية الدليل الكتابي المقررة للمحررات العرفية، وهذا إذا اكتملت عناصر الدليل واستوفى التوقيع عليه شروط صحته من حيث نسبته إلى صاحبه، وارتباط التوقيع بالمحرر على نحو يدل على قبوله، بما وضع التوقيع عليه وطالما لم ينكر المدعي عليه شيئا من ذلك[2].

يمكن القول أن المشرع الفرنسي قد استجاب كغيره من الدول الأوروبية للتوجيهات الأوروبية، والتي تدعو الاتحاد الأوروبي إلى استكمال المنظومة التشريعية الوطنية على نحو يمكن من خلاله استيعاب الدعامات الالكترونية في إثبات المعاملات الالكترونية، بالتالي بفضل هذا التدخل التشريعي فإنه اتخذ خطوة هامة ومباشرة نحو الاعتراف بالمحررات الموقعة إلكترونيا، ومساواتها بالمحررات العرفية من حيث الوظيفة ومن حيث الحجية في الإثبات .

د ـ القانون المصري:

كرس المشرع المصري مبدءا عاما يقض بالمساواة من حيث الحجية في الإثبات، بين التوقيع والكتابة والمحرر التقليدي والتوقيع والكتابة والمحرر الالكتروني، بمعنى عدم التمييز بين المحررات على أساس الدعائم أو الوسائط التي تقوم بها، وبعبارة أخرى، عدم إنكار الأثر القانوني للمحرر والتوقيع الالكتروني لمجرد اتخاذه الشكل الالكتروني.

[1]- حسن عبد الباسط جميعي ، مرجع سابق، ص.99.

[2] ـ سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق، مرجع سابق، ص.245.

أقر المشرع المصري مبدأ المساواة بين التوقيع والكتابة والمحرر التقليدي والتوقيع والكتابة والمحرر الالكتروني ونظم ذلك على مستويين:

- يتمثل المستوى الأول في المساواة بين التوقيع الالكتروني والتوقيع الخطي من حيث الحجية في الإثبات، إذ منح التوقيع الالكتروني ذات الحجية الثبوتية المقررة للتوقيع الخطي[1].

- يتمثل المستوى الثاني في المساواة بين المحررات الالكترونية والمحررات الورقية، حيث قرر معاملة المحررات المدونة على وسائط الكترونية بنفس الحجية الثبوتية التي تتمتع بها المحررات المدونة على وسائط ورقية[2].

ه ـ موقف المشرع الجزائري:

اعترف المشرع الجزائري بمبدأ التعادل الوظيفي بين الكتابة في الشكل الإلكتروني والكتابة على الدعامة الورقية، وجعلت لهما نفس الأثر والفعالية من حيث الحجية والإثبات، وذلك بشرط استيفائها للشروط التي نصت عليها المادة 323 مكرر 1 من القانون المدني الجزائري بنصها على أنه : **" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"**[3]، فيلاحظ أن المشرع لم يكتفي بأن أعطى للكتابة في الشكل الإلكتروني مكانة لها ضمن وسائل الإثبات، وإنما أعطى لها نفس الحجية التي تتمتع بها المحررات المدونة على دعامة ورقية مكرسا بذلك مبدأ التعادل الوظيفي.

يمكن من خلال التفسير الواسع للنصوص وفي غياب التحديد التشريعي للمقصود بالكتابة والمقصود بالتوقيع الالكتروني، قبول الكتابة الالكترونية والتوقيع الالكتروني كدليل كتابي كامل، لذلك يعد محررا إلكترونيا كل محرر يتمتع بذات المواصفات التي يتمتع بها المحرر

[1]- المادة 14 من قانون التوقيع الالكتروني المصري

[2]- راجع المادة 15 من القانون المصري رقم 15- 2004 .

[3] - المادة 323مكرر 1 من الأمر رقم 05-10 المتضمن التقنين المدني الجزائري .

الكتابي التقليدي من حيث توفر الثقة في أن التوقيع منسوب للموقع، وأنه تم وضعه على الورقة المحررة إلكترونيا بما يحقق ارتباطا وثيقا بينهما ويدل على قبوله بما ورد فيها.

لما كانت حجية الإثبات تعطي للكتابة التي يتضمنها المحرر الالكتروني، فيجب أن تمنح للمحكمة سلطة في تقدير حجية الكتابة الالكترونية[1]، ولما كان الأصل أن لمحكمة الموضوع التي تقدم أمامها المحررات الكتابية سلطة تقديرية واسعة في التحقيق من صحتها وإسقاط أو إنقاص قيمتها في الإثبات، فإن المحرر الإلكتروني إذا كان مشوبا بشائبة التزوير أو التصنيع فإن للمحكمة أن لا تأخذ بهذا المحرر، وكذلك لها أن تتركه إذا كان عدم صحته ظاهرا بوضوح كأن يكون المحرر الذي ينكره الخصم منسوبا لشخص لا يعرف القراءة أو الكتابة أو يجهل استخدام الحاسب الآلي والإنترنت، لأن التعامل بهذه المحررات يفترض بها العلم باستخدام هذه الأجهزة[2]، فلا تخول السلطة الممنوحة للمحكمة رفض المحرر الالكتروني لمجرد أنه عبارة عن بيانات أو معلومات مدونة على وسائط إلكترونية، وللقاضي سلطة واسعة في تقدير مدى قيمة الدليل الالكتروني المقدم أمامه وفي مراعاة توفر ضوابط الكتابة الالكترونية.

2- الأهمية العملية لمبدأ المساواة بين المحرر الإلكتروني والمحرر الورقي:

تكمن الأهمية العملية على اعتماد مبدأ المساواة بين المحررات الالكترونية والمحررات الورقية في السلطة التقديرية للقاضي في تطبيق مبدأ التعادل الوظيفي، فطالما تم إنشاء المحرر الإلكتروني وفق الشروط التي نص عليها القانون فإنه يتمتع بنفس الحجية التي يتمتع بها المحرر الورقي في الإثبات، بالتالي أثار ذلك تنازع بين الأدلة الكتابية والأدلة الورقية ولمعالجة هذه المشكلة أوردت بعض التشريعات حلولا لذلك نذكر من بينها:

[1] - محمد حسين منصور، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص.280، عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لنجاوزها، منشورات الحلبي الحقوقية، بيروت، 2010، ص.145.

[2] - ثروت عبد الحميد،، التوقيع الالكتروني، مرجع سابق، ص.115.

أ ـ القانون الفرنسي :

أورد التشريع الفرنسي نصا يتعلق بالترجيح بين المحررات في شكلها الإلكتروني والتقليدي في المادة 02/1316 من التقنين المدني بأنه : " **إذا لم يكن هناك نص أو إنفاق بين الأطراف يحدد أسس أخرى، فإنه على القاضي مستخدما كل الوسائل أن يفصل في النزاع القائم بين الأدلة الكتابية عن طريق ترجيح السند القريب إلى الاحتمال أيا كانت الدعامة المستخدمة في تدوينه**"[1].

يتضح من خلال هذا النص أن المشرع الفرنسي منح القاضي سلطة تقديرية واسعة في الترجيح بين المحررات على أساس معيار المصداقية مهما كانت دعامتها، وبكافة الطرق والوسائل المتوفرة لديه، والأخذ في الأخير بالمحرر الذي يراه أقرب إلى ذلك المعيار متى استوثق به، بالتالي لا يكون هناك محل للتمييز بين المحرر المدون على وسيط ورقي والمحرر الإلكتروني أو تفضيل الأول على الثاني، بالمقابل قيد المشرع هذه السلطة المخولة له وهذا في حالة وجود اتفاق بين الأطراف، فإن القاضي ينظر إلى المحرر الذي اتفق عليه الأطراف ويصرف النظر عن المحررات الأخرى بشرط عدم وجود نص قانوني ينظم مثل هكذا تنازع.

يتحقق القاضي من الكتابة محل النزاع عند عدم معرفة من نسبت إليه الكتابة، وله إصدار القرار ودون أن يأخذ في الاعتبار إذا كان الإنكار أو رفض الاعتراف حول التوقيع المكتوب أو التوقيع الكتروني، كما عليه أن يتحقق أيضا في مدى توافر الشروط التي تفرضها المواد 1/1316 و4/1316 من التقنين المدني الفرنسي[2] .

[1] - Article 1316-2 du C.C.F. dispose que : « ***Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support ».***

[2] -Article1316- 4 du C.C.F. dispose que :***« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.***

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve

أوجد المشرع الفرنسي قواعد موضوعية يتبعها القاضي للفصل في النزاع وهي:

1- النظر فيما إذا كان هناك اتفاق مسبق بين الطرفين حول ترجيح دليل على آخر وما هذا إلا تطبيق للقواعد العامة التي مفادها أن القواعد الموضوعية في الإثبات هي قواعد ليست من النظام العام وضعت لمصلحة الأطراف ومع ما يتلاءم وظروفهم.

2 - حالة عدم وجود اتفاق يقوم القاضي بتحديد السند الأقرب للاحتمال مهما كانت طبيعته تقليدي أو الكتروني والمقصود بها هو أن يكون هذا المحرر الأقرب إلى التصديق في الظروف الواردة فيها[1].

ب - القانون المصري :

لم يبين المشرع المصري دور القاضي في الترجيح بين المحرر التقليدي والمحرر الالكتروني، بل أقتصر دوره فقط على اعتماد حجية الكتابة الالكترونية متى تماثلت مع الكتابة التقليدية واستوفت شروطها التي ذكرناها سابقا.

يلاحظ أيضا أن عدم ورود نص تشريعي في هذا الصدد، ترك المشرع تقدير قوة المحرر الالكتروني في الإثبات لسلطة القاضي التقديرية، وعليه ينبغي المثول لإرادة أطراف النزاع، فإذا كان أطراف النزاع قد اتفقوا على أن تكون العلاقة بينهم وفقا للأدلة الكتابية التقليدية، أو الأدلة الكتابية الالكترونية، يلتزم المشرع بإرادة الأطراف، ومن ثم الرضوخ لإرادتهم في هذا الشأن فإذا لم يكونوا قد اتفقوا على ذلك، فإنه يرجح المشرع المحرر الرسمي على المحرر العرفي سواء أكانت تلك المحررات تقليدية أو إلكترونية ثم الرجوع إلى الأقدم ثبوتا في التاريخ فالأحدث، إلا إذا كان الأطراف قد اتفقوا على الأحدث، فإذا لم يثبت تاريخ وقت نشوء الدليل يتم الرجوع لسلطة القاضي التقديرية في النزاع.

---

contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat ».

[1]- حامد شاكر محمود الطائي، حجية المراسلات التجارية في ضل التطور التقني الحديث ، مجلة الحقوق، جامعة المستنصرية،،المجلد1، 2017 ، ص33.

ج ـ موقف المشرع الجزائري:

لا يوجد في التشريع الجزائري أي نص يفاضل بين المحرر الورقي والمحرر الالكتروني، فلم يرد نص يتعلق بحالة إذا ما عرض على القاضي ملف يتضمن الادعاء بإثبات حق معين، بحيث يقدم أحد الأطراف محررا مكتوبا مجسد على دعامة ورقية، والطرف الآخر يقدم محررا الكترونيا محاولا دحض ما جاء به خصمه.

نخلص في الأخير أن مبدأ المساواة في الحجية بين المحررات الإلكترونية والمحررات الورقية أثار شكلا جديدا من أشكال التنازع، ويتمثل ذلك على وجه الخصوص حول سلطة القاضي في الترجيح بين الأدلة الإلكترونية والأدلة الورقية، مما دفع ببعض التشريعات إلى السعي حول إيجاد حلول قانونية لهذه المسألة ونذكر في مقدمتهم المشرع الفرنسي الذي قدم حلا لهذه المشكلة، والذي نص على أنه يتوجب على القاضي إذا طرح أمامه محرر إلكتروني مقدم من أحد أطراف النزاع ومحرر ورقي مقدم من الطرف الآخر أن يرجع أولا إلى النصوص القانونية التي تنظم هذا التنازع ويعمل بها إن وجدت، كما أنه إذا وجد هناك اتفاق بين الطرفين ويكون صحيحا فإن للقاضي سلطة تقديرية في التقيد به والحكم بمدى صحته من عدمه، أما في حالة عدم وجود نص أو اتفاق ينظم مسألة الترجيح بين المحررات، فإنه يقع على القاضي تحديد المحرر الأقرب إلى الاحتمال وأكثر مصداقية وذلك بكل الوسائل التي يمكن من خلالها تكوين عقيدته.

ثانيا: تطبيقات المحرر الالكتروني

يتصل المحرر الالكتروني بمجموعة مهمة من الأنظمة الإدارية و التجارية والمالية التي تمتد لتشمل الدولة والأفراد على حد سواء، لذا فإن المحرر الالكتروني يعد الأداة الرئيسية لتنفيذ فكرة الإدارة الالكترونية والتي يشاع تسميتها بالحكومة الالكترونية إذ أنها تقضي باستخدام نظم المعلومات الرقمية في إنجاز المعاملات الإدارية وتقديم الخدمات المرفقية بشكل يسهل التعامل مع الأجهزة الحكومية بفضل الاتصال بالمواقع الخاصة بالوزارات والمؤسسات التابعة لها،

فضلا عن ذلك فهو يحقق فائدة كبيرة في مجال إبرام عقود التجارة الإلكترونية والتي اقتضت استخدام وسائط الكترونية تتناسب وطبيعتها الإلكترونية.

1 ـ المحرر الإلكتروني أداة تنفيذ للحكومة الالكترونية:

لم يعد التغيير الحاصل في العالم بسبب ثورة المعلومات وتكنولوجيا الإعلام والاتصال أن تبقى الحكومة الكلاسيكية دون مواجهة هذه التغييرات، بل بات من الضروري إعادة النظر جذريا بنموذجها وفي تغيير أسلوبها، بإيجاد نماذج جديدة تماما تتوافق مع الوضع القائم وهذا في نطاق البيئة الرقمية لتحول الحكومة القائمة إلى حكومة إلكترونية تؤدي جميع مهامها باستخدام الشبكة العنكبوتية للمعلومات والانترنت.

تعتبر أهم مجالات تطبيقات التوقيع الالكتروني هي الحكومة الالكترونية، حيث تشمل المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام، ومنها التصاريح المختلفة والخدمات التي تقدمها الجمارك والضرائب ومصلحة الأحوال المدنية، وكذلك ما يقدم إلى الجهات الحكومية من طلبات والتي من الممكن ووفقا لهذا المشروع، أن تتم عن طريق المحررات الالكترونية التي تصدرها الجهات المشار إليها ويتم توقيعها من قبل الموظفين العموميين في هذه الجهات، مما يضفي على تلك المحررات الالكترونية الحكومية صفة المحررات الرسمية بسبب قيام الموظف العام بالتوقيع عليها إلكترونيا[1]، ويستهدف هذا كله رفع كفاءة العمل الإداري، والارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع متطلبات العصر.

بهدف تيسير معاملات المواطنين مع جهات الإدارة الحكومية، فقد أتاحت الحكومة الفرنسية جميع النماذج التي يتم تحريرها لتقديم الطلبات الخاصة بمعاملات الأفراد على الشبكة الرقمية، وحيث أن الهدف من وضع هذه النماذج على الشبكة هو تمكين الأفراد من التعامل مع جهات الإدارة بدون حاجة إلى الانتقال والتواجد ماديا أمام الموظف المختص، فقد وردت نصوص هذه اللائحة بأنه: **" لا تستطيع الوزارات وجهات الإدارة والمصالح الحكومية رفض الطلبات المقدمة من الأفراد عن طريق الشبكة الإلكترونية، وتكون لهذه المحررات قوة**

[1] ـ مصطفى يوسف كافي، الإدارة الالكترونية، دار رسلان، ، دمشق، 2011، ص.333.

المحرر العرفي في الإثبات طالما أنه يوجد ما يدل إلى أنه قد حدث تلاعب بها أو تعديل فيها على الموقع الخاص بجهة الإدارة "[1].

يعد هذا النص ذو أثر كبير في اعتراف المشرع بقوة المحررات الإلكترونية في الإثبات، وذلك لضخامة حجم المعاملات التي يتم إنجازها يوميا عن هذا الطريق مع جميع جهات الإدارة الحكومية.[2]

أدى الاستخدام المتكرر من قبل الأفراد والحكومات لتكنولوجيا المعلومات والاتصالات وشبكة الإنترنت، خصوصا إلى الاستغناء عن خدمات بعض المرافق كخدمة مرفق البريد العادي وتعويضه بخدمة البريد الالكتروني (E-MAIL)[3]، كما أن اعتماد السلطات على تسهيل وتطوير الإجراءات القضائية ظهر ما يسمى التقاضي الإلكتروني عن طريق توفير نظام معلوماتي كامل ومقنن متصل بشبكات الاتصال الحديثة.

أ ـ البريد الإلكتروني:

يعد البريد الالكتروني[4] من أهم الخدمات التي تقدمها شبكة الانترنت، بحيث ساهم بصفة كبيرة في زيادة التواصل بين مستخدميها، بحيث، أصبح بالإمكان لأي شخص تملك عنوان بريد

[1] ـ مشار إليه: حسن عبد الباسط جميعي، مرجع سابق، ص.105.

[2] ـ المرجع ذاته، ص.105.

[3]- Définition du mot E-MAIL, "Electronic Mail". Désigne les messages échangés entre des utilisateurs par le moyen d'Internet, les messages sont stockés sur des serveurs avant d'être lus par les destinataires . http://dictionnaire.phpmyvisites.net/definition-E-MAIL-4438.htm

[4] ـ يرجع الفضل في ظهور البريد الالكتروني إلى العالم الأمريكي راي توملينسون Ray Tomlinson ، والذي يعتبر وبحق مخترع البريد الالكتروني حيث صمم على شبكة الانترنت برنامج لكتابة الرسائل يسمى send message،وكان الهدف منه هو تمكين العاملين بالشبكة من تبدل الرسائل فيما بينهم، ثم ما لبث أن اخترع برنامجا آخر سمي CYPNET يسمح بنقل الملفات من جهاز كمبيوتر إلى جهاز آخر، ثم قام بدمج البرنامجين في برنامج واحد، ونتج عن ١٩٧١ الدمج ميلاد البريد الالكتروني. يقوم عمل البريد الالكتروني على جزأين رئيسيين هما ((Header)) ونص ((Body)) ويحتوي الرأس على معلومات حول المرسل والمتلقي (المرسل إليه) و المعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب ، ويحتوي النص على الرسالة التي تم تكوينها , وعندما يرسل شخص ما رسالة إلى شخص آخر فإنها تنتقل من كومبيوتر المرسل عبر خط تليفون إلى كومبيوتر الخادم (مزود الخدمة) أو ما يسمى ملقم البريد (Server Mail) والذي يوجد به صندوق بريد المرسل ومن ثم تنتقل على نحو مباشر إلى كومبيوتر خادم آخر يخزن صندوق بريد المرسل إلية وعندها يستطيع

الكتروني خاص به، حيث يخصص لكل شخص صندوق بريد خاص به[1]، وأهم ما يميزه سرعة الإرسال والاستقبال، وقلة التكلفة بحيث يمكن إرسال أكثر من رسالة لأكثر من شخص في وقت واحد[2].

تتمثل رسائل البريد الإلكتروني في استخدام شبكة الإنترنت كمكتب للبريد، بحيث يستطيع مستخدم الإنترنت بواسطتها إرسال الرسائل إلى أي شخص له عنوان بريد إلكتروني، كما يمكنه أيضا تلقي الرسائل من أي مستخدم آخر للإنترنت ، وتتم هذه الخدمة مجانا، ولا يستغرق إرسال الرسالة واستقبالها سوى بضعة ثواني، ويجب أن يكون لدى مستخدم الإنترنت برنامج للبريد الإلكتروني يدرج ضمن البرامج التي يحتويها جهازه الخاص، فلكي يتمكن المرسل إليه من مطالعتها فما عليه سوى أن يستعمل برنامج بريده الإلكتروني، ويصدر أمرا بتحميل الرسائل على صندوق بريده الإلكتروني[3].

تعددت تعريفات البريد الالكتروني لدى فقهاء القانون فعرفه البعض بأنه: " **طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات بما فيها التبادل الالكتروني بين أجهزة الحواسيب**"[4] .

عرفه البعض الآخر بأنه: " **تلك المستندات التي يتم إرسالها أو استلامها بواسطة نظام اتصالات بريدي إلكتروني، وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه**

المرسل إليه أستر جاع محتويات صندوق بريده الالكتروني عند اتصاله بالخادم الخاص به وفق ما يسمى بالتحميل التحتي[(10)] (Down Loading) ويتم ذلك وفق برتوكولات عدة مثل برتوكول (POP) والتي هي اختصار (Post Office Protocol) أو(IMAP). هي اختصار لكلمة بروتوكول وصول الرسائل ويتحكم ببعض الطرق التي يصل بها برنامج البريد الالكتروني الجديد من الملقم. . محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2007، ص.30.

[1] ـ عبد الله بن إبراهيم بن ناصر، العقود الالكترونية ، دراسة فقهية تطبيقية مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون ، الإمارات العربية المتحدة، 10-12ماي 2003ن المجلد الخامس، ص2123 .

[2] - Marie Pierre Fenoll Trousseau et Gérard Haas, Internet et protection des données personnelles, LITEC, Paris 2000, p .73 .

[3] - عايض راشد عايض المري، مرجع سابق، ص72.

[4] - Verbiest Thibauult et wéry Etienne, Le droit de l'internet et de la société de l'information, Larcier, Bruxelles, 2001, p.611.

استصحاب مرفقات به مثل معالجة الكلمات، وأية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها"[1].

عرف المشرع الأردني البريد الالكتروني بأنه وسيلة من الوسائل التي توجد بها رسالة المعلومات وذلك من خلال تعريفه للمحرر الالكتروني طبقا لنص المادة 06/2 من قانون 85 لسنة 2001 الخاص بالمعاملات الالكترونية بالنص على أن: " **المعلومات التي يتم إنشاؤها وإرسالها أو تسليمها أو تخزينها بوسائل إلكترونية أو بوسائل مشابهة بما في ذلك تبادل البيانات أو البريد الالكتروني..."**[2].

كما عرفه المشرع الفرنسي في القانون الصادر في 22جويلية 2004 المتعلق بالاقتصاد الرقمي في المادة الأولى منه البريد الالكتروني بأنه: " **كل رسالة أيا كان شكلها نصية أو صوتية أو مرفقة بصور أو أصوات يتم إرسالها عبر شبكة عامة للاتصالات ويتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعادته"**[3].

تتم عملية التراسل عن طريق البريد الالكتروني بواسطة المحررات الالكترونية وذلك بكتابة رسالة البيانات، ثم كتابة عنوان المرسل إليه على الشبكة ثم الضغط على أمر الإرسال، فيقوم برنامج البريد الالكتروني الخاص به بإرسال الرسالة إلى الخادم، وعندما يتصل المرسل إليه بالخادم يقوم هذا الأخير بتوصيل الرسالة إلى جهازه، حيث تخزن في صندوق بريد المرسل إليه فيما يسمى الوارد، وعندما يفتحه هذا الأخير يمكن قراءة الرسالة[4]، بالتالي فإن البريد

[1] ـ يتكون عنوان البريد الالكتروني دائما من قسمين يفصل بينهما الرمز @حيث يوجد على يسار الرمز اسم المستخدم صاحب البريد الالكتروني والذي اختاره الأخير، وعلى يمين الرمز يكون اسم مقدم الخدمة، للمزيد راجع : عبد العادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة، 2005، ص.27.

[2] ـ المادة 06/02 من قانون المعاملات الإلكترونية الأردني رقم 85 لسنة2001.

[3] ـ عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، 2005، القاهرة، ص.43.

[4] خالد ممدوح إبراهيم، إبرام العقد الالكتروني، مرجع سابق، ص.51.

الالكتروني عادة ما يكون بشكل كتابي أو بياني يمكن أن يرسل من مستخدم إلى آخر وهو شبيه بالبريد التقليدي ولكنه أسرع وقليل التكلفة عند استخدامه[1].

يرى بعض الفقهاء أن رسائل البريد الالكتروني هي أحد تطبيقات المحررات الالكترونية، وحتى يعتد به كوسيلة للإثبات ويحتج به، لا بد أن يحقق هذا النوع من المحررات أهدافا تتمثل كالآتي:

- **الموثوقية في مضمون الرسالة:** بمعنى أن تكون الرسالة قد صدرت من مرسلها الحقيقي دون غيره.
- **السلامة في مضمون الرسالة:** يعنى أن مضمون الرسالة لم يتعرض لأي تزوير أو تعديل سواء بالحذف أو الزيادة ، بمعنى آخر أن الرسالة التي تم تلقيها من قبل المرسل إليه هي نفسها الرسالة المرسلة من قيل المرسل عن طريق البريد الالكتروني.
- **السرية في مضمون الرسالة:** يعنى ذلك أن الرسالة لا يمكن قراءتها وأن لا أ يطلع عليها ولا من قبل أي شخص غير الشخص المسموح له ذلك[2]، وتستخدم الشبكات الخاصة للبريد الالكتروني كوسيلة لتبادل البيانات إلكترونيا بين المنشآت التجارية المشاركة في الشبكة[3].

ب ـ التقاضي الإلكتروني :

يعتبر استخدام المحررات الإلكترونية في التقاضي الالكتروني بمثابة توجه الحكومات إلى تبني نظام الحكومة الإلكترونية في الإدارة العمومية وفي قطاع العدالة على سبيل التحديد، فيقصد بالتقاضي الالكتروني:" **عملية نقل محررات التقاضي إلكترونيا إلى المحكمة عبر البريد**

[1] ـ كمال أحمد الكركي، التحقيق في جرائم الحاسوب، المؤتمر الأمني والإداري، أكاديمية شرطة دبي، الإمارات العربية، 2003، ص.427.

[2] - Jacques Larrieu ,Droit de l'internet, ellipses, Paris,2010,p.20.

[3] ـ خالد ممدوح إبراهيم، حجية البريد الالكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية، 2008،، ص.32.

الالكتروني، حيث يتم فحص هذه المحررات بواسطة الموظف المختص، وإصدار قرار بشأنها بالقبول أو الرفض وإرسال إشعار إلى المتقاضي يفيده علما بما تم بشأن هذه المحررات[1]" ووفقا لهذا التعريف فإن المتقاضي أو المحامي عند رغبته في إقامة الدعوى بطريقة إلكترونية سوف يرسل صحيفة الدعوى عبر البريد الالكتروني من خلال موقع إلكتروني مخصص لهذا الغرض، وهذا الموقع متاح أربعة وعشرين ساعة يوميا وعلى مدار سبعة أيام في الأسبوع، حيث تستلم هذه المستندات بمعرفة الشركة القائمة على إدارة هذا الموقع ثم تقوم بإرساله إلى المحكمة المختصة، حيث يتسلمه الموظف المختص بقلم كتاب المحكمة ويقوم بفحص المحررات ثم يقرر قبول هذه المحررات أو عدم قبولها ويرسل للمتقاضي رسالة الكترونية يعلمه فيها باستلام مستنداته والقرار الصادر بشأنها[2].

تمتاز إجراءات التقاضي الالكتروني بعدم وجود أية وثائق ورقية متبادلة في إجراءات المعاملات، إذ أن كافة الإجراءات والمراسلات بين طرفي التقاضي تتم الكترونيا دون استخدام الأوراق[3]، وهو ما يتفق مع الغرض من التقاضي عبر الانترنت وهو خلق مجتمع المعاملات الالكتروني التي لا يكون للورق فيها دور، بالتالي في حالة نشوء أي نزاع بين طرفين فإن الرسالة الالكترونية هي السند القانوني الوحيد المتاح لهما.

لا يختلف التقاضي الالكتروني عن التقاضي التقليدي ولكنه يختلف فقط من حيث طريقة تنفيذه، وكونه يتم باستخدام وسائط الكترونية في تنفيذ إجراءات التقاضي الإلكتروني عبر شبكة الإنترنت، ويعتبر الحاسب الآلي المتصل بهذه الشبكة هو الوسيط بين طرفي التقاضي والذي يتم بواسطة التعبير عن الإرادة الإلكترونية[4]، وتلك الوسائط هي التي دفعت إلى اختفاء الكتابة

[1] ـ عمر لطيف كريم العبيدي، التقاضي الإلكتروني وآلية التطبيق، مجلة جامعة تكريت للحقوق، السنة 1 ، المجلد 3 ، الجزء 1، مارس2017. ص.512.

[2] ـ خالد ممدوح إبراهيم، التقاضي الالكتروني، مرجع سابق، ص.13.

[3] - Alain Bensoussan, Informatique et télécoms Internet, Francis LEFEBVRE ,Paris, 1997,P.16.

[4] ـ عمر لطيف كريم العبيدي، مرجع سابق، ص.5.

التقليدية التي تقوم على الدعائم الورقية لتحل محلها الكتابة الالكترونية التي تقوم على دعائم الكترونية[1] .

2 ـ المحرر الإلكتروني أداة لتحقيق التجارة الالكترونية أهدافها:

يؤدي إضفاء الحماية القانونية على المحررات الالكترونية إلى حماية الأموال المتداولة إلكترونيا جراء التعاملات التجارية الالكترونية، ومن ثم تكون هذه الأخيرة محل ثقة المتعاملين، وهو الأمر الذي يفضي إلى سهولة المعاملات التجارية وسرعة إنجازها وإلى توفير النفقات[2]، فلهذا نجد أن أغلب التشريعات حاولت إيجاد أنظمة تشريعية، ووضع أطر قانونية تشريعية لدعم البيئة الملائمة للتجارة الالكترونية والمحررات الالكترونية.

لم يقدم القانون النموذجي للتجارة الالكترونية تعريفا للتجارة الالكترونية ونفس الأمر بالنسبة للقانون الخاص بشأن التوقيعات الالكترونية الذي أصدرته نفس اللجنة.

عرف قانون التوجيه الأوروبي رقم 2000-11 لسنة 2000 وفق تعريفه للاتصال التجاري، وهذا في المادة 02 منه على أنه : " كل شكل من أشكال الاتصال يستهدف تسويقه بصورة مباشرة أو غير مباشرة بضائع أو خدمات أو صورة مشروع أو منظمة أو شخص يباشر نشاط تجاري أو صناعي أو حرفي أو يقوم بمهمة منظمة[3].

عرف البرلمان الأوروبي والمجلس الأوروبي التجارة الالكترونية عند تعريفه للعقد عن بعد وهذا في المادة 02 من التوجيه رقم 27/97 التي نصت على أن كل عقد يتعلق بالبضائع أو الخدمات أبرم بين مورد ومستهلك في نطاق نظام لبيع أو تقديم خدمات عن بعد ن نظمه المرد الذي يستخدم لهذا العقد فقط تقنية أو أكثر للاتصال عن بعد لإبرام العقد وتنفيذه[4].

[1] ـ خالد ممدوح إبراهيم، التقاضي الالكتروني، نفس المرجع، ص.39.

[2] ـ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، ، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي،10- 12 ماي2003، ص.484

[3] ـ عبد الفتاح بيومي حجازي الحكومة الالكترونية، دار الكتب القانونية، مصر، 2007، ص.235.

[4] ـ مشار إليه لدى: عبد الفتاح بيومي حجازي، نفس المرجع، ص.245.

عرف المشرع الأردني التجارة الالكترونية من خلال المادة 02 من قانون المعاملات الالكترونية لسنة 2001 في إطار تعريفه للمعاملات الالكترونية على أنها: **" المعاملات التي تنفذ بوسائل إلكترونية، كتقنية استخدام وسائل كهربائية أو مغناطيسية أو ضوئية أوإلكترومغناطيسية، أو أية وسائل مشابهة في تبادل المعلومات وتخزينها"**، وهذه المبادلات الالكترونية يقصد بها من خلال نفس الفصل المبادلات التي تتم باستعمال المحررات الالكترونية.

شهدت المعاملات الالكترونية تطورا كبيرا في مجال الإثبات مقارنة بالمعاملات الورقية، فهذه الأخيرة تعتبر أكثر عرضة للتزوير خاصة من ناحية الأمن التقني لها، فالمعاملات الالكترونية لا تربط بوجود أية وثائق ورقية متبادلة في إجراء وتنفيذ المعاملة، حيث أن كافة عمليات التفاعل بين طرفي المعاملة تتم إلكترونيا ودون استخدام أي وثائق مما يشكل صعوبة في إثبات العقود والتعاملات[1]، وتصبح المحررات الالكترونية هي الدليل الوحيد في الإثبات، وبالتالي تتضح لنا العلاقة بين المحرر الإلكتروني والتجارة الإلكترونية، فيتميز العقد الالكتروني بصفته العالمية التي تعطي أي دولة بالعالم لكونه يتم في معظم الأحيان عن طريق شبكة المعلومات[2]، فعرفه بعض الفقه بأنه العقد الذي يتلاقى فيه الإيجاب بالقبول عبر شبكة اتصالات دولية باستخدام التبادل الالكتروني للبيانات أو يقصد إنشاء التزامات تعاقدية، فهو إذن العقد الذي يتلاقى فيه الإيجاب بالقبول عبر شبكة اتصالات دولية باستخدام التبادل الالكتروني للبيانات، وبقصد إنشاء التزامات تعاقدية[3]، عرفته المادة الثانية من التوجيه الأوروبي الصادر في 1997/5/20 والمتعلق بحماية المستهلك في العقود المبرمة عن بعد فقد عرف التعاقد عن بعد (العقد الالكتروني) بأنه: **"أي عقد متعلق بالسلع والخدمات يتم بين موردو مستهلك من**

---

[1]- Éric Labbé, La multiplicité des normes encadrant le contrat électronique: l'influence de la technologie sur la production des normes ,Article disponible sur le site : **https://www.lex-electronica.org/auteur-e-s/labbe-eric/**

[2] ـ أسامة عبد العليم الشيخ، مجلس العقد وأثره في عقود التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية ، 2013، ص.23.

[3] ـ خالد ممدوح إبراهيم،، عقود التجارة الالكترونية، أوراق عمل مؤتمر التجارة الالكترونية وأمن المعلومات ،الفرص والتحديات، القاهرة، نوفمبر2008، منشور بموقع مركز العدالة للتحكيم والاستشارات: https://www.aladalacenter.com/

خلال الإطار التنظيمي الخاص بالبيع، بعد أو تقديم الخدمات التي ينظمها المورد، والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الالكترونية حتى إتمام التعاقد"[1]. وعرفه مشروع قانون المعاملات الأردنية بأنه : " **الاتفاق الذي يتم انعقاده بوسائل الكترونية كليا أو جزئيا"**[2].

عرف المشرع الجزائري التجارة الإلكترونية في المادة06 من القانون 18- 05 بأنه: " **النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية"**[3]، وتشمل عملية التعاقد الالكتروني بخلاف الإيجاب والقبول الالكتروني، على العديد من المعاملات الالكترونية، مثل العروض والإعلان عن السلع والخدمات، وطلبات الشراء الالكترونية والفواتير الالكترونية، وأوامر الدفع الالكترونية، ويدخل في نطاق العقد الالكتروني الاتصالات والرسائل والبيانات الالكترونية المتبادلة بين منشأة تجارية ومنشأة تجارية أخرى، ولكن لا يشمل الاتصالات داخل المنشأة الواحدة إذ لا تعدو أن تكون الأخيرة مجرد تبادل للبيانات والمعلومات لا ترقى إلى مستوى التعاقد الالكتروني[4].

يرى البعض أن المقصود بالعقد الالكتروني هو ذلك الذي يتم إبرامه عبر شبكة الانترنت، فهو عقد عادي إلا أنه يكتسب الطابع الالكتروني من الطريقة التي ينعقد بها، أو الوسيلة التي يتم إبرامه من خلالها، فالعقد ينشا من تلاقي القبول بالإيجاب بفضل التواصل بين الأطراف بوسيلة

[1] - Article 2 de la directive 97/7 du parlement européen du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance dispose que: « ***contrat à distance: tout contrat concernant des biens ou services conclu entre un fournisseur et un consommateur dans le cadre d'un systéme de vente ou de prestations de services à distance organisé par le fournisseur, qui, pour ce contrat, utilize exclusivement une ou plusieurs techniques de communication à distance jusqu'à la conclusion du contrat, y compris la conclusion du contrat elle-meme*** ».

[2] ـ المادة 02 من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015.

[3] ـ راجع المادة 06 من القانون رقم 18-05 مؤرخ في 10 ماي 2018 ، يتعلق بالتجارة الإلكترونية ، ج.ر.عدد28، صادر في 16 ماي سنة 2018.

[4] ـ خالد ممدوح إبراهيم، إبرام العقد الالكتروني، مرجع سابق، ص.52.

مسموعة مرئية[1] عبر شبكة دولية مفتوحة الاتصال عن بعد، وأن السمة الخاصة لذلك العقد تكمن في عملية ترويج وتبادل السلع والخدمات وإتمام صفقاتها باستخدام وسائل الاتصال وتكنولوجية تبادل المعلومات الحديثة عن بعد لا سيما شبكة المعلومات الدولية الانترنت دون حاجة لانتقال الأطراف والتقائهم في مكان معين، ويتم تبادل عروض السلع والخدمات عبر الشبكة من جانب أشخاص متواجدين في دول مختلفة وذلك بالتفاعل بينهم من أجل إشباع حاجاتهم المتبادلة بإتمام العقد[2].

ينصب العقد الالكتروني في خصوصيته والذي يتمثل أساسا في الطريقة التي ينعقد بها، فهو يتم تحريره في صورة محرر الكتروني، والتي من أحد عناصره الكتابة الالكترونية التي تحتوي على بيانات العقد الذي يتم بوسيلة الكترونية وأن العنصر الثاني فيه هو التوقيع الالكتروني، وهذان العنصران يمثلان وسيلة إثبات العقد الالكتروني الذي يعتبر أحد تطبيقات المحرر الالكتروني، وليس العقد في حد ذاته، بمعنى أن وسيلة إثباته سواء تمثلت هذه الوسيلة في الورقة المدون عليها بيانات العقد والمحتوية على التوقيع (المحرر الورقي)، أو تمثلت هذه الوسيلة في (محرر الكتروني) يحتوي على بيانات عقد تم على دعامة إلكترونية.

كما تعتمد التجارة الإلكترونية في التعامل أساسا على وسائل الاتصال وأجهزة الحواسيب الآلية، فقد أدى ذلك إلى تغيير محل التجارة الإلكترونية ووسائل تحقيقها، حيث تم استبدال الأوراق التقليدية الورقية بالأوراق الإلكترونية والتوقيع الإلكتروني وبالتالي أفرزت لنا عدة وسائل مستحدثة تقنية ووسائل حديثة تعتمد أساسا على الدعائم الإلكترونية بحيث سوف تختفي تماما المراسلات الورقية بين طرفي المعاملة ، حيث سيتحول الشيك ووسائل الدفع إلى بيانات أو معلومات تنساب عبر شبكات الاتصالات الحديثة والتي من أهمها الانترنت ، وهذه الوسائل جاءت كأسلوب مبتكر في مثل هذه المعاملات، بالتالي سنحاول أن نذكر على سبيل المثال لا الحصر:

[1] ـ أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الانترنت، دار النهضة العربية، 2000، ص.39.

[2] ـ محمد حسين منصور، المسؤولية الالكترونية، مرجع سابق، ص.18.

ـ المحفظة الإلكترونية :

تعرف المحفظة الإلكترونية بأنها عبارة عن برامج كمبيوتر يقوم العميل بتنزيله وتركيبه على جهاز الكمبيوتر الخاص به، وهي تشبه في خدمتها الوظيفة المماثلة للمحافظ المادية التي يحفظ فيها بطاقات الائتمان والنقد الإلكتروني والهوية الشخصية، قد تكون المحفظة الإلكترونية بطاقة ذكية يمكن تثبيتها على الكمبيوتر الشخصي أو تكون قرصا مرنا يمكن إدخاله في فتحة القرص المرن في الكمبيوتر ليتم نقل القيمة المالية منه أو إليه عبر الإنترنت[1].

ـ الشيك الالكتروني :

يعد الشيك الالكتروني المكافئ الالكتروني للشيكات الورقية التقليدية التي أعتدنا التعامل بها، والشيك الالكتروني هو رسالة موثقة ومؤمنة يرسلها مصدر الشيك إلى مستلم الشيك ـ حامله ليعتمده ويقدمه للبنك الذي يعمل عبر الانترنت، ليقوم البنك أولا بتحويل قيمة الشيك ـ حامله ـ ليكون دليلا على أنه قدم على صرف الشيك وإعادته الكترونيا إلى مستلم الشيك ـ حامله ـ ليكون دليلا على أنه قدم على صرف الشيك فعلا، ويمكن لمستلم الشيك أن يتأكد الكترونيا من أنه قد تم بالفعل تحويل المبلغ غلى حسابه[2].

يرى البعض أن الشيكات الالكترونية عبارة عن رسالة تحتوي على جميع البيانات التي يمكن أن يجدها بالشيك الورقي العادي، بحيث يقوم المشتري بتحرير شيك الكتروني للبائع وإرساله له إلكترونيا عبر أية وسيلة الكترونية، كالفاكس أو البريد الالكتروني في أغلب الأحيان[3]، وتكون جميع التوقيعات التي يتضمنها هذا الشيك توقيعات الكترونية أو رقمية[4].

---

[1] ـ خالد ممدوح إبراهيم، التقاضي الإلكتروني، مرجع سابق، ص.91.

[2] ـ منير الجهنمي، ممدوح الجهنمي، البنوك الالكترونية، دار الفكر الجامعين الإسكندرية، 2005، ص.49.

[3] محمد أمين الرومي، المستند الالكتروني، ص.62.

[4] يعتمد استخدام الشيك الالكتروني كوسيلة للدفع على وجود وسيط يقوم بإرجاء عملية المقاصة ، وغالبا ما يكون أحد البنوك على النحو التالي:

يقوم المشتري بفتح حساب جاري لدى البنك، ويتم تحديد التوقيع الالكتروني للمشتري وتسجيله في قاعدة البيانات الخاصة بالبنك، ويجب أن يكون البائع هو الآخر لديه حساب جاري بنفس البنك ويتم تحديد توقيع الكتروني خاص به، تسجيله بالمثل في قاعدة البيانات الخاصة بالبنك، ثم يقوم المشتري بتحرير شيكا الكترونيا للبائع مقابل السلعة أو الخدمة التي يرغب في شرائها ويوقع هذا الشيك توقيعا الكترونيا

يرى بعض الفقه أن هناك من الفقه من يدخل الشيكات الالكترونية تحت مسمى الوسائط الالكترونية الجديدة، ويدخل تحتها نظام القابض الافتراضي الأول، والقابض عبارة عن وسيط بين المتعاملين يتلقى طلبات موقعة على الشبكة ويتولى مباشرة عملية عرض السلعة أو الخدمة والتسليم والوفاء نظير عمولة معينة[1].

مشفر ويرسله للبائع عبر البريد الالكتروني المؤمن، يقوم البائع باستلام الشيك الالكتروني الموقع من المشتري ويقوم بالتوقيع عليه ـ كمستفيد ـ بتوقيعه الالكتروني المشفر ويقوم بإرساله إلى البنك. ثم يقوم البنك بمراجعة الشيك وبالتحقق من صحة الأرصدة والتوقيعات وبناء على ذلك يقوم بإخطار كل من المشتري والبائع بإتمام إجراءات المعاملة المالية (خصم الرصيد من المشتري وإضافته للبائع) راجع في ذلك : محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.64.

[1] ـ محمد حسين منصور، المسؤولية الالكترونية، مرجع سابق، ص.128.

المطلب الثاني

أنواع المحررات الالكترونية

تضفي على المحررات الالكترونية في الوقت الحاضر سواء كانت رسمية أو عرفية حجية في الإثبات تتفاوت في درجة الإثبات حسب نوعها، وهي تحوي توافق إرادتين على إحداث أثر قانوني أو إرادة واحدة، فالمحررات الرسمية هي التي يثبتها الموظف العام أو الشخص المختص ما تم على يديه أو ما تلقاه من ذوي الشأن من محررات تكون معدة سلفا للإثبات، وهي أقوى المحررات حجة، أما المحررات الإلكترونية العرفية فهي التي تكون دليل إثبات لكن تتفاوت حجيتها في ذلك حسب نية أطراف رابطة الالتزام، وحسب ما إذا كانت المحررات الإلكترونية معدة للإثبات والتي تحمل توقيعات الأطراف أم غير معدة للإثبات وهي عادة لا تحمل توقيعاتهم.

يمكن تقسيم المحررات الالكترونية عموما إلى محررات إلكترونية معدة للإثبات **(الفرع الأول)**، وأخرى محررات إلكترونية غير معدة للإثبات **(الفرع الثاني)**.

الفرع الأول

المحررات الإلكترونية المعدة للإثبات

يمكن أن تكون المحررات الإلكترونية المعدة للإثبات محررات رسمية يقوم بتحريرها موظف عام أو ضابط عمومي أو شخص مكلف بخدمة عامة، أو أي شخص مختص وفقا للأوضاع المقررة قانونا **(أولا)**، وإما أن تكون محررات عرفية وهي التي يقوم بتحريرها أصحاب الشأن فيما بينهم أعدت مقدما لإثبات تصرف أو واقعة قانونية معينة **(ثانيا)**.

أولا : المحررات الالكترونية الرسمية

يعد المحرر الرسمي الالكتروني كل كتابة الكترونية مثبتة لواقعة قانونية في تصرف قانوني يترتب عليه آثار قانونية معينة، بمعنى آخر هو الوثيقة التي تدون فيها البيانات والمعلومات

والتي يتدخل في تحريرها موظف عام، مختص بإثباتها وتحريرها وفقا للإجراءات المنصوص عليها قانونا، لكن بشرط مراعاة الشروط القانونية الخاصة بتحرير ذات المحرر الرسمي في صورته التقليدية، وبالتالي تثبت لها حجية قبل الكافة عن البيانات المثبتة فيها، فيختلف شكل المحرر الرسمي الإلكتروني عن المحرر الرسمي الورقي لكن لهما نفس الأثر والفعالية من حيث الحجية وصحة الإثبات، وذلك ما أقرته أغلب التشريعات الوطنية والدولية التي اعترفت بالمحررات الإلكترونية كمقابل وظيفي للمحررات الخطية.

ينشأ المحرر الالكتروني الرسمي في بيئة الكترونية وفقا لضوابط فنية وتقنية، تنظم كيفية تدخل الموظف العام في إضفاء صفة الرسمية عليه.

اشترط الفقه شروطا ثلاثة يلزم توافرها في المحرر حتى ينال وصف المحرر الرسمي، وهي صدور الورقة من موظف عام أو شخص مكلف بخدمة عامة، وأن تصدر من الموظف العام في حدود سلطته واختصاصه، ومراعاة الأوضاع القانونية في تحرير الورقة[1].

قدم المشرع الفرنسي تعريفا للمحررات الرسمية وذلك في نص المادة 1317 من التقنين المدني بأنها **:" الورقة الرسمية التي يتلقاها موظف عام له حق التوثيق في الجهة التي كتبت فيها الورقة وذلك وفقا للأوضاع الشكلية المتطلبة"**[2]، وفي سبيل تطويعه للمحررات لقبول تكنولوجيا المعلومات والتوقيع الالكتروني، فإنه أضاف فقرة ثانية إلى المادة **1317**، نص فيها على أن **"يمكن وضعه على دعامة إلكترونية، إذا تم إنشاؤه وحفظه وفقا للشروط التي يضعها مرسوم من مجلس الدولة"**[3]، وهو بهذا التعديل قد أتاح المجال أمام تقبل فكرة تطور المحررات الرسمية من محررات مثبتة على دعامات ورقية إلى محررات مثبتة على دعامات لا ورقية أو إلكترونية.

---

[1]- محمد محمد سادات، حجية المحررات الموقعة إلكترونيا في الإثبات، مرجع سابق، ص.169.

[2]-Article 1317/01 du C.C.F. dispose que: ***« L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises ».***

[3]- Article 1317/02 du C.C.F. dispose que ***:« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. ».***

أجاز المشرع المصري في قانون التوقيع الالكتروني إنشاء المحرر الرسمي على دعامة الكترونية وهو نفس الحكم الذي أخذ به المشرع الفرنسي صراحة، حيث قرر إمكانية اكتساب المحرر الالكتروني الصفة الرسمية بتدخل موظف عام وبتوقيعه على المحرر، وكل ذلك يفيد أن تدخل الموظف العام شرط لإضفاء الصفة الرسمية على المحرر الالكتروني، ورغم أن المشرع المصري لم يورد نصا صريحا في هذا المعنى، إلا أن الراجح لدينا هو اشتراط هذا التدخل من قبل الموظف العام، لأن هذا هو مقتضى ما قرره المشرع المصري في المادة 15من قانون التوقيع الالكتروني من حيث مبدأ المساواة بين المحررات الالكترونية الرسمية والعرفية وبين المحررات الرسمية والعرفية[1]، أين نصت على " **متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون"**، كما نص في المادة 17 من قانون الإثبات المصري على أنه: " **تسري في شأن إثبات صحة المحررات الإلكترونية الرسمية و العرفية و التوقيع الإلكتروني و الكتابة الإلكترونية، فيما لم يرد بشأنه نص في ها القانون أو في لائحة تنفيذية، الأحكام المنصوص عليها في قانون الإثبات في المواد المدنية و التجارية"**[2].

عرف المشرع الجزائري المحرر الرسمي بموجب نص المادة 324 من القانون المدني الجزائري بمصطلح العقد فنص على أنه : " **العقد الرسمي عقد يثبت فيه موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة ما تم لديه أو تلقاه من ذوي الشأن وذلك طبقا للأشكال القانونية وفي حدود سلطته واختصاصه"**[3].

يلاحظ أن اشتراك شخص ذي صفة رسمية في تحرير المحرر الرسمي وما يستلزم ذلك من ضرورة توفير الثقة في أعماله، جعل للمحرر الرسمي ضرورة توفير الثقة في أعماله، مما جعل للمحرر الذي يقوم بتحريره حجية أقوى من حجية المحرر العرفي الذي يحرره الأفراد العاديون، فيلزم لإنكار صحة ما في المحرر الرسمي من بيانات رسمية اتخاذ طريق الطعن

[1] ـ محسن عبد الحميد إبراهيم البيه، مرجع سابق، ص.144.

[2] ـ مشار غليه لدى: محمد أحمد العابدين، الورقة الرسمية والعرفية في الإثبات، منشأة المعارف ، الإسكندرية، 2002، ص.11.

[3] ـ المادة 324 من الأمر رقم 05-10، المتضمن التقنين المدني الجزائري.

بالتزوير، في حين أن القانون لم يجعل للمحرر العرفي قوة كدليل كتابي، إلا إذا اعترف به من يتمسك به ضده، وإذا أثبت المتمسك به صحته إذا أنكره من صدر منه[1].

ثانيا: المحررات الالكترونية العرفية المعدة للإثبات

تعرف المحررات العرفية المعدة للإثبات بأنها المحررات التي يقوم الأفراد بتحريرها فيما بينهم والتي يلزم لاعتبارها دليلا كتابيا كاملا أن يوقع عليها أطرافها[2]، والتي لا يتدخل موظف عام في تحريرها[3]، كما أنها الكتابة التي يوقعها شخص لإعداد دليل على واقعة، وأن تكون بالورقة كتابة مثبتة لواقعة قانونية[4] ، فلا يخرج المحرر العرفي الإلكتروني عن هذا المفهوم، إلا أن الاختلاف يكمن في اعتبار أن الكتابة إلكترونية والتوقيع إلكترونيا، فالمحررات العرفية الإلكترونية هي تطور للمحررات العرفية التقليدية ولكن في شكل إلكتروني[5] .

نص المشرع الجزائري في المادة 327 من التقنين المدني على أنه: **" يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه، ما لم ينكر صراحة ما هو منسوب إليه، أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق....".**

يلاحظ من خلال هذا أن المحررات التي تقدم للإثبات إما أن تكون محررات رسمية محررة بمعرفة شخص و بصفة رسمية أي موظف من موظفي الدولة أو شخص مكلف بخدمة عامة، وإما أن تكون محررات عرفية محررة بمعرفة أشخاص عاديين ليست لهم هذه الصلة، وهي محررات معدة مسبقا للإثبات فيما قد يثور من منازعات بين الأطراف مستقبلا وما يميزها هو

[1] - إبراهيم الدسوقي أبو الليل، الحجة القانونية للتعاملات الإلكترونية، مجلس النشر العملي، الكويت،2003، ص.11. و محمد سعيد خليفة، مرجع سابق، ص.120.

[2] - حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، مرجع سابق، ص.16.

[3] - محمد محمد سادات، حجية المحررات الموقعة إلكترونيا في الإثبات، مرجع سابق، ص.78.

[4] - محسن عبد الحميد إبراهيم البيه، مرجع سابق، ص.78.

[5] - محمد محمد سادات، حجية المحررات الموقعة إلكترونيا في الإثبات، مرجع سابق، ص.79.

توقيع الأطراف عليها، فكل من المحرر الرسمي والمحرر العرفي دليل كتابي له ما لهذا الدليل من قوة بالنسبة للأدلة الأخرى.

الفرع الثاني

المحررات الالكترونية غير المعدة للإثبات

تعرف المحررات الإلكترونية غير المعدة للإثبات، بأنها أي كتابة إلكترونية لا تحمل توقيعا إلكترونيا موثقا وفقا للطرق والإجراءات التي نصت عليها التشريعات الخاصة بالمعاملات الإلكترونية في هذا الشأن، فهي محررات لها حجية بين المتعاقدين ما لم يتم إنكارها والدفع فيها بالجهالة وتكون لها حجية بالنسبة للغير إذا كان لها تاريخ ثابت، فهي لا تكون قابلة للتنفيذ إلا إذا صدر بشأن تنفيذها حكم قضائي للمحررات العرفية التي لم تعد أصلا للإثبات ولا تكون عادة موقعة من ذوي الشأن ومع ذلك فإن القانون يمنح لها حجية في الإثبات تتفاوت بحسب الأحوال.

فالمحررات العرفية غير المعدة للإثبات هي المحررات التي لا تحمل توقيع الأطراف، ولم تعد أصلا للإثبات، رغم أن إرادة الأطراف لا تذهب إلى إعدادها كدليل للإثبات، إلا أن المشرع قد جعل لها حجية في الإثبات تتفاوت قوة وضعفا تبعا لنوع المحرر.

أولا: الدفاتر التجارية

ألزم المشرع الجزائري على كل شخص اكتسب صفة التاجر أن يمسك بدفاتر يقيد فيها العمليات التجارية وكل ما يرتبط بتجارته بشكل يوضح فيه مركزه المالي،أو أن يراجع على نتائج هذه العمليات شهريا بشرط أن يحتفظ في هذه الحالة بكافة الوثائق التي يمكن معها مراجعة تلك العمليات يوميا، فينبغي على التاجر مراعاة إجراءات معينة في استعمال الدفاتر وتنظيمها حتى يكون لها حجة في الإثبات طبقا للمادة 330 من التقنين المدني[1]، والدفاتر التجارية قد تكون

[1] ـ تنص المادة 330 من القانون المدني الجزائري : **" دفاتر التجار لا تكون حجة على غير التجار، غير أن هذه الدفاتر عندما تتضمن بيانات تتعلق بتوريدات قام بها التجار، يجوز للقاضي توجيه اليمين المتممة إلى أحد الطرفين فيما يكون لإثباته بالبينة، وتكون دفاتر التجار حجة على هؤلاء التجار، ولكن إذا كانت هذه الدفاتر التجارية منتظمة فلا يجوز لمن يريد استخلاص دليل لنفسه أن يجزئ ما ورد فيها واستبعاد ما هو مناقض لدعواه".**

حجة على التاجر كما يمكن أن تكون حجة له، وقد أجاز للمحكمة أن تطلب تقديمها إليها لاستخلاص ما يتعلق بالنزاع المعروض عليه.

منح المشرع الفرنسي المحررات الإلكترونية الحجية المقررة للدفاتر التجارية الورقية، وذلك بصدور القانون رقم 85-353 بتاريخ 30أفريل 1983، بشأن السماح باستخدام الوسائط الإلكترونية والمستخدمة في تدوين حسابات التجار والشركات التجارية كبديل عن الدفاتر التجارية ومنحها ذات الحجية المقررة لدفاتر التجار بموجب القانون المدني الفرنسي[1].

ثانيا: الرسائل و البرقيات

نص المشرع الجزائري في المادة (329 /1) من التقنين المدني على أنه **" تكون للرسائل الموقع عليها قيمة الأوراق العرفية من حيث الإثبات..."**، فقد منح المشرع للرسالة نفس حجية المحرر العرفي متى كانت موقعة، لذلك فهي تصلح كدليل كتابي كامل، وتأخذ نفس أحكام المحرر العرفي من حيث الحجية ومن حيث وجوب ثبوت التاريخ للاحتجاج بها على الغير.

أما بالنسبة للبرقيات، فباستقرائنا لنص المادة (02/329) التي نصت على أنه: **" تكون للبرقيات هذه القيمة أيضا إن كان أصلها المودع في مكتب التصدير موقعا عليه من مرسلها، وتعتبر البرقية مطابقة لأصلها.."** فالمشرع الجزائري منح للبرقية نفس قيمة الرسالة الموقعة والمحرر العرفي إذا كان أصل هذه البرقية المودعة في مكتب التصدير موقعا عليها من المرسل، فالبرقية تكون مطابقة لأصلها حتى يقوم الدليل على عكس ذلك، أما إذا كان هذا الأصل غير موقع عليه فلا تكون للبرقية أية قيمة في الإثبات،

نصت المادة 16 من قانون الإثبات المصري على أنه :**" تكون للرسائل و البرقيات الموقع عليها قيمة المحرر العرفي من حيث الإثبات، وتكون للبرقيات هذه القيمة أيضا إذا كان أصلها**

[1] - حسن عبد الباسط جميعي، مرجع سابق، ص.101.

المودع في مكتب التصدير موقعا أيضا عليها من مرسلها، وتعتبر البرقية مطابقة لأصلها حتى يقوم الدليل على عكس ذلك، وإذا أعدم أصل البرقية فلا يعتد بالبرقية إلا بمجرد الاستئناس"[1].

منح المشرع المصري قرينة قانونية مفادها أنه متى كان أصل البرقية موقعا ومحفوظا في مكتب التصدير أفترض مطابقة البرقية للأصل وعلى من يدعي خلاف ذلك إقامة الدليل العكسي، ويعتبر تاريخ البرقية تاريخا ثابتا لأن خاتم المكتب يختم به الأصل الذي يحمل تاريخ الإرسال ويمكن التأكد من صحة التاريخ بالرجوع إلى الدفتر المعد لذلك.

لكن من جهة أخرى لا يعتد بالبرقية في حالة ما إذا كان أصل البرقية غير موجود في مكاتب التصدير إلا على سبيل الاستئناس وفقا لما تقتضي به الفقرة الأخيرة من نفس المادة.

يلاحظ من خلال اعتراف التشريعات المقارنة بمبدأ المساواة بين المحرر الالكتروني والمحرر الورقي التقليدي من حيث القوة الثبوتية كدليل إثبات، إنما كان المقصود منه المحرر الذي يتدخل فيه وسيط موثوق فيه بـتأمينه من حيث مضمونه ونسبته إلى صاحبه وحفظه، أما المحرر الالكتروني الذي ينشئه الأطراف دون تدخل وسيط في تأمينه من حيث الحجية ، فأغلب التشريعات لم تعترف له بأية حجية وبالتالي تركت أمر حجيته للقواعد العامة.

[1] - سمير حامد عبد العزيز الجمال، مدى حجية المحرر الإلكتروني في الإثبات في المسائل المدنية و التجارية في ضوء قواعد الإثبات النافذة ، دار النهضة العربية ، القاهرة، 2004، ص.248 .

المبحث الثاني

عناصر المحرر الالكتروني

حتى نكون أمام محرر الكتروني يكون بديلا للمحرر الورقي في إثبات التصرفات القانونية المبرمة عبر وسائل الاتصال الحديثة، لا بد أن يتوفر على عنصريه من كتابة إلكترونية وتوقيع إلكتروني والذي لا يقوم مكتملا إلا بتوفرهما.

يتعين تحديد مفهوم الكتابة أن يكون في إطار وظيفتها في الإثبات وليس على أساس نوع الوسيط الورقي بالمفهوم التقليدي، فيشترط في الكتابة الالكترونية ما يشترط في الكتابة العادية حتى تؤدي وظيفتها في الإثبات، فلا اختلاف في المضمون وإنما الاختلاف يكمن فقط في الوسيلة المستخدمة للكتابة والتي تتمثل بالوسائط الإلكترونية أين يتم من خلالها تبادل البيانات والمعلومات بين أطراف العلاقة، سواء كانت هذه الوسائط كهربائية أو مغناطيسية أو ضوئية أو أية وسيلة مشابهة لتوصيل المعلومة بينهما، أو من أجل إثبات حق أو نفيه أو للقيام بعمل معين، **(المطلب الأول)**.

فالتوقيع الإلكتروني يشكل العنصر المهم والجوهري لجعل المحرر الإلكتروني دليلا كاملا في الإثبات، فهو يعتبر وسيلة لتحديد هوية الموقع من ناحية، ويؤكد انصراف إرادته إلى الالتزام لمحتوى ما وقع عليه من ناحية أخرى، لذلك فإن أهمية التوقيع الإلكتروني على المحرر الإلكتروني ترجع إلى قيامه بوظائف تؤكد نسبة مضمون الكتابة الموقع عليها إلى صاحب التوقيع مع ما يترتب على ذلك من آثار قانونية، **(المطلب الثاني)**.

المطلب الأول

الكتابة الالكترونية

يجب عند تناول مفهوم الكتابة النظر إليها على أساس أن الأسلوب الالكتروني في الكتابة يصلح كوسيلة لإثبات جميع التصرفات القانونية في كافة المعاملات المدنية والتجارية، فالكتابة بجانب الدعامة المكتوبة عليها تكون المحرر الذي يعتبر وسيلة يتم توظيفها لإعداد دليل على وجود التصرف القانوني وتحديد مضمونه، بما يمكن الأطراف من الرجوع إليه في حالة نشوب خلاف، وعرضه على القاضي المختص ليفصل بينهم في ضوء ما تم الاتفاق عليه، وعليه فتحديد مفهوم الكتابة والمقصود منها يجب أن يتم في ضوء وظيفة الكتابة والغرض منها، وليس على أساس طريقة الكتابة أو المادة المستخدمة في الكتابة أو طريقة صياغتها، بالتالي يقتضي تغيير مفهوم فكرة المحرر، فلم تعد قاصرة على المحرر التقليدي المكتوب بل تستوعب كذلك المحرر الالكتروني **(الفرع الأول)**.

أصبح للكتابة الالكترونية مفهوم واسع وحديث يشمل الكتابات المستخرجة من الوسائل التقنية الحديثة، فالكتابة الالكترونية لا يمكن قراءتها بشكل مستقل، ذلك أنها عبارة عن جزئيات دقيقة مجهزة ومثبتة إلكترونيا ومغناطيسيا على دعامة بشكل يسمح للحاسب الآلي فقط بقراءتها، وأن تحمل نوعا من الثبات النسبي، أي ألا تزول تلقائيا، وأن تبقى ما لم يتعرض المحرر للتلف، فالكتابة الالكترونية يمكن تعديلها بسهولة مما ينتفي معه اتسامها بالثبات على غرار الكتابة التقليدية، بالتالي لا بد من أن تتوافر على شروط وضوابط معينة حتى يمكن الاعتداد بها كدليل للإثبات ويعطيها قوة ثبوتية كاملة للمحررات التي تحتوي هذه الكتابة، فلا بد أن تكون قابلة للقراءة حتى تدل على مضمون التصرف القانوني أو البيانات المدونة في المحرر، أن تكون مستمرة بحيث يمكن لأصحاب الشأن الرجوع إليها عند الحاجة، أن تتضمن عدم التعديل في مضمونها سواء بالإضافة أو الحذف، وذلك حتى تتمتع بالثقة والأمان وبالتالي تؤدي وظيفتها القانونية الكاملة في الإثبات، **(الفرع الثاني)**.

الفرع الأول

تحديد مفهوم الكتابة في الشكل الإلكتروني

لم تعد الكتابة الإلكترونية تحتاج منا إلى عناء كبير في بيان مفهومها وحقيقة معناها، فهي كالكتابة التقليدية، حروف وكلمات ذات دلالات معينة تنتظم في عبارات ورموز وصور تعبر عن معنى محدد على وسيط إلكتروني، وبالتالي يصبح الباب مفتوحا أمام قبول كل الدعامات أيا كانت مادة صنعها في عملية الإثبات القانوني، بالتالي أدى ذلك إلى إعادة النظر في مفهوم الكتابة، فلقد تطرق جانب من الفقه إلى تعريف الكتابة الإلكترونية وتوضيح معناها، أما التشريعات المقارنة فلقد اختلفت وتباينت في تعريف الكتابة الإلكترونية، وعلى هذا الأساس سنتناول التعريف الفقهي أولا، ثم التعريف الإتفاقي ثانيا.

أولا: التعريف الفقهي للكتابة الالكترونية

حاول بعض الفقهاء تعريف الكتابة الالكترونية كما يلي: **" كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك"**[1]، فالكتابة لا تتعدى كونها رموزا تعبر عن الفكر والقول ولا يشترط لفهم هذا التعبير استناده إلى وسيط معين، فالعبرة هي في قدرة الوسيط على نقل رموز الكتابة وبالتالي الاعتداد بها[2].

ثانيا: تعريف الكتابة الالكترونية في المواثيق الدولية والتشريعات الوطنية

تتبنى العديد من الاتفاقيات الدولية فكرة أن الكتابة الالكترونية يمكن أن تكون على دعامات متعددة ولا تقتصر في مفهوم وجودها على الورق، ومن الأمثلة على تلك الاتفاقيات الدولية:[3]

[1] - لورنس محمد عبيدات، مرجع سابق، ص.79.

[2] - محمد إبراهيم أبو الهيجاء، عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص.62.

[3] - عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، مرجع سابق، ص.253.

1 ـ **اتفاقية نيويورك بشأن التقادم في البيوع الدولية للبضائع لعام 1972** : وتشير هذه الاتفاقية في المادة 09 منها على أن مصطلح الكتابة ينصرف أيضا إلى المراسلات الموجهة في شكل برقية أو تلكس .

2 ـ اتفاقية الأمم المتحدة الموقعة في فيينا بشأن النقل الدولي للبضائع لعام 1981:

حيث تقضي المادة 13 منها على أن مصطلح الكتابة ينصرف إلى المراسلات الموجهة في شكل برقية أو تلكس.

3 ـ قانون الأونسترال بشأن التجارة الإلكترونية لسنة 1996:

لم يعرف قانون الأونسترال الكتابة الالكترونية وإنما عرف المحرر الالكتروني والذي عبرت عنه بمصطلح رسالة البيانات، ويظهر ذلك من خلال المادة 02/ أ " **يراد بمصطلح رسالة البيانات المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية، أو البريد الالكتروني، أو البرق، أو التلكس، أو النسخ البرقي"**[1].

4 ـ القانون الفرنسي:

يعتبر التشريع الفرنسي من الأوائل في تبني نظام المعاملات الالكترونية، وهذا ما انعكس ايجابيا على منظومتها التشريعية، إذ أن مجلس الدولة الفرنسي قد أشار على الحكومة في أحد تقاريره على تعديل قواعد الإثبات لتتلاءم والتطور التكنولوجي الراهن[2].

تم بالتالي تعديل القانون المدني في سنة 2000 خاصة ما يتعلق بمجال الإثبات وأعاد صياغة مفهوم الإثبات بالكتابة كمفهوم عصري حديث، إذ تنص المادة 1316 من التقنين المدني على أنه: " **الدليل الخطي أو الدليل الكتابي، ينتج عن تتابع حروف ، خصائص، أرقام أو أي**

[1]ـ المادة 02/أ من قانون الأونسترال النموذجي بشأن التجارة الالكترونية لسنة 1996، على موقع:
https://www.uncitral.org/pdf/arabic/texts/electcom/ml-ecomm-a_ebook.pdf

[2]ـ رحيمة صغير ساعد نمديلي ، العقد الإداري، دار الجمعة الجديدة، الإسكندرية، 2007، ص. 143

علامات أو رموز أخرى لها معنى واضح، مهما كانت الوسيلة التي تتضمنها أو طريقة إرسالها"، فكرس المشرع الفرنسي مبدأ عاما وهو عدم التمييز بين المحرر المعد للإثبات من حيث الطريقة المستعملة في تداولهن أو الطريقة التي استخدمت في إنشائه[1].

نلاحظ أن المشرع الفرنسي ومن خلال التعريف الواسع للأدلة الكتابية قد فصل بين مفهوم الكتابة والوسيلة التي تتضمن هذه الكتابة، فالتعريف إذن جاء موضوعيا مهتما بوظيفة الكتابة بغض النظر عن الوعاء الذي تتضمنه هذه الكتابة، فالمهم قيام الكتابة بأداء المهام القانونية المناط بها دون أي قيد سوى ضرورة تعبير الكتابة عن فكرة مفهومة، معبرة وذات دلالة ممكنة للإدراك، فالعبرة إذن في تحديد المقصود بلفظ الكتابة ودورها والغرض منها.

5 ـ القانون المصري:

نص المشرع المصري في المادة 01 من توضيح للمصطلحات التقنية الحديثة، جاء في الفقرة 1" **الكتابة الالكترونية : كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك[2]"**.

نجد أن المشرع المصري اقتبس نص المادة 1316 من التقنين المدني الفرنسي وخالف التشريعات العربية المقارنة التي اعتمدت على قوانين الأونسترال، فأخذ بالمفهوم الواسع للكتابة سواء كانت بحروف مشفرة أو على شكل رموز وعلامات، فضلا عن إجازته أن يكون الوعاء الخارجي للكتابة الكترونيا أو ضوئيا أو بأي وسيلة أخرى، مما ترك الباب مفتوحا أمام أية وسيلة أخرى ستفرزها التكنولوجيات الحديثة مستقبلا.

[1] -Florence Mas, La conclusion des contrats du commerce électronique, PARIS , 2005, p 233.

[2] ـ المادة 01 من القانون المصري رقم 15- 2004 السالف الذكر.

6 ـ موقف المشرع الجزائري:

اعترف المشرع الجزائري بالكتابة كدليل إثبات حيث نصت المادة 323 مكرر أنه:" **ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها**"، كما ساوت المادة 323 مكرر بين الإثبات بالكتابة على الورق والإثبات بالكتابة في الشكل الالكتروني بشروط من خلال نصه على أنه " **يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها**"[1].

يعتبر نص المادة 323 مكرر من القانون المدني الجزائري، أول نص عرف من خلاله المشرع الجزائري الكتابة التي يمكن استعمالها كوسيلة إثبات التصرفات القانونية بما فيها التصرفات الالكترونية، وبهذا تحاشى المشرع الجزائري الجدل الذي قد يثور حول الاعتراف بالكتابة الالكترونية كدليل إثبات.

لم يقدم المشرع الجزائري رغم إقراره للإثبات بالكتابة إلا أنه أي تعريف يحدد معناها، كما لم يهتم بتحديد دعامة الكتابة، إلا أنه بالمقابل أخذ بالمفهوم الواسع للكتابة مهما كانت الوسيلة التي تضمنها، فهذا التعريف يستوعب أي وسيلة الكترونية قد تفرز عنها التكنولوجيا العلمية في المستقبل.

[1] ـ المادة 323 مكرر1 من التقنين المدني الجزائري.

الفرع الثاني
ضوابط الكتابة الالكترونية

أهم ما يميز الكتابة الالكترونية هي أن لها طبيعة خاصة تتم وتنفذ بأسلوب إلكتروني، فهي وسيلة من وسائل الإثبات ودليل من أدلتها سواء كانت بشكلها التقليدي أم الالكتروني، فالكتابة بجانب الدعامة المكتوبة عليها تكون المحرر الذي يعتبر وسيلة يتم توظيفها لإعداد دليل على وجود التصرف القانوني وتحديد مضمونه، فتناولتها معظم التشريعات الوطنية والدولية حيث أن أغلبها ساوى بينها وبين الكتابة الالكترونية واعترفت كدليل في الإثبات مثل الكتابة الورقية شريطة أن تعبر عن شخصية واضعيه، بالتالي يشترط في الكتابة الالكترونية ما يشترط في الكتابة العادية حتى تؤدي وظيفتها في الإثبات، ونظرا لاختلاف طبيعة الكتابة الالكترونية عن الكتابة التقليدية، فإن ثمة شروط يجب على الكتابة الالكترونية استيفائها لإضفاء الثقة والأمن فيها، وهذه الشروط تتمثل أساسا في قابلية الكتابة الالكترونية للقراءة والفهم **(أولا)**، أن تتصف الكتابة الالكترونية بالديمومة والثبات **(ثانيا)**، أن تكون غير قابلة للتعديل والتحوير **(ثالثا)**، وسنتناول هذه الشروط بالتفصيل كما يلي:

أولا : قابلية الكتابة الإلكترونية للقراءة والإدراك

يقصد بقابلية الكتابة الالكترونية للقراءة والإدراك، أن تكون المعلومات المدونة على المحرر بصفة خاصة أو المحرر بأكمله بصفة عامة، قد تم إنشاؤه بالشكل الذي يجعله قابلا للقراءة والإدراك، من قبل الإنسان في أي وقت، سواء عند إنشائه لأول مرة، أو عند الرجوع إليه بعد حفظه[1]، والمحررات الالكترونية على خلاف المحررات الورقية لا يمكن قراءتها وإدراك مضمونها بطريقة مباشرة، ويرجع ذلك إلى أن تدوينها يتم بلغة الحاسب الآلي، والتي لا يتمكن الإنسان من قراءتها بشكل مباشر، بل يمكنه ذلك بشكل غير مباشر، إما من خلال اللجوء إلى

[1] ـ محمد محمد سادات، حجية المحررات الالكترونية الموقعة الكترونيا في الإثبات، دار الجامعة الجديدة، الإسكندرية، 2011.، ص.199.

برامج الحاسب الآلي التي تتيح الاطلاع على الكتابة المخزنة على دعامة إلكترونية[1]، والتي بإمكانها ترجمة هذه اللغة التقنية إلى لغة يستوعبها الإنسان لتظهر على شاشة الحاسب الآلي، أو بعد استخراجها على أوراق مطبوعة كالمحرر الالكتروني الموجود على قرص مرن، فهو لا يمكن قراءته بمجرد النظر إلى القرص، بل لا بد من وضع الأخير في جهاز الحاسب الآلي، حتى نستطيع قراءة مضمون المحرر[2].

اهتمت التشريعات المختلفة التي تولت النص على المحررات الإلكترونية وتنظيمها بالتأكيد على هذا الشرط، وهذا الشرط نجده متوفر في الكتابة أو المحررات الالكترونية، وذلك على الرغم من أن لغة الكتابة في تلك المحررات والتي تعد بواسطة جهاز الحاسب الآلي هي لغة الآلة، إلا أن هذه اللغة من الممكن ترجمتها إلى اللغة التي يتحدث بها قارئها باستخدام جهاز الحاسب الآلي أيضا، وتكون مفهومة ومقروءة ويتوافر بها الشرط السابق[3]، غير أنه ليس ثمة ما يمنع أن تكون بلغة أخرى غير مفهومة للموجه إليه الخطاب، وفي هذه الحالة يمكن لصاحب الشأن أن يلجأ إلى الاستعانة بالترجمة حتى يتسنى له قراءة مضمون الكتابة [4].
هذا الشرط أكد عليه قانون الأونسترال النموذجي بشأن للتجارة الإلكترونية لعام1996 في المادة السادسة منه والذي نص على أنه: " **عندما يشترط القانون أن تكون المعلومات مكتوبة، فإن رسالة البيانات تستوفي ذلك الشرط إذا تيسر الاطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليه لاحقا** "[5]، فأخذ في سبيل تحقيق ذلك المبدأ بشروط الكتابة التقليدية وقررها على الكتابة الإلكترونية المكونة للمحرر الالكتروني، والمتمثلة في كون المحرر مقروءا وقابلا للإطلاع عليه.

اعترف المشرع المصري في القانون رقم 15 لسنة 2004 بالحجية القانونية للكتابة الالكترونية، فنص في المادة 15 من القانون على أنه: **" للكتابة الالكترونية وللمحررات**

[1] - R. Bisciari, Les contrats et la preuve dans l'environnement électronique, UGA, Bruxelles, 2004, p.138.

[2] - رحيمة الصغير ساعد نمديلي ، مرجع سابق، ص.82 . سامح عبد الواحد التهامي، التعاقد عبر الانترنت، مرجع سابق، ص.521.

[3] - زياد خليف العنزي، المشكلات القانونية لعقود التجارة الالكترونية، دار وائل للنشر والتوزيع،عمان، 2010، ص.38.

[4] - محمد عمار تيبار، مرجع سابق، ص.5.

[5] - المادة 06 من قانون التجارة الالكترونية بشأن للتجارة الالكترونية لسنة 1996.

الالكترونية في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون، ووفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون"[1].

يذهب رأي في الفقه المصري على نقد تعريف المشرع للكتابة الالكترونية، وذلك لأن العبرة في تحديد مدلول الكتابة ليس بقابليتها للإدراك، وإنما يكون لتعبيرها عن أفكار مترابطة، ذلك أن الحرف أو الرقم أو الرمز يتوافر فيه الإدراك، ولا يتوافر فيه المعنى المترابط، لذا فإن صياغة هذا التعريف منتقدة، وكان الأصح منها هو ما فعله المشرع الفرنسي بنص المادة 1316 من القانون الذي ورد فيه أن الكتابة تتضمن كل تدوين للحروف أو العلامات أو الأرقام أو أي إشارات أو رموز أخرى ذات دلالة تعبيرية مفهومة للآخرين أيا كان الوسيط أو الدعامة التي تقع عليه وأيا كانت طريقة نقله[2].

أقر المشرع الجزائري بهذا الشرط في نص المادة 232 مكرر من القانون المدني على أنه: **" ينتج الإثبات بالكتابة من تسلسل حروف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم"**، وأن عبارة "مفهوم" قصد منها المشرع إمكانية قراءته لأنه لا فهم دون قراءة لأمر مكتوب،[3] وهو تقريبا نفس المعنى الذي جاءت به المادة 1316 من التقنين المدني الفرنسي.

قام المشرع الفرنسي بإعادة صياغة مفهوم الإثبات بالكتابة كمفهوم عصري وهذا عند تعديله للتقنين المدني خاصة فيما يتعلق بمجال الإثبات، فنص في المادة 1316 من التقنين المدني الفرنسي على أن **:" ينشأ الإثبات الخطي، أو الإثبات بالكتابة من تتابع للحروف أو العلامات أو الأرقام أو أي رمز أو إشارة أخرى ذات دلالة مفهومة، أيا كانت دعامتها أو شكل إرسالها"**، فاشترط أن تكون الحروف أو الأشكال المكونة للدليل الذي سيقدم للإثبات أمام القضاء ذات دلالة مفهومة ومنطقية، فيجب تقديم الدليل الكتابي الالكتروني مقروءا للقاضي عن

[1] ـ المادة 15 من القانون رقم 15 لسنة 2004 .

[2] ـ أيمن عبد الله فكري، الجرائم الالكترونية،مكتبة القانون والاقتصاد، الرياض، 2015، ص.72.

[3]- حمودي ناصر، مرجع سابق، ص.242.

طريق معالجته بالوسائل التقنية المناسبة[1]، ويسري ذلك الأمر سواء على الدليل الإلكتروني أو الدليل الكتابي التقليدي، فهذا التعريف هو تعريف موضوعي، فهو لم يشر إلى الدعامة التي تتضمن الكتابة، وإنما حدد وظيفة الكتابة وهو تعبير الكتابة عن فكرة مفهومة ومعبرة وذات دلالة ممكنة للإدراك.

لم يختلف الأمر في القانون المصري للتوقيع الإلكتروني أو في لائحته التنفيذية وذلك في تعريف الكتابة الإلكترونية والتي عرفها بأنها **"عبارة عن حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك"**[2]، ومعنى القابلية للإدراك، أنه يمكن فهمها وإدراك معناها ، ولن يتسنى ذلك إلا إذا كان من الممكن قراءتها[3]

يلاحظ أن هذه النصوص تتفق على أنه تكون المعلومات المدونة على المحرر بشكل يمكن من قراءتها والإطلاع عليها في أي مرحلة كانت سواء عند إنشائها لأول مرة، أو عند استرجاعها بعد حفظ المحرر الإلكتروني.

يلاحظ مما سبق بأن شرط القراءة، وأمام تشكيك البعض في إمكانية نهوض الكتابة الإلكترونية بنفس مهمة ودور الكتابة الورقية التقليدية، من حيث إمكان الإطلاع عليها بقراءتها وفهم المراد منها، فإن التكنولوجيا الحديثة قدمت طرقا عديدة لإمكانية قراءة ما هو مدون إلكترونيا، لكل من يعرض عليه المحرر الإلكتروني وذلك أنه قد تم إيجاد برامج خاصة يجري تحميلها على جهاز الحاسب لتقوم بترجمة لغة الآلة إلى لغة الإنسان وهو ما يعني استيفائها للشرط المتعلق بإمكان القراءة والفهم[4]، طالما أن اللغة التي تظهر على الشاشة هي لغة مفهومة

[1]- أحمد شرف الدين، حجية المحررات الالكترونية في الإثبات، ورقة عمل مقدمة في ندوة المعاملات القانونية الالكترونية وعقود التجارة الالكترونية، المنعقدة في دبي، الإمارات العربية المتحدة، فيفري 2007، منشورات المنظمة العربية الإدارية ، 2008، ص.14.

[2]- محمد محمد سادات، حجية المحررات الالكترونية الموقعة الكترونيا في الإثبات، مرجع سابق، ص.198 .

[3] - محسن عبد الحميد إبراهيم البيه، مرجع سابق، ص.22.

[4]- عمر خالد زريقات، مرجع سابق، ص.216. محمد إبراهيم عرسان أبو الهيجاء ، التحكيم بواسطة الإنترنت، دار الثقافة، الأردن،2002، ص.76.

ومقروءة[1]، **وهذا ما أكدته** منظمة المواصفات العالمية[2]ISO بخصوص المواصفات الخاصة بالمحررات أن المحرر هو: **" مجموعة المعلومات والبيانات المدونة على دعامة مادية يسهل قراءتها هن طريق إنسان أو باستخدام آلة مخصصة لذلك، غير أن قيمة المحرر لا ترتبط بنوع معين من الدعامات التي تحمل عليها تلك المعلومات الموجودة به"**[3].

يعد هذا الشرط من الشروط الأولية التي يجب توافرها في كتابة المحرر، أي تكون معبرة وواضحة ومفهومة[4]، بحيث يمكن لصاحب الشأن الوصول إلى إدراك مضمون الكتابة وقراءته بسهولة ويسر، فالقراءة هي عملية فهم للنص، وتأويل له أيضا، وطريقة قراءة النص هي التي تحدد مفهوم النص، وبالتالي يمكن أن تقود قراءة النص إلى وضع سياق في المضمون بِدي بطريقة مختلفة إلى تغيير في العلاقة الدلالية للنص، لذلك يجب أن يكون المحرر الكتابي مدونا بحروف أو رموز مقروءة ومفهومة للشخص الذي يراد الاحتجاج عليه بمضمون هذا المحرر[5].

يتم تدوين المحررات الالكترونية على دعامات الكترونية لا يمكن أن يقرأها الشخص مباشرة دون أن يتم برمجة الحاسب الآلي ببرامج لها القدرة على ترجمة لغة الآلة إلى لغة يفهمها صاحب الشأن في ذلك.

ب ـ شرط ديمومة الكتابة الالكترونية وإمكانية استرجاعها:

يجب أن تحظى الكتابة بشرط الاستمرارية وإمكانية استرجاعها وهذا لن يتحقق إلا إذا أوجدت وحررت الكتابة على دعامة مستقرة كالورق مثلا، حيث تسمح لأطراف العلاقة

[1] ـ حسن عبد الباسط جميعي، مرجع سابق، ص. 19. صفاء فتوح جمعة، مرجع سابق، ص.127.

[2] ـ هي مختصر لكلمة "International Organization for Standardization" " وهي اتحاد عالمي مقره في جنيف ويظم ، وهي سلسلة من المواصفات والمقاييس المعتمدة عالميا وتستخدم في توكيد جودة العمليات والنشاطات، هذه المواصفات تقدم الشهادة على ممارسة لنظام إدارة الجودة والذي يطبق على العمليات والأنشطة المختلفة في المؤسسة، وليس على المنتج أو الخدمة نفسها، على الموقع: www.konan3.93arabyate.net

[3] ـ مشار إليه لدى: عبد الفتاح بيومي حجازي، الحكومة الالكترونية، دار الكتب القانونية، مصر، 2007، ص.192.

[4] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.47.

[5] ـ حسن عبد الباسط جميعي، مرجع سابق، ص.201.، الصالحين محمد العيش، الكتابة الرقمية طريقا للتعبير عن الإرادة ودليلا للإثبات، منشأة المعارف، الإسكندرية، 2008، ص.165.

الرجوع إليها[1]، أما بالنسبة للوسائط الالكترونية فهي تتسم بدرجة حساسية عالية، بالتالي فإنه في حالة اختلاف شدة التيار الكهربائي أو الاختلاف الشديد في درجة حرارة تخزين هذه الوسائط، فإن هذا يؤدي إلى حدوث تلف بتلك الوسائط الالكترونية، ويترتب على ذلك عدم تحقق شرط الاستمرارية، إلا أنه في وقتنا الراهن فقد تم التغلب على ذلك باستخدام وسائط إلكترونية متطورة يتحقق فيها عنصر الثبات والاستمرارية بالنسبة لما دون عليها، حيث يمكن الاحتفاظ بتلك المعلومات لمدة طويلة ربما تفوق قدرة الأوراق، التي تتأثر هي الأخرى بعوامل الزمن، أو الحريق أو الرطوبة أو الحشرات[2]، فحفظ الوثيقة الالكترونية على حامل إلكتروني يتيح الاطلاع على محتواها طيلة مدة صلاحيتها، وحفظها بشكلها النهائي بصفة تضمن سلامته محتواها، وحفظ المعلومات الخاصة بمصدرها، ووجهتها وكذلك تاريخ ومكان إرسالها واستلامها"[3].

أشار قانون الأونسترال النموذجي للتجارة الالكترونية على هذا الشرط وهذا في المادة 1/10أ بنصها على أن : **" الاطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا"**، بالإضافة إلى ذلك نص في المادة 6 من نفس القانون صراحة على هذا الشرط في أنه: **" عندما يشترط القانون أن تكون المعلومة مكتوبة ، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا"**.

نص المشرع الفرنسي على هذا الشرط في المادة 1/1316 من التقنين المدني وهو أن يكون تدوين الكتابة وحفظها قد تم في ظروف ذات طبيعة تضمن تكاملها[4].

نص المشرع على هذا الشرط فيا لمادة 323 مكرر 1 في تعديله الأخير للتقنين المدني بأنه**: " وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"**، فقد أوجب المشرع ضرورة الحفظ

[1] - محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.82.

[2] - أيمن مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته، دار الجامعة الجديدة ، الإسكندرية، 2008، ص.194.

[3] - عصام عبد الفتاح مطر، التحكيم الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2009، ص. 45.

[4] - Article 1316 -1du C.C.F. dispose que: *« …**sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*.

لإمكانية الاسترجاع من أجل الحفاظ على المراكز القانونية للأطراف المتعاقدة الكترونيان طالما أن المعلومات الواردة فيه تدل على من أنشأه ،أو تسلمه وتاريخ إرساله وتسلمه.

نص القانون الأردني في المادة 08 بأنه **"إذا استوجب القانون الاحتفاظ بمستند لأي سبب، فيعتبر الاحتفاظ به على شكل سجل إلكتروني منتجا لآثاره على أن تتوافر فيه الشروط المنصوص عليها في المادة 07 من هذا القانون"**[1].

نص على ذلك أيضا قانون إمارة دبي وذلك في المادة (1/8/ب) بأن **"بقاء المعلومات محفوظة على نحو يتيح استخدامها و الرجوع إليها لاحقا"**[2].

ج ـ شرط الثبات أو عدم قابلية الكتابة للتعديل:

يقصد ثبات أو عدم قابلية الكتابة للتعديل، حفظ المحرر الالكتروني دون أدنى تعديل أو تغيير من حذف أو محو أو حشو، ليتسنى بعد ذلك الاعتداد بالمحرر المكتوب، إذ أن قدرة المحرر في الإثبات تعتمد على مدى سلامته من أي عيب قد يؤثر في شكله الخارجي.

تثير إمكانية التلاعب وتغيير الكتابة الالكترونية صعوبة كثيرة على مستوى التصرفات والمعاملات الإلكترونية التي تتم بواسطة المحررات الإلكترونية، فإمكانية تعديل النصوص أو حتى محوها عن طريق الإمكانيات المتعددة لبرامج معالجة النصوص، شكلت خطرا حقيقيا فيما يتعلق بالتحري عن المعنى أو عن الحقيقة التي يرغب المتعاقدون في التعبير عنها عن طريق الكتابة[3]، فيمكن أن يتم تحريف كل أو بعض تلك المعلومات دون أن يترك ذلك أثرا ملحوظا حتى أنه يمكن أن يتم حذف معلومات المحرر كلها أو بعضها بسبب الخلل التقني في الأجهزة المستعملة التي تهدد سلامة تخزين المعلومات، أو بفعل فاعل مثل إطلاق الفيروس عن البرنامج

[1] - قانون المعاملات الإلكترونية الأردني رقم15 لسنة2015 على الموقع:http://www.cbj.gov.jo/

[2] - القانون الإماراتي رقم02 لسنة2002 بشأن المعاملات والتجارة الإلكترونية على الموقع:
http://www.aidmo.org/etl/index.php?option=com_docman&It

[3]- تامر محمد سليمان الدمياطي، إثبات التعاقد الالكتروني عبر الانترنت، رسالة لنيل شهادة دكتوراه في الحقوق، كلية الحقوق،قسم القانون المدني، جامعة عين شمس، 2008 ، ص.225.

المعلوماتي لاختراقه أو لتدميره[1]، فهو يشكل تهديدا وخطرا حقيقيا فيما يتعلق بالتحري عن المعنى الحقيقي الذي يتضمنه المحرر الالكتروني، لكن في الوقت الحالي أصبح ذلك متجاوزا وهذا راجع إلى التقنيات المتطورة التي تكفل سلامة المحرر الإلكتروني ضد المخاطر وذلك باستخدام تقنيات التوقيع الالكتروني المعتمد على نظام التشفير.

نصت المادة 1/10/ب من قانون الأونسترال النموذجي بشان التجارة الالكترونية لسنة1996 بأنه:" **الاحتفاظ برسالة البيانات بالشكل الذي أنشأت أو أرسلت أو استلمت به، أو بشكل يمكن إثبات أن يمثل بدقة المعلومات التي أنشأت أو أرسلت أو استلمت[2]**"، وهو ما نص عليه أيضا المشرع الجزائري في المادة 323 مكرر1 من القانون المدني بالنص: "**.. في ظروف تضمن سلامتها**"[3].

تتميز كتابة المحرر الورقي بالكفاءة في منع الغير من تعديلها، نظرا أن تدوينها بالأحبار يتصل مباشرة بتركيبة الورقة الكيميائية[4]، ويتم تدوينها على وسيط يسمح بثبات الكتابة عليه واستمرارها ومن هنا لا يمكن فصلها إلا إذا طرأت عليها تعديلات، يسهل التعرف عليها من طرف الخبرة بسبب الآثار المادية التي تمكن القاضي من تقدير مدى تأثيرها على قيمة المحرر في الإثبات[5]، فمما لا شك فيه أن خاصية عدم القابلية للتعديل متوافرة في المحرر الكتابي الورقي، حيث تجرى الكتابة عليه بواسطة الأحبار التي يتشربها الورق، أو تنطبع عليه بشكل يؤدي إلى التصاقها كيميائيا بالتركيب المادي لهذه الأوراق، فلا يمكن فصلها إلا بإتلاف هذه

[1]- سمير حامد عبد العزيز الجمال، مرجع سابق، ص.200. محمد حسين منصور، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص.271.

[2] - المادة 1/10/ب من قانون الأونسترال النموذجي بشأن التجارة الالكترونية لسنة 1996.

[3] - المادة 323 مكرر 1 من القانون المدني الجزائري.

[4] - حسن عبد الباسط جميعي، مرجع سابق، ص.23.

[5] - محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.49.

الأوراق أو إحداث تغييرات مادية فيها سواء بالإضافة أو المحو، ولذا يسهل اكتشافها بالمناظرة بالعين المجردة، أو من خلال الاستعانة بالخبرة[1].

تقوم أيضا الكتابة في المحررات الالكترونية حتى يعتد بها في الإثبات كدليل كامل على شرط الثبات، بمعنى أن تسمح الدعامة المدونة عليها بثباتها والإبقاء عليها وحفظها كما هي، وبصورة مستمرة، لكي يتسنى الرجوع إليها عند الحاجة، لكن لا يعني ذلك أن تستمر الدعامة للأبد، وإنما يجب أن تدوم الكتابة المدة اللازمة لانقضاء الالتزام بالتقادم، ولكن هذه الخاصية لا تتوافر في الكتابة الإلكترونية، لأن الدعائم الإلكترونية بوجه عام تتسم بالحساسية الشديدة[2]، مما يجعلها عرضة للتلف وتدمير ما عليها من بيانات ومعلومات، سواء لأسباب فنية بحثه كسوء التخزين أو حدوث أعطال، أو بسبب مخاطر الخطأ الفني في إدخال البيانات وتصميم البرامج أو عند نقل المعلومة من دعامة إلى أخرى، ولعل أهم هذه المخاطر إطلاق الفيروس المعلوماتي على البرامج لإتلافها والنيل منها[3].

نجد أن هناك أنواعا عديدة من المحررات التي يمكن محو كتابتها بصورة إرادية، ولعل من أوضح الأمثلة عليها هو تلك المحررات المكتوبة بقلم الرصاص، فهذه لم تمنع قابلية محو كتابتها من اعتبارها محررات ذات حجية تامة في الإثبات، أما فيما يتصل بالتغيير غير الإرادي المتولد بفعل الزمن فلا شك أن قدرة المحررات الإلكترونية على تجاوزه وحفظ الكتابة، هي أكبر بكثير من قدرة المحررات الورقية التي تكون أقصر عمرا من المحررات الإلكترونية[4].

لا تمثل الخصائص المادية للوسيط الالكتروني عقبة في سبيل تحقق هذا الشرط، ذلك أن التكوين المادي للشرائح الممغنطة وأقراص التسجيل المستخدمة في التعاقد عن طريق شبكة الاتصالات الالكترونية تتميز بقدرة كبيرة على الاحتفاظ بالمعلومات المثبتة عليها بكفاءة أعلة

[1] - عبد العزيز المرسي حمود، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة ، مجلة البحوث القانونية والاقتصادية ، كلية الحقوق، جامعة المنوفية، العدد21، السنة11، أفريل2002، ص.27.

[2] - سمير حامد عبد العزيز الجمال، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية و التجارية في ضوء قواعد الإثبات النافذة، مرجع سابق، ص.200.

[3] - محمد حسين منصور، الإثبات التقليدي والالكتروني، مرجع سابق، ص.271.

[4] - نبيل مهدي زوين ، مرجع سابق، ص.10 .

من الأوراق العادية التي تتأثر هي الأخرى بعوامل الزمن وقد تتآكل بفعل الرطوبة نتيجة لسوء التخزين[1].

يلاحظ أن أغلب التشريعات المقارنة اشترطت أن يحقق الحفظ إمكانية استرجاع البيانات الموجودة في المحرر الإلكتروني في الصورة التي أنشئت بها لأول مرة، ففي هذه الحالة نجد أن توافرها على الشبكة يحقق فاعلية أكثر بطريقة تمكن من استرجاع هذه البيانات من خلال أي جهاز إلكتروني يمكن ربطه على الشبكة، أما في حال حفظه على قرص صلب أو مرن فإنه يتوجب ربط هذه الأقراص ليتمكن المستخدم من استرجاع هذه البيانات وهذا التصرف يحقق الفعالية المباشرة و السرعة المرجوة في التعامل من خلال الشبكة[2].

[1] - حسن عبد الباسط جميعي، مرجع سابق، ص.24 .

[2] - لورنس محمد عبيدات، مرجع سابق، ص.86 .

المطلب الثاني

التوقيع الالكتروني

يعد التوقيع الإلكتروني العنصر الأهم والأبرز من عناصر المحرر الإلكتروني باعتباره العنصر الذي يؤكد نسبة ما ورد فيه لأطرافه، فإذا كانت الكتابة الإلكترونية تقوم بذات الدور الذي تؤديه الكتابة التقليدية، فإن التوقيع الإلكتروني أصبح الآن يزاحم التوقيع اليدوي في ذات وظيفته، فهو يساهم في تأمين سلامة المحررات الإلكتروني والحفاظ على سرية مضمونها والتحقق من صحتها من الإطلاع عليه أو أي تعديل أو تحريف، لذلك توالت التشريعات المقارنة إلى الاعتراف بمشروعيته ومساواته بالتوقيع التقليدي، وعليه نجد أن أغليها لا تشترط اقتران كل محرر الكتروني بالتوقيع الالكتروني إلا إذا نص القانون على ذلك في تصرفات معينة يحددها، فعدم اقتران التوقيع الالكتروني بالمحرر الالكتروني لا يترتب على ذلك فقدان آثاره القانونية.

يتفوق التوقيع الالكتروني على التوقيع التقليدي من حيث الوظيفة والهدف، بالتالي لا مجال للانتظار حتى ينشب النزاع للبحث في مدى صحة المحرر الالكتروني الموقع إلكترونيا كما هو الشأن بصدد المحررات الموقعة بخط اليد، ويعود ذلك على ما توفره التقنية الحديثة المستخدمة في تأمين التوقيع الإلكتروني عن طريق ما يسمى نظام المعاملات الالكترونية الآمنة، وتتعدد وتتنوع صور التوقيع الالكتروني ولعل أهم الأنواع المعروفة حتى الآن والتي توصلت التكنولوجيا المتطورة إليها تتمثل في: التوقيع الرقمي، التوقيع بالقلم الالكتروني، التوقيع بالرقم السري، والتوقيع البيومتري، ولا يعني ذلك الاقتصار على هذه الأشكال والصور فقط بل يمكن أن يظهر في أي وقت شكلا جديدا للتوقيع الالكتروني ما دام أن ذلك الشكل يحقق الغاية والهدف المقصود منه ويكون على درجة عالية من الثقة والأمان، **(الفرع الأول).**

حتى يمكن مساواة التوقيع الالكتروني من حيث الحجية مع التوقيع التقليدي لا بد من وضع ضوابط فنية تضمن قيام التوقيع الالكتروني بمهمته في الإثبات، لذلك يستلزم بيان مدى تحقيق التوقيع الالكتروني للوظيفة والثقة التي تستند عليها أغلب التشريعات المقارنة التي منحت

الحجية القانونية له، في مدى قدرته على أداء هذه الوظائف والتي تتمثل أساسا في تحديد هوية الشخص الذي أصدره، مدى قدرته في التعبير عن إرادة موقعه بالالتزام بمضمون المحرر، ومدى تحقيقه لسلامة المحرر عند وضع التوقيع عليه، **(الفرع الثاني)**.

الفرع الأول

تحديد مفهوم التوقيع في الشكل الالكتروني

أصبح لزاما على النظم القانونية القائمة خاصة مع نمو المعاملات الالكترونية في السنوات الأخيرة، وضع القواعد التي تكفل قبول التوقيع الالكتروني وإثبات صحته على هذه المعاملات وحجيتها القانونية، خاصة في ظل سهولة تعديل بيانات المحررات الالكترونية، وإمكان إنكار بعض الأطراف لعلاقتهم بهذه المعاملات، وكحل يتفق مع الطبيعة التقنية لهذه التطورات، استخدمت تقنية التوقيع الالكتروني، بالتالي سنتطرق إلى تعريف التوقيع الالكتروني **(أولا)**، ثم إلى صوره **(ثانيا)**.

أولا: تعريف التوقيع الالكتروني

يعتبر التوقيع شرط جوهري للمحرر الالكتروني لأنه هو الذي ينسب الكتابة إلى صاحب التوقيع، ونظرا لأهمية التوقيع الالكتروني بالنسبة للمحرر الالكتروني فإن بعض الفقه اختلف في وضع تعريف جامع مانع للتوقيع الالكتروني، كما لا يوجد في الواقع تعريفا قانونيا جامعا شاملا للتوقيع الالكتروني سواء في التشريعات الوطنية أو الدولية.

1 ـ تعريف لتوقيع الالكتروني في الفقه :

اختلف الفقه في تعريفه للتوقيع الالكتروني وفي تحديد المقصود منه، ومن بين التعريفات الفقهية تلك التي حاول أصحابها الجمع بين التعريف التقني للتوقيع الالكتروني بمعنى التعريف الذي يرتكز على الوسائل التقنية التي يقوم عليها التوقيع الالكتروني، والتعريف الوظيفي الذي يرتكز على الوظائف التي يقوم بها التوقيع.

عرف بعض الفقه التوقيع الالكتروني بأنه :" **تعبير شخص عن إرادته في الالتزام بتصرف قانوني معين عن طريق تكوينه لرموز سرية يعلمها هو وحده تسمح بتحديد هويته**"[1].

عرفه البعض الآخر بأنه**: " بيان مكتوب في شكل الكتروني يتمثل في حرف أو رقم أو إشارة أو صوت أو شفرة خاصة ومميزة من إتباع وسيلة آمنة وهذا البيان يلحق أو يربط منطقيا ببيانات المحرر الالكتروني للدالة على هوية الموقع على المحرر والرضاء بمضمونه"**[2] .

يركز هذا التعريف على ضرورة قيام التوقيع الالكتروني بالوظائف التقليدية له، وهي تمييز هوية الشخص والتعبير عن رضائه الارتباط بالتصرف القانوني، لكنه لا يغفل إصدار التوقيع الالكتروني وتوثيقه، والتي ما يتولاها شخص مرخص له من الجهات المختصة بذلك، وهذه الإجراءات تضمن أن يخص التوقيع صاحبة وحده دون غيره، كذلك تضمن عدم السطو عليه، وأيضا تضمن عدم تعديل أو المساس بالبيانات الموقع فيها.

نميل من جهتنا إلى تفضيل التعريف الذي يركز على الجانب الوظيفي دون الجانب التقني، فالتعريف الوظيفي يقوم على أساس وظائف التوقيع وهي ثابتة، على عكس التعريف التقني الذي ينظر إليه على أنه لا يمكن من خلاله حصر صور التوقيع التي تكون قابلة للتطور، لذلك نتفق مع من يذهب إلى تعريف التوقيع الالكتروني على أنه مجموعة من الإجراءات التقنية يمكن من خلالها تحديد شخصية من يصدر عنه هذه الإجراءات، وقبول بمضمون التصرف الذي يصدر التوقيع بشأنه.

---

[1] ـ مشار إليه لدى: محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، مصر،2003، ص.179.أبو هبة نجوى، التوقيع الالكتروني، دار النهضة العربية، القاهرة، 2002، ص.41،. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، عمان، 2009، ص.55.

[2] ـ مشار إليه لدى: أبو زيد محمد محمد، تحديث قانون الإثبات، مكانة المحررات الالكترونية بين الأدلة الكتابية، دار النشر، 2002، ص171.

2 ـ تعريف التوقيع الالكتروني في المواثيق الدولية والتشريعات الوطنية:

تعددت التشريعات التي تناولت التوقيع الإلكتروني والتي قامت بوضع تعريف له، فسنتعرض أولا إلى تعريف التوقيع الإلكتروني في المواثيق الدولية أولا ثم إلى التعريف الذي قدمته التشريعات الوطنية على النحو التالي:

أ- تعريف التوقيع الالكتروني في المواثيق الدولية:

اهتمت التشريعات الدولية بالتوقيع الإلكتروني لما له من دور كبير في إثبات إقرار الموقع بما ورد في مضمون المحرر، فقد تعددت التعريفات القانونية التي تناولت التوقيع الإلكتروني، حيث أوضحت بعض هذه التعريفات الطبيعة الإلكترونية للتوقيع الإلكتروني وبينت الدور الوظيفي الذي يقوم به.

1 ـ تعريف التوقيع الالكتروني في القانون النموذجي للتجارة الالكترونية الدولية لسنة 1996:

عرف القانون النموذجي للتجارة الالكتروني لسنة 1996 التوقيع الالكتروني في المادة السابعة على أنه:" **عندما يشترط القانون وجود توقيع من شخص يستوي ذلك الشرط بالنسبة إلى رسالة البيانات إذا :**

- استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

- كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف ن بما في ذلك أي إنفاق متصل بالأمر"[1].

ركز هذا التعريف على ضرورة قيام التوقيع الالكتروني بالوظائف التقليدية للتوقيع وهي تمييز هوية الشخص، والتعبير عن رضائه الارتباط بالعمل القانوني، على نحو ما ورد في

[1] ـ المادة 07 من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996.

الفقرة (أ)، كما ركز أيضا على أنه يتعين أن تكون طريقة التوقيع الالكتروني والواردة في الفقرة (ب) طريقا موثوقا به، ولم يحدد تلك الطرق أو الإجراءات التي يتعين إتباعها، وإنما فتح المجال لكل دولة تحددها بطريقتها المناسبة ووفقا لتشريعها.

أورد قانون الأونسترال تعريفا للتوقيعات الالكترونية لسنة 2001 في نص المادة02 بأن التوقيع الالكتروني المؤمن هو: " **بيانات في شكل إلكتروني مدرجة في رسالة بيانات ، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ن ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات**"[1].

وفقا لهذا التعريف فالتوقيع الالكتروني المؤمن هو الذي يستوفي الشروط التالية:

ـ أن تكون بيانات إنشاء التوقيع الالكتروني مرتبطة في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر.

ـ أن تكون بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.

ـ أن يكون أي تغيير في التوقيع الالكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف.

ـ أن يكون الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع، وأي تغيير في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف.

حدد هذا التعريف مسألتين مهمتين تتمثلان في هوية الشخص الموقع وبيان موافقته على المعلومات الواردة في المحرر، وهو بذلك أكد على شخص الموقع بالموافقة على التزامه بما وقع عليه، كما وضع هذا النص من خلال تعريفه للتوقيع الالكتروني المؤمن ضوابط أشد صرامة من التوقيع الالكتروني العادي، كما يتضح جليا من خلال هذا التعريف أن قانون الأونسترال لم يحدد الطريقة أو التقنية التي يتم بها استخدام التوقيع الالكتروني فاتحا المجال أمام أية تقنية للدلالة على هوية الموقع وإبراز نيته في الالتزام بمضمون المحرر.

[1]ـ المادة 02 من قانون الأونسترال بشأن التوقيعات الإلكترونية لسنة 2001.

2 - تعريف التوقيع الالكتروني في التوجيه الأوروبي رقم 1999/93:

عرف التوجيه الأوربي التوقيع الالكتروني في المادة 1/2 بأنه: "**عبارة عن معطيات ذات شكل الكتروني مرتبطة أو مدرجة بمعطيات الكترونية أخرى التي يمكنها أن تقوم بوظيفة التعريف**"[1].

أصدر الاتحاد الأوربي أيضا في عام 1999 توجيها حول التوقيع الإلكتروني، فعرفه في المادة (8) بأنه: "**معلومة في شكل إلكتروني تقرن أو تربط منطقيا بمعلومات أخرى الكترونية تستخدم كوسيلة توثيق**"[2]، فالتوجيه الأوروبي اعتبر التوقيع وسيلة تكنولوجية تحقق الأمن المعلوماتي وهو تعريف تقني، كما فرق التوجيه بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم، والذي نص في المادة (2/2) منه: "**التوقيع الإلكتروني المتقدم يراعي المتطلبات الآتية:**

1- أن يكون مرتبطا فقط بالموقع ويسمح بتحديد هوية الموقع.

2- أن ينشأ بوسائل يستطيع الموقع من خلالها الاحتفاظ به، وإبقائه تحت سيطرته الحصرية.

3- أن يكون مرتبطا بالمعطيات المحتواة في الرسالة، بشكل يمكن اكتشاف كل تعديل لاحق على هذه المعطيات"[3].

ميز التوجيه الأوروبي المذكور بين نوعين من التوقيع ،التوقيع الالكتروني المقدم أو المؤمن والتوقيع الالكتروني البسيط أو العادي، فالتوقيع الالكتروني المؤمن هو الذي يكون معتمدا من

---

[1] - Article 2 /1 du Directive 1999/93LCE , dispose que : « ***signature électronique, une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autre données électroniques et qui sert de méthode d'authentification*** » ,sur le site : https://eur-lex.europa.eu.

[2] - Article 08 du Directive 1999/93LCE, dispose que : ***« Une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électronique et qui sert de méthode d'authentification*** ».

[3] -Article 2/2 du Directive 1999/93LCE dispose que : ***« signature électronique avancée , une signature électronique qui satisfait aux exigences suivantes : être liée uniquement au signataire, permettre d'identifier le signataire, être crée par des moyens que le signataire puisse garder sous son contrôle exclusif, être liée aux données auxquelles elle se rapporte de telle sorte que toutes modification ultérieure des données soit détectable »***.

أحد مقدمي خدمات التصديق الالكتروني، والذي يمنح شهادة تفيد صحة هذا التوقيع، بعد التحقق من نسبة التوقيع إلى صاحبه، ويتمتع هذا التوقيع بالحجية القانونية الكاملة في الإثبات إذا توفر على شروط معينة وفقا للمادة 02/02 من التوجيه الأوروبي السالف ذكره وهي: أن يرتبط التوقيع بشخص الموقع حصرا، أن يكون قد أنشئ بوسائل تبقى تحت رقابة الموقع الحصرية، وأن يرتبط التوقيع بالبيانات التي يحيل إليها على نحو يسمح بكشف كل تعديل لاحق عليها.

يلاحظ من خلال هذه النصوص أن التوجيه الأوربي منح للتوقيع المتقدم حجية أكبر من حيث الاعتراف الكامل بحجيته أمام القضاء، بالمقارنة بحجية التوقيع الإلكتروني البسيط، والذي يتمتع بالحجية القانونية في حالة عدم إنكاره، أما في حالة إنكاره فيقع على عاتق من أدلى به إقامة الدليل على أنه قد تم بطريقة تقنية موثوق بها[1]، كما أنه اعترف بالتوقيع العادي لكن بدرجة أقل من التوقيع المتقدم من حيث الحجية القانونية في الإثبات[2]، فميز هذا التوجيه بين التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم، ويتطلب التوجيه الأوربي في التوقيع الإلكتروني المتقدم عددا من الشروط الخاصة بضمان الأمان والثقة، والتي لا تعتبر مطلوبة في حال ذلك التوقيع الإلكتروني البسيط، فالتوقيع الالكتروني البسيط يلبي الحد الأدنى من الاشتراطات اللازمة لإعطاء التوقيعات الالكترونية قيمة قانونية.

3 ـ تعريف التوقيع الالكتروني في القانون العربي الاسترشادي للإثبات بالطرق الحديثة:

عرف هذا القانون الذي تبنته الجامعة العربية وصادق عليه مجلس الوزراء العدل العرب بموجب القرار رقم24د/771 المؤرخ في 27 نوفمبر 2008، التوقيع الالكتروني في المادة03/1 بأنه: " **ما يوضع على محرر الكتروني ويتخذ شكل حروف، أرقام ، إشارات، أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره"**[3].

[1] ـ الياس ناصيف، العقد الالكتروني في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص.331.

[2] ـ برهم نضال إسماعيل، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2005، ص.171 .

[3] ـ نص القرار على الموقع الإلكتروني: https://www.carjj.org/legal-terms/4671/print

يؤخذ على هذا التعريف أنه عرف التوقيع الالكتروني تعريفا عاما بأنه ما يوضع على محرر الكتروني ولم يميز بين التوقيع الالكتروني المؤمن وبين التوقيع الالكتروني العادي، عكس التوجيه الأوروبي الذي ميز بينهما.

ب - تعريف التوقيع الالكتروني في التشريعات الوطنية:

تعددت التعاريف التي أعطيت للتوقيع الالكتروني بحسب النظم القانونية السائدة، فاهتمت العديد من التشريعات الوطنية الحديثة بمحاولة الإحاطة بكل ما يتعلق بمنظومته الالكترونية، لإثبات التصرفات القانونية التي تنشأ عبر وسائل الاتصال الحديثة حتى لا يكونوا أمام قصور تشريعي، مما دفع ببعض الدول إلى إزالة ما يواجه هذا المفهوم الجديد من مشكلات قانونية في مجال الإثبات، وتحديدا في مفهومه، وذلك بعدما فرض هذا النوع من التوقيع نفسه في ظل انتشار وازدهار التجارة الإلكترونية[1]، فمن بين هذه التشريعات المقارنة :

1 - القانون الأمريكي:

نصت المادة 101 من التشريع الفدرالي الأمريكي بشأن التوقيعات الالكترونية لعام2000 على أنه" **رغما عن أي تنظيم أو قانون لأية ولاية أو أية قاعدة قانونية في أي قانون في أي معاملات مالية ، سواء في داخل الولايات أو ف ي التجارة الأجنبية ، يجب مراعاة أنه عقد خاص بالمعاملات المالية، لا ينكر أثره أو حجيته أو قابليته للتنفيذ بسبب استخدام التوقيع الالكتروني في كتابته أو صياغته"**[2].

أورد أيضا تعريفان للتوقيع الإلكتروني:

الأول: في القانون الفدرالي للتوقيع الإلكتروني حيث جاء في المادة 8/108 من التوقيع الإلكتروني هو " **التوقيع الذي يصدر في شكل الكتروني، ويرتبط بسجل إلكتروني"**.

[1]- Arnaud-François fausse, La signature électronique transaction et confiance sur internet, DUNOD, Paris, 2001, p.87.

[2] - مشار إليه لدى: مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الإنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص: قانون الأعمال، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص.270.

الثاني: هو قانون المعاملات الإلكترونية الموحد الذي عرف في المادة 5/206 التوقيع الإلكتروني بأنه: **"صوت أو رمز أو إجراء يقع في شكل الكتروني يلحق بعقد أو سجل آخر ينفذ أو يصدر من شخص يقصد التوقيع على السجل"**[1]، ما يلاحظ في هذا القانون أنه حدد صورا للتوقيع الالكتروني بالتالي يفتح المجال أمام الاعتراف بجميع صور التوقيع الإلكترونية التي تتمتع بالثقة الكافية و تحقيق وضائق التوقيع، فاكتفى القانون الفدرالي بأن يكون التوقيع في شكل إلكتروني فقط أيا كان هذا الشكل[2].

يلاحظ أيضا أن التعريف أشار إلى بعض صور التوقيع الإلكتروني على سبيل المثال لا الحصر، فقد ذكر الأصوات والرموز، ثم فتح المجال أمام أية وسيلة أخرى تقع في شكل إلكتروني لتكون قادرة على تحقيق متطلبات التوقيع الإلكتروني، ومن ثم الاعتراف بها كوسيلة صالحة للتوقيع.

يلاحظ على هذا القانون أنه يطبق على التصرفات والتعاملات الالكترونية التي ينتمي أطرافها إلى ولايات مختلفة، وعلى التصرفات القانونية التي تتم مع أطراف أجنبية خارج الولايات المتحدة، يقر هذا النظام بحجية المحررات الالكترونية والتوقيعات الالكترونية في الإثبات ويتطلب هذا القانون الحصول على شهادة توثيق تثبت موافقة أو قبول جهة أخرى على ذلك التوقيع[3].

2 ـ القانون الفرنسي:

أدخل المشرع الفرنسي في نصوص الإثبات نصوصا جديدة، وما يلاحظ من خلالها، أنه لم يميز بين التوقيع الالكتروني العادي والتوقيع الالكتروني المؤمن، مع العلم أن نصوص التوجيه الأوروبي التي أوردناها سابق قد ميزت بين هاذين التوقيعين، لكن بعد ذلك ومع ارتبط فرنسا

[1] - مشار إليه لدى: أحمد شرف الدين، مرجع سابق، ص.293. الصالحين محمد العيش، مرجع سابق ، ص.11 .

[2]- THIEFFRY Patrick, commerce électronique, droit international et européen, LITEC, Paris, 2002, p.183.

[3] - فيصل سعيد الغريب، مرجع سابق، ص.256.

بدول الاتحاد الأوروبي والتزاما منها بتوجيهات التوجيه الأوربي، دفع مجلس الدولة الفرنسي إلى تعديل قوانينها تنفيذا للتوجيه الأوروبي الذي ألزم مجموعة الدول الأوروبية بتبني الإطار التشريعي الذي وضعته، فقد عرف التوقيع الإلكتروني وفقا للقانون 230/2000 الصادر بتاريخ13 مارس 2000 نص في المادة 2 /1 على أنه: **" إن التوقيع الرقمي يرتبط بالمعلومات التي يرغب المرسل في إرسالها إلى الطرف الآخر"**، فهذا التعريف ركز على وظائف التوقيع[1]، ولا يكون للتغييرات التي قد تحدث أية قيمة، وما نلاحظه هو نفس التعريف الذي جاء به التوجيه الأوروبي رقم 99/93 الصادر بتاريخ 1999/12/13 [2]، كما نصت المادة الجديدة 4/1316 من القانون المدني الفرنسي بأنه **: "التوقيع الضروري لإكمال التصرف القانوني، و التعريف بهوية صاحبه، و المعبر عن رضا الأطراف بالالتزامات الناشئة عنه"**[3].

كما نصت المادة 1316 فقرة 1 من القانون المتعلق بالتوقيع الالكتروني الفرنسي على أنه: **" تتمتع الكتابة الالكترونية بذات الحجية المعترف بها للمحررات الكتابية في الإثبات، شريطة أن يكون بالإمكان تحديد شخص مصدرها على وجه الدقة، وأن يكون تدوينها وحفظها قد تم في ظروف تدعوا إلى الثقة"**[4].

يلاحظ من خلال تعريف المشرع الفرنسي للتوقيع الإلكتروني بأنه عرفه من خلال وظيفته والمتمثلة في تحديد هوية صاحب التوقيع، والتعبير عن رضا هذا الشخص بمضمون المحرر وموافقته عليه واتجاه إرادته على الالتزام بمضمونه، بالتالي التوقيع في الأحكام القضائية

[1] - مشار غليه لدى: علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات، دار الثقافة، الأردن، 005 ، ص.27 .

[2] - باطلي غنية، حجية المستند الإلكتروني، المجلة الجزائرية للعلوم القانونية الاقتصادية والسياسية، جامعة الجزائر، كلية الحقوق، عدد3، سبتمبر 2011 ، ص.175 .

[3] - Article 1316-4 du C.C.F. relatif à la signature électronique, dispose que :*« **La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'oppose ,elle manifeste le consentement des parties aux obligations qui découlent de cet acte »***.

[4] - Article 1316/1 du C.C.F relatif à la signature électronique, dispose que : ***« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».***

الفرنسية يعد قانونيا، ويأخذ بكل توقيع باسم مستعار وبلقب ديني أو بالاسم الأول فقط[1]، أو بمجرد التأشير أو باستخدام علامة غير مقروءة ما دام من الثابت إسناده لشخص معين .

3 - القانون الأردني:

عرف المشرع الأردني التوقيع الإلكتروني في المادة 02 من قانون المعاملات الإلكتروني الأردني رقم 15 لسنة 2015 بأنه: **" البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو أية وسيلة أخرى مماثلة في السجل الإلكتروني، أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتمييزه عن غيره"**[2] .

يلاحظ أن المشرع الأردني عرف التوقيع الإلكتروني بأنه بيانات وحاول أن يبين أشكال هذه البيانات، فقد تكون عبارة عن حروف أو أرقام أو رموز أو إشارات أو غيرها، واشترط أن تكون هذه البيانات والمعلومات مدرجة في المحرر الإلكتروني وهو ما يعبر عنه بشرط اتصال التوقيع بالمحرر.[3]

د- القانون المصري:

عرف قانون التوقيع الإلكتروني المصري التوقيع الإلكتروني في المادة (1/ج) بأنه : **"ما يوضع على محرر إلكتروني، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره "**، وفقا للفقرة (ه) من نفس المادة، فإن الموقع هو **"الشخص الحائز على بيانات إنشاء التوقيع، ويوقع عن نفسه، أو عمن ينيبه أو يمثله قانونا"**.

[1] - ناهد فتحي الحمودي، الأوراق التجارية الإلكترونية، دار الثقافة، الأردن،2010، ص.80 .و: منير محمد الجنبيهي ، ممدوح محمد الجنبيهي، مرجع سابق ، ص.191

[2] - المادة 02 من قانون المعاملات الإلكترونية الأردني رقم15 لسنة 2015 على الموقع: http://www.cbj.gov.jo/

[3] - مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الانترنت، دار الكتب القانونية، مصر، 2010، ص.154.

نص المشرع المصري أيضا في المادة 18 من القانون 15- 04 ذاته على ثلاثة شروط حتى يكون التوقيع الالكتروني موثوقا منه كالآتي: **" يتمتع التوقيع الالكتروني والكتابة الالكترونية والمحررات الالكترونية بالحجية في الإثبات ،إذا ما توافرت فيها الشروط الآتية:**

ـ ارتباط التوقيع الالكتروني بالموقع وحده دون غيره.

ـ سيطرة الموقع وحده دون غيره على الوسيط الالكتروني.

ـ إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكتروني أو التوقيع الالكتروني"[1].

نلاحظ أن المشرع المصري عرف التوقيع الالكتروني تعريفا عاما بأنه ما يوضع على المحرر الالكتروني، كما عرف أيضا من خلال نص الفقرة ب من نص المادة على التوقيع الالكتروني المؤمن، أين ميز بينه وبين التوقيع الالكتروني العادي من خلال نصه على الشروط التي يجب أن يستوفي عليها التوقيع الالكتروني ليعتد به في الإثبات.

4 ـ موقف المشرع الجزائري:

عرف المشرع الجزائري وبموجب القانون رقم 15- 04 الخاص بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، التوقيع الالكتروني في مادته الثانية بأنه:" **بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة للتوثيق"**[2].

من خلال هذا التعريف نلاحظ أن المشرع الجزائري قد أخذ بتعريف قانون الأونسترال النموذجي مع تغيير طفيف في بعض العبارات والتي أراد منها أن هذه البيانات المرفقة والمرتبطة منطقيا هي في الأساس تستخدم لتوثيق هوية الموقع وبيان موافقته على مضمون ما وقع عليه، وهذا ما أكدت عليه المادة السادسة من نفس القانون بعبارة :**" يستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات مضمون الكتابة في الشكل الالكتروني"**[3].

[1] ـ قانون رقم 15- 2004 المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات، ج. ر عدد17، الصادرة في 22 أبريل سنة 2004، على موقع: http://www.tra.gov.eg/en/regulation/DocLib/Law-No-15-of-2004.pdf

[2] ـ المادة 02 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

[3] ـ المادة 06 من القانون ذاته.

كما فصل المشرع الجزائري في القانون 15- 04 لسنة 2015 في آلية إنشاء التوقيع الالكتروني من خلال تعريفه لكل من آلية وبيانات إنشاء التوقيع الالكتروني، حيث عرفت المادة 03/02 بيانات إنشاء التوقيع الالكتروني على أنها:" **بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع"**[1].

عرفت المادة 04/02 من القانون 15-04 آلية إنشاء التوقيع الالكتروني على أنها: " **جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الالكتروني"**[2].

نص أيضا ضمن نفس المادة 02/02 بأن الموقع: " **شخص طبيعي يحوز بيانات إنشاء التوقيع الالكتروني، ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله"**. فهما بالنسبة للموقع حصره المشرع الجزائري في تعريفه للموقع بأنه شخص طبيعي دون الشخص المعنوي.

ميز المشرع الجزائري بين نوعين من التوقيع وهذا بنص المادة 07 من نفس القانون 15-04 بين التوقيع الالكتروني العادي أو البسيط والتوقيع الالكتروني المؤمن أو الموصوف بحيث عرف هذا الأخير بأنه التوقيع الذي تتوفر فيه المتطلبات التالية:

- أن ينشا على أساس تصديق إلكتروني موصوفة.
- أن يرتبط بالموقع دون سواه.
- يكون مصمم بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم المحتكر للموقع.
- أن يكوم مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

نخلص القول إلى أن تعريف التوقيع الإلكتروني في كافة القوانين المنظمة له والمنظمة للمعاملات الالكترونية، يعتبر تقريبا تعريفا موحدا مع الاختلاف في الألفاظ ولكن مع وحدة

[1] - المادة 03/02 من من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2] - المادة 4/02 من القانون ذاته.

المضمون رغم اختلاف أسلوب الصياغة في وضع التعريف، كما أن بعض التشريعات ميزت في التعريف بين التوقيع الالكتروني الموصوف أو المؤمن وبين التوقيع الالكتروني العادي، فالتوقيع الالكتروني المؤمن هو الذي تحدد له إجراءات معينة للتأكد من صحته وضمان عدم العبث به، أما التوقيع الالكتروني العادي أو البسيط فهو التوقيع الذي يرتكز على أنه في حالة إنكاره يقع على عاتق من أدلى به إقامة الدليل على أنه قد تم بطريقة تقنية موثوق بها.

ثانيا : تمييز التوقيع الالكتروني عن التوقيع التقليدي

يهدف كل من التوقيع الالكتروني والتوقيع التقليدي إلى تحقيق غاية واحدة وهي التعبير عن إرادة صاحب التوقيع، وكذا هويته والتأكد على موافقة الموقع على ما يحتويه المحرر، إلا أن التوقيع الالكتروني يختلف عن التوقيع التقليدي، فأغلب التشريعات حددت صور التوقيع الكتابي إما يكون عن طريق في الإمضاء أو بصمة الختم أو بصمة الأصابع، أما بالنسبة للتوقيع الالكتروني فإن القوانين لم تضع صورة معينة للتوقيع الالكتروني بل يمكن أن يتخذ أي شكل، شريطة أن يتميز به صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني أو الرضا بمضمونه[1].

يتميز أيضا التوقيع الالكتروني بأنه قابل للتزييف بسهولة على الرغم من تفاوت شكل التوقيع من شخص إلى آخر، كما أن عملية التحقيق من صحة التوقيع اليدوي غير عملية تعتمد بشكل كبير على مهارة الشخص الذي يقوم بمطابقة التوقيع، أو على معرفته السابقة بالشخص الموقع، وفي أحيان كثيرة لا تتم مطابقة التوقيع على الإطلاق، بينما التوقيع الالكتروني يؤكد هوية المرسل بشكل قاطع، ويمنع حدوث أي تغيير أو عبث في الوثيقة الموقع عليها، كما أن المحرر الالكتروني لديه آليات تقنية للحماية تمنع الغير من الاعتداء عليه وهذا بطبيعة الحال إذا أنشأ بشكل صحيح.

يكمن من خلال ما عرضناه سابقا حصر هذا الاختلاف في عدة جوانب أهمها:

[1] ـ عبد الحميد ثروت،التوقيع الإلكتروني، مرجع سابق، ص.51.

1 ـ من حيث الطبيعة:

يعرف المحرر الالكتروني بأنه ليس له كيان مادي ولا يحمل توقيعا تقليديا، فيعد الشكل الالكتروني أهم صفة تميز التوقيع الالكتروني وتفرق بينه وبين التوقيع التقليدي[1]، بالتالي لا يمكن التفرقة بين الأصل والنسخة التي تستخرج منه ويسهل تعديل بياناته وتغيير أو إضافة بيانات أخرى إليه باتفاق طرفيه دون كشف هذه التعديلات أو الإضافات، بينما على خلاف ذلك فإن التوقيع التقليدي يعتمد على المحرر الورقي المادي، كما أن المحرر التقليدي يمكن تمييزه عن النسخة التي تستخرج منه ويمكن كشف تغيير بياناته بسهولة.

2 ـ من حيث الوسيط أو الدعامة التي يوضعان عليها:

يتم التوقيع في الشكل الكتابي عبر وسيط مادي ملموس وهي في الغالب دعامة ورقة، حيث تذيل به الكتابة فيتحول إلى محرر صالح للإثبات، أما التوقيع في الشكل الالكتروني فيتم كليا أو جزئيا عبر وسيط إلكتروني، من خلال أجهزة الحاسب الآلي وعبر الانترنت حيث أصبح في إمكان أطراف العقد الاتصال ببعضهم البعض والاطلاع على وثائق التعاقد، والتفاوض بشأن شروطه، وإبرام العقود وإفراغها في محررات إلكترونية والتوقيع عليها إلكترونيا، لكن لا يشترط أن يتم التوقيع في الصورة السابقة بعينها، بل يمكن أن يتم نقل الوثائق المتفق عليها على أسطوانة أو أية وسيلة إلكترونية أخرى[2].

3 ـ من حيث أداة التوقيع:

يعتبر التوقيع التقليدي عبارة عن رسم يقوم به الشخص فهو يعتبر فنا وليس علما ومن هنا يسهل تزويره أو تقليده[3]، أما التوقيع الالكتروني فهو من حيث الأصل وفي حدود أمن استخدام برنامجه من قبل صاحب البرنامج علم وليس فنا بالتالي يصعب تزويره، وإن كان هذا لا يعني

[1] ـ محمد محمد سادات، خصوصية التوقيع الالكتروني، دار الفكر والقانون، المنصورة، 2011، ص.103.

[2] ـ ثروت عبد الحميد، التوقيع الالكتروني، مرجع سابق، ص.52.

[3] ـ عماد حسن سليمان، القيمة القانونية للإثبات بالتوقيع الالكتروني، مجلة القانون للدراسات والبحوث القانونية، جامعة ذي قار، كلية القانون، العراق، المجلد2، العدد1، جوان 2006. ص.60.

أنه يمكن عند اختلال معايير الأمن المعلوماتي أن يتم استخدام توقيع الغير الالكتروني، وتكمن صعوبة التزوير في اختيار أجزاء من المحرر المرسل ذاته ومن ثم تشفير هذه الأجزاء، وهو ما يقوم به برنامج الكمبيوتر وليس الشخص، فتحصين التوقيع الالكتروني رهن بحماية سرية كلمة السر ومفتاح التشفير[1].

4 ـ بمدى حرية الشخص في اختيار توقيعه :

يتصل التمايز بين نوعي التوقيع بمدى حرية الشخص في اختيار توقيعه وصيغته، حيث يتمتع الشخص بحرية كبيرة بالنسبة للتوقيع التقليدي، فيجوز له أن يعتمد الإمضاء طريقا لإقرار المحررات أو يستبدله ببصمة الختم أو بصمة الأصابع، أو يجمع بين طريقتين بين الإمضاء وبصمة الأصابع ويجمع بين هذه الأخيرة وبصمة الختم دون الحاجة إلى الحصول على ترخيص من الغير أو تسجيل هذا الاختبار، أما بالنسبة للتوقيع في الشكل الالكتروني فإن الأمر مختلف إذ يجب أن تستخدم في إجراءاته تقنية آمنة، بحيث تسمح بالتعرف على شخصية الموقع ضمانا لسلامة المحرر من العبث أو التحريف كتوثيق التوقيع الالكتروني[2]، ففي بيئة التوقيع العادي على الأوراق أو المحررات يمكن اقتطاع الوثيقة عن التوقيع الوارد عنها أو اقتطاع جزء منها واستبداله، في حين ذلك ليس أمرا متاحا في الوثيقة الالكترونية الموقعة رقميا، فالتوقيع الرقمي لا يثبت الشخص منظم الوثيقة فقط بل يثبت بشكل محدد الوثيقة محل هذا التوقيع بأنه جزء منها ورموز مقتطعة ومشفرة، ولدى فك التشفير يتعين أن ينطبق التوقيع ذاته على الوثيقة[3].

5 ـ من حيث الثبات والاستمرارية:

لا يفرض على صاحب التوقيع إذا تم تقليد أو تزوير التوقيع التقليدي من قبل الغير عند اكتشاف التزوير أو التقليد تغيير شكل توقيعه، في مقابل ذلك فإن صاحب التوقيع الالكتروني

[1] ـ مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الإنترنت، دار الكتب القانونية ، مصر ، 2010، ص.156.

[2] ـ ثروت عبد الحميد، التوقيع الالكتروني، مرجع سابق، ص.54.

[3] ـ عبد الرسول عبد الرضا، محمد جعفر هادي، مرجع سابق، ص.141.

يجب تغيير توقيعه إذا اكتشف توصل الغير إلى المنظومة التي تنشئه وذلك بإبلاغ الجهة المصدرة له[1].

ثانيا: صور التوقيع الالكتروني

يتخذ التوقيع الالكتروني صورا مختلفة بحسب الطريقة أو الأسلوب الذي يتم به، ويعود السبب الأول في تعدد صور التوقيع الالكتروني إلى اختلاف التقنية المستعملة في تشغيل منظومة التوقيع الالكتروني، والسبب الثاني هو اختلاف درجة الثقة بها ومستوى ما تقدمه من ضمان لصاحبها بحسب الإجراءات المتبعة في إصدارها وتأمينها.

يعتمد التوقيع الالكتروني على عدة صور في انتظار ما ستفرزه التكنولوجيا مستقبلا، لأن ظهور هذه الصور يرجع أساسا إلى التطورات التقنية والفنية عبر مراحل مختلفة في مجال المعلوماتية، بالتالي يصعب حصر هذه الصور، فمنها ما يتم عن طريق نقل التوقيع الخطي بالماسح الضوئي ومنها ما يتم عن طريق التوقيع بالقلم الالكتروني ومنها ما يتم بالتوقيع البيومتري والتوقيع المفتاحي، فأغلب التشريعات التي نظمت هذا التوقيع لم تنص على شكل معين له، وإنما تركت تحديد ذلك إلى ما ستفرزه التكنولوجيا مستقبلا، لكن بالمقابل حددت الأسس والضوابط العامة التي يجب أن يقوم عليها.

أولا: التوقيع باستخدام الماسح الضوئي

يعرف التوقيع الإلكتروني لاستخدام الماسح الضوئي بأنه نقل التوقيع الالكتروني المكتوب بخط اليد على المحرر إلى الملف المراد نقله إليه باستخدام جهاز الماسح الضوئي[2]، حيث ينقل المحرر موقعا عليه صاحبه إلى شخص آخر باستخدام الانترنت،وهكذا يمكن نقل هذا التوقيع وطبعه عل أية وثيقة كلما دعت الحاجة إلى ذلك[3].

[1] ـ عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة، عمان، 2009، ص.87.

[2] ـ حسن عبد الباسط جميعي، مرجع سابق، ص.36.

[3] ـ محمد إبراهيم أبو الهيجاء، عقود التجارة الالكترونية، مرجع سابق، ص.130.

تواجه هذه الطريقة الكثير من المعوقات تتمثل في عدم الثقة، بحيث يمكن للمستقبل أن يحتفظ بهذا التوقيع الموجود على المحرر الذي أستقبله عن طريق شبكة الانترنت عبر جهاز الماسح الضوئي ووضعه على أي محرر آخر لديه دون وجود أي طريقة يمكن من خلالها التأكد من أن صاحب هذا التوقيع هو الذي وضعه على هذا المحرر وقام بإرساله إليه[1]، لكن هذا الشكل من التوقيعات يعاب عليه أنه لا يتوافر على ضمانات الأمان حيث يعتمد على نقل التوقيع الخطي كما هو إلى الوثيقة المعالجة الكترونيا للإقرار بمضمونها، ومن هنا يمكن للشخص الاحتفاظ بنسخة من التوقيع المصور بجهاز الماسح لاستخدامه على وثيقة الكترونية لا علاقة لها به، أي وضع التوقيع على أي محتوى موجود على دعامات الكترونية[2].

ثانيا: التوقيع باستخدام الرقم السري PIN

يعتبر استخدام البطاقات الممغنطة المقترنة بالرقم السري الأكثر شيوعا لدى الجمهور، ولا يتطلب استخدامها الكثير من العناء أو تتطلب خبرة معينة، بل يمكن لكل شخص أن يستخدمها، كما أنها تستلزم أن يمتلك الشخص جهاز حاسب آلي، وأن يكون جهازه متصلا بشبكة الانترنت[3].

يظهر هذا التوقيع عند استخدام بطاقات الائتمان المقترن بالرقم السري، فنتيجة تطور التكنولوجيا وازدياد التعامل بأسلوب التجارة الالكترونية ظهرت البطاقات الممغنطة البنكية التي تستخدم عن طريق ماكينة الصرف الآلي ATM ، تحتوي هذه البطاقات على شريط تسجيل مغناطيسي للمعلومات مثل اسم المستخدم ورقم الهوية وتاريخ صلاحية البطاقة ورقم تعريف الشخصية، أما ذاكرة البطاقة فتحتوي على نظام دفاعي للحماية، لأنه يعد إجراء عدة محاولات غير ناجحة لكي يتعرف المستخدم الرقم السري فإن العملية لا تتم، كما أن البطاقة يمكن سحبها بواسطة ماكينة الصرف.

[1] ـ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية،2003 ، ص.31.

[2] ـ سعيد السيد قنديل، التوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2006، ص.26.

[3] ـ عبد الحميد ثروت، التوقيع الالكتروني، مرجع سابق، ص.56.

تتم عملية سحب النقود آليا من خلال ماكينة الصرف عن طريق إدخال البطاقة ثم إدخال الرقم السري الخاص بالمستخدم، فإذا كان الرقم صحيحا واتبعت الإجراءات تمت عملية السحب، وهكذا حل التوقيع السري محل التوقيع اليدوي[1].

ثالثا: التوقيع البيومتري

يعتمد هذا النوع على الخواص الكيميائية والطبيعية للأفراد، إذ يتم تعيين الخواص الذاتية للعين مثلا عن طريق أخذ صورة دقيقة لها وتخزينها في الحاسب الآلي لمنع أي استخدام من أي شخص آخر، وهذا الحال بالنسبة لبصمة الأصابع أو خواص اليد البشرية أو نبرة الصوت[2] أو التوقيع الشخصي[3]، ففي كل حالة لا يجوز لأي شخص عادي الدخول لهذا الحاسب واستخدام ما به من معلومات وبيانات إلا لهؤلاء الذين يتم التحقق من مطابقتهم لما تم تخزينه على الحاسب الآلي، سواء من بصمة الأصابع أو خواص اليد البشرية أو نبرة الصوت أو التوقيع الشخصي أو خواص العين، أما إذا ما تبين أنه يوجد أي اختلاف مهما كان بسيطا فلا يسمح لهم بالدخول على هذا الحاسب، وتعد الطريقة من أهم الطرق التي تحقق الأمان للحاسبات لأنها لا تسمح بالولوج لمن هم غير مسموح لهم بالدخول[4].

يمكن الإشارة في هذا الصدد بأن هذا النوع من التوقيع ما زال في تطوراته الأولى ناهيك عن ما حصل من تطور تقني سريع في نسخ توقيع المستخدم واستعماله من قبل المرسل إليه أو من قبل الغير حيث أن الاعتماد على هذا النوع فيه مأخذ يمكن الإشارة إليها في هذا المقام

[1] ـ خالد ممدوح إبراهيم، التقاضي الالكتروني، دار الفكر الجامعي،الإسكندرية، 2007، ص.280.

[2] ـ منير الجنبيهي،ممدوح محمد الجنبيهي، التوقيع الالكتروني وحجيته في الإثبات، مرجع سابق، ص.12.

[3] ـ يجب أن ننوه هنا أنه عند استخدام أي من هذه الخواص يتم أولا الحصول على صورة للشكل وتخزينها داخل الحاسب الآلي حتى يمكن الرجوع إليها عند الحاجة، وهذه البيانات الذاتية يتم تشفيرها حتى لا يتمكن أي شخص من الوصول إليها ومحاولة تعديلها أو العبث بها، وفي ذات الوقت السماح للأشخاص المصرح لهم باستخدامها، ولما كانت الخواص المميزة لكل شخص كالبصمة الشخصية وبصمة العين وبصمة الصوت، تختلف عن تلك العائدة لغيره، فإن التوقيع البيومتري يعتبر وسيلة يمكن الوثوق بها والاعتماد عليها لتمييز الشخص وتحديد هويته نظرا لارتباط الخصائص الذاتية به، وهو ما يتيح استخدامها في إقرار التصرفات القانونية التي تبرم باستخدام وسيلة الكترونية، انظر في ذلك: عبد الحميد ثروت، التوقيع الالكتروني، مرجع سابق، ص.60.

[4] ـ منير الجنبيهي،ممدوح محمد الجنبيهي، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2005، ص.195.

وخاصة ما يحصل من تغيير في الخواص الفيزيائية للإنسان نتيجة مرور فترات من الزمن[1]، مما ترك بعض الفقه يتحفظون على استعمال مثل هكذا تواقيع نظرا لإمكانية نسخ هذا التوقيع، بالإضافة إلى كلفة التقنية الخاصة بهذا الشكل من التوقيعات الالكترونية وتغير الخواص الفيزيائية مع التقدم في السن والإرهاق[2]، لذا فإن تأمين الثقة في التوقيع البيومتري يتطلب استخدام منظومة بيانات مؤمنة للتوقيع الالكتروني بحيث تضمن انتقاله دون إمكانية التلاعب فيه، إضافة إلى توافر الضوابط الفنية والشروط والمتطلبات القانونية اللازمة للاعتماد عليه كحجة في الإثبات[3].

رابعا: التوقيع الرقمي

يعتبر التوقيع الرقمي إحدى صور التوقيع الالكتروني التي تستخدم في إبرام التصرفات القانونية عبر الوسائط الالكترونية التي تتم من خلال الانترنت، فهو أساسا يرتكز بالذات على التشفير كآلية توقيع ذات موثوقية عالية يجعله يحتل مرتبة الصدارة[4]، بحيث من شأنه تأمين المحرر الالكتروني والتحقق من صحته لتأكيد عدم تعرضه لأي تغيير أثناء نقله[5]، تقوم هذه التقنية بتزويد المحرر الالكتروني بتوقيع مشفر مميز يحدد الشخص الذي قام بتوقيع الوثيقة والوقت الذي قام فيه بالتوقيع على المحرر، وجرد معلومات عن صاحب التوقيع، ويتم تسجيل التوقيع الرقمي بشكل رسمي عند جهات تعرف باسم سلطات التصديق، وهي طرف محايد مهمتها التأكد من صحة ملكية التوقيع الرقمي للأشخاص الذين يقومون بتوقيع المحررات الالكترونية.

تعتبر التوقيعات الرقمية القائمة على ترميز المفاتيح العمومية والمفاتيح الخاصة هي الأكثر شيوعا، والمفاتيح العامة هي التي تسمح لكل من يهتم بقراءة الرسالة أن يقرأها دون أن يستطيع

[1] ـ سمير عبد السميع الأودن، العقد الالكتروني، منشأة المعارف، الإسكندرية، 2005، ص.183.

[2] ـ حسن عبد الباسط جميعي، مرجع سابق، ص.41.

[3] ـ عبد الحميد ثروت، التوقيع الالكتروني، مرجع سابق، ص.60.

[4] ـ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، مرجع سابق، ص.89.

[5] ـ عمر ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الالكتروني، دار وائل، عمان، 2010، ص.52.

إدخال أي تعديل عليها، فإذا ما وافق على مضمونها وأراد إبداء قبول بشأنها وضع توقيعه عليها من خلال مفتاحه الخاص قبل إعادة الرسالة إلى مرسلها[1].

يؤخذ على التوقيع الرقمي أن هناك احتمال تعرضه للسرقة أو الضياع[2]، وبالتالي البعض يتخوف من تطور وسائل القرصنة والاحتيال إلى حد اختراق رسالة البيانات من خلال كسر المفتاح الخاص، خاصة أن التوقيع الرقمي يعتمد أساسا على الرموز السرية والمفتاحين غير المتناسقين العام والخاص[3]، وقد أقر القضاء الفرنسي واعترف بصلاحية التوقيع الرقمي الذي يتم بواسطة شخص من خلال الرقم الخاص المستخدم في بطاقات الدفع، وهذا بالنسبة للاتفاقيات المتعلقة بإثبات التصرفات[4].

خامسا: التوقيع بالقلم الالكتروني

يعتمد التوقيع بالقلم الالكتروني على تحديد نمط خاص تتحرك به يد الموقع أثناء توقيعه، إذ يتم توصيل قلم إلكتروني بجهاز الكمبيوتر فيقوم الموقع باستخدام هذا القلم الذي يسجل حركات يد الشخص أثناء التوقيع كسمة مميزة لهذا الشخص، فهو عبارة عن قلم الكتروني حسابي يمكن استخدامه في الكتابة على شاشة الحاسب الآلي الخاص بالموقع، ويتم ذلك باستخدام برنامج هو المسيطر والمحرك لهذه العملية، ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من

[1] - منير الجنبيهي،ممدوح الجنبيهي، الطبيعة القانونية للعقد الإلكتروني، مرجع سابق، ص.197.

[2] - يرد البعض على ذلك بأن التوقيع التقليدي هو أيضا عرضة للتقليد والتزوير، وسرية الرقم تكفي للدلالة على صدور الرقم عن صاحبه بحسب الأصل وعميل البنك ملزم بسرية الرقم السري للبطاقة حسب الاتفاق مع البنك، وإذا تسرب للآخرين فهو مسئول عن ذلك، ولذلك فإن العميل ملزم بالمحافظة على الرقم السري للبطاقة، إلا أن مسئولية صاحب التوقيع الإلكتروني تنفي عند قيامه بالإبلاغ عن سرقة أو فقدان البطاقة، وذلك بالنسبة لجميع العمليات التي تتم بعد الإبلاغ. أنظر في ذلك: عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني، مرجع سابق، ص.35.

[3] -Philippe Le Tourneau, Contrats informatiques et électroniques, DALLOZ, Paris, 2004, p296. Arnaud Fausse, op.cit , P.25 .

[4] - عبد الحميد ثروت، التوقيع الالكتروني، مرجع سابق، ص.62.

التوقيعات، الأولى وهي خدمة التقاط التوقيع، والثانية هي خدمة التحقق من صحة التوقيع[1]، بالتالي فإن البرنامج يتلقى أولا بيانات العميل عن طريق بطاقته الخاصة التي يتم وضعها في الآلة، وتظهر بعد ذلك التعليمات على الشاشة، ثم تظهر بعد ذلك رسالة إلكترونية تطلب توقيعه باستخدام قلم على مكان محدد داخل شاشة الحاسب الآلي، ويقوم هذا البرنامج بقياس خصائص معينة للتوقيع من حيث الحجم والشكل والنقاط والخطوط والالتواء[2]، وعند الموافقة يتم تشفير البيانات الخاصة بالتوقيع وتخزينها باستخدام البرنامج، ثم تأتي مرحلة التحقق من صحة التوقيع عن طريق مقارنة البيانات مع التوقيع المخزن ويتم إرسالها إلى برنامج الحاسب الآلي الذي يحدد فيها إذا كان التوقيع صحيحا أم مزورا[3].

يؤخذ على هذا النوع من التوقيع الإلكتروني أنه يضعف الثقة في المحررات الموقع عليها إلكترونيا، وبالتالي فإنه يقلل من حجية التوقيع الإلكتروني في الإثبات[4]، لأنه بإمكان المرسل إليه الاحتفاظ بنسخة من التوقيع الذي وصله ووضعه على أي محرر آخر.

يعتبر هذا النوع أكثر استخداما في الجزائر خاصة في جوازات السفر الالكتروني أو ما يسمى الجواز البيومتري، أين يعتمد عن استخراجه استخدام التوقيع بالقلم الالكتروني الذي يحدد هوية صاحبه، وذلك استجابة لهذا النوع من الوثائق التي تتم إلكترونيا.

[1] ـ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، مرجع سابق، ص.30. خالد ممدوح إبراهيم، العقد الإلكتروني، مرجع سابق، ص.200. محمد أمين الخرشة، نايف عبد الجليل الحمايدة، الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، مجلة جامعة الأزهر، غزة، سلسلة العلوم الإنسانية، 2014، المجلد 16، العدد1، ص.333.

[2] ـ عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني، مرجع سابق، ص.32.

[3] ـ منير الجنبيهي،ممدوح الجنبيهي، التوقيع الالكتروني وحجيته في الإثبات، مرجع سابق، ص.10.

[4] ـ وسن كاظم زرزور، التوقيع الإلكتروني كدليل من أدلة الإثبات، مجلة رسالة الحقوق،جامعة واسط، العراق، السنة الثالثة، العدد 2، 2011، ص.144، على موقع: https://www.iasj.net/iasj?func=fulltext&aId=19165

الفرع الثاني

وظائف التوقيع الالكتروني

يحقق التوقيع الالكتروني عدة وظائف أشارت إليها اغلب التشريعات المقارنة، فأية وسيلة أو أسلوب يحقق هذه الوظائف قد يصلح أن يكون توقيعا بالمنظور القانوني، وتكون له حجية التوقيع بالأساليب التقليدية، فالتوقيع الإلكتروني يمكنه في ظل ضمانات قانونية وتقنية أن يقوم بذات الدور الذي يؤديه التوقيع التقليدي ويحقق نفس الوظائف متى كان صحيحا وأمكن إثبات نسبته إلى موقعه، ويحقق الأمان والخصوصية والسرية في نسبته للموقع ويتم ذلك عن طريق إمكانية تحديد هوية الموقع ومن ثم حمايته من أي اعتداء يمس به، بالتالي لا بد من تحقيق التوقيع في الشكل الإلكتروني ثلاث وظائف أساسية تتمثل أساسا في قدرة التوقيع الالكتروني على تحديد هوية الموقع **(أولا)**، قدرة التوقيع الالكتروني في التعبير عن إرادة الموقع في الالتزام بمضمون المحرر الالكتروني **(ثانيا)**، بالإضافة إلى سلامته وتأمينه من أي عبث وتلاعب بمحتوياته **(ثالثا)**، وسوف نتناول هذه الوظائف بشيء من التفصيل على النحو التالي :

أولا: تحديد هوية الموقع

ذهب رأي من الفقه الفرنسي من أن التشريعات ما كان لها أن تنص على ذلك الشرط بالنسبة إلى المحرر الإلكتروني، ولم تكن هناك حاجة لتحديد المحرر الإلكتروني هوية منشئه، فذلك الأمر من سمات التوقيع الإلكتروني وأحد وظائفه التي يجمع عليها الفقه، فتحديد هوية الشخص منشئ المحرر بصفة عامة دون تخصيص لمحرر تقليدي أو محرر إلكتروني تعتبر أول وظيفة يتولى التوقيع تحقيقها وليس المحرر، فليس المهم تحديد هوية محرر الكتابة أو منشئ المحرر، وإنما المهم هو تحديد هوية الموقع الذي سيلتزم بما ورد في المحرر وما هو مدون به[1].

[1] - CAPRIOLI Eric , Le juge et la preuve électronique , Article disponible sur le site : www.caprioli-avocats.com

حتى يتسنى للتوقيع القيام بأداء وظيفته يجب أن يكون دالا على شخصية الموقع[1]، بمعنى أن التوقيع علامة شخصية بحيث أن الشخص يتولى بنفسه وضع التوقيع، فإذا وقع شخص آخر باسم الموقع فلا يعتد بهذا التوقيع ويكون باطلا[2] ولو تم ذلك برضاء صاحب التوقيع، فالعبرة هنا بأن يكون التوقيع صادرا ممن يراد أن يحتج به عليه[3]، فطريقة التعبير من خلال الوسيط الالكتروني وجهات التصديق الالكتروني تسمح بالتعرف على هوية صاحب التوقيع بطريقة محسوسة كما في حالة التوقيع في شكله الكتابي، ومع خلال تقدم التقنيات التي تستهدف التثبت من التوقيع الالكتروني يمكن تحديد هوية صاحب التوقيع من خلال أنظمة فعالة تكشف عمليات التسلل والقرصنة، وحماية الأطراف في ضل تقنيات عالية وبرامج أمنية للتأكد من هوية أصحاب التوقيع بما يؤكد سلامة التوقيع ويعزز الثقة فيه، ويدل على موافقة كل طرف على المعلومات الواردة بالمحرر الالكتروني[4].

نصت المادة 2/9 من قانون الأونسترال بشأن التجارة الإلكترونية [5] على أنه: **"يعطي للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجيته في الإثبات، وفي تقدير حجية رسالة البيانات في الإثبات، يولي الاعتبار لجدارة الطريقة التي استخدمت في إنشاء أو تخزين أو إبلاغ رسالة البيانات، ولجدارة الطريقة التي استخدمت في المحافظة على سلامة المعلومات، وللطريقة التي حددت بها هوية منشئها، ولأي عامل آخر يتصل بالأمر".**

[1] ـ خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2007 ، ص.95.

[2] ـ هناك مسألة أخرى تتصل بتمييز هوية الموقع وتحديد شخصيته، وهي الخاصة بتحديد أهلية الشخص للتوقيع على المحرر، والتأكد من سلطاته لإبرام التصرف القانوني، وعلى وجه الخصوص إذا كان الشخص الذي يتولى التوقيع ليس طرفا في العمل القانوني المراد إبرامه، كما لو كان وكيلا أو وليا أو وصيا على القاصر، أو ممثلا عن الشخص المعنوي، إذ يجب في هذه الفروض أن يحدد هويته بنفسه، كما يوضح مصدر سلطته في التوقيع. للمزيد راجع في ذلك: عبد الحميد ثروت، التوقيع الالكتروني، مرجع سابق، ص.32 .

[3] ـ إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، 2008، ص.273.

[4] ـ خالد ممدوح إبراهيم، التوقيع الالكتروني، الدار الجامعية، الإسكندرية، 2010، ص.117. خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني، نفس المرجع، ص.95.

[5] ـ المادة 2/9 من قانون الأونسترال بشأن التجارة الإلكترونية لسنة 1996 .

نص القانون الفرنسي في المادة 1316-1 من التقنين المدني على أنه: **"تقبل الكتابة في الشكل الإلكتروني في الإثبات شأنها شأن الكتابة على دعامة ورقية، شرط أن يكون في الإمكان تحديد هوية الشخص الذي صدرت عنه[1]"**، لكن هناك صعوبات في تحقيق هذا الشرط، تتمثل في عدم المقدرة في التعرف على هوية المتراسلين أو المتعاقدين ذلك أن شخصيتها تبقى إلى حد ما غير أكيدة[2].

تشابهت في القانون المصري شروط حجية المحررات الإلكترونية مع شروط حجية التوقيع الإلكتروني والكتابة الإلكترونية، فكانت جميعها شروطا واحدة ولم تختلف عنها، وتولت اللائحة التنفيذية إزالة التشابه بينها، وذلك في المادة (8/ب) منها، إذ نصت على أن: **" مع عدم الإخلال بالشروط المنصوص عليها في القانون، تتحقق حجية الإثبات المقررة للكتابة الإلكترونية والمحررات الإلكترونية الرسمية أو العرفية لمنشئها، إذا كان متاحا فنيا تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الرسمية أو العرفية ودرجة سيطرة منشئها على هذا المصدر وعلى الوسائط المستخدمة في إنشائها".**

نص المشرع الجزائري في المادة 323 مكرر1 من القانون المدني على شرط إمكانية التأكد من هوية الشخص الذي أصدرها[3]، كما نصت المادة 06 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونين الجزائري **" يستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الالكتروني[4]"**، كما نص المادة 3/7 من نفس القانون **" أن يمكن من تحديد هوية الموقع"[5]**.

---

[1] -Article 1316 -1 du C.C.F. dispose que : ***« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane» .***

[2] -MICHEL Jaccard, Problèmes juridiques liés à la sécurité des transaction sur le réseau , p 2, article disponible sur le site : www.signelec.com

[3] - راجع نص المادة 323 مكرر 1 من القانون المدني الجزائري.

[4] - المادة 06 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

[5] - المادة 03/7 من القانون ذاته.

يتضح من خلال أحكام هذه المادة أن المشرع الجزائري قد نص صراحة على أن من وظائف التوقيع الالكتروني هو تحديد هوية الشخص الموقع بالإضافة إلى التعبير عن إرادة الموقع بمضمون المحرر.

يتضح مما سبق أن التوقيع لا يميز بين وسيلة إصداره بمعنى لا يشترط أن يتم التوقيع بخط يد الموقع بل يمكن إتمامه بأداة منفصلة عن شخصه، فهو من وظيفته الأساسية التعرف على صاحبه بحيث يكون مميزا ومحددا لشخص صاحب التوقيع.

ثانيا: قدرة التوقيع الالكتروني في التعبير عن إرادة الموقع

يقصد بهذا الشرط أن يكون التوقيع ضمن المحرر كلا لا يتجزأ وذلك حتى يمنح المحرر قيمته القانونية، ويكون التوقيع دالا على رضا موقعه بمضمون المحرر، ومعنى ذلك أنه لا بد أن يكون هذا التوقيع متصلا اتصالا ماديا ومباشرا بالمحرر المكتوب[1]، وهذا يتعلق أساسا بكفاءة التقنيات المستخدمة في تأمين مضمون المحرر المدون إلكترونيا، وبالتالي تأمين ارتباطه بشكل لا يقبل الانفصال عن التوقيع، ولا يمكن لأحد غير صاحب المحرر الالكتروني من التدخل بتعديل مضمونه[2].

يتعين أن يكون توقيع الموقع دالا على موافقته على المحرر الالكتروني وعلى اتجاه إرادته إلى الالتزام بموجبات مضمون المحرر أو ادعائه بمحتوى هذا المحرر ومعبرا عن إرادة الموقع وإقراره بمضمون التصرف[3].

نص المشرع الجزائري في المادة 08 من القانون 15-04 على أنه: " **يعتبر التوقيع الالكتروني الموصوف وحده مماثلا للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي**"[4].

[1] ـ مخلوفي عبد الوهاب، مرجع سابق، ص.220.

[2] ـ علاء محمد عيد نصيرات، مرجع سابق، ص.67.

[3] ـ سعيد السيد قنديل، التوقيع الالكتروني، مرجع سابق، ص.80.

[4] ـ المادة 08 من قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

نلاحظ من خلال ذلك أن المشرع الجزائري بالنسبة للشخص الطبيعي أو المعنوي، إذا استعمل التوقيع الموصوف دليل على أن الموقع أثبت موافقته على مضمون المحرر الالكتروني والبيانات الواردة فيه، فهو يعتبر قرينة على قبول وسيلة التعبير عن قبول ورضا الموقع بما ورد في المحرر ما لم يثبت خلاف ذلك.

ثالثا: إثبات سلامة المحرر

يستطيع التوقيع الالكتروني أن يؤدي وظيفة الحفاظ وإثبات سلامة المحرر خاصة وأن رسائل الأمان في مجال المحررات الالكترونية مهمة وصعبة جدا نظرا لطبيعة البيئة التي يتم فيها التعاقد[1].

نقصد بضمان سلامة المحرر التحقق من صحته عند تقديمه للاستدلال به بوصفه دليلا في الإثبات، فالمحافظة على سلامة المحرر من العبث والتلاعب بمحتوياته تؤمن من خلال تقنية التوقيع الالكتروني، خلافا للطبيعة المادية للمحرر الكتابي الورقي التي تؤمن هذه السلامة بصورة واضحة[2]، ومن ثم يسهل كشف أي تلاعب أو تزوير فيها، بينما لا يتمتع المحرر

[1] ـ يوسف أحمد النوافلة، مرجع سابق، ص.155.

[2] ـ رغم توافر عناصر أمان فيها بقدر أكبر بعض الوسائل قد تترك أثرا مكتوبا ولكن هذا الأثر المكتوب غير معتبر قانونا وخير دليل على ذلك حالة التيلكس، فبالرغم من مزايا التيلكس وقوته في بعض نواحي وعناصر الأمان القانونين على تجنب العيوب الموجودة في غيره من الأجهزة لا سيما الفاكس،إلا أن الأثر المكتوب الذي يمكن الحصول عليه عبر التلكس يفتقر إلى أهم عنصر ممكن أن يقوي من حجية الوثيقة الصادرة عنه ألا وهو عنصر التوقيع،لأن الورقة تصل عبر جهاز التلكس تكون مقسمة إلى بيانات المرسل والتي تظهر باللون الأحمر، وبيانات المرسل إليه، والتي تظهر باللون الأسود، وذلك دون وجود أية إمكانية تقنيا لإضافة توقيع أي من الطرفين، وبالتالي فإن التيلكس في أحسن الأحوال لا يعتد بها كقرينة على بعض الأمور المحددة، وليس على كل ما يتعلق بالواقعة المطلوب إثباتها كوحدة واحدة لا تتجزأ، وليس الأمر بأحسن حال إذا ما دار الحديث عن غيرها من الوسائل كوسيلة الفاكس مثلا أو المحررات الواردة عبر الإنترنت، ولا يختلف الأمر كثيرا فيما يخص المحررات الواردة أو المستخرجة من الانترنت، بل قد يزداد الأمر تعقيدا أكثر لعدم إمكانية نسبة المحرر للشخص المعني، نظرا لصعوبة ثبوت نسبة البريد الالكتروني للشخص المقصود، لا سيما إذا لم يكن هذا الشخص قد سجل بياناته الحقيقية عند بدء استعماله لذلك البريد ، ناهيك عن حجية التوقيع الإلكتروني وما تثيره من إشكالات، للمزيد راجع في ذلك: رامي وشاح، مرجع سابق، ص.24.

الالكتروني بهذه الصفة لأن الكتابة الالكترونية قابلة للمحو والتعديل والتلف ودون ترك أثر ملحوظ يكشف هذا التلاعب[1].

لا بد إذن وللتأكد من صحة التوقيع الإلكتروني من تحويل البيانات المشفرة إلى بيانات مقروءة ومفهومة باستخدام المفتاحين العام والخاص، فإن كان التوقيع صحيحا والبيانات لم يعبث بها توصلنا إلى هذه النتيجة وإن كان التوقيع غير صحيح أو البيانات قد تم تغييرها، فلا يمكن فك الرموز لوجود ربط منطقي بين الكتابة الالكترونية والتوقيع عليها فالتوقيع الالكتروني إذن يؤدي وظيفة ضمان سلامة المحرر من أي عبث أو تعديل أو تغيير.

أصبح تحديد وظائف التوقيع الالكتروني وانطباقها على وظيفة التوقيع التقليدي من الضمانات اللازمة من أجل توفير الأمان في استخدام الوسائل التكنولوجية الحديثة في النظم المعلوماتية، وهذا ما يعزز الثقة في صحة التوقيع الالكتروني وبالتالي يؤمن الثقة والأمان والمصداقية في سلامة المحرر الالكتروني.

[1] ـ عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.180.

الفصل الثاني

ضمان سلامة المحرر الالكتروني محل الحماية

يعتبر عدم مضاهاة المحرر الإلكتروني للمحرر الورقي من حيث القدرة على توفير الثقة في شأن انتسابه لمصدره، وفي شأن صحة ما ورد به من بيانات يخالف واقع الأمور، بحيث أن المحررات الإلكترونية متى أمكن ربطها بالتوقيع الإلكتروني بتقنيات تأمين المحرر والتوقيع، فإنها توفر قدرا من الثقة في سلامة المحرر الإلكتروني وعدم إدخال تعديلات عليه، وذلك يؤدي بالضرورة إلى مساواة المحرر الإلكتروني بالمحرر التقليدي من حيث الحجية في الإثبات، فتحقيق الثقة في البيانات المدونة في المحرر الإلكتروني لا يكون إلا من خلال حفظها في صيغتها النهائية وبشكل لا يقبل التعديل إلا بإتلافها أو محوها تماما.

فضمان سرية وسلامة محتوى المحرر الإلكتروني وتأمين بياناته يتم عن طريق وسائل فنية وتقنية حديثة، تتمثل أساسا في وضع أنظمة معلومات مؤمنة جديرة بالثقة، تسمح بتوثيق البيانات والمعلومات ونسبتها إلى منشئها والتأكد بصفة موثوق منها من مضمونها، لذلك وفي سبيل استقرار النظام القانوني والحد من المنازعات المتعلقة بالمحرر الإلكتروني، عمدت أغلب التشريعات الدولية والوطنية على وضع منظومة تقنية تتمثل أساسا في تقنية التشفير والتصديق الإلكتروني، فالوسائل والأدوات والإجراءات التي تلجأ إليها هذه المنظومة التقنية لسلامة المحرر ترتبط ارتباطا وثيقا بالتقنيات المستخدمة في الحفظ والاسترجاع، والتي تتعلق أساسا بوجود سجل إلكتروني يعمل على حفظ المحرر الإلكتروني بدءا من اللحظة التي يكتسب فيها الحجية القانونية، وبتحديد طرق الحفظ التقني من خلال حفظها عبر الزمن، إلا أن تقييم مدى قدرة هذه الوسائل وكفاءة التقنية المستخدمة على تأمين بيانات المحرر سوف يخضع بالضرورة إلى تقدير قاضي الموضوع عند تدخله بشأن قبولها كدليل في الإثبات، وعلى هذا الأساس لا بد أن نتطرق أولا إلى مسألة ضمان المحرر الإلكتروني من خلال بيان متطلبات عملية حفظ المحررات الالكترونية وشروطها في **(المبحث الأول)**، ثم بيان الوسائل التقنية في ضمان الأمن

القانوني للمحررات الإلكترونية التي تتمثل أساسا في منظومة التشفير والتصديق الإلكتروني **(المبحث الثاني).**

المبحث الأول

تأمين المحرر الالكتروني وحفظه

تعتمد استمرارية منح الحجية القانونية للمحرر الالكتروني بصفة أساسية وضمان صحته، على عملية حفظ المحرر بما يكفل ضمان الحفظ على محتواه والرجوع إليه عند الحاجة[1]، ولم تبين مختلف التشريعات التي تبنت مبدأ التعادل الوظيفي بين المحررات الإلكترونية والمحررات الورقية طرق الحفظ أو ضوابطه القانونية، فتنفيذ طريقة الحفظ الإلكتروني للمحررات الإلكترونية يجب أن لا يؤدي إلى إدخال أي تعديل على حالته الأصلية، بحيث يتعين حفظ المحرر الإلكتروني بالحالة التي نشأ عليها وأن يظل محتفظا بهذه الحالة مدة حفظه واسترجاعه، لأن ذلك من شأنه تكريس الثقة في البيئة الإلكترونية وبالتالي يعتد به كدليل إثبات عند الحاجة، ففي حالة نشوء نزاع فإن الأطراف بإمكانهم الرجوع إلى السجل الالكتروني وإظهار المحرر الالكتروني الموثق وإعادة نسخه إلكترونيا، وذلك باستخدام التقنيات الكفيلة لبقائها وعدم تعرضها للتلف أو الزوال لأطول فترة ممكنة تسمح بها الإمكانيات التقنية المتاحة والتكنولوجيا المتوفرة، وعلى هذا الأساس سنحاول أن تتطرق أولا إلى الضمانات التقنية التي ترتبط مع إعطاء المحررات الالكترونية حجية الدليل الكتابي في الإثبات، وتضمن عدم إساءة استخدام هذه المحررات أو التلاعب فيها، وتساعد على تأمين وظائف الأمن والسرية من أجل قبولها في الإثبات[2]، لاسيما أن هناك عوامل تساعد على هذا التلاعب، وذلك بوصف أن المحررات الالكترونية تؤسس على فكرة عدم الحضور المادي لأطراف أصحاب التعامل بها، إذ يتم التعامل بين الأفراد وهم لا يرتبطون بمعرفة سابقة وإن لم يحصل أي تلاقي بينهم مما يعني أن هناك إمكانية للتحايل والعبث بهذه المحررات، بالتالي سنتناول أولا نظام التشفير كآلية

[1]- Alain Bensoussan, Le Commerce électronique, op.cit , p.54

[2] - باسيل يوسف، الاعتراف القانوني بالسندات والتواقيع الإلكترونية في التشريعات المقارنة، مجلة دراسات قانونية، العدد الثاني، السنة الثالثة ، بغداد،، 2001، ص.23.

للحفاظ على سلامة المحررات الإلكترونية **(المطلب الأول)**، لنتناول ثانيا متطلبات عملية الحفظ وطرقها **و**بيان شروط حفظ المحررات الإلكترونية في **(المطلب الثاني).**

المطلب الأول

نظام التشفير كآلية لتأمين المحرر الإلكتروني

تتطلب عملية الحفاظ على بيانات ومعاملات الأطراف استخدام تقنية التشفير التي تعتبر إحدى أهم وأبسط وسائل الحماية والأمن والسرية للمعلومات المتداولة عبر وسائل الاتصال الحديثة خاصة شبكة الانترنت، فهو إجراء تقني يسمح بتأمين هذا النوع المستحدث من المحررات وحمايتها من أي اعتداء أو اختراق من الغير سواء المحفوظة منها أو المتبادلة إلكترونيا، فهو يؤكد صحة وأصلية البيانات، وقد أولت لها التشريعات أهمية كبيرة في قوانينها المنظمة للمعاملات الالكترونية لكي تضمن ثقة المتعاملين في استخدام هذه الوسائط، لأن أمن هذه الوسائط من أمن المحررات الإلكترونية.

لكي يكون نظام التشفير موثوقا به، يجب أن تكون أدوات التشفير مواكبة للتطور السريع لتكنولوجيا المعلومات، ذلك أن برامج التشفير قد تحتوي على طفرة تكنولوجية، يمكن استثمارها في كشف المحررات الالكترونية المشفرة، لذلك يجب مواكبة هذا التطور لكشف أي احتمالات لاختراق التشفير.

حتى يكون التشفير قانونيا ومشروعا يجب أن يخضع لمجموعة من الضوابط والقواعد التي حددتها أغلب التشريعات التي تبنت هذه الأنظمة، و يمكن حصرها في ثلاثة ضوابط وهي: مشروعية تشفير البيانات والمعلومات، الحق في خصوصية البيانات المشفرة، اعتبار النص المشفر محررا.

لذا سنتناول في هذا المطلب مفهوم نظام التشفير في **(الفرع الأول)**، ثم بيان الضوابط التي يجب أن يخضع إليها هذا النظام في **(الفرع الثاني).**

الفرع الأول

مفهوم نظام التشفير

ازدادت أهمية التشفير وتطورت مع زيادة حجم التبادلات عبر شبكة الانترنت حيث تمثل إحدى الركائز الأمنية التي توفر الأمان والسرية للمحررات الالكترونية وتضمن سلامتها[1]، فالتشفير كآلية لتأمين البيانات والمعلومات يعتبر من أبسط الطرق وأهمها لضمان عدم اختراق الأنظمة المعلوماتية في الحاسب الآلي أو على شبكة الانترنت، فهو وسيلة يستخدم لإثبات أن المعلومات أصلية ومنشئها الذي أرسلت منه أصلي بمعنى أنه لم يتم تعديلها أثناء عملية التداول، وتتعدد أنظمة التشفير مع التغيير المستمر لبرامج الحاسب الآلي وطرق اختراق الأنظمة المعلوماتية فمنها أنظمة التشفير المتماثل، أنظمة التشفير غير المتماثل، أنظمة التشفير المزدوج، وأنظمة التشفير عن طريق تأمين تقنيات المحررات الالكترونية.

أولا: تعريف تقنية التشفير

يرى جانب من الفقه أن الإشكال في الثبات يتحول أكثر فأكثر من إشكال قانوني إلى إشكال تقني يرتبط بالنظام التقني المثالي للمحررات الالكترونية، وبالرغم من عدم وجود نظام تقني يعطي مستوى الأمان المطلق بمصداقية هذه المحررات، فإن دور المشرع لا بد أن يظهر بتنظيم الوسائل التقنية لضمان الثقة والأمن عند تعامل الأفراد بها، ومن أبرز النظم التقنية التي نظمتها التشريعات المتقدمة هو نظام التشفير، وهذه النظم التي تم ابتكارها تجعل من الصعب التلاعب بالمحررات الالكترونية وتعطي مصداقية وثقة عالية عند أثبات التصرف القانوني عن طريقه[2].

[1] - إيمان طارق مكي الشكري، زيد عماد الموسوي، الحماية الخاصة للمشتري في عقد البيع الإلكتروني، مجلة الحلبي للعلوم القانونية والسياسية، السنة السابعة، عدد03، 2015، ص.76.

[2] - عباس العبودي ، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.231.

1 ـ التعريف الفقهي لنظام التشفير:

عرفه بعض الفقه بأنه: **" التغيير الذي يطال شكل المعلومات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات تحول دون قراءتها أو تغييرها"**[1].

عرفه البعض الآخر بأنه: **" كل العمليات التي تؤدي بفضل البروتوكولات السرية إلى تحويل معلومات أو إشارات مفهومة، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية، فهو مجموعة من التقنيات التي تسمح بحماية المعلومات من أي تعديل غير مرغوب فيه أو الحفاظ على خصوصيتها من أي اختراق، بفضل الاستعانة برموز خاصة يطلق عليها "المفاتيح"**.[2]

عرفه البعض الآخر بأنه **: " عملية تحويل النص إلى رموز وإشارات غير مفهومة تبدو غير ذات معنى لمنع الغير من الاطلاع عليها، إلا الأشخاص المرخص لهم بالاطلاع على النص المشفر وفهمه، حيث تنصب عملية التشفير على القيام بتحويل النصوص العامة إلى نصوص مشفرة مع إمكانية إعادة النص المشفر إلى نص عادي بعد فك التشفير بمفتاح التشفير الذي تم إنشاءه للتشفير وفكه"**[3].

نلاحظ أن جل التعاريف التي قدمها الفقه جاءت في مجملها متشابهة وركزت أساسا على الدور والهدف من التشفير ووسائله وسبب وجوده، ولم يقدموا تعريفا واضحا حول معنى هذه التقنية، ولعل الأمر يرجع إلى كون هذه الوسيلة تقنية أكثر مما هي قانونية، كما أجمعوا على التأكيد في ذلك على أن التشفير تقنية تساهم بفاعلية في ضمان سرية المعلومات والمراسلات بين المرسل والمرسل إليه.

---

[1] ـ مشار إليه لدى:عبد الفتاح بيومي حجازي، مقدمة في التجارة الالكترونية العربية ، شرح قانون المبادلات والتجارة الالكترونية التونسي، دار الفكر الجامعي، الإسكندرية، 2004، ص.266.

[2] - BOCHURBERG Lionel ,Internet et commerce électronique, 2e édition, DELMAS , Paris,2001, p154.

[3] ـ مشار إليه لدى: سمير حامد عبد العزيز الجمال، نفس المرجع، ص. 217. لورنس محمد عبيدات، إثبات المحرر الالكتروني، مرجع سابق، ص.136.

عموما فإن التشفير ما هو إلا تدبير احترازي بقصد مواجهة الجرائم المرتكبة باستخدام التقنيات العلمية الحديثة والتدخلات غير المشروعة من الغير بقصد ضمان عدم تسرب المعلومات والبيانات المخزونة الكترونيا إلى الغير، حيث يقوم الترميز أو التشفير بالحيلولة دون الدخول غير المشروع للغير في الاتصالات والمبادلات التي تتم بين طرفي العقد، لأنه يكون أمام نص مشفر عبارة عن رموز غير مفهومة وهذا يؤدي بالنتيجة إلى حمايته[1].

2 - التعريف القانوني لنظام التشفير في التشريعات المقارنة:

يعد استخدام تقنيات التشفير بوصفها من الوسائل المهمة التي تتضمن توفير الحماية والأمن والسرية في المحررات الالكترونية وهو من المسائل المعقدة والشائكة، لذلك فإن أغلب التشريعات التي نظمت هذه التقنيات تفاوتت بين إباحتها كليا وبين إخضاعها إلى إجراءات رقابية صارمة تصل إلى حضرها كليا .

أصدر الاتحاد الأوروبي مشروع نظام في 1998/5/15 فيما يتعلق باستخدام برامج الكتابة المشفرة داخل دول الإتحاد الأوروبي، يتضمن إطارا اتحاديا موحدا في موضوع المراقبة على تصدير معدات وأدوات التشفير، ويزيل هذا المشروع القيود القائمة على تبادل مثل هذه المعدات والأدوات بين الدول الأعضاء ويستبدلها بإجراءات مبسطة تنحصر بالتبليغ.[2]

اعترف المشرع الفرنسي بهذه التقنية وكان من الأوائل الذين أخذوا بها في ضمان أمن البيانات والمعلومات فعرفها بكونها: **" جميع الخدمات التي تسعى إلى تحويل معلومات أو إشارات واضحة إلى أخرى غير مفهومة من خلال اتفاقيات سرية، أو إلى إنجاز عكس هذه العملية، باللجوء إلى وسائل أو معدات أو برامج معلوماتية مسخرة لهذه الغاية"**[3].

[1] ـ عبد المجيد عصمت، أثر التقدم العلمي في العقد، مرجع سابق، ص.131.

[2] ـ عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.237.

[3] - Article 28 de la loi 90- 1170 du 29 /12/1990 sur la réglementation des télécommunications , dispose que : ***" On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles***

نلاحظ أنه من خلال هذه المادة أن المشرع الفرنسي أعطى تعريفا شاملا يحيط ويلم بكل جوانب التشفير، فهذا التعريف بين بوضوح المقصود بهذه التقنية من خلال بيان دورها وكيفية العمل بها.

عرف المشرع التونسي التشفير بأنه: " **إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول المعلومة بدونها**"[1] .

لم يكتف المشرع التونسي بإيراد تعريف التشفير، بل أشار أيضا إلى ضمانات آلية للتشفير، عند تحديده لمنظومة التدقيق في الإمضاء بوصفه مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الإلكتروني.[2]

جاء قانون التوقيع المصري خاليا من الإشارة لتحديد المقصود بالتشفير، وقد تم تدارك هذا الأمر من قبل اللائحة التنفيذية لهذا القانون، فعرفه في المادة (09/1) بأنه: **"منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونيا بحيث تمنع استخلاص هذه البيانات و المعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة"**[3].

عرفته أيضا في نص المادة (9/1) من اللائحة التنفيذية لقانون التوقيع الالكتروني رقم(15) لسنة 2005 بقرار وزير الاتصالات رقم (109) لسنة 2005 بأنه: " **منظومة تقنية حسابية**

---

pour des tiers, ou à réaliser inverse grace à des moyens, matériels ou logiciels conçus à cet effet", disponible sur le site: https://www.legifrance.gouv.fr

كانت قبل صدور هذا القانون حول تنظيم الاتصالات عن بعد في كل وسائل التشفير في فرنسا تندرج ضمن لائحة المصنفات العسكرية من الدرجة الثانية، مما يخضعها إلى مراقبة شديدة من قبل الدولة الفرنسية علما أن هذا القانون قد عدل بموجب قانون صدر بتاريخ 26جويلية1996، لتفاصيل أكثر، راجع : عمر خالد زريقات ، مرجع سابق، ص.269 .

[1] ـ المادة 5/2 من قانون التجارة الإلكترونية التونسي رقم 83 لسنة 2000 .

[2] ـ المادة 7/2 من القانون ذاته.

[3] ـ المادة(9/1) من اللائحة التنفيذية 109 لسنة 2005 لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري.

تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة ".

لم يعرف قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015 نظام التشفير لكنه أورد جملة تعريفات تتعلق بالمعاملات الالكترونية[1]، ففي نص المادة 02 من نفس القانون أشار إليه عند تعريفه للمفتاح الخاص في الفقرة 15 منها بأنه: " **الرمز الذي يستخدمه الشخص لإنشاء توقيع إلكتروني في معاملة الكترونية أو رسالة معلومات**"، وعرف المفتاح العام في الفقرة 16 منها بأنه: " **الرمز الذي تخصصه أو تعتمده جهات التوثيق الالكتروني لمستخدم شهادة التوثيق الالكتروني بهدف التحقق من صحة التوقيع الالكتروني**".

نصت المادة 01 من قانون التجارة الالكترونية البحريني رقم (28) لعام 2002، أن بيانات التحقق من التوقيع هي نفس البيانات التي تستعمل للتحقق من صحة التوقيع الإلكتروني، أو مفاتيح التشفير العامة.

أشارت المادة 02 من قانون المعاملات والتجارة الالكترونية الإماراتي رقم (2) لعام 2000، لنظام التشفير عند تحديدها لإجراءات التوثيق بأنها : " **الإجراءات التي تهدف إلى التحقق من أن رسالة إلكترونية، قد صدرت من شخص معين والكشف عن أي خطأ أو تعديل في المحتويات، أو في نقل أو تخزين رسالة الكترونية أو سجل الكتروني خلال فترة زمنية محددة، ويشمل ذلك أي إجراء يستخدم مناهج حسابية أو رموز أو كلمات أو أرقام تعريفية أو تشفير أو إجراءات للرد أو لإقرار الاستلام، وغيرها من وسائل إجراءاتي حماية المعلومات**".

لم يأتي المشرع الجزائري بتعريف للتشفير على نحو صريح كما هو في بعض القوانين الأخرى المذكورة سلفا أين بينت بوضوح معنى هذه التقنية، إنما ذكره تحت باب التعريفات في المادة02 من القانون 15-04 معرفا لمصطلح بيانات إنشاء التوقيع الالكتروني في الفقرة03 بأنها: "**بيانات فريدة كالرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الالكتروني**"، ثم عرف في الفقرة 05 من نفس المادة بيانات التحقق من التوقيع

[1] ـ يوسف أحمد النوافلة، حجية المحررات الالكترونية في الإثبات، مرجع سابق، ص.99.

الالكتروني بأنها: **"رموز أو مفاتيح التشفير العمومية أو بيانات أخرى مستعملة من أجل التحقق من التوقيع الالكتروني"**، ثم في الفقرة 08 عرف مفتاح التشفير الخاص بأنه: **"عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي"**، وكما عرف أيضا مفتاح التشفير العمومي في الفقرة 09 من نفس المادة بأنه: **"عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني، وتدرج في شهادة التصديق الالكتروني"**[1]، يمكن القول أنه من خلال هذا القانون المشرع تحاشى تعريف التشفير نظرا أن التشفير يصعب الإلمام بخفاياه فهو ذات طبيعة تقنية، فهو وسيلة تقنية أكثر مما هي قانونية لكنه بالمقابل اعتبره من بيانات إنشاء التوقيع الالكتروني يعتمد في استعماله من طرف الموقع عند إنشائه لهذا التوقيع، بالإضافة أنه حدد أن الغرض منه هو التحقق من التوقيع الالكتروني، كما حدد من خلال المادة 2 نوعي التشفير أين عرف كلا من المفتاح الخاص والمفتاح العام وميز بينهما على اعتبار أن المشرع أخذ بمعيار الوظيفة التي يؤديها كل منهما.

يتضح مما تقدم أن أغلب التشريعات التي ذكرناها سلفا عند محاولتها تعريف نظام التشفير أشارت إليه بصورة عرضية وهامشية، وكان من المفروض أن يكون تنظيم أحكام التشفير مسألة أساسية في هذه التشريعات، وذلك لأهمية هذا النظام بوصفه يوفر الأمن والسرية وسلامة إصدار المحررات الالكترونية عند التعامل بين الأفراد[2]، ومن جهتنا ومن وجهة نظرنا لهذا الموضوع يمكن القول أن عدم تقديم تعريف واضح لتقنية التشفير يعود ربما أساسا إلى كون هذا النظام تقني أكثر منه قانوني، وبالتالي يصعب على رجال القانون الإلمام بخفايا هذه التقنية.

نخلص مما سبق أنه بوجود وسائل مواجهة مهددات الأمن المعلوماتي خاصة منها التشفير الذي يعد أهم آليات حفظ البيانات والمعلومات، إلا أن هذه المواجهة تبقى دائما غير مجدية نظرا أن أغلب هذه الوسائل تتقادم مع التطور التكنولوجي التقني المتسارع رغم المميزات المتعددة لها، ونظرا للصفة الدولية التي تتميز بها نظم المعلومات، فلا بد إذن من أنظمة تشريعية رادعة

[1] - الماد 02 من القانون 15 - 04 المتعلق بالتوقيع والتصديق الالكترونيين.

[2] - عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.242.

تعاقب كل من اخترق أنظمة المعلومات واستولى عليها أو أتلفها أو دمرها، ومكافحتها عن طريق التعاون الدولي القضائي والأمني واستحداث هيئات دولية خاصة بهذا النوع من الجرائم.

ثانيا: الغرض من التشفير

يعد التشفير الآلية المثلى لحماية المحررات الإلكترونية والمحافظة على سرية البيانات والمعلومات وخصوصيتها، فهو يتيح إخفاء مضمونها من شكلها المقروء أو الواضح إلى شكل لا يمكن معه قراءة محتواها أو معاينتها إلا للمصرح لهم بذلك، فنظام التشفير ما هو إلا وسيلة تقنية مستخدمة للحفاظ على التوقيع الإلكتروني والكتابة الإلكترونية، كما يعتبر نظام أمان للتبادل الرقمي يقوم بوظائف السرية والحفظ و التأريخ [1] ، يمكن تلخيصها على النحو التالي:

1- توثيق الموقع:

ينسب تشفير الرسالة إلى الموقع في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد، ولا يمكن تزوير التوقيع الالكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر)، كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية[2].

2- توثيق الرسالة:

يعمل التشفير على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق، فعملية التثبت من الصحة تكشف أي تلاعب حيث أن أي مقارنة بين الواحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة تبين ما إذا كانت الرسالة هي نفسها عندما تم توقيعها[3].

[1] - RENARD Isabelle , Vive la signature électronique, DALLOZ ,paris, 2002 ,P19 .

[2] - عبد الرسول عبد الرضا جابر، محمد جعفر هادي، المفهوم القانوني للتوقيع الالكتروني، مجلة المحقق الحلبي للعلوم القانونية والسياسية، كلية القانون، جامعة بابل، السنة الرابعة ، عدد 01، 2012، ص.148.

[3] - عبد الرسول عبد الرضا جابر، محمد جعفر هادي، نفس المرجع، ص.148.

3- الفعالية:

تتطلب عمليات إنشاء التوقيع الالكتروني والتثبت من صحته بالتشفير مستوى عال من الضمان بأن التوقيع الالكتروني هو للموقع بدون تكلف أو رياء، مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة وتستغرق الكثير من الجهد بحيث أنه نادرا ما يتم استخدامها بالواقع، فإن التوقيعات الالكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيرا على الموارد المطلوبة للمعالجة[1].

يتضح مما سبق أن التشفير يعتبر أنجع وسيلة تضمن عدم الإتلاف والتحريف بمحتوى المحررات الالكترونية، وبالتالي الحفاظ على أهم مقوماتها المتمثلة في الأمان والثقة خاصة أثناء حفظها أو تبادلها، فالتشفير إذن هو ضرورة لا بد منه لحفظ المحرر الالكتروني وإمكانية إعادته إلى حالته الأصلية، والذي يعتبر مضمون الأمن التقني للمحررات الالكترونية.

ثالثا: أنظمة التشفير

يتم نظام التشفير من خلال استعمال المفاتيح الخاصة بعملية تشفير رسالة البيانات ومن ثم فك تشفيرها، وذلك عن طريق تحويل النص إلى إشارات ورموز غير مفهومة، ومن ثم إعادته إلى حالته الأولى التي كان عليها قبل التشفير، وبالتالي يسمح نظام التشفير كوسيلة مأمونة في إضفاء الثقة فيما يحتويه المحرر من معلومات إلى حماية المحرر الإلكتروني، وفي هذا الصدد توجد طريقتين للتشفير هما:

1 – نظام التشفير المتماثل:

يقوم نظام التشفير المتماثل على استخدام مفتاح واحد بمعنى أن كل من المرسل و المستقبل يستخدم نفس المفتاح السري لتشفير الرسالة وفك رموزها وقراءتها[2]، حيث يتفق الطرفان في

[1] - عبد الرسول عبد الرضا جابر، محمد جعفر هادي، مرجع سابق ، ص.148.

[2] - عمر حسن المومني التوقيع الالكتروني وقانون التجارة الالكترونية، مرجع سابق، ص.55. يوسف أحمد النوافلة، مرجع سابق، ص.101. هالة جمال الدين محمد محمود، أحكام الإثبات في عقود التجارة الالكترونية، دار النهضة العربية، القاهرة، 2012، ص.72.

التشفير بتحويل عبارة المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها ،ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة، فبعد أن يتم استقبال الرسالة، يستخدم المستقبل نفس عبارة المرور لفك النص المشفر، حيث تقوم برمجيات التشفير مرة أخرى بترجمة عبارة المرور عن طريق تشكيل المفتاح الثنائي الذي يتولى إعادة تحويل النص المشفر إلى شكله الأصلي المفهوم[1]، فالثقة في هذا النوع من التشفير يعتمد أساسا على الأمن والسرية في انتقال المفتاح بين المرسل والمرسل إليه.

عرف المشرع المصري المفتاح الخاص بأنه: **" أداة إلكترونية خاصة بصاحبها تنشأ بواسطة عملية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الالكترونية ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة"**[2].

نلاحظ من خلال تعريف المشرع المصري لمفتاح التشفير الخاص أنه استعمل مصطلح أداة قانونية وهو تعريف عام وشامل، بحيث أن هذه الأداة مرتبطة بصاحبها وخاصة بحيث يقوم الموقع عن طريق هذه الأداة بوضعها على المحرر الإلكتروني بطريقة خاصة تمكنه من الاحتفاظ بها على بطاقة ذكية توفر له الأمان اللازم عند استخدامها.

عرف المشرع الجزائري في نص المادة 02/ 03 من القانون 15-04 نظام التشفير المتماثل على اعتباره عنصرا في بيانات إنشاء التوقيع الإلكتروني فعرفه بأنه : **"بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني"**[3].

من خلال ما تقدم يمكن القول أن نظام التشفير المتماثل هو نظام يستخدم في عملية التشفير وفك التشفير نفس المفتاح، حيث يفرض على المرسل والمستخدم استخدام نفس المفتاح أثناء عملية التبادل أن يحافظا على سريته وعدم كشفه إلى أي طرف آخر، فمن ايجابيات هذا النظام

[1] - الصالحين محمد العيش، مرجع سابق، ص.14.

[2] - المادة(12/1) من اللائحة التنفيذية 109 لسنة 2005 لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري.

[3] - المادة 03/02 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

أن هذه العملية لا تحتاج إلى حاسب آلي كما يسهل أيضا إجراء عملية التشفير وفتح بيانات المحرر الإلكتروني، لكن يؤخذ على هذا النوع من التشفير أنه لا يحقق درجة كبيرة من الثقة والأمان، ذلك أن المفتاح المستخدم قد يتعرض وبكل سهولة إلى عملية الاختراق من قبل الغير أثناء عملية إرساله أو عند وصوله إلى متلقي الرسالة، ونظرا لعدم كفاءة هذا النظام لجأ خبراء تكنولوجيا المعلومات إلى إيجاد بديل له يحقق الغاية المرجوة منه، فلجئوا إلى إيجاد نظام يعتمد على وجود مفتاحين عام وخاص، أطلق على تسميته نظام التشفير غير المتماثل أو غير التناظري .

2 – أنظمة التشفير غير المتماثلة:

جاء استخدام هذا النوع من التشفير نتيجة العيوب التي ظهرت في نظام التشفير المتماثل، فكان لا بد من إيجاد نظام يحل محله، فظهر نظام التشفير غير المتماثل والذي يعتمد أساسا على مفتاحين: أحدهما خاص بشخص معين وهو يملك حق تغيير أو تعديل المحرر الإلكتروني، والآخر عام وهو مفتاح يكون معروفا للجميع، أي يكون معروفا للمرسل والمستقبل ولا يتم الاحتفاظ به سرا[1]، إذ يستخدم هذا الأخير للتشفير والمفتاح الخاص لفك التشفير، يتكون المفتاح الخاص من مجموعة من الرموز و الأرقام، التي يمكن تخزينها على بطاقة إلكترونية ويتم الوصول إليه عن طريق الرقم الشخصي لصاحبه، ويكون هذا المفتاح معروفا لطرف واحد فقط هو المرسل والذي يضل محتفظا بسريته ولا يستطيع أي شخص الإطلاع عليه أو معرفته، باستثناء الشخص الذي قام بالتوقيع[2]، ويستخدم هذا المفتاح لتشفير الرسالة وفك شفرتها[3]، إذ يقوم المرسل إليه بتشفير توقيعه بواسطة الرقم السري ويعيد إرسال الرد إلى المرسل والذي يتمكن بواسطة المفتاح العام من فك التشفير، وبذلك فإنه يتأكد من أن المرسل إليه هو الذي قام

[1] ـ علاء محمد نصيرات، مرجع سابق، ص.17.

[2] ـ عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، مرجع سابق، ص.219.

[3] ـ محمد المرسي زهرة، مرجع سابق، ص.17.

بإرسال الرسالة وهو صاحب المفتاح الخاص[1]، بالتالي فإن المفتاح العام وإن كان يختلف عن المفتاح الخاص إلا أنهما مرتبطان في عملهما ويكمل أحدهما الآخر.

عرف المشرع المصري المفتاح العام على أنه: **" أداة إلكترونية متاحة للكافة تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر الالكتروني والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي"**[2].

نلاحظ أن المشرع المصري استخدم مصطلح أداة الكترونية للتعبير عن المفتاح العام متاحة للجميع وذكر أن الغرض من هذه الأداة يتمثل أولا في التحقق من هوية الموقع على المحرر الإلكتروني، وثانيا التأكد من سلامة محتوى أصل هذا المحرر.

عرف المشرع التونسي هذا النظام في الفصل الثاني الفقرة 7 على اعتبار المفتاح العام الذي يقوم عليه نظام التشفير عنصرا في منظومة التدقيق قي الإمضاء الإلكتروني حيث نص على أن: **" منظومة التدقيق في الإمضاء مجوعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الإلكتروني"**.[3]

نلاحظ أن المشرع التونسي استخدم أيضا مصطلحا آخر لنظام التشفير غير المتماثل واعتبره منظومة تحتوي على مجموعة من المعدات والتي من خلالها يمكن التدقيق في الإمضاء الإلكتروني.

عرف المشرع الجزائري في المادة 05/02 نظام التشفير غير المتماثل بأنه: **" رموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى مستعملة من أجل التحقق من التوقيع الإلكتروني"**.[4]

---

[1] ـ يوسف أحمد النوافلة، حجية المحررات الالكترونية في الإثبات، مرجع سابق، ص.101.

[2] ـ المادة (11/1) من اللائحة التنفيذية 109 لسنة 2005 لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري.

[3] ـ الفصل 02 فقرة 7 من القانون رقم83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية التونسي.

[4] ـ المادة 02 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

نلاحظ أن المشرع الجزائري اعتبر أن نظام التشفير غير المتماثل هو النظام الذي يستعمل رموزا أو مفاتيح عمومية أو أية بيانات أخرى، من أجل التحقق من التوقيع الإلكتروني إلا أنه بالمقابل نجد أنه قدم تعريفا مستقلا لكلا المفتاحين الخاص والعام وربط بينهما، حيث أن المفتاح الخاص يرتبط بمفتاح تشفير عمومي يحوزه حصريا الموقع فقط، أما المفتاح العام فهو يكون موضوعا في متناول الجمهور الغرض منه التحقق من التوقيع الإلكتروني، بحيث أنه يدرج في شهادة التصديق الإلكتروني.

يلاحظ مما تقدم أن تعريف نظام التشفير غير المتماثل الذي أوردته مختلف التشريعات المذكورة تبين الدور والهدف من هذا النظام، وهو التحقق أو التدقيق من صحة التوقيع الالكتروني، بحيث أن مستعمل هذا النوع من التشفير يحتاج إلى مفتاحين أحدهما عام يكون متاحا لمن يرغب بالتعامل مع صاحب المفتاح، والآخر خاص يحتفظ به لنفسه بحيث يجب أن يكون سريا لا يعلمه إلا صاحبه ويكون الغرض منه فك التشفير، فكلا المفتاحين مرتبطان فيما بينهما .

يمكن القول من خلال ما تقدم أن هذه المنظومة يعيب عليها أنها بطيئة الاستخدام وذلك بسبب المساحة الحاسوبية الواسعة لها، كما أنه يمتاز بنوع من التعقيد[1]، حيث أنه يحتاج إلى وقت أطول من التشفير المتماثل للقيام بعملية التشفير ويحتاج إلى نفس الوقت لفك التشفير.

نستخلص مما سبق أنه بالرغم من وجود نظام التشفير إلا أن الأمر يحتاج إلى وجود جهة محايدة موثوقة تقوم بمعاينة تسليم المفتاح العام من المرسل إلى المرسل إليه، وكذلك تقوم بإصدار شهادات إلكترونية تحدد بواسطتها هوية المتعاملين وصحة المعلومات التي يقدمها الأطراف بواسطة رسائلهم.[2].

[1] ـ محمد إبراهيم عرسان أبو الهيجاء، مرجع سابق، ص.74.

[2] ـ إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، مرجع سابق، ص.183.

3 ـ أنظمة التشفير المزدوج:

استحدث في الآونة الأخيرة نظام جديد ثالث يجمع كلا النظامين وبالتالي تجاوز سلبيات النظامين السابقين، والغرض منه تحقيق أكبر قدر ممكن من الأمن والثقة، سمي بالنظام المزدوج .

تتم عملية التشفير باستخدام النظام المزدوج كالآتي:

أ ـ يقوم المنشئ بعد كتابة الرسالة بتشفيرها بالمفتاح المماثل.

ب ـ تشفير المفتاح المتماثل بالمفتاح العام للمرسل إليه.

ج ـ يتم إرسال كل من الرسالة المشفرة بالمفتاح المماثل، وكذا المفتاح المماثل المشفر بالمفتاح العام للمرسل إليه.

د ـ يقوم المرسل إليه عند استقباله للرسالة بفك شفرة المفتاح العام بواسطة مفتاحه الخاص به، حينها سيحصل على رسالة مشفرة مع المفتاح المتماثل، فيقوم بواسطة هذا الأخير بفك شفرة الرسالة، وبالتالي الحصول على محتوى الرسالة[1].

4- التشفير عن طريق تأمين تقنيات المحررات الالكترونية:

تستخدم هذه التقنية في تشفير مجموعة البيانات التي تتضمنها المحررات الالكترونية عبر وسائل الاتصال الفوري، إلى درجة تقتصر إعادة محتوى هذه المحررات على مرسلها والمستقبل فقط، بالتعاون مع نظام كاتب العدل الالكتروني، الذي يمنح شهادة الكترونية موثقة[2]،

[1] ـ محمد إبراهيم عرسان أبو الهيجاء، مرجع سابق، ص.75.

[2] ـ لتوضيح هذه العملية فإننا نفترض مثلا أن هناك شخصان(أ)و(ب) وكل واحد منهما يملك مفاتيح سرية ويريدان مراسلة بعضهما البعض بطريقة آمنة، فيقوم الطرف (أ) بتشفير الرسالة باستخدام مفاتيحه الخاصة، ثم يعيد تشفيرها باستخدام المفاتيح العامة للطرف (ب)، وعندما تصل الرسالة إلى (ب) فإنه يقوم بفك شفراتها بمفاتيحه الخاصة، ثم يفك تشفيرها مرة أخرى باستخدام المفاتيح العامة للطرف (أ)، وهكذا يستحيل على أي مخترق فك هذه الشفرة، إلا إذا حصل على المفتاحين العام والخاص لكلا الطرفين. راجع في ذلك: عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبان النظام القانوني لتجاوزها، مرجع سابق، ص.224.

وتحقق هذه التقنية ضمان الجمع بين سرية المعاملات التجارية وعقد صفقات أمنة، فحينما تقوم إحدى الشركات بإنشاء موقع لها باستخدام جهاز خدمة آمن، يقوم الحاسوبان عن طريق رموز حسابية ومفاتيح تشفير خاصة[1]، تستخدم تقنية تامين السندات في تفكيك هذه الرموز وإعادة جمعها وتزويد كل مستخدم بمفتاحين للتشفير، أحدهما خاص والآخر عام، وحينما يرغب أحد الأطراف بإرسال بيانات مشفرة يستخدم الطرف الثاني، مفتاح التشفير العام، لإتمام عملية الاتصال[2]، لذلك لا يمكن قراءة أي محرر إلكتروني مشفر إلا بعد مطابقة المفتاحين العام والخاص معا[3].

نخلص مما سبق أن عملية التشفير عن طريق المحررات الالكترونية ما هي إلا عملية تتم بصورة معكوسة للتشفير غير المتماثل، بحيث تتم هذه العملية عن طريق المفتاح العام للمرسل إليه والمفتاح الخاص للمرسل، ويفك التشفير بالمفتاح الخاص للمرسل إليه والمفتاح العام للمرسل.

[1] - عمر حسن المومني، التوقيع الالكتروني وقانون التجارة الالكترونية، مرجع سابق، ص.42.

[2] - عباس العبودي ، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، نفس المرجع، ص.230.

[3] - لتوضيح ذلك: نفترض أن هناك شخصان (أ و ب) ولدى كل منهما مفاتيح سرية ويريدان مراسلة بعضهما في شأن رسالة آمنة، فيقوم الطرف(أ) بتشفير الرسالة، باستخدام مفاتيحه الخاصة، ثم يعيد تشفيرها باستخدام المفاتيح العامة لدى الطرف (ب)، وعندما يقوم الطرف (ب) باستلام الرسالة متعددة الشفرات، يقوم أولا بفك شفرتها باستخدام مفتاحه الخاص و بالتالي، يصبح هو القادر وحده على فك شفرة الرسالة، ثم بعد ذلك يستخدم المفاتيح العامة لدى الطرف (أ)، من أجل استكمال عملية فك الشفرة، وهكذا يستحيل على أي شخص فضولي متلصص، فك شفرة هذه الرسالة إلا إذا حصل على مفتاحي التشفير الخاص والعام المتخصصين لكل منهما.راجع في ذلك: نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، مرجع سابق، ص.139.

الفرع الثاني
ضوابط التشفير

رغم الأهمية التي يكتسبها التشفير في ضمان الأمن التقني للمحررات الالكترونية، إلا أنه يجب مراعاة مجموعة من الضوابط و القواعد حتى يكون تشفيرا قانونيا ومشروعا يقوم بالمهام التي يتوخاها المشرع، تتمثل هذه الضوابط في مشروعية تشفير البيانات والمعلومات، الحق في خصوصية البيانات المشفرة، واعتبار النص المشفر محررا، يمكن تلخيص هذه النقاط الثلاثة كالآتي:

1 ـ مشروعية تشفير البيانات والمعلومات:

يعتبر تشفير البيانات والمعلومات التي يتم تدوينها عبر وسائط الكترونية أمرا مباحا من الناحية القانونية، فلم يتم التوصل إلى إيجاد نظام التشفير بمحض الصدفة وإنما عن طريق إجراء دراسات وأبحاث عدة، مما دعا أغلب التشريعات إلى وضع قواعد ونصوص قانونية تعالجه، فصدرت قوانين خاصة بالتجارة الإلكترونية لتعالج التشفير إلا أنها اختلفت في أسلوب معالجتها له، فنجد على سبيل المثال لا الحصر أن المشرع التونسي في القانون الخاص بالمبادلات والتجارة الالكترونية عالجه بشكل مباشر من خلال نصوص خاصة[1]، في الفصل الثالث، وأباح استخدامه في المراسلات عير الإنترنت وفي تصرفات التجارة الالكترونية وكافة التصرفات التي يتم بوسائل إلكترونية، حيث نص على أنه: **" يخضع استعمال التشفير في المبادلات والتجارة الالكترونية عبر الشبكات العمومية للاتصالات إلى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات"**[2].

[1] ـ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية،2002، ص.143

[2] ـ لورنس محمد عبيدات، مرجع سابق، ص.137.

تعامل المشرع التونسي في القانون الخاص بالمبادلات والتجارة الإلكترونية بشكل مباشر من خلال نصوص خاصة، وأجاز استخدامه في المراسلات الإلكترونية وفي التعاملات الإلكترونية التجارية عبر شبكة الإنترنت[1].

نص المشرع المصري على هذا الشرط في المادة (9/1) من القرار رقم 109 لسنة 2005 بخصوص تحديد الضوابط الخاصة بتشفير التوقيع الإلكتروني وبطاقات الائتمان وغيرها من البيانات التي يتم نقلها وتخزينها عبر وسائط إلكترونية، بحيث أنه اشترط على ذلك أن يتم استخلاص البيانات والمعلومات المقروءة الكترونيا فقط عن طريق استخدام مفتاح أو مفاتيح فك الشفرة، حيث نص على أنه: **" ... تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة"**.[2]

أشار المشرع الجزائري في المادة 02/ 06 من القانون 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين إلى آلية التحقق من التوقيع الإلكتروني باعتبارها جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني، كما أشار في المادة 09 /3 من نفس القانون أنه لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني.

2 ـ الحق في خصوصية البيانات المشفرة:

يقصد بالحق في خصوصيات البيانات المشفرة الحق في سرية البيانات والمعلومات المشفرة وذلك بالاعتراف أو الإقرار بحق الأشخاص بسرية البيانات المشفرة ومعاقبة كل من يتعدى عليها[3].

[1] ـ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001، ص.31.

[2] ـ المادة 9/1 من القرار رقم 109 لسنة 2005 المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري.

[3] ـ عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة، مرجع سابق، ص.136.

اعتبر مشروع قانون التجارة الالكترونية المصري أن الاعتداء على البيانات المرسلة بين طرفي العقد من خلال الإنترنت اعتداء على خصوصية طرفي العلاقة، لأن البيانات التي يتم تبادلها بين الطرفين تمتاز بالخصوصية وتعبر عن إرادتهم بالقيام بتصرف قانوني، واطلاع الغير على هذه البيانات من الممكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة والاعتداء على خصوصيتهم بمعرفة البيانات التي تم كشفها بعد فك التشفير[1]، كما عاقب كل من يقوم بانتهاك سرية البيانات المشفرة وإفشائها، سواء كان ذلك بشكل مباشر، أو عن طريق النص على أن أي اعتداء يقع على التجارة الإلكترونية يعد مخالفا لأحكام القوانين وبالتالي يعاقب العقوبة المقررة[2].

اعتبر المشرع التونسي أن الاعتداء على البيانات المرسلة بين طرفي العقد من خلال الإنترنت اعتداء على خصوصية طرفي العلاقة، بالإضافة إلى تأكيده على احترام سرية البيانات المشفرة وعاقب كل من يقوم أو يحاول القيام بالاعتداء عليها، سواء كان من خلال محاولة فك الشفرة، أم الإطلاع على محتوى البيانات بالشكل الحقيقي دون أخذ الإذن من طرفي العلاقة الذين أجريا عملية التشفير، هذا وقد وضع أيضا نصوصا في قوانين التجارة الإلكترونية تعاقب من يقوم بانتهاك البيانات المشفرة وسريتها وإفشائها[3].

نص المشرع الجزائري في المادة 68 من القانون 15-04 على هذا الشرط بحيث أنه عاقب كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من مليون دينار إلى خمسة ملايين دينار[4].

نص في المادة 69 من نفس القانون على أن كل من يخل عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة، يعاقب بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من عشرين ألف دينار إلى مائتي ألف دينار أو بإحدى هاتين العقوبتين فقط[1].

---

[1] ـ راجع في ذلك المواد 6، 7 8 و9 من الفصل الرابع من قانون التجارة الالكتروني المصري، مشار إليه لدى: لورنس محمد عبيدات، مرجع سابق، ص.138. عبد الفتاح بيومي حجازي، نفس المرجع، ص.206

[2] ـ مدحت عبد الحليم رمضان، مرجع سابق، ص.138.

[3] ـ المواد من 38-42 من قانون التجارة الإلكترونية التونسي رقم 83 لسنة 2000.

[4] ـ راجع نص المادة 68 من القانون رقم 15- 04 المتعلق بالتوقيع والتصديق الإلكترونيين.

نص أيضا في المادة 14 من نفس القانون على أنه يتم التأكد من طرف الهيئة الوطنية المكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه، من مطابقة الآلية المؤمنة لإنشاء التوقيع الإلكتروني الموصوف، والآلية الموثوقة للتحقق من التوقيع الإلكتروني الموصوف[2].

3 ـ اعتبار النص المشفر محررا إلكترونيا:

أقرت أغلب التشريعات بأن النصوص المشفرة لها حجية في الإثبات، بالتالي نتيجة لهذا الإقرار فإن النص المشفر يعتبر من المحررات الالكترونية التي تنتج عن الأجهزة الالكترونية بالرغم من أنها غير مفهومة للعامة، لأنه من السهل أن يتم تحويل الرموز والإشارات إلى نصوص مقروءة تكون حجة على من قام بمخالفة أحكام الاتفاق الذي أبرم والتي تكون في شكل رموز وإشارات غير مفهومة إلا بعد فك تشفير المحررات الكترونية، كونها يمكن تحويلها إلى نصوص مقروءة ومفهومة تكون لها حجية في الإثبات بمجرد فك التشفير[3].

نخلص مما تقدم أن تقنية التشفير هو ضرورة لا بد منها حتى لا تفقد أهم مقوماتها المتمثلة أساسا في الثقة والأمان في إثبات المعاملات الإلكترونية، وبالتالي لا بد من منع الغير من العبث بمضمون ومحتوى المحررات الإلكترونية ومعاقبة كل من يقوم بإفشاء البيانات والمعلومات وانتشارها، فالتشفير يعتبر من أهم الضمانات في الحفاظ على سلامة المعلومات والمعطيات وتأمين خصوصية وشرعية التعامل عن طريق المحررات الإلكترونية.

[1] ـ المادة 69 من القانون15ـ 04 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2] ـ المادة 14 من نفس القانون.

[3] ـ هدى حامد قشوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص.60.عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع سابق، ص.206. لورنس محمد عبيدات، مرجع سابق، ص.138.

المطلب الثاني

حفظ المحرر الالكتروني

تحيط بالمحرر الإلكتروني عدة مخاطر من لحظة صدوره من مصدرها إلى لحظة وصوله إلى المرسل إليه، مما دعا إلى ضرورة استخدام نظام حفظ إلكتروني يضمن الحفاظ على صحته والبيانات الواردة فيه وعناصره المرتبطة به، بشكل يحقق إسهاما فعليا في تطوير نظم المحافظة على هذه المحررات في شكلها الإلكتروني، بحيث يكون هذا النظام مستقل وغير خاضع لسيطرة منشئ هذه المحررات أو لسيطرة المعني بها، كما أن الاستخدام الأمثل لها يكفل لها الفعالية في التعامل والقبول في التعاملات الإلكترونية، كما أن التطور المتزايد في وسائل التكنولوجيات الحديثة أدى إلى ازدياد كمية البيانات والمعلومات الإلكترونية وتراكمها، مما أثار مشكلة كبيرة في حفظها وتخزينها لفترة طويلة، بالتالي جاء الحاسب الآلي لحل تلك المشكلة حيث يحفظ المعلومات بداخله دون حاجة إلى حيز كبير، فيتم الحفاظ على المحررات الإلكترونية في هذا الجهاز من خلال أوعية إلكترونية وكذلك الأقراص الضوئية الممغنطة، إلى غير ذلك من وسائل الاحتفاظ الأخرى التي أفرزتها لنا التكنولوجيا الحالية أو التي ستفرزها مستقبلا، بالتالي أمكن الاحتفاظ بها لمدة طويلة ربما تفوق قدرة الاحتفاظ بالمحررات الورقية التي تتأثر هي الأخرى بعوامل الزمن، بالتالي سنتناول في هذا المطلب أولا متطلبات عملية حفظ المحررات الإلكترونية في **(الفرع الأول)**، ثم بيان شروط حفظ المحررات الإلكترونية في **(الفرع الثاني)**.

الفرع الأول

متطلبات عملية حفظ المحررات الإلكترونية

تتطلب عملية حفظ المحررات الالكترونية أمرين، يتمثل الأمر الأول في الأمان الذي يستلزم استعمال ضوابط ومعايير معينة لحفظ المعلومات المدونة على الدعائم الالكترونية ضد التلف أو أي تعديل يمكن أن يرد عليها، بحيث إذا رجعنا إلى المحرر كان هو ذات المحرر المنشأ أو المرسل أو المستلم، وهذا يعتمد أساسا من خلال التزام كل مزود خدمات مصادقة إلكترونية مسك سجل إلكتروني لشهادات المصادقة على ذمة الأشخاص المعنيين والمستعملين له، بحيث يمكن الإطلاع على المعلومات المدونة فيه بصفة مستمرة وبشكل إلكتروني، أما الأمر الثاني هو الدوام، فلا بد من تبني التكنولوجيا في مجال حفظ واسترجاع المحررات وتداولها على أوعية إلكترونية، بالتالي سنتناول فكرة السجل الإلكتروني **(أولا)**، ثم فكرة حفظ المحرر الإلكتروني عبر الزمن أو الأرشيف الإلكتروني **(ثانيا)**.

أولا: السجل الالكتروني

يعد السجل الالكتروني من الأمور الهامة التي يتعين مراعاتها في مجال التبادل الالكتروني للبيانات، حتى إذا ثار نزاع بين أطراف التعامل أمكن حينئذ إقامة دعوى لإثبات الحق بناء على ما سجل من بيانات متبادلة داخل الكمبيوتر، أو قد يتم بغرض تقديمه كدليل أو مراقبته للتأكد من سلامته أو طباعته.

يحتوي السجل على العديد من البيانات الخاصة بالمعاملات الالكترونية، والتي من أهمها البيانات التالية:

- الهوية والبريد الالكتروني لصاحب السجل.
- الاسم والعنوان والهوية والبريد الالكتروني للطرف الأخر في العملية.
- تاريخ وزمان إرسال واستلام الرسائل الالكترونية.
- حجم التعامل بين الأطراف كما هو مبين في الرسائل المسلمة.

ـ نسخة طبق الأصل من السجل يحتفظ بها في الأرشيف.
ـ بيان المعايير الخاصة للتبادل الالكتروني للبيانات، التي تم تسليم الرسائل بموجبها وذلك كصيغة نموذجية يستخدمها الأطراف فيما بينهم بعد ذلك في المعاملات المستقبلية[1].

تحتاج غالبية المحررات التقليدية إلى وجود وسائل مكتوبة، أو سجل مادي ملموس يمكن للأطراف الرجوع إليه في حالة الشك أو الخلاف، فإنه في التعاقد الإلكتروني يوجد مثل هذا السجل في شكل رسائل بيانات إلكترونية، هذا السجل يحتفظ به وقتيا فقط حتى تمام التعاقد، وقد يكون الاطلاع عليه متاحا فقط للطرف الذي يتم إبرام العقد من خلال نظام المعلومات الخاص به[2].

يجب الافتراض بأن المعلومات التي تكون بصيغة سجل الكتروني صحيحة ما لم يستدل إلى وجود ما يناقض ذلك، كأن تكون الطريقة التي استخرج بها السجل الالكتروني أو خزن بها أو تم توصيله بها لا يمكن الاعتماد عليها، أو أن الطريقة التي تمت المحافظة بها على المعلومات لا يمكن الاعتماد عليها، أو نتج بفعل عامل آخر له علاقة بذلك[3].

1ـ الاعتراف القانوني بالسجل الإلكتروني:

نظرا لأهمية السجل الالكتروني في المعاملات الالكترونية فإن الاتفاقيات الدولية والتشريعات الوطنية الحديثة بشأن المعاملات الالكترونية تشترط وجود سجل إلكتروني، بحيث لا يجب أن يرفض الاعتراف سريان المعلومات أو صلاحيتها أو قابلية تنفيذها القانوني بالاستناد فقط إلى أنها محفوظة في هذا السجل، وعندما يشترط نص قانوني ضرورة أن تكون المعلومات محررة كتابيا فإنه يتم استيفاء ذلك الشرط بواسطة سجل الكتروني، شريطة إمكان الاطلاع على المعلومات التي يتضمنها بحيث يكون قابلا للاستعمال والرجوع إليه لاحقا عن طريق البث أو الطباعة أو غير ذلك.

[1] ـ خالد ممدوح إبراهيم، التقاضي الإلكتروني، مرجع سابق، ص.237.
[2] ـ خلد ممدوح إبراهيم، أمن المعلومات الالكترونية، الدار الجامعية، الإسكندرية،2008 ، ص.87.
[3] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص. 177.

يجب الافتراض بأن المعلومات التي تكون بصيغة سجل الكتروني صحيحة ما لم يستدل إلى وجود ما يناقض ذلك، كأن تكون الطريقة التي استخرج بها السجل الالكتروني أو خزن بها أو تم توصيله بها لا يمكن الاعتماد عليها، أو أن الطريقة التي تمت المحافظة بها على المعلومات لا يمكن الاعتماد عليها، أو نتج لأي عامل آخر له علاقة بذلك[1].

نص قانون الأونسترال في المادة 10فقرة 1 على شرط توافر سجل الكتروني يتضمن مجموعة من البيانات الخاصة بالأطراف، تاريخ ومكان إرسال واستلام الرسائل الإلكترونية[2].

نص التوجيه الأوروبي الصادر سنة 2000 بشأن التجارة الالكترونية في المادة (01/10) على أنه : **" الشخص الذي يعرض منتجات وخدمات من خلال نظم معلومات يمكن للجمهور الوصول إليها يلزم بأن يوفر وسائل لتخزين أو طباعة العقد، وليس هناك ما يخالف المنطق في اشتراط تقديم بيانات ومعلومات معينة أو توفير وسائل تقنية لإتاحة شروط العقد بطريقة تسمح بتخزينها لاسيما وأن التبادل الالكتروني للبيانات من الممكن أن يتم في ظل وجود اتفاق مسبق بين الأطراف"[3].**

قامت الجمعية الفرنسية للتوحيد القياسي[4] "AFNOR" في سنة 1998 بوضع معيار خاص بالسجلات الالكترونية أطلق عليه معيار أفنور للسجل الالكتروني، والغرض منه تحديد الشروط اللازمة والملامح الفنية الواجب توافرها في البيانات المسجلة إلكترونيا في أنظمة المعلومات

[1] - ، محمد أمين الرومي، المستند الالكتروني، مرجع سابق ص.177.

[2] - تنص المادة 1/10 من قانون الأونسترال النموذجي للتجارة الإلكترونية لسنة 1996 على أنه :**" عندما يقضي القانون بالاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضى إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية: تيسير الإطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقا، الاحتفاظ برسالة البيانات بالشكل الذي أنشأت أو أرسلت أو استلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشأت أو أرسلت أو استلمت، الاحتفاظ بالمعلومات إن وجدت التي تمكن من استبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها واستلامها".**

[3] - مشار إليه لدى: خلد ممدوح إبراهيم، أمن المعلومات الالكترونية ، مرجع سابق، ص.88.

[4] - الجمعية الفرنسية للتوحيد القياسي AFNOR هي منظمة حرفية أنشئت أثناء الحرب العالمية الثانية بمقتضى قانون صدر في 1941/05/24، وتضم المحترفين وعملائهم تحت إشراف الدولة، وقد قصد بها إيجاد قناة التعاون بين السلطات العامة والمحترفين باعتبارهم أهل الخبرة الفنية اللازمة لتحديد المواصفات القياسية للمنتجات، وتتولى هذه الجمعية إدارة مرفق عام يعني بالتوحيد القياسي.راجع في ذلك: خالد ممدوح إبراهيم، التقاضي الإلكتروني، مرجع سابق، ص.241..

ومدة وشروط صلاحية حفظ المحرر الكترونيا، ويوجد في هذا المعيار العديد من الاختبارات لنظم تأمين السجل الالكتروني من خلال عملية ا لتحكم والتشفير.

وضعت لجنة أفنور للسجل الالكتروني مجموعة من التوصيات التي يمكن اعتبارها الإطار العام للمواصفات الفنية، التي تبين كيفية إتمام عملية التسجيل إلكترونيا واسترجاع الوثائق الالكترونية بالحالة التي حفظت عليها، ومن هذه التوصيات:

- وضع نظام فني مرن الغرض منه التأكد من إتمام عمليات الحفظ اليومية بطريقة آمنة وخالية من سوء النية وليس فيها تحايل على القانون.
- إلزام المؤسسات والنشاطات التجارية بالقيام بالفحص الدوري والمنتظم لأنظمة السجلات الالكترونية وذلك بغرض اكتساب ثقة العملاء في عمليات التسجيل الالكتروني[1].

عرف القانون الموحد للإثبات الالكتروني الكندي السجل الالكتروني بأنه : **" البيانات التي يتم تسجيلها وتخزينها على وسائط أو بواسطة نظام كمبيوتري أو أية وسيلة أخرى مشابهة يمكن أن تقرأ أو تفهم بواسطة شخص أو نظام كمبيوتري أو أية وسيلة مشابهة وتشمل البيانات المقروءة أو المخرجات الكمبيوترية المطبوعة أو أي مخرجات أخرى من هذه البيانات"**[2].

أوجب المشرع التونسي في الفصل (14) من قانون المبادلات والتجارة الالكترونية على كل شخص طبيعي أو معنوي مختص بخدمة المصادقة والتوثيق الالكترونية الإمساك بسجل الكتروني، خاص بشهادة المصادقة على ذمة المستعملين مفتوح للاطلاع إلكترونيا بصفة مستمرة على المعلومات المدونة به، ويجب أن يتضمن عند الضرورة تاريخ تعليق شهادات

[1] - خلد ممدوح إبراهيم، أمن المعلومات الالكترونية، مرجع سابق، ص.91.

[2] - مشار إليه لدى: خالد ممدوح إبراهيم، التقاضي الإلكتروني، مرجع سابق، ص.234.

المصادقة وإلغائها، كما ألزم القانون كل مزود بخدمات مصادقة الكترونية بحماية هذا السجل الالكتروني من كل تغيير أو تحريف غير مرخص به [1].

عرف القانون الأردني للمعاملات الالكترونية رقم 15 لسنة 2015 في المادة (2) منه السجل الالكتروني بأنه: **" رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوع آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو نسخها أو إرسالها أو تبليغها أو تسلمها باستخدام الوسيط الإلكتروني"** [2].

أضاف المشرع الأردني في المادة 08 من قانون المعاملات الأردني على أنه: **" إذا استوجب القانون الاحتفاظ بمستند لأي سبب فيعتبر الاحتفاظ به على شكل سجل إلكتروني منتجا لآثاره، على أن تتوافر فيه الشروط المنصوص عليها في المادة 7 من هذا القانون"**، بحيث تنص المادة 07/أ من هذا القانون على أنه**: " إذا اشترط أي تشريع تقديم النسخة الأصلية من أي قيد أو عقد أو مستند أو وثيقة، فيعتبر السجل الالكتروني مستوفيا لهذه الشروط بتوافر ما يلي: حفظه بالشكل الذي تم به إنشاؤه أو إرساله أو تسلمه وبشكل يضمن عدم إجراء أي تغيير أو تعديل على محتواه، حفظه على نحو يتيح الوصول إلى المعلومات الواردة فيه واستخدامها والرجوع إليها في أي وقت، التمكن من التعرف على المنشئ والمرسل إليه وتاريخ ووقت إنشائه أو تسلمه..."** [3].

يتضح من خلال هذه النصوص أن السجل الالكتروني يشمل أي حامل أو وسيط أو دعامة معدة لإنشاء البيانات والمعلومات، أو حفظها أو إرسالها أو استلامها الكترونيا، ويعتبر منتجا لآثاره القانوني متى كان مستوفيا للشروط وهو حفظه من أي تعديل أو تغيير في محتواه والرجوع إليه عند الحاجة.

[1]- الفصل 14 من قانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية، ينص على أنه: **" على كل مزود خدمات مصادقة إلكترونية مسك سجل إلكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للإطلاع إلكترونيا بصفة مستمرة على المعلومات المدونة به، ويتضمن سجل شهادات المصادقة عند الاقتضاء تاريخ تعليق الشهادات أو إلغائها، ويتعين حماية هذا السجل وشهادة المصادقة من كل تغيير غير مرخص به ".**

[2] - المادة 02 من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015 السالف الذكر.

[3] - المادة 8 والمادة 7/أ من القانون ذاته.

يتمثل الهدف من استخدام السجل الالكتروني في توثيق المعلومات بطريقة تضمن سلامتها واسترجاعها كاملة عند اللزوم لأطراف التعاقد أو الأشخاص المرخص لهم بذلك، وهو ما يقتضي تهيئة بيئة تحمي السجل من كافة المؤثرات السلبية الطبيعية أو البشرية وتوفير الصيانة المستمرة و المنتظمة[1].

2- مزايا السجل الالكتروني:

يعتبر من أهم ايجابيات السجلات الالكترونية أنها تحتاج إلى حيز مكاني أقل مقارنة بالسجلات الورقية، ونظرا لزيادة الحاجة إلى حفظ السجلات أصبح من الضروري تقليل حجم المكان اللازم لهذه السجلات، وبالتالي تجميع كميات ضخمة من المعلومات في قرص أو أسطوانة مضغوطة لا تشغل أي حيز يذكر، فإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الاتصالات ولجأ إلى ضمان الأمن القانوني لها بما يحفظها، فإن هذه الإجراءات مع ذلك قد أفضت إلى استغلال الجناة لهذه الإجراءات في ارتكاب جرائمهم باستخدام وسائل اتصال يصعب اختراقها أو الوقوف على محتواها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة القوة والفاعلية في ارتكاب جرائمهم.

ثانيا: حفظ المحرر الإلكتروني عبر الزمن

يعرف حفظ المحرر الالكتروني عبر الزمن بأنه الحفاظ على البيانات الالكترونية في دعامة الكترونية بطريقة ثابتة لا يمكن تغييرها إلا من جانب المحتفظ بها، ويتحقق ذلك إذا كان المحرر الإلكتروني قابلا للاحتفاظ بالمعلومات والبيانات الواردة فيه، بمعنى أن تسمح طبيعته بحمل ما تم تدوينه عليه من معلومات، بالإضافة إلى إمكانية تخزينه لهذه المعلومات على الدوام بحيث يتسنى الرجوع إليه في أي وقت في حال نشوب خلاف في ذلك بن أطراف المحرر الإلكتروني مستقبلا، وهذا الأمر لا يمكن تحقيقه إذا ما كانت طبيعة الدعامة التي تم تدوين المعلومات عليها تتأثر بمرور الزمن[2]، ولإمكانية الحفظ الأحسن اقترح المتخصصون في المجال أن يتولى هذه

[1] - خلد ممدوح إبراهيم، أمن المعلومات الالكترونية، مرجع سابق، ص.91.

[2] - بشار محمد دودين، الإطار القانوني للعقد المبرم عبر شبكة الانترنت، دار الثقافة، عمان، 2006، ص.229.

المهمة مسئولا بمهمة الحفظ وتسمى : "مصلحة الأرشيف"، وهذا عن طريق مفتاح خاص غير معرض للفتح، ويشرف عليها مقدمي خدمات التصديق الالكتروني، مما يجعل من الدعامات الالكترونية ذات فعالية تضمن درجة عالية من الأمان ودليل ذلك الشهادة الالكترونية المقدمة من طرفهم.[1]

يجب على المسئول عن الحفظ أن يعد أرشيفا إلكترونيا يحفظ فيه كل الوثائق والبيانات الإلكترونية الملزم بحفظها، ويجب أن يضع في اعتباره أن هذا الأرشيف ممكن أن يستمر مدة طويلة[2].

يشترط على المسئول عند حفظ المحرر الإلكتروني تحديد وقت وتاريخ إنشاء المحرر الإلكتروني، فهو يتعلق أساسا بالتصرف القانوني المثبت في المحرر أكثر من تعلقه بالمحرر الالكتروني ذاته، ذلك أن تحديد زمن إنشاء التصرف تعد من الأمور الهامة التي يترتب عليها الكثير من الآثار في القانون المدني، فعلى سبيل المثال يمكن من خلاله معرفة ما إذا كان أحد الأطراف قد أبرم التصرف قبل بلوغه سن الرشد، أم بعد بلوغه ذلك السن، وهو ما يترتب عليه بالضرورة تحديد ما إذا كان بإمكانه التمسك ببطلان التصرف أم لا[3].

لكي يتم الحفظ لدى مسئول الأرشيف الالكتروني لا بد لصاحب المصلحة من القيام بجمع كل الوثائق والبيانات الالكترونية المراد حفظها، وأن يحدد ويبين في هذه الوثائق زمان وتاريخ المعاملة[4]، وأن يضع في اعتباره أن هذا الأرشيف يمكن أن يمتد لمدة طويلة، وأنه يمكن أن يطلب في أي وقت.

لم تذكر التشريعات الوطنية ولا الدولية مدة حفظ المحررات الالكترونية، بالتالي وانطلاقا بمبدأ التعادل الوظيفي الذي أخذت به أغلب التشريعات المقارنة أين ساوت بين المحررات

[1]- Alain Bensoussan, L'informatique et le droit , Tome 2, HERMES ,paris,1995, p.724

[2] - محسن عبد الحميد إبراهيم البيه، مرجع سابق ، ص.93 .

[3] - خالد ممدوح إبراهيم، إبرام العقد الالكتروني، مرجع سابق، ص.373.

[4] - أيمن سعد سليم، مرجع سابق، ص.56.

الالكترونية وبين المحررات التقليدية، فإن تحديد مدة قانونية لحفظ البيانات المدونة في المحررات الالكترونية أو مدة التقادم القانوني لهذه البيانات المثبتة والمحفوظة إلكترونيا، هي نفسها مدة التقادم الخاصة بالتصرفات القانونية التي تتم بالطرق العادية التقليدية[1].

يمكن أن نقول أن هدف الحفظ هو تأمين سلامة المحررات الإلكترونية من كل تحريف أو تغيير أو إتلاف وقابلة للاسترجاع حتى تؤدي دورها في الإثبات، فطبيعة المحررات الإلكترونية وخاصياتها تجعلها عرضة لمثل تلك المخاطر، وعلى اعتباره كذلك ينشأ على دعامة إلكترونية فإنه ينبغي حفظه أيضا على وسيط إلكتروني يضمن دوام البيانات والمعلومات التي يحتويها لمدة طويلة، لذلك فإن وسيلة الحفظ يجب أن تؤمن بقاء المحرر على شكله النهائي وتحميه من الأخطار السالفة الذكر.

الفرع الثاني

شروط حفظ المحررات الالكترونية

يعتبر تحقيق شرط حفظ المحرر الالكتروني مرهون بضرورة حفظ هذا المحرر على نحو يضمن سلامة البيانات التي يحتويها، وبقائها بنفس الشكل الذي تم به إنشاؤها أو إرسالها أو تسلمها طيلة مدة صلاحيتها، بحيث تتطابق بيانات المحرر والتوقيع الالكتروني المرسلين مع بيانات المحرر والتوقيع الإلكتروني اللذين وصلا إلى المرسل إليه حتى يمكن الرجوع إليه عند الحاجة، فالمحررات الورقية تسمح بالرجوع إليها بكل سهولة كذلك الحال بالنسبة للمحررات الالكترونية، لأنه يتم الاحتفاظ بالمعلومات والبيانات على وسيط إلكتروني يسمح لها بالبقاء مدة طويلة، وقد تكون مدة أطول من المحررات الورقية التي قد تتلف مع مرور الزمن سواء بفعل عوامل داخلية أو خارجية، فسنتعرض أولا إلى ضمان أصلية بيانات المحرر الإلكتروني **(أولا)**، ثم بعد ذلك نتطرق إلى إمكانية استرجاع المحررات الإلكترونية المحفوظة **(ثانيا).**

[1]- أيمن سعد سليم، مرجع سابق، ص.58.

أولا: ضمان أصلية بيانات المحرر الالكتروني

يرتبط مدى قبول المحرر الالكتروني كدليل في إثبات التصرفات القانونية التي تتم عبر الوسائط الالكترونية الحديثة، بضرورة حفظ هذا المحرر على نحو يضمن سلامة البيانات التي يحتويها من أي اعتداء يمس بها وبقائها بنفس الشكل الذي تم إنشاؤها أو إرسالها أو تسلمها.[1]

يقوم حفظ المعلومات طوال مدة التقادم التي يخضع لها التصرف المحفوظ وذلك ببقاء محتوى المحرر كما هو عند إنشائه، فضمان أصلية بيانات المحرر الالكتروني تقتضي مطابقة للبيانات الأصلية التي أنشأها المرسل، وعلى هذا فإن سلامة المحررات الالكترونية تقتضي إنشاء المحرر الإلكتروني في ظروف تضمن سلامته، وحفظه في ظروف تضمن هي الأخرى سلامته[2].

تفترض فكرة سلامة المحرر الإلكتروني أن يتم إنشائه على دعامات إلكترونية، بحيث يضل فيها طول مدة الحفظ على حالته التي أنشأ عليها دون تلف أو تعديل أو تدمير لمضمونه، فتحقق عنصر الثبات والاستمرارية بالنسبة لما دون عليها يحقق شرط ثبات مضمون المحرر الإلكتروني، وهذا ما يؤكد فكرة الترابط الوثيق بين سلامة المحرر ومضمونه وسلامة الدعامة التي حرر عليها.

تعد المحررات الالكترونية محفوظة بطريقة سليمة متى أمكن اكتشاف أي تعديل أو تغيير فيها وبقيت على حالتها الأولى وقت إنشائها، ولقد أوجد الباحثون عدة طرق للحفظ، وللتعرف أكثر على وسائل الاحتفاظ بالمحررات الإلكترونية، فإننا سوف نستعرض هذه الوسائل التي بدأت تنتشر مع انتشار المعلومات بواسطة الحاسوب الآلي، سواء كانت ممغنطة أو ضوئية أو عن طريق المصغرات الفيلمية أو غيرها من الوسائل، حيث من المتوقع أن تقيم بنوك المعلومات في المستقبل مستودعا للمخرجات و المحررات الإلكترونية، فعملية التخزين تتم

[1] - محمد محمد سادات، مرجع سابق، ص.199.

[2] - المرجع نفسه، ص.211 .

بوسائل علمية معدة خصيصا لهذه الأمور، فمن بين هذه الوسائل نذكر على سبيل المثال لا الحصر:

1 ـ المصغرات الفيلمية:

تقوم المصغرات الفيلمية على تصغير الوثائق وطبعها على أفلام صغيرة للرجوع إليها بسهولة ويسر عند الحاجة بعد تكبيرها إلى حجمها الاعتيادي بصورة فورية، فالمصغرات الفيلمية هي عبارة عن أوعية غير تقليدية للمعلومات، فهي تتيح للأفراد الذين يستخدمونها مشاهدة الصور المسجلة عليها بالبصر وذلك عن طريق طبعها بصورة مكبرة على مادة ورقية وتكبيرها مباشرة بواسطة جهاز القراءة[1].

استعملت المصغرات الفيلمية كوسيلة لحفظ وتخزين البيانات كبديل عن الأوراق، وذلك لسهولة حفظها وعدم حاجتها إلى مساحات واسعة للتخزين مثل الملفات والأوراق، ويتم ذلك باستخدام تكنولوجيا تسجيل المخرجات بصورة مصغرة جدا بدلا من تسجيلها بصورتها العادية، والتسجيل يتم على شرائح المايكرو فيش أو على الميكروفيلم[2]، فهذه الأخيرة مفيدة خاصة في الحالات التي لا يكون استخدام المخرجات كثيفا مثل الأرشفة[3].

2 ـ وحدة الأقراص الصلبة أو الجامدة:

يتميز القرص الصلب بسعاته التخزينية الكبيرة جدا، وكذلك بسرعة تسجيل واسترجاع البيانات التي تفوق سرعة الأقراص المرنة، وتتكون وحدة الأقراص الصلبة من مجموعة من الأقراص المعدنية الممغنطة والمرتبطة محوريا، ويتم تثبيت مجموعة من الأقراص الصلبة معا في محور واحد داخل غلاف محكم، وتتم قراءة البيانات أو كتابتها على القرص عن طريق عدة

[1] ـ محمد حسام لطفي، مرجع سابق، ص.11.

[2] ـ الميكروفيلم هو عبارة عن تصوير وتصغير للمعلومات الورقية على مادة فيلمية حساسة بحيث تصل نسبة التصغير إلى درجة لا يمكن معها قراءة المعلومات بالعين المجردة مما يستدعي الاستعانة بجهاز لقراءة هذه المعلومات، للمزيد راجع في ذلك:الصالحين محمد أبو بكر العيش، الجوانب القانونية لاستخدام المعلوماتية في المعاملات التجارية، بحث مقدم للمؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، الفترة 28-29 أكتوبر2009، ص.5.

[3] ـ عماد صباغ، نظم المعلومات، دار الثقافة،عمان، 2014، ص.66.

رؤوس للقراءة والكتابة[1]، ويتمثل الغرض من وراء استخدام هذا النوع من الأقراص التي تحتويها معظم أجهزة الحاسبات الآلية، في قدرتها على الاحتفاظ بحجم هائل من البيانات بعد قطع التيار عن الحاسب الآلي، بحيث يستطيع القرص الصلب أن يحتفظ ويخزن البيانات والمعلومات الرقمية على هيئة مغناطيسية تدوم مدة زمنية طويلة.

3 ـ الأشرطة المنسابة:

تقوم الأشرطة المنسابة بتخزين البيانات في كتل تفصل بينهما أجزاء ميتة غير مستخدمة تسمى فجوات الأشرطة المنسابة، في الجانب الآخر تقوم بخزن البيانات من دون كتل أو فجوات، وهذا يعني أن البيانات ستجرى من دون توقف أي أنها تكتب وتقرأ دون توقف أو البدء من جديد، ويمكن أن تكون هذه التكنولوجيا ذات فائدة عند استخدامها لحفظ نسخ إضافية من البيانات[2].

نخلص في الأخير أن حفظ المحرر الإلكتروني يتعلق أساسا بوسيلة حفظه، حيث أن حفظه يتطلب تحديد وسائل الحفظ وتبيان الشروط الواجب توفرها بالنسبة لتلك الوسائل من ناحية، ومن ناحية أخرى نجد أنه لا يمكن أن تكون هذه الوسائل بمنأى عن الأخطار الداخلية أو الخارجية، إذ قد يحدث وأن تتعرض ذاكرتها أو برامجها وأنظمة تشغيلها التقنية إلى عطل سواء متعمد أو غير متعمد، ينشأ عنه إصابة هذه الوسائل والأجهزة بخلل قد يتسبب في إزالة أو محو كلي أو جزئي للمعلومات و البيانات الواردة فيها أو بواسطتها، كما يمكن التلاعب في بيانات الحاسب الآلي من طرف أشخاص غير مرخص لهم باستعمال هذه الأنظمة، فهذه الوسائل هي دائما عرضة للتغيير نظرا للتطور التقني التكنولوجي السريع والمستمر في مجال تكنولوجيا المعلومات والاتصالات، فهذه المسألة تعتبر واردة بحسب الطبيعة التقنية والفنية لوسائل الاتصال خاصة والوسائل التكنولوجية بصفة عامة.

[1] ـ فيصل سعد غريب، التوقيع الالكتروني وحجيته في الإثبات، مرجع سابق، ص.156.

[2] ـ عماد صباغ، نظم المعلومات، مرجع سابق، ص.74.

ثانيا: قابلية المحررات الإلكترونية المحفوظة للاسترجاع

يشترط للاحتجاج بمضمون المحرر الإلكتروني أن يكون تدوين الكتابة على وسيط يسمح بثباتها عليها واستمرارها دون تبديل أو تعديل، من خلال نظام النص الثابت الذي لا يمكن التدخل فيه أو تعديله، بمعنى قراءة البيانات التي يتم تخزينها بها بنفس الطريقة التي احتفظت بها، بحيث يستدعي ذلك إمكانية قراءة مضمون المحرر مدة من الزمن حتى يتسنى الرجوع إليه كلما تعين ذلك أيا كانت الدعامة المحفوظة عليها الكتابة، فمفهوم سلامة المحرر الإلكتروني لا يقتصر على لحظة إنشائه بل يمتد إلى لحظة استلامه، بمعنى التأكد من أن المحرر الإلكتروني الذي تم استلامه هو نفس المحرر الالكتروني الذي تم إنشائه واستلامه.

نصت على هذا الشرط عدة تشريعات من بينها:

أشار قانون الأونسترال النموذجي للتجارة الإلكترونية بصدد ذكرها للشروط الواجب توافرها في المحرر الإلكتروني في المادة 10 على شروط الاحتفاظ برسائل البيانات[1]، ومن بينها إمكانية الاطلاع على المعلومة الواردة في المحرر الإلكتروني بما يتيح استخدامها في أي وقت لاحق، ويمكن الاستعانة بخدمات شخص آخر لتحقيق ذلك.

نص القانون الأردني في المادة (2/أ/7) بأنه: "**...حفظه على نحو يتيح الوصول إلى المعلومات الواردة فيه واستخدامها والرجوع إليها في أي وقت...**"[2].

لم يحدد المشرع في المادة 323 مكرر 1 من القانون المدني الجزائري الظروف التي تضمن سلامة المحرر، ولم يحدد معايير الحفظ الكفيلة بضمان السلامة، وذلك عند ما اشترط أن يكون المحرر معدا ومحفوظا في ظروف تضمن سلامته، يمكن من خلال نص هذه المادة القول أن المشرع الجزائري ترك المجال مفتوحا أمام أي تطور قد يظهر مستقبلا في وسائل وتقنيات

[1] - راجع في ذلك المادة 10 من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996.

[2] - قانون المعاملات الإلكترونية الأردني رقم15 لسنة2015 على الموقع : http://www.cbj.gov.jo/

الحفظ، بالتالي يجوز نقل محتوى المحرر إلى دعامة جديدة بمواصفات الدعامة السابقة التي أنشأ عليها ما دام يستوفي ذلك على شرط المحافظة على سلامة المحرر.

يمكن القول إذن أنه حتى يحقق الحفظ إمكانية استرجاع البيانات الموجودة في المحرر الإلكتروني في الصورة التي أنشئت بها لأول مرة، يجب أن تدون الكتابة على دعامة تحفظها لفترة طويلة من الزمن بحيث يمكن الرجوع إليها لاحقا[1].

يخضع تقدير مدى صحة البيانات المحفوظة إلكترونيا لتقدير قاضي الموضوع، كما أن على الشخص المسئول عن الأرشيف الالكتروني، أن يقدم كل المعلومات المتعلقة بالبيانات والمعلومات المحفوظة وكيفية الحفظ ووسيلة الحفظ إلى قاضي الموضوع، وذلك كلما استدعت الحاجة إلية بطلب من المحكمة أو من الأطراف، فسلامة المحرر الإلكتروني لا تكمن فقط في لحظة إنشائه بل يمتد أيضا على لحظة استلامه بمعنى عند الرجوع إليه، لأن المحرر الإلكتروني قد يكون عرضة للتعديل أو التغيير في بياناته، بالتالي حرصت أغلب التشريعات على بيان الضوابط التقنية والفنية لضمان الأمن القانوني للمحررات الإلكترونية، وهذا ما سنتطرق إليه بشيء من التفصيل في المبحث الثاني.

[1] - Thibault Verbiest, La protection juridiques du cyber- consommateur, LITEC ,Paris,2002 ,p.81.

المبحث الثاني

التصديق الإلكتروني كوسيلة لضمان سلامة المحررات الالكترونية

يعد ضمان الأمن القانوني للمحررات الالكترونية من أبرز التحديات التي تؤثر على تقدير مدى الحجية القانونية للإثبات بالمحررات الالكترونية، لأن انعدام هذا الأمن سيكون له تأثيرا واضحا على مدى مصداقيتها في مطابقتها للحقيقة في إثبات التصرفات القانونية.

يظهر عنصر الأمن القانوني في أمرين وهما الثقة ومدى انعكاسها على الوسيط الالكتروني المستخدم لتثبيت مضمون التصرف القانوني، والأمر الثاني هو أمان الوسيلة المستخدمة ويتعلق هذا الأمر بعدم وجود مسح للبيانات التي تتضمنها المحررات الالكترونية، وعليه فإن الإثبات بهذه المحررات يواجه تحديات تقنية حقيقة، وأن تجاهل هذه التحديات سوف يؤدي إلى انعدام الأمن القانوني في هذه المحررات وعدم ثقة الأفراد عند التعامل بها، لأن هذه المحررات تتعرض إلى التعدي الذي يهدف إلى التلاعب فيها.

اتسع مجال استخدام المحررات الالكترونية في الوقت الحالي أين أصبحت أغلب التعاملات الالكترونية والتصرفات القانونية تتم عبر شبكة الانترنت وعبر مختلف الوسائط الإلكترونية، وعليه لا بد من إيجاد بيئة الكترونية آمنة ومضمونة للأفراد المتعاملين عبر هذه الوسائل، واستوجب ذلك البحث عن آليات تستجيب لمقتضيات وخصوصية هذه التعاملات خاصة أن تدفق المعلومات عبر هذه الوسائط يهدد أطراف التعامل ويمس بخصوصياتهم، يعتبر أبرز دافع لضمان الأمن القانوني للمحررات الالكترونية هو إيجاد نظام يسمح بذلك بالشكل الذي يجعل المتعاملين يطمئنون لمثل هكذا تحديات، والتي أصبحت تكتسح كل مجالات الحياة المدنية منها والتجارية والإدارية وغيرها، فالمحرر الإلكتروني لا بد من توثيقه وذلك بتدخل طرف ثالث لدى جهة التصديق الإلكتروني التي تسلم شهادات المصادقة الإلكترونية للأطراف المتعاقدة التي تؤكد صحة المحرر الذي صدر لتكون حجة على من يدعي غير ذلك، بالتالي يتطلب إصدار أي محرر إلكتروني ذات قيمة قانونية توثيقه لدى جهة مختصة معتمدة، فالتوثيق يؤدي إلى الحفاظ على حقوق المتعاملين من أي اعتداء أو غش يمكن أن يمارس عليهم من الغير، فهو يترك أثر

بالغ الأهمية على المحرر الالكتروني سواء من حيث مصداقيته ومطابقته للواقع أو من حيث دعمه للثقة وضمان حقوق الأطراف المتعاملين به، والذي يتم عن طريق استخدامه تقنيات حديثة تعمل على وضع حلول لمشاكل التعامل بهذا النوع المستحدث من المحررات، ولتحقيق هذه الثقة يستلزم الأمر وجود طرف ثالث محايد موثوق به يؤكد هوية المتعاقدين، ويؤكد صدور الإرادة ممن نسبت إليه عن طريق إصدار شهادة المصادقة الالكترونية وهو ما يسمى بمؤدي خدمات التصديق الالكتروني، وعليه فسنتناول مفهوم التصديق الإلكتروني **(المطلب الأول)**، لنتعرض إلى شهادة التصديق الإلكتروني **(المطلب الثاني)**.

المطلب الأول

مفهوم التصديق الإلكتروني

لرفع مستوى الأمن والمصداقية في التعاملات الإلكترونية، لا بد من إيجاد حل تقني يساعد على أمن وسرية تبادل المعلومات ورسائل البيانات، ولا يتم ذلك إلا عن طريق توثيق المعلومات ورسائل البيانات والتصديق على محتواها بشكل يمكن التعرف على هوية الأطراف وصدورها عمن نسبت إليه دون تحريف أو تبديل، بالتالي لا بد من تعريف للتصديق الإلكتروني **(الفرع الأول)**، وتحقيقا لمستلزمات الثقة والأمان التي تعتبر من الضمانات الأساسية للتعاملات الإلكترونية، ظهرت الحاجة لوجود طرف ثالث مستقل عن أطراف العلاقة القانونية يعرف بجهة التصديق الإلكتروني **(الفرع الثاني)**.

الفرع الأول

تعريف التصديق الإلكتروني

يعتبر التصديق الإلكتروني وسيلة فنية آمنة تهدف إلى التحقق من صحة المحرر الإلكتروني، يتم نسبتها إلى جهة معينة أو طرف ثالث محايد، بهدف تأمين وحماية مضمون المحرر الإلكتروني وتحقيق الثقة والسلامة في المعاملات الإلكترونية، ولم يهتم الفقه والتشريع بتحديد تعريف للتصديق الالكتروني بالقدر الذي اهتم فيه بتعريف جهات التصديق الالكتروني، وعليه سنتناول التعريف الفقهي للتصديق الالكتروني **(أولا)**، ثم إلى تعريف التشريعات المقارنة له **(ثانيا).**

أولا: التعريف الفقهي للتصديق الالكتروني

وردت تعريفات فقهية عديدة للتصديق الإلكتروني:

عرفه جانب من الفقه بأنه: **" تقنية تكنولوجية مستخدمة في توثيق التوقيع الالكتروني، وذلك للتأكد من صحة التوقيع ونسبته إلى صاحبه، وكذا تأمين المحرر الالكتروني من أي تعديل أو تحريف[1]".**

يلاحظ أن هذا التعريف للتصديق الإلكتروني يعني تدخل الغير لضمان الرابطة بين الإمضاء وصاحبه دون تدخل منه بمضمون المحرر، الذي لا يمكن أن يدركه بحكم سرية المعلومة التي تتضمنه.

عرف جانب آخر التصديق الإلكتروني بأنه: **" وسيلة أو إجراء تقني يسمح بتحديد هوية المتعامل الالكتروني، وكذا المحرر الالكتروني وحمايته من أي غش أو احتيال، وذلك بالاعتماد على تقنية التوقيع الالكتروني وتصديقه واستخدام نظم معلوماتية موثقة تساعد على**

[1] - إيمان محمود أحمد سليمان، مرجع سابق، ص.306.

التأكد من صحة البيانات المتداولة بين المتعاملين، وذلك بالاعتماد على هيئات خاصة أو عامة تقوم بذلك تسمى مقدم خدمات التصديق الالكتروني"[1].

يلاحظ أن هذا التعريف تضمن تعريفا واضحا لمفهوم التصديق الالكتروني فهو ربط بين عملية التصديق الالكتروني وتقنية التوقيع الالكتروني، حيث أن عملية التصديق على التوقيع الالكتروني يثبت من خلالها هوية الموقع لأنه بدون هذا التصديق لا يمكن تحديد هوية الموقع بشكل قاطع، وبدونه لا يمكن للأطراف المتعاقدة عبر وسائل الاتصال الحديثة التأكد من هوية المتعاملين معهم، ومن ثم فإن شهادة التصديق تشهد بصحة التوقيع الالكتروني ونسبته لمن صدر عنه، فإذا قام أحد الأطراف بوضع توقيعه على محرر إلكتروني وضمنت جهة محايدة صحتها فإن ذلك يؤكد صدور التوقيع عن صاحبه.

ثانيا: التعريف التشريعي للتصديق الالكتروني

اهتم التشريع بالتصديق الإلكتروني لما له من دور في بعث الاطمئنان والأمان لدى المتعاملين إلكترونيا.

عرف قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015 في المادة 14/02 منه على أن التوثيق الالكتروني هو: **" التحقق من هوية مستخدم شهادة التوثيق الالكتروني وصحتها وصلاحيتها"**[2].

يلاحظ أن المشرع الأردني من خلال تعريفه للتوثيق الإلكتروني حدد الغرض والهدف من هذه الشهادة، وهو التحقق من الشخص المستخدم لشهادة التوثيق الالكتروني وصحة البيانات التي تتضمنها وصلاحية العمل بها .

عرف القانون الاتحادي للمعاملات والتجارة الالكترونية الإماراتي رقم 02 لسنة 2002 التصديق الالكتروني من خلال تعريفه لإجراءات التصديق الالكتروني المحكمة في المادة01

[1] ـ علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات، مرجع سابق، ص.126.

[2] ـ المادة 02 /14 من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015.

منه بأنها: **" الإجراءات التي تهدف إلى التحقق من أن الرسالة الالكترونية قد صدرت من أو إلى شخص معين، والكشف عن أي خطأ أو تعديل في محتويات أو في إرسال أو تخزين رسالة الكترونية أو سجل الكتروني خلال فترة زمنية محددة، ويشمل ذلك أي إجراء يستخدم مناهج حسابية أو رموز أو كلمات أو أرقام أو تشفير أو إجراءات للرد أو لإقرار الاستلام وغيرها من وسائل إجراءات حماية المعلومات"**[1].

يتضح من خلال هذا التعريف أن التصديق الالكتروني هو عبارة عن جملة من الإجراءات محددة من طرف أطراف العلاقة، وذلك للتأكد من أن الرسالة الالكترونية أو المحرر الالكتروني قد صدر من قبل شخص محدد، ويحقق الغرض المطلوب عن طريق الكشف عن أي خطأ أو تعديل في محتوياتها أو حتى في تحديد مدة تخزينها، أو أية إجراءات أخرى للتعرف على الرموز والكلمات والأرقام وفك التشفير.

عرف قانون المعاملات الالكترونية البحريني التصديق الالكتروني من خلال تعريفه لنظام الأمان، حيث نص في المادة 01 فقرة 18 منه على أنه : **" نظام يستخدم للتحقق من أن توثيقا الكترونيا أو سجلا الكترونيا يخص الشخص المعني، أو يستخدم لكشف أية تغييرات أو أخطاء في محتوى سجل إلكتروني طرأ عليه منذ أن تم بثه من قبل المنشئ"**[2] .

تعرض المشرع البحريني من خلال تعريفه للتصديق الالكتروني في الأساس إلى تعريف إجراءات التصديق الالكتروني تحت مصطلح نظام أمان، واقتصر تعريفه على بيان أهمية هذا النظام دون التطرق إلى الوسائل التي يمكن التحقق من خلالها، وجود أي تلاعب أو تحريف أو تعديل في محتوى المحرر الالكتروني بعد إنشائه من قبل صاحبه.

عرف المشرع التونسي التصديق الالكتروني من خلال الإجراءات المتبعة في التصديق، واستخدم في ذلك مصطلح منظومة التدقيق في الإمضاء، فنص في الفصل الثاني فقرة 07 على

[1] ـ المادة 01 من القانون الاتحادي رقم 1لسنة 2006 بشأن المعاملات والتجارة الإلكترونية الإماراتي.

[2] ـ قانون رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية البحريني .

أنها: **" مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الالكتروني"**[1].

يؤخذ على تعريف المشرع التونسي، أنه اقتصر فقط على ذكر العناصر المستخدمة في التدقيق في الإمضاء الالكتروني دون تحديد الغرض منه، ودون بيان الأهمية المرجوة من استعمال هكذا نظام.

لم يتطرق المشرع الجزائري إلى تعريف مصطلح التصديق الالكتروني كمصطلح خاص، بل اقتصر فقط على تقديم بعض التعريفات حول سياسة التصديق الالكتروني بحيث عرفها في المادة 15/02 من القانون 15-04 بأنها**: " مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الالكترونيين"**[2]، وكان بالأحرى أو الأجدر على المشرع الجزائري من خلال هذا القانون أن يفرد تعريفا مباشرا للتصديق الالكتروني كغيره من التشريعات الأخرى.

يلاحظ من خلال هذه التعريفات التشريعية والفقهية أنه مهما كانت تسميتها منظومة التدقيق الالكتروني أو نظام الأمان أو التوثيق الالكتروني، إلا أنها لم تعرف المقصود بها وإنما اقتصرت على تنظيمها لإجراءات التصديق والجهات المؤدية لهذه الخدمة والشهادات الصادرة عنها، إلا أن ما يمكن استخلاصه من خلالها أن التصديق الالكتروني هو عبارة عن جملة من الإجراءات المحددة من طرف أطراف العلاقة، وذلك للتأكد من أن المحرر الالكتروني قد صدر من قبل شخص محدد، وذلك باستعمال مختلف الوسائل التي يمكن التحقق من خلالها عدم وجود أي تلاعب أو تحريف أو تعديل في محتوى المحرر الالكتروني، والتحقق من صحته البيانات المتداولة بين المتعاملين، وذلك من التاريخ المحدد لإجراءات التوثيق مع الاحتفاظ بها في سجل الكتروني للاحتجاج بها في حال النزاع.

[1]- قانون رقم 02- 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية التونسي .

[2] - المادة 15/02 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

الفرع الثاني
جهة التصديق الإلكتروني

تتم أغلب المعاملات الالكترونية بين طرفين لا يعرف أحدهما الآخر مما أثار مشكلة سلامة وأمن تلك المراسلات والمعاملات، فشرط توافر عنصري الثقة والأمان بات أمرا ضروريا وملحا في مثل هذه العلاقة، فلا بد إذن من وجود طرف آخر في العلاقة تكون مهمته توثيق التعاملات بين الأطراف الذين يستخدمون الوسائط الالكترونية في معاملاتهم، وعليه عمدت أغلب التشريعات المتعلقة بالمعاملات الالكترونية إلى إيجاد طرف ثالث وظيفته توثيق وتأكيد هذه التعاملات بين أطراف التصرف، وهذا من خلال شهادة التصديق الإلكتروني التي تحتوي على مجموعة من البيانات وظيفتها توثيق العلاقة بين الموقع وتوقيعه الالكتروني، وهذه العملية يطلق عليها التصديق أو التوثيق الالكتروني، حيث أجازت التشريعات المقارنة تأسيس جهات تقوم بإصدار شهادات المصادقة الالكترونية المؤمنة بمصداقية توقيع الجهة الصادر عنها، حيث يستطيع كل طرف في التعامل التعرف على هوية الطرف المقابل وعلى مصداقية توقيعه بمجرد الاطلاع على شهادة المصادقة، وعليه سنتناول أولا تعريف جهة التصديق الالكتروني **(أولا)**، لنتناول شروط ممارسة نشاط مؤدي خدمات التصديق الالكتروني **(ثانيا)**،ثم مهام جهة التصديق الإلكتروني **(ثالثا)**، ثم نتعرض إلى التزامات مقدم خدمات التصديق الالكتروني **(رابعا)**، وفي الأخير نتناول مسئولية مقدمي خدمة التصديق الالكتروني**(خامسا)**، وذلك بشيء من التفصيل على النحو التالي:

أولا: تعريف جهة التصديق الالكتروني

تباينت الآراء الفقهية في تعريف جهة التصديق الإلكتروني واختلفت التشريعات المقارنة فيما بينها بشأن تحديد الجهة المختصة بوظيفة التصديق الإلكتروني، وعليه سنتناول التعريف الفقهي أولا، ثم إلى تعريف التشريعات المقارنة لجهة التصديق الإلكتروني ثانيا، وذلك على النحو التالي:

1- التعريف الفقهي لمؤدي خدمات التصديق الالكتروني:

تعددت التعريفات الفقهية حول مؤدي خدمات التصديق الالكتروني بحيث عرفه جانب منه على أنها: **"شركات أو أفراد أو جهات مستقلة ومحايدة تقوم بدور الوسيط بين المتعاملين لتوثيق معاملاتهم الالكترونية فتعد طرفا ثالثا محايدا"**[1].

عرفها جانب آخر بأنها : **" هيئة عامة أو خاصة، تعمل على ملئ الحاجة إلى وجود طرف ثالث موثوق في التجارة الالكترونية، بأن يصدر شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الالكتروني، كتأكيد نسبة التوقيع الالكتروني إلى شخص معين، وتأكيد نسبة المفتاح العام المستخدم إلى صاحبه، و تعتبر شهادة التصديق الالكتروني بمثابة بطاقة هوية الكترونية تستخرج من شخص مستقل ومحايد ومرخص له بمزاولة هذا النشاط "**[2].

تعرف أيضا بأنها: **" جهة مختصة طبيعية أو معنوية تعمل بترخيص من السلطات المختصة في الدولة، وتحت إشرافها ضمن أحكام تحدد نطاقها وماهية الواجبات الملقاة على عاتقها، ومدى مسؤوليتها عن الأضرار التي تلحق بالمتعاقدين شهادة إلكترونية مأخوذة عن سجل معلومات يحتوي بيانات متعددة تحدد هوية الموقع وربطها بالمفتاح العام"**[3].

نلاحظ من خلال هذه التعريفات أن جهة التصديق الإلكتروني هي هيئة عامة أو خاصة تعمل تحت إشراف السلطة المختصة في الدولة، تختص بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني، وذلك عن طريق وضع متطلبات فنية وتقنية مؤمنة تتفق مع حماية التوقيع الإلكتروني وقواعد البيانات.

---

[1] ـ مشار إليه لدى: عبد الفتاح بيومي حجازي، التوقيع الالكتروني، مرجع سابق، ص.210.

[2] -SEDALLIAN Valérie, Preuve et signature électronique , article disponible sur le site : www.juriscom.net/chr/2/fr20000509.htm.

[3] ـ مشار إليه لدى: عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، مرجع سابق، ص.113.

2- تعريف جهة التصديق الإلكتروني في التشريعات الوطنية والمواثيق الدولية:

سعت بعض المنظمات الدولية التي اهتمت بتنظيم المعاملات الالكترونية إلى وضع قوانين نموذجية وتوجيهات دولية، من أجل مساعدة الدول على وضع أطر تشريعية خاصة بالمعاملات الالكترونية، ونظرا إلى الدور المهم لمؤدي خدمات التصديق الالكتروني، صدرت العديد من التشريعات الوطنية التي سعت إلى تحديد وتنظيم القواعد المطبقة على الهيئات وكذا شهادات التصديق الصادرة عنها، واختلفت التشريعات الدولية والوطنية حول تعريف جهة التصديق الإلكتروني من حيث التسمية وحتى من خلال المهام التي منحتها لها هذه القوانين لهذه الجهة.

عرف القانون النموذجي للتوقيعات الإلكترونية سنة 2001 جهة التصديق الالكتروني وذلك في نص المادة 02 مصطلح " مقدم خدمات التصديق" فعرفه بأنه: **" شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية"**[1].

يلاحظ على هذا التعريف أنه ألزم جهة التوثيق بضرورة توفير خدمات التصديق الإلكتروني كحد أدنى، ومع ذلك هناك إمكانية لتقديم خدمات أخرى يكون لها علاقة بالتوقيع الإلكتروني، وهذا يعني إمكانية أن يكون نشاط أو خدمة التصديق الإلكتروني هو النشاط الوحيد الرئيسي لجهة التوثيق، كما يمكن أن يكون هذا النشاط هو أحد الأنشطة الفرعية لهذه الجهة[2].

نصت المادة 11/2 من المرسوم الخاص بالنموذج الأوربي المشترك للتوقيع الإلكتروني رقم 93 لسنة 1999 بشأن التوقيع الالكتروني على أنه: **" كل كيان أو شخص طبيعي أو معنوي يصدر شهادات أو خدمات متعلقة بالتوقيع الالكتروني، أو يتولى تقديم خدمات أخرى متصلة بالتوقيعات الالكترونية"**[3].

[1] - المادة(2) من القانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001 .

[2] - خالد ممدوح إبراهيم، التوقيع الإلكتروني، مرجع سابق، ص.175.

[3]- Article 2/11 de la directive 1999/93/CE du parlement européen et du Conseil, du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, dispose que: ***« Prestataire de service de certification toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques»,*** disponible sur le site : https://eur-lex.europa.eu/

يقصد بالخدمات المرتبطة بالتوقيع الإلكتروني التقنيات التي تسمح بإصدار توقيع نموذجي، أو خدمات النشر والإطلاع والخدمات المعلوماتية الأخرى كالحفظ والأرشيف[1].

أورد المشرع الفرنسي تعريفا يدخل في نفس سياق التعريف الذي أورده التوجيه الأوروبي، واستخدم مصطلح " مكلف خدمة التوثيق" وفقا للمادة 11/01 من المرسوم الصادر في 2001/03/30 بشأن تطبيق المادة 1316-04 من القانون المدني الفرنسي فعرفه بأنه: **" كل شخص يصدر شهادات تصديق إلكتروني أو يقدم خدمات أخرى تتعلق بالتوقيعات الإلكترونية"**[2].

يلاحظ أن المشرع الفرنسي ذكر كلمة شخص مثله مثل قانون الأونسترال فهي كلمة عامة تشمل الشخص الطبيعي والشخص المعنوي، فالمكلف بخدمة عامة هو إذن كل شخص معنوي أو طبيعي، مهمته إصدار شهادات التصديق الإلكترونية بالإضافة إلى قيامه بمهام أخرى ذات لها علاقة بالتوقيع الإلكتروني.

عرف المشرع التونسي مزود خدمات التصديق في الفصل الثاني الفقرة 4 بشأن المبادلات والتجارة الالكترونية لسنة 2000 بأنه: **" كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة، ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني "**[3].

يلاحظ أن هذا التعريف ركز في تحديده لمفهوم مزود خدمات التصديق على بيان الوظيفة الأساسية لهذه الجهة والتي تتعلق أساسا بإصدار شهادات المصادقة، بالإضافة إلى تقديمه خدمات أخرى ذات صلة بالإمضاء الإلكتروني.

---

[1]. زيد حمزة مقدم، النظام القانوني للتوثيق الإلكتروني، مجلة الشريعة والقانون والدراسات الإسلامية، جامعة إفريقيا العالمية، السودان، العدد 24،أوت 2014،ص.133، مقال منشور على موقع: http://dspace.iua.edu.sd/handle

[2]- Article 01/11 du décret 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, dispose que **:** ***« prestataire de services de certification électronique, toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ».***

[3]- الفصل 4/02 من القانون رقم 02-83 المتعلق بالمبادلات و التجارة الالكترونية التونسي لسنة 2000. على موقع: http://www.legislation.tn/

جاء قانون التوقيع الالكتروني المصري خاليا من أي تعريف لجهة التوثيق الالكتروني، فمزاولة نشاط إصدار شهادات التصديق الالكتروني لا يكون إلا بعد الحصول على ترخيص بذلك من الهيئة المختصة، وهي هيئة تنمية صناعة تكنولوجيا المعلومات وفقا للقواعد والإجراءات التي تحددها اللائحة التنفيذية[1]، لكن في اللائحة التنفيذية لقانون التوقيع الالكتروني المصري في المادة 01 فقرة 6 فقد عرفه بأنه: **" الجهات المرخص لها بإصدار شهادات التصديق الالكتروني وتقديم خدمات تتعلق بالتوقيع الالكتروني"**[2].

يلاحظ أن تعريف المشرع المصري لجهة التصديق الإلكتروني ركز على الأشخاص المعنويين فقط، وذلك باستخدامه كلمة جهة دون الأشخاص الطبيعية لإمكانية قيامهم بإصدار شهادات التصديق الإلكتروني، أو تقديمها لأية خدمات لها صلة بالتوقيع الإلكتروني، إلا أن هذه الجهة يجب أن يكون مرخصا لها من طرف السلطة المختصة.

تناول المشرع الجزائري جهة التصديق الإلكتروني في المادة 03 من المرسوم رقم07-162 **بأنه:"...مؤدي خدمات التصديق الالكتروني هو كل شخص في مفهوم المادة (8/8) من القانون رقم03/2000، يسلم شهادات الكترونية أو يقدم خدمات أخرى في مجال التوقيع الالكتروني"**[3].

[1] ـ خالد حسن أحمد، الحجية القانونية للمستندات الالكترونية بين الفقه الإسلامي والقانون الوضعي، مركز الدراسات العربية، 2016، ص.198.عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، مرجع سابق، ص.115.

[2] ـ المادة 01 /11 من اللائحة التنفيذية للقانون المصري رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[3]- المادة 03 من المرسوم التنفيذي رقم 07- 162 مؤرخ في 30 ماي 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123المؤرخ في 09ماي 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، المعدل و المتمم بالمرسوم التنفيذي رقم 07- 162 المؤرخ في 30ماي2007 ، الجريدة الرسمية للجمهورية الجزائرية، العدد37، صادر في07 جويلية 2007.

اعتمد المشرع الجزائري في المادة 8/8 من المرسوم رقم 03/2000 مصطلح **"موفر الخدمات"** حيث عرفه بأنه**: " كل شخص معنوي أو طبيعي يقدم خدمات مستعملا وسائل المواصلات السلكية واللاسلكية"**[1].

عرف المشرع الجزائري مقدم خدمات التصديق الإلكتروني من خلال نص المادة 02 من القانون04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه: **" أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية ، أو نظام للاتصالات ، وأي كيان آخر يقوم بمعالجة أو بتخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليه"**[2].

لسد الثغرات الموجودة في هذا المرسوم أصدر المشرع الجزائري قانونا خاصا وهو القانون رقم 15- 04 المتعلق بالتوقيع والتصديق الالكترونيين**.**

عرف المشرع الجزائري في المادة 12/02 من القانون 15-04 جهة التصديق الالكتروني بأنها**: "مؤدي خدمات التصديق الالكتروني شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكترونية موصوفة، وقد يقدم خدمات التصديق أخرى في مجال التصديق الالكتروني"**[3].

يجب الإشارة إلى أن المشرع الجزائري فرق بين مؤدي خدمات التصديق الإلكتروني وبين الطرف الثالث الموثوق بإصدار الشهادات لهيئات خاصة حددها في المادة 13/02من القانون 15-04، فعرفه بأنه شخص معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يقدم

[1] ـ المادة 8/8 من القانون رقم 2000-03 المؤرخ في 5أوت 2000 المتعلق بتحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، جريدة رسمية العدد 48 ، صادر في 06 أوت 2000.

[2] ـ المادة 02 من القانون 04/09 المؤرخ 05 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية العدد 47، صادر في 16 أوت 2009.

[3] ـالمادة 02/ 12 من القانون رقم 15- 04 المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، جريدة رسمية العدد 06، صادر في 20 فيفري2015.

خدمات أخرى متعلقة بالتصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي، تتمثل هذه الهيئات في:

- المؤسسات والإدارات العمومية والهيئات العمومية المحددة في التشريع المعمول به.
- المؤسسات الوطنية المستقلة وسلطات الضبط.
- المتدخلين في المبادلات ما بين البنوك.
- كل شخص أو كيان ينتمي إلى الفرع الحكومي بحكم طبيعته أو مهامه.

يلاحظ من خلال هذه التعريفات مهما كانت تسميتها مقدم خدمات التصديق أو جهة التصديق الإلكتروني، إلا أن جميعها تجعل المهمة الأولى لجهات التصديق الإلكتروني هي إصدار الشهادات الإلكترونية، وكذلك القيام بأية خدمات تتعلق بتلك الشهادات أو تكون متعلقة بالتوقيع الإلكتروني.

ثانيا: شروط ممارسة نشاط مؤدي خدمات التصديق الالكتروني

يتطلب مزاولة خدمة المصادقة الالكترونية توفر مجموعة من الشروط، فقد حدد المشرع الجزائري في المادة 34 من القانون 15- 04 شروط ممارسة نشاط مؤدي خدمات التصديق الإلكتروني في المادة 34 والتي تنص: **" يجب على كل طالب ترخيص لتأدية خدمة التصديق الالكتروني أن يستوفي الشروط التالية:**

- أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي.

- أن يتمتع بقدرة مالية كافية.

- أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي.

ـ أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الالكتروني"[1].

يلاحظ من خلال نص المادة أن المشرع الجزائري اشترط لمزاولة نشاط مؤدي خدمة المصادقة الالكترونية بالنسبة للشخص الطبيعي أن يتمتع بالجنسية الجزائرية، أما الشخص المعنوي فاشترط أن يكون خاضعا للقانون الجزائري.

اشترط أيضا المشرع الجزائري الحصول على ترخيص مسبق من سلطة البريد والمواصلات، وهذا طبقا لنص المادة 03 من المرسوم التنفيذي 01-123 المعدلة بالمادة 02 من المرسوم التنفيذي 07- 162[2] حيث ينص على أنه: " **يخضع لترخيص تمنحه سلطة الضبط البريد والمواصلات السلكية، إنشاء واستغلال خدمات التصديق الالكتروني، غير أن ترخيص مصالح التصديق الالكتروني يكون مرفقا بدفتر شروط يحدد حقوق وواجبات مؤدي الخدمات والمستعمل"**، فمزاولة نشاط مؤدي خدمة التصديق الالكتروني يقتضي الحصول على إذن مسبق من سلطة ضبط البريد والموصلات.

ثالثا: مهام جهة التصديق الإلكتروني

تتم أغلب المعاملات الالكترونية بين طرفين لا يعرف أحدهما الآخر، بالتالي فإن مهام مقدم خدمات التصديق الالكتروني تقوم من خلال إصدار شهادات إلكترونية لكل مشترك، تصادق على صحة المعلومات والبيانات الواردة فيها، كما أنها تقوم بدور هام في ضمان قبول التوقيعات الالكترونية والاعتراف بها قانونا، وضمان المعاملات الالكترونية وسلامة وتبادل البيانات والمحررات عبر شبكة الإنترنت، وضمان صدورها عن صاحبها والتأكد من ذلك، ويمكن حصرها من خلال التعريفات السالفة الذكر كالتالي:

[1] ـ المادة 34 من القانون 15 -04 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2] ـ المادة 02 من المرسوم التنفيذي رقم 07 -162 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

1 - إصدار شهادات التصديق على التوقيع الالكتروني:

منحت التشريعات المقارنة تراخيص لبعض الجهات التابعة للدولة تقديم خدمات التصديق الالكتروني وذلك في إطار قانوني وتقني، على أن تكون تلك التراخيص اختيارية وليست إجبارية، ومن الالتزامات التي يقدمها مؤدي خدمات التصديق الالكتروني باعتباره كجهة تصديق إلكتروني هي خدمة إصدار شهادات التصديق الالكتروني مع احترامه للنظام المعمول به، فقد نص المشرع في المادة 41 من القانون 15-04 على أن مؤدي خدمات التصديق الالكتروني هو المكلف بإصدار شهادات التصديق الإلكتروني، بشرط موافقة السلطة الاقتصادية للتصديق الإلكتروني وذلك طبقا لسياسة التصديق الإلكتروني الخاصة به[1].

2- التحقق من هوية الشخص الموقع:

يتم تحديد هوية المتعاملين في التعاملات الإلكترونية وتحديد أهليتهم القانونية للتعاقد والتعامل[2]، والتحقق من مضمون هذا التعامل وسلامته وكذا جديته وبعده عن الغش والاحتيال، ويكون لمقدم خدمة التصديق الالكتروني أن يطلب من الموقع عند تسجيل الشهادة ما يفيد صحة المعلومات الواردة بها وبصفة خاصة ما يتعلق بتحديد هوية الموقع[3]، فيجب على جهات التوثيق إمساك سجلات خاصة بالتواقيع الإلكترونية توضح فيها من الذي قام بهذه التوقيعات وما الذي تم إلغاؤه منها، ما ثم إبطاله، كذلك ما تم إيقافه وتعليق العمل به، فالسلطة التي تمنح الترخيص بإصدار هذه الشهادات شهادات التوثيق الإلكتروني هي سلطة واحدة، لكن مصدري هذه الشهادات قد يتعددون و ذلك بقيام الشركات التي تعمل في مجال خدمة الانترنت بوضع برامج إحداث التوقيعات الإلكترونية، ثم منح الشهادات بصحة هذه التوقيعات[4]، وفيما يخص الأشخاص المعنوية فقد نص المشرع الجزائري في المادة 44 من القانون 15-04 على أنه: **"يحتفظ مؤدي خدمات التصديق الالكتروني بسجل يدون فيه هوية وصفة الممثل القانوني**

[1] - راجع نص المادة 41 من القانون 15 - 04 المتعلق بالتوقيع والتصديق الإلكترونيين.

[2] - سعيد السيد قنديل، مرجع سابق، ص.90.

[3] - إيمان مأمون أحمد سليمان، مرجع سابق، ص.320.

[4] - حمودي ناصر، مرجع سابق، ص.310.

للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الالكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الالكتروني"[1]، ولا يمكن لمؤدي خدمات التصديق الالكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة وذلك نظرا لأهمية وخطورة هذه البيانات، ولا يجوز له أيضا أن يجمع إلا البيانات الشخصية الضرورية فقط لمنح وحفظ شهادة التصديق الالكتروني، بحيث لا يجوز استعمال هذه البيانات خارج نطاق نشاط التصديق الإلكتروني، ولا حتى إضافة أو حذف البيانات المقدمة له من طرف العميل ولا يمن له حفظ أو نسخ بيانات إنشاء توقيع الشخص الذي منحت له شهادة التصديق الإلكتروني الموصوفة[2].

3 ـ إصدار المفاتيح الالكترونية:

تتولى جهات التصديق الالكتروني إصدار المفاتيح الالكترونية سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الالكترونية، أو المفتاح العام الذي يتم بواسطته فك هذا التشفير، وعليه تضمن هذه الجهات أن المفتاح العام هو المناظر حيث تتحقق من تطابقه وصلاحية، كما تقوم هذه الجهة بإصدار التوقيع الرقمي، حيث يقوم طالب التوثيق بتقديم البيانات اللازمة على جهة التوثيق، ثم يتم إصدار المفتاح الخاص من جهاز حاسب آلي واحد فقط وذلك حتى يتم التأكد من أن التوقيع الرقمي صادر من صاحبه، لذا يتعين على الموقع بالمفتاح الخاص أن يحتفظ به سريا ولا يطلع عليه أحد بحيث لا يجوز لمن اتصل علمه بها بحكم عمله إفشاؤها للغير، أما المفتاح العام فتحتفظ به عادة جهة التوثيق، حيث تقوم بإرساله بالبريد الالكتروني إلى كل من يرغب في التعامل مع صاحب التوقيع الالكتروني وبذلك يمكن التحقق من صحة التوقيع، ويجب على جهة التوثيق أن تنقل التوقيع الالكتروني بمفتاحه الخاص بطريقة آمنة موثوق بها دون احتفاظ بصورة من التوقيع بمفتاحه الخاص[3].

[1] ـ المادة 44 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

[2] ـ راجع المادة 43 من القانون 15-04 من القانون ذاته.

[3] ـ سعيد قنديل، مرجع سابق، ص.81.

رابعا: التزامات مقدم خدمات التصديق الالكتروني

يتبين لنا من مراجعة قوانين المعاملات الالكترونية في التشريعات الوطنية أن العديد منها قد وضعت بعض الالتزامات التي يجب أن يتقيد بها مقدم خدمات التصديق الالكتروني، وهذا لضمان أمن وسلامة وسرية المعلومات والبيانات المتداولة، بحيث تكون هذه الضمانات كفيلة بإرساء الأمن القانوني ووضع الثقة فيه، تنقسم هذه الالتزامات إلى قسمين: التزامات فرضها القانون على مزودي خدمات التصديق الالكتروني والمتعلقة بنشاط وممارسة العمل من قبل تلك الجهات، أما القسم الثاني فهي الالتزامات المتعلقة بإصدار شهادات التصديق ومضمونها.

1- الالتزامات المتعلقة بمزاولة النشاط وممارسة العمل:

تتميز الالتزامات الملقاة على عاتق جهة التصديق الالكتروني بأهميتها العملية نظرا لما تقدمه خاصة في مجال دعم الثقة بين أطراف التعامل، وضمان أمن وسلامة وسرية المحررات الالكترونية المتداولة، وتتمثل الالتزامات الرئيسية التي تتعلق بمزاولة النشاط ومزاولة العمل من قيل جهات التوثيق الالكتروني في:

أ - الحصول على الترخيص اللازم من الهيئة المختصة قبل البدء في ممارسة نشاطه :

أشارت المادة 7 فقرة 1 من قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001 إلى هذا الشرط بنصها على أنه: " **يجوز لأي شخص أو جهاز أو سلطة تعينهم الدولة المشرعة جهة مختصة سواء كانت عامة أو خاصة**"[1]، حيث أن لكل بلد جهة تمنح التراخيص لمزاولة أعمال التصديق الالكتروني، وقد منحت التشريعات المقارنة تراخيص لبعض الجهات التابعة للدولة تقديم خدمات التصديق الالكتروني وذلك في إطار قانوني وتقني، على أن تكون تلك التراخيص اختيارية وليست إجبارية.

اعتمد المشرع الفرنسي على المبدأ الذي جاء به التوجيه الأوربي رقم 93 لسنة 1999 الخاص بالتوقيعات الالكترونية، ضمن المادة 1/03 والذي ألزم الدول الأعضاء بعدم فرض أية

[1] - المادة1/07 من قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001.

قيود على إنشاء سلطات التصديق أو تطلب أي ترخيص مسبق[1]، ووفقا لهذا المبدأ تكون هناك حرية في ممارسة نشاط إصدار شهادات التصديق الالكتروني، حيث يحق لأي هيئة أن تمارس هذا النشاط دون حاجة للحصول على ترخيص مسبق من السلطات الفرنسية، وضمن المشرع الفرنسي هذا المبدأ في المرسوم رقم 272 لسنة 2001 والذي يسمح التوجه الأوربي للدول الأعضاء إنشاء أنظمة الاعتماد وجهات التصديق الالكترونية، وبالفعل أنشأ المشرع الفرنسي نظاما لاعتماد جهات التصديق لكن هذا طوعي، بمعنى يحق لجهة التصديق الالكتروني أن تمارس عملها دون حاجة للحصول على اعتماد من قبل الجهة التي أنشأتها الدولة، ومقابل ذلك لها الحق في تقديم طلب لاعتمادها بشرط أن تتوافر فيها الشروط التي ينص عليها القانون، لكن يلاحظ أن الواقع العملي يجبر جهات التصديق على تقديم طلب لاعتمادها، والسبب في ذلك أن القانون الفرنسي اشترط لكي يتمتع التوقيع الالكتروني بالحجية يجب أن يتم التأكد من صحته بمقتضى شهادة التصديق الالكتروني المعتمد.[2]

يتولى في مصر مهمة منح الترخيص هيئة تنمية صناعة تكنولوجيا المعلومات وهذا في نص المادة 02 من قانون التوقيع الالكتروني رقم 15 لسنة 2015 التي نص على أنه: **" تنشأ هيئة عامة تسمى هيئة تنمية تكنولوجيا المعلومات."** [3] وجاء أيضا في نص المادة 19 من القانون المصري بشأن التوقيع الالكتروني على أنه: **" لا يجوز مزاولة نشاط إصدار شهادة التصديق الالكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها وفقا للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون."**[4]

[1] - Article 03/1 de la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, dispose que: ***« Les États membre ne soumettent la fourniture des services de certification à aucune autorisation préalable. »*** , sur le site : https://eur-lex.europa.eu/

[2] ـ سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دار الكتب القانونية، مصر، 2008، ص.417.

[3] ـ المادة 02 من قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004.

[4] ـ المادة 19 من القانون ذاته.

يتولى مراقب خدمات التصديق في تونس الوكالة الوطنية للمصادقة الالكترونية بموجب الفصل الثامن من قانون المبادلات التجارية الالكترونية بنصها على أنه: **" أحدثت مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي أطلق عليها اسم الوكالة الوطنية للمصادقة الالكترونية"**[1]، كما نص المشرع التونسي في الفصل 11 من نفس القانون على أنه: **" يتعين على كل شخص طبيعي أو معنوي يرغب في تعاطي نشاط مزود خدمات المصادقة الالكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية."**[2]

أما في القانون الجزائري فقد نص المشرع في القانون رقم 15- 04 لسنة 2015 المتعلق بالتوقيع التصديق الالكترونيين على سلطات التصديق الالكتروني وقسمها إلى ثلاثة أقسام :

- **السلطة الوطنية للتصديق الالكتروني:**

تطرق المشرع الجزائري في القانون15-04 إلى تشكيلة ومهام وسير السلطة الوطنية للتصديق الالكتروني ومهامها وسيرها، حيث عرف هذه السلطة في نص المادة 16 بأنها**: "سلطة إدارية مستقلة تنشأ لدى الوزير الأول تتمتع بالشخصية المعنوية والاستقلال المالي، تسمى السلطة الوطنية للتصديق الالكتروني وتدعى في صلب النص السلطة"**، ونص بموجب المادة 18 على أنه تكلف السلطة بترقية استعمال التوقيع والتصديق الالكترونيين، وتطويرهما وضمان موثوقية استعمالهما[3].

- **السلطة الحكومية للتصديق الالكتروني:**

عرف المشرع الجزائري السلطة الحكومية للتصديق الالكتروني وهذا في نص المادة من 26 من القانون 15- 04 بأنها: **" سلطة حكومية تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال تتمتع بالاستقلال المالي والشخصية المعنوية"**، كما بين في المادة 28 منه

[1] - الفصل 08 من قانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية التونسي.

[2]- الفصل11 من نفس القانون.

[3] - راجع نص المادة 18 من القانون من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين .

على الدور الذي تقوم بها عن طريق تكليفها بمتابعة ومراقبة نشاط التصديق الالكتروني للأطراف الثلاثة الموثوقة، وتوفير خدمات التصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي[1].

- **السلطة الاقتصادية للتصديق الالكتروني:**

أورد المشرع في المادتين 29 و30 من القانون 15 - 04 كل ما يتعلق بالسلطة الاقتصادية للتصديق الالكتروني، ففي نص المادة 29عرفها بأنها السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، كما أنه بموجب نص المادة 30 فإن السلطة الاقتصادية للتصديق الالكتروني تكلف بمتابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذين يقدمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور[2].

يمكن بناءا على ذلك أن تقدم جهات أن تقدم جهات حكومية أو مقدمو خدمات بالقطاع الخاص بالعمل كسلطات تصديق، ومن المتوقع ولأسباب تتعلق بالسياسة العامة أن لا يؤذن إلا للهيئات الحكومية بالعمل كسلطات تصديق، ويرى البعض أنه من المفترض أن تكون خدمات التصديق مفتوحة للمنافسة من جانب القطاع الخاص، وعليه فإن الدولة يجب أن تنظم هذه العملية وفق قوانينها والسماح لجهات عامة أو خاصة، بالترخيص بمزاولة نشاط اعتماد التوقيعات الالكترونية وإصدار الشهادات التي تفيد استيفاء التوقيع الالكتروني للعناصر التي توفر الثقة، وتضمن ارتباطه بشخص صاحبه، وارتباطه بالمحرر وتأمينه ضد أي تعديل أو تحريف، وما يلاحظ أن المشرع عندما يمنح تلك الجهات التراخيص المنصوص عليها فإن ذلك يكون في إطار تفويض منها لممارسة مهنة خاصة بها وتقوم بالرقابة عليها وتعهد إليها بالحقوق والالتزامات، حيث يرى معظم الفقه أن الأهلية والكفاءة تعد شرطا لاستمرار مزاولة مثل هذه الخدمة[3].

[1] - راجع نص المادة 26 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

[2] - راجع نص المادة 30 من نفس القانون.

[3] - خالد حسن أحمد، مرجع سابق، ص.201.

نلاحظ أنه رغم اختلاف التسميات إلا أنها تؤدي نفس المعنى فأغلبها ركز على نطاق عملها والمهام الموكلة لها، ويعتبر الحصول على ترخيص من الجهة المختصة قبل ممارسة النشاط نوعا من الرقابة تمارسها السلطة المختصة على هذا النوع من النشاط، وهو ما يبعث الثقة والأمان في المعاملات الالكترونية التي تتم بين الأطراف المتعاقدة.

ب ـ الالتزام بتأمين وحماية سرية المعلومات :

يتم إثبات مضمون التبادل الالكتروني عن طريق تعقب المواقع التجارية على شبكة الانترنت للتحري عنها وعن جديتها ومصداقيتها، فإذا تبين لها عدم أمن أحد هذه المواقع فإنها تقوم بتوجيه رسالة تحذيرية إلى المتعاملين معها توضح فيها عدم مصداقية هذه المواقع[1].

يلتزم مقدم الخدمة وضع متطلبات فنية وتقنية مؤمنة تتفق مع حماية التوقيع الالكتروني وقواعد البيانات، كما يجب على مقدم خدمة التصديق عدم إفشاء سرية البيانات الالكترونية، والمقصود بالسرية هنا هو واجب الحفاظ على البيانات الشخصية التي تتمثل بالمعلومات المتعلقة بهوية الشخص المحدد أو القابل للتحديد[2]، والتي قدمها العميل إلى الجهة المسئولة بإصدار الشهادات ويعتبر هذا الالتزام من أخطر الالتزامات الملقاة على عاتقه، وأكثر الالتزامات التي قد تقوم مسؤولية جهات التوثيق تجاه صاحب الشهادة الالكترونية، ويعتبر هذا الالتزام التزاما بتحقيق نتيجة ولا يقتصر على بذل عناية، فيجب أن تتحقق النتيجة المتمثلة في ضمان سرية البيانات بصرف النظر عن الوسيلة المستخدمة، وتقوم مسئولية جهة التوثيق بمجرد عدم تحقق النتيجة المطلوبة[3].

نص المشرع التونسي في الفصل الخامس عشر منه على أنه**: " يتعين على مزودي خدمات المصادقة الإلكترونية وأعوانهم، المحافظة على سرية المعلومات التي عهدت إليهم في إطار**

[1]ـ عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة، مرجع سابق، ص.103. إيمان مأمون أحمد سليمان، مرجع سابق، ص.315.

[2]- Arnaud-François fausse, op.cit, p.97.

[3] ـ إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به، دار الراية، عمان، 2009، ص.109.

تعاطي أنشطتهم، باستثناء تلك التي رخص صاحب الشهادة كتابيا أو إلكترونيا في نشرها، أو إعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل" [1].

يلاحظ أن المشرع التونسي أوجب على مزود خدمات المصادقة الإلكترونية وأعوانهم، الالتزام بالمحافظة على سرية المعلومات التي حصلوا عليها بسبب نشاطاتهم، باستثناء المعلومات التي سمح صاحب الشهادة كتابيا أو إلكترونيا بنشرها أو الإعلام بها، أو في الحالات المنصوص عليها في النظام المعمول به، بالمقابل لم يشر إلى نوعية البيانات والمعلومات التي يجب عدم نشرها والإعلام بها وعدم إفشائها، كما جاء الحظر عاما مطلقا باستثناء الحالة التي نص عليها القانون الجاري به العمل.

نص المشرع المصري في المادة 21 من قانون رقم 15 لسنة 2004 على أن **:" بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله".**

يلاحظ أن المشرع المصري ومن خلال نص المادة أنه ألزم جهة التصديق الالكتروني ومساعديهم بخصوص المعلومات والبيانات المتداولة فيما بينهم وفيما يخص عملهم، المحافظة على السرية وعدم استخدامها في غير الغرض، سواء التي قدمت إليهم أو التي هم على اتصال بها، وهو التزام مطلق يطبق على كل العاملين في خدمات التصديق الالكتروني بخلاف المشرع التونسي الذي أورد استثناءا على ذلك.

نص عليه المشرع الجزائري بنص المادة 42 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكترونيين أنه : **" يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة."** [2]

[1] ـ الفصل الخامس عشر من قانون المبادلات والتجارة الالكترونية التونسي رقم 83 لسنة 2000 .

[2] ـ المادة 42 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

نصت أيضا المادة 43 من نفس القانون أنه: **" لا يمكن لمؤدي خدمات التصديق الالكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة، ولا يمكن له أيضا أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الالكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى."** [1]

يلاحظ هنا أن المشرع الجزائري أن الالتزام الذي أورده في نص المادتين 42 و43 هو التزام عام ومطلق يلتزم به كافة مؤدي خدمة التصديق الالكتروني ولم يورد أي استثناء وإنما جاء الحظر مطلق وعلى كل المكلفين في خدمات التصديق الالكتروني.

2 ـ الالتزامات المتعلقة بإصدار شهادة التصديق الالكتروني:

يعتبر مؤدي خدمات التصديق الالكتروني المكلف بإصدار شهادة التصديق الالكتروني، والتي يطلق عليها كذلك اصطلاح بطاقة إثبات الهوية الالكترونية لمن يرغب في التأكد من صحة المحرر الالكتروني، أو التوقيع الالكتروني المرسل إليه من طرف صاحب التوقيع المتعاقد مع مزود الخدمات، ويمكن إيجازها في النقاط التالية:

ـ إصدار شهادات التصديق الالكتروني، وتسليمها وحفظها وفقا للترخيص الصادر له من الهيئة والضوابط والإجراءات التي تحددها اللائحة.

نص المشرع الجزائري في المادة 35 من القانون رقم 15-04 أنه **: " تمنح شهادة التأهيل لكل طالب الترخيص لتأدية خدمة التصديق الالكتروني قبل الحصول على الترخيص لمدة سنة واحدة قابلة للتجديد مرة واحدة، وتمنح لكل شخص طبيعي أو معنوي لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني، وفي هذه الحالة يتم تبليغ الشهادة في أجل أقصاه ستون يوما إبتداءا من تاريخ استلام الطلب المثبت بإشعار بالاستلام، ولا يمكن لحامل هذه الشهادة تأدية هذه الخدمة إلا بعد الحصول على الترخيص"**[2].

[1] ـ المادة 43 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين..

[2] ـ المادة 35 من القانون ذاته.

نلاحظ أن المشرع الجزائري ومن خلال نص هذه المادة قد وضع شروطا خاصة في غاية الصرامة لطالب إنشاء هيئات التصديق الالكتروني، كما حرص على ضرورة توفر مقدم خدمات التصديق على العناصر الأساسية اللازمة لتأدية خدمات التصديق الالكتروني، وهذا كله قبل حصوله على الترخيص.

3 ـ الالتزام بضمان صحة المعلومات المصدقة :

يعتبر القائم على خدمة التصديق مسئولا عن صحة البيانات التي صدق عليها، وكذلك عن نسبة التوقيع لصاحبه في تاريخ تسليم الشهادة لمن يتسلمها، وبالتالي يكون على مقدم خدمة التصديق إثبات عدم وجود أي إهمال أو خطأ في جانبه وهذا أمر دقيق فيما يتعلق بإثباته، وبذلك نجد أنه هناك التزاما على عاتق مقدم خدمة التصديق بإيجاد وسائل أمان للنظم التي يستعملها[1]، لأن أي نقص في أحد البيانات أو ثبت تزويرها، في هذه الحالة لا بد على الجهة المصدرة للشهادة الامتناع عن إصدارها[2]، فأهم واجب لجهة التصديق الالكتروني هو أن يضمن هوية صاحب الشهادة وصحة التوقيعات الواردة فيها، وأن تضع كل المعلومات المتضمنة شهادة المصادقة الصادرة عنها تحت تصرف المتعاملين، وبصورة خاصة عليها الإعلان عن تاريخ إصدار الشهادات وتاريخ انتهاء مدة صلاحيتها أو وقف مفعولها أو إلغائها[3].

يضمن مقدم خدمة التصديق الإلكتروني صحة البيانات الواردة في الشهادة له عند إصدارها وله أن يطلب من طالبها كل ما يفيد من وثائق تأكيد هويته، والتي لا يتحمل مسؤولية تزويرها من قبل مقدمها ففي حالة حدوث التزوير من صاحب الشأن سواء كان تزويرا ماديا أو معنويا، فلا يكون مقدم خدمة التصديق مسئولا عن البيانات المسجلة في الشهادة[4]، كما أنه يجب على الغير أن يتأكد من صلاحية شهادة التصديق، وذلك من حيث مدتها وما لحقها من تعديل أو

[1] ـ سعيد السيد قنديل ، مرجع سابق، ص.92.

[2] ـ عاطف عبد الحميد حسن، التوقيع الالكتروني، دار النهضة العربية ، القاهرة، 2008، ص.109.

[3] - Arnaud-François fausse , op.cit, p111.

[4] ـ خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني، دار الجامعة الجديدة ، الإسكندرية ، 2007، ص.152. خالد حسن أحمد، الحجية القانونية للمستندات الالكترونية بين الفقه الإسلامي والقانون الوضعي، مرجع سابق، ص.208.

إلغاء، والغرض من استخدامها وذلك بالرجوع إلى السجل الإلكتروني الذي ينشره مقدم خدمة التصديق عبر الانترنت[1].

يرى الفقه أن جهة التصديق لا تكون مسئولة إلا عن البيانات الصحيحة التي يقدمها لها العميل، إلا أن على جهة التصديق فحص البيانات المقدمة إليها من خلال الوثائق المرسلة والتحري فيما إذا كانت تلك البيانات مزورة أو مغلوطة، فإذا ثبت التزوير من قبل مقدم الوثائق، فإنه لا تقع على عاتق الجهة التي أصدرت الشهادة أية مسئولية، إذا كان ظاهر هذه البيانات لا يدل على تزويرها أو انتهاء سريانها بصورة معقولة[2]، فيعتبر مقدم خدمة التصديق غير مسئول عندما يضع حدودا للشهادة التي قام باعتمادها والتصديق عليها سواء من حيث المدة أو حدود الصفقة، وذلك عندما يقوم المشترك باستخدام هذه الشهادة متجاوزا حدودها، مثل استخدامها بعد انتهاء صلاحيتها أو إبرام صفقة بمبلغ يجاوز المبلغ المحدد في الشهادة لإبرام الصفقات، ففي هذه الحالات يكون المسئول هو المشترك مستخدم الشهادة و ليس مقدم خدمة التصديق[3].

نص المشرع الجزائري على هذا الالتزام من خلال نص المادة 44 /01 من القانون 15-04 على أنه: **" يجب على مؤدي خدمات التصديق الالكتروني، قبل منح شهادة التصديق الإلكتروني، أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع"**[4].

كما نص أيضا في نص المادة53 من القانون 15-04 بأنه: **" يكون مؤدي خدمات التصديق الإلكتروني الذي سلم شهادة تصديق إلكتروني موصوفة، مسئولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الإلكتروني هذه، وذلك فيما يخص صحة جميع المعلومات الواردة في شهادة التصديق الإلكتروني الموصوفة في التاريخ**

[1] - سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة ، مرجع سابق، ص.346 .

[2] - عيسى غسان الربضي، مرجع سابق، ص.132.

[3] - سعيد السيد قنديل، مرجع سابق، ص.96 .

[4] - المادة 01/44 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

الذي منحت فيه، ووجود جميع البيانات الواجب توفرها في شهادة التصديق الإلكتروني الموصوفة ضمن هذه الشهادة."[1].

نلاحظ أن المشرع الجزائري أقر بمسؤولية مزودي خدمات التصديق الالكتروني، الأمر الذي يبعث الثقة والأمان والسرية للمعاملات الإلكترونية وللمحررات الإلكترونية، ويعتبر الالتزام بالتحقق من صحة البيانات هو التزام بمدى مطابقة المعلومات الواردة في شهادة التصديق الالكترونية عن طريق فحصها، وليس بمدى صحة مضمون ومحتوى الوثائق المسلمة إليه من طرف طالب الشهادة، بالتالي فان التزام مؤدي خدمات التصديق هو التزام ببذل عناية ما دام أن المشرع أجاز له في نص المادة53 في الفقرة الأخيرة من نفس القانون بأنه لا يكون مسئولا في حالة ما إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت أنه لم يرتكب أي إهمال، أو أن يثبت أن الضرر يعود أساسا لسبب أجنبي لا يد له فيه .

خامسا: مسؤولية مؤدي خدمات التصديق الالكتروني

تترتب مسئولية مؤدي خدمات التصديق الالكتروني عن أي ضرر حاصل لشخص حسن النية نتيجة لعدم إلغاء الشهادة أو تعليقها إذا طلب ذلك [2]، فهو بإصداره لهذه الشهادات يكون قد أعلن مسئوليته والتزاماته بما تحتويه الشهادة من بيانات ومعلومات، مما يوفر الأمان للأفراد ويمنحهم الثقة بصحة تعاقداتهم مع الطرف الآخر،[3]ويعتبر منح الثقة بصحة البيانات والمعلومات التي تتضمنها شهادة التصديق الالكتروني بمثابة صحة التعاقد مع الطرف الآخر وبصحة الشهادة، وعليه فإذا كانت العلاقة القانونية عقدية مثل العلاقة بين مزود خدمة التصديق الالكتروني وصاحب الشهادة الالكترونية فإننا نطبق أحكام المسئولية العقدية، أما إذا كان الإخلال ناشئ عن خطأ حاصل في العلاقة بين مزود خدمة التصديق الالكتروني والغير، فإن أحكام المسئولية هي التي تطبق، ويثار في هذا الصدد أساس المسئولية التي يمكن أن تتحقق هنا، فهي لا تكون على توصيف واحد وإنما تكون عقدية أو تقصيرية بحسب الأحوال.

[1] ـ المادة 41 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

[2] ـ برهم نضال إسماعيل، أحكام عقود التجارة الالكترونية، مرجع سابق، ص.197.

[3] ـ عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، دار وائل ، عمان، 2010، ص.119.

أ ـ المسئولية العقدية لمؤدي خدمات التصديق الالكتروني :

تفترض المسئولية العقدية عقدا يربط بين الغير المتضرر ومقدمي خدمات المصادقة يفرض بدوره على هذه الأخيرة التزاما بالضمان لمصلحة الأول، وهذا الافتراض بشقيه لا يتحقق دائما في الغالب لانعدام العلاقة العقدية المباشرة بين مقدم الخدمة وصاحب الشهادة الالكترونية[1]، تكون مسئولية مزود خدمات التصديق الالكتروني مسئولية عقدية، وذلك في مواجهة المتعاقد معها لارتباطهما بعقد [2]، فتقوم المسئولية هنا بتوفر أركانها من خطأ وضرر وعلاقة السببية بينهما، وبإعمال هذه الأركان وهي الخطأ العقدي الذي من أهم صوره بالنسبة لمزود الخدمة عدم إصدار الشهادة المطلوبة منه، أو التأخر في إصدارها أو إصدارها ولكن على وفق معلومات غير صحيحة كأن تكون مزورة أو مغلوطة[3]، ويلتزم بتعويض الأضرار التي تلحق بأي طرف تعاقد معه لإصدار شهادة إلكترونية، فهو يعتبر التزام بتحقيق نتيجة وليس التزاما ببذل عناية، حيث يلتزم بإصدار شهادة إلكترونية تفيد صحة البيانات الواردة فيها، لذلك تعتمد هذه الجهة على تقنيات فائقة الدقة تمكنه من القيام بذلك، لذلك فإذا ثبت خطأ مزود خدمات التصديق تجاه المتعاقد معه، فإنه ملزم بتعويض هذه الأضرار وفقا للقواعد العامة التي تحكم المسئولية العقدية[4].

يرى جانب من الفقه أن مسئولية مزود خدمات التصديق الالكتروني العقدية لا تقف في حدود علاقته بالموقع والمرسل إليه بل كذلك بينه وبين الغير، وذلك على أساس وجود اتفاق يجمع بينه وبين الغير، وهو اتفاق مستقل عن العقد المبرم بينه وبين صاحب التوقيع الالكتروني، وهذا الاتفاق يترجمه طلب الحصول على شهادة إلكترونية تؤيد صحة توقيع الكتروني معين، وهو إيجاب من الغير يقابله قبول من مؤدي خدمات التصديق الالكتروني بمنح الشهادة

[1] ـ بلقاسم حامدي، إبرام العقد الالكتروني، رسالة لنيل شهادة دكتوراه علوم، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة،2015، ص.248.

[2] ـ نور خالد عبد المحسن العمد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات عبر شبكة الانترنت، رسالة دكتوراه في الحقوق، جامعة عين شمس، كلية الحقوق، مصر، 2009، ص.321.

[3] ـ عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني، مرجع سابق، ص.176.

[4] ـ سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، مرجع سابق، ص.350.

المطلوبة، وعند إخلال مؤدي الخدمات بهذا الاتفاق كتقديمه لشهادة غير دقيقة للبيانات، فتقوم المسئولية العقدية في جانبه، انتقد هذا الرأي لأنه يقتصر على الحالة التي يرتبط فيها الغير الشهادة من مؤدي خدمات التصديق، وهي حالات نادرة لأنه في الغالب يتم طلبها من الموقع[1].

يرى جانب آخر من الفقه في فرنسا إلى أن هذا العقد هو عقد تقديم خدمة إلكترونية، لأن عمل جهة التصديق الالكتروني تجاه العميل أو الغير من شأنه أن يدعم مصداقية التوقيعات الالكترونية وتوثيقها، وذلك يسهم في الحد من المخاطر المحتملة المترتبة على نظم السداد الالكتروني[2].

يرى جانب آخر بأن المسئولية التي تقام عند إخلال مؤدي الخدمات بالتزاماته تجاه الموقع أو الغير هي مسئولية عقدية ناشئة عن علاقة مباشرة، وهذا لوجود علاقة عقدية بين صاحب التوقيع وجهة التصديق الالكتروني، ويترتب على هذا العقد التزام مؤدي خدمات التصديق الالكتروني بإصدار شهادة الكترونية باسم صاحب التوقيع لمصلحة الغير الذي يحتاج إلى تلك الشهادة في تعامله مع الموقع، وبذلك نكون أمام حالة من حالات الاشتراط لمصلحة الغير، حيث يكون فيها الموقع في مركز المشترط ومؤدي الخدمات في موقع المتعهد، أما الغير فيكون في مركز المنتفع[3].

ب ـ المسئولية التقصيرية لمقدمي خدمة التصديق الالكتروني:

تنشأ هذه المسئولية التقصيرية عندما لا توجد علاقة عقدية بين جهة التصديق والغير المتضررين، ويندرج تحت وصف الغير هنا أي شخص لا تربطه علاقة مباشرة بعقد ما مع مركز التصديق الالكتروني ولم يعتبر مشترط لمصلحته من عقد لتوقيع الكتروني ما.

[1] ـ زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2013، ص.291.

[2] ـ إبراهيم الدسوقي أبو الليل، الجوانب القانونية في المعاملات الالكترونية، مرجع سابق، ص.21.

[3] ـ زروق يوسف، حجية وسائل الإثبات الحديثة، مرجع سابق، ص.293.

يعتبر أي إهمال أو تقصير يخل بالتزامات جهة التصديق الالكتروني مسئولية مدنية تقصيرية وذلك عند توفر الخطأ والضرر والعلاقة السببية بينهما، ويقوم الإخلال إذا أقيم الدليل على أن جهة التوثيق الالكتروني لم تبذل العناية اللازمة ولم يراعي الحيطة والحذر والتحقق من البيانات المقدمة له في الشهادة، وبالتالي ذلك الإثبات لا يكفي لوحده لإثبات الخطأ من جانب جهة التصديق، وإنما على الشخص المتضرر أن يثبت أنه ثمة ضرر محقق قد أصابه، وأن هذا الضرر كان نتيجة لقيام خطأ تقصيري من جهة التصديق[1].

ج ـ انتفاء مسؤولية مقدم خدمة التصديق الالكتروني :

تنتفي مسؤولية مقدم خدمة التصديق الالكتروني، إذا كانت البيانات والمعلومات المقدمة من المشترك قد جاءت صحيحة، وأثبت مقدم خدمة التصديق أنه اتخذ كل الإجراءات اللازمة لمراجعة صحة هذه البيانات وكذلك في حالة عدم تأكد الغير، ويجوز لمقدم خدمات التصديق أن يحدد نطاق مسؤوليته، وذلك بأن يضع بعض القيود على استخدام الشهادة التي يصدرها مثل تحديد مدة سريانها، وقيمة التصرف التي تحويه، بحيث لا يكون مسئولا عن تجاوز هذه القيود سواء من صاحب الشهادة أو من الغير الذي يولي ثقته بها، شريطة أن يكون بوسع الغير العلم بهذه القيود بوسيلة تقنية ميسورة[2].

تنتفي مسئولية جهات التوثيق الالكتروني وفقا للمادة 02/06 من التوجيه الأوروبي الصادر بشان التوقيعات الالكترونية لسنة 1999 حيث نصت عل أنه تسهر الدول الأعضاء على أن يكون المكلف بخدمة التوثيق الذي أصدر شهادة معتمدة للجمهور مسئولا عن الضرر الذي يصيب الشخص الطبيعي أو المعنوي مستفيدا من الشهادة، إلا إذا أثبت أنه لم يرتكب أي إهمال،

[1] ـ عصمت عبد المجيد بكر، دور التقنيات الحديثة في تطور العقد، دار الكتب العلمية، بيروت ،2015، ص.421.

[2] ـ سامح عبد الواحد التهامي، التعاقد عبر الانترنت، مرجع سابق، ص.436. سمير حامد عبد العزيز الجمال، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة، مرجع سابق، ص.438.

إلا أنه يمكن لمزود خدمة التصديق الالكتروني أن ينفي مسئوليته وذلك بأن يثبت أن الضرر يعود أساسا لسبب أجنبي لا يد له فيها.[1] .

يعفى مزود خدمة التصديق الالكتروني من المسئولية في قانون المبادلات والتجارة الالكترونية التونسي حيث نص في الفصل 02/22 في الحالات التالية : **" لا يكون مزود خدمات المصادقة الالكترونية مسئولا عن الضرر الناتج عن عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث إمضائه الالكتروني، و عند قيام مزود الخدمة بتعليق العمل بشهادة المصادقة أو إلغائها بناءا على طلب صاحب الشهادة وحصول ضرر للغير نتيجة هذا التعليق أو الإلغاء"**[2]، فإذا كان أساس الضرر هو الموقع ذاته أو المتعامل فإن جهة التصديق الالكتروني يمكن أن تنفي على عاتقها الخطأ إذا أثبتت أنها قامت ببذل العناية اللازمة لتحقيق النتيجة المفروضة عليها وهذا من خلال إثبات أنها قامت بفحص المستندات ظاهريا ولم يتبين أن هناك تزويرا أو عيبا بالمستندات ولكن المعلومات ذاتها المقدمة من الموقع غير صحيحة، أو إثبات أن جهة التصديق قامت بإيقاف العمل بالشهادة أو إلغائها، لكن المتعامل لم يقم بالاستجابة لهذا العمل المشروع، وبالتالي كان المتعامل يعلم أو كان بوسعه أن يعلم وفقا للمجرى العادي للأمور أن تلك الشهادة قد تم إيقافها أو إلغائها، ومع ذلك قام بالتعامل بناءا عليها، فإن مسئولية جهة التوثيق تنتفي عن تعويض تلك الأضرار[3].

نص المشرع الجزائري على حالات انتفاء مسؤولية جهات التصديق الإلكتروني في المواد 53 إلى 57 من القانون 15 -04 والتي يمكن إيجازها كالآتي :

---

[1] - Article 06/2 de la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, dispose que: ***« Les États membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié soit responsable du préjudice causé à une entité ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune*** **negligence** **».** sur le site*:* https://eur-lex.europa.eu/

[2] ـ الفصل 02/22 من القانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية.

[3] ـ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، مرجع سابق، ص.223.

ـ حالة ما إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت أنه لم يرتكب أي إهمال من حيث الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الإلكتروني.

ـ حالة ما إذا قدم مؤدي خدمات التصديق الإلكتروني ما يثبت أنه لم يرتكب أي إهمال من حيث حدوث ضرر ناتج عدم إلغائه لشهادة التصديق الموصوفة المسلمة من طرفه والذي يلحق بأي هيئة أو شخص طبيعي أو معنوي اعتمدوا على تلك الشهادة.

ـ حالة الضرر الناتج عن استعمال شهادة التصديق الإلكتروني الموصوفة عند تجاوز الحدود المفروضة على استعمالها.

ـ حالة ما تجاوز صاحب شهادة التصديق الالكتروني الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها هذه الشهادة، بحيث يجب أن يكون الحد الأقصى لقيمة المعاملة وحدود استعمالها واضحة ومفهومة من طرف الغير.

ـ حالة عدم احترام صاحب شهادة التصديق الإلكتروني لشروط استعمال بيانات إنشاء التوقيع الالكتروني[1].

[1] ـ راجع في ذلك المواد من53 إلى 57 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.

المطلب الثاني

شهادة التصديق الإلكتروني

يقصد بشهادة التصديق الإلكتروني الحصول على تأكيد نسبة المحرر الالكتروني إلى مصدره وأنه صادر ممن نسب إليه، وتعرف شهادة التصديق الإلكتروني بأنها الشهادة التي تصدر عن مقدم خدمة المصادقة الالكترونية لإثبات نسبة المحرر الالكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة، حيث يمكن من خلال هذه الشهادة التأكد من شخصية المرسل وتشهد بصحة البيانات المدونة بالمحرر الالكتروني وعدم قابليتها للتعديل، وهذا من شأنه أن يمنح الأمان والثقة للمتعاملين المتعاقدين عبر الإنترنت، بالتالي يقتضي منا توضيح مفهوم شهادة التصديق الإلكتروني من خلال تعريفها وتوضيح البيانات الواجب توفرها في شهادة التصديق الإلكتروني **(الفرع الأول)**، ثم نتناول كيفية إيقاف شهادة التصديق الإلكتروني وإلغاؤها **(الفرع الثاني)**.

الفرع الأول

مفهوم شهادة التصديق الإلكتروني

اختلفت النصوص التشريعية والآراء الفقهية في تقديم مفهوم موحد لشهادة التصديق الإلكتروني مما ترتب عليه تعدد البيانات الواردة فيها، فسنتناول **(أولا)** تعريف شهادة التصديق الإلكتروني، ثم نتعرض إلى الاعتراف بشهادة التصديق الأجنبية **(ثانيا)**، ثم إلى البيانات الواردة فيها **(ثالثا)**.

أولا: تعريف شهادة التصديق الالكتروني

أولت التشريعات الوطنية والدولية عناية كبيرة لإبراز كافة المسائل القانونية والمواصفات التقنية لها، على غرار الدراسات الفقهية التي بدورها حاولت أن تزيل الكثير من الغموض فيما يتعلق بهذه الشهادة، بالتالي سنتعرض على تعريف شهادة التصديق الالكتروني فقهيا ثم إلى تعريف شهادة التصديق الالكتروني في التشريعات الدولية والوطنية.

أ- التعريف الفقهي لشهادة التصديق الإلكتروني :

قدمت لشهادة التصديق الالكتروني عدة تعريفات من قبل الفقهاء حاولوا من خلالها بيان مفهوم هذه الشهادة .

عرف بعض الفقه شهادة التصديق بأنها **:"شهادة التوثيق عبارة عن صك أمان صادر عن جهة مختصة، يفيد صحة وضمان المعاملة الالكترونية، وذلك من حيث صحة البيانات ومضمون المعاملة وأطرافها"**[1].

عرفت أيضا بأنها: **" مجموعة من المعلومات عن التوقيع الرقمي تؤكد من قبل سلطة متعارف عليها وموثوق فيها من مجتمع مستخدمي الشهادات"**[2].

كما عرفها آخرون بأنها: **" الشهادة التي يصدرها مقدمو خدمات التصديق المرخص لهم من الجهات المسئولة في الدولة لتشهد بأن التوقيع الالكتروني هو توقيع صحيح ينسب إلى من أصدره ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه"**[3].

يلاحظ من خلال هذه التعريفات أن شهادة التصديق الالكتروني تعتبر من أكثر الوسائل أهمية في بنية التوقيعات الرقمية على حل مشكلة الهوية الرقمية، فهي تقدم تأكيدا أن توقيع ما يخص شخصا معينا بحيث يتم الاعتماد عليها في تحديد هوية المتعاملين، كما أن مضمون هذه الشهادة هو صحة البيانات المتبادلة بين الطرفين، وعليه فإن الشهادة الرقمية هي الوسيلة الوحيدة لتحديد الهوية في البيئة الرقمية عن طريق جهة تصديق مختصة، تفيد بصحة التوقيع الالكتروني ومضمون المعاملة وأطرافها، كما تعتبر إجراء تقني لحماية المحرر الالكتروني من الغش والاحتيال، وبالتالي تساعد على التأكد من صحة البيانات الواردة فيه.

[1] - مشار إليه لدى: محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، مرجع سابق، ص.43.

[2] - مشار إليه لدى: محمد محمد سادات، مرجع سابق، ص.113 .

[3] - مشار إليه لدى: إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، ص.183. عصمت عبد المجيد بكر، دور التقنيات العلمية في تطوير العقد، مرجع سابق، ص.403.

ب- تعريف شهادة التصديق الإلكتروني في المواثيق الدولية والتشريعات الوطنية:

عرفها قانون الأونسترال النموذجي بشأن التوقيع الالكتروني لسنة 2001 شهادة التصديق الإلكتروني بأنها: " **الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبيت الارتباط بين الموقع وبيانات إنشاء التوقيع"**[1]، يؤخذ على هذا التعريف أنه أغفل الجهة التي تصدر شهادة التوثيق الالكتروني.

عرفت المادة 02/ 9 من التوجيه الأوروبي رقم 1999/93 شهادات التصديق الإلكتروني بأنها:"**شهادة إلكترونية تربط بين أداة التوقيع وبين شخص معين، وتؤكد شخصية الموقع"**[2].

يؤخذ على هذا التعريف أنه لم يحدد بأن جهة التصديق يجب أن تكون مرخصة ومعتمدة عكس تعريف قانون الأونسترال النموذجي السابق ذكره.

عرف المشرع الفرنسي شهادة التصديق الإلكتروني في المرسوم رقم 272-01 في المادة **(9/1)** بأنها" **مستند في شكل الكتروني تثبت توافر الرابطة بين بيانات التحقق من صحة التوقيع الإلكتروني وبين الموقع."**[3]

عرف المشرع المصري في المادة 01 فقرة (و) شهادة التصديق الإلكتروني في قانون التوقيع الإلكتروني لسنة 2004 بأنها: "**الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع و بيانات إنشاء التوقيع."**[4]

---

[1] - المادة(2/ب) من قانون الأونسترال النموذجي بشأن التوقيع الإلكتروني لسنة2001 .

[2] - Article 06/2 de la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, dispose que :

« une attestation électronique qui lie des données afférente à la vérification de signature à une personne et confirme l'identité de cette personne ».

[3] - Article 1/9 du décret n° 2001- 272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, dispose que: ***«Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique en un signataire*** » .

[4] - المادة (1/و) من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 .

عرفها المشرع التونسي الخاص بالمبادلات التجارية الإلكترونية شهادة المصادقة الالكترونية بأنها: **" الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها، أثر المعاينة، على صحة البيانات التي تتضمنها."**[1]

عرف المشرع الأردني في المادة 12/02 من قانون المبادلات والتجارة الالكترونية الأردني رقم 15 لسنة 2015 شهادة التوثيق الإلكترونية بأنها**: " تلك الشهادة الصادرة عن جهة التوثيق الالكتروني لإثبات نسبة توقيع إلكتروني إلى شخص معين استنادا إلى إجراءات معتمدة"**، وأضاف في الفقرة 18 من نفس المادة بأن**: " شهادة التوثيق الالكتروني الجذرية هي شهادة تصدرها جهات التوثيق الالكتروني لنفسها لتمكين جهات التوثيق الأخرى من الوثوق بالشهادات الصادرة عنها"**[2].

عرفها المشرع الجزائري في المادة 03 من المرسوم التنفيذي رقم 07 -162 شهادة التوثيق الإلكتروني بأنها: " **وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع"**، فنصت المادة 04 منه على المساواة بين الشهادات التي يقدمها مقدمي خدمات التصديق وتلك التي يقدمها مؤيدي خدمات تصديق يقيم في بلد أجنبي، وهذا يساعد على تطور التجارة الالكترونية المتصفة عادة بالطابع الدولي .[3]

أولى المشرع الجزائري في القانون 15-04 اهتماما كبيرا بالتوقيع والتصديق الالكتروني، بحيث أنه في هذا القانون ميز بين نوعين من شهادات التصديق الالكتروني وهما الشهادة العادية وشهادة التصديق الموصوفة.

[1] - الفصل 2 الفقرة 3 من قانون عدد83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية التونسي .

[2] - المادة 2/ 12و18 من قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015 .

[3]- المادة 03 من المرسوم التنفيذي رقم 07- 162 السالف الذكر.

1 ـ شهادة التصديق العادية :

عرفها في المادة 7/2 من القانون 15-04 على أنها: "**جهاز أو برنامج معلومات معد لتطبيق بيانات التحقق من التوقيع الالكتروني**"[1].

2 ـ شهادة التصديق الالكتروني الموصوفة:

عرف المشرع الجزائري شهادة التصديق الموصوفة في نص المادة 15 من القانون 15- 04 على أنها شهادة تصديق الكتروني تتوفر فيها بيانات إلزامية وشكل خاص عكس شهادة التصديق العادية، وهذه البيانات من شأنها أن توافر أمانا أكثر فيما يتعلق بصحة بيانات إنشاء التوقيع الالكتروني .[2]

يلاحظ من خلال التعريفات السابقة أن المشرع المصري والأردني في تعريف شهادة التصديق الالكتروني لم يتطرقا ولم يبينا طبيعة البيانات الواردة في الشهادة، وحتى طبيعة الشهادة في حد ذاتها هل هي محرر إلكتروني أم محرر تقليدي، على عكس المشرع التونسي الذي ذكر طبيعة الشهادة وذلك من خلال نصه على أنها وثيقة إلكترونية، وحدد وظيفة الشهادة وهي إثبات صحة البيانات التي تتضمنها بخلاف المشرع الجزائري الذي عرف شهادة التصديق الالكتروني الموصوفة والعادية وميز بينهما وبين الدور الذي تقوم به، من خلال تأكيده على أن الغرض من الشهادة هو لتأكيد صحة التوقيع الالكتروني والمحرر حتى يكون دليلا كامل في الإثبات.

يمكن أن نستخلص من خلال التعريفات التي قدمتها التشريعات الوطنية والدولية وكذلك الفقه أن شهادة التصديق الالكتروني هي وثيقة إلكترونية تثبت صحة البيانات المتعلق بالشهادة، التي تصدر من جهة التصديق المرخصة لها أو المعتمدة، والتي تسمح بتحديد هوية المتعامل الالكتروني، وحماية المحرر الالكتروني من أي غش أو احتيال، كما يلاحظ أيضا أن الغرض

[1] ـ المادة 7/2 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين .

[2] ـ المادة 15 من القانون ذاته .

من إنشاء شهادة التصديق الالكتروني، هو بمثابة إقرار وشهادة على أن المحرر أو التوقيع الالكتروني صحيح ومنسوب لمصدره، وأنه يستوفي الشروط والضوابط والمعايير التقنية والفنية المنصوص عليها في التشريعات المذكورة آنفا، بمعنى أن المحرر الالكتروني أو التوقيع الالكتروني لم يطرأ عليه أي تبديل سواء بالإضافة أو المحو أو التغيير، فالشهادة هي إذن لإثبات صحة البيانات التي تتضمنها.

يمكن القول إذن من خلال ما تقدم أن شهادة التصديق الإلكتروني قد حظيت بأهمية مميزة سواء تشريعيا أو فقهيا، فأضحت تلك الشهادات صك أمان بالنسبة للمتعاملين عبر وسائل الاتصال الحديثة، لأنها ستفيد أطراف المعاملات الالكترونية بصحة التوقيع والبيانات المتبادلة، لكن أغلب التشريعات الوطنية اهتمت أكثر في تعريفها لشهادة التصديق الالكتروني على تحديد مفهوم هيئات التصديق الالكتروني، فيمكن تعريف شهادة التصديق الالكتروني بأنها وسيلة فنية آمنة للتحقق من صحة التوقيع والمحرر، حيث يتم إلحاقه إلى الشخص الذي أصدره عبر جهة مختصة وموثوق بها، أو طرف محايد يطلق عليه مقدم خدمات التصديق الالكتروني.

ثانيا: الاعتراف بشهادة التصديق الالكتروني الأجنبية

تتم أغلب التصرفات الالكترونية وتنشأ في وسط افتراضي لا يعترف بالحدود الجغرافية للدول، وبالتالي أغلب المعاملات الالكترونية تتجاوز حدود الدولة التي أبرمت فيها، فعندما يقوم مقدم خدمة التصديق الالكتروني بإصدار شهادة التصديق الالكتروني في دولة معينة يجب أن يكون لهذه الشهادة قيمة قانونية تتعدى حدود الدولة التي صدرت فيها، فيمكن تعريف شهادة التصديق الالكترونية الأجنبية بأنها الشهادات المؤمنة بواسطة التوقيع الالكتروني والصادرة من جهة تصديق أجنبية ومعترف بها بصحة البيانات التي تتضمنها وتماثل نظيرتها من الشهادات الصادرة داخل إقليم الدولة [1]، فلا بد إذن من تحقيق المساواة بين شهادة التصديق الوطنية الصادرة من مؤدي خدمة التصديق الالكتروني الوطني وشهادة التصديق الأجنبية الصادرة من

[1] ـ خاد مصطفى فهمي، إبرام العقد الالكتروني في ضوء التشريعات العربية والمنظمات الدولية، دار الجامعة الجديدة، مصر، 2007، ص. 69.

مؤدي خدمات تصديق أجنبي وتطبيقا لذلك اعترفت معظم التشريعات الوطنية والدولية بشهادة التصديق الالكتروني الأجنبية.

نظمت المادة 12 من قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001 الاعتراف بالشهادات والتوقيعات الالكترونية التي تتم في دولة أجنبية حيث تضمنت ما يفيد بأن الشهادة سارية المفعول قانونيا، ولا يولي أي اعتبار عن الموقع الجغرافي الذي تصدر فيه الشهادة، ويكون للشهادة التي تصدر في دولة أجنبية نفس المفعول القانوني للشهادة التي تصدر في الدولة المشرعة طالما استوفيت الشروط التي تضفي عليه الثقة، والمعايير الدولية المعترف بها، ويجوز للأطراف الاتفاق فيما بينهم على استخدام أنواع معينة من الشهادات، ويكون هذا الاتفاق ساري المفعول عبر حدود الدول المختلفة بشرط أن يكون هذا الاتفاق صحيحا وغير مخالف للقانون المطبق.

اشترطت أيضا المادة 02/12 من نفس القانون المساواة في الأثر أو الحجية للشهادة في الدولة التي صدرت فيها مع الشهادة الأجنبية التي صدرت من دولة أخرى، بمعنى أن الشهادة الأجنبية تعامل مع الشهادة الوطنية مرتبة ذات الأثر القانوني، شرط أن تتوافر فيها الضمانات المقررة في الشهادة ذات المنشأ الوطني، كما نصت في المادة 04/12 على الحكم ما إذا كانت شهادة التصديق الالكتروني الأجنبية لها قوة إثبات تعادل تلك المعمول بها في الدولة الأجنبية المطلوب تطبيق الشهادة فيها لأنه يتم مراعاة المعايير الدولية المعمول بها في هذا الخصوص وأية عوامل أخرى ذات صلة .

أضافت الفقرة 05 من المادة 12 من نفس القانون أن اتفاق الأطراف على استخدام أنواع معينة من شهادات التصديق وجعله مقدما على ما عداه، بالتالي يعتبر هو المطبق ما لم يكن ذلك الاتفاق مخالفا للنظام العام والآداب العامة، أو يكون هنا تعارض مع القانون المطبق مع الدولة التي تطبق الشهادة فيها.[1]

[1] - راجع في ذلك نص المادة 12 من قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001 .

اعترف المشرع المصري بشهادة التصديق الصادرة من بلد أجنبي حيث منح هيئة تنمية صناعة تكنولوجيا المعلومات، وهي الهيئة التي تمنح التراخيص لمزاولة نشاط إصدار شهادات التصديق الالكترونية، سلطة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الالكترونية وذلك نظير المقابل الذي يحدده مجلس إدارتها وبذلك يكون لشهادة التصديق الأجنبية ذات الحجية في الإثبات المقررة، كما لو كانت صادرة في مصر، وذلك وفقا للقواعد والضمانات والإجراءات التي تقررها اللائحة التنفيذية لهذا القانون، وقد قصد المشرع من ذلك تحري مدى استيفاء الجهات الأجنبية المناظرة ما ورد في اللائحة التنفيذية من قواعد وضمانات وإجراءات[1]، فنص في المادة 22 قانون التوقيع الالكتروني المصري إلى أنه : " **تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الالكتروني، وذلك نظير المقابل الذي يحدده مجلس إدارة الهيئة، وفي هذه الحالة تكون الشهادات التي تصدرها تلك الجهات ذات الحجية في الإثبات المقررة لما تصدره نظيراتها في الداخل من شهادات نظيرة، وذلك كله وفقا للقواعد والإجراءات والضمانات التي تقرها اللائحة التنفيذية لهذا القانون**"[2].

فاشترط المشرع المصري من خلال نص هذه المادة أنه للاعتراف بشهادة التصديق الالكتروني الأجنبية، أن يعترف أولا بمقدم خدمات التوثيق الأجنبي وهو شرط يخضع للقواعد والإجراءات والضمانات التي تقررها اللائحة التنفيذية ويقع على عاتق هيئة تنمية صناعة تكنولوجيا المعلومات.

اعترف المشرع التونسي بشهادات المصادقة الأجنبية في الفصل23 من قانون المبادلات والتجارة الإلكترونية رقم 83 لسنة 2000 على أنها: " **تعتبر الشهادات المسلمة من مزود خدمات المصادقة الإلكترونية الموجودة ببلد أجنبي كشهادات مسلمة من مزود خدمات المصادقة الالكترونية موجود بالبلاد التونسية، إذا تم الاعتراف بهذا الهيكل في إطار اتفاقية اعتراف متبادل تبرمها الوكالة الوطنية للمصادقة الالكترونية.**[3]

[1] ـ إيمان مأمون أحمد سليمان، مرجع سابق، ص.335 .

[2] ـ المادة 22 من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 .

[3] ـ الفصل 23 من قانون عدد 83 لسنة 200 المتعلق بالمبادلات والتجارة الإلكترونية التونسي .

يلاحظ أن المشرع التونسي عند اعتماده لشهادة التصديق الأجنبية المسلمة من مزود خدمات المصادقة الإلكترونية الموجود ببلد أجنبي، لم يذكر التوقيع الإلكتروني الأجنبي على غرار المشرع المصري، كما أن هذا الاعتماد لا بد أن يكون هناك اعتراف متبادل مبرم بين الأطراف من قبل الوكالة الوطنية للمصادقة الالكترونية.

اعترف المشرع الجزائري بشهادة التصديق الأجنبية وذلك في نص المادة 63 من القانون 15-04 بأنها: **" تكون لشهادات التصديق الالكتروني التي يمنحها مؤدي خدمات التصديق الالكتروني للمقيم في بلد أجنبي، نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الالكتروني للمقيم في الجزائر، بشرط أن يكون مؤدي الخدمات الأجنبي هذا قد تصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها السلطة".**[1]

يلاحظ أن المشرع الجزائري قد اشترط للاعتراف بالشهادات الصادرة عن مؤدي خدمات التصديق الالكتروني الموجودة بدولة أجنبية وجود اتفاقية اعتراف متبادل مبرم مع الدول الأجنبية من قبل السلطة الوطنية للتصديق الالكتروني باعتبارها المخولة قانونا بمراقبة عملية التصديق، فالمشرع الجزائري مثله مثل المشرع المصري والتونسي ربط مسألة الاعتراف بشهادة التصديق الأجنبية بالاعتراف بمقدم خدمة التصديق الالكتروني الأجنبي، لكن المشرع الجزائري ربط ذلك بشرط أن يكون هذا الأخير قد تصرف في إطار اتفاقية مبرمة مع الدولة الأجنبية.

يمكن القول مما سبق أن دولية شهادات التصديق الالكترونية لا تخرج عن الحالات التالية:

أ ـ الاستجابة للشروط المتعارف عليها دوليا لإصدار الشهادة الالكترونية:

تتمثل في حالة استجابة جهة التصديق الالكتروني لشروط الثقة والتوثيق المطلوبة قانونا، أو الشروط القياسية المتعارف عليها دوليا لإصدار الشهادات الالكترونية والمفاتيح المشفرة، فحتى

[1] ـ المادة 63 من القانون رقم 15- 04 المتعلق بالتوقيع والتصديق الالكترونيين.

لو لم يقدم الموثق الالكتروني طلب اعتماده بالخارج فكلها نافذة قانونا، وإن كانت غالبية تلك الشروط تقنية أكثر منها قانونية.

ب ـ طلب مقدم الخدمة طلب الاعتراف من الدولة الأجنبية للشهادات التي يصدرها:

تتمثل هذه الحالة عندما يقدم مقدم خدمة التصديق الالكتروني طلب اعتماده في الخارج لدى دولة أجنبية غير الدولة المنتمي إليها، بمعنى أنه طلب الاعتراف بما يصدره من شهادات، فهنا يجب على هذا الموثق الالكتروني أن يحترم دفتر الشروط الذي تضعه تلك الدولة بخصوص منتجات التوثيق الالكتروني، وأن يتكيف مع قانونها الوطني وأن يخضع في نشاطه لرقابة تلك الدولة[1].

ج ـ وجود اتفاقية اعتراف متبادل مبرم مع الدول الأجنبية:

تكون لشهادات التصديق الالكتروني التي يمنحها مؤدي خدمات التصديق الالكتروني للمقيم في بلد أجنبي، نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الالكتروني، على أساس الاتفاق بين الدول حول استخدام الشهادات الالكترونية التي تصدر في دولة أجنبية أبرمتها السلطة الاقتصادية للتصديق الإلكتروني[2].

ثالثا: البيانات الواجب توافرها في شهادة التصديق الإلكتروني

حتى تكون للشهادة قيمة قانونية في الإثبات يجب أن تشمل على بيانات معينة، منها ما يتعلق بصاحب الشهادة، وأخرى متعلقة بمصدرها، وبيانات مرتبطة بذات الشهادة، وهذا حتى تكون الثقة في مضمون الشهادة وتبعث الاعتقاد بسلامة محتواها.

بين قانون الأونسترال النموذجي للتوقيعات الإلكترونية لسنة2001 بعض البيانات الأساسية التي يجب أن تتضمنها شهادة التصديق الإلكترونية، والتي تتعلق أساسا بالطريقة المستخدمة في تحديد هوية صاحب التوقيع، حدود الغرض والقيمة التي تستخدم شهادة المصادقة الإلكترونية

[1] ـ طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، المنشورات الحقوقية، بيروت، 2007، ص.229 .

[2] ـ راجع نص المادة 63 من القانون 15 ـ04 المتعلق بالتوقيع والتصديق الإلكترونيين.

من أجلها، البيانات اللازمة لإنشاء تواقيع إلكترونية صحيحة، وحدود المسؤولية القانونية لمقدم خدمات التوثيق الإلكتروني .

أقدم المشرع المصري في المادة 2/20 من اللائحة التنفيذية لقانون التوقيع الالكتروني على توضيحه، حين تطلب ضرورة أن تشتمل نماذج شهادات التصديق الإلكتروني التي يصدرها مقدم الخدمات على ما يفيد صلاحية تلك الشهادة للاستخدام في التوقيع الإلكتروني، واشتمالها كذلك على موضوع الترخيص الصادر لمقدم الخدمات المرخص له، موضحا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه[1].

نص المشرع الجزائري على هذه البيانات في المادة 15 من القانون 15-04 وتتمثل أساسا في تحديد هوية اسم الموقع عن طريق اسمه الشخصي أو المستعار أو عن طريق إدراج صفة خاصة له وذلك حسب الغرض، تحديد هوية مقدم خدمة التصديق الالكتروني المصدر للشهادة والبلد الذي يقيم فيه، ذكر البيانات التي تتعلق بالتحقق من التوقيع الالكتروني ومطابقة للبيانات إنشاء التوقيع الإلكتروني، الإشارة إلى تاريخ ومدة صلاحية الشهادة وحدود صلاحيتها، وعند الاقتضاء يذكر حدود كل من استعمال الشهادة وقيمة المعاملات التي قد تستعمل من أجلها والإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر والتأشير على الشهادة على أنه تم منحها على أنها شهادة تصديق الكترونية موصوفة[2].

يلاحظ على هذه النصوص أنها تتماثل فيما تتطلب من بيانات لشهادة التصديق الإلكتروني، وعليه إذا استوفيت شهادة التصديق الالكتروني على هذه البيانات أصبحت صالحة للتعامل بها، وتتعدد شهادات التصديق الإلكتروني بحسب استخدامها والغرض منها، فإلى جانب شهادة التصديق الالكتروني توجد شهادات أخرى مثل شهادة توثيق تاريخ الإصدار التي توثق تاريخ ووقت إصدار التوقيع الرقمي، حيث يقوم صاحب الشهادة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها و توقيعها من جهتها ثم تعيدها إلى مرسلها، وأيضا

[1]- راجع نص المادة 2/20 من قرار رقم 109 لسنة 2005 المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[2] - راجع المادة 15 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

شهادة الإذن، وبمقتضاها يتم تقديم معلومات إضافية عن صاحبها مثل عمله، مؤهلاته، التراخيص التي يملكها، كذلك شهادة البيان التي تفيد في بيان صحة واقعة أو حدث ما ووقت وقوعه[1]، وعليه تظهر أهمية هذه الشهادات من حيث الدور الذي تقوم به خاصة التأكيد على صدور المحرر الإلكتروني والتوقيع الالكتروني عن أصحابها، وأن ذلك المحرر لم يطرأ عليه أي إضافة أو حذف أو تغيير، بحيث إذا قام أحد الأطراف بوضع توقيعه الالكتروني المصدق بتلك الشهادة على محرر إلكتروني، فإن ذلك يعزز بأن التوقيع صادر عمن نسب إليه وأن هذا التوقيع صحيح، بالتالي فهي شهادة تمكن الغير من الاعتماد عليها في تحقيق الأمن والثقة في التعاملات التي تتم بشكل إلكتروني.

الفرع الثاني

الآثار القانونية لشهادة التصديق الإلكتروني

يتبين ربما بعد إصدار الشهادة أنه لا يعول عليها، كما يحدث في الحالات التي يقدم فيها الموقع إلى مقدم خدمات التصديق هوية غير هويته، وفي ظروف أخرى قد يكون من الممكن التعويل على الشهادة حين صدورها، لكنها تفقد إمكانية التعويل عليها بعد ذلك، فإذا تعرض المفتاح الخصوصي لما يثير الشبهة، كأن يفقد الموقع سيطرته على ذلك المفتاح الخصوصي، فإن الشهادة قد تفقد جدارتها بالثقة أو تصبح غير قابلة للتعويل عليها، وقد يقوم مقدم خدمات التصديق، بناء على طلب الموقع أو حتى بدون موافقته إلى تعليق الشهادة أو إلغائها، كما يمكن أن يتوقع من مقدم خدمات التصديق أن ينشر إشعارا بالإلغاء أو التعليق، أو أن يبلغ الأمر إلى الأشخاص الذين يعرف أنهم تلقوا توقيعا رقميا يمكن التحقق من صحته بالرجوع إلى الشهادة التي لا يمكن التعويل عليها[2]، وتجدر الإشارة أنه في حال حدوث أي تغيير للمعلومات الواردة في الشهادة أو انتفاء سريتها، فيلتزم صاحب الشهادة بإبلاغ مقدم خدمة التصديق الالكتروني بأي تغيير للمعلومات الواردة في الشهادة أو انتفاء سريتها، كما يجوز لصاحب الشهادة التي أوقفت

[1] - خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، مرجع سابق، ص.252 .

[2] - دليل تشريع قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية2001، ج2، البند 57 ، ص.35 .

أو ألغيت إعادة استعمال عناصر التوقيع الالكتروني للشهادة المعنية لدى مقدم خدمات تصديق آخر[1]، وبالتالي سنتطرق إيقاف العمل بشهادة التصديق الإلكتروني وإلغائها **(أولا)**، ثم إلى مسؤولية صاحب شهادة التصديق الالكتروني **(ثانيا)**.

أولا: إيقاف العمل بشهادة التصديق الإلكتروني وإلغائها

يقصد بتعليق العمل بالشهادة بأنه الوقت المؤقت لسريان الشهادة وهو ما يعني تعطيل العمل بالأثر القانوني المترتب على الشهادة تمهيدا لإلغائها[2].

1 ـ تعليق العمل بشهادة التصديق الالكتروني:

يمكن لصاحب شهادة التصديق الالكتروني ولظروف معينة إيقاف العمل بالشهادة مدة من الزمن حتى يزول ذلك الظرف، إما لحماية توقيعه الإلكتروني نتيجة اختراق أحدهم لمنظومته أو أنه لا يرغب باستخدام توقيعه في الوقت الحالي، مما يؤدي إلى تعطيل العمل بها بصورة مؤقتة تمهيدا لإلغائها أو استئناف العمل بها إذا ما تبين عدم صحة السبب الذي أوقف العمل بالشهادة بناءا عليه.

لم يتطرق القانون النموذجي الصادر من الأمم المتحدة والخاص بالتوقيعات الالكترونية إلى تعليق الشهادة وحالات التعليق، ونفس الموقف أخذ به المشرع الجزائري بحيث أنه لم ينص على الحالات التي تعلق فيها الشهادة واكتفى بذكر الحالات التي تلغى فيها عكس بعض التشريعات الأخرى كالمشرع التونسي.

نص القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة في المادة 23على أنه تقوم جهة التوثيق بتعليق العمل بالشهادة بناءا على طلب صاحب الشهادة، أو إذا تبين أن الشهادة سلمت

[1] ـ مخلوفي عبد الوهاب، مرجع سابق، ص.243.

[2] ـ غاني جدير السعدي، أكرم محمد حسن، النظام القانوني لشهادة التوثيق الالكتروني، مجلة الحلبي للعلوم القانونية والسياسية، العدد الثاني، السنة التاسعة، 2017، ص.202.

معلومات غير صحيحة وتبين أن المعلومات المتضمنة بالشهادة قد تغيرت، واستعملت الشهادة بغرض التدليس أو الغش، أو إذا تم انتهاك أداة إنشاء التوقيع الإلكتروني.[1]

نص المشرع المصري في المادة 12 من اللائحة التنفيذية لقانون التوقيع الالكتروني إلى إمكانية تعليق العمل بشهادة التصديق الالكترونية، إذا ما توفرت إحدى حالات التعليق التي نصت عليها اللائحة، كحالة العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها، سرقة أو فقدان المفتاح الشفري الخاص أو البطاقة الذكية أو عند الشك في حدوث ذلك، حالة عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم بينه وبين المرخص له"[2].

نص قانون المبادلات والتجارة الإلكترونية التونسي في الفصل 19 من الباب الرابع على تعليق العمل بشهادة المصادقة الالكتروني بأنه يتولى مزود خدمات المصادقة الالكترونية تعليق العمل بشهادة المصادقة حالا بناءا على طلب من صاحبها أو عندما يتبين بأن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة أوقد تغيرت واستعملت بغرض التدليس، أو تبين أيضا أن منظومة إحداث الإمضاء قد انتهكت.[3]

يمكن من خلال النصوص القانونية السابقة يمكن أن نحصر الحالات التي يمكن لمقدم خدمة التصديق الالكتروني تعليق العمل بشهادة التصديق الالكتروني:

أ ـ تعليق العمل بشهادة التصديق الالكتروني بناءا على طلب صاحب الشهادة:

يجب على مؤدي خدمة التصديق الالكتروني تعليق العمل بشهادة التوثيق إذا طلب منه صاحب الشهادة، وما على مقدم خدمة التصديق الالكتروني إلى الخضوع والامتثال لرغبته دون قيد أو شرط، باستثناء استخدام شهادة التصديق الالكتروني لغرض الغش أو التدليس.

[1] ـ راجع نص المادة 23 من القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، على موقع: https://carjj.org/

[2] ـ راجع نص المادة 12 من قرار رقم 109 لسنة 2005 المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[3] ـ راجع الفصل 19 من قانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية التونسي.

ب ـ تغير المعلومات التي تتضمنها شهادة التوثيق الالكتروني :

يقوم مؤدي خدمة التصديق الالكتروني بتعليق شهادة التصديق إذا حدثت هناك تغييرات وتعديلات في المعلومات، أو البيانات الإلزامية في الشهادة ذاتها، أو المتعلقة بصاحبها أو مصدرها إلى حين إزالة هذا التغيير أو التعديل، لأن حجية الشهادة تكمن في تحقيق الثقة والمصداقية والأمان فيها.

ج ـ تعليق الشهادة إذا تبين أنها سلمت بناءا على معلومات مزيفة أو مغلوطة :

يمكن في بعض الحالات تعليق العمل بشهادة التصديق الالكترونية وهذا في حال إذا ما صدرت بناءا على معلومات مزيفة أو مغلوطة،[1] تتحقق هذه الحالة إذا قدم صاحب طلب الحصول على شهادة التصديق لمستندات تثبت قدرته على إبرام التصرفات القانونية، ويتبين فيما بعد لمقدم خدمة التصديق الالكتروني أن شهادة التصديق الالكتروني تم إصدارها وفقا لمعلومات غير صحيحة، الشيء الذي يدفعها إلى إيقاف العمل بها فورا[2].

د ـ عدم التزام الشخص المصدر له شهادة التصديق ببنود العقد المبرم مع المرخص له:

يترتب على إخلال الشخص المصدر له شهادة التصديق الالكترونية بالتزامه ببنود العقد المبرم إيقاف العمل بالشهادة مؤقتا، ويكون نظام إيقاف الشهادات وفقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة[3].

[1] ـ المعلومة المغلوطة: هي معلومات صحيحة ولكنها تخص شخصا آخر، فإذا ما سلمت المعلومات ثم أدخلت لغير صاحبها لتشابه في الأسماء مثلا، فإن ذلك يعني أن مزود الخدمة قد وقع في غلط، وعليه المسارعة إلى تعليق العمل بالشهادة، والشهادة هنا صحيحة، ولكن البيانات الواردة فيها تخص شخصا آخر، فإذا قام الغير باستخدام الشهادة رغم علمه بالغلط، شكل ذلك جريمة لاتخاذه اسما أو صفة كاذبة،أما المعلومة المزيفة هي معلومة غير صحيحة ولا وجود لها في الواقع، كأن يقوم شخص بتزوير بطاقته الشخصية أو غير ذلك من الوثائق الرسمية، ثم يقدمها لمزود الخدمة وتصدر شهادة التصديق بناء عليها، للمزيد راجع في ذلك: عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة ، مرجع سابق، ص.176.

[2] ـ خالد ممدوح إبراهيم، مرجع سابق، ص.177.

[3] ـ خالد حسن أحمد، الحجية القانونية للمستندات الالكترونية بين الفقه الإسلامي والقانون الوضعي، مرجع سابق، ص.207.

و ـ انتهاك منظومة أمن إحداث التوقيع الالكتروني :

يدفع التلاعب بمنظومة إنشاء التوقيع الالكتروني الموصوف بمقدم خدمة التصديق الالكتروني إلى تعليق العمل بشهادة التصديق فورا، لذا يجب على الموقع عند استخدامه لأداة إحداث توقيع إلكتروني مأذون بها من طرف مقدمي خدمة التصديق الالكتروني موثوق به، أن يمارس العناية اللازمة لتفادي استخدامها خارج النطاق المرخص به، وأن يخطر مقدم الخدمة أو الطرف المعول على الشهادة عند تعرض بيانات إنشاء التوقيع الإلكتروني لما يثير الشبهة فيها أو عند الشك في حدوث ذلك[1].

ي ـ تعليق العمل بالشهادة إذا ثبت فقدان الموقع لمفتاحه الخاص:

ألزمت أغلب التشريعات المنظمة للمعاملات الالكترونية بإيقاف العمل بشهادة التصديق الالكتروني متى ثبت فقدان مفتاح التشفير الخاص بالموقع، أو حتى عند الشك في حدوث ذلك[2].

2 ـ إلغاء شهادة التصديق الالكتروني:

يعني الإلغاء انعدام الأثر القانوني للشهادة وكأنها لم تكن، فيمكن أن يحدث في بعض الحالات ما يستوجب إيقاف أو إلغاء شهادات التصديق الالكتروني، كالحالات التي قد يحدث فيها اختراق لبرنامج المعلومات المسئول عن سلامة المحرر الالكتروني وصحة تواقيعه، الأمر الذي يجعل تلك الشهادات عرضة للعبث ببياناتها والاطلاع على المعلومات السرية لمستخدمي خدمة التوقيع الالكتروني، وكذلك يمكن فقدان المفتاح الشفري الخاص أو انتهاء مدة صلاحية شهادة المصادقة الالكترونية.

نص المشرع التونسي في قانون المبادلات والتجارة الالكترونية في الفصل 20 الباب الرابع إلى أنه **:" يلغي مزود خدمات المصادقة الالكترونية حالا للشهادة في الحالات التالية: عند طلب صاحب الشهادة، عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي**

[1] ـ عبد الفتاح بيومي حجازي، مرجع سابق، ص.177.

[2] ـ خالد ممدوح إبراهيم، التوقيع الالكتروني، مرجع سابق، ص.228.

صاحب الشهادة، عند القيام باختبارات دقيقة بعد تعليقها وتبين أن المعلومات مغلوطة أو مزيفة أو أنها غير مطابقة للواقع أو أنه قد تم انتهاك منظومة إحداث الإمضاء أو الاستعمال المدلس للشهادة".[1]

نص المشرع الجزائري في المادة 45 من القانون رقم 15- 04 المتعلق بالتوقيع والتصديق الالكترونيين على أن **: " يلغي مؤدي خدمات التصديق الالكتروني شهادة التصديق الالكتروني في الآجال المحددة في سياسة التصديق الالكتروني، بناءا على طلب صاحب شهادة التصديق الالكتروني الموصوفة الذي سبق تحديد هويته".**

كما أنه يلغي مؤدي خدمات التصديق الالكتروني أيضا شهادة التصديق الالكتروني الموصوفة نهائيا، عندما يتبين لمقدم خدمة التصديق الالكتروني أنه قد منح شهادة التصديق الالكتروني بناء على معلومات خاطئة أو مزورة، أو تم تغيير في المعلومات التي بحوزته بالتالي لم تعد شهادة التصديق الالكتروني مطابقة لسياسة التصديق، أو عندما يتبين بيانات إنشاء التوقيع قد انتهكت سريتها، أو تم إعلامه بوفاة الشخص الطبيعي أو بحل الشخص المعنوي صاحب شهادة التصديق الالكتروني، وعليه يجب إخطار صاحب شهادة التصديق الالكتروني الموصوفة بإلغاء هذه الأخيرة مع تسبيب ذلك، كما يجب عليه تبليغ صاحب شهادة التصديق الالكتروني الموصوفة بانتهاء مدة صلاحيتها في الآجال المحددة في سياسة التصديق[2].

يلاحظ من خلال هذه المادة أن المشرع الجزائري لم يتطرق للحالات التي يتم فيها تقديم طلب الإلغاء، واكتفى فقط بتبليغ صاحب الشهادة الموصوفة بانتهاء مدة صلاحيتها في الآجال المحددة في سياسة التصديق، كما أنه ألزم مؤدي خدمة التصديق الإلكتروني بإخطار صاحب الشهادة دون تحديد الكيفية ولا الطريقة إنما ذكر فقط واجب ذكر سبب الإلغاء.

يلاحظ مما سبق أن مقدم خدمة التصديق الالكتروني ملزم بإلغاء الشهادة إذا ما توافرت إحدى الحالات السابقة، ويجب عليه أن يقوم بإلغاء الشهادة حالا دون تأخير، بالإضافة أنه يجب

[1] - الفصل 20 من قانون عدد 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية التونسي.

[2] - راجع نص المادة 45 /02 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

عليه إعلام الموقع بهذا الإلغاء، ويتحمل بدوره أي خطأ بسبب إيقاف الخدمة أو إخلاله بالالتزامات المترتبة عليه.

يمكن بناءا علية ومن خلال النصوص السالفة الذكر أن نجمل الحالات التي يتسبب فيها إلغاء شهادة التصديق الالكتروني كالآتي:

أ ـ إلغاء شهادة التصديق الالكتروني بناءا على طلب صاحب الشهادة:

يجب على مقدم خدمة التصديق الالكتروني إذا طلب منه صاحب الشهادة الفعلي إلغائها مباشرة وفورا، وإعلام الموقع بهذا الإلغاء لأن أي تأخير في ذلك يوجب مسئولية مقدم الخدمة عن ضرر يلحق صاحب الشهادة أو الغير، وهذا إما نتيجة عدم الإعلام بأن الشهادة انتهى العمل بها ولا يجب على صاحب الشهادة ذكر أي سبب أو مبررات في طلبه، وذلك لأنها تحمل صفة شخصية لصاحب الشهادة الفعلي.

ب ـ وفاة الشخص الطبيعي أو انقضاء الشخص المعنوي صاحب الشهادة:

يجب على مقدم خدمة التصديق الالكتروني إلغاء الشهادة فور إعلامه بوفاة الشخص الطبيعي صاحب الشهادة، أوفي حالة انقضاء الشخص المعنوي، على اعتبار أن شهادة التصديق الالكتروني هي من العقود التي تقوم على الاعتبار الشخصي.

ج ـ إلغاء الشهادة التي تم تعليق العمل بها بصفة مؤقتة:

لا يمكن لمقدم خدمة التصديق الالكتروني إلغاء شهادة التصديق الالكتروني التي تم تعليق العمل بها، إلا إذا تحرى بنفسه وتأكد أن الأسباب التي دفعته إلى اتخاذ قراره صحيحة وجدية، وأن النتيجة مطابقة لسبب الإيقاف وجب عليه إلغاء الشهادة بصفة نهائية.

د ـ توقف مقدم خدمات التصديق الالكتروني عن تقديم الخدمات المرخص لها:

يتعين على مقدم خدمة التصديق الالكتروني في حالة التوقف عن مزاولة نشاطه، أن يلتزم بعد الحصول على الموافقة المسبقة من طرف السلطة المختصة بذلك إلغاء كل شهادات التوثيق

المصدرة عنه للمتعاملين معه، وهذا اعتبارا من تاريخ التوقف عن الخدمة، ويلتزم بتعويض الأضرار التي تلحق بصاحب الشهادة أو الغير إذا دعت الضرورة لذلك.

ثانيا: مسئولية صاحب شهادة التصديق الالكتروني

ألزم قانون الأونسترال النموذجي للتوقيعات الالكترونية في المادة 01/08 منه على كل موقع أن **"يولي عناية معقولة لاجتناب بيانات إنشاء توقيعه استخداما غير مأذون به"**[1].

أورد المشرع في القانون 15-04 على التزامات صاحب شهادة التصديق الالكتروني فنص في المادة61 منه على أنه: **"يعتبر صاحب شهادة التصديق الالكتروني فور التوقيع عليها المسئول الوحيد عن سرية بيانات إنشاء التوقيع، وفي حالة الشك في الحفاظ على سرية بيانات إنشاء التوقيع، أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات المتضمنة في شهادة التصديق الالكتروني، فإنه يجب على صاحب الشهادة أن يعمل على إلغائها من طرف خدمات التصديق الالكتروني، ولا يجوز لصاحب شهادة التصديق الالكتروني عند انتهاء صلاحيتها أو عند إلغائها استعمال بيانات إنشاء التوقيع الموافقة لها من أجل توقيع أو تصديق هذه البيانات نفسها من طرف مؤدي خدمات التصديق الإلكتروني".**

أضاف المشرع في المادة 62 منه على أنه**: " لا يجوز لصاحب شهادة التصديق الالكتروني الموصوفة استعمال هذه الشهادة لأغراض أخرى غير تلك التي منحت لأجلها"**[2].

يلاحظ من خلال ما تقدم أن صاحب الشهادة يعد مسئولا عن سلامة وسرية بيانات إنشاء التوقيع الالكتروني الخاصة به، ويعد صادرا منه كل استعمال لهذه البيانات، بحيث يلزم عليه التقيد بشروط استعمال الشهادة ومدة صلاحيتها وشروط إنشاء بيانات التوقيع الموافقة لها.

نخلص مما تقدم أن التصديق الإلكتروني هو وسيلة فنية آمنة، يعود الغرض الأساسي من استخدامه هو التأكد من صحة التوقيع الإلكتروني أو المحرر الإلكتروني، بحيث يتم نسبة هذا

[1] ـ المادة 01/08 من قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001السالف الذكر.

[2] ـ المادة 61 و62 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.

التوقيع إلى صاحبه، عن طريق جهة تسمى بمؤدي خدمات التصديق الإلكتروني، حيث يقوم هذا الأخير بإصدار شهادة التصديق الإلكتروني التي تعتبر مستندا إلكترونيا تتفق ونظم المعالجة الآلية للمعطيات، وطبيعة التعاملات الإلكترونية التي تتم بين الأطراف والتي يتم إبرامها عبر وسائل الاتصال الحديثة، أين يتحمل مؤدي خدمة التصديق الإلكتروني كافة التبعات القانونية والمسئولية المترتبة عن أي ضرر يمكن أن يقع في الشهادة، لأن وظيفته تكمن أساسا في خلق بيئة تعاملات إلكترونية آمنة عن طريق لعب دور الوسيط المؤتمن بين المتعاملين في هذه البيئة، وذلك لضمان سلامة مضمون المحررات الإلكترونية المتداولة، من خلال الإجراءات التي يتم استخدامها لاكتشاف أي تلاعب أو تحريف في التوقيع أو المحرر الالكتروني بداية من تاريخ إجراء التوثيق، مما يمنح له الحجية القانونية سواء في مواجهة أطراف العلاقة أو الغير.

خلاصة الباب الأول

أتاح التطور التقني في مجال المعلومات والاتصالات استخدام وسائل الاتصال الحديثة في العديد من المعاملات، عن طريق نظام تبادل رسائل البيانات الموقعة توقيعا إلكترونيا، بالتالي أصبح من الضروري على التشريعات الوطنية إيجاد تنظيم قانوني يتلاءم مع التطور الذي طرأ على المحررات الإلكترونية، ويزيل العقبات التي تقف دون قبول الكتابة الإلكترونية والتوقيع الإلكتروني في الإثبات.

حتى يكون للمحرر الإلكتروني مكانته ضمن وسائل الإثبات ومساواته مع المحرر الورقي التقليدي، لا بد من استيفائه لمجموعة من الشروط التي أقرتها أغلب التشريعات المقارنة التي تبنت مبدأ التعادل الوظيفي، والمتمثل أساسا في أن الطبيعة التي أنشأ عليها تسمح له بالاحتفاظ بمحتواه لمدة أطول حتى يمكن الرجوع إليه عند الحاجة، بحيث لا يطرأ عليه أي تغيير أو محو أو أي عبث به من لحظة الإنشاء إلى لحظة الاستلام، وأن يكون قابلا للقراءة والإدراك وله دلالة واضحة على الشخص الذي أنشأها أو تسلمها وتاريخ وقت الإرسال والتسليم، فعناصر المحرر الإلكتروني من كتابة وتوقيع ترد على وسيط أو دعامة إلكترونية، وهو وسيلة قابلة للتخزين وحفظ واسترجاع المعلومات بطريقة إلكترونية، فقد قدمت التكنولوجيا الحديثة ولا تزال تقدم باستمرار تقنيات عالية الدقة تضمن وتؤمن حفظ المحرر الإلكتروني لثباتها واستمرارها دون أي تعديل أو عبث بها، ومن بين هذه التقنيات المصغرات الفيلمية، الأقراص المغناطيسية، ذاكرة الحالة الصلبة، الأشرطة المنسابة، إلى غيرها من الوسائل العلمية المعدة خصيصا لهذه الأمور.

تتمتع المحررات الالكترونية سواء كانت رسمية أو عرفية بحجية في الإثبات تتفاوت قوتها بحسب نوعها، فالمحرر الرسمي هو الذي يقوم بتحريرها موظف عام أو شخص مكلف بخدمة عامة يثبت ما تم على يديه أو ما تلقاه من ذوي الشأن، فهذه المحررات تكون معدة مقدما للإثبات، فالمحرر الإلكتروني الرسمي هو نفسه المحرر الرسمي ولكن في صورة كتابة إلكترونية، أما المحررات العرفية فهو الذي يقوم الأشخاص بتحريرها للرجوع إليها

عند الحاجة، ومنها ما يكون معدا مقدما للإثبات وموقعة من ذوي الشأن والتي يلزم لاعتبارها دليلا كتابيا كاملا أن يوقع عليها أطرافها، ومنها غير معدة للإثبات كالرسائل والبرقيات، والتي يجب أن تتضمن الكتابة فيها معنى وجود واقعة تنشئ حقا لمصلحة من يتمسك بهذه المحررات في مواجهة من وقع عليها، فهي لا تعتبر دليلا كتابيا كاملا بحيث يمكن دحضها ونقض ما هو مدون بها بكافة طرق الإثبات.

أدى استخدام تقنيات الاتصال الحديثة أن أصبحت فيها الكتابة الالكترونية ترد على وسيط أو دعامة إلكترونية، بحيث أنها تتيح إمكانية تعديل مضمونها بكل يسر سواء بالإضافة أو الحذف أو المحو عن طريق الإمكانيات المتعددة لبرامج معالجة البيانات دون ترك أثر، بالإضافة إلى اتسام الدعامة الالكترونية بالحساسية الشديدة التي تجعل من الكتابة عليها قابلة للتلف بسرعة، بالتالي حتى يمكن الاعتداد بالكتابة الإلكترونية من الناحية القانونية يجب أن تنطوي على ما تشمله الكتابة بمعناها التقليدي من شرط الثبات وشرط الجدية، وقدرتها على التخزين والحفظ الإلكتروني وإمكانية قراءتها والاطلاع عليها في وقت لاحق دون أن يطرأ تغيير في مضمونها، وإمكانية استرجاعها كلما دعت الحاجة إلى ذلك، بالتالي يمكن الاعتراف بحجية معينة إذا ما استوفى الشرط الثاني من شروط الأدلة الكتابية وهو التوقيع الالكتروني.

ظهر التوقيع الالكتروني كضرورة ملحة في إيجاد بديل يحل محل التوقيع اليدوي، وذلك لاعتبارات أمنية فرضها شكل وخصوصية التعامل على شبكة الانترنت لاسيما في مجال المحررات الإلكترونية، من حفاظ على سرية البيانات والمعلومات المتبادلة بين أطراف التعامل، فيتميز التوقيع الإلكتروني بمنح الحجية القانونية لأي محرر إلكتروني صادر من وسائل الاتصال الحديثة ويكون معترفا به أمام القضاء، وعليه اشترطت التشريعات المقارنة بشأن التوقيع الإلكتروني للاحتجاج به عدة شروط وهي أنه يجب أن يكون القصد منه إثبات هوية الطرف الموقع، أن يتم التوقيع بوسائل خاصة به وتحت سيطرته، أن ينفرد به الشخص الذي أصدره، أن يكون التوقيع مرتبطا بالرسالة الإلكترونية، وأن يقوم الموقع ببذل العناية المعقولة لتفادي استخدام توقيعه الإلكتروني استخدام غير مأذون، بالتالي نجد أن التوقيع

الإلكتروني لا يختلف كثيرا عن التوقيع العادي من حيث الوظيفة والهدف والحجية، لكن الاختلاف الجوهري يكمن فقط في الوسيلة أو الدعامة المستخدمة.

يلتزم القاضي بقبول المحررات الإلكترونية الذي يتم تأمين بياناتها كدليل كامل متى كانت موقعة من أطرافها وإلا أدى ذلك إلى إضعاف الثقة فيها، وذلك يستوجب وجود سند تشريعي يحدد نطاق وشروط اعتماد الكتابة الموقعة إلكترونيا، ولا يتم ذلك إلا بتطوير مفهوم عناصر المحرر الإلكتروني المتمثلة في الكتابة والتوقيع الإلكترونيين، ليشملا أية وسيلة لإحداثهما متى كانت تؤدي وظائفها.

يعتمد لإضفاء الثقة والأمان التي تعتبر من الضمانات الأساسية في تأمين المحررات الإلكترونية، التحقق من صحتها و نسبتها إلى جهة معينة أو طرف محايد مستقل عن أطراف العلاقة القانونية، يضمن احترام سرية المعلومات وعدم إفشائها أو السماح للغير بالإطلاع عليها وإذاعة محتوياتها، فتحقيق شرط الحفظ الذي تم إنشائه به يستوجب بالضرورة اعتماد نظام الحفظ الإلكتروني، المتمثل في نظام التصديق الإلكتروني والذي يقوم في نهاية الأمر بإصدار شهادات المصادقة الإلكترونية، لذلك يجب على مقدم خدمة التصديق الإلكتروني اتخاذ التدابير والإجراءات التي تكفل حماية وتأمين المحررات الإلكترونية بكافة الوسائل المتاحة له، بالإضافة إلى نظام التشفير الذي يعد الوسيلة التقنية التي تساعد على تأمين وظائف الأمن والسرية للمحررات الإلكترونية، وتضمن عدم تسرب المعلومات والبيانات المخزونة إلكترونيا إلى الغير، وهذا كله يؤدي بالنتيجة إلى فرض قدر من المحافظة على سرية مضمونها وسلامتها من أي تحريف أو اعتداء من أي كان عليها.

الباب الثاني

الحماية الجنائية للمحررات الالكترونية

الباب الثاني

الحماية الجنائية للمحررات الالكترونية

الباب الثاني

الحماية الجنائية للمحرر الالكتروني

ساهم التقدم العلمي في تكنولوجيا المعلومات إلى إنجاز العديد من المعاملات بشكل سريع وموثوق به، مما أدى إلى تغيير حياة الأفراد اليومية وعلاقاتهم الاجتماعية حتى أصبحت هذه التكنولوجيا مهيمنة على كافة جوانب الحياة المعاصرة، ونتيجة لهذا التطور التكنولوجي في وسائل التقنيات الحديثة، ظهر صنف جديد من الجرائم يتخذ أنماطا جديدة تستند بصورة أساسية على الذكاء الإجرامي والذي بات يعرف بالجرائم الإلكترونية، والتي أصبحت تمثل تحديا جديا وجديدا في العصر الحالي، حيث يستغل بعض المجرمين هذه التكنولوجيا في ارتكاب جرائمهم بطرق محكمة ودون ترك أي أثر واضح لتلك الجرائم، فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة، وأن عدم مواكبة التشريعات لهذا التطور السريع لأشكال الجريمة يمكن أن يؤدي إلى حدوث فراغ تشريعي، وثغرات قانونية تمكن مرتكبو هذه الجرائم من الإفلات من المتابعة والعقاب في كثير من الأحيان، وبالتالي سيساهم ذلك في تنامي صور الاعتداء على المحررات الالكترونية، لذلك اهتمت التشريعات المقارنة بسن قوانين لمواجهة هذه الظاهرة المستحدثة، ومواكبتها مع إيجاد الحلول التشريعية لمكافحتها، وعدم الاكتفاء بالنصوص التقليدية التي أضحت عاجزة سواء من الناحية الموضوعية أو من الناحية الإجرائية، فقد فرض ذلك أن وضعت أغلب التشريعات التي تتبنى هذا النوع من المعاملات تشريعات خاصة تكفل الحماية الجنائية للمحررات الإلكترونية من خلال القواعد الموضوعية والقواعد الإجرائية.

تتلخص القواعد القانونية الموضوعية في تجريم السرقة، النصب، الاحتيال، والتزوير بالإضافة إلى تجريم الصور المستحدثة من الاعتداء بواسطة هذه التقنية الحديثة كالدخول والبقاء غير المشروع لنظم المعالجة الآلية للمعطيات، وجريمة الإتلاف في مجال المحررات الالكترونية وذلك حتى لا يسمح بمرور الكثير من الجرائم الإلكترونية دون عقاب، فإذا كان التطور المتجدد في وسائل التعدي على المحررات الإلكترونية يحجم صورة التجريم الحالية عن

مواكبة ما يطرأ من صور إجرامية مستحدثة، إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، أما القواعد الإجرائية فهي تلك القواعد المنظمة للاختصاص القضائي وجمع دلائل التحقيق والمحاكمة، فيعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، لما تثيره من إشكالات إجرائية، ككيفية تفتيش الأنظمة المعلوماتية واستخلاص الأدلة الجنائية الرقمية، معاينة مسرح الجريمة المعلوماتية، ضبط الأدلة الجنائية الرقمية، والصعوبات التي تعترض هذه الإجراءات وحجيتها أمام القضاء الجنائي، فلا يقتصر جمع الأدلة على أساليب الحصول على الدليل الجنائي الإلكتروني، وإنما يتعدى ذلك إلى الأشخاص الذين يتعاملون معه سواء كانوا محققين أو خبراء أو قضاة، فأسلوب جمع الأدلة الجنائية وآليات الحصول عليها في الجرائم الماسة بالمحررات الإلكترونية، يصعب على جهات التحقيق القيام بمهامها بإتباع الطرق التقليدية نفسها للحصول على الدليل الإلكتروني، وإنما يستوجب ذلك المعرفة الفنية والتأهيل التقني لجهات التحقيق عند التعامل مع هذا النوع المستحدث من الأدلة.

بالتالي فإن الأمر يقتضي أولا التطرق إلى الحماية الجنائية للمحررات الإلكترونية من خلال التعرض إلى الإطار المفاهيمي لجرائم المحررات الإلكترونية، وأشكال الجرائم التي يمكن أن تمس بأمنها وسلامتها **(الفصل الأول)**، ثم التطرق ثانيا إلى الحماية الجنائية الإجرائية لهذه المحررات والذي يقودنا إلى البحث عن الحماية الجنائية الإجرائية لها قبل مرحلة المحاكمة، ثم إلى الحماية الجنائية الإجرائية لها في مرحلة المحاكمة **(الفصل الثاني)**.

الفصل الأول

الحماية الجنائية الموضوعية للمحررات الالكترونية

أحدث التطور التقني للنظم المعلوماتية انعكاسات كبيرة أثرت على المنظومة القانونية بصفة عامة والقانون الجنائي بصفة خاصة، مما أثار إشكالية الحماية الجنائية لها سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها، فتطبيق القواعد التقليدية على مثل هذه الجرائم يثير مشاكل عديدة ومعقدة فيما يتعلق بالقانون الجنائي الموضوعي، بحثا عن إمكانية تطبيق هذه القواعد على هذا النوع المستحدث من الجرائم مع احترام مبدأ الشرعية والتفسير الضيق للنصوص الجنائية، سيما أن هذا النوع من الجرائم يرتكز على تقنيات عالية يقوم بارتكابها مجرم معلوماتي يتصف بالذكاء، وبالتالي فهي بحاجة إلى تشريعات قادرة على التعامل معها بشكل ينسجم مع تطور هذه الجرائم، لأن الاكتفاء بالنصوص التقليدية أضحت غير ملائمة للانطباق على هذا النوع المستحدث من الجرائم، مما أدى إلى توجه أغلب الدراسات القانونية إلى البحث في الأبعاد والمضامين القانونية لظاهرة الجريمة الالكترونية، فسارعت الكثير من الدول من خلال الجهات القانونية المعنية بالبحث في مواجهة تلك الظواهر المستحدثة من الإجرام، فاجتهد الفقه في البحث عن الحماية الملائمة للنظم المعلوماتية وذلك لكي يمهد الطريق أمام التشريعات باختيار وانتقاء الحماية الملائمة لمواجهة تلك الجرائم، حيث أفضى هذا الاهتمام إلى إعادة النظر في كثير من المسائل القانونية المتعلقة بالجريمة عموما، لذا تتخذ الجريمة الإلكترونية أهمية استثنائية لسلامة التعامل مع هذا النوع المستحدث من الجرائم، عن طريق إدراك ماهيتها واستظهار خصائصها وسمات مرتكبيها ودوافعهم **(المبحث الأول)**.

تقوم الحماية الجنائية الموضوعية للمحرر الالكتروني على عدة اعتبارات وأسس قانونية تقوم على حمايته من العديد من الجرائم الماسة به وبصحته وقوته القانونية، فتختلف صور المساس بمحتواه، فمنها ما يتعلق بأفعال التزوير والنصب والسرقة، ومنها ما يقوم على استحداث نصوص خاصة تجرم المساس بالمحررات الإلكترونية كجريمة الدخول والبقاء غير

المشروع في أنظمة المعالجة الآلية للمعطيات، وجريمة الإتلاف المعلوماتي في مجال المحررات الإلكترونية **(المبحث الثاني).**

المبحث الأول

الإطار المفاهيمي للجرائم الماسة المحررات الالكترونية

تعد الجرائم الالكترونية كظاهرة إجرامية حديثة نظرا لارتباطها الشديد بالتكنولوجيات الحديثة، وجاء تطور هذا النوع من الجرائم بالتزامن مع التطورات التي تشهدها مختلف التقنيات ووسائل التواصل وانتقال المعلومات، والذي دفع ببعض المجرمين إلى استغلال مميزات هذه التقنية في الأنشطة الإجرامية بكفاءة وسرعة تفوق قدرات المحققين، بعد أن أدخلوا هذه التقنيات والوسائل الفنية مع الجرائم التقليدية التي يقومون بها وذلك لتسهيل ارتكابهم لها، فهم مجرمون عادة يكونون من ذوي الاختصاص والمعرفة في هذا المجال، وبالتالي ظهرت هناك أنماط مختلفة ومغايرة تماما عن أشكال السلوك غير المشروع في ارتكاب الجرائم، فلا تختلف الأحكام العامة للجريمة المعلوماتية عن الأحكام العامة للجريمة العادية التقليدية إلا فيما ندر في ركنها المادي، وخاصة فيما يتعلق بعدم خضوعها لحدود المكان والزمان، وما يتعلق بصعوبة إثبات هذه الجرائم نظرا أنها لا تترك في أغلب الأحيان أثرا ماديا ظاهرا يمكن ضبطه، مما يشكل البيئة التي يفضلها أغلب المجرمين، خصوصا أنه يمكن تحقيق مكاسب طائلة من وراء هذا النوع من الجرائم.

اعتبرت بعض التشريعات المقارنة الجرائم الالكترونية جرائم خاصة وتعاملت معها كظاهرة إجرامية مستجدة، تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي المجسدة لكل جريمة من هذه الجرائم، وحسمت الجدل القائم والواسع حول مدى انطباق النصوص القائمة على هذه الجرائم لجهة وضع تشريعات ونصوص جديدة، تكون قادرة على الإحاطة بمفردات ومتطلبات وخصوصية هذا النوع المستحدث من الجرائم.

لذا سنتناول هذا المبحث من خلال بيان مفهوم الجريمة الإلكترونية **(المطلب الأول)**، ثم بعد ذلك نتطرق إلى مرتكب هذه الجريمة الإلكترونية الذي يطلق علية تسمية المجرم المعلوماتي **(المطلب الثاني)**.

المطلب الأول

مفهوم الجريمة الالكترونية

تعد الجريمة الالكترونية من الجرائم المستحدثة في عصرنا الحديث وهذا يعود أساسا إلى ارتباط هذه الجريمة بوسائل وتقنيات الاتصال الحديثة، فلقد تباينت الصور الإجرامية لظاهرة الجريمة الالكترونية وتشعبت أنواعها، وبالتالي أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بهذا التقدم التقني، فالتطور المستمر لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل بمفهوم الجريمة المعلوماتية أو الالكترونية، ومما لا شك فيه أن عدم وضع تعريف للجريمة المعلوماتية يثير العديد من المشكلات العملية لعل أهمها صعوبة مواجهتها، وتعذر إيجاد الحلول المناسبة لمكافحتها، لا سيما الآثار السلبية التي خلفتها هذه التكنولوجيا الحديثة في وسائل الاتصال، مما استدعى دراستها من أجل تحديد مفهوم موحد لها وتحديد طبيعتها القانونية، وسنحاول أن نتناول من خلال هذا المطلب تعريف الجريمة الالكترونية **(الفرع الأول)**، ثم سنتعرض إلى خصائص الجريمة الالكترونية **(الفرع الثاني)**.

الفرع الأول

تعريف الجريمة الالكترونية

ترتبط الجريمة المعلوماتية بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات والحاسب الآلي، فهي تثير الكثير من الغموض، بالتالي تعددت الجهود الرامية إلى وضع تعريف محدد لها، بل أن أغلب الفقهاء رجحوا إلى عدم وضع تعريف لها بحجة أن الجريمة الالكترونية هي جريمة تقليدية، وهي امتداد لها ترتكب بمساعدة التكنولوجيا الحديثة باستخدام أجهزة الحاسب الآلي وتكنولوجيا الاتصالات، فجهاز الحاسب الآلي يؤدي دورا مهما في إتمام أي نشاط إجرامي في ارتكاب الجريمة، كما أن اختلاف النظم القانونية والثقافية بين الدول أدى إلى عدم الاتفاق على مصطلح واحد للدلالة عليها خشية حصرها في مكان ضيق، وبالتالي أدى ذلك إلى عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وعليه سنحاول من خلال هذا الفرع تحديد مفهوم الجريمة الالكترونية من خلال إلقاء الضوء على أهم آراء الفقه التي تناولت موضوع الجريمة الالكترونية، وإلى مختلف التشريعات التي حاولت تقديم تعريف لها **(أولا)**، ثم إلى التعريف التشريعي للجريمة الإلكترونية **(ثانيا).**

أولا: التعريف الفقهي للجريمة الالكترونية

اختلف الفقه في وضع تعريف جامع ومحدد للجريمة الالكترونية بل اختلف حتى في تسمية هذا النوع من الجرائم، فأطلقت على هذه الظاهرة المستحدثة عدة أسماء منها : الجريمة المعلوماتية أو الجريمة الالكترونية أو الجرائم المرتبطة بالكمبيوتر أو جرائم الكمبيوتر والانترنت أو الجرائم التقنية العالية أو جرائم الشبكة العنكبوتية[1]، ولصعوبة إيجاد هذا التعريف أدى بالبعض إلى القول بأن هذه الجريمة مستعصية على التعريف، ويستدلون على ذلك بالمحاولات العديدة التي بذلت لتعريفها والتي استخدمت عدة كلمات من أجل ذلك، لكن دون

[1]- أسامة أحمد المناعسة، جلال محمد الزغبي، مرجع سابق، ص.62. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة ،القاهرة، 2015، ص.9. حسين طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2004، ص.24.

التوصل إلى تعريف موحد لها[1]، بالمقابل أغلب الفقهاء أجمعوا على الأخذ بالاتجاه الذي ينظر إلى الوسائل الالكترونية في ارتكاب الجريمة، وفي نفس الوقت إلى موضوع الجريمة الالكترونية وهي البيانات والمعلومات.

عرفها بعض الفقه بأنها: **" جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"**[2].

يلاحظ أن هذا التعريف يحصر الجريمة المعلوماتية في الحالات التي تستدعي إلماما وقدرا كبيرا من المعرفة الفنية والتقنية لارتكابها، وهذا مفهوم خاطئ نظرا أن أغلب الحالات التي ترتكب فيها الجريمة الالكترونية يكون فيها المجرم غير ملما بهذا القدر من المعرفة.

عرفها جانب آخر بأنها: **" كل جريمة تتم في محيط أجهزة الكمبيوتر، فهي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"**[3].

ثانيا: تعريف الجريمة الإلكترونية في المواثيق الدولية والتشريعات الوطنية

عرف خبراء منظمة التعاون الاقتصادي والتنمية (O.C.D.E) الجريمة المعلوماتية بأنها: **" أي سلوك غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر اعتداء على الكمبيوتر"**[4].

يتبين لنا من خلال هذا التعريف أن التعريف اقتصر فقط على الجرائم المرتكبة بواسطة الحاسب الآلي دون ذكر الجرائم الواقعة على الحاسب الآلي.

[1] ـ هشام محمد فريد رستم، مرجع سابق، ص.29.

[2] ـ مشار إليه لدى: عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص.23.

[3] ـ مشار إليه لدى: خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الإسكندرية، 2011، ص.357. نبيل عمر نايل، الحماية الجنائية للمحل الالكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، القاهرة، 2012، ص.23. طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق، مجلة الشريعة والقانون، العدد28، المجلد 1، 2013، ص.211.

[4] ـ مشار إليه لدى: طارق إبراهيم الدسوقي عطية، مرجع سابق، ص.159.

عرفته منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا سنة 200 بأنها: **" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"**[1].

يلاحظ من خلال هذا التعريف أنه لم يحصر الجرائم الالكترونية، بل ترك المجال واسعا لاستيعاب جميع الأنواع والصور التي ستظهر مستقبلا نظرا للتطور السريع في مجال التكنولوجيا الحديثة، كما أن هذا التعريف لم يركز على فاعل الجريمة وخبرته التقنية ولا على وسيلة ارتكاب الجريمة، وذلك كله لعدم إتاحة المجال أمام إفلات العديد من صور الجريمة من الجزاء.

يجب الإشارة قبل التطرق إلى تعريف الجريمة المعلوماتية إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، والبعض الآخر يطلق عليها الجريمة المعلوماتية.

سارعت أغلب الدول نظرا لأهمية هذا النوع من الجرائم المستحدثة في العصر الحالي، إلى إيجاد قانون خاص يعالج المشاكل الناتجة عن الأفعال غير المشروعة، عبر استخدام أجهزة الحاسوب أو أية وسيلة تقنية المعلومات، لذا نجد بعض التشريعات اهتمت بتوضيح أو بتعريف بعض المصطلحات القانونية ذات العلاقة بالجريمة الالكترونية، كما أن أغلبها استعمل مصطلح الجريمة المعلوماتية كمصطلح عام على كل الجرائم المتعلقة بالحاسوب والانترنت.

لم يعرف المشرع الفرنسي الجريمة الالكترونية وإنما جرم بعض الأفعال المساهمة في حدوثها بنصوص قانونية، وبالتالي كعادته ترك مسألة تعريف الجريمة الالكترونية للفقه، فتحكم الجرائم الالكترونية في التشريع الفرنسي قواعد قانونية أعلى قيمة من القواعد القانونية في

[1] ـ مشار إليه لدى: أسامة أحمد المناعسة، مرجع سابق، ص.78.

القانون الفرنسي، تتمثل بقواعد قانون الاتحاد الأوربي[1]، كما نجد في قانون العقوبات الفرنسي الجديد الذي نص في المادة 1/323و2و3و4 في التعديل الأخير لقانون العقوبات الصادر في 1994، أن المشرع الفرنسي اكتفى بتجريم بعض الأفعال التي تساهم في حدوث الجريمة الالكترونية، وذلك بإدراجه في الفصل الثالث من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على الجريمة الالكترونية، كتجريمه لفعل البقاء والدخول بطريق الغش إلى نظام المعالجة الآلية للمعطيات.

لم يقدم المشرع الجزائري تعريفا للجريمة الالكترونية وإنما تطرق إليها بموجب قانون العقوبات رقم 04-15 في تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وهذا لسد الفراغ التشريعي بنصوص تجرم فعل المساس بأنظمة المعالجة الآلية للمعطيات، ثم أدخل تعديلا آخر على قانون العقوبات بموجب قانون رقم 06- 23 أين قام بتعديل نصوص القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أنه شدد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في نفس هذا القانون، وهذا نظرا لاستفحال هذه الظاهرة بشكل رهيب في المجتمع الجزائري.

تطرق المشرع الجزائري في القانون رقم 09-04 [2] والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حول تنظيم مثل هذه الجرائم، فقد تبنى المشرع الجزائري من خلال هذا القانون تعريفا موسعا للجرائم الالكترونية، فبالإضافة إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر7، أضاف عبارة أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظم للاتصالات الالكترونية، وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء، بل توسع نطاقها لتشمل إضافة إلى ذلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها، فقد

[1] ـ محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مرجع سابق، ص.7.

[2] ـ القانون رقم 09-04 المؤرخ في 14شعبان عام 1430 الموافق 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جريدة رسمية العدد 47، صادر في 16 أوت 2009.

كانت الجريمة الالكترونية قبل صدور القانون 09- 04 تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، وفقا لدلالة الكلمة فهي تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات.

نخلص مما سبق عدم بأنه لا يوجد تعريف متفق عليه لهذه الجريمة وعدم وجود اصطلاح قانوني موحد يطلق عليها، لأن هذه الجريمة هي في الأساس ناشئة أساسا من التقدم التكنولوجي والتطورات التي تؤثر عليها بصفة دائمة ومستمرة.

يمكن من خلال التعريفات السابقة أن نقدم تعريفا للجريمة الالكترونية بأنها كل سلوك يخالف القوانين الجزائية، و يؤدي إلى حدوث جريمة تقنية، وكل نشاط غير مشروع موجه للنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسب الآلي، أو التي يتم من خلاله تبادل البيانات، أو أية وسيلة إلكترونية أخرى.

يركز هذا التعريف على الأفعال المتعلقة بالتلاعب بمضمون المحررات الالكترونية والوصول إليها بطريقة غير مشروعة، وهذا التعريف هو الأنسب والأهم في إطار دراستنا للجرائم الماسة بالمحررات الالكترونية.

الفرع الثاني
خصائص الجريمة الإلكترونية

تعتبر الجريمة الالكترونية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات والحاسب الآلي، والتي أتى بها التطور الحاصل لها في هذا المجال فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي، لذلك فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية حديثة لم يشهدها العالم من قبل، فهي جرائم ذات بعد عالمي (أولا)، جرائم مستحدثة (ثانيا)، صعوبة اكتشاف وإثبات الجريمة الالكترونية (ثالثا)، جريمة أداتها الرئيسية الحاسب الآلي والمعرفة التقنية به (رابعا)، بالإضافة إلى تميز محلها عن محل الجريمة التقليدية (خامسا)، بالتالي سنحاول أن نبين أهم هذه الخصائص التي ميزت هذا النوع المستحدث من الجرائم بشيء من التفصيل على النحو التالي:

أولا: الجرائم الالكترونية هي جرائم ذات بعد عالمي

تعتبر الجريمة الالكترونية من نوع الجرائم التي يتم ارتكابها عبر المسافات حيث لا يتواجد الفاعل على مسرح الجريمة، فلم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين، ويقبل على التنفيذ في بلد آخر، ويهرب إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة[1]، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء[2].

تعد الجريمة عالمية إذا وقعت أحداثها في أكثر من دولة، والجريمة الالكترونية باعتبارها من مخرجات التطور التكنولوجي المذهل في وسائل الاتصالات، تجاوزت الحدود الجغرافية والسياسية للدول إلى مجتمع افتراضي بحيث أسهمت الطبيعة المتفردة للشبكة الدولية للمعلومات

[1]- فتوح عبد الله الشاذلي، المواجهة التشريعية للجرائم المستحدثة، بحث مقدم لمؤتمر الأمن والسلامة، المنعقد من طرف وزارة الداخلية بدولة الإمارات العربية المتحدة، أبو ظبي، الفترة من 5إلى 8 أكتوبر 2003، ص.1.

[2] - خالد ممدوح إبراهيم، التقاضي الالكتروني، مرجع سابق، ص.323.

في خلق ما يسمى بالمجتمع المعلوماتي[1]، فهذا المجتمع غير مقيد لا بالحدود الجغرافية ولا المادية التي تعارف عليها مجتمعنا المادي، وهذه الطبيعة التي تتميز بها الجريمة الالكترونية[2]، كونها جريمة عابرة للحدود أثارت العديد من المشاكل القانونية حول تحديد الدولة صاحبة الاختصاص القضائي فيما يخص هذه الجريمة، وغيرها من الجرائم العابرة للحدود بشكل عام، الأمر الذي يكشف عن الحاجة الملحة إلى التعاون الدولي في مجال مكافحة هذه الجرائم وضبط مرتكبيها والحد من أضراره[3].

ثانيا: جرائم مستحدثة

ظهرت الجريمة الالكترونية وذلك تبعا للتطور الهائل في مجال تكنولوجيا المعلومات، وهو ما يجعل أمر تحديد هذا النوع من الجرائم ضمن طائفة الجرائم التقليدية المعروفة والتي يكتنفها صعوبات ترجع إلى الطبيعة الخاصة بها باعتبارها تطال المعلومات، فهي إذن تعد من أبرز أنواع الجرائم الحديثة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعد الجرائم الالكترونية سواء التي تتعرض لها أجهزة الكمبيوتر، أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحثة[4]، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.

[1]- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم الانترنت، أطروحة دكتوراه، كلية الحقوق، الجامعة الإسلامية، لبنان، 2004، ص.140.

[2] - رانيا صبحي محمد عزب، العقود الرقمية في قانون الانترنت، دار الجامعة العربية ، مصر، 2012، ص.28.

[3]- محمد عبد الله محمد العوا، المسئولية الجنائية الناشئة عن جرائم الأموال عبر الانترنت، أطروحة دكتوراه، جامعة الإسكندرية، مصر، 2012، ص.24.

[4] - خالد ممدوح إبراهيم، الجرائم المعلوماتية ، مرجع سابق، ص.86.

ثالثا: صعوبة اكتشاف وإثبات الجريمة الالكترونية

يعتبر أهم ما تتميز به الجريمة الالكترونية في أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا ما قورنت بما يتم اكتشافه من الجرائم التقليدية[1]، وتعود الأسباب التي تقف وراء الصعوبة في اكتشافها إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، سيما أن قدرة الجاني على تدمير الدليل يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم[2]، كما أن تغيير في بيانات الحاسب الآلي أو الاحتيال المعلوماتي وغيرها من الجرائم الماسة بالمحررات الالكترونية يتم بواسطة إدخال رموز وأرقام، وهي أمور تقنية تتسم بتعقيدها وصعوبة اكتشافها أو إثباتها، وهي لا تستغرق إلى ثواني معدودة يتم فيها محو الدليل والتلاعب به[3] أو تشويهها أو تعطيل الأنظمة التي تحتويها[4].

رابعا: جريمة أداتها الرئيسية الحاسب الآلي والمعرفة التقنية به

تعتبر الجرائم المعلوماتية بأنها جرائم تحتاج إلى دقة عالية ومعرفة فنية تخصصية ودقيقة، لهذا فإن المجرم المعلوماتي يجب أن يكون على معرفة فنية علمية بجهاز الحاسب الآلي، وكيفية التعامل مع هذه النظم حتى يتمكن من إتمام جريمته، بالمقابل فإن المجرم العادي في الجرائم التقليدية غالبا ما يتميز بالقوة العضلية ونادرا ما يتميز بعضهم بعنصر الذكاء[5] وعدم الاختصاص في الجرائم التي يرتكبونها.

خامسا: بالنسبة لمحل الجريمة

استتبع التغيير الذي حدث في مفهوم محل الجرائم من المفهوم المادي إلى المفهوم المعنوي وغير المادي، بحيث تغيرت معه طريقة وقوع النشاط الإجرامي فهو يرتبط بموضوع الجريمة

[1] ـ محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور المعاملات المدنية، دبي، الإمارات العربية المتحدة، المجلد الثاني، 26- 28 أفريل2003، ص.361.

[2] ـ هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، مرجع سابق، ص.22.

[3] ـ جميل عبد الباقي صغير، مرجع سابق، ص.17.

[4] ـ محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان ، 2004، ص.165.

[5] ـ هدى حامد قشوش، جرائم الحاسب الآلي، مرجع سابق، ص.27.

وينصب عليه، فصار له مفهوم آخر يتفق مع تلك الطبيعة غير المادية للمحل الذي يرد عليه، إلى حيازة المجني عليه إلى حيازة الجاني، تحول في مجال الجريمة الالكترونية إلى حيازة المال فقط دون أن يترتب عليه منع حيازة المجني عليه إلى احتيال يقع على ما يمكن أن يسمى بالعقل الالكتروني أو النظام المعلوماتي، فيسلم للجاني هذا المال[1].

المطلب الثاني

المجرم المعلوماتي

يعتبر المجرم المعلوماتي هو ذلك المجرم الذي يخرج عن القواعد التي تحدد العلاقات والحقوق والواجبات السارية في المجتمع، وهذا من خلال انتهاك حقوق الآخرين ومنح نفسه حق التعدي على معلوماتهم وأموالهم وخصوصياتهم، من خلال اختراق نظم معلوماتهم ومحاولة استغلال تعاملاتهم لصالحه.

لم تعد الجريمة الالكترونية تقتصر على سرقة المعلومات والبيانات أو محتوى المحرر الالكتروني والتعدي عليها، بل اكتسبت منحى آخر، وبالتالي ظهرت جرائم أخرى كالنصب والتحايل والتزوير التي يرتكبها المجرم المعلوماتي، والذي لم يعد إجرامه يقتصر على المعلومات والبيانات بل تعدى إلى سرقة الأموال وتحويلها لحسابه الخاص، أو الشراء عن طريق استخدام بطاقات الائتمان الخاصة بالآخرين وأرقامهم السرية وكذلك تزوير المحررات الالكترونية والتوقيع الالكتروني على معاملات الآخرين وأرقامهم السرية.[2]

يطلق أغلب الخبراء في مجال التقنية والأنظمة المعلوماتية على أمن المعلومات[3] والبيانات الرقمية مصطلح هاكرز،[1] وهو الشخص الذي يقوم بعمليات الاختراق والتخريب عبر شبكة

[1] ـ أيمن عبد الله فكري، الجرائم الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2014، ص.10.

[2] ـ عبد الله بن مسعود محمد السراني، مرجع سابق، ص.41.

[3] ـ يقصد بأمن المعلومات من زاوية أكاديمية بأنه النظام الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، واستخدم اصطلاح أمن المعلومات وإن كان استخداما قديما سابقا لظهور وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال ن تعتمد المعاملات الالكترونية

الانترنت، ويكون غالبا من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الالكترونية والحاسب الآلي، كما أطلقت التسمية على المتخصصين بفك شفرات البرامج بالكراكرز[2]، وليس تخريب الشبكات فهو نوع من الهاكرز المتخصص في العلوم الإلكترونية، ويعتبر هذا النوع من أكثر الأنواع التي يلجأ إليها مرتكبي الجرائم الالكترونية.

يعرف المجرم المعلوماتي الرقمي بأنه الشخص الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها، باستخدام الحاسوب الرقمي وملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابا في المجتمع الدولي أو المحلي نتيجة لمخالفة الضبط الاجتماعي محليا ودوليا[3].

يعتبر المجرم المعلوماتي هو محور ارتكاب الجريمة في المجال المعلوماتي عامة وفي ارتكاب جرائم المحررات الالكترونية بصفة خاصة، نظرا أن التعامل مع هذا النوع يستدعي درجة علمية وتخصص في التكنولوجيا الحديثة للقيام بارتكاب الجريمة، وعليه فإن المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم في الجرائم التقليدية وذلك من عدة جوانب، فسنتناول سمات المجرم المعلوماتي **(الفرع الأول)**، لنتناول بعد ذلك الدوافع المحفزة في ارتكاب الجريمة الالكترونية **(الفرع الثاني)**.

بصفة أساسية على تكنولوجيا التبادل الالكتروني للبيانات، والتي يقصد بها تبادل البيانات المتعلقة بالأعمال التجارية في أشكال نمطية بين أجهزة الكمبيوتر للأطراف المتعاملة من خلال شبكة اتصالات إلكترونية دون حاجة لاستخدام مستندات ورقية، للمزيد راجع في ذلك: خالد ممدوح إبراهيم، أمن المعلومات الالكترونية، مرجع سابق، ص.31.

[1]- الهاكرز يطلق عليهم أيضا" **صغار نوابغ المعلوماتية**"، وهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج وتدابير الحامية التي تم اتخاذها إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من اختراق جهاز أو شبكته للمزيد راجع في ذلك: منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الالكترونية، مرجع سابق، ص.28.

[2]- نظرا لعدم وجود ترجمة لكلمة الهاكرز باللغة العربية حتى الآن نستخدم الكلمة كما هي ، وإن كان مصطلح " مخترقو أمن الشبكات" هو اقرب تفسير للمعاني ويطلق عليه أيضا اصطلاح المجرم الرقمي، للمزيد راجع في ذلك: خالد ممدوح إبراهيم، جرائم المعلوماتية، مرجع سابق، ص.26.

[3]- المرجع نفسه، ص.26.

الفرع الأول

من حيث شخصية المجرم المعلوماتي

يختلف المجرم في الجرائم التقليدية عن المجرم المعلوماتي من حيث أن هذا الأخير يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات، فهو يسعى بشغف إلى معرفة الطرق الجديدة المبتكرة والتي لا يعرفها أحد سواه من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ومن ثم نيل ما يصبو إليه، فمن بين أهم السمات التي تتعلق بشخصية المجرم المعلوماتي هي أن المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء (أولا)، المجرم المعلوماتي إنسان اجتماعي (ثانيا)، المجرم المعلوماتي يبرر ارتكاب جريمته (ثالثا)، تمتع المجرم المعلوماتي بالحقوق والمزايا تمكنه من ارتكاب جريمته (رابعا)، خوف المجرم من كشف جريمته (خامسا)، المجرم المعلوماتي مجرم عائد إلى الإجرام (سادسا)، وسنتعرض لها بشيء من التفصيل على النحو التالي:

أولا: المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء

يتمتع مجرمي المعلوماتية بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والانترنت، بل أن بعضهم متخصصين في مجال معالجة المعلومات[1] آليا، كما يتميز غالبا بالذكاء[2]، فالذكاء يعتبر من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج، وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكي يتمكن من ارتكاب تلك الجرائم[3]، حيث أن هذا النوع

[1] ـ عرف البعض المعلومة بأنها:" ***كل رسالة يمكن نقلها إلى الغير بأية وسيلة كانت*** " وسبب وجود المعلومة هو قابليتها للنقل للغير، وتتكون المعلومة من عنصرين وهما الصياغة والنقل، وتنقسم إلى ثلاث طوائف، الطائفة الأولى: المعلومات الاسمية، و الطائفة الثانية المعلومات المتمثلة في مصنفات فكرية، والطائفة الثالثة المعلومات الشاغرة، للمزيد راجع في ذلك: محمد حسام الدين لطفي، الإطار القانوني للمعاملات الإلكترونية، دراسة في قواعد الإثبات في المواد المدنية والتجارية، دار النهضة العربية، القاهرة، 2002، ص.54. انظر كذلك: خالد ممدوح إبراهيم، أمن التوقيع الالكتروني، مرجع سابق، ص.31

[2] ـ محمد سامي الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، مرجع سابق، ص.34.

[3] ـ أيمن عبد الحفيظ، مرجع سابق، ص.13.

من الإجرام، يحتاج إلى مقدرة عقلية وذهنية عميقة، فهو يستخدم مقدرته العقلية ولا يلجأ إلى العنف أو الإتلاف المادي، بل يحاول أن يحقق أهدافه بهدوء، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة مع الإجرام العادي الذي يميل إلى العنف.

تكمن أيضا مهارة المجرم المعلوماتي في مدى مواظبته على تحقيق أهدافه، فاختراق أنظمة المعلومات والإنترنت محل الجريمة قد يستغرق في بعض الأحيان شهورا طويلة من أجل بلوغ غايته.

ثانيا: المجرم المعلوماتي إنسان اجتماعي

يعتبر المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية، بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله[1]، فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عداء مع المجتمع الذي يحيطه، بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه، فهو إنسان تزداد خطورته الإجرامية إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[2].

ثالثا: المجرم المعلوماتي يبرر ارتكاب جريمته

يعني ذلك أن المجرم المعلوماتي لا يدرك أن سلوكه يستحق العقاب، وقد ساعد على ذلك عدم وجود احتكاك مباشر بالمجني عليه، وهو ما يسهل ارتكابهم للجريمة المعلوماتية دون الإحساس بعدم مشروعية أفعالهم.

رابعا: تمتع المجرم المعلوماتي بالحقوق والمزايا التي تمكنه من ارتكاب جريمته

تكون لدى غالبية مجرمي المعلوماتية سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، فالسلطة هي الحق في استعمال الأنظمة المعلوماتية أو حتى مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة، وتتمثل هذه السلطة مثلا في الشفرة الخاصة بالدخول أو

[1] ـ نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص.79.

[2] ـ محمد أمين الرومي، جرائم الكمبيوتر والانترنت، مرجع سابق، ص.23.

الولوج إلى النظام الذي يحتوي على المعلومات، وهذه الشفرة تعطي للمجرم المعلوماتي مزايا متعددة تمكنه مثلا من فتح الملفات وقراءتها أو كتابتها أو محو المعلومات و تعديلها[1]، أو أي فعل آخر مجرم.

خامسا : خوف المجرم من كشف جريمته

يتصف مرتكبو هذه الفئة من الجرائم بالخوف من كشف جرائمهم وافتضاح أمرهم ، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم، إلا أنها تميز مجرمي هذه الفئة من الجرائم بصفة لما يترتب على كشف أمرهم من ارتباك مالي، وفقد المركز الوظيفي في كثير من الأحيان، وهذا الخوف لديهم مرده انتمائهم في الغالب الأعم إلى وسط اجتماعي متميز سواء من حيث التعليم أو الثقة أو المستوى المهني وطبيعة العمل[2].

سادسا : المجرم المعلوماتي مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلوماتية إلى ارتكاب جرائم أخرى في مجال الحاسوب، انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام وقد ينتهي بهم الأمر كذلك في المرة التالية تقديمهم إلى المحاكمة من جديد[3].

تتكون هذه النزعة الإجرامية المتوفرة في المجرم المعلوماتي لتأثره بعوامل نفسية صاحبت نشأته، ومع اقتران تلك العوامل بعنصر آخر جديد يساعد على استثارة الحالة الإجرامية ويزيد من قدرة عوامل الإجرام وتفوقها على موانع الإقدام، وهذا العنصر هو الذي أكسب الشخص للمهارة العلمية والتكنولوجية[4].

[1] ـ نهلا عبد القادر المومني، مرجع سابق، ص.87.

[2] ـ المرجع نفسه، ص.79.

[3] ـ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص.83. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومات، منشورات زين الحقوقية ، لبنان، 2013، ص.107.

[4] ـ خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص.135.

الفرع الثاني

من حيث الدوافع المحفزة في ارتكاب الجريمة الالكترونية

يسعى المجرم المعلوماتي كذلك في بعض الأحيان إلى ارتكاب الكثير من الجرائم الالكترونية بدافع الكبرياء، أو الرد على تعرضه للفصل من العمل أو الاستغناء عن خدماته تارة، أو بدافع الحصول على منفعة مالية تارة أخرى، وعليه يمكن تقسيم هذه الدوافع إلى دوافع مادية **(أولا)**، ثم دوافع خارجية كالانتقام من رب العمل وإلحاق الضرر به، ودافع التعاون والتواطؤ على إحداث الأضرار **(ثانيا)**.

أولا: الدوافع المادية

يمكن رد الدوافع والأسباب لارتكاب المجرم المعلوماتي للجريمة الالكترونية إلى دوافع مادية وهذا سعيا منه للحصول على الأموال التي تحقق له الربح[1]، كالاحتيال المعلوماتي الذي يعتبر أكثر انتشارا واستعمالا في الجرائم الالكترونية عامة وجرائم المحررات الالكترونية بصفة خاصة، فأنظمة التمويل الالكتروني التي تقوم بها البنوك لا يتطلب ذلك سوى الحصول على الرموز والأرقام السرية التي تمكن المجرم المعلوماتي من القيام بهذا التحويل، دون ترك في بعض الحالات أي أثر مادي ملموس[2].

ثانيا : الدوافع الخارجية لارتكاب الإجرام المعلوماتي:

تكون هذه الدوافع الغرض منها ليس ماديا وإنما هناك عوامل خارجية أثرت عليه لاقتراف الجريمة المعلوماتية، فمن بين أهم هذه الدوافع:

1 ـ دافع التعاون والتواطؤ على إحداث الأضرار:

ترتكب هذه الجرائم في أغلب الأحيان من متخصص في الأنظمة المعلوماتية، يقوم الجانب الفني من المشروع الإجرامي وشخص أخر من المحيط أو خارج المؤسسة المجني عليها

[1] ـ أيمن عبد الله فكري، جرائم نظم المعلومات، مرجع سابق، ص.67.

[2] - Abbas JABER, Les infractions commises sur Internet, L'Harmattan, Paris,2009, p.30.

لتغطية عملية التلاعب وتحويل المكاسب المالية إليه، وقد اعتاد المتلصصون على الأنظمة المعلوماتية والحواسيب على تبادل المعلومات بصفة منتظمة حول أنشطتهم[1].

2 ـ الانتقام من رب العمل وإلحاق الضرر به:

يدفع في كثير من الأحيان المجرم المعلوماتي إلى ارتكاب جريمته الانتقام من رب العمل الذي طرده من عمله، أو بدافع إظهار قدرته على اختراق الأجهزة والمواقع[2].

[1] ـ محمد عبد الله أبو بكر سلامة، مرجع سابق، ص.95.

[2] ـ محمد علي العريان، مرجع سابق، ص.77.

المبحث الثاني

الجرائم الماسة بأمن وسلامة المحررات الالكترونية

يشترط لإضفاء الحماية الجنائية على المحررات الالكترونية أن تكون عبارة عن معلومات ذات قيمة مالية، حيث أن هذه المعلومات هي عبارة عن تغيير وصياغة مخصصة لتبليغ رسالة أو بيانات عبر وسائل الاتصال الحديثة التي تكون قابلة للتنقل إلى الغير، والأهم أن تكون المعلومات مبتكرة وسرية، وألا تكون عامة حيث أنه في الحالة الأخيرة لا نكون أمام سرقة، فسرية المعلومات تدعوا إلى الحماية الجنائية، حيث أن سرية المعلومات وإفشائها من طرف الغير يعتبر هذا اعتداء على الحيازة في حد ذاتها[1]، فهناك العديد من الجرائم التي يمكن أن تقع أو تمس بالمحرر الالكتروني، بالتالي سنتناول أولا الجرائم المتعلقة بالمحررات الالكترونية في إطار النصوص التقليدية والتي تتمثل في كل من جريمة التزوير في المحررات الالكترونية، جريمة النصب في مجال المحررات الإلكترونية، جريمة سرقة المحرر الالكتروني **(المطلب الأول)**، ثم سنتناول الجرائم المستحدثة المتعلقة بالمحررات الإلكترونية في كل من جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة الإتلاف في مجال المحررات الإلكترونية **(المطلب الثاني)**، وهذا ما سنوضحه على النحو التالي :

[1] محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.112.

المطلب الأول

الجرائم المتعلقة بالمحررات الالكترونية في إطار النصوص التقليدية

يتم المساس بمحتوى المحرر الالكتروني وتغييره في أي وقت ولا يتسنى كشفه أو الوقوف عليه أو إقامة الدليل على وقوعه، ومن ناحية أخرى فإن عددا كثيرا من الأفراد يجوز لهم الاطلاع على المحررات الالكترونية والتعامل معها يفوق بكثير المتعاملين في المحررات الالكترونية، كما أن المساس بمحتوى المحرر الالكتروني يبدوا أكثر سهولة من المساس بالمحرر العادي[1]، تتمثل الجرائم الواقعة على المحررات الإلكترونية أساسا في طرق ضبطها وإثباتها، وذلك أنها ترتكب في مسرح خاص داخل عالم افتراضي يختلف كليا عن المسرح الذي ترتكب فيه هذه الجرائم في صورتها التقليدية، وذلك يرجع إلى افتقار الآثار التقليدية التي قد تتركها الجرائم الماسة بالمحررات الإلكترونية، فالبيانات يتم إدخالها مباشرة في الجهاز دون أن تتوقف على وجود محررات ورقية، لأنه غالبا ما تكون هناك برامج معدة ومخزنة داخل النظام المعلوماتي، وذلك عن طريق إدخال البيانات في الأماكن المعدة سلفا لذلك، وعليه يستدعي ذلك ضرورة تحديث التشريعات العقابية لتتلاءم مع خصوصية جريمة التزوير وجريمة السرقة والنصب في مجال المحررات الإلكترونية، لأن القوانين التقليدية تظهر قاصرة عن تغطية هذه الجرائم رغم إمكانية تطبيق القواعد التقليدية عليها، ولو على وجه من الصعوبة والتعقيد، وعلى هذا الأساس سنتعرض لجريمة تزوير المحررات الإلكترونية **(الفرع الأول)**، جريمة النصب في مجال المحررات الإلكترونية **(الفرع الثاني)**، ثم جريمة السرقة في مجال المحررات الإلكترونية **(الفرع الثالث)**.

[1] - أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.26.

الفرع الأول

جريمة تزوير المحررات الالكترونية

تعتبر جريمة التزوير في المحررات الالكترونية من أخطر أنواع الجرائم التي يشهدها عصرنا الحالي، فآثارها لا تقتصر على فرد معين أو مؤسسة أو على الدولة الواحدة وإنما تتجاوز الحدود الإقليمية لها، فمثلا جريمة تزوير التوقيع التقليدي تختلف عن جريمة تزوير التوقيع الالكتروني سواء في طريقة التزوير أو في أسلوب اكتشاف هذا التزوير، فطريقة الكشف عن التوقيع التقليدي المزور تكون عن طريق مضاهاة التوقيع المزيف بتوقيع الشخص المنسوب إليه هذا التوقيع، بينما في حالة تزوير التوقيع الالكتروني لا يمكن استخدام تلك الطريقة لاكتشاف تزوير التوقيع، إذ أن التوقيع سليم لكنه ليس صادرا من الشخص مالك منظومة التوقيع الالكتروني[1].

يكون تزوير البيانات بالدخول بطريقة مشروعة أو غير مشروعة على قاعدة البيانات الموجودة في نظم المعلومات وتعديل البيانات، سواء بإلغاء بيانات موجودة بالفعل، أو بإضافة بيانات لم تكن موجودة من قبل[2]، أو عن طريق التلاعب في معلومات ذات قيمة في ترتيب حق معين، فمن السهل تزوير مخرجات الحاسب الآلي المتضمن هذه المعلومات، سواء كانت تمثل أثرا إداريا أو قانونيا، ومن السهل إدخال صورة توقيع أي شخص أو بصمته، أو صورة ختمه عن طريق الماسح الضوئي إلى جهاز الحاسب الآلي، مع إضافة التوقيع إلى المحرر الذي يحتوي على البيانات المزورة، وهنا تتحقق أركان جريمة التزوير بعد كتابة البيانات وتوقيعها أو ختمها أو طبع البصمة الشخصية عليها دون انصراف إرادة صاحبها، أي نسبتها إليه دون علمه.[3]

يعتبر التزوير الذي يمس المحررات الالكترونية أبسط وأسهل بكثير من التزوير في المحررات العادية أو الورقية، لأنه لا يحتاج إلى إزالته باستخدام الأدوات والمواد الكيميائية

[1] ـ منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، مرجع سابق، ص.54.

[2] ـ نائلة عادل محمد فريد قورة، مرجع سابق، ص.98.

[3] ـ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.184.

لتغيير معاني الكلمات أو كشط توقيعات سابقة، لكنه يحتاج فقط إلى إدخال كلمات أو تغيير معاني كلمات بالحذف أو الإضافة أو التعديل عليها[1]، وبذلك يصدر المحرر النهائي مطابقا للأصل وإن كان مزورا في مضمونه، وعلى هذا الأساس سنتعرض إلى تعريف جريمة التزوير في المحررات الإلكترونية **(أولا)**، ثم إلى أركان جريمة تزوير المحررات الإلكترونية **(ثانيا).**

أولا : تعريف جريمة تزوير المحررات الالكترونية

اختلف الفقهاء ورجال القانون في وضع تعريف جامع مانع لجريمة تزوير المحررات الالكترونية وذلك لأنه من الصعب وضع تعريف محدد لها، لكونها تتعلق بتكنولوجيا تتطور باستمرار ولا تقف عند حد معين، فتنوع واختلاف وسائل التزوير وتجدد أشكاله جعل أغلب الفقهاء لم يتفقوا على وضع تعريف له، بحجة أن التزوير في هذا النوع من الجرائم ما هو إلا تزوير تقليدي يرتكب بأسلوب إلكتروني، بالتالي سنستعرض أهم آراء الفقه التي حاولت سد الفراغ التشريعي ووضع تعريف محدد لجريمة تزوير المحررات الالكترونية، وقد ارتأينا إلى أن نتطرق إلى التعريف الفقهي لها أولا، ثم التعريف القانوني لها ثانيا، وذلك على النحو التالي:

1- التعريف الفقهي لجريمة تزوير المحررات الالكترونية:

عرف الفقه جريمة تزوير المحررات الالكترونية في الفقه بأنها: **" تغيير للحقيقة الذي يرد على المحررات الالكترونية المستخرجة من الحاسب الآلي، سواء كانت هذه المحررات على هيئة أوراق مكتوبة، أو شرائط ممغنطة مسجل عليها المعلومات"**[2]، واختلف الفقه والقضاء حول مدى جواز تطبيق النصوص المقررة على الأفعال التي تشكل تغييرا للحقيقة في البيانات المخزونة إلكترونيا في الحاسبات الآلية، والتي يتحقق بها الركن المادي لجريمة التزوير المعلوماتي[3].

[1] - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.189.

[2] - مشار إليه لدى: محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، 2006، ص.179

[3] - داديار حميد سلمان، دور السندات المستخرجة عن طريق الإنترنت لإثبات المسائل المدنية،رسالة ماجستير، كلية القانون، جامعة صلاح الدين،2005، ص.146.

عرف البعض الآخر جريمة تزوير المحررات الالكترونية بأنها:" **تغيير البيانات والمعلومات في المحررات المعالجة آليا باستخدام أجهزة وبرمجيات اختراق، وتعد للحصول على محررات تحاكي الأصل، ولكن مزورة في مضمونها وصيغتها، بنية استخدامها في تحقيق مصلحة لمرتكب التزوير أو لشخص آخر**"[1].

تتمثل خطورة التزوير المعلوماتي بأن هذا التزوير يتجاوز التزوير الورقي المعروف بالأدلة الكتابية الخطية، وإن كان هذا التزوير يتحد معه في المفهوم الوظيفي بالنسبة إلى تحريف الحقائق أو البيانات، غير أنه في الجانب التقني، لا يقتصر فقط على معالجة الدعامة الورقية الملموسة والمقروءة، بل يتطلب التعامل مع تقنيات المعلوماتية والشرائح الإلكترونية أو المكملة لها، مما يصعب إمكانية كشفه من قبل القضاة غير المختصين أساسا بهذه التقنيات[2]، فهو تغيير لحقيقة في محرر وذلك عن قصد وبإحدى الطرق المنصوص عليها قانونا، ويترتب عن ذلك ضرر حال أو محتمل للغير، فتغيير الحقيقة في المحرر هو الأساس الذي تقوم عليه جريمة التزوير وهو يعني استبدال الحقيقة بما يخالفها، وإذا انتفى هذا العنصر فلا تقوم جريمة التزوير، كأن يقوم احدهم بإثبات بيانات مطابقة للحقيقة فلا تقوم جريمة التزوير حتى لو كان ذلك الشخص يعتقد بعدم صحة البيانات حتى لو ترتب على صحة فعله ضرر في حق الغير[3].

نخلص مما تقدم أنه ونظرا لضيق نطاق النصوص المقررة في قانون العقوبات، فإنه من الضروري تعديل أحكام هذا القانون بشكل يستوعب جريمة التزوير المعلوماتي وذلك لتوفير الحماية القانونية للمحررات الالكترونية، وأيا كان شكلها، لا سيما بعد أن تزايد الاعتماد على هذه المحررات في معاملات الأفراد، وعمدت العديد من التشريعات إلى تجريم هذا النوع المستحدث من التزوير في القوانين الجنائية وفقا لنصوص خاصة نظمتها هذه التشريعات.

[1] ـ مشار إليه لدى: عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص.23.

[2] ـ وسيم شفيق الحجار، الإثبات الإلكتروني، منشورات الحلبي الحقوقية، لبنان، 2001، ص.144.

[3] ـ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.137.

2 ـ موقف التشريعات المقارنة من جرائم التزوير في المحررات الالكترونية

يعتبر التزوير الالكتروني بصفة عامة تزوير المستندات والبيانات الموجودة على جهاز الكمبيوتر وتزوير المعلومات والمحررات، بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية، وكمظهر من مظاهر التزوير باستخدام تقنية المعلومات والاتصالات ظهرت جرائم المحررات الالكترونية التي تختلف طبيعتها ومضمونها عن جرائم المحررات الورقية، مما جعل النظم والقوانين الحالية غير كافية لمواجهة هذا النوع من الجرائم سواء في مجال التجريم أو العقاب، مما استدعى بعض الدول إدخال في تشريعاتها مثل هذه الأنماط من الجرائم في مواجهة ومكافحة هذا النوع من السلوك الإجرامي في تقنية المعلومات، فمن بين التشريعات المقارنة في تجريم تزوير المحرر الإلكتروني:

أ ـ القانون الفرنسي:

ذهب الشارع الفرنسي إلى تجريم تزوير المحررات الالكترونية بنصوص عامة في قانون العقوبات فيما يلي:

يرجع تجريم التزوير في المحررات الالكترونية إلى ما تقدم به أحد نواب البرلمان الفرنسي في 5 أوت سنة 1986، من اقتراح يرمي إلى إدخال بعض التعديلات على جريمة التزوير في المحررات المنصوص عليها في قانون العقوبات، لتشمل أيضا تغيير الحقيقة في البيانات الإلكترونية، غير أن هذا الاقتراح لم يؤخذ به، ورأى مجلس الشيوخ اعتبار تزوير المحررات الالكترونية جريمة مستقلة عن جريمة التزوير في المحررات، وقد صدر القانون رقم 88-19 الذي صدر في 5 يناير 1988 الذي انطوى على تجريم صورتين: الأولى هي تزوير المحررات المعالجة آليا أيا كان شكلها إذا كان من شأنها الإضرار بالغير (المادة 462-5) والصورة الثانية فهي الخاصة باستعمال المحررات المزورة سالفة الذكر(462-6)[1].

[1] - عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية، القاهرة، 1995، ص79. طارق سرور، ذاتية جرائم الإعلان الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص.84. أيمن عبد الله فكري، مرجع سابق، ص.484

ألغى بعد ذلك المشرع الفرنسي نص المادتين السالفتين الذكر، وأخذ باقتراح تعديل نص جريمة التزوير الأصلية ليستوعب أيضا المحررات الإلكترونية، فلم يعد يقصر التزوير على المحررات الورقية بل يشمل جميع المحررات حتى الالكترونية، وبأي وسيلة مادية أو معنوية[1] ويظهر ذلك بتعديله لقانون العقوبات بموجب القانون رقم 92-1335 المؤرخ في 16-03-1994حيث نص في المادة 441-1 منه على تعريف جريمة التزوير على النحو التالي: **" التزوير هو كل تغيير بطريق الغش في الحقيقة ويكون من شأنه إحداث ضرر ويرتكب بأي طريقة كانت، سواء أكان ذلك بالكتابة أو بأي سند أخر للتعبير عن الفكر والذي يكون الغرض منه أو كنتيجة له شأنا في إثبات حق أو واقعة لها أثار قانونية"**[2]، والصياغة الجديدة لنص المادة 441-1 سالفة الذكر تسمح باستيعاب النص لكل صور التعبير عن الفكر والتي تكون في شكل إلكتروني، بل وحتى تلك التي يتوصل إليها لا علم بعد، متى كان لها شأن في إثبات حق أو واقعة لها نتائج قانونية، كما أن الشارع الفرنسي بهذا النص لم يقصر طرق التغيير في الحقيقة على طرق معينة محددة على سبيل الحصر، وإنما أطلق النص من أي قيد يحدد كيفية وقوع التزوير[3]، لكن مع شرط إمكانية استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف وأن يصلح لإثبات حق أو تصرف له آثار قانونية[4]، كما أنه من خلال نص المادة توسع في مفهوم المحرر الذي يقع عليه التزوير حيث أصبحت تشمل إلى جانب المحرر بشكله التقليدي كل وسيط آخر للتعبير عن فكرة، ويشمل ذلك بطبيعة الحال الأقراص الممغنطة والاسطوانات المدمجة وغيرها من وسائط تخزين المعلومات، أو يمكن أن ينتج عنها دليل على حق أو واقعة ذات آثار قانونية[5].

---

[1] - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.164.

[2] - Article 441-1du C.P.F dispose que : « ***Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques*** », Modifié par Ordonnance n°2000-916 du 19 septembre 2000 -art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 sur le site: https://www.legifrance.gouv.fr/

[3] - عمر فاروق الحسيني، مرجع سابق، ص.88.

[4] - إيهاب فوزي السقا، مرجع سابق، ص.56.

[5] - عبد الفتاح بيومي حجازي، التجارة الالكترونية، مرجع سابق، ص.165.

ينبغي التفرقة بين التزوير الذي يتم في تغيير البيانات المسجلة في ذاكرة الكمبيوتر ويترتب على معالجة هذه البيانات وإخراجها وطبعها، وجود مستند به معلومات غير مطابقة للحقيقة أو الواقع وبين التزوير الذي يحدث على المحرر ذاته[1].

اتجه القضاء الفرنسي إلى التفسير الموسع للمحررات الالكترونية، حيث قضت محكمة النقض الفرنسية بجواز التمسك بالنسخة المرسلة عبر الفاكس وبالتالي أقرت حجيتها في الإثبات، كما أصبحت تعاقب على أي تزوير في أي محررات لها قيمة في الإثبات قبل تدخل المشرع بنص صريح[2].

ب ـ القانون المصري:

اقتصرت بعض التشريعات على تجريم بعض صور تزوير المحررات الإلكترونية ومن بينها القانون المصري، إذ اقتصر الشارع المصري على تجريم تزوير السجلات والدفاتر الإلكترونية للأحوال المدنية[3]، ولم يضع نصوصا عامة تجرم تزوير البيانات والمحررات الإلكترونية، فجرم المشرع المصري تزوير السجلات الإلكترونية الخاصة بالأحوال المدنية، وسبق أن ذكرنا أن المشرع المصري قد ساوى في قانون الأحوال المدنية رقم 143 لسنة 1994 بين السجلات الورقية والإلكترونية في تطبيق أحكامه، وقد اعتبر المشرع المصري البيانات المسجلة بالحاسبات الآلية بمراكز الأحوال المدنية بيانات واردة في محررات رسمية، فنص في المادة 72 من القانون السابق على أنه: **" 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، ببيانات واردة في محررات رسمية، فإذا وقع التزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات."**[4]

[1] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.79.

[2] ـ أسامة محمد المناعسة وآخرون، جرائم الحاسب الآلي والانترنت، دار وائل، الأردن، 2001، ص.159.

[3] ـ شيما عبد الغني عطا الله، مرجع سابق، ص.38.

[4] ـ مشار إليه لدى: أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.28.

أوردت المادة 23 من قانون التوقيع الإلكتروني المصري صورا للتزوير الإلكتروني التي تكون محلا للمساءلة الجنائية، وبالتالي يمكن الإدعاء بها أمام القضاء، ويمكن إيجاز هذه الصور فيما يلي:

1- إتلاف أو تعييب المحرر أو التوقيع الإلكتروني أو الوسيط الالكتروني المستخدم في إنشائه.

2- اصطناع أو تعديل أو تحوير المحرر أو الوسيط الإلكتروني.

3- اختراق الوسيط الإلكتروني أو اعتراضه أو تعطيله عن أداء وظيفته.

4- التوصل بأية وسيلة إلى الحصول ـ بغير حق ـ على توقيع أو محرر أو وسيط إلكتروني.

5- وضع توقيع إلكتروني على محرر إلكتروني وإسناده إلى الشخص المحتج عليه بالمحرر دون أن يكون هذا التوقيع خاصا به.

6- وضع توقيع إلكتروني على محرر إلكتروني وإسناده إلى الشخص المحتج عليه بالمحرر دون أن يكون هذا التوقيع خاصا به.[1]

تختلف عقوبة تزوير المحرر الالكتروني في مصر بحسب نوع المحرر الالكتروني المزور، فالوضع يكون أشد إذا كان هذا التزوير متعلق بمحرر إلكتروني رسمي، بمعنى أي محرر تدخل في تحريره موظف عام، وتكون العقوبة أخف إذا كان المحرر الالكتروني الذي تم تزويره محرر إلكتروني عرفي، فالمساس بمحتوى المحرر الالكتروني وذلك عن طريق تزويره يكون أشد صعوبة من تزوير المحرر الورقي، وذلك لأن المحرر الالكتروني بمجرد التوقيع عليه الكترونيا يندمج مباشرة المحرر الالكتروني بالتوقيع الالكتروني ويصبحان كتلة واحدة مكونا للمحرر الالكتروني[2].

ج ـ القانون الأردني:

عرف المشرع الأردني في المادة 260 من قانون العقوبات التزوير بأنه: **" تحريف مفتعل للحقيقة في الوقائع و البيانات التي يراد إثباتها، بصك أو مخطوط يحتج به ما نجم أو يمكن**

[1] ـ المادة 23 من قانون رقم 15 لسنة 2004 المتعلق بالتوقيع الالكتروني وإنشاء هيئة تنمية تكنولوجيا المعلومات المصري.

[2] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.88.

أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"[1]، فالتغيير أو التحريف هنا يقع على مضمون السند سواء البيانات أو التوقيع، وقد يتمكن الشخص من تزوير محرر إلكتروني ما واستخدام حاسب المرسل وإرسال المحرر المزور إلى شخص أخر دون علم المرسل بالأمر مما يؤدي إلى إلحاق الضرر بمصالح الطرفين[2].

يتم التزوير إما بإضافة بيانات لم تكن موجودة أصلا أو بحذف بيانات ضرورية كانت موجودة، أو تغيير وتبديل بعض البيانات وذلك بحذف بيان وإضافة آخر بدلا منه، وطالما أن المحرر الإلكتروني يتضمن كتابة وفق ما أسلفنا فإن من الممكن أن يتعرض للتزوير، بل أن أكثر ما تتعرض له المحررات الالكترونية هو التزوير وذلك لسهولة القيام به، فكما نعلم فإن البيانات المثبتة على القرص داخل جهاز الحاسب، وبكبسة زر يستطيع العابث أن يغير ويبدل في المحرر الإلكتروني وإضافة أو حذف بيانات لم تكن موجودة.

يمكن من احتج عليه بمحرر إلكتروني مزور اللجوء للمدعي العام و إقامة دعوى جزائية بالتزوير بأوراق خاصة أو رسمية، وعند ذلك يتوجب على قاضي الموضوع وقف النظر في الدعوى الحقوقية إلى حين البث في دعوى التزوير الجزائية، وذلك كون نتيجة الفصل في الدعوى الحقوقية تتوقف على نتيجة الفصل في الدعوى الجزائية[3].

د ـ موقف المشرع الجزائري:

أخذ المشرع الجزائري بنفس التعريف الذي قدمه المشرع الفرنسي إلا أنه بالمقابل لم يشر إلى التزوير على الدعائم الحديثة لتلقي البيانات التي لا يشملها القانون الجزائري، ربما إقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير،

[1]ـ استعمل المشرع الأردني مصطلح تحريف مفتعل للحقيقة، بينما استخدمت التشريعات الأخرى لفظ تغيير الحقيقة، فالتشريعات الأخرى استعملت التعبير الأصوب لأن لفظ التحريف تنصرف في الأغلب إلى التزوير المادي أو إحدى صوره، فالتحريف بعني لغويا: افتراض شيء موجود على صورة معينة تم تحريفه ليصبح على صورة معينة أخرى، في حين أن التزوير في المحررات أهم وأشمل من ذلك، فقد يتم التحريف في شيء موجود وقد يصطنع شيئا غير موجود، للمزيد راجع في ذلك: نهلا عبد القادر المومني، مرجع سابق، ص.141.

[2] ـ يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات في القانون الأردني، مرجع سابق، ص.148.

[3] ـ المرجع نفسه، ص. 149.

وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا[1]، كما أن المشرع الجزائري لم يستحدث نصا خاصا بالتزوير في المحرر الالكتروني، لكنه تدارك ذلك من خلال القانون 15- 04 والمتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي، وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي، كما أنه لم يساير الاتجاه الحديث الذي تبنتها التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

نخلص مما سبق أن أغلب التشريعات المقارنة اقتصرت على تجريم بعض صور المحررات الالكترونية، ولم تضع نصوصا خاصة تجرم تزويرها مادام أن أغلبها ساوت بين المحررات الورقية والمحررات الالكترونية، وعليه لا بد من تكامل التشريعات بسن تشريع جنائي يجرم التزوير المعلوماتي والذي يمس بالمحررات الالكترونية ويحدد عقوبات تكون كافية للردع ، ولا يكتفي فقط تطبيق مبدأ التعادل الوظيفي ومساواة المحررات الورقية بالمحررات الالكترونية في الإثبات، فالمساس بمحتوى المحرر الالكتروني عن طريق تزويره يكون أشد صعوبة من تزوير المحرر الورقي.

ثانيا : أركان جريمة تزوير المحررات الالكترونية

لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية والتي كما هو معروف لا تتحقق إلا أثناء تكوين المحرر بالنسبة إلى الجريمة محل البحث[2]، بينما من المتصور وقوع فعل تغيير الحقيقة بالنسبة لهذه الجريمة من خلال طرق التزوير المادية، ولكن بشرط أن يكون التزوير لاحقا على نشأة المحرر الأصلي والحقيقي المعالج آليا فلا تتحقق تلك الجريمة من

[1] - لا بد من التفرقة بين المحرر المعالج آليا و المحرر المعلوماتي:

المحرر المعالج آليا: يقصد بالمحرر المعالج آليا كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية للمعلوماتية، بعبارة أخرى يقصد بالمحرر المعالج آليا الدعامة المادية التي تم تحويل المعطيات المسجلة عليها بلغة الآلة.

المحرر المعلوماتي: هو ذلك المحرر غير المعالج آليا وتعتبر محررات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد، للمزيد راجع في ذلك: أمال قارة، مرجع سابق، ص.135.

[2] - علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية ، القاهرة، 2002، ص.70.

خلال فعل تغيير الحقيقة باستخدام طريقة التزوير المادية أثناء نشأة المحرر على خلاف جريمة التزوير العادية[1].

يتمثل النشاط الإجرامي للتزوير الالكتروني في تغيير الحقيقة في بيانات محرر ما[2]، وهو أشد خطورة من التزوير الورقي[3]، وتكمن خطورته في كونه يستند على ركائز تقنية، مما يصعب اكتشافه، بخلاف التزوير الذي يحصل في المحررات الورقية[4]، بالتالي لقيام جريمة التزوير في المحررات الالكترونية توافر ركنين هما الركن المادي والركن المعنوي الذي يتضمن القصد الجنائي العام والقصد الجنائي الخاص.

1- الركن المادي:

يتكون الركن المادي في جريمة تزوير المحررات من النشاط الإجرامي والمتمثل في تغيير الحقيقة في محرر بإحدى الطرق المنصوص عليها قانونا، مما يترتب عليه ضررا بالغير، فيقصد به تغيير للحقيقة يرد على المحررات الالكترونية المعالجة آليا وذلك بنية استعمالها[5]، وهذا الركن يتكون من ثلاثة عناصر هي :

أ - تغيير الحقيقة:

يقصد بتغيير الحقيقة هو إبدالها بما يغايرها،[6] بالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر أو حذف منه طالما ظل مضمون المحرر في حالته قبل الإضافة أو الحذف، ويقوم ذلك بصدد المحررات الالكترونية في حالة حذفها أو إضافتها أو التلاعب فيها بأي

[1] - علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.60.

[2] - عبد الله بن سعود محمد السراني، مرجع سابق، ص.60.

[3] - محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.88.

[4] - جمال محمود الكردي، تنازع القوانين بشأن المسئولية عن سوء استخدام الانترنت، دار النهضة العربية، القاهرة، 2007، ص.24.

[5] - عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.63.

[6] - أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2006، ص.435.

صورة، سواء كانت هذه البيانات مخزنة في ذاكرة الحاسب الآلي أم كانت تمثل جزء من برنامج التشغيل أو برامج التطبيق، ويجب في هذه الحالة أن يكون محلا للتجريم[1].

يجب أن يكون التزوير للحقيقة قد وقع في محرر مكتوب أي محرر موجود من الأصل، ولا يهم اللغة التي كتب بها المحرر سواء كانت العربية أو أية لغة أجنبية، ولذلك لا يعد تزوير الحقيقة الذي يقع دون كتابة بقول أو فعل، بالتالي فإن البيانات المخزنة آليا سواء في ذاكرة الحاسب الآلي أو الأسطوانات الممغنطة أو أشرطة أو برامج غير مقروءة، لا يمكن للمعنى الذي تحمله أن ينتقل عن طريق البصر أو المشاهدة، لأن تسجل على هيئة نبضات إلكترونية مثبتة على دعامة يسمح للحاسب فقط بقراءتها[2].

لا يشترط أن يتم التزوير على المحررات المطبوعة على أوراق بواسطة الطابعة، فيمكن أن يتم التزوير على المعلومات المعالجة آليا داخل جهاز الكمبيوتر والمسجل على الأسطوانة الممغنطة، ولا بد أن يرد فعل التزوير على المعلومات المعالجة آليا، أما التزوير الذي يحدث على برامج الكمبيوتر، أي إدخال معلومات مغلوطة للبرامج، فلا يعد تزوير لمحرر إلكتروني، وإنما يمكن أن يشكل جريمة إتلاف للبرنامج، ويرجع السبب في ذلك استبعاد البرنامج من ضمن المحررات الالكترونية إلى أنها ليست معدة كدليل إثبات[3].

ب ـ وجود محرر إلكتروني:

يجب أن يكون التزوير للحقيقة قد وقع في محرر مكتوب أي محرر موجود من الأصل، ولا يهم اللغة التي كتب بها، ولا يعد تزويرا تزوير الحقيقة الذي يقع دون كتابة بقول أو فعل، وفي جرائم المعلوماتية فإن البيانات المخزنة آليا سواء في ذاكرة الحاسب أو اسطوانات ممغنطة أو أشرطة أو برامج غير مقروءة، ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق البصر أو

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

[2] ـ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص.140.

[3] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.80.

المشاهدة، لأنها تسجل على هيئة نبضات إلكترونية مثبتة على دعامة بشكل يسمح للحاسب فقط بقراءتها[1].

ج ـ الضرر في جريمة تزوير المحرر الالكتروني:

حتى يكتمل الركن المادي في جريمة التزوير لا بد أن يؤدي ذلك إلى تغيير الحقيقة في محرر مكتوب بإحدى الطرق المحددة قانونا، إحداث الضرر على الآخرين أو احتمال تعويضهم لهذا الضرر، فإذا لم يقع ضرر على الآخرين لا يكتمل الركن المادي وتنتفي جريمة التزوير[2]، فالضرر هو إخلال بحق أو مصلحة يحميها القانون، وقد يكون الضرر ضررا ماديا أو معنويا أو ضررا فرديا أو اجتماعيا، وقد يكون كذلك ضررا محتملا ولا يشترط وقوعه بالفعل بل يكفي احتمال حدوثه[3]، فلا يشترط أن يكون ماديا بل يكفي أن يكون معنويا[4]، والضرر المعنوي أو الأدبي هو الضرر الذي يصيب الإنسان في ذمته المالية الأمر الذي يترتب عليه الإنقاص من عناصرها الايجابية أو الزيادة في عناصرها السلبية، ويعرف الضرر الفردي أو الخاص بأنه الضرر الذي يصيب شخصا أو جهة معينة بالذات أو هيئة خاصة، أما الضرر الاجتماعي أو العام فهو الضرر الذي يصيب المجتمع أو المصلحة العامة، والمقصود بالضرر المحتمل هو الضرر الذي لم يتحقق بعد ولكن احتمال تحققه قائم وفقا للمجرى العادي للأمور، ففي جريمة التزوير يكفي الشروع في استعمال المحرر المزور، أما الضرر المحقق فهو الضرر الذي يتحقق باستعمال المحرر المزور فعلا[5].

يقاس ضابط الضرر على أساس ما للمحرر الالكتروني من قيمة قانونية في الإثبات، أي يصلح لأن يحتج به في مواجهة الغير أو التمسك به في مواجهة الغير، أو التمسك به في

[1] ـ عبد الله بن سعود محمد السراني، مرجع سابق، ص.6.

[2] ـ محمد علي العريان، مرجع سابق، ص.65.

[3] ـ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص.174.

[4] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.82.

[5] ـ نهلا عبد القادر المومني، مرجع سابق، ص.146.

مواجهته، ويستوي بعد ذلك أن يكون هذا المحرر قد أعد من البداية لهذا الغرض أم أنه يتمتع بتلك القيمة وعلى سبيل المصادفة[1].

2- الركن المعنوي:

يتضمن التزوير المعنوي إقرارات ذوي الشأن، أو جعل واقعة مزورة في صورة واقعة صحيحة، أو جعل واقعة غير معترف بها في صورة واقعة معترف بها[2]، والتزوير المعنوي غالبا ما يقع عند إنشاء المحرر وهناك صعوبة في إثباته، على عكس التزوير المادي الذي يثبت من فحص المحرر نفسه، أما التزوير المعنوي فهو يثبت من أمور أخرى تتيسر أحيانا وتتعذر في أحيان أخرى[3].

تعتبر جرائم التزوير في المحررات الالكترونية جرائم عمديه يلزم لوقوعها توافر القصد الجنائي بشقيه العام والخاص، فالجاني يكون عالما بأن الأفعال التي يرتكبها تجرمها القوانين والأنظمة وأنه يسعى لتغيير الحقيقة في محرر، وأن ذلك يترتب عليه الإضرار بالغير، وأن ينصرف علمه إلى أنه يغير الحقيقة بسلوكه فإذا ثبت جهله انتفى القصد الجنائي، أما العنصر الثاني فهو أن تكون نية الجاني فد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله[4]، أي الاحتجاج به على اعتبار أنه صحيح[5].

أ ـ القصد الجنائي العام:

يقوم القصد الجنائي العام على عنصري العلم والإرادة، فالعلم والإرادة شرطان أساسيان لتوافر القصد الجنائي العام[6]، فلا بد أن يدرك الجاني أنه يقوم بتحريف مفتعل للحقيقة في صك أو مخطوط أو مستند، فلا بد أن يكون الجاني مدركا أن هذا التزوير سيترتب عليه ضرر محقق

[1] ـ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.153.

[2] ـ محمد علي العريان، مرجع سابق، ص.142.

[3] ـ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.203.

[4] ـ جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص.176.

[5] ـ براهمي حنان، جريمة التزوير في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، مرجع سابق، ص.266.

[6] ـ عبد الله بن مسعود محمد السراني، مرجع سابق، ص.65.

أو احتمالي، أي لا بد من أن ينصرف علم الجاني إلى أنه يغير الحقيقة في محرر معلوماتي بإحدى الطرق المحددة في القانون[1]، وعلم الجاني وحده لا يكفي لقيام جريمة التزوير بل لا بد من أن تتجه إرادته إلى القيام بالركن المادي المكون لجريمة التزوير[2].

ب ـ القصد الجنائي الخاص:

يتمثل القصد الجنائي الخاص في نية استعمال المحرر المزور فيما زور من أجله سواء لتحقيق مصلحة شخصية، أو دفع ضرر، أو تحقيق مصلحة شخص آخر، أو إيقاع الضرر بشخص آخر[3]، فإذا انتفت هذه النية انتفى القصد الجنائي، وتطبيقا لذلك لا يسأل عن جريمة التزوير مثلا من يصطنع سندا بدين على شخص معين ويوقع عليه بإمضاء هذا الشخص متى ثبت أنه لم يقصد بذلك سوى اختبار قدرته على التقليد، وأن نيته كانت متجهة إلى إعدام المحرر في الحال[4].

[1] ـ عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.152.

[2] ـ نهلا عبد القادر المومني، مرجع سابق، ص.147.

[3] ـ محمد علي العريان، مرجع سابق، ص.66.

[4] ـ نهلا عبد القادر المومني، نفس المرجع، ص.148.

الفرع الثاني
جريمة النصب في مجال المحررات الالكترونية

برزت ظاهرة النصب المعلوماتي في العصر الحديث بوصفها ظاهرة خطيرة تمثل تهديدا حقيقيا لعملية الإثبات بالمحررات الالكترونية، ويرجع البعض هذا التهديد إلى ضعف التدخل الإنساني المباشر من جانب بعض أطراف العلاقة، مما يعطي الفرصة للطرف الآخر بإمكانية الغش[1]، وعليه ينصرف اصطلاح النصب بوجه عام إلى الغش والخداع الذي يصبوا إليه أي شخص للحصول من الغير دون وجه حق على فائدة أو منفعة أو ميزة ما، أما النصب المعلوماتي فنعني به إساءة استخدام الحاسبات الآلية والتلاعب في نظم المعالجة الالكترونية للبيانات والمعلومات، للحصول بغير حق على محررات الكترونية وأموال أو أي منفعة أخرى.[2]

تتميز جريمة النصب في المحررات الإلكترونية بأنها إذا وقعت وانتهت بمجرد ارتكابها نكون أمام جريمة وقتية، أما إذا كانت حالة مستمرة فترة من الزمن فتكون الجريمة مستمرة طوال هذه الفترة، فالعبرة في استمرار إرادة الجاني في الفعل المعاقب عليه تداخلا متتابعا متجددا، فالفيصل بين الجريمة الوقتية والجريمة المستمرة يكمن في طبيعة الفعل المادي المكون للجريمة سواء كان هذا الفعل إيجابيا أو سلبيا[3]، ويتم الاحتيال المعلوماتي في مجال المحررات الالكترونية من خلال تزييف المحرر الالكتروني مثل بطاقات الائتمان التي يتم الاحتيال عليها بتغيير الشريط الممغنط الثابت عليها، أو عن طريق تقليد الحروف البارزة الموجودة على البطاقة.

وعليه فسنتناول في هذا الفرع تعريف جريمة النصب المعلوماتي في الفقه والتشريع المقارن **(أولا)**، لنتناول بعدها متطلبات قيام جريمة النصب في مجال المحررات الالكترونية **(ثانيا)**.

[1] - محمد حسام محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، مرجع سابق، ص.6.

[2] - عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.101.

[3] - فتحي محمد أنور عزت، جرائم العصر الحديث، دار الفكر والقانون، المنصورة، 2010، ص.236.

أولا: تعريف جريمة النصب في مجال المحررات الالكترونية

اختلف الفقه والتشريع في الوصول إلى تعريف محدد لجريمة النصب المعلوماتي ويعود ذلك إلى تطور أساليب ارتكابها، بحيث لا يمكن الإحاطة بالصور الجديدة التي قد تظهر بها هذه الجريمة مستقبلا نظرا للتطور المتسارع للتقنيات الحديثة، وعليه سنتناول التعريف الفقهي لجريمة النصب في مجال المحررات الالكترونية ، ثم موقف التشريعات المقارنة من هذه الجريمة، وذلك على النحو التالي:

1 ـ التعريف الفقهي لجريمة النصب في مجال المحررات الالكترونية:

اختلف الفقه في تسمية جريمة النصب المعلوماتي عامة وفي جريمة النصب في مجال المحررات الالكترونية خاصة، فالبعض يسميها بالغش المعلوماتي أو غش الحاسوب، بينما البعض الآخر يسميها النصب المرتبط بالحاسوب، لكن كل التسميات والتعريفات المقدم لها أغلبها يراها من زاوية النظر إلى صفة الجرم، بأنه سلوك احتيالي أو خداعي مرتبط باستخدام الحاسوب، يهدف مرتكبه إلى تحقيق فائدة أو مصلحة مالية.

عرفها جانب من الفقه جريمة النصب المعلوماتي بأنها: **" أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي"**[1].

عرفها جانب آخر بأنها: **" التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير"**[2].

[1] ـ مشار إليه لدى: عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، 2000، ص.441.

[2] ـ مشار إليه لدى: نائلة عادل فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005، ص.425.

يلاحظ أن هذا التعريف ربط بين السلوك الاحتيالي وبين استخدام الحاسب الآلي بنية وهدف الوصول إلى تحقيق فائدة أو مصلحة مالية أو إلحاق الضرر بالغير، وذلك عن طريق التلاعب العمدي بمعلومات وبيانات لها قيمة مادية من شأنها التأثير على الحاسب الآلي.

2 ـ التعريف التشريعي لجريمة النصب المعلوماتي:

لم تورد أغلب التشريعات المقارنة تعريفا لجريمة الاحتيال بل تطرقت إلى مرتكب هذه الجريمة، فصياغة التعاريف ليست من مهام المشرع وإنما من اختصاص الفقهاء، كما أن بعض التشريعات أوردت لهذه الجريمة تحت تسمية النصب، كقانون العقوبات المصري وقانون العقوبات الجزائري، بينما في قانون العقوبات الأردني نجد أن هذه التشريعات أطلقت على هذه الجريمة باسم الاحتيال.

أ ـ اتفاقية بودابست لسنة 2001:

استخدمت اتفاقية بودابست لعام 2001 تسمية **"الاحتيال المرتبط بالحاسوب"** على جريمة الاحتيال المعلوماتي، واعتبر أنها تقع عندما يقوم شخص عن قصد وبدون وجه حق، وعلى نحو يسبب خسارة في ممتلكات الغير بما يلي:

ـ أي إدخال أو تعديل أو حذف أو كتم لبيانات الحاسوب.

ـ أي تدخل في وضائق نظام الحاسوب.

وبنية احتيالية أو غير شريفة بغرض الحصول دون حق على منفعة اقتصادية لنفسه أو لغيره[1].

ب ـ القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها:

أورد القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، المعتمد من قبل جامعة الدول العربية عام 2003 وصفا لجريمة الاحتيال المعلوماتي والتي أطلق عليها تسمية: **" جريمة الاحتيال عن طريق الشبكة المعلوماتية والحاسوب"**، حيث أشار القانون على أنه : **" كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي**

[1] ـ المادة 08 من اتفاقية بودابست لسنة 2001 وبنود الاتفاقية متوفرة على الموقع : https://rm.coe.int/

وما في حكمها، إلى الاستيلاء لنفسه أو لغيره، على مال منقول أو على سند ،أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية، أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه"[1].

ركز هذا التعريف على ماديات الجريمة وانصراف إرادة الجاني إلى الحصول وتحقيق كسب غير مشروع عن طريق حيازة مال مملوك للغير، كما أن هذا التعريف لم يحصر آليات الجريمة رغم أنه ذكر عبارة اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، إلا أنه ترك المجال واسعا عن طريق استعانة المجرم المعلوماتي بأية وسيلة احتيالية، لأن هذه الوسائل لا يمكن حصرها في ضل التطور التكنولوجي وظهور آليات أخرى للاحتيال مستقبلا.

ج ـ القانون الفرنسي:

عرف المشرع الفرنسي في المادة 1/313 من قانون العقوبات الجديد الاحتيال على أنه:**"واقعة خداع شخص طبيعي أو معنوي، سواء باستعمال نص كاذب أو صفة كاذبة أو التعسف في صفة غير صحيحة أو باستعمال حيلة تدليسية من شأنها حمل الغير على تسلم أموال أو قيمة مالية أو تقديم خدمة أو الموافقة على عمل ينتج عنه تحمل الغير على تسليم الأموال إلى الجاني"**[2].

يلاحظ أن المشرع الفرنسي استخدم عبارة: " أموال أو قيمة مالية " كمحل لجريمة النصب بدلا من لفظ "الأشياء" الوارد في قانون العقوبات قبل التعديل الجديد، بمعنى لا يشترط في المال بالضرورة أن يكون من الأموال المادية، كذلك تقوم جريمة النصب المعلوماتي وفقا لنص هذه

[1]ـ المادة 10 من القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[2] - Article 313-1 Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 , dispose que ***:« L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge »***.

المادة متى كان محلها تقديم خدمة بناء على النشاط الإجرامي الصادر من الجاني، فاستعمال الطرق الاحتيالية للحصول على هذه الخدمة يعد حسب نص هذه المادة جريمة نصب معلوماتي.

د ـ موقف المشرع الجزائري:

نص المشرع الجزائري في المادة 372 من قانون العقوبات على جريمة النصب بأنها: **" كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية، أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول أو على أي منها، أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها، أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث، أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر**[1]**..."**.

يلاحظ أن المشرع الجزائري ومن خلال نص المادة أنه لم يقدم تعريفا لجريمة النصب، بل اكتفى ببيان صور ارتكاب الأفعال على سبيل الحصر، كما أنه لم يتطرق إلى النصب الذي يقع على النظام المعلوماتي أو في مجال المعاملات الالكترونية بنصوص خاصة وقانون خاص يجرم النصب المعلوماتي، وعليه يمكننا القول من خلال دراستنا حول الطبيعة القانونية للمحرر الالكتروني باعتباره مال معلوماتي، فإن نص المادة 372 السالفة الذكر يمكن أن تشمل جريمة النصب في مجال المحررات الالكترونية النشاط الإجرامي الذي يقع على الأموال، من خلال التلاعب في البيانات والمعلومات المحيطة به، والذي يؤدي في النهاية إلى الاستيلاء على ذلك المال من قبل من ليس له حقا فيها.

نستخلص مما سبق أن أغلب التشريعات المقارنة تعتمد على نصوص خاصة للعقاب على النصب المعلوماتي باستعمال الكمبيوتر أو ما شابهه، فلم تعد خاضعة للقواعد العامة إذ يمكن افتراض حالتين: الحالة التي يستعين المتهم بجهاز الكمبيوتر للنصب على شخص معين ففي هذه الحالة تكون الاستعانة في النصب على جهاز الحاسب الآلي، وذلك بقيام المتهم بنشر دعاية

[1] ـ الأمر 66- 156 المتضمن قانون العقوبات السالف الذكر.

كاذبة بغية تحقيق أرباح من نشاطه التجاري غير المشروع، والحالة التي يقوم فيها المتهم بالاستعانة بجهاز الحاسب الآلي للنصب على جهاز حاسب آلي آخر، فنجد أن الآلة تحل محل المجني عليه وهذا لا يعني أنه يمكن إعفاءه من المسؤولية بل المسؤولية تقع على صاحبه[1].

ثانيا: متطلبات قيام جريمة النصب في مجال المحررات الالكترونية

يتطلب لقيام جريمة النصب في مجال المحررات الالكترونية توافر الركن المادي الذي يتمثل في فعل النصب (الاحتيال) التي حددتها القوانين على سبيل الحصر، والنتيجة التي تترتب عليه تسليم المجني عليه مالا إلى المتهم، وعلاقة السببية بين الفعل المادي وهو الاحتيال، والنتيجة وهي الاستيلاء على مال الغير، كما تتطلب ركنا معنويا يتخذ صورة القصد الجنائي الذي يتمثل في علم المتهم أن التلاعب الذي يحدثه بنظام الحاسب الآلي أو المعلومات التي يقوم بإدخالها إلى هذا النظام، من شأنها أن تجعل الحاسب يستجيب وفقا لهذه المعلومات.

1 ـ الركن المادي:

يتكون الركن المادي لجريمة النصب من ثلاثة عناصر هي:

أ ـ فعل الاحتيال :

حددت أغلب التشريعات المقارنة المذكورة آنفا وسائل قيام جريمة النصب على سبيل الحصر وهي: الطرق الاحتيالية، التصرف في مال ليس ملكا للمتهم وليس له حق التصرف فيه، اتخاذ اسم كاذب أو صفة غير صحيحة.

ذهب جانب من الفقه إلى القول بأن التلاعب في البرامج والبيانات والتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها مما يجعله يسلم بها، يعد من أحد أساليب التحايل حسب هذا الاتجاه أن الحاسوب ليس سوى مجرد وسيط للتحايل، وقد ذهب بعض الفقه الفرنسي إلى أن غش أنظمة الحاسوب وخداعها للاستيلاء على الأموال تتحقق به صفة الطرق الاحتيالية، بالتالي قيام جريمة الاحتيال، واستندوا في ذلك على أن إدخال وسائل الغش أو خداع الأنظمة

[1] ـ شيماء عبد الغني محمد عطا الله، مرجع سابق، ص.62.

المعلوماتية يدخل ضمن الطرق الاحتيالية، وأن خداع الآلة يمكن تصوره على أساس أنه يوجد خلف الآلة إنسان وهو من قام ببرمجة هذه الآلة، ويعتبر هذا الرأي أن المعلومات المدخلة إلى النظام المعلوماتي تمثل وقائع تدعم الكذب المصاحب للخداع[1].

ب ـ النتيجة الإجرامية:

تتمثل النتيجة الإجرامية في استيلاء المجرم المعلوماتي على مال الغير عن طريق الاحتيال على المجني عليه دون وجه حق، وذلك باستخدام الحاسب الآلي بوصفه أداة ايجابية في هذا الاستيلاء، فالحاسب الآلي يعد أداة إيجابية في جريمة النصب المعلوماتي متى تم التدخل مباشرة في المعطيات بإدخال معلومات وهمية، أو بتعديل البرامج أو خلق برامج صورية وليس هناك صعوبة في اكتشاف الطرق الاحتيالية في هذه الحالات، وكذلك كأثر للاستخدام التعسفي لبطاقات الائتمان الممغنطة متى استخدمت كأداة في جريمة النصب المعلوماتي[2] .

ج ـ علاقة السببية :

يقصد بعلاقة السببية في جريمة النصب المعلوماتي أن يكون التسليم الحاصل للمال من المجني عليه للجاني مترتبا على سلوك هذا الأخير، فإن لم يكن مترتبا عليه فإن الجريمة لا تعد نصبا لانتفاء ركنها المادي، فعلاقة السببية تنص على أن النصب هو السبب الفعلي والدافع على التسليم، وأن يكون التسليم لاحقا على فعل النصب ونتيجة لانخداع المجني عليه ويكون مبنيا على الضرر.

2 ـ الركن المعنوي لجريمة النصب المعلوماتي:

تتطلب جرائم النصب إبتداءا توافر القصد الجنائي العام، بالإضافة إلى القصد الجنائي الخاص، فلا يكفي العلم بالواقعة وإرادتها، وإنما يلزم إلى جانب ذلك توافر نية محددة لدى الجاني.

[1] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص.185.

[2] ـ عبد الصبور عبد القوي علي منصور، التنظيم القانوني للتجارة الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2012، ص.111.

أ ـ القصد الجنائي العام :

يقصد بالقصد الجنائي العام انصراف إرادة الجاني إلى تحقيق الواقعة الإجرامية مع العلم بتوافر أركانها، بحيث يجب أن يكون الجاني على علم بنشاطه الإجرامي المتمثل في عملية النصب، وأن تتجه إرادته إلى الطرق الاحتيالية بحيث يكون عالما بما يقوم به، وأن المال الذي ينوي الحصول عليه ليس ملكا له بل هو مملوك لغيره.

ب ـ القصد الجنائي الخاص:

يتمثل القصد الجنائي الخاص في انصراف نية الجاني إلى الاستيلاء والحيازة الكاملة للمال المجني عليه، بالتالي إذا لم يكن قصد الجاني منصرفا إلى تملك المال الذي تحصل عليه من حائزه بطريقة الحيلة انتفى قيام القصد الجنائي الخاص.

نستخلص مما سبق أن تعدد الأساليب التي ترتكب بها أفعال النصب المعلوماتي في مجال المحررات الالكترونية، يجمعها كلها عامل واحد يتمثل في التصدي على البرامج والمعلومات المخزنة آليا والتلاعب فيها للحصول بغير حق على أموال غير مشروعة، فجرائم النصب تقوم على كل غش وخداع للأنظمة المعلوماتية، وذلك بسلب المال عن طريق استعمال الطرق الاحتيالية بالكذب الذي يِؤدي إلى إيقاع الجاني بضحاياه، وتمرير أعماله الإجرامية تحت غطاء يوهم للمجني عليهم أن أعماله مشروعة، بالتالي تخضع جريمة النصب على المحررات الالكترونية لذات أحكام جريمة النصب ولأركانها وهما الركن المادي والركن المعنوي، في أن الركن المادي يتطلب وقوع فعل مادي يتمثل في استعمال الطرق الاحتيالية للحصول على محررات ليست ملكا للمتهم وليس له حق التصرف فيه، وحدوث نتيجة تتمثل في الاستيلاء على تلك المحررات، بالإضافة إلى قيام رابطة السببية بين الفعل المادي والنتيجة، أما الركن المعنوي فيتمثل في القصد الجنائي القائم على العلم والإرادة، وذلك لتحقيق مصلحة شخصية وانصراف نيته في تملك الشيء محل الجريمة.

الفرع الثالث

جريمة السرقة في مجال المحررات الالكترونية

تختلف طريقة وكيفية الاستيلاء على الشيء بالضرورة باختلاف طبيعة الشيء الذي يقع عليها الاستيلاء، فالقواعد العامة لجريمة السرقة لا تدخل الأموال المعنوية ضمن الاعتداء في نصوص جريمة السرقة كون المال يقع على كيان مادي، وعلى الرغم من ذلك إلا أنه إذا أمكن حيازته داخل إطار معين للاستئثار بها، فإنه يقع تحت طائلة السرقة وإن كانت طبيعة المعلومات والبيانات التي تتضمنها المحررات الالكترونية سواء المخزنة على الحاسب الآلي أو المتبادلة عبر شبكة الإنترنت يصعب حيازتها ما لم تثبت على وسيلة لنقل أو نسخ المعلومات بحيث تصلح محلا للسرقة لأن النسخ أو إعادة الإنتاج يعد بالنظر إلى طبيعة البيانات المخزنة إلكترونيا طريقة ممكنة لاختلاسها، لأن الاستيلاء عليها يتحقق به، فالمجرم المعلوماتي لا يستهدف في جريمة سرقة المحررات الالكترونية الحصول على القيمة المادية بل يسرق ما هو مدون بها، وعليه فإن هذه الجريمة تنشأ عن طريق كل فعل من شأنه الاستيلاء على هذه المحررات المملوكة للغير من داخل الحاسب الآلي والمخزن على الدعامات الالكترونية، وذلك سواء تم ذلك عن طريق الاستيلاء على الشريط الممغنط أو الاسطوانة أو الذاكرة، أو عن طريق تشغيل جهاز الحاسب الآلي والاطلاع على هذه المحررات وتصويرها بمعنى الحصول على نسخة ضوئية منها، وعليه سنتناول في هذا الفرع موقف كل من الفقه والتشريع المقارن من جريمة السرقة في مجال المحررات الالكترونية **(أولا)**، لنتعرض إلى أركان جريمة السرقة في هذا النوع المستحدث من المحررات **(ثانيا)**.

أولا: تعريف جريمة السرقة في مجال المحررات الالكترونية

اختلف الفقه والتشريع في الوصول إلى تعريف محدد لجريمة السرقة في مجال المحررات الالكترونية، ويعود ذلك إلى طبيعة المعلومات والبيانات التي تتضمنها هذه المحررات، وعلى خلاف ذلك اعتبر الفقه والتشريع المقارن أن سرقة مضمون ومحتوى هذه المحررات تقوم بناءا على سرقة الشريط الممغنط أو الملف، بالتالي فإن سرقة هذا الأخير دليل على قيام جريمة سرقة

هذه المحررات، وعليه سنتناول موقف الفقه من جريمة السرقة في مجال المحررات الالكترونية أولا، لنتناول بعدها بيان موقف التشريعات المقارنة من هذه الجريمة ثانيا، وذلك على النحو التالي:

1 ـ موقف الفقه من جريمة السرقة في مجال المحررات الالكترونية:

اعتبر الفقه المحرر الالكتروني بأنه معلومات إلكترونية ترسل أو تسلم بوسائل إلكترونية أيا كانت وسيلة استخراجها في المكان المستلمة فيه، بالتالي يجمع فقهاء كل من فرنسا والولايات المتحدة الأمريكية وبلجيكا وغيرهم على اعتبار المعلومات محلا يقبل السرقة، ومن ثم جواز انطباق النصوص المتعلقة بتجريم هذا السلوك عليه، فيعتبر هذا الجانب من الفقه أن سرقة المعلومات ضد إرادة مالكها أو حائزها الشرعي إنما يعد اختلاس لمال مملوك للغير، ما يعد مكونا لجريمة السرقة، ويتفق أنصار هذا الاتجاه على مجموعة من القواعد الأساسية المشتركة والتي يتمثل أهمها في ضرورة صدور سلوك مادي عن الجاني، وإلا فإنه لا يمكن أن ينسب إليه سلوك يعاقب عليه، ويذهب رأي آخر إلى القول بإمكانية أن يكون اختلاس المعلومة بمجرد الالتقاط الذهني لها سواء تم ذلك بواسطة السمع أو البصر[1].

2- موقف التشريع المقارن من جريمة السرقة في مجال المحررات الالكترونية:

لم توضح أغلب التشريعات مسألة تجريم السرقة في مجال المحررات الالكترونية أو إضفاء الطابع الجنائي على المحرر الإلكتروني من جريمة السرقة، وذلك لصعوبة تحديد المفاهيم والطرق التي تقوم عليها هذه الأنواع من الجرائم.

أ ـ القانون الفرنسي:

نص المشرع الفرنسي في نص المادة1/311من قانون العقوبات الجديد الذي دخل حيز التنفيذ في مارس1994 على أن: **" السرقة هي اختلاس شيء مملوك للغير"**[2] ، فذكر كلمة (شيء)[1]

[1] ـ نائلة عادل محمد فريد قورة، مرجع سابق، ص.151.

[2] - Article 311-1du C.P.F. dispose que ***: « Le vol est la soustraction frauduleuse de la chose d'autrui» .***

مطلقة دون قيد ودون أن يصف هذا الشيء بأنه مادي أو مجسم، وهذا يعني أن المشرع الفرنسي لم يقصر محل السرقة على الأشياء المادية وحدها، وإنما يشمل هذا المحل مطلق الأموال أو كل عناصر الذمة المالية، حتى ولو كانت هذه الأموال أو العناصر غير مادية طالما تقبل الاختلاس[2].

ب ـ القانون المصري:

جرم المشرع المصري بطريقة غير مباشرة جريمة السرقة، حيث أنه جرم سرقة المحرر الذي حصل عليه بوسيلة غير قانونية قد تكون سرقة أو اختلاس، " **كل من توصل بأية وسيلة من الحصول بغير حق على وسيط أو محرر إلكتروني**"[3]، إلا أن بعض الفقه اتجه إلى عدم إضفاء هذه الصيغة على المحرر الإلكتروني، واستند على ذلك أن جريمة السرقة تقع على الأشياء المادية الملموسة، وبهذا اتجه هذا الرأي إلى إخراج صفة السرقة من مجال المحرر الالكتروني، وهذا الرأي تم الطعن فيه إذ من الفقهاء من ذهب عكس ذلك أي أن اعتبار المحرر الإلكتروني قيمة معنوية يجب أن يخضع للاستيلاء[4].

ج ـ موقف المشرع الجزائري:

نص المشرع الجزائري في المادة 350 من قانون العقوبات الجزائري على أنه: " **كل من اختلس شيئا غير مملوك له يعد سارقا**"، فلم يشترط هنا صراحة بضرورة أن يكون المال محل الجريمة ماديا، وإنما يمكن أن تقع جريمة السرقة على الأشياء غير المادية بمعنى المعنوية، إذا ما اعتبرنا عبارة الشيء التي أوردها في نص هذه المادة تنصرف على المال

---

[1] ـ يذهب بعض الفقه الفرنسي إلى أن كلمة شيء الوارد ذكرها في المادة 1/311 من قانون العقوبات الفرنسي الجديد، ترتبط بذات الوصف الذي تعبر عنه كلمة مادية، وإن كان من شأن ذلك أن يقلص مضمونها- أي كلمة شيء إلى الأشياء المادية الملموسة، ويرى هؤلاء الفقهاء أن لفظ شيء الوارد ذكرها، يجب أن لا تفسر بمعزل عن صلته بفعل الاختلاس، وإن كان هناك تحكم في إعطاء لفظ الشيء مفهوما أضيق من مفهومه، فثمة تحكم أيضا في إعطاء فكرة الاختلاس مضمونا أوسع من الدلالة الطبيعية للفظها، راجع في ذلك: محمد أمين أحمد الشوابكة، مرجع سابق، ص.149.

[2] ـ عفيفي كامل عفيفي، مرجع سابق، ص.121.

[3] ـ المادة 23 من قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004.

[4] ـ محمد أمين الرومي، المستند الالكتروني، مرجع سابق، ص.110.

المعلوماتي، لأن المعلومات تعتبر على الأرجح برامج أو قواعد بيانات، كما أن هذا التعريف يهتم بالجانب الموضوعي للسرقة حيث يتطلب لقيامها أن يقوم الجاني بارتكاب فعل مادي محدد بسلوك إجرامي وهو الاختلاس، وأن ينصب هذا الاختلاس على منقول مملوك للغير.

يلاحظ أن نص المادة 350 من قانون العقوبات الجزائري ونص المادة 311 من قانون العقوبات المصري و نص المادة1/311من قانون العقوبات الفرنسي الجديد، لم تتشترط أن ينصب فعل الاختلاس المكون للركن المادي لجريمة السرقة على محل مادي، وبالتالي يصلح أن يكون موضوعا لجريمة سرقة الأشياء غير المادية أو المعنوية، حتى لا تجرد هذه الأشياء من الحماية القانونية مما يفتح المجال واسعا للاعتداء عليها، وبالتالي يمكن القول بصلاحية المحررات الالكترونية أن تكون محلا أو موضوعا لنصوص جريمة السرقة بوضعها الحالي، وهو ما استقر عليه الفقه والقضاء استنادا لعمومية النص الجنائي المنظم لهذه الجريمة.

ثانيا: أركان جريمة السرقة في مجال المحررات الالكترونية

استقر الفقه والقضاء على أن السرقة هي اختلاس مال منقول مملوك للغير بطريق الغش وبنية تملكه[1]، ويستوي في فعل الاختلاس أن يكون الجاني قد استولى على المال خلسة أو قوة بنية تملكه أو تسلمه بناء على يد عارضة فغير نيته واستولى عليه[2]، ويقتضي الاختلاس السيطرة الكاملة للجاني على المال المختلس، مما يفترض وقوع هذا الأخير تحت سيطرة واحدة أو حيازة واحدة[3]، فمن خلال هذا التعريف يتضح لنا أن لجريمة السرقة ثلاثة أركان: الركن المادي وهو فعل الاختلاس، محل الجريمة والذي يعتبر مال منقول مملوك للغير، وأخيرا ركن معنوي والذي يقصد به القصد الجنائي.

[1] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص.139.

[2] ـ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.319.

[3] ـ عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الالكترونية، مرجع سابق، ص.193.

1 ـ الركن المادي:

يتكون الركن المادي عادة من سلوك ونتيجة وعلاقة سببية بين السلوك والنتيجة[1]، ويتمثل الركن المادي وفقا للقواعد العامة للسرقة في فعل الاختلاس[2]، واتفق الفقه والقضاء على اعتبار أنه أخذ مال الغير دون رضاه، بمعنى لا بد أن يتم نزع المال من مالكه بالقوة وهو الاستيلاء على حيازة الشيء بغير رضا مالكه أو حائزه، ويتوافر الاختلاس إذا قام الجاني بحركة مادية لينقل الشيء على حيازته أيا كانت الطريقة، ويشترط أن يكون الاستيلاء بفعل الجاني، والاختلاس لا يعني مطلق الاستيلاء على مال الغير وانتزاعه من صاحبه وإنما الاستيلاء عليه بوسيلة معينة[3]، ويتحقق فعل الاختلاس بتوافر العنصرين المادي والمعنوي، فيتحقق العنصر المادي بانتقال الحيازة عن طريق السلب سواء كانت كذلك أم مجرد حيازة، وذلك دون رضا المجني عليه، أي المالك الأصلي، كما أن التسليم الذي ينفي الاختلاس في جريمة السرقة لا بد وأن تتوفر فيه شروط ثلاثة وهي:

1ـ أن يكون التسليم إراديا.

2 ـ أن يكون صادرا من الحائز.

3 ـ أن يكون مقصودا به نقل الحيازة[4].

لا تدخل الأموال المعنوية ـ وفقا للقواعد العامة ـ تحت حكم مواد السرقة، إذ أنه من غير المتصور سرقة شيء معنوي دون ارتباطه بالشيء المادي وذلك نظرا لطبيعة هذا الشيء، إلا

---

[1] ـ علي عبد القادر القهوجي، الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، 26-27 أفريل 2003، ص.98.

[2] ـ يعرف الاختلاس ـ طبقا للنظرية التقليدية ـ على أنه : نقل الشيء أو نزعه من المجني عليه بغير علمه ورضاه وإدخاله إلى حيازة الجاني، ويذهب البعض إلى الربط ما بين فعل الاختلاس ومفهوم الحيازة للشيء، بحيث يعتبر الاختلاس استيلاء على حيازة الشيء دون رضا صاحبه، راجع في ذلك: محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مرجع سابق، ص.155، ويقوم فعل الاختلاس على عنصرين: أحدهما عنصر موضوعي ويتمثل في الاستيلاء على الحيازة وهو كل فعل يأتيه الجاني ويترتب عليه إخراج الشيء من حيازة مالكه وإدخاله في حيازة أخرى سواء كانت حيازة الجاني أو غيره، راجع في ذلك: عمرو عيسى الفقي، جرائم الحاسب الآلي والانترنت، المكتب الجامعي الحديث، الإسكندرية، 2006، ص.39.

[3] ـ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص.408.

[4] ـ شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الالكترونية، مرجع سابق، ص.45.

أنه إذا أمكن تحيزه داخل إطار معين و الاستئثار به[1]، فإنه يقع تحت طائلة السرقة التي تشمل الإطار كل ما يحتويه من معلومات، أما فيما يتعلق بالمعلومات التي تظهر على الشاشة فإنها لا تعتبر بمثابة شيء ولا تصلح لأن تكون محلا للسرقة، فالاختلاس إذن في مجال المحررات الالكترونية لا يتم إلا إذا كانت المحررات مدونة على دعامات مادية، وإن لم يكن كذلك فالأمر يتعلق بخدمات وليس بأموال، وعليه فإذا قام صاحب المعلومة ببثها عبر شبكة معينة وقام شخص آخر باعتراضها بوسيلة أو بأخرى، كاستعمال كلمة السر مثلا بطريق الغش فإن الأمر لا يتعلق بسرقة أو نصب، ويرجع ذلك إلى عدم توفر صفة المنقول في المعلومات محل البث[2]، فكل شيء له كيان ملموس يصلح أن يكون محلا لجريمة السرقة.

2 ـ الركن المعنوي:

يتخذ الركن المعنوي في جريمة السرقة في مجال المحررات الالكترونية صورة القصد الجنائي العام والخاص ويتحقق القصد الجنائي العام بتوافر العلم والإرادة[3]، فيتحقق العلم في حال قيام الجاني باختلاس مال منقول مملوك للغير مع علمه بذلك، فإذا انتفى هذا العلم ينتفي القصد الجنائي وتنتفي معه الجريمة، أما الإرادة فتقتضي أن تتجه إرادة الجاني إلى فعل الاختلاس الذي ينصب على مال منقول مملوك للغير، الأمر الذي يؤدي إلى خروج هذا المال من سيطرة حائزه إلى الحيازة الكاملة للجاني، فإذا انتفت الإرادة انتفى القصد ومن ثم أنتفت الجريمة[4]، وتتخذ صورة القصد الجنائي الخاص نية التملك التي يقصد بها انصراف إرادة الجاني إلى الظهور على الشيء بمظهر المالك، وتتألف هذه النية من عنصرين سلبي وهو إرادة

[1] ـ تعد خاصية الاستئثار أمرا هاما في جميع الجرائم التي تنطوي على اعتداء قانوني على الأموال، فالفاعل الذي استولى على شيء يستأثر به على ميزة تخصص الغير، وفي مجال المعلومات تتوافر صفة الاستئثار، إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين، للمزيد راجع في ذلك: عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص.156.

[2] ـ عبد الفتاح بيومي حجازي، الحكومة الالكترونية، مرجع سابق، ص.271.

[3] ـ خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، مرجع سابق، ص.105. محمد أمين الشوابكة، مرجع سابق، ص.160.

[4] ـ عفيفي كامل عفيفي، مرجع سابق، ص.140.

حرمان المالك من سلطاته على الشيء، وعنصر إيجابي قوامه إرادة الجاني أن يحل محل المالك في سلطاته الفعلية على الشيء[1].

أ ـ القصد الجنائي العام في جريمة السرقة في مجال المحررات الالكترونية:

لا يقوم الدخول إلى النظام المعلوماتي العام الذي يمكن أن يدخل إليه أي مستخدم بغرض الحصول على معلومات اعتباره جريمة السرقة، ولكن انتهاكا للنظام المعلوماتي الخاص والمبرمج بسرقة كلمة مرور واختراق نظامه الأمني، هو الدليل على توافر علم الجاني بدخوله إلى نظام خاص وبالتالي توافر القصد الجنائي، بالإضافة إلى علمه بدخوله للنظام بطريقة غير مشروعة، يتعين أيضا أن تتجه إرادته إلى الاستيلاء على المعلومات وإخراجها من حوزة صاحبها وإدخالها في حيازته[2].

يتحقق القصد الجنائي العام بتوافر عنصرين:الإرادة والعلم.

أ ـ الإرادة:

تتمثل الإرادة في نشاط نفسي يتجه على تحقيق غرض معين عن طريق وسيلة معينة، فهي القوة الدافعة لسلوك الإنسان لكي يتعرف على وجه معين لإشباع حاجاته المتعددة، ومن ثم يتعين أن يصدر هذا النشاط عن وعي وإدراك، مما يفترض معه العلم بالغرض المستهدف وبالوسيلة المستعملة لتحقيق هذا الغرض.

يرى الفقه في جريمة السرقة أنه لا بد أن تتجه إرادة الجاني إلى اختلاس المال المنقول المملوك للغير، بإخراجه من حيازة صاحبه إلى حيازته هو وإخضاعها إلى سيطرته المادية التي تمكنه من الظهور عليه بمظهر المالك، فإذا توافرت الإرادة بالنسبة للشق الأول وهو فعل

[1] ـ هشام محمد فريد رستم، مرجع سابق، ص.266.

[2] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص.161.

الإخراج ولم تتوافر في الثاني وهو إدخال المال في حيازة الجاني أو الغير فلا يتوافر القصد الجنائي[1].

ب ـ العلم :

لا تكفي الإرادة وحدها لقيام القصد الجنائي العام في جريمة السرقة المعلوماتية، وإنما يجب توافر العلم والإحاطة من قبل الجاني بحقيقة الوضع الإجرامي من حيث الوقائع وماهيته ومن حيث القانون[2]، فالعلم هو إدراك الفاعل للأمور[3] بحيث يعلم الجاني أن يعير في الحقيقة ويأتي أفعالا مادية أو مظاهر خارجية يؤيد بها إدعاءاته الكاذبة، لأن الأصل في ذلك أن المجرم المعلوماتي يوجه سلوكه الإجرامي نحو ارتكاب جريمة السرقة المعلوماتية مع علمه وقاصدا ذلك، ومهما يكن لا يستطيع انتفاء علمه للقصد الجنائي العام.

يلاحظ أن الدخول إلى النظام المعلوماتي العام الذي يمكن أن يدخل إليه أي مستخدم بغرض الحصول على معلومات لا يقوم به جرم السرقة، ولكن انتهاك النظام المعلوماتي الخاص والمبرمج بسرقة كلمة مرور واختراق نظامه الأمني، هو الدليل على توافر علم الجاني بدخوله إلى نظام خاص وبالتالي توافر القصد الجنائي،[4] وبالإضافة إلى علمه بدخوله للنظام بطريقة غير مشروعة يتعين أيضا أن تتجه إرادته إلى الاستيلاء على المعلومات وإخراجها من حوزة صاحبها وإدخالها في حيازته.

ب ـ القصد الجنائي الخاص في جريمة السرقة في مجال المحررات الالكترونية:

يفترض لقيام جريمة السرقة توفر القصد الجنائي الخاص والذي يقصد به نية التملك، باعتبار أنها هي التي يمكن من خلالها كشف نية الجاني في حيازته للشيء، وكذلك نية الاستحواذ على

[1] ـ أحمد خليفة الملط، مرجع سابق، ص.229.

[2] ـ حسين الغافري، جرائم الانترنت، دار النهضة العربية، القاهرة، 2009، ص.256.

[3] ـ فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الرابع عشر حول الجرائم الالكترونية المنعقد في الفترة من 24إلى 25مارس 2017، طرابلس، ص.120، منشور على موقع: www.jilrc.com

[4] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص.161.

الشيء المسروق[1]، والتي تتحقق بحرمان المالك الشرعي من سلطاته على المال محل السرقة، والحلول محل المالك في سلطته على هذا المال[2].

تبدأ جريمة السرقة المعلوماتية من أول الدخول غير المشروع إلى النظام المعلوماتي، فالقصد فيها يتخذ صورتين:

ـ **الأولى:** تتمثل في حالة الدخول العام وهو الذي يدخل فيه المستخدم للجهاز والحصول على المعلومات وهو لا يمثل سرقة.

ـ **الثانية:** تتمثل في انتهاك للنظام المعلوماتي الخاص، والذي له كلمة سر ونظام أمني خاص يدل على وجود قصد وسوء النية من مرتكب الفعل، ويتوفر فيها القصد العام والخاص ويظهر القصد الخاص في فترة البقاء غير المشروع، إلا أن المشكلة التي تعترض ذلك هي كيفية إثبات سوء النية[3].

يلاحظ مما سبق أن جريمة السرقة في مجال المحررات الالكترونية هي من الجرائم الالكترونية التي تستدعي قيامها، أن ينصب علم الجاني بالسلوك والفعل الإجرامي غير المشروع الذي قام به، كما يجب أن يرتبط هذا العلم مع الإرادة التي تعكس قيام الجاني بهذا السلوك الإجرامي، ويجب أيضا أن يترافق معها القصد العام الذي يقتضي توافر علم الجاني بالعناصر التي اشترطها القانون في جريمة السرقة، فيعمد إلى ارتكابها مع علمه بفعلته واتجهت إرادته إليها، أو كان عالما أن فعله الذي سيقوم به يؤدي إلى نتيجة غير مشروعة، بالإضافة إلى القصد الخاص الذي يقصد به نية التملك لدى الجاني إذ بانتفائها لا تعد سرقة.

[1] ـ أحمد خليفة الملط، مرجع سابق، ص.274.

[2] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص.148.

[3] ـ أحمد خليفة الملط ، نفس المرجع، ص.275.

المطلب الثاني

الجرائم المستحدثة المتعلقة بالمحررات الالكترونية

ساهم التطور التكنولوجي في وسائل الاتصال الحديثة في اتساع نطاق الجريمة الالكترونية مما أدى إلى ظهور عدة أنماط إجرامية مستحدثة، بالتالي أدى ذلك إلى تعدد صور الأفعال الماسة بالمحرر الالكتروني من جهة، وتنوع السلوك الإجرامي في ارتكابها من جهة أخرى، فمن بين المخاطر المستجدة في الإجرام الإلكتروني والتي تهدد أمن المحرر الالكتروني، تلك التي سواء تستهدف إفشاء وإذاعة ما يحتويه من معلومات قد تكون ذات الشأن، خاصة المتعلقة منها بالمعلومات التي تصنف في نطاق أسرار الدولة والمعلومات التي لها قيمة اقتصادية، أو تلك التي تجرم الدخول أو البقاء بطريقة كلية أو جزئية داخل منظومة معالجة المعلومات التي يحتويها المحرر الإلكتروني، فتقع جريمة الدخول في حالة عدم حصول الجاني على تصريح من صاحب المعلومات ودخوله إليها دون علمه أو دون السماح له بذلك، وتقع جريمة البقاء عند بقاء الجاني داخل النظام المعلوماتي وتجاوز الوقت المصرح به، وقد تتحقق جريمة البقاء مستقلة عن جريمة الدخول داخل نظام المعالجة الآلية للمعطيات وقد تجتمعان في جريمة واحدة، بالإضافة إلى جريمة إعاقة سير العمل في نظام المعالجة الآلية للمعطيات، والذي يتمثل في جريمة الإتلاف المعلوماتي والتي هي من الجرائم التي أفرزها التطور التكنولوجي، والذي أضفى عليها طابعا مميزا عن جريمة الإتلاف التقليدية، بحيث أنها ترتكب من طرف أشخاص يمتلكون المهارة والمعرفة الفنية بالنظم المعلوماتية، بالتالي من خلال هذا سنتاول في هذا المطلب جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات **(الفرع الأول)**، ثم جريمة الإتلاف في مجال المحررات الإلكترونية **(الفرع الثاني).**

الفرع الأول

جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

تقع جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات من أي إنسان أيا كانت صفته، سواء كان يعمل في مجال الأنظمة أم لا علاقة له بالحاسب الآلي وشبكاته، وسواء كانت لديه المقدرة الفنية على الاستفادة من النظام أم لا، إنما يكفي أن لا يكون له حق الدخول إلى النظام[1]، وتقع هذه الجريمة أيضا متى ما وضع مالك النظام قيودا على الدخول إلى النظام ولم يحترم الجاني هذه القيود، ويجب لقيام جريمة الدخول والبقاء في أنظمة المعالجة الآلية للمعطيات[2] توافر معلومات مخزنة داخل النظام المعلوماتي، فتتحقق جريمة الدخول عند عدم حصول الجاني على تصريح من صاحب المعلومة، ودخوله إليها دون علمه أو دون السماح له بذلك، أو إذا اشترط عليه من له حق السيطرة على النظام دفع مبالغ مالية وتم دخول الجاني دون دفعه للمبلغ المستحق[3]، أما جريمة البقاء فتتحقق عند ما يتواجد الجاني داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على نظام المعالجة الآلية للمعطيات، وعلية سنتناول جريمة الدخول والبقاء غير المشروعين في نظام المعالجة الآلية

---

[1] ـ عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها القانوني، مرجع سابق، ص.361.

[2] ـ تعرف نظم معالجة البيانات حسب تعريف مجلس الشيوخ الفرنسي بأنها:**" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي يتم عن طريقها تحقيق نتيجة معينة وهي معالجة المعطيات ،على أن يكون هذا المركب خاضع لنظام المعالجة الفنية"**، راجع في ذلك: عبد الفتاح بيومي حجازي، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص.329. ومحمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2007، ص.26.

ـ كما تبنى المشرع الجزائري هذا التعريف بموجب أحكام المادة 02/ب من قانون 04/09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وأطلق عليه تسمية " منظومة معلوماتية" وعرفها بأنها: **" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين"**. ويلاحظ من خلال هذه المادة أن نظام المعالجة الآلية يقوم على عنصرين، يتمثل العنصر الأول في مركب يتكون من عناصر مادية ومعنوية مختلفة ترتبط فيما بينها نتيجة علاقات توحدها بهدف تحقيق هدف محدد، أما العنصر الثاني يتمثل في ضرورة خضوع النظام لحماية فنية.

[3] Xavier linant de bellefonds, Alain Hollande, Pratique du droit de l’informatique et de l’internet, 6eme édition, Delmas, Paris, 2008, p.236.

للمعطيات **(أولا)**، لنتناول أركان جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات **(ثانيا)**.

أولا : موقف التشريعات المقارنة من جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي:

يتخذ فعل الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات صورتين أو شكلين، منها الصورة البسيطة وتتمثل في مجرد الدخول أو البقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية للمعطيات أو محاولة القيام بذلك، ومنها الصورة المشددة وتتحقق بتوفر ظرف التشديد وهو حذف أو تغيير أو تخريب هذا النظام بعد الدخول إليه والبقاء فيه[1]، وتبعا لذلك فإن جريمة الدخول والبقاء غير المشروع داخل النظام المعلوماتي يتمايزان فيما بينهما، فالدخول غير المصرح به يعتبر جريمة وقتية بينما يعتبر البقاء داخل النظام جريمة مستمرة،[2] وهو ما يقتضي وجود تمييز في الوسائل المستخدمة في ارتكاب كل واحد منهما.

تباينت مختلف التشريعات الوطنية حول جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي، ويعود ذلك أساسا إلى الطبيعة الخاصة والطابع التقني التي يتميز بها هذا النوع من الجرائم الالكترونية، وحداثتها مما أثار مشكلة اعتماد مصطلحات تقنية غير معهود التعامل بها، بالإضافة إلى الاختلافات حول أنماط صياغة النصوص التي تجرم الأفعال المكونة لها، فسنحاول أن نبين موقف بعض التشريعات التي عالجت هذا النوع من الإجرام بنصوص خاصة، وذلك على النحو التالي:

[1] - هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، ص.69.

[2] - مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص.51.

1 ـ القانون الفرنسي:

أفرد المشرع الفرنسي نصوصا تجرم الاعتداء بالدخول أو البقاء بطريق الغش أو التدليس إلى نظام المعالجة الآلية للمعطيات[1]، وهذا في المواد 1/323 إلى 7/323، فتعاقب المادة 1/323 منه الحبس لمدة سنتين وغرامة قدرها 6000 أورو، وعندما ينتج عن ذلك حذف أو تعديل البيانات الواردة في النظام، أو تغيير طريقة عمل هذا النظام، تكون العقوبة هي السجن لمدة ثلاث سنوات وغرامة قدرها 100000أورو. [2]

يلاحظ أن نص المادة 323-1 يتطلب أن يكون الدخول أو البقاء بالنظام المعلوماتي تم بطريق الغش أو التدليس، وبناء علية إذا كانت قاعدة البيانات مفتوحة للجمهور كان الدخول مشروع، ومع ذلك يكون البقاء متسما بعدم المشروعية، كما يلاحظ أن المشرع الفرنسي شدد العقاب إذا ترتب على فعل الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتوي عليها النظام، أو ترتب عليها تعطيل النظام عن القيام بعمله، وقد شدد المشرع العقاب في تلك الحالة نظرا لخطورة الأضرار الجسيمة المترتبة على تلك الأفعال[3].

2 ـ القانون المصري:

لم يضع المشرع المصري نصوصا تقرر تجريم الدخول غير المشروع و المساس بالبيانات الإلكترونية المحفوظة، لكن في قانون التوقيع الالكتروني ومشروع قانون التجارة الإلكترونية تضمنا نصوصا تتعلق بتجريم اختراق نظم معالجة البيانات[4]، ففي مشروع قانون التجارة

[1] ـ وسيم طعمة، السرقة المعلوماتية، مجلة جامعة البعث، المجلد 39، العدد68، 2017، ص.167.

[2]- Article 323-1 du C.P.F ,dispose que : « ***Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende .***

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende ».

[3] ـ أيمن عبد الله فكري، مرجع سابق، ص.271.

[4] ـ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.342.

الالكترونية المصري نصت المادة 26 منه على أنه: **" مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر يعاقب بالحبس وبغرامة لا تقل عن ثلاثة آلاف جنيه أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات أو قاعدة تتعلق بالتوقيعات الإلكترونية، ويعاقب بنفس العقوبة من اتصل أو أبقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة."**[1]

نص أيضا في قانون التوقيع الإلكتروني رقم 15 لسنة 2004 في المادة 123 منه على أنه: **" مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر يعاقب بالحبس وبغرامة ...أو بإحدى هاتين العقوبتين كل من...توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اختراق هذا الوسيط أو اعتراضه أو عطله عن أداء وظيفته"**[2].

3 ـ موقف المشرع الجزائري:

قام المشرع الجزائري بتجريم أفعال المساس بأنظمة الحاسب الآلي وذلك بموجب القانون رقم 04-15، المتضمن "**المساس بأنظمة المعالجة الآلية للمعطيات**"[3]، أين نص على عدة جرائم وهي:

ـ الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات[4] أو محاولة ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

---

[1] ـ المادة 20 من مشروع قانون التجارة الالكترونية المصري السالف الذكر .

[2] ـ المادة 123 من قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004السالف الذكر.

[3] ـ تمم الفصل الثالث من الباب الثاني من الكتاب الثالث بالقانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 ، ج. ر. عدد 71، ص11و12 قسم سابع مكرر تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**"، ويتضمن المواد من 394 إلى المادة 394 مكرر، ص.113.

[4] ـ هناك اختلاف بين المعلومات والمعطيات، إذ أن المعطيات تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للاستخدام، أما عن المعلومات فهي المعنى الذي يستخلص من هذه المعطيات.أنظر في ذلك : هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص.26. المعطيات تعتبر المادة الأولية التي تستخرج منها المعلومات باستخدام معالجة آلية في عملية الاستخراج، إذ يتم تجميع وتشغيل المعطيات للحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات، والتي يحصل تجميعها

- الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة.
- إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية.[1]
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، بالإضافة إلى حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[2]، فأدرك المشرع الجزائري من خلال المادة 394 مكرر من هذا القانون الطبيعة الخاصة في جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات، وحرص على تجريم الفعل والنتيجة، ويتجسد ذلك في فعل أو عدة أفعال مادية، ففي الحالة البسيطة أي الدخول والبقاء غير المشروعين في نظام المعالجة الآلية للمعطيات تكون العقوبة هي الحبس من 03 أشهر إلى سنة والغرامة من 50000 د.ج إلى100.000 د.ج، أما في الحالة المشددة فنفرق بين حالة توفر الحذف أو التغيير في المعطيات فهنا تكون العقوبة المضاعفة، أما في حالة توفر ظرف التخريب فتكون العقوبة الحبس من 06 أشهر إلى سنتين والغرامة من 50000 د.ج إلى 150000 د.ج.

يلاحظ أن المشرع جرم كل من الفعل الذي يقوم على الدخول غير المصرح به إلى النظام المعلوماتي، وميز هنا بين حالتين حالة فعل الدخول والبقاء في النظام المعلوماتي وحالة نتيجة الفعل، أين شدد المشرع الجزائري العقوبة إذا ترتب على الفعل نتيجة مباشرة والمتمثلة في حدوث أضرار بالمعطيات ونظم معالجتها.

يلاحظ أيضا من خلال هذه المادة أن المشرع أقر العقوبة لمجرد الدخول و البقاء في كل أو جزء من منظومة المعالجة الآلية للمعطيات بنية الغش، وعلى محاولة الدخول و البقاء بنية الغش، وتشدد العقوبة إذا ترتب على الدخول والبقاء حذف أو تغيير، كما عاقب على الأفعال المذكورة، إذا ترتب تخريب اشتغال المنظومة.

ومعالجتها مرة أخرى للحصول على معلومات إضافية، للمزيد راجع في ذلك : انتصار غريب، أمن الكمبيوتر والانترنت، دار الراتب الجامعية، بيروت، 1998، ص.81.

[1] - المادة 394 مكرر من قانون العقوبات الجزائري .

[2] - المادة 394 مكرر 2من قانون العقوبات الجزائري السالف الذكر.

ثانيا: أركان جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

يلزم لقيام جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات، أن يقوم المجرم المعلوماتي بنشاط خارجي ملموس، أو فعل مادي يعبر به عن إرادته في انتهاك نظم الحماية المعلوماتية من محاولا ت استهدافها، أو التعبير في البقاء داخل هذه النظم بنية الغش، فلقيامها إذن يتطلب اشتمالها على ركنين وهما الركن المادي والركن المعنوي، وعليه سنتعرض إلى الركن المادي الذي يتكون من نشاط إجرامي يتمثل في الولوج والبقاء في نظام المعالجة الآلية للمعطيات أولا، ثم نتناول الركن المعنوي لجريمة الدخول والبقاء والذي يتخذ صورة القصد الجنائي باعتبارها من الجرائم العمدية ثانيا، وذلك على النحو التالي:

1 - الركن المادي:

يتكون الركن المادي لهذه الجريمة المستحدثة من نشاط إجرامي يتمثل في فعل الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات أو في جزء منه[1]، أو البقاء غير المشروع، فتتحقق الجريمة بفعل الدخول إلى النظام المعلوماتي والذي يشكل الركن المادي في هذه الجريمة[2]، بحيث لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الالكتروني لهذا النظام، ويتساوى في هذا المجال أنه إذا تم هذا الدخول بطريق مباشر إلى المعلومات أو تم عن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي[3]، فالإذن يعني الدخول إلى موقع الكتروني أو نظام معلومات الكتروني، أو شبكات المعلومات بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير

[1]- Xavier linant de bellefonds, op.cit, p.250

[2]- تباينت مختلف التشريعات حول موقفها تجاه تحديد محل جريمة الدخول غير المصرح به على نظام المعالجة الآلية للمعطيات، وبذلك يمكن أن نميز ثلاث صور المحل هذه الجريمة، تتمثل الصورة الأولى في المعلومات في ذاتها، وتتمثل الثانية في أنظمة المعالجة الآلية للمعطيات التي لا ترتبط فيما بينها من خلال شبكة الاتصال، أما الصورة الثالثة فتتمثل في شبكات المعلومات، للمزيد راجع في ذلك: نائلة عادل قورة، مرجع سابق، ص.323.

[3] - نهلا عبد القادر المومني، مرجع سابق، ص.158.

مشروعة[1]، فقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له، ويدخل إلى كامل النظام أو إلى جزء آخر يحظر عليه الدخول إليها، وهذا الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي[2]، فلا تتطلب عملية الدخول إلى النظام المعلوماتي سوى تشغيل جهاز الحاسوب، وفي بعض الأحيان يتطلب ذلك أمورا أكثر تعقيدا كما هو الحال في محاولة الحصول على الرقم السري حتى يمكن الدخول إلى النظام، وقد يتم ذلك أحيانا أخرى باستخدام برامج خبيثة يتم دمجها في أحد البرامج الأصلية لجهاز الحاسوب حيث تعمل كجزء منه، وتقوم هذه البرامج بتسجيل الشفرات التي يستخدمها المستخدمون الشرعيون للدخول إلى النظام واستعمالها بعد ذلك لاختراق النظام المعلوماتي، وهناك وسائل تعتمد على ضعف الأنظمة ذاتها أو على الأخطاء الناجمة عن عملية البرمجة، ووسائل الدخول غير المشروع من الصعب حصرها لأنها تعتمد على التطور التقني في مجال المعلوماتية[3] .

تعد جريمة الدخول غير المشروع إلى النظام المعلوماتي من الجرائم الشكلية التي لا يتطلب قيام الركن المادي فيها نتيجة ما، وبالرغم من إمكانية حدوث أضرار معينة بالمعلومات بمحوها أو بتعديلها أو إفساد نظام التشغيل نتيجة عملية الدخول غير المصرح به[4]، إلا أن ذلك لا يغير من طبيعة الجريمة باعتبارها جريمة شكلية.

يمكن أن يكون البقاء غير المشروع حقا لاحقا على دخول قد تم بوجه مشروع، ويتحقق ذلك بتجاوز شخص النطاق الزمني أو الغرض المصرح له في الاتصال بنظام المعلومات[5]، والتي تفترض اختلاس وقت النظام وتتخذ صورة الجريمة المستمرة[1].

[1] ـ حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، المنصورة، 2015، ص.31.

[2] ـ مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دار النهضة العربية ، القاهرة، 2015 ، ص.81.

[3] ـ نهلا عبد القادر المومني، مرجع سابق، ص.158.

[4] ـ هناك بعض الأنظمة المعلوماتية القوية خاصة الطابعات السرية والتي تصدر عند أدائها لوظيفتها إشعاعات الكترومغناطيسية، وقد ثبت أنه بإمكان شاحنة صغيرة مجهزة تجهيزا خاصا وتقف بمحاذاة مبنى مكتظ بالحاسبات الآلية أين تلتقط وتسجل هذه الإشعاعات، ويمكن عن طريق جهاز فك الشفرة أن يطلب من طابعة متصلة بنظيرتها الموجودة في المركز المستهدف إتمام النسخ الحرفي لنفس المعلومات، للمزيد راجع في ذلك: عارف التميمي، شبكات الحاسوب والانترنت، دار اليازوردي العلمية، عمان، 1999، ص.74.

[5] ـ جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجيا الحديثة، مرجع سابق، ص.150.

يمكن أن يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وقد يجتمعان، ويكون البقاء معاقبا عليه وحده حين الدخول إلى النظام مشروعا، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام، ويدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك[2]، ويتحقق في هذا العرض الاجتماع المادي للجريمتين الدخول والبقاء غير المشروعين[3]، فبينما يتطلب الدخول اختراق الأنظمة الأمنية التي تحمي النظام، فإن فعل البقاء لا يتطلب ذلك لأن الدخول كان مشروعا[4].

تتحقق جريمة الدخول إلى النظام والبقاء فيه بأي وسيلة تقنية من ذلك مثلا :

ـ انتهاك كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها.

ـ عن طريق برنامج أو شفرة خاصة.

ـ استعمال الرمز السري لشخص آخر.

ـ الدخول من خلال شخص مسموح له بالدخول[5].

ـ يتحقق الدخول أيضا متى كان هذا الدخول مخالفا لإرادة صاحب النظام ومن له حق السيطرة عليه [6].

يمكن أيضا أن يتحقق الاتصال غير المشروع بطريقة خداعية، ويفسر تعبير" طرق الخداع" تفسيرا واسعا، فهو لا يتطلب أن يستخدم الجاني وسائل تدليسية في إحداث هذا الاتصال، بل يكفي أن يتحقق دون أن يكون الجاني مأذونا له به متى كان القصد الجنائي متوافر لديه[7]، يرى القضاء الفرنسي بأن نص المادة 1/323 يتطلب أن يكون الدخول أو البقاء بالنظام المعلوماتي تم بطريق الغش أو التدليس، وبناء عليه إذا كانت قاعدة البيانات مفتوحة للجمهور كان الدخول

---

[1] ـ نائلة فريد قورة، مرجع سابق، ص361. أحمد حسام طه تمام، مرجع سابق، ص301. أيمن عبد الله فكري، مرجع سابق، ص.270.

[2] ـ محمد أمين الشوابكة، مرجع سابق، ص.133. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية ، مرجع سابق، ص.52.

[3] ـ عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.89.

[4] ـ يعيش تمام شوقي ، خليفة محمد، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل الأبحاث القانونية المعمقة، العدد 25، السنة الثالثة، ماي2015 ، ص.20.

[5] - Xavier linant de bellefonds , Alain Hollande ,op.cit, p.328.

[6] ـ علاء عبد الباسط خلاف، مرجع سابق، ص.70.

[7] ـ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.34.

مشروع، ومع ذلك يكون البقاء متسما بعدم المشروعية كما اشترط المشرع الفرنسي في هذه المادة أن يتم إحداث تلك النتائج بطريق الغش أو أيا من المصطلحات التي تدل على تتطلبه لتوافر القصد العمدي في إحداث تلك النتيجة[1].

يترتب على عدم استيفاء هذه القيود أن يصبح الاتصال الإلكتروني غير مشروع، ويتوافر الخداع إذا تمكن الجاني من فك الشفرة السرية للدخول، بل ويتوافر الخداع أيضا إذا تمكن الجاني من استخدام كلمة السر أو الشفرة الحقيقية في هذا الدخول متى لم يكن مأذونا له بالدخول، ويستوي أن يكون الدخول على النظام قد تم مباشرة أو بطريق غير مباشر[2].

2 ـ الركن المعنوي (القصد الجنائي):

حتى يتوافر الركن المعنوي يجب أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء مع علمه بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به أو مشروع، أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل وجود خطر من جراء الدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول[3]، فهذه الجريمة تعد من الجرائم المستمرة[4]، فهي تبقى قائمة طالما أن الجاني مازال باقيا على الاتصال بنظام المعلومات الذي تم بدون قصد، فتوافر القصد الجنائي بعنصريه العلم والإرادة، لا يتأثر بالباعث على الدخول أو البقاء، فيضل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام.

يعد القصد الجنائي في جرائم الدخول إلى نظام معالجة البيانات أو البقاء فيه بحكم طبيعته جريمة عمديه، إذ أنه من المفترض أن أفعال العرقلة تعطيل لا تكون إلا عمديه وهذا ما يميزه

[1] ـ أيمن عبد الله فكري، مرجع سابق، ص.278.

[2] ـ مدحت عبد الحليم رمضان، مرجع سابق، ص.51.

[3] ـ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.137.

[4] ـ يتفق الفقه على أن جريمة البقاء جريمة مستمرة، لأن الفترة الزمنية التي تستمر فيها جريمة الدخول قصيرة نسبيا بحيث يمكن اعتبارها مستمرة أو وقتية ذات أثر ممتد، راجع في ذلك: جميل عبد الباقي صغير، جرائم التكنولوجيا الحديثة، مرجع سابق، ص.59.

عن الاعتداء غير العمدي لسير النظام، والذي يشكل ظرفا مشددا لجريمة الدخول والبقاء غير المشروع داخل النظام[1].

لقيام القصد الجنائي يجب أن يعلم الجاني بأنه يدخل إلى موقع لا يجوز له الدخول فيه أو البقاء فيه[2]، وأن تتجه إرادته إلى ذلك، بحيث يعلم ويدرك الجاني بأن السلوك الذي يقترفه يمثل اعتداء غير مشروع، فهو يعلم بماهية سلوكه الإجرامي من حيث ضرورة العمل من أجل الحصول على الأرقام السرية واسم المرور إلى المواقع، ومحاولة اختراق جدران الحماية الإلكترونية حتى ولو تم تغييرها بواسطة التشفير.

يؤكد كل هذا توفر القصد الجنائي بمعنى الإرادة الإجرامية لدى الجاني[3]، ومن ثم لا تتوافر إذا كان الدخول أو البقاء قد تم بطريق الخطأ، وتطبيقا لذلك ينتفي القصد الجنائي إذا ثبت أن الجاني قد دخل على قواعد البيانات مصادفة وأنه كان وليد خطأ ولم يكن فعله كاشفا عن توافر هذا القصد، ومن القرائن الدالة عليه 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 بسرقة هذه البطاقة أو بكسر هذه الشفرة، وإذا توافر القصد الجنائي فإنه لا عبرة بالبواعث التي تكون وراء قيام الجاني بفعله، فيستوي أن يكون هذا الدخول قد تم بدافع الفضول أو حب الاستطلاع أو إثبات القدرة على التغلب على قيود النظام، أو أن يكون الغرض هو الاستفادة من المعلومات والبيانات التي تحتويها السجلات وقوائم البيانات الالكترونية، أو القيام بأي عمل آخر غير مشروع[4]، فالقصد الجنائي إذن مفترض يستنتج من طبيعة الأفعال المجرمة[5].

[1] ـ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.142.

[2] ـ شيماء عبد الغني عطا الله، الحماية الجنائية للمعاملات الالكترونية، مرجع سابق، ص.126.

[3]- رضا متولي وهدان، النظام القانوني للعقد الالكتروني والمسؤولية عن التعاقدات الالكترونية، مرجع سابق، ص.140. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص.67.

[4]- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.35.

[5] ـ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، نفس المرجع، ص.142.

الفرع الثاني

جريمة الإتلاف في مجال المحررات الإلكترونية

يهدف الجاني من خلال ارتكابه جرائم المحررات الالكترونية إتلاف البيانات المعالجة آليا والمعلومات المخزنة بالنظام المعلوماتي، وينصب الإتلاف على نوعين: فالنوع الأول هو الذي تنصب أفعال الإتلاف على نظام التشغيل الذي يحتوي المحرر الالكتروني فيؤدي بالتبعية إلى إتلافه، والنوع الثاني هو الذي ينصب على إتلاف البيانات التي يحويها المحرر، كما يشكل الإتلاف العمدي محو المعلومات داخل البرامج أو البيانات من أسهل طرق الإتلاف، كون أنه من خصائص الجرائم الالكترونية قدرة الجاني على محو وتدمير آثار الجريمة بسرعة وفي وقت وجيز، وذلك بالضغط على زر المحو على لوحة المفاتيح و تشويشها على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال، فالتشريعات المقارنة أخذت أغلبها بعين الاعتبار طبيعة المال المعلوماتي بوصفه مال لا مادي، وبالتالي يعد محلا للإتلاف، وعليه سنتناول في هذا الفرع موقف التشريعات المقارنة من جريمة الإتلاف في مجال المحررات الالكترونية **(أولا)**، لنتناول أركان جريمة الإتلاف في المحررات الالكترونية **(ثانيا)**، ثم وسائل وأساليب الإتلاف في المحررات الالكترونية **(ثالثا)**.

أولا: موقف التشريعات المقارنة من جريمة الإتلاف في مجال المحررات الالكترونية

يعرف الإتلاف بأنه التأثير في مادة الشيء على النحو الذي يذهب ويقلل من قيمته الاقتصادية، عن طريق الإنقاص من كفاءته للاستعمال في الغرض الذي أنشأ من أجله[1]، والعبرة بالإتلاف في المحرر الالكتروني هو الذي يقع على المكونات المعنوية للنظام المتمثل

[1] - جميل عبد الباقي صغير، مرجع سابق، ص153. هدى حامد قشوش، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة من 25- 28 أكتوبر1993، ص.564. عفيفي كمال عفيفي، مرجع سابق، ص.183.

في المعلومات المنظمة في البرنامج المعلوماتي[1]، أو هو جعل الشيء غير صالح للاستعمال بإعدام صلاحيته أو تعطيله (وقف عمله) سواء بصفة كلية أو جزئية[2].

تقع جريمة الإتلاف في نطاق المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسيب وشبكاته الداخلية (المحلية)- أو العالمية (الإنترنت)- ويكون ذلك بطريق التلاعب بالبيانات، سواء بإدخال معلومات مصطنعة أو بإتلاف المعلومات المخزنة بالحواسيب والمتبادلة عبر الشبكة العالمية بمحوها أو تعديلها أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي، بما يؤدي إلى إعاقة سير عمل النظام الآلي بصوره المختلفة[3].

2 ـ تعريف جريمة الإتلاف في المحررات الالكترونية في التشريعات المقارنة:

قامت بعض التشريعات الوطنية باستحداث نصوص الإتلاف التقليدية وتعزيزها بنصوص مستحدثة تعالج فيها إتلاف المعطيات المعلوماتية، والبعض الآخر حسم الخلاف الدائر حول هذه المسألة بإصدارها تشريعات خاصة حول جريمة الإتلاف المعلوماتي.

أ ـ القانون الفرنسي:

جرم المشرع الفرنسي جريمة تعطيل أو تغييب تشغيل نظام معالجة البيانات (المادة 323-2) وتتحقق هذه الجريمة بصورة مختلفة، فقد تكون وسيلة التعطيل مادية كما لو وقع على الأجهزة عنف أو تخريب أو قطع وسائل الاتصال مما أدى إلى تعطلها، وقد تتحقق بوسيلة معنوية مثل إدخال فيروس في نظام التشغيل، ويستوي مع التخريب أن يقوم الجاني بتشويه المعلومات

[1] ـ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص.137.

[2] ـ جميل عبد الباقي الصغير، مرجع سابق، ص.153. أحمد حسام طه تمام، مرجع سابق، ص.346. محمد أمين أحمد الشوابكة، مرجع سابق، ص.216.

[3] ـ يجب التمييز بين الإتلاف بمعناه إفناء مادة الشيء أو هلاكه كليا، وبين التخريب الذي يقصد به توقف الشيء تماما عن أن يؤدي منفعته حتى ولو لم تفنى مادته، سواء كان هذا التوقف كليا أو جزئيا، ويكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل، أمل التعطيل فيكون بتوقف الشيء عن القيام بوظيفته فترة مؤقتة للمزيد راجع في ذلك: علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص.111.

المخزنة على نحولا يجعلها غير صالحة للاستعمال، وأما التغييب فهو لا يؤدي توقف الأجهزة عن العمل، وإنما يؤدي إلى جعلها لا تعمل بصورة معتادة مما يؤثر على أدائها.

يلاحظ أن تعطيل جهاز الحاسب المخزن به المستندات و الوثائق الإلكترونية عن العمل لا يدخل في مدلول التخريب والتغييب في تطبيق نص المادة 332-2 من قانون العقوبات الفرنسي، وإنما يعتبر من قبيل الإتلاف المادي المعاقب عليه طبقا لنص المادة 322-2 من قانون العقوبات الفرنسي[1].

يمكن القول بأن هذه النصوص تعاقب على مختلف صور الإتلاف التي يمكن أن تلحق بسير العمل في نظام المعالجة الآلية للبيانات، ولا سيما نص المادة 323 ويعاقب المشرع على الشروع في الجرائم الواردة فيها بذات العقوبة المقررة للجريمة الكاملة.

تجدر الملاحظة بأن جريمة إعاقة سير العمل في نظام المعالجة الآلية للبيانات التي جاء بها القانون الفرنسي الجديد تدخل في مجال قانون العمل، وفي مجالات أخرى كجريمة عمل لجنة المعلوماتية والحريات.[2]

يستند هذا الرأي إلى القول بأن المشرع توسع في قاعدة الحماية لسير نظم المعلوماتية من حيث الدخول فيها وإلغاء المعطيات التي يحتويها نظرا لخطورة هذه الأفعال، وذلك لأن الهدف المتوخى هو الوصول إلى تجريم هذه الأفعال، حتى وأن تعلق الأمر بنظم معلوماتية عامة ومفتوحة للجمهور ولا سيما نظم العمل الداخلية وقطاعات المعلومات الحساسة[3].

أصدر المشرع الفرنسي قانون 5جانفي 1988 المتعلق بجرائم الغش المعلوماتي، ثم قام بتعديل هذا النص في سنة 1994 ليتواكب مع خطورة ظاهرة الإجرام المعلوماتي، حيث تم تعديله بموجب المادة 1/323 لتكون عقوبة جريمة الدخول غير المشروع والبقاء داخل نظام المعالجة الآلية للبيانات، و الحبس سنة ومائة ألف فرنك غرامة، وفي حالة ما إذا نتج عن هذا

[1] - طارق سرور، مرجع سابق، ص.86.

[2] - أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص.350.

[3] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.227.

الدخول محو أو تعديل في المعلومات أو إتلاف تكون العقوبة الحبس سنتين ومائتين ألف فرنك غرامة.

نص أيضا في المادة 3/323 على معاقبة كل من: " **أدخل بيانات بطريق الغش في نظام معالجة البيانات أو محي أو عدل البيانات التي يحتوي عليها النظام بطريق الغش**"، وقد طبقت محكمة النقض الفرنسية المادة 3/323 على قيام أحد الأشخاص بتعديل وإلغاء لمعلومات تتعلق باللوائح المطبقة بإحدى الشركات بطريق العمد، وقد أقرت المحكمة بأنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات تم ارتكابها بواسطة شخص ليس له حق الدخول في النظام ولا يشترط أن يتوافر لدى الجاني نية الإضرار، وبناء على ذلك أيدت حكم محكمة الاستئناف الذي أدان المتهم عن هذه الجريمة بعدما استخلصت أركانها من قيام الشخص بتعديل البيانات والتي سبق وان قام بتسجيلها بطريقة نهائية على نظام آلي للمحاسبة كن يقوم بالإشراف عليه[1].

لا يحمي المشرع الفرنسي بهذا النص النظام من الناحية المادية، ولكنه يوفر بهذا النص الحماية للبيانات الموجودة بالنظام من أي نشاط إجرامي[2]، تتضمن هذه الجريمة صورا ثلاثة : الإدخال، المحو، التعديل، ولا يشترط أن تتوافر هذه الصور جميعا، بل يكفي لتحقق الجريمة أن تتوافر إحداها، وموضوع الجريمة هو المعلومات التي تتم معالجتها إلكترونيا ، وهو ما يعني شمولها لكافة البيانات الواردة في المستندات الالكترونية، ويقصد بفعل الإدخال إضافة بيان جديد على النظام، ويستوي في ذلك وجود بيانات سابقة تم إضافة البيان الجديد إليها، أو أن يكون موضع الإضافة كان خاليا من البيانات قبل تحققها[3].

عاقب المشرع الفرنسي على المساهمة في جماعة أو الاتفاق بين مجموعة من الأشخاص، للتحضير بعمل أو أعمال مادية بقصد ارتكاب جريمة أو أكثر، من جرائم تعطيل أو تغييب أو

[1] - أيمن عبد الله فكري، مرجع سابق، ص.286.

[2] - مدحت عبد الحليم رمضان، مرجع سابق، ص.55.

[3] - أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.29.

المساس ببيانات نظام معالجة البيانات (المادة 323- 4)[1]، ويمثل هذا النص خروجا عن القواعد العامة في التجريم، إذ يعاقب المشرع الفرنسي على الأعمال التحضيرية، ويعلل ذلك الخروج هو رغبته في كفالة حماية وقائية لنظم المعلومات و البيانات الإلكترونية، ويعاقب أيضا على هذا النشاط بعقوبة الجريمة الأصلية، ويلاحظ أنه إذا تمت الجريمة التي تم التحضير لها بالفعل وساهم الجناة فيهما، فإننا نكون بصدد تعدد مادي للجرائم لا يقبل التجزئة، على أنه يجب أن تتوافر علاقة السببية في هذه الحالة بين الأفعال التحضيرية وبين الجريمة التي ارتكبت.

أجاز المشرع الفرنسي مساءلة الأشخاص المعنوية عن ارتكاب صورتي الإتلاف المنصوص عليهما في المادة 232-2 من قانون العقوبات الفرنسي، وذلك طبقا للنصوص العامة التي تقرر المسؤولية الجنائية لهذه الأشخاص (المادة 323- 6)[2]، وقد يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا فيها، كما أنه يسأل عن الجريمة التامة أو الشروع فيها، غير أنه يجب لتحقق هذه لمسؤولية أن يثبت أن الجريمة قد ارتكبت بواسطة أحد أعضاء أو ممثلي الشخص المعنوي وأن تكون قد ارتكبت باسم أو لحساب هذا الشخص[3].

يلاحظ أيضا أن المشرع الفرنسي لم يوضح في شرط وقوع الجريمة أن يكون هناك إتلافا كليا أو جزئيا للمعطيات كمحو أو تعديل المعلومة أو تشويهها، أو أنه يكفي لوقوع الجريمة هو فقط مجرد الإضرار بسير العمل في نظام المعالجة الآلية للمعطيات.

[1] - Article 323-4 du C.P.F Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004, dispose que: « ***La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée*** ».

[2] - Article 323-6 du C .P .F Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124: « ***Les personnes morales déclarées responsables pénalement …*** ».

[3] - أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.30.

ذهب البعض إلى أن مجرد عرقلة العمل بالنظام يؤدي إلى قيام الجريمة، ومرد ذلك أن هذه الحالة هي نفسها كحالة محو أو تعديل أو إلغاء المعلومات، بل هي تأخذ شكلا أكثر اتساعا من الأشكال المتبعة في قرصنة المعلومات، وبالتالي فإن النص ينطبق على كل إضرار بسير العمل، سواء نجم عنه إتلاف للمعطيات أو كان يمكن أن يؤدي إلى ذلك، فالشروع في هذه الجريمة معاقب عليه بذات العقوبة المقررة للجريمة الكاملة[1].

ذهب البعض الآخر إلى أن المادة (2/323 و3) تنطبق على كل اعتداء على سير النظام المعلوماتي أو الدخول فيه بطريقة غير شرعية أو إتلاف أو إلغاء المعلومات في النظام المعلوماتي الخاص المغلق أو النظام المفتوح، رغم ما يثيره هذا التفسير من مخاطر[2]، كما أنه لم يضع شروطا حول طبيعة المعلومات، ولكن النص جاء عاما شاملا كافة المعلومات[3].

ب ـ القانون المصري:

نص المشرع المصري في المادة23 فقرة (ب) من قانون التوقيع الالكتروني على أنه: **" كل من أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر"[4].**

يلاحظ أن المشرع المصري عاقب على فعل الإتلاف الذي يقع على المحرر الالكتروني، فكل إتلاف مهما كانت صورته سواء كانت بالولوج إلى نظم المعلوماتية أو بالتأثير عليها عن طريق الاصطناع، أو قيام الجاني بتعديل البيانات والمعلومات بأي شكل من الأشكال أو بأية طريقة كانت، كما يلاحظ أن المشرع يجرم الاعتداء على المحررات الالكترونية بنص واحد يشمل كل من الإتلاف والتعييب والتزوير بدلا من النص على كل جريمة على حده.

[1] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.225.

[2] - أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص.353.

[3] - Michel Bibent, Le Droit du traitement de l'information, Nathan, Paris,2000, p.121.

[4]- المادة 23 من قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004.

ج ـ موقف المشرع الجزائري:

نص المشرع الجزائري على جريمة الإتلاف المعلوماتي في نص المادة 394 مكرر من قانون العقوبات على أنه: **" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000دج إلى 150000دج".**

أضاف في المادة 394 مكرر 1 بنصه على أنه: **" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 د.ج إلى 2000000 د.ج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها "**[1].

يلاحظ أن المشرع الجزائري لم يدرج جريمة الإتلاف المعلوماتي كجريمة مستقلة بحد ذاتها، وإنما نص على تجريمها في الإتلاف غير المباشر لمنظومة المعالجة الآلية للمعطيات أو الشروع في جريمة الدخول غير المشروع، وهذا بخلاف المشرع الفرنسي الذي أدرجها في نصوص مستقلة تشكل جريمة بحد ذاتها، كما أن المشرع الجزائري عاقب بظرف مشدد على الاعتداءات العمدية على المعطيات الموجودة داخل النظام وعلى المساس العمدي بالمعطيات خارج النظام، سواء كانت هذه المعطيات مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية، ما دامت تستعمل كوسيلة لارتكاب هذا النوع من الجرائم، بحيث أنه لم يشترط اجتماع هاذين النوعين من الاعتداء العمدي، بل يكفي أن يصدر عن الجاني إحداهما فقط حتى تقوم الجريمة، كما أضاف في المادة 394 مكرر 1، أن جريمة الإتلاف تقوم أيضا عند إدخال معطيات جديدة لم تكن موجودة من قبل، عن طريق الغش على نظم المعالجة

[1] ـ المادة 394 مكرر والمادة 394 مكرر1 من قانون العقوبات الجزائري .

الآلية للمعطيات، وذلك بهدف إزالة أو تعديل أو محو يكون الغرض منه التأثير على صحة البيانات والمعلومات التي يتضمنها على وجه الخصوص المحررات الإلكترونية.

ثانيا : أركان جريمة الإتلاف في المحررات الالكترونية

تأخذ جريمة الإتلاف في نطاق المعلوماتية إما صورة الإتلاف المادي، وذلك بالاعتداء على المكونات المادية للحاسب الآلي من أجهزة، ودعامات وشرائط، وأقرا ص ممغنطة وما تحتويه من معلومات وشاشات، وكوابل، وغير ذلك، وهنا لا تثار أية عقبة قانونية في تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف على مثل هذه الاعتداءات، وهو ما يسمى بالإتلاف المادي.

يتخذ الإتلاف صورة الاعتداء على البرامج أو البيانات والمعلومات المخزنة في قواعد الحاسب الآلي والمتبادلة بين الحواسيب عبر قنوات الاتصال في شبكة الانترنت، سواء تم ذلك بمحوها أو تعديلها أو تغيير نتائجها وهو ما يسمى بالإتلاف المعنوي.

1- الركن المادي لجريمة الإتلاف في المحررات الالكترونية:

يتمثل جوهر الإتلاف في تخريب الشيء محل الإتلاف أو الانتقاص من منفعته بمعنى يجعله غير صالح للاستعمال أو تعطيله[1]، ويتحقق الركن المادي لإتلاف البيانات المعلوماتية بإتلافها أو تخريبها أو تعطيلها أو بجعلها غير صالحة للاستعمال[2].

تتحقق جريمة الإتلاف بتحقق إحدى هذه النتائج، أما التعديل الذي يمكن أن يتخذ صورة الإضافة أو الحذف أو التغيير في البيانات ذاتها، فنجد أن المشرع الفرنسي فرق بين تطبيق القواعد العامة في التزوير وبين جريمة الإتلاف، فجريمة التزوير تتعلق بالبيانات ذاتها وهي غير ملائمة له في تلك الصورة من صور العبث بالبيانات[3].

[1] - هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، مرجع سابق، ص.564.

[2] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.219.

[3] - شيما عبد الغني عطا الله، الحماية الجنائية للتعاملات الالكترونية، مرجع سابق، ص.13.

2- الركن المعنوي لجريمة الإتلاف:

تعتبر جريمة الإتلاف من 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 للاستعمال مما يؤدي إلى إلحاق الضرر به[1]، وبناءا عليه إذا اعتقد الجاني أن البيانات المعلوماتية المادية محل الإتلاف مملوكة له، فإن القصد الجنائي ينتفي لديه لعدم العلم كمن يعتقد ملكيته لأقراص ممغنطة أو أجهزة حاسب ألي أو ملحقاته ثم يثبت ملكيتها للغير.

يتعين بالإضافة إلى توافر العلم بذلك أن تتجه إرادة الجاني إلى تحقيق نتيجة فعله، وذلك بإحداث الإتلاف أو التخريب أو التعطيل بشكل يؤدي إلى توافر الضرر الناتج عن فعله، ولذلك إذا كان الإتلاف غير مقصود كما لو حدث شيء عارض وتسبب في إتلاف جزء من الحاسب الآلي أو معداته وملحقاته، فإن الفاعل يسأل عن الخطأ نتيجة إهماله أو رعونته أو تقصيره، كمن يستخدم قرص ممغنط في جهاز الحاسب الآلي يحتوي على فيروسات مما يؤدي إلى الإضرار به أو دون أن يستخدم مضاد الفيروسات[2].

يجب إذن حتى تقوم جريمة إتلاف المحرر الالكتروني أن يتوفر القصد الجنائي لكونها من الجرائم العمدية، كما جاء في نص المادة 323 فقرة 2 من قانون العقوبات الفرنسي والذي استعمل المشرع الفرنسي عبارة "سوء النية"، فمع توافر العلم والإرادة في هذه الجريمة تطلب توافر نية إحداث الضرر بالغير.

ثالثا : وسائل وأساليب الإتلاف في المحررات الالكترونية

يقوم الإتلاف على عدة وسائل وأساليب تتنوع خطورتها من أسلوب إلى آخر فأهم هذه الوسائل وأكثرها ضررا هو استخدام الفيروسات[3]، والتي تتميز بالتكاثر والانتشار من نظام إلى

[1] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.221..

[2] - نهلا عبد القادر المومني، مرجع سابق، ص.131.

[3] - نائلة عادل محمد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، مصر، 2005، ص.192.

آخر واختفائها مما يشكل صعوبة في اكتشافه، وتقوم بتدمير البرامج وتغيير المعلومات دون ترك، كما يمكن استخدامه لأغراض حمائية للنسخ الأصلية من خطر النسخ غير المرخص به، ومن بين الوسائل كذلك البرامج المنطقية والزمنية[1] أو ما يصطلح عليه بالقنبلة المعلوماتية.

لا يوجد تجريم لإتلاف المحرر الالكتروني على نحو أصيل، وإنما يمكن التوصل إلى حماية هذا المحرر من الأفعال التي تعتبر إتلافا له بصورة غير مباشرة، وذلك من ناحيتين :

- أن تنصب أفعال الإتلاف على نظام التشغيل الذي يحتوي المحرر الالكتروني ، فيؤدي بالتبعية إلى إتلاف هذا المحرر[2].
- أن ينصب الإتلاف على البيانات التي يحتويها المحرر وفي هذه الحالة تكون الحماية مقررة للبيانات الإلكترونية بصفة عامة، غير أنها تمتد بطريق التبعية إلى المحرر الإلكتروني بمعناه الدقيق[3].

يقع الإتلاف على النظام المعلوماتي، سواء أكان ذلك بالدخول العمدي للنظام المعلوماتي أو باستخدام الجاني الطرق التقنية والفنية للإتلاف كالفيروسات، أو كان ذلك نتيجة الخطأ أثناء التواجد بالنظام أو الخروج منه.

1 - إعاقة سير العمل في نظام المعالجة الآلية للمعطيات:

يتمثل إعاقة سير العمل في النظام المعلوماتي في فعل بسبب تباطؤ عمل نظام المعالجة الآلية للبيانات أو إرباكه، مما يؤدي إلى تغيير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت[4].

تتمثل أساليب الإعاقة في تعديل البرامج في نظام المعالجة أو عمل برنامج احتيالي [5]، أو إذا قام الجناة بإرسال عدد كبير من الرسائل الالكترونية إلى أحد المواقع مما أدى إلى ارتباك العمل بها وتعطيلها[1].

---

[1] - نهلا عبد القادر المومني، مرجع سابق، ص.132.

[2] - أشرف توفيق شمس الدين، حماية المستند الإلكتروني، مرجع سابق، ص.543.

[3] - أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.28.

[4] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.223.

[5] - عمر الفاروق الحسيني، مرجع سابق، ص.75.

2 ـ الاعتداء على البيانات داخل نظام المعالجة الآلية للبيانات:

لا يعني الاعتداء أو المساس ببيانات نظام المعالجة بإدخال بيانات أو محوها أن نكون بصدد صورة من صور تزوير هذه البيانات، وإنما الأثر الذي يحدثه هذا المساس بتلك البيانات هو إتلاف النظام وعدم قدرته على القيام بعمله[2]، فالاعتداء على البيانات والبرامج داخل النظام المعلوماتي بإتلافها يتخذ إحدى الصورتين:

الصورة الأولى : أن يتم محو البيانات والمعلومات كلية وتدميرها إلكترونيا.

الصورة الثانية : أن يتم تشويه المعلومة أو البرامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل الصورة الثانية: أن يتم تشويه المعلومة أو البرامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل انتقالها[3].

3 ـ الطرق الفنية لإتلاف البيانات والبرامج:

تعتبر مسألة إمكانية حدوث خلل ما يؤثر على أمن البيانات[4] واردة بحسب الطبيعة التقنية والفنية لوسائل الاتصال خاصة والوسائل التكنولوجية بصفة عامة، إذ قد يحدث وأن تتأثر

---

[1] ـ جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية ، القاهرة، 2012، ص.63.

[2] ـ أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مرجع سابق، ص.29.

[3] ـ هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن ، مرجع سابق، ص.567.

[4] ـ يعبر عن مصطلح البيانات بالأمور التالية:

أ- السرية والموثوقية: بمعنى أن تكون البيانات المتداولة عبر الأجهزة التكنولوجية في مأمن من أن تكون عرضة لإطلاع الغير عليها، وبالتحديد الأشخاص غير المخولين بالإطلاع عليها.

ب- التكاملية وسلامة المحتوى: يقصد بها أن تكون تتم عمليات نقل المعلومات والبيانات قد تمت بطريقة سليمة، وأن محتوى تلك البيانات لم يتعرض لا للتحريف ولا للتشويه ولا العبث به خلال مراحل النقل والمعالجة، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع.

ج- استمرارية توفر المعلومات أو الخدمة: التأكد من استمرار عمل النظام المعلوماتي، واستمرار تقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات سيكون بوسعه في أي وقت الدخول والإطلاع على تلك البيانات أو المعلومات.

د- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به، ويقصد به ضمان تحديد الشخص الذي قام بتصرف ما متصل بالمعلومات وسد الطريق على أي محاولة من جانبه لإنكار قيامه بالتصرف.راجع في ذلك: رامي علي وشاح ، الصعوبات المادية التي تعترض الإثبات بالمحررات الالكترونية، مرجع سابق، ص.50.

البيانات والمعلومات المتناقلة بواسطتها إلى خلل قد يؤدي إلى مسح جزئي أو كلي لتلك البيانات، نتيجة لضعف برامج تشغيل تلك الأجهزة أو بسبب إصابة ذاكرتها بفيروسات تؤثر على أدائها.

أ- فيروسات الحاسب الآلي:

يتزايد خطر إطلاق الفيروسات يوما بعد يوم ، فلا يكاد يوم يمر دون ظهور فيروس جديد يستهدف أجهزة الحاسب الآلي التي تستخرج منها المحررات الالكترونية، وأن هذه المخاطر ستؤدي إلى عزوف مستخدمي أجهزة الحاسب الآلي والإنترنت عن استخدامها.[1]

يتزايد خطر إطلاق الفيروسات يوما بعد يوم، فلا يكاد يمر يوم دون ظهور فيروس[2] جديد يستهدف أجهزة الحاسب الآلي التي تستخرج منها المحررات الالكترونية، وأن هذه المخاطر ستؤدي إلى عزوف مستخدمي أجهزة الحاسب الآلي و الانترنت عن استخدامها[3]، وتتميز فيروسات الحاسب الآلي عن غيرها من البرامج التخريبية الأخرى، هو إنتاجها نسخا من نفسها، وقدرتها أثناء عملية الإنتاج الذاتي على التغيير و التطور والتكييف مع البرامج المتنوعة وبقدرتها الفائقة على الاختفاء والاختراق و التدمير، تلحق أضرارا بالغة باستخدام المحررات الالكترونية، لا سيما عند نسخ برامج المعلومات من مستخدم إلى آخر، إذ تحتوي هذه البرامج والمعلومات على أسرار معلومات في الغالب، تكون ذا قيمة مالية كبيرة [4]، وتستخدم الفيروسات في أحد غرضين حمائي وتخريبي:

[1] - رامي علي وشاح، الصعوبات المادية التي تعترض الإثبات بالمحررات الالكترونية، مرجع سابق، ص.49.

[2] - يستخدم مصطلح فيروس ليشير إلى بعض البرامج المصممة للإضرار بأجهزة الحاسب الآلي، فهذه البرامج تبدو مثل الألعاب ولكنها في الحقيقة تقوم بتهيئة الأقراص الصلبة وتمسح جميع البيانات الموجودة فوقها وتنتقل الفيروسات من جهاز لأخر عن طريق الأقراص والفلاش قي الغالب، ويمكن أن تنتقل الفيروسات عبر كامل الشبكات لذلك قد تتعرض أجهزة الحاسب الآلي المرتبطة بالشبكات لهجوم الفيروسات بصفة مستمرة: للمزيد من التفاصيل : راجع: محمد دباس الحميد، حماية أنظمة المعلومات، دار حامد، عمان، 2005، ص.54.

[3] - عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص.98.

[4] - محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.160.

1- الغرض الحمائي:

يكون ذلك لحماية البيانات والبرامج من خطر النسخ غير المشروع، إذ ينشط الفيروس بمجرد النسخ ويدمر نظام الحاسب الذي يعمل عليه.

2- الغرض التخريبي:

يكون ذلك بهدف الدعاية أو الابتزاز، حيث يرمي واضع الفيروس للتخريب بهدف التخريب ذاته أو بهدف الحصول على منافع شخصية[1].

ب – خصائص الفيروس:

تتميز فيروسات الحاسب الآلي عن غيرها من البرامج التخريبية الأخرى، هو إنتاجها نسخا من نفسها، وقدرتها أثناء عملية الإنتاج الذاتي على التغيير و التطور والتكييف مع البرامج المتنوعة وبقدرتها الفائقة على الاختفاء والاختراق والتدمير[2]، تلحق أضرارا بالغة باستخدام المحررات الالكترونية، لا سيما عند نسخ برامج المعلومات من مستخدم إلى آخر، إذ تحتوي هذه البرامج والمعلومات على أسرار معلومات في الغالب، تكون ذات قيمة مالية كبيرة، وتعدد أنواع الفيروسات التي تصيب برامج الحاسب الآلي، فمنها الفيروسات الدودية والقنابل الموقوتة وأحصنة طروادة، ولا نريد الخوض في تفاصيل هذه الفيروسات لأنها تتعلق بأمور فنية.
يتميز فيروس الحاسب الآلي بعدة خصائص:

- العدوى:

فهو برنامج يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب، وعند تحميل البرنامج ينتقل الفيروس من جهاز إلى آخر بسرعة فائقة وينتشر داخل الذاكرة وينسخ نفسه بسرعة غير عادية[3].

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

[2] - عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها ، مرجع سابق، ص.99.

[3] - محمد حسين منصور، المسؤولية الالكترونية، مرجع سابق، ص.292.

ـ الاختفاء:

يتميز فيروس الحاسب بالقدرة على الارتباط بالبرامج الأخرى و التخفي من مستخدم الجهاز والتمويه عليه كالدخول في ملفات مخفية أو موضع الذاكرة.

ـ الاختراق:

يتميز الفيروس بقدرة فائقة على دخول النظام والتسلل إليه واختراق كل سبل الحماية التي يضعها المستخدم.

ـ التدمير:

لعل أهم أعراض الإصابة هو بطئ تشغيل النظام الإلكتروني، حيث يصيب عامل السرعة كأهم ميزة في النظام، ثم يقوم بمسح البيانات المخزنة على وسائط التخزين ويؤدي إلى شغل ذاكرة الجهاز على نحو يتعذر التعامل مع البيانات أو المعلومات وتتوقف الاستجابة لنظام التشغيل[1].

ج ـ أساليب الحماية من الفيروس:

نظرا لخطورة الفيروس الجسيمة وآثاره المدمرة على النشاط المعلوماتي والتجارة الإلكترونية، ظهرت ما يسمى بأساليب الوقاية والتي تتمثل في:

- اتخاذ الإجراءات الاحتياطية لمنع الإصابة بالفيروس أو انتشاره، حيث ينبغي توخي الحيطة والحذر بصفة دائمة نظرا لكثرة و تعدد وتطور أنواع الفيروسات، ومن ثم يتعين البحث عن الحلول المستمرة.
- مراجعة نظام التشغيل و الملفات بشكل دوري ومستمر بحثا عن الفيروسات، ومراجعة الأجهزة من وقت لأخر درءا لخطر الفيروس[2].

[1] ـ محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.162.

[2] ـ هشام محمد فريد رستم، مرجع سابق، ص.157.

1 ـ برامج الدودة:

يتميز هذا النوع من البرامج أنه لديها إمكانية تعطيل أو إيقاف نظام الحاسب بصورة كاملة وذلك عن طريق استغلال أي خلل أو فجوة في نظام تشغيل الحاسب متنقلة من حاسب لآخر لتغطي الشبكة بأكملها ، فهذا النوع قد ينتقل من شبكة إلى أخرى من خلال الموصلات الرابطة بينهما وأثناء عمليات انتقالها وقد يتكاثر عددها عم طريق إنتاج نسخ منها[1].

تستهدف هذه البرامج أساسا شغل أكبر ممكن من سعة الشبكة مما يؤدي إلى التقليل أو الخفض من قدراتها، وقد تتجاوز ذلك في بعض الأحيان وتقوم بأعمال تخريب حقيقية للملفات والبرامج وأنظمة تشغيل الحاسب وبروتوكولات الاتصال الخاصة به[2].

2 ـ القنابل المنطقية أو الموقوتة أو الزمنية:

القنبلة المعلوماتية اصطلاح يطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف، ويمكن أن نقسم القنبلة المعلوماتية إلى قسمين: القنبلة الزمنية أو الموقوتة والتي هي 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، أما القنبلة المنطقية فهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو في كل فترة زمنية منظمة، ويتم وضعه في الشبكة المعلوماتية بهدف تحديد ظروف أو حالة سكون لمدة معينة قد تطول أو تقصر[3].

يتميز هذا النوع من القنابل بأنه عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة النظام بغرض تسهيل تنفيذ عمل غير مشروع.

[1] ـ عفيفي كامل عفيفي، جرائم الكمبيوتر، مرجع سابق، ص.206.

[2] ـ هشام محمد فريد رستم، مرجع سابق، ص.161.

[3] ـ نهلا عبد القادر المومني، الجرائم الالكترونية، مرجع سابق، ص.132.

يتضح إذن أن القنابل المنطقية تضل ساكنة وبدون فاعلية ، وبالتالي غير مكتشفة لمدة تطول أو تقصر يحددها مؤشر موجود في برنامج القنبلة.

4 ـ أساليب الإتلاف المعلوماتي:

تتنوع أساليب الإتلاف التي قد تكون نتيجة فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، أو قد تكون نتيجة استخدام الطرق التقنية والفنية كاستخدام فيروسات الحاسب الآلي[1].

1- التدخل في المعطيات:

تمثل المعطيات أو البيانات المعلومات المدخلة في النظام الآلي للحاسب بغرض معالجتها، ويكون التدخل فيها إما بإدخال معلومات وهمية في النظام المعلوماتي أو بتزوير المعطيات الموجودة.

أ- إدخال معلومات وهمية :

يقصد بذلك إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة[2].

ب ـ إدخال معلومات مزورة:

تستهدف جريمة تزوير المحررات والبيانات بشكل واسع البيانات الممثلة للمستحقات المالية للإيداعات المصرفية، وحسابات ونتائج الميزانيات، وأوامر الدفع، وقوائم المبيعات، وأنظمة التحويل الإلكترونية للأموال والودائع المصرفية[3].

[1]- محمد أمين الشوابكة، مرجع سابق، ص.229.

[2] - هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص.569.

[3] - محمد أمين أحمد الشوابكة، نفس المرجع، ص.232.

2- التدخل في الكيان المنطقي:

يمثل الكيان المنطقي مجموعة البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي، ويكون ذلك بتعديل البرنامج أو بخلق برنامج جديد.

أ – تعديل البرنامج:

يعد البرنامج كيانا ماديا يمكن رؤيته على شاشة الحاسب كترجمة إلى أفكار، كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسب ، ويأخذ هذا الفرض أحد الصور الآتية:

- التلاعب في البرامج:

يتم ذلك ببرمجة الجهاز الآلي والنظام المعلوماتي بشكل يؤدي إلى اختفاء البيانات بشكل كلي أو جزئي.

- اختلاس نتائج الحاسب أو الإدارة:

يتم ذلك عن طريق إعادة نسخ المعطيات عن بعد أو عن طريق النقل الإلكتروني للبيانات، وذلك بإتباع أسلوب التجسس المعلوماتي عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر شبكة الإنترنت.

- تغيير نظام التشغيل:

يكون ذلك بتزويد برنامج نظام التشغيل بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة كلمة السر، أو مفتاح الشفرة وأداة الربط بحيث تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسب الآلي[1].

ب - خلق برنامج جديد:

بمعنى أن يكون البرنامج المصطنع وهميا، أو أن يكون برنامجا ناقصا من الناحية الفنية

[1] - جميل عبد الباقي صغير،الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص.48.

- خلق برنامج وهمي:

بمعنى اصطناع برنامج كامل ومخصص فقط لارتكاب فعل الغش المعلوماتي .

- إعداد برنامج ناقص من الناحية الفنية:

يقوم الجاني في هذه الحالة وهو غالبا ما يكون هو المبرمج، بإدخال فجوات في برنامج الحاسب الآلي حتى يتمكن من تنفيذ التعديلات الضرورية بإدخال شفرات في برنامج الحاسب الآلي، وذلك حتى يتمكن من تنفيذ التعديلات الضرورية بإدخال شفرات إضافية أو إدخال مخارج وسيطة[1].

[1] - محمد أمين أحمد الشوابكة، مرجع سابق، ص.237.

الفصل الثاني

الحماية الجنائية الإجرائية للمحررات الإلكترونية

تعد متابعة الجرائم الماسة بالمحررات الإلكترونية من أهم التحديات التي تواجه سلطات التحقيق وذلك نظرا للطبيعة الخاصة التي تتميز بها، فالإجراءات التي تسبق مرحلة المحاكمة تتمثل أساسا في إجراءات التحقيق والفحص وجمع الأدلة المثبتة لوقوع الجريمة ونسبتها إلى فاعلها، كالمعاينة والتفتيش والضبط، بالإضافة إلى التسرب واعتراض المراسلات السلكية واللاسلكية كإجراءات حديثة في البحث والتحري حول المكونات المعنوية لنظم الحاسب الآلي والإنترنت، من بيانات ومعلومات وبرامج معنوية مستخدمة في أنظمة الاتصال الحديثة، ومدى قابليتها لاستخدامها فيما بعد كأدلة إثبات أثناء المحاكمة ضد مرتكب هذا النوع المستحدث من الجرائم **(المبحث الأول)**.

تخضع في الأساس الأدلة الإلكترونية التي تقدم إلى القاضي الجنائي أثناء النظر في الدعوى إلى السلطة التقديرية له، فسلامة الحكم تتوقف على سلامة تقدير الأدلة التي تعتبر جوهر الحكم، بالتالي فله أن يستعين في استخلاص هذا الدليل بالخبير المعلوماتي أو بالشاهد المعلوماتي خاصة في المسائل الفنية البحتة، حتى تتكون لديه قناعة قضائية تجاه كل ما يطرح عليه من تقارير وآراء ونتائج ومعلومات جوهرية تتعلق بموضوع الدعوى، فالقاعدة العامة في الإثبات الجنائي هو أن القاضي لا يتقيد بأي دليل إثبات في تكوين عقيدته، فهولا يستطيع أن يطرح ما ورد بتلك المحررات الإلكترونية سواء كانت هذه المحررات موضوع السلوك الإجرامي ذاته، أو كانت تتضمن دليلا على ارتكاب الجريمة، إلا إذا اطمئن إلى صحة المحرر الإلكتروني ذاته، فهي بطبيعتها تخضع لسلطة القاضي التقديرية فله أن يأخذ بها أو يطرحها من غير أن يكون ملزم بتسبيب ذلك، فحجية الأدلة الإلكترونية المتحصل منها من الوسائل الإلكترونية تكمن في عدم تعرضها للتغيير في فحواها أو لطمس الحقيقة فيها، بالتالي ينبغي في أي دليل يقدم أمام القضاء الجنائي أن يكون مشروعا بمعنى أن يكون وليد إجراءات صحيحة، وأن يكون قد طرح في الجلسة، وأن يكون مبنيا على الجزم واليقين **(المبحث الثاني)**.

المبحث الأول

الحماية الجنائية الإجرائية للمحررات الإلكترونية قبل مرحلة المحاكمة

يعتمد استخلاص الدليل الإلكتروني على عدة ضوابط تحكمه وذلك وفقا لقواعد إجرائية معينة، هذه الضوابط تتمثل أساسا في وسائل الإثبات الرئيسية أهمها التفتيش، المعاينة وضبط الأشياء المتعلقة بالجريمة، فضبط الجريمة وإثباتها يقوم على جمع الأدلة التي حددها القانون على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة المتحصل عليها عن تلك التي اعترف لها التشريع بالقيمة القانونية، ولما كنا بصدد تناول الجريمة الإلكترونية بصفة عامة وجرائم المحررات الإلكترونية بصفة خاصة، فإن قواعد الضبط القضائي في هذا النوع المستحدث من الجرائم يتطلب أساسا نفس الضوابط المعتمدة في الأحوال العادية، فالاختصاص الأصيل لسلطة التحقيق في ضل الجرائم الإلكترونية هي التفتيش والمعاينة والضبط، ويعد كل منها إحدى وسائل جمع الأدلة ولكل منها قواعده يتم إتباعها، وليس على المحقق الالتزام بإتباع ترتيب معين في مباشرة هذه الإجراءات بل هو غير ملزم أساسا بمباشرتها جميعا، وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضي به المصلحة وما تسمح به هذه الظروف، فسنتناول هذا المبحث في مطلبين، فسنتناول المعاينة في مجال جرائم المحررات الالكترونية **(المطلب الأول)**، تفتيش وضبط الأدلة في مجال المحررات الإلكترونية **(المطلب الثاني)**، ثم نتعرض إلى التسرب واعتراض المراسلات السلكية واللاسلكية كإجراءات حديثة في البحث والتحري **(المطلب الثالث)**.

المطلب الأول

المعاينة في مجال جرائم المحررات الالكترونية

تعتبر المعاينة من الإجراءات الهامة والتي تتولى القيام بها النيابة العامة، الغرض منها إظهار الجريمة على حقيقتها، وذلك بالانتقال إلى مسرح الجريمة ومعاينة الآثار المترتبة عنها بعد جمع الأشياء والعناصر المتعلقة بمحل الجريمة.

يرى بعض الفقهاء أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية وذلك لقلة الآثار المادية التي قد تنتج عن هذا النوع من الجرائم، وكثرة عدد الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها[1]، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها، يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار[2]، فعند تلقي بلاغ عن وقوع إحدى الجرائم الالكترونية وخاصة في مجال المحررات الالكترونية، وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ومسرح الجريمة المعلوماتية يختلف عن مسرح الجريمة التقليدية، فهي قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية كالسرقة والاحتيال، كما قد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة وضبط الأدلة[3]، وعلية سنحاول أن نبين مفهوم المعاينة من خلال بيان تعريف هذه المعاينة في مجال الجرائم الماسة بالمحررات الإلكترونية وأهميتها **(الفرع الأول)**، ثم كيفية الانتقال إلى العالم الافتراضي،

---

[1] ـ وليد عاكوم، التحقيق في جرائم الحاسوب، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، 26-27 أفريل 2003، ص.7 على موقع: https://www.f-law.net/law/archive/index.php/-

[2] ـ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة،أسيوط، 1994، ص.59.

[3] ـ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة ،2002، ص.364.
عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12إلى 14 نوفمبر 2007، ص.17.

وأشكال هذه المعاينة، والخطوات الواجب إتباعها قبل التحرك والانتقال إلى مسرح الجريمة **(الفرع الثاني)**.

الفرع الأول

مفهوم المعاينة في جرائم المحررات الالكترونية

معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة له أهميته المتمثلة في تصوير كيفية وقوع الجريمة، وظروف وملابسات ارتكابها، وتوفير الأدلة المادية التي يمكن تجميعها عن طريق المعاينة، وتعرف المعاينة بصورة عامة بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة، ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك كشف الأشياء التي تفيد في كشف الحقيقة[1]، فهي من إجراءات التحقيق الابتدائي ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، والمعاينة في مجال الجرائم الماسة بالمحررات الالكترونية تتضاءل من حيث درجة أهميتها مقارنة بالمعاينة التي تتم في مجال الجرائم الماسة بالمحررات التقليدية، ويعود ذلك أساسا على أنه تقريبا لا تترك آثارا مادية نظرا أن الانتقال لا يكون إلى العالم المادي وإنما إلى الفضاء الإلكتروني، فالمجرم المعلوماتي صاحب الخبرة يمكنه التلاعب في البيانات عن بعد أو محوها في الفترة بين ارتكاب الجريمة واكتشافها، وهذا يفتح مجالا للشك على الدليل المستخلص من المعاينة، وعليه سنتناول تعريف المعاينة في مجال الجرائم الماسة بالمحررات الالكترونية **(أولا)**، لنتعرض إلى أهميتها **(ثانيا)**، وذلك على النحو الآتي:

أولا: تعريف المعاينة في مجال الجرائم الماسة بالمحررات الالكترونية

تعرف المعاينة في علم التحقيق الجنائي بأنها مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له لإثبات حالته بالكيفية التي تركها بها الجاني[2]، فمعاينة مسرح الجريمة

[1] ـ حسون عبيد هجيج، صفاء كاظم غازي، *آثار جريمة قرصنة البريد الالكتروني*، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، المجلد السابع، عدد2، ديسمبر2016، ص.179.

[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.149

يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية[1].

عرف جانب من الفقه المعاينة بأنها: **" رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"**[2].

عرفها جانب آخر من الفقه بأنها: **"عمل ووصف شامل لمكان الجريمة سواء بالكتابة أو بالرسم التخطيطي أو التصوير لإثبات حالته كما تركها الجاني"**[3].

يتبين من خلال هذه التعريفات أن المعاينة هي ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته، والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة[4]، بالتالي تقتضي في ذلك سرعة الانتقال إلى محل تلك الواقعة قبل ضياع الأدلة، وعليه فهي تتمتع بأهمية كبيرة تتمثل في التيسير على سلطة التحقيق في عملها، إذ هي وسيلة لتكوين الفكرة الأولى عن كيفية ارتكاب الجريمة، كما أنها تساهم في الاستدلال على الجريمة، وبالتالي تعد أساسا لاستفاء العديد من الحقائق الأساسية عن الجريمة مثل وقت ارتكابها والدافع إلى ارتكابها والمكان الذي ارتكبت فيه والظروف المحيطة به[5]، بالتالي يعد لزاما على ضابط الشرطة القضائية الانتقال إلى ذلك المكان، لمعاينة وإثبات الآثار المادية للجريمة والمحافظة عليها وإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة[6]، فهي إذن تلعب دورا هاما باعتبارها أهم مصادر الأدلة الجنائية في إثبات كيفية ارتكاب الجريمة الالكترونية.

---

[1] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.151.

[2]- مشار إليه لدى: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص.79.

[3] ـ مشار إليه لدى: خالد ممدوح إبراهيم، نفس المرجع، ص.149.

[4]- جميل عبد الباقي صغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص. 26. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010، ص.134.

[5] ـ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص.205.

[6]- خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، 2014، ص.622.

يعتبر الأصل في المعاينة أنها إجراء من إجراءات التحقيق، ولذلك ففي غير حالات التلبس التي نص عليها القانون يلزم أن تقوم بها سلطة التحقيق بنفسها، أو تنتدب مأمور الضبط للقيام بها، ويقتضي ذلك تحرير محضر بها عن طريق كاتب، لأنها من الإجراءات التي تستلزم من المحقق تفرغا ذهنيا وتتبع في شأنها أيضا جميع القواعد التي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة وزمانها ليتمكنوا من الحضور أثناء إجرائها، كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة، سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[1]، ومع أهمية إجراء المعاينة وجوازها في كافة الجرائم إلا أنها ليست بالضرورة مجدية دائما أو صالحة لكشف الحقيقة في كل الجرائم، لذلك فهي إجراء هادف ليس تلقائي[2] فبمقتضاه ينتقل المحقق الجنائي إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الجريمة[3]، فالمعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها[4]، وفي مجال المعلوماتية يرى البعض أن أهمية المعاينة تتضاءل وذلك لندرة تخلف الآثار المادية عند ارتكاب الجريمة المعلوماتية، كما أن طول الفترة بين وقوع الجريمة وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار[5].

ثانيا: أهمية المعاينة في الجرائم الماسة بالمحررات الالكترونية

لا تتمتع المعاينة في مجال الكشف عن الجرائم الالكترونية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية[6]، كما أن دورها في مجال كشف غموض الجريمة الإلكترونية

[1] ـ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001، ص.27.

[2] ـ خالد مرزوق سراج العتيبي، مرجع سابق، ص.62.

[3] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.149.

[4] ـ هشام محمد فريد رستم، مرجع سابق، ص.106.

[5] ـ خالد مرزوق سراج العتيبي، نفس المرجع، ص.62.

[6] ـ خالد ممدوح إبراهيم، نفس المرجع، ص.153.

الإلكترونية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها، لا ترق إلى نفس الدرجة من الأهمية ومرد ذلك إلى الاعتبارات الآتية :

1- أن الجرائم الإلكترونية قلما يتخلف عن ارتكابها أثارا مادية، فما ينتج عنها من أدلة ما هو إلا بيانات غير مرئية.

2- تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة بين ارتكابها واكتشافها، مما يفسح المجال لحدوث إتلاف أو تغيير أو عبث بالآثار المادية[1]، مما يدخل الشك على الدليل المستمد من المعاينة.

3- إمكانية تلاعب الجاني في البيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية[2]، لذلك ينبغي على المشرع أن يقرر جزاءات جنائية على كل من يقوم بإجراء أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب أي وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات، قبل قيام سلطة التحقيق بإجراء المعاينة، وهو ما نص عليه المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية الجزائري[3]، والمشرع الفرنسي من خلال المادة (1/55) من قانون الإجراءات الجنائية الفرنسي[4]، حرصا منهما على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ أن أحكام هذه النصوص وإن كانت تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب

[1] ـ خالد مرزوق سراج العتيبي، مرجع سابق، ص.63.

[2] ـ أحمد محمود مصطفى، مرجع سابق، ص.134.

[3] ـ تنص المادة 43 من قانون الإجراءات الجزائية الجزائري: " **يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة ، أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة 200 إلى 100 د.ج،غير أنه يستثنى من هذا الخطر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة و الصحة العمومية أو تستلزمها معالجة المجني عليهم".**

[4] - Article 55 du C.P.P.F, dispose que : **« *Dans les lieu ou un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la 4°classe, à toute personne non habilitées, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvement quelconques* ». ,** sur le site **:** https://www.legifrance.gouv.fr/

ذات الطابع المادي كأشرطة الحاسوب وشاشة العرض الخاصة به و الأقراص وغيرها، بخلاف معاينة المكونات غير المادية لأنها تتطلب إجراءات خاصة[1].

لا تعتمد طبيعة المعاينة على صفة من يجريها، بل على مدى ما يقتضيه إجرائها من مساس بحقوق الأفراد، فالمعاينة قد تكون من إجراءات التحقيق، وقد تكون من إجراءات الاستدلال، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال، أما إذا اقتضت دخول منزل أو له حرمة خاصة كانت إجراء تحقيق[2].

الفرع الثاني
معاينة مسرح الجريمة الماسة بالمحرر الإلكتروني

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها قاضي التحقيق، أو ضباط الشرطة القضائية هو الانتقال إلى مسرح الجريمة، لأن هذا الأخير حجر الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، فسنتناول تحديد مسرح الجريمة الماسة بالمحرر الإلكتروني **(أولا)**، ثم سنتعرض إلى الضوابط الفنية التي يجب التقيد بها عند إجراء معاينة مسرح الجريمة والتي تتمثل في القواعد الفنية الواجب توفرها قبل الانتقال لمعاينة مسرح الجريمة الالكترونية، والخطوات الواجب مراعاتها عند الوصول إلى مسرح الجريمة **(ثانيا)**.

[1]- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص.896. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.83. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص.217. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص.29.

[2]- نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الإنسانية والاجتماعية، المجلد15، العدد13، أفريل 2017، ص.314.

أولا: تحديد مسرح الجريمة الماسة بالمحرر الإلكتروني

لم تهتم التشريعات الجنائية الحديثة بتعريف مسرح الجريمة ولم تقم بتحديد النطاق المكاني له كما هو الحال بالنسبة للتفتيش الذي سنتعرض له لاحقا، بالتالي معظم التشريعات تعبر عنه بمحل الواقعة[1]، ويرجع عدم الاهتمام بتحديد مسرح المعاينة إلى اعتبارين:

ـ أن معظم القوانين الجنائية لا ترتب آثارا قانونية بالبطلان أو الانعدام على تجاوز مسرح الجريمة الحدود المكانية عند إجراء المعاينة، طالما فيه مصلحة للتحقيق ولا يوجد خروج على قواعد الاختصاص.

ـ لا تثور عادة بشأن تحديد مسرح الجريمة منازعة بين الخصوم في الدعوى الجزائية أو طلب البطلان تأسيسا على تجاوز النطاق المكاني، لأن المعاينة هي إجراء واجب من إجراءات التحقيق تفرضه القوانين على المختصين بمجرد علمهم بوقوع الجريمة، فلا يجوز لأي طرف الاعتراض على هذا الإجراء[2].

ينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

1 ـ مسرح تقليدي:

يقع خارج بيئة الحاسوب والإنترنت ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك فيها الجاني أثار عدة، كالبصمات وبعض متعلقاته الشخصية، أو وسائط تخزين رقمية، كما لا توجد صعوبة مادية لتقرير صلاحية مسرح الجريمة المعلوماتية الذي يضم المكونات المادية، كأشرطة الحاسب، مفاتيح التشغيل، الأقراص وغيرها لمعاينتها من طرف ضباط الشرطة القضائية، وكذا وضع الأختام في الأماكن التي تمت معاينتها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها مع إخطار وكيل الجمهورية بذلك[3]، كما لا يوجد مانع من وضع نص

[1] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.162.

[2] ـ أحمد محمود مصطفى، مرجع سابق، ص.134.

[3] ـ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.182.

يمكن من خلاله السماح لضباط الشرطة القضائية بالانتقال عبر العالم الافتراضي خارج نطاق اختصاصه[1].

2 - مسرح افتراضي :

يقع داخل البيئة الإلكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت، في ذاكرة الأقراص الصلبة الموجودة بداخله[2].

تتم المعاينة في الجرائم الإلكترونية عامة وجرائم المحررات الالكترونية خاصة كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هنا لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي، فيستطيع عضو سلطة التحقيق أن ينتقل إلى العالم الافتراضي لمعاينته من مكتبه من خلال الحاسوب في ذلك الأخير، كما يمكنه اللجوء إلى مقهى الإنترنت، أو إلى بيت الخبرة القضائية أو إلى الخبرة الاستشارية أيضا إذا توفر له في التشريع ما يبيح له ذلك، وأيضا يجوز له اللجوء إلى مقر مزود الإنترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة[3].

تثير المكونات غير المادية للبيئة الالكترونية صعوبات في إثبات معاينة مسرح الجريمة والتي تكمن في نقطتين أساسيتين:

- قلة الآثار المادية التي قد تتخلف عن هذا النوع من الجرائم.
- كثرة الأشخاص الذين يترددون على مسرح الجريمة خلال المدة بين اقتراف الجريمة والكشف عنها، وهو ما يتسبب عادة في إتلاف الآثار المادية للجريمة، الأمر الذي يصبغ الدليل المستقى من الجريمة بالشك والريبة[4].

[1] - عمر محمد أبو بكر يونس، مرجع سابق، ص.832.

[2] - عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.84.

[3] - عمر محمد أبو بكر يونس، نفس المرجع، ص.859.

[4] - محمد أمين الشوابكة، مرجع سابق، ص.123.

ثانيا: الضوابط الفنية التي يجب التقيد بها عند إجراء معاينة مسرح الجريمة

أصبح لزاما عند إجراء معاينة مسرح الجريمة الالكترونية التقيد ببعض الضوابط الفنية، تنقسم هذه الضوابط إلى قواعد فنية قبل الانتقال لمعاينة مسرح الجريمة، وقواعد ما بعد الوصول إلى مسرح الجريمة ويمكن تلخيصها كالتالي :

1- القواعد الفنية الواجب توفرها قبل الانتقال لمعاينة مسرح الجريمة الالكترونية :

يعود اختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم، كون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعامل خاص معه وذلك من خلال إعداد خطة عمل تحتوي على إعداد شامل للأدوات المستعملة في المعاينة، وتقسيم المهام بين الفنيين القائمين على هذا الإجراء[1]، كما يجب أيضا إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية والتي تتمثل أساسا في:

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة المتوقع مداهمتها وشبكات الاتصال الخاصة بها.

- إعداد خطة واضحة ومفهومة للجميع، مع تفصيلها بالرسومات ومراجعتها مع أعضاء الفريق قبل التحرك لمسرح الجريمة مع مراعاة الحالة، الرسالة، التنفيذ، المداخل والمخارج، والاتصالات[2].

- إعداد فريق التفتيش من المتخصصين، على أن يكون هذا الفريق مرفقا بالأمر القضائي اللازم للقيام بالتفتيش، لأن أغلب الجرائم الإلكترونية تكون داخل أمكنة لها خصوصياتها[3].

- الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل.

[1] - كاظم محمد عطيات ومحمد رضوان هلال، كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص، المجلة العربية الدولية للمعلوماتية، السعودية، المجلد 3، العدد5 ، 2015، ص.46.

[2] - محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15 ، العدد 30، الرياض، جامعة نايف العربية للعلوم الأمنية، ص.356.

[3] - عمر أبو بكر بن يونس، مرجع سابق، ص.895.

ـ تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الحاسب الآلي، وبالتالي فقدان كافة العمليات التي يتم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة[1].

2 ـ الخطوات الواجب مراعاتها عند الوصول إلى مسرح الجريمة:

يجب على المحقق الجنائي أو ضابط الشرطة القضائية إتباع الخطوات التالية عند الوصول إلى مسرح الجريمة وهي:

ـ تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسب وملحقاته ، مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة[2].

ـ العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار[3].

ـ عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أية مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة[4]، والبحث عن خادم الملف لتعطيل حركة الاتصالات[5].

---

[1] ـ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.60.

[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.180.

[3] ـ سليمان احمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007، ص.290. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية،2006، ص.104.عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.64.

[4] ـ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مرجع سابق، ص.111.

[5] ـ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.61.

ـ التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها، ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة[1].

المطلب الثاني

التفتيش وضبط الدليل في مجال الجرائم الماسة بالمحررات الالكترونية

أفرزت وسائل الاتصال الحديثة ومن بينها شبكة الانترنت أنماطا مستحدثة من الجرائم لم يعهد بها الإنسان، فهي جرائم معقدة سواء في طرق ارتكابها أو في وسائل اكتشافها، حتى أضحت الجريمة الالكترونية كظاهرة عالمية يصعب معها الكشف عن مرتكبيها نظرا لطبيعتها الخاصة واستخدامها لأحدث تكنولوجيات الأنظمة المعلوماتية والحاسب الآلي، فالتفتيش في جرائم المحررات الالكترونية هو إجراء قانوني يهدف إلى كشف أدلة الجريمة التي وقعت أو المحتمل وقوعها، ويعود السبب في خطورة التفتيش بشكل كبير في هذا النوع المستحدث من الجرائم، إلى أن محل التفتيش فيها هو نظام المعالجة الآلية للمعطيات وهو نظام ذو طابع غير مادي، فالمحررات الالكترونية هي مجرد معلومات الكترونية ليس لها مظهر مادي محسوس في العالم الخارجي كما هو الحال في المحررات الورقية، إلا أنه يمكن ضبطها واستنساخها على الورق أو أية وسيلة أو دعامة أخرى، وهذا يتطلب ضرورة توفير وسائل وإجراءات حديثة للجهات القضائية المختصة لمحاربة هذا النوع من الجرائم، خاصة ما تعلق بإجراء التفتيش الذي يهدف إلى استخراج محررات إلكترونية كأدلة معلوماتية مرتبطة بأنظمة قانونية مختلفة وليس بنظام واحد، بالتالي سنتناول في هذا المطلب التفتيش الذي يرتكز أساسا على الدليل الالكتروني الذي يحتاج إلى قواعد إجرائية تختلف عن القواعد الإجرائية التقليدية وذلك من خلال بيان مفهومه والضوابط القانونية التي تحكمه من ضوابط شكلية وضوابط موضوعية **(الفرع الأول)**، ثم سنتطرق إلى ضبط الدليل الالكتروني الذي يعتبر النتيجة الطبيعية التي ينتهي إليها التفتيش وكأثر مباشر له والتي يتم الحصول عليها أثناءه **(الفرع الثاني)**.

[1]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.87. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص.220 .

الفرع الأول

التفتيش في مجال الجرائم الماسة بالمحررات الإلكترونية

يعد التفتيش من أهم إجراءات التحقيق في كشف الحقيقة يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم، فهو يتطلب أوامر قضائية لمباشرته، غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم[1]، كما يعتبر أيضا وسيلة الغرض منها الوصول إلى أدلة مادية يستند فيها في بيان وظهور الحقيقة، ونتيجة لذلك يعد تفتيش نظام الحاسوب والإنترنت من أخطر المراحل حيث تثار بشأنه عدة تحديات، خاصة ما يتعلق منها بتحديد الإطار القانوني الملائم لإجراء التفتيش داخل النظام المعلوماتي، والبحث عن الدليل الالكتروني في المكونات المنطقية للحاسب الآلي، أو المخزنة على شبكة الانترنت من بيانات ومعطيات ومحررات إلكترونية، وإمكانية الولوج إلى هذه البيئة والقيام بإجراء التفتيش والكشف عن مرتكبي هذا النوع المستحدث من الجرائم، بالتالي سنتعرض في هذا الفرع إلى مفهوم التفتيش في البيئة الالكترونية **(أولا)**، ثم سنتناول بعد ذلك شروط إجراء تفتيش النظم الحاسوبية والإنترنت **(ثانيا)**.

أولا: مفهوم التفتيش في البيئة الالكترونية

لا يختلف المفهوم القانوني للتفتيش بالنسبة للجرائم الالكترونية عن مفهومه السائد في فقه الإجراءات الجنائية، فعرف بأنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات، بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها[2].

[1]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، 2006، ص.192. نديم محمد حسن الترزي، مرجع سابق، ص.321.

[2] - هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997، ص.73.

يعرف الفقه التفتيش بأنه: **"إجراء من إجراءات التحقيق يقوم به الموظف المختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم"**[1]، وعلى خلاف إجراءات التحقيق الأخرى التي هدفها جمع الأدلة المادية كالخبرة والمعاينة، فإن التفتيش يمس بحرمة الحياة الخاصة وحرمة المسكن لذلك نجد التشريعات تقرر أبطاله في حالة عدم مراعاة الضمانات والقيود المقررة لإجرائه[2].

عرفه جانب آخر بأنه: **" البحث في مستودع سر المتهم وهو إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته"**[3].

عرفه الفقه الفرنسي بأنه: **" البحث الدقيق لكل عناصر الأدلة التي يمكن استخدامها في الدعوى الجزائية والتي تجري على مسكن المتهم"**[4].

يجب التنويه هنا أن جانبا من الفقه يرى أن الاصطلاح الواجب إطلاقه على عملية البحث عن أدلة الجريمة المرتكبة في العالم الافتراضي هو" الولوج أو النفاذ "، باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح "التفتيش" فيعني البحث القراءة التفحص التدقيق في البيانات، وهو مصطلح تقليدي أكثر، وهناك من يستخدم المصطلحين معا بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة[5].

[1] ـ مشار إليه لدى: عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2007، ص.358.

[2] ـ مشار إليه لدى: مصطفى محمد موسى، التحقيق في الجرائم الالكترونية، دار التجهيزات الفنية، القاهرة، 2009، ص.189.علي عدنان الفيل، مرجع سابق، ص.38.

[3] ـ مشار إليه لدى: يونس عرب، جرائم الحاسب الآلي والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، 2002، ص.513.

[4] ـ مشار إليه لدى: علي حسن محمد الطوالقة، التفتيش على نظم الحاسوب والانترنت، عالم الكتب الجديدة، الأردن، 2004، ص.12.

[5] ـ هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، مرجع سابق، ص.164.

عرف المجلس الأوربي هذا النوع من التفتيش في البيئة الالكترونية المتعلق بمكافحة الجرائم المعلوماتية بأنه: **" إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني"**[1].

يتضح من خلال التعريفات السابقة أن التفتيش ما هو إلا وسيلة للإثبات المادي، ذلك لأنه إجراء يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا ما يتنافر مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي وكذا شبكة الانترنت، فهناك صعوبات إجرائية تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية[2]، فهي مجرد برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي، وعلى ذلك فلا سبيل لأن يرد عليها تفتيش أو ضبط، ومن الأجدر إخضاعها لأحكام مستقلة تتلاءم وطبيعتها الخاصة[3].

يقع التفتيش في إطار جرائم الإنترنت على موضوعين اثنين:

ـ قد يرد على المكونات المادية للحاسب الآلي وملحقاته، وهذه لا خلاف يذكر حول خضوعها للتفتيش بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية، كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك تبعا للمكان أو الحيز الموجود فيه[4].

ـ الشبكة وما تتضمنه من مكوناتها، مع الأخذ في الحسبان في الحالتين الشيء المتواجد فيه كلا الموضوعين.

تتكون نظم الحاسب الآلي من مكونات مادية ومكونات معنوية أو برمجية، كما أنه تربطه بغيره من الحاسبات شبكات اتصال بعدية على المستوى المحلي أو الدولي.

سنتناول فيما يلي مدى خضوع هذه المكونات للتفتيش على النحو التالي:

---

[1] ـ مشار إليه لدى: علي عدنان الفيل، مرجع سابق، ص.39.

[2] ـ عفيفي كامل عفيفي، مرجع سابق، ص.344.

[3] ـ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص.223.

[4] ـ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.64.

1- تفتيش مكونات الحاسوب المادية:

تشمل المكونات المادية للحاسب الآلي وحدة الإدخال أو وحدة الذاكرة الرئيسية، وحدة الحساب والمنطق ووحدات الإخراج وكذا وحدة التحكم، وأخيرا وحدة التحكم الثانوية، وتشمل كل وحدة من هذه الوحدات على مجموعة من المفردات المعلوماتية[1].

يدخل تفتيش المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة إلكترونية، يفيد في كشف الحقيقة عنها وعن مرتكبها في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة قانونا في التشريعات المختلفة[2]، بمعنى أن حكم تلك المكونات يتوقف على طبيعة المكان الموجود فيه سواء من الأماكن العامة أو الأماكن الخاصة، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في أغلب التشريعات الجنائية، كالقانون المصري أين يشترط لصحة تفتيش منزل المتهم صدور الأمر القضائي المسبب ولو في حالة التلبس، وذلك بعد الحكم بعدم دستورية المادة 47 إجراءات جنائية مصري، فضلا عن شروط التفتيش العامة[3]، بالمقابل فإن القانون الجزائري خالف نص المادة 64 من قانون الإجراءات الجزائية[4] وأورد عليها استثناءات، بموجب قانون رقم 06-22 المعدل و المتمم للأمر رقم 66-155 والمتضمن قانون الإجراءات الجزائية، حيث استثنى المشرع تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في المادة 02/45 من القانون رقم 06-22 ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث نص في المادة 02/64 بأنه: " **غير أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 03/47 من هذا القانون، تطبق**

[1]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص.387. أسامة أحمد المناعسة وآخرون، مرجع سابق، ص.274.

[2] - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.195.

[3] - حسين سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص.387

[4] - تنص المادة 64 من ق.إ. ج.ج :" **لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه".**

الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر"[1]، حيث أجاز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.

يلاحظ من خلال استقرائنا لنص المادة أنه يشير إلى التعدي المشروع على حرمة الحياة الخاصة للفرد، فالمشرع الجزائري غلب في هذه الحالة مصلحة المجتمع على مصلحة الفرد في تحقيق العدالة، ومبرر ذلك هي تلك الطبيعة الخاصة للجريمة الإلكترونية، فهي جريمة قابلة للمحو والتعديل بسرعة، ومرتكبها ذو دراية بالأمور التقنية، وقد تكون الصعوبة أكثر إذا كان الدليل الإلكتروني الوحيد في الدعوى الجنائية، لذلك أجاز المشرع إجراء تفتيش منازل[2] المتهم في حالة واحدة وهي حالة صدور إذن من وكيل الجمهورية المختص.

2 - مدى خضوع مكونات الحاسوب المعنوية للتفتيش (Logiciel) :

تنقسم المكونات المعنوية للحاسب الآلي إلى الكيانات المنطقية الأساسية، أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقا لاحتياجات العميل، ويستلزم الحاسب بمكوناته مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات، وهم مشغلو الحاسب وخبراء البرامج سواء كانوا مخططي برامج تطبيقات، أم كانوا مخططي برامج نظم ومحللين ومهندسي الصيانة ومديري النظم المعلوماتية[3].

---

[1]- تنص المادة 3/47 من القانون رقم06-22 على: **"عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية، أو الجرائم الماسة بأنظمة الحاسب و الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص".**

[2] - المنزل أو المسكن هو مستودع سر الأفراد، إلا أن قانون الإجراءات الجزائية لم يحدد له تعريفا عدا ما جاء في المادة 22 منه على أنه: **" غير أنه لا يسوغ لهم الدخول في المنازل و المعامل والمباني أو الأفنية و الأماكن المسورة المتجاورة إلا بحضور أحد ضباط الشرطة القضائية "** .ورغم ذلك نجد له تعريفا في المادة 355 من قانون العقوبات " **يعد منزلا مسكونا كل مبنى أو دار أو غرفة أو كشك ولو متنقل متى كان معدا للسكن، وإن لم يكن مسكونا وقتذاك وكافة توابعه ....".**

[3]- أسامة أحمد المناعسة وآخرون، مرجع سابق، ص.276.

أثار تفتيش المكونات المعنوية للحاسب الآلي خلافا كبيرا في الفقه[1]، بشأن جواز تفتيشها من عدمه، فالجرائم التي تقع على الكيانات المعنوية للكمبيوتر يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، أما إذا تحولت إلى مستخرجات أو محررات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها أو بواسطتها.

ذهب بعض الفقهاء في فرنسا أن النبضات الإلكترونية أو الإشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، بالتالي لا تعتبر شيئا ماديا بالمعنى الحقيقي، مما دفع المشرع الفرنسي إلى إحداث تعديلات في نصوص التفتيش استجابة لهذه التغييرات[2]، وهذا بالقانون رقم 545-2004 المؤرخ في 21جوان 2004 حيث قام بإضافة عبارة **" المعطيات المعلوماتية"** في المادة 94 من قانون الإجراءات لتصبح على النحو التالي: **"يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة"**[3]، وقد حذا المشرع الجزائري حذو المشرع الفرنسي بتجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004.

نتفق مع الرأي الذي يرى إمكانية التفتيش في الكيانات المعنوية، لأن المكونات المعنوية يمكن تصنيفها وتحليلها لاستظهار الدليل المعلوماتي، باعتبارها محتوى لمعلومات وبيانات وحوار وكلمات سر.

[1]- يقع التفتيش على مكونات الحاسوب والبيانات المرتبطة به، ولا توجد مشكلة في تنفيذ التفتيش للمكونات المادية للكمبيوتر، لإمكانية ذلك وسهولته ولأنه يقع على أشياء مادية نظرا لحساسية البيانات التي تحتويها أجهزة الحاسوب وإمكانية إتلافها أو محوها بسهولة، لكن المشكلة في إمكانية تفتيش وضبط مكونات الحاسوب المعنوية كالبرامج والنظم الخاصة بالتشغيل وقواعد البيانات، والتي يمكن أن تخزن طريقة ارتكاب الجريمة بواسطة الحاسوب. علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوردي العلمية، عمان، 2009، ص.116. نديم محمد حسن الترزي، مرجع سابق، ص.299.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي، مرجع سابق، ص.200.

[3] - Article 94 du C.P.P.F dispose que : « ***Les perquisitions sont effectuées dans tous les lieux ou peuvent se trouver des objets ou des données informatique dont la découverte serait utile à la manifestation de la vérité*** ».

3 ـ مدى خضوع الحاسب الآلي للتفتيش عن بعد:

تتضمن إجراءات تفتيش الحاسب الآلي وجود وسائل فنية حديثة لتفتيش الشبكات المرتبطة به، والمراقبة الإلكترونية لنظم المعلومات والشبكات المعلوماتية، رغم أن ذلك يتعرض لحقوق الأشخاص وحرياتهم، إلا أن ذلك لا ينبغي أن يحدث دون الحصول على موافقة القضاء، وأن يكون محدد المدة والنطاق[1]، كما أن الطبيعة التقنية الرقمية زادت من التحديات والصعوبات التي تواجه القائمين على التفتيش والضبط في الجرائم المعلوماتية، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي، في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش، كما يمكن أن يكون الموقع الفعلي للبيانات والمعلومات يدخل ضمن الاختصاص القضائي لدولة أخرى، مما يعقد الصعوبات التي قد تواجه مكافحة الجرائم المعلوماتية، ويزيد من أهمية وجود تعاون دولي في مكافحة مثل هذا النوع[2]، ويمكن تفصيل هذه النقطة في ثلاث احتمالات:

الاحتمال الأول: اتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر داخل الدولة

يعتبر من الصعوبات والتحديات التي تواجه التفتيش عن بعد هو مدى إمكانية امتداد الحق في التفتيش، خاصة إذا تبين أن الحاسب أو نهاية طرفيه في مكان أخر مملوك لشخص غير المتهم، هنا بعض التشريعات الوطنية والدولية وجدت بعض الحلول لهذه المشكلة :

1ـ الاتفاقية الأوربية للجرائم المعلوماتية:

نصت الاتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001 في المادة 19 من القسم الرابع، على أنه من حق السلطة القائمة بتفتيش الحاسوب المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد التفتيش غلى جهاز آخر، إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الآلي محل التفتيش، بالتالي هذه الاتفاقية سمحت للدول الأعضاء تمديد مجال التفتيش

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص.161.

[2] - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.200.

الذي كان محله جهاز حاسب به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش.

2 ـ القانون الفرنسي:

تعتبر فرنسا من الدول السباقة للتوقيع على اتفاقية بودابست، لذلك سعى المشرع الفرنسي إلى ملائمة الآليات والقواعد الإجرائية التي جاءت بها اتفاقية بودابست في مجال البحث عن الجريمة الالكترونية[1].

نص في المادة 1/17 من القانون رقم 239- 03 بشأن الأمن الداخلي الصادر في 18 مارس 2003 بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهم عملية البحث والتحري، تنص المادة 17 منه على أنه: " **يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق و المخزنة في النظام المذكور أو في أي نظام معلوماتي أخر ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أن يتم الدخول إليها أو تكون متاحة ابتدءا من النظام الرئيسي**"[2].

نلاحظ انطلاقا مما سبق ذكره أن ذاتية تفتيش الحاسوب وقصور القواعد التقليدية، تظهر بصورة جلية أثناء امتداد التفتيش إلى الأجهزة المرتبطة به من خلال الحالتين التاليتين:

[1] - CAPRIOLI Eric, les moyens juridiques de lute contre la cyberciminalité, Revue 46 Risques n° 51, septembre 2002, p.50. article disponible sur le site : : www.caprioli-avocats.com

[2]- Article 17-1 de la LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France , dispose que : ***« Les officiers de police judiciaire ou, sous leur responsabilité , les agents de police judiciaire peuvent au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux ou se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, des lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial*** **»** .

1- إذا كانت الأجهزة المتصلة بالجهاز الذي صدر إذن تفتيش بخصوصه ينتمي إلى شخص غير المتهم، ومن ثم يتعين تفتيش هذه الأجهزة المرتبطة به بناء على الإذن الأول، وهذا ما يتناقض مع بعض التشريعات الإجرائية، حيث تشترط صدور الأمر القضائي المسبب لتفتيش شخص غير المتهم في حالة ما إذا كانت النيابة العامة هي التي تتولى التحقيق.

2- الأصل أنه في حالة التلبس لا يشترط الحصول مسبقا على إذن لتفتيش الجهاز حيث يمكن أن يرد التفتيش على الأجهزة المرتبطة به، ومن ثم يمكن التفتيش دون دخول مسكن غير المتهم، فالانتقال غير مهم إلى مكان الجهاز الثاني، بل إن ذلك يتم باستعمال وسائل تقنية حديثة "برامج العدول".

3 ـ موقف المشرع الجزائري:

نص المشرع الجزائري في المادة 05 /02 من القانون رقم 09- 04 بأنه: **" في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.."**.

يلاحظ أن المشرع الجزائري أجاز تمديد نطاق التفتيش الذي يكون محله جهاز الحاسب الآلي معين إلى غيره، بشرط إعلام السلطة القضائية المختصة مسبقا بذلك، بشرط أن تكون هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى أو جزء منها ، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى.

الاحتمال الثاني: اتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر خارج الدولة

يقوم وفقا لهذا الفرض مرتكبو الجرائم الإلكترونية بتخزين بياناتهم في أنظمة تقنية خارج الدولة، عن طريق شبكات الاتصالات بهدف عرقلة سلطات التحقيق في جمع الأدلة[1]، ومن ثم عرقلة سير العدالة، ونتيجة لذلك أدخلت تعديلا على قانون الإجراءات الجنائية لتجيز تفتيش الأنظمة المتصلة، حتى ولو كانت متواجدة خارج إقليم الدولة.

جاء في تقرير المجلس الأوربي بأن الاختراق المباشر يعتبر انتهاكا لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشأن، ويؤيد الفقه الألماني ما جاء بتقرير المجلس الأوربي حيث أن السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى، وخرقا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية[2].

أجاز المشرع الفرنسي في نص المادة 2/17 من قانون الأمن الداخلي رقم 239- 03 لمأمور الضبط القضائي، أن يقوموا بتفتيش الأنظمة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[3].

أجاز المشرع الجزائري بموجب المادة 03/05 من القانون 09-04 تفتيش الأنظمة حتى ولو كانت خارج إقليم الدولة، كما أجاز الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة، طبقا للاتفاقيات الدولية ذات الصلة وفقا

[1] - عبد الفتاح بيومي حجازي، نحو صياغة عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2009، ص.655.

[2] - عبد الله حسين محمود، سرقة المعلومات في الحاسب الآلي، مرجع سابق، ص.376.

[3]- Article 17/2 de la Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France, dispose que : ***« S'il est probablement avéré que ces données , accessible à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des condition d'accès prévues par les engagements internationaux en vigueur »***.

لمبدأ المعاملة بالمثل[1]، كما أجاز أيضا في المادة 16 من القانون ذاته أنه وفي إطار التحقيقات والتحريات القضائية التي تمت مباشرتها وتتبع الجرائم المنصوص عليها في ذات القانون والكشف عن مرتكبيها، فإن السلطات المختصة بإمكانها تبادل المساعدات القضائية على المستوى الدولي[2].

يلاحظ أنه إذا كان امتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي، له أهمية في إمكانية الحصول على الدليل عن بعد وفي بضع ثواني، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاكا لسيادة الدولة الأجنبية[3]، أما إذا اقتضت ضرورة التحقيق القيام به، فينبغي مراعاة العديد من الضمانات يكون متفق عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهو ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية.

الاحتمال الثالث: التصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي

يعتبر التصنت والأشكال الأخرى للمراقبة الإلكترونية رغم كونها وسائل مثيرة للجدل القانوني حول مدى مشروعيتها، إلا أنه يسمح بها وفق ظروف معينة في جميع دول العالم تقريبا[4].

نص المشرع الجزائري في المادة 65 مكرر5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باعتراض المراسلات وتسجيل الأصوات والتقاط الصور[5]، كما أجاز المشرع الجزائري بموجب المادة 04 من القانون 09-04 حول الحالات التي تسمح باللجوء إلى المراقبة

[1]- راجع نص المادة 5 فقرة 3 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] - راجع المادة 16 من نفس القانون.

[3] - هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص.78.

[4] - موسى مسعود أرحومة، مرجع سابق، ص.13.

[5] - راجع نص المادة 65 مكرر 5 من قانون العقوبات الجزائري.

الالكترونية بحيث استثنى في الفقرة ج الحالة التي يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[1].

ثانيا: شروط إجراء تفتيش النظم الحاسوبية والإنترنت

استقرت أغلب التشريعات على إحاطة التفتيش بشروط وضمانات أساسية يمكن إتباعها بوصفه إجراء يمس صميم الحرية الشخصية، الغرض منها تحقيق الموازنة الضرورية بين مصلحة المجتمع في القصاص من المجرم وردعه، وبين الحريات الشخصية للأفراد[2].

تخضع إجراء تفتيش النظم الحاسوبية والإنترنت لمجموعة من القواعد العامة التي تتوافر في القوانين الإجرائية العامة في ضل غياب النصوص الإجرائية الخاصة[3]، وهنا يجب ملاحظة أن بعض المواد التي يتم تفتيشها عبارة عن أجهزة ومعدات وبعضها الآخر كيانات غير مادية، ربما تكون عبارة عن برمجيات أو شبكات أو حتى ملفات مشفرة لا يستطيع القيام بتشفيرها العكسي لفتحها إلا الأشخاص المعينون لذلك، ويتم التفتيش من خلال مجموعة من القواعد الشكلية المتعلقة بمن يحضر التفتيش، ومن يقوم بإعداد المحاضر الخاصة بذلك وإجراءات تنفيذ التفتيش، فيجب عند القيام بالتفتيش تحديد النظام المراد تفتيشه بأكبر قدر ممكن من الدقة، والقيام بذلك بوجود أفراد متخصصين لتحسب عدم القيام بخطوات قد تتسبب بتلف الكيان المراد تفتيشه، ومجموعة أخرى من القواعد الموضوعية التقليدية التي تفرض طبيعة المراد تفتيشه تحوير النصوص لتتناسب معها وتشملها، حيث يجب تحديد سبب تفتيش النظام والأجهزة وتحديد المحل المراد تفتيشه من أشخاص وأشياء و أماكن[4].

[1] ـ راجع نص المادة 4 من القانون رقم 09-04 السالف الذكر.

[2] ـ علي حسن محمد الطوالقة، التفتيش الجنائي على نظم الحاسوب والانترنت، مرجع سابق، ص.7.

[3] ـ المرجع نفسه، ص.7.

[4]ـ محمد نافع فالح رشدان العدواني، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات قي المسائل الجزائية، رسالة ماجستير في القانون العام، قسم القانون العام، جامعة الشرق الأوسط، 2015، ص.75.

من الشروط والضمانات التي يجب توافرها لإجراء التفتيش ما هو موضوعي، ومنها ما هو شكلي، وعلى هذا الأساس نقسم دراستنا لشروط التفتيش في العالم الافتراضي إلى شروط شكلية وأخرى موضوعية.

1 ـ الشروط الشكلية للتفتيش في البيئة الالكترونية:

يخضع التفتيش للخصائص العامة والتي تخضع لها كافة إجراءات التحقيق الابتدائي، وهي وجوب حضور الخصوم ووكلائهم كلما أمكن ذلك، كما يجب أن يكون أمر التفتيش مسببان وهذا التسبيب ضمان لتوافر العناصر الواقعية التي يتوافر بها سبب التفتيش بالمعنى الدقيق، وحتى يكون ذلك التسبيب تحت رقابة هيئة الحكم وكذلك الدفاع، حتى يمكن مراقبة ما إذا كان إذن التفتيش صدر وفقا للشروط القانونية من عدمه، وحتى يمكن تقدير جدية صدوره وهو أمر يقدره المحقق تحت رقابة محكمة الموضوع، وفي جميع الأحوال يحق للدفاع مراقبة ذلك انبعاثا من كفالة حق الدفاع[1].

أ ـ الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الإلكترونية:

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، والغاية من تقرير هذا الشرط تتمثل في اطمئنان الخاضع لهذا التفتيش إلى تطبيقه وفقا للقانون والحيلولة دون تعسف الجهة التي تقوم بالتفتيش[2].

لم تشترط معظم التشريعات الإجرائية صحة تلك الإجراءات في حضور شهود أثناء تفتيش الأشخاص.

اشترط المشرع المصري في المادة 51 من قانون الإجراءات الجنائية المصري حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة أحد مأموري الضبط القضائي، ويشترط أن

[1] - محمد نافع فالح رشدان العدواني، مرجع سابق، ص.103 .

[2]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.359. محمد الأمين البشري، مرجع سابق، ص.30.

يكون هذان الشاهدان بقدر الإمكان من أقارب المتهم البالغين أو القاطنين معه بالمنزل أو من الجيران ويثبت ذلك في المحضر[1].

أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة، فيصح اتخاذ هذا الإجراء دون حاجة لاستدعاء الشهود، وهذا بنص المادة 92 من قانون الإجراءات الجنائية المصري، ويستوي الأمر عند قيام مأمور الضبط القضائي بمباشرة التفتيش بناءا على ذلك من سلطة التحقيق، فلا يلتزم باستدعاء شهود لأن المندوب يحل محل النائب تماما[2].

نص المشرع الجزائري على واجب إجراء التفتيش بحضور أشخاص معينين بالقانون وهم المتهم، القائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، والتي جاء فيها أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية القائم بالتفتيش، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية الجزائري، على أنه: " **لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**".

يلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون 06-22 مس المادة 45 منه حيث استغنى المشرع عن ضمانة حضور الأشخاص المحددين في الفقرة الأولى من هذه المادة، فنص في الفقرة الأخيرة على ما يلي:"...**باستثناء الأحكام المتعلقة بالحفاظ على السر المهني...**"[3]، والغاية من ذلك ترجع إلى ضرورة إضفاء

[1] ـ تنص المادة 51 إجراءات جنائية مصري على أنه:" **يجب أن يكون بحضور شاهدين، ويكون هذان الشاهدان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران، ويثبت ذلك في المحضر**".

[2] ـ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص.165 .

[3] ـ المادة 45 من قانون الإجراءات الجزائية رقم 17-07 المؤرخ في 28 جمادي الثانية عام 1438 الموافق ل 27مارس سنة2017.

نوع من السرية أثناء إجراء التفتيش وفي جمع الدليل الإلكتروني، كما أن المادة 45 من قانون الإجراءات الجزائية الجزائري هو ترجمة حرفية للمادة 57 إجراءات جنائية فرنسي[1] .

يشترط المشرع الجزائري أثناء التحقيق الابتدائي في نص المادة 64 من قانون الإجراءات الجزائية بأنه لا يجوز تفتيش المسكن إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، وحدد المادة شكل الرضا الذي يكون مكتوبا بخط يد صاحب الشأن، فإذا كان لا يعرف الكتابة، فبإمكانه الاستعانة بشخص يختاره بنفسه وينوه عن ذلك في المحضر .

ب - ميعـــاد إجراءات تنفيذ تفتيش نظم الحاسوب الآلي:

تتميز هذه الإجراءات بخصوصية من حيث دقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسب الآلي[2].

يلاحظ في نطاق تفتيش نظم الحاسوب أن أغلب التشريعات الإجرائية لم تحدد مدة لتنفيذ إجراء التفتيش، كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو في

[1]- Article 57 du C.P.P.F. dispose que : ***« Sous réserve des articles 56-1 à 56-5 et du respect du secret professionnel et des droits de la défense mentionné à l'article 56, les opérations prescrites par ledit article sont faites en présence de la personne au domicile de laquelle la perquisition a lieu.***

En cas d'impossibilité, l'officier de police judiciaire aura l'obligation de l'inviter à désigner un représentant de son choix ; à défaut, l'officier de police judiciaire choisira deux témoins requis à cet effet par lui, en dehors des personnes relevant de son autorité administrative » , sur le site : www.legifrance.gouv.fr/

[2]- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012 ، ص.131.

الليل وذلك لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية[1].

مما سبق يمكن القول أنه بخصوص جرائم الحاسوب الآلي المتصل بالانترنت، نجد أنه لا توجد نصوص تشريعية تحدد وقتا معينا يتم فيه إجراء تفتيش الحواسيب المتصلة بالإنترنت، والتي تمت عن طريقها تلك الجريمة، الكائنة في المنازل وما في حكمها.

ج ـ إعداد محضر التفتيش المتعلق بالجريمة الالكترونية:

يكون إعداد محضر التفتيش المتعلق بالجريمة الالكترونية بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات الأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص[2].

تنص المادة 2/68 من قانون الإجراءات الجزائية الجزائري بأنه: **"تحرر نسخة عن هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"**.

يلاحظ أن المشرع الجزائري ألزم أثناء القيام بإجراءات التحقيق سواء كانت معاينة أو ضبط أو تفتيش أو الشهادة، ينبغي كتابتها ويجب أن يؤشر كاتب التحقيق أو ضابط الشرطة القضائية على كل نسخة بمطابقتها للأصل، كما أنه يجب عند التأشير على النسخة ذكر جميع البيانات الواجب توافرها في المحضر، وكل المؤهلين في تحريره.

---

[1]- نص المشرع الجزائري في المادة 47 بعد تعديلها بموجب القانون رقم06- 22 المؤرخ في 20 ديسمبر 2006 على إجراءات جزائية " **عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال أو الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف ، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص ".**

[2]- عفيفي كامل عفيفي، مرجع سابق، ص.65.

لم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تتطلبه القواعد العامة في المحاضر عموما، والتي تقتضي بأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره، وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[1]، ونفس الأمر بالنسبة لمحضر تفتيش نظم الحاسوب، فإنه يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسوب والإنترنت يرافقه للاستعانة به في مجال الخبرة الفنية الضرورية، وفي صياغة مسودة محضر التفتيش[2].

2 - الشروط الموضوعية للتفتيش في البيئة الإلكترونية:

يقصد بالشروط الموضوعية للتفتيش في الجرائم الالكترونية، الشروط أو الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له في المعتاد، ويمكن حصرها في ثلاثة شروط أساسية هي: السبب، المحل، الإذن بالتفتيش.

أ - وجود سبب للتفتيش في البيئة الإلكترونية:

من المتفق عليه في الحالات التقليدية أن سبب التفتيش إنما يعني السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث، يمكن إجماله بصورة مختصرة في وقوع جريمة ما جناية أو جنحة، واتهام شخص أو أشخاص معينين بارتكابهما أو المشاركة فيها، وفي قيام قرئن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو في مسكنه، أو بشخص غيره أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما يمكن تفصيله على النحو الآتي:

[1]- نبيلة هبة هروال، مرجع سابق، ص.236.

[2]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.113.

1 - وقوع جريمة إلكترونية سواء كانت جناية أو جنحة:

يقتضي المنطق لإجراء عملية التفتيش والذي الغاية منه هو جمع الأدلة التي تثبت وقوع الجريمة وكشف هوية صاحبها، ضرورة وقوع جريمة بصورة فعلية سواء أكانت جناية أو جنحة، أي بمفهوم المخالفة، لا يجوز التفتيش لمجرد ورود معلومات تبين و تشير إلى إمكانية وقوع جريمة في المستقبل، حتى ولو قامت التحريات و الدلائل[1] الكافية على أنها ستقع.

تطبيقا لمبدأ شرعية الجرائم والعقوبات لا بد أن يكون التفتيش ثابتا بطلب إذن[2] من الجهات المختصة، وهو ما قام به المشرع الجزائري من خلال القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004، حيث أدرج المشرع الجزائري فصلا خاصا – الفصل السابع- بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا أنه في بعض الأحيان تقع عدة استثناءات ويكون التفتيش رغم عدم قانونيته ساري المفعول خاصة فيما يتعلق بالحالات التي تمس المحرر الالكتروني.

ففي جرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات، تضمن هذا القانون استحداث نصوص عقابية على الاعتداءات الماسة بالأنظمة المعلوماتية وهي المواد 394 مكرر إلى 394 مكرر 7، تماشيا مع التشريع الدولي في مجال مكافحة الإجرام المعلوماتي خاصة الاتفاقية الدولية حول الإجرام المعلوماتي المبرمة بتاريخ 2001/11/08 من طرف المجلس الأوربي بمدينة بودابست (المجر)[3]، وأمام التوسع الكبير في استعمال الإعلام الآلي وظهور بوادر الاعتداء على الأنظمة المعلوماتية سواء على المستوى المحلي أو الدولي.

---

[1]- الدلائل تعني علامات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها بأن جريمة قد وقعت، وأن شخصا معينا هو مرتكبها، ومن ثم هي مجرد افتراضات قد لا تصلح وحدها سببا للإدانة، أو هو ذلك القدر الضئيل المبني على احتمال معقول تؤديه الظروف والاستنتاجات التي تكفي للاعتقاد بارتكاب جريمة، وتبرر اتخاذ بعض الإجراءات الماسة بالحرية الفردية ضمانا لحسن سير العدالة. أنظر خلد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.211.

[2]- يستغرق صور الإذن بعض الوقت وهذا يؤدى إلى تلاشي الدليل واندثاره بالمحو والإتلاف، وهذا يعيق الوصول إلى الدليل وتحصيله، فالجاني قد يحاول العبث بالدليل كي لا ينكشف أمره قبل صدور الإذن، للمزيد راجع في ذلك: موسى مسعود أرحومة، مرجع سابق، ص.9.

[3] - تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس في دورتها التاسعة بعد المائة ، في08 نوفمبر 2001، وفتح باب التوقيع على الاتفاقية في بودابست في 23 نوفمبر 2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية. للمزيد من التفاصيل حول نص الاتفاقية، على موقع: https://rm.coe.int/explanatory-report-budapest-convention-in-

2 ـ الاعتداءات العمدية على سلامة المعطيات:

نصت عليها المادتين 394 مكرر 1 إلى 394 مكرر 2 من قانون العقوبات[1] ونصت عليها كذلك المواد03 و04 و08 من الاتفاقية الدولية للإجرام المعلوماتي وتأخذ هذه الاعتداءات صورتين أو شكلين :

ـ الاعتداءات العمدية على المعطيات الموجودة داخل النظام :

وهي بدورها تأخذ أشكال ثلاثة ونصت عليها المادة 394مكرر 1 وهي: الإدخال، المحو، التعديل.

لا يشترط إجماع هذه الحالات بل يكفي حصول إحداها فقط حتى يقوم الركن المادي للجريمة وهذه الحالات تقتضي اللاعب في المعطيات سواء بإضافة معلومات جديدة أو تعديل ما هو موجود أو الإنقاص منه (الحذف) .

ـ الاعتداءات العمدية على المعطيات الموجودة خارج النظام:

نصت عليها المادة 394 مكرر 2 من قانون العقوبات وهدفها حماية المعطيات وهي خارج نظام المعالجة الآلية للمعطيات فمحل الجريمة هو المعطيات سواء كانت مخزنة على أشرطة أو أقراص أو تلك المعالجة أليا أو المرسلة عن طريق منظومة معلوماتية، ويكون استعمالها كوسيلة لارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات، وهنا تجرم أفعال التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإيجار في المعطيات، كما جرمت أفعال الحيازة والإفشاء والنشر والاستعمال لأي غرض كان للمعطيات المتحصل عليها عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

فيما يخص الجزاءات المقررة لهذا الصنف من الجرائم جاءت على النحو الآتي في حالة الاعتداءات العمدية على معطيات داخل النظام تكون العقوبة الحبس من 06 أشهر إلى 03

[1] - القانون رقم 04-15 المؤرخ في 10نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، جريدة رسمية عدد 71، صادر في 2004 المعدل والمتمم.

سنوات والغرامة من 500.000 د.ج إلى 2.000.000 د.ج [1](المادة 394 مكرر 1)، أما في حالة الاعتداءات العمدية على معطيات خارج النظام تكون العقوبة الحبس من شهرين إلى 03 سنوات وغرامة من 1000000 د.ج إلى 5000000 د.ج، هذا فيما يخص العقوبات الأصلية أما العقوبات التكميلية التي نص عليها المشرع في المادة 394 مكرر 6 فتشمل مصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، مع مراعاة حقوق الغير حسن النية.

3 ـ العقوبات المطبقة على الشخص المعنوي:

نص المشرع الجزائري في المادة 394 مكرر 04 على أنه: **" يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القسم، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"**[2].

4 ـ عقوبة الاتفاق الجنائي:

نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وعقوبة الشروع في الجريمة نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي، وتبنى المشرع الجزائري هذه العقوبة في المادة 394 مكرر 7 من قانون العقوبات فالجرائم الماسة بالأنظمة المعلوماتية ذات طابع جنحي، والقاعدة القانونية تنص على أنه لا عقوبة على المحاولة في الجنح إلا بنص صريح في القانون، لهذا فالمادة 394 مكرر7 نصت صراحة على معاقبة الشخص الذي يشرع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها .

أما المشرع المصري لم يجرم جميع صور الإجرام الإلكتروني، بخلاف المشرع الجزائري والفرنسي، بل اقتصر في الحماية على حماية برامج الحاسب الآلي وقواعد البيانات ضمن

[1] ـ المادة 394 مكرر 1 من قانون العقوبات الجزائري السالف الذكر.

[2] ـ المادة 394 مكرر 4 من القانون ذاته.

المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة (181) من القانون رقم (82- 02)[1] والخاص بحماية حقوق الملكية الفكرية.

5 ـ الفاعل الأصلي والشريك في اتهامهم بارتكاب جريمة إلكترونية:

لا يكفي لقيام سبب التفتيش مجرد وقوع جريمة ما سواء أكانت جناية أو جنحة، بل لا بد أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية[2] تدعوا إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أو شريكا، مما يستوجب اتهامه بها، وفي حالة العكس، كان على قاضي التحقيق أن يصدر أمرا بأن لا وجه لإقامة الدعوى.

لا يكفي وقوع الجريمة في بيئة الإنترنت، بل لا بد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء، أو بصيغة أخرى، يجب توفر دلائل كافية تدعو للاعتقاد بأن ذلك المشتبه فيه قد ساهم في ارتكاب تلك الجريمة، سواء كفاعل أصلي أو شريك[3].

ب ـ تحديد محل التفتيش في البيئة الالكترونية:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون وهو ذلك الذي يستودع في محل له حرمة، كالمسكن أو الشخص

[1] ـ المادة 181 من قانون رقم 82 لسنة 2002 بإصدار قانون حقوق الملكية الفكرية متوفر على موقع:
http://www.du.edu.eg/upFilesCenter/qaap/1388160304.pdf

[2] ـ يقصد بالدلائل الكافية في الجرائم الإلكترونية بأنها مجموعة المظاهر أو الأمارات المعينة التي تنهض على السياق العقلي والمنطقي لملابسات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة جريمة الإنترنت إلى شخص معين سواء بوصفه فاعلا أو شريكا، مثل ارتباط عنوان انترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور فاضحة مع رقم حساب المتهم لدى مزود الخدمات، ووجود رقمين للتلفون لديه يستخدمان في ذلك، للمزيد راجع في ذلك: هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة،1997.ص.68. شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص.282.

[3] ـ عمر محمد أبو بكر بن يونس، مرجع سابق، ص.842.

والرسائل[1]، ومحل التفتيش في الجريمة الإلكترونية هو الحاسب الآلي بمكوناته المادية والمعنوية[2]، وشبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش[3]، وتشمل جميع مكوناته المادية والمكونات المعنوية التي تشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقا لاحتياجات العميل، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة ومهارة تقنية في نظم الحاسب الآلي كمشغلي الحاسب الآلي وخبراء البرامج ومديري النظم المعلوماتية[4].

تجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون قائما بذاته، وإنما يشمله مكان أو عقار ما، أو يكون بصحبة مالكه أو حائزه، أي أن الشيء الذي يوجد فيه الحاسب الآلي هو بطبيعته شيء مادي (مكتب، منزل، عقار....)، أو شخصي[5] ـ كما هو الشأن في الحاسوب المحمول سواء أكان شخصيا أو هاتفا نقالاـ ، ولذلك وجب على سلطة التحقيق عند استصدارها لإذن التفتيش، أن تحدد محل ذلك الإجراء تحديدا دقيقا وكذا الغرض منه، وأن يتأكد من أنه مما يجوز تفتيشه، فهناك محالا لا يمكن تفتيشها لكونها تتمتع بحصانات معينة ومن أهمها الهيئات الدبلوماسية، وكذا الهيئات البرلمانية، وإلا كان باطلا[6].

لا يجوز وفقا للأصل العام حث سلطة التحقيق على إصدار قرارها بالتفتيش ومباشرته كما سبق ذكره، مجرد وقوع جناية أو جنحة، كما لا يكفي اتهام شخص معين بارتكابها أو المشاركة

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، عمان، 2011، ص.49.

[2]- أحمد الفضل، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2008، ص.301

[3] - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان، الأردن، 2011، ص.110.

[4]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والانترنت، مرجع سابق، ص388. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي، من 26إلى 28 أفريل 2003، ص.610. عبد الناصر محمد فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12إلى 14 نوفمبر، 2007، ص.20.

[5] - عمر محمد أبو بكر بن يونس، مرجع سابق، ص.865.

[6] - نبيلة هبة دروال، مرجع سابق، ص.865.

فيها، بل يجب أن تتوافر هناك شروط كافية في ذلك، فلا يجب عدم إجراء التفتيش إلا إذا توفرت للمحقق دلائل كافية على أنه يوجد في المكان، أو لدى شخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة المعلوماتية، أو أشياء متحصله منها أو أي محررات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى الشخص المتهم بارتكاب جريمة معلوماتية[1]، تجدر الإشارة هنا إلى وجوب الأخذ بعين الاعتبار الإجراءات القانونية التي يتم بها تفتيش المتهم أو منزله.

تطبيقا لمبدأ شرعية الجرائم والعقوبات، فلا محل لإصدار الإذن بتفتيش نظم الحاسوب إلا إذا كان المشرع قد نص صراحة على الأفعال التي تشكل جرائم من هذا النوع، كما أن الإذن بالتفتيش غير جائز إلا إذا كانت الجريمة جناية أو جنحة، ومن ثم تم استبعاد المخالفات لأنها قليلة الأهمية ولا تستحق التعرض لحريات الأشخاص أو انتهاك خصوصياتهم[2].

من المستقر عليه في التشريعات المقارنة أن الإذن بالتفتيش يلزم أن يصدر بناءا على تحريات جدية[3]، فيجب عدم إجراء التفتيش إلا إذا توفرت للمحقق دلائل كافية بأنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة المعلوماتية أو أشياء متحصله منها أو أي محررات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى الشخص المتهم بارتكاب جريمة معلوماتية أو غيرها، بالتالي يجب الأخذ بعين الاعتبار الإجراءات القانونية التي يتم تفتيش غير المتهم أو منزله، هذا من جهة ومن جهة أخرى فإنه يشترط أن يسبق ذلك التفتيش تحريات جدية تسوغ الأمر كله[4].

يلاحظ أيضا من خلال نص المادة 47 مكرر من قانون الإجراءات الجزائية أن المشرع الجزائري لم ينص على إذن التفتيش فيما يخص المحرر الإلكتروني، لكن ما يمكن استخلاصه،

[1] - خلد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.211.

[2] - هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص.121.

[3] - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.103.

[4] - هلالي عبد اللاه أحمد، نفس المرجع، ص.221.

هو أن الأمر يستوجب طلب الإذن لأجل تفتيش المحررات أو الرسائل الإلكترونية للتحقق من الأدلة، أو الوقائع المنصبة داخل المحرر الذي استخدم فيما يخل بالقانون بحد ذاته.

يختلف شرط الإذن باختلاف نوعية المحرر الذي يمتاز بالسرية، وبالتالي هناك ضرورة حماية هذا المحرر الذي يحتوي على معلومات بقدر السرية والخصوصية، وهذا حفاظا على حقوق أصحابها ولا تنتهك سرية هذا النوع من التعاملات، فالواجب تقرير بعض الحقوق لصاحب المعلومة التي يتضمنها المحرر الالكتروني.

الفرع الثاني

ضبط الأدلة في مجال الجرائم الماسة بالمحررات الإلكترونية

يعرف الضبط بمفهومه التقليدي بأنه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها[1]، تجدر الإشارة أن النتيجة الحتمية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه، فيختلف الضبط في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية وهي البيانات، المراسلات والاتصالات الالكترونية، أما الثاني فيرد على أشياء مادية، وقد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا واختلافا تشريعيا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبتة عليها[2]، ويرجع السبب في ذلك أن الضبط في الأصل لا يرد إلا على الأشياء المادية، كما تثار أيضا مشكلة صعوبة ضبط النظام أو الشبكة كلها، مقارنة بضبط العناصر المعلوماتية المنفصلة عن هذا النظام الذي يحتوي على عناصر لا يمكن فصلها، وعليه سنتناول في هذا الفرع مدى إمكانية ضبط أدلة الجرائم الإلكترونية **(أولا)**، ثم سنتعرض إلى مكونات هذه الأدلة محل الضبط **(ثانيا)**.

[1]- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.93. نبيلة هبة هروال، مرجع سابق، ص.264.

[2]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.218. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.114

أولا: مدى إمكانية ضبط أدلة الجرائم الإلكترونية

يرد الضبط بحسب الأصل على أشياء مادية، فلا وجود للصعوبة في ضبط الأدلة في الجرائم الواقعة على المكونات المادية للنظام المعلوماتي، ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في الجريمة ، وذلك لعدم وجود دليل مرئي في هذه الحالة ولسهولة تدمير هذا الأخير في ثواني معدودة[1].

اختلفت التشريعات المقارنة وتعددت الآراء الفقهية حول ضرورة أن يترتب عن تفتيش المكونات المعنوية للحاسوب، أن يترتب عليها أثرا مباشرا في إباحة ضبطها، وانقسمت إلى ثلاث اتجاهات رئيسية :

الاتجاه الأول:

يرى أنصار هذا الاتجاه أنه من غير المتصور أن يرد الضبط على مثل تلك البيانات لانتفاء الكيان المادي عنها، وأن ذلك الإجراء يمكن أن يتم إلا في حالة إذا ما جسدت هذه البيانات الإلكترونية في دعامة مادية، كما لو كانت مطبوعة في مخرجات الحاسوب، أو في أي وعاء آخر للبيانات، أو في حالة التصوير الفوتوغرافي لشاشة الحاسوب[2].

الاتجاه الثاني:

يذهب أنصار الاتجاه الثاني عكس الاتجاه الأول، فهم يرون وجود مانع من أن يرد الضبط على البيانات الالكترونية في حد ذاتها[3]، ويجد هذا الاتجاه تجسيده التشريعي والفقهي في كل من كندا والولايات المتحدة الأمريكية وبلجيكا[4]، فالمحقق الجنائي في هذه الحالة يصطدم بعوامل عدة تحول دون ضبطه للبيانات التي تعد دليلا على ارتكاب الجريمة، وتكمن هذه العوامل في عدم وجود دليل مرئي يمكن فهمه بالقراءة، بالإضافة إلى عدم وجود آثار مادية يمكن على

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.284.

[2] - بكري يوسف بكري، مرجع سابق، ص.2011.

[3] - هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص.201.

[4] - عمر محمد أبو بكر بن يونس، مرجع سابق، ص.869

أساسها الاستدلال على وجود دليل على ارتكاب الجريمة، ويتجلى ذلك في جرائم الاختلاس والتزوير التي تستعمل فيها التقنية الالكترونية، وحتى البيانات التي يمكن الوصول إليها يستطيع الجاني أن يدمرها في فترة زمنية قصيرة تعد بالثواني، بالإضافة إلى الخبرة الفنية المتطلبة لفحص هذه الأدلة لتحديد البيانات التي تصلح كأدلة إدانة للجاني من عدمه[1].

الاتجاه الثالث:

يأخذ أنصار هذا الاتجاه الموقف الوسط، وذلك بدعوتهم إلى ضرورة تدخل تشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط، لتشمل إلى جانب الأشياء المادية، الأشكال المختلفة للبيانات الالكترونية[2].

أدى هذا الاختلاف في الآراء الفقهية حول نطاق الضبط الالكتروني عن طريق الوسائل الفنية المستخدمة في الجريمة المعلوماتية، إلى قيام بعض الدول إلى تطوير النصوص التشريعية المتعلقة بتفتيش النظام المعلوماتي، وإلى إصدار تشريعات تتعلق بالقواعد الإجرائية الخاصة بمعالجة البيانات إلكترونيا.

أدخل المشرع الفرنسي تعديلات على قانون الإجراءات الجزائية الفرنسي لسد هذا الفراغ التشريعي في تفتيش النظام المعلوماتي يتعين نسخها على دعامات، ثم يتم تحريز هذه المعلومات في أحراز مختومة بالشمع الأحمر، وذلك بموجب قانون الأمن الداخلي رقم 239 لسنة 2003 حيث استحدثت المادة 01/57[3] التي تنص على أن البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي، يتعين نسخها على دعامات ثم يتم تحريز هذه الدعامات في أحراز

[1] - محمد حماد الهيتي، جرائم الحاسب الآلي، دار المناهج للنشر والتوزيع، الأردن، 2017، ص.239.

[2] - هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.94. نبيلة هبة هروال، مرجع سابق، ص.265. هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص.199.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص.218.

[3] - Article 176 1/3 de la Loi n° 2003- 239 du 18 mars 2003 pour la sécurité intérieure en France dispose que : « ***Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support . Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code*** ».

مختومة بالشمع الأحمر، كما أن فرنسا هي من الدول الموقعة على اتفاقية بودابست لسنة 2001.

تدخل المشرع الجزائري بموجب القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، أين استحدثت المادة 06 منه والتي تنص على أنه: **" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها، على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية....."**[1] .

يلاحظ أن المشرع الجزائري أجاز التفتيش في المنظومة المعلوماتية بالتالي أقر ضم البيانات والمعطيات الالكترونية إلى محل الضبط باعتبار هذا الأخير كأثر مباشر للتفتيش، كما استخدم مصطلح النسخ بدلا من مصطلح الضبط مثله مثل المشرع الفرنسي وذلك على اعتبار أن البيانات والمعطيات الالكترونية لا يمكن ضبطها مباشرة لأنها ذات طبيعة معنوية، بالتالي يستدعي ذلك أولا نسخها على دعامات تخزين الكترونية، ثم حجزها ووضعها في أحراز مع مراعاة إجراءات الضبط المنصوص عليها والمقررة في قانون الإجراءات الجزائية.

نعتقد أن الاتجاه الثالث هو الذي يجب أن تأخذ به الدول وذلك بإدماج أو ضم البيانات الالكترونية، إلى جانب الأشياء المادية في محل الضبط، فلا بد إذن من تطوير النصوص القانونية التقليدية المتعلقة بالتفتيش والضبط في جرائم المعلوماتية، لتشمل البيانات الالكترونية، فيجب أن يدخل في نطاق التفتيش والضبط، المكونات المعنوية للحاسب الآلي كالبيانات الإلكترونية والمراسلات والاتصالات الالكترونية، وإلا أدى ذلك إلى إيجاد العديد من الصعوبات أمام جهات التحقيق فيما يتعلق بجمع الأدلة التي تفيد في كشف الحقيقة في الجريمة المعلوماتية، وقد يؤدي عدم اعتبار المكونات المعنوية للحاسب الآلي من الأشياء التي تخضع

[1] ـ المادة 06 من القانون 09 ـ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها السالف الذكر.

للتفتيش إلى عدم قيام الجريمة المعلوماتية، وذلك متى كانت هذه المكونات المعنوية هي السبيل الوحيد للوصول إلى حقيقة الجريمة المعلوماتية.

ثانيا: مكونات الأدلة محل الضبط في جرائم المحررات الإلكترونية

لا تثور أية مشكلة قانونية عند القيام بالضبط على عناصر معلوماتية منفصلة مثل الأقراص والاسطوانات الممغنطة أو غيرها من هذه الوسائل، لكن الصعوبة تثار عندما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنها تحتوي على عناصر لا يمكن فصلها، ومع ذلك يتعين ضبطها لأنها تتضمن عناصر مهمة للإثبات في الجريمة، لذلك يتم إعمال مبدأ التناسب من أجل إقامة التوازن بين مصلحتين، مصلحة الدولة في كشف الحقيقة ومصلحة صاحب النظام في تسيير أعماله وعدم ضياع فرص الربح خاصة في المشروعات الاقتصادية[1].

1 ـ الأشياء التي يتم ضبطها من جراء التفتيش في النظم المعلوماتية:

تختلف عملية ضبط البيانات المعالجة آليا عن ضبط المكونات الملموسة كجهاز الحاسب الآلي وملحقاته، وتتم هذه العملية إما بأسلوب النسخ والذي يستخدم فيه برامج متخصصة، أو بأسلوب تجميد التعامل بالحاسب الآلي أو إحدى القطع المكونة له والتي استخدمت في ارتكاب الجريمة[2]، ويعتبر ضبط الحاسوب كوسيلة لارتكاب الجريمة من أهم وسائل الضبط في جرائم تكنولوجيا المعلومات، ومن بين هذه الوسائل نذكر على سبيل المثال:

أ ـ أسلوب النسخ:

يتمثل النسخ كإحدى أساليب الضبط المستخدمة في حالة عدم وجود إمكانية لضبط القطع الصلبة المتضمنة للمواد غير المشروعة[3].

[1] ـ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، مرجع سابق، ص358. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.116.

[2] ـ أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة العربية، مصر،2015، ص.78.

[3] ـ عمر محمد أبو بكر بن يونس، مرجع سابق، ص.871.

تتم طريقة النسخ من خلال نسخ المضبوطات الالكترونية باستخدام برامج معدة خصيصا لهذا الغرض بحيث يتم أخذ نسخة من البيانات أو المضبوطة الالكترونية ومن ثم يتم لصقها وخزنها باسم معين على إحدى وسائط النقل مثل: (DVD.CD .FLACHE DISK) أو غيرها من وسائل التخزين ونقل البيانات الخاصة بالجهة القائمة بالضبط، وتبقى بعدتها إلى حين انتهاء التحقيق أو المحاكمة، على أنه يفضل على رأي البعض حفظ نسخة أخرى من تلك المضبوطات لدى المحضرين بالمحكمة، كي تكون بديلا للأولى في حالة تلفها أو ضياعها[1].

ب ـ أسلوب التجميد:

تقوم هذه الطريق على تجميد التعامل بالحاسوب أو إحدى القطع المكونة له، والتي استخدمت في ارتكاب الجريمة، أو النظام المعلوماتي الذي تتواجد فيه المضبوطات الالكترونية والذي يتخذ عدة مظاهر، ولعل أبرزها هو نظام الضغط الذي يتم على محتويات القرص الصلب، وكذلك نقل المحتويات إلى أقراص صلبة متعددة أو ممغنطة، فهذا البرامج يقوم بتقليص حجم الملفات والمضبوطات عن طريق ضغطها داخل ملف أو عدة ملفات صغيرة الحجم بصيغة (ZIP) أو (RAR)، ومن دون أن يؤثر ذلك في سلامة تلك الملفات، بحيث تبقى محتفظة بكامل خواصها الأصلية، ومن ثم يتم حفظ الملفات المضغوطة على أقراص (CD ,DVD)، أو على قرص التخزين، ومن ثم يتم فتح الملفات المضغوطة على أي كمبيوتر آخر من خلال برامج خاصة مثل برنامج (winrar)[2].

يمكن ضبط الوحدات المعلوماتية الآتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم عن طريق:

- ضبط جهاز الحاسب الآلي وملحقاته: يعني ذلك أن ضبطه أمر مهم جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية وأنها مرتبطة بالمكان و الشخص الحائز على الجهاز، ولأجهزة الكمبيوتر أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه والتعرف على مواصفاته بسرعة.

[1] ـ أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية ، القاهرة، 2010، ص.158.

[2] ـ عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.289.

- ضبط المعدات المستعملة في شبكة الإنترنت وأهمها المودم وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.

وسائط التخزين المتحركة كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة والأشرطة المغناطيسية.

- ضبط البرمجيات فإذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

- ضبط البريد الإلكتروني والذي يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية، فهو يمثل إحدى الميزات الرئيسية للإنترنت، وأكثر خدماتها انتشارا واستخداما في جميع الشبكات المرتبطة بها، كما يعد هذا الأخير أول مكتشفات تقنية الإنترنت التي تم تحقيقها[1].

2 - قواعد تحريز المضبوطات المعلوماتية وتأمينها فنيا:

يتميز الدليل في جرائم الإنترنت بخصوصية مميزة فهو عبارة عن معطيات مخزنة في نظام معلوماتي أو إلكتروني، وعليه يجب أن يكون المحقق في مثل هذه الجرائم مؤهلا ومدربا على التعامل مع تلك الأدلة وإلا فإنه قد يساعد على إتلافها وإفساد دلالتها، لذا كان تأمين ضبطها مقتضيا، فضلا على الإجراءات التي وضعها المقنن للمحافظة على سلامة المضبوطات من المنقولات عامة[2]، اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث[3].

يمكن تجميع أبرزها تحت النقاط التالية:

[1]- مصطفى محمد موسى، مرجع سابق، ص.169. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.355.

[2]- تعرض هذه المضبوطات كغيرها على المتهم ، ويطلب منه إبداء ملاحظته عليها ويعمل بذلك محضر يوقع عليه المتهم أو يذكر فيه امتناعه عن التوقيع، وتوضع الأشياء و الأوراق التي تضبط في حرز مغلق كلما أمكن، ويختم عليها ويكتب عل شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء، ويشار إلى الموضوع الذي حصل الضبط من أجله ، ولا تفض الأختام إلا بحضور المتهم أو وكيله أو من ضبط عنده هذه الأشياء أو بعد دعوتهم لذلك، راجع في ذلك: المادة 45 و 84 من قانون الإجراءات الجزائية الجزائري، والمادة 55 من قانون الإجراءات الجنائية المصري.

[3] - نبيلة هبة هروال، مرجع سابق، ص.232.

1- ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها.
2- عدم ثني القرص لان ذلك قد يؤدي إلى تلفه وفقدان البيانات المسجلة عليه.
3- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة.
يجب التنويه إلى أنه إذا كانت المضبوطات المحرزة عبارة عن بطاقات ورقية مثقبة أو أشرطة متصلة من الورق، كتلك المستخدمة في طباعة مخرجات الحاسب الآلي، فيجب حمايتها من التعرض للتداول العنيف أو الخشن بتحريزها في علب أو صناديق معدنية مغلقة وتخزينها في ذات الظروف السابقة[1].
4- عدم تعريض القرص للأتربة والدخان.
5- عدم الضغط عليه بوضع أشياء ثقيلة ، وعدم كتابة بيانات اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص لأن الضغط بالقلم قد يفسد سطح القرص[2].

تختلف طريقة ضبط المعلومات المعالجة آليا عما هي عليه عند ضبط المكونات المحسوسة كالأقراص المرنة، المودم، والخادم...الخ..

نص المشرع الجزائري في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على وضع طريقين لضبط الأدلة الرقمية.
فالطريقة الأولى تكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز، حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية، أما الطريقة الثانية فتكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى.

يخضع الدليل الرقمي في ضبطه إلى قواعد تحرير الأدلة الجنائية عموما، لكن بما أنه له طبيعته الخاصة فإن عملية ضبطه وتحريره تحتاج إلى بعض الإجراءات الخاصة لحمايته

[1] - هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص.130.
[2] - هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي، مرجع سابق، ص.210.

والحفاظ عليه وصيانته من إمكانية العبث، وهو ما أوجبه المشرع الجزائري في المادة 3/06 من القانون 04/09 من أن على السلطات التي تقوم بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات، ومن هذه الإجراءات الخاصة في هذا الإطار نذكر على سبيل المثال:

- أخذ نسخة احتياطية عن المعطيات والعمل عليها لضمان عدم المساس بالدليل الأصلي.
- عدم تنفيذ برامج على الحاسوب مسرح الجريمة خوفا من إتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات وعدم السماح للمشتبه به بالتعامل مع الحاسوب.
- ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.
- عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدانه للمعلومات المسجلة عليه.

3 - الصعوبات التي تواجه المحقق أثناء عملية الضبط:

يحتوي النظام المعلوماتي أو الشبكة المعلوماتية على عناصر لا يمكن فصلها ومع ذلك يتعين ضبطها، لأنها تتضمن عناصر الإثبات فيلزم بالضرورة ضبط النظام أو الشبكة كلها وهو الأمر الذي قد يترتب عليه التوقف عن العمل في المشروعات صاحبة النظام، لذلك فإنه يتعين في هذه الحالة إعمال مبدأ التناسب والذي يقصد به اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة ولها علاقة بالجريمة[1].

- كما أنه قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات التحقيق الوطنية.
- من الصعوبات كذلك التي تعيق الوصول إلى ضبط الدليل الرقمي تلك الأحزمة الأمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحويها هذا النظام، ومما يزيد من صعوبة الأمر على المحقق الجنائي عدم معرفته لكلمات السر أو شفرات المرور أو شفرات ترميز البيانات وقد لا يبدي المشتبه فيه تعاونه في الكشف عن هذه الشفرات لجهات التحقيق[2].

[1] - شيماء عبد الغني محمد عطا الله،الحماية الجنائية للتعاملات الالكترونية، مرجع سابق، ص.358.

[2] - عمر أبو بكر بن يونس، مرجع سابق، ص.169.

ـ ضخامة البيانات التي من الواجب فحصها من قبل المحقق، وذلك نتيجة حجم الشبكة التي تحتوي على هذه البيانات، الأمر الذي يتطلب من الخبرة الفنية ما يلزم لتحديد البيانات التي تصلح كأدلة جنائية من عدمه[1].

نخلص في الأخير أنه وبالنظر لطبيعة هذه الجرائم فإنها لا تترك أثرا ماديا في مسرح الجريمة، بالإضافة إلى قدرة الجاني على إتلاف وتشويه الدليل في وقت قصير وتظهر جملة من التحديات.

فبالنسبة لإجراءات التفتيش، فإن الجرائم الماسة بالمحررات الإلكترونية تعتمد على نظم المعلومات وقد تتجاوزه إلى أنظمة أخرى غير نظام المشتبه به، وهذا الإجراء يعتمد على تمديد نطاق التفتيش على نظام غير نظام محل المشتبه به[2]، كما أن إجراءات الضبط لا تتوقف على جهاز الكمبيوتر بل تمتد من ضبط المكونات المادية إلى مختلف أجزاء النظام، وعليه فتمتد إلى المعلومات والمعطيات والبيانات والبرامج المخزنة في النظام، أو إلى النظم المرتبطة بالنظام محل الاشتباه وكل الأشياء ذات الطبيعة المعنوية، لأنها معرضة بسهولة للتلف والضياع، وتعتبر كلها بيانات معنوية كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ، وهي تثير جملة من الإشكاليات أمام القضاء من حيث مدى قبولها وحجيتها مع وسائل الإثبات التقليدية.

بالتالي فإن أهم التحديات التي تواجه الجريمة المعلوماتية تتمثل في :

ـ الحاجة إلى سرعة الكشف عن الجريمة وتعقبها و خشية ضياع الدليل، بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم[3].

ـ أن الجريمة الالكترونية هي جريمة في الغالب يتم ارتكابها عن طريق الحاسب الآلي ومن قبل أشخاص يستغلون معارفهم وقدراتهم في مجال المعلوماتية، للقيام بأفعال غير قانونية ومنافية

[1] ـ عفيفي كامل عفيفي، مرجع سابق، ص.355.

[2] ـ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص.47.

[3] ـ محمد أمين أحمد الشوابكة، مرجع سابق، ص..13.

للأخلاق بلغت حد المساس بالأمن العام في العديد من الدول، لأن البيانات والمعطيات قد توجد في شبكات وأجهزة تابعة لدولة أجنبية.

كما أن إثبات الجرائم الالكترونية يعتمد أساسا على أدلة لا يمكن استخلاصها إلا بإتباع ذات القواعد التي تحكم التقنية المعلوماتية، بالتالي لا بد من استحداث أساليب التحقيق لما يتلاءم مع الطبيعة الخاصة لهذه الجرائم، فمن حيث إجراءات التحقيق في جرائم المحررات الإلكترونية نجد أن أغلب التشريعات المقارنة تجيز البحث وضبط أي دليل يمكن أن يسهم في كشف الحقيقة عن جريمة ما، بما فيها البيانات المخزنة أو تلك المعالجة إلكترونيا عن طريق الحاسب الآلي، والقيام بأي شيء ضروري لجمع الأدلة الإلكترونية القائمة على وقوع الجريمة ونسبتها إلى فاعلها، وحماية هذا الدليل الجنائي الإلكتروني، ومن أهم هذه الإجراءات هي المعاينة والتفتيش والضبط، فمباشرة سلطات التحقيق بغية الحصول والوصول إلى الدليل الجنائي المستند من الواقعة الإجرامية يجب أن يتضمن ضوابط شرعية عند القيام بهذه الإجراءات، وأن أية مخالفة للقواعد العامة الإجرائية والمبادئ القانونية في تحصيل الدليل الجنائي يعد دليلا غير مشروع، بالتالي لا يجوز للقاضي أن يقبل به في إدانة المتهم، لأن أساس الأدلة التي يؤسس عليها حكم الإدانة يجب أن تكون مشروعة، فبطلان أي إجراء يمتد إلى جميع الآثار التي تترتب علية مباشرة، فالقانون يفرض على القاضي أن يلتزم بعدم قبول أي دليل تكون طريقة البحث عنه والحصول عليه غير مشروعة، بالتالي هناك ارتباط وثيق بين شرعية إجراءات التحقيق الجنائي ومشروعية الدليل الالكتروني المستمد منها.

المطلب الثالث

التسرب واعتراض المراسلات السلكية واللاسلكية كإجراءات حديثة في البحث والتحري

تعتبر الجريمة المنظمة من الجرائم التي يصعب تتبعها وذلك نظرا لتعدد صور الاعتداء عليها خصوصا بظهور الوسائل العلمية الحديثة، والتي يمكن من شأنها أن لا تترك أثرا يوحي بالإطلاع عليها، بالتالي أصبحت وسائل التحري العادية لا تستطيع مواجهة هذا النوع المستحدث من الجرائم، مما دفع بمعظم التشريعات على غرار المشرع الجزائري إلى ابتكار مجموعة من أساليب التحري الحديثة، ولعل أهمها أسلوب التسرب واعتراض المراسلات.

استحدث المشرع الجزائري في قانون الإجراءات الجزائية إجراءات جديدة تتمثل في التسرب واعتراض المراسلات السلكية واللاسلكية وذلك بموجب القانون رقم 06 -22 المعدل لقانون الإجراءات الجزائية، وذلك عملا منه على تطوير وتحديث وسائل البحث والتحري للكشف عن الأدلة والحجج في معاقبة الدولة كل من يخل بالنظام العام والأمن العام داخل المجتمع، بالتالي سنتعرض إلى عملية التسرب **(الفرع الأول)**، لنتناول اعتراض المراسلات السلكية واللاسلكية **(الفرع الثاني)**.

الفرع الأول

عملية التسرب

يعتبر التسرب أو الاختراق تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضباط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ويقدم المتسرب نفسه على أنه فاعل أو شريك[1].

[1]- حريزي ربيعة ، إجراءات جمع الأدلة ودورها في الكشف عن الجريمة، مذكرة لنيل شهادة ماجستير في القانون، كلية الحقوق، جامعة الجزائر 2001، ص59.

عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 بأنه: " **يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسئولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جنائية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف**".

أولا: شروط عملية التسرب:

أحاط المشرع الجزائري عملية التسرب بعدة شروط تستوجب مراعاتها عندما تقتضي ظروف التحري والتحقيق اللجوء إليها، وذلك لإنجاح عملية التسرب وتسهيل مهام الشخص المتسرب.

1- الشروط الشكلية:

اشترط المشرع الجزائري من خلال المادة 65 مكرر 11 ضرورة حصول المتسرب على إذن من وكيل الجمهورية المختص، وأن يكون الإذن مكتوبا وإلا كان الإجراء باطلا، بحيث حيث يذكر في الإذن وهوية ضابط الشرطة الذي تتم العملية تحت مسؤوليته، وأن يتم التسرب تحت إشرافه ومراقبته أو من قاضي التحقيق، كما وجب على مانح الإذن إخطار وكيل الجمهورية بذلك، كما يجب تحديد المدة المطلوبة في عملية التسرب، والتي لا يجب ألا تتجاوز 4 أشهر، ويمكن أن تجدد حسب مقتضيات التحري والتحقيق، ضمن نفس الشروط الشكلية، إلا أنه بالمقابل يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

يتم إبقاء الإذن بالتسرب خارج ملف الإجراءات حتى الانتهاء من العملية، وكل هذا من أجل الحفاظ على السرية المطلوبة بين القاضي وضابط الشرطة القضائية المشرف على عملية التسرب، بالإضافة إلى شرط وجود تقرير مسبق محرر وبشكل مفصل من طرف ضابط الشرطة القضائية، حتى يتمكن القاضي من الإطلاع على ظروف العملية ومتطلباتها.

2- الشروط الموضوعية:

الشرط الأول: يتمثل في تحديد نوع الجريمة والتي تمس بأنظمة المعالجة الآلية للمعطيات[1].

الشرط الثاني: أن يكون الإذن بالتسرب مسببا، بمعنى توضيح وبيان العناصر التي تبرر اللجوء إلى هذا الإجراء من طرف الجهات القضائية المختصة، بالإضافة إلى العناصر التي دفعت ضابط الشرطة القضائية المكلف بتنسيق عملية المراقبة المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل أصلي أو شريك[2]، بالإضافة إلى السرية لعملية التسرب لأن السرية في التحقيق عامل أساسي لضمان سير إجراءات العملية ونجاحها،فهي ليست فقط حماية للمتهم من التشهير الذي يمسه بسبب التحقيق، وإنما من أجل المصلحة العامة التي يهدف إليه التحقيق وهو كشف الحقيقة.

ثانيا: آثار عملية التسرب

يقوم العون المتسرب مباشرة بعد صدور الإذن بالتسرب بمباشرة المهام المنوطة به وذلك حسب ما يقتضيه عمله، وذلك بتسخير كل الوسائل المادية والقانونية، وبعد إتمام عملية التسرب أو انتهائها يقوم وكيل الجمهورية وقاضي التحقيق بالوقوف على التفاصيل الأساسية لارتكاب الجرائم، وتحرير محاضر لتقديمها كأدلة أمام القضاء[3]، وتجدر الإشارة أن بعد انتهاء ئ عملية التسرب فأن هذا العون المتسرب يمكن أن يتعرض إلى مخاطر جسيمة تمس بحياته أو حياة أفراد عائلته، بالتالي لا بد من حمايته، وهو ما نص عليه المشرع الجزائري في المادة 65 مكرر 16 من قانون الإجراءات الجزائية التي تنص على معاقبة كل شخص يكشف هوية ضباط الشرطة القضائية بالحبس من سنتين إلى 5 سنوات وبغرامة من 500000دج إلى 200000دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص تكون العقوبة بالحبس من 19 سنوات إلى 20 سنة والغرامة من 50000 د.ج إلى 1000000د.ج .

[1]- راجع نص المادة 65 مكرر 05 من ق.إ.ج..ج.
[2]- راجع نص المادة 65 مكرر 12 من نفس القانون.
[3]- راجع نص المادة 65 مكرر 14 من القانون ذاته.

الفرع الثاني

اعتراض المراسلات السلكية واللاسلكية

يعتبر اعتراض المراسلات السلكية واللاسلكية بأنه إجراء خاص يقوم على التدخل الوسطي لتحويل مسار المراسلات في خط مشترك بوسيلة ممغنطة، والقيام بتسجيلها ونسخها[1]، كما يقصد به أيضا التتبع السري والمتواصل لمراسلات المشتبه فيه قبل وأثناء وبعد ارتكاب الجريمة[2].

ورد في لجنة الخبراء للبرلمان الأوربي بسترانسبورغ المؤرخ في 2006/02/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية تعريف لإجراء اعتراض المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري من الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم [3].

ينصرف إجراء اعتراض المراسلات إلى اعتراض عملية البث والإرسال لبيانات الكمبيوتر، كما هو الوضع في اتفاقية بودابست الموقعة في 23نوفمبر 2011، والمتعلقة بالإجرام المعلوماتي، التجسس، التنصت على المعلومات والبيانات، حيث أشارت المادة 3منها على أن يقوم كل طرف من الدول الأطراف في الاتفاقية بإقرار هذه الإجراءات التشريعية وغيرها من الإجراءات الأخرى، كلما كان ذلك ضروريا لإصدار نص قانوني أو تشريعي بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكابها عن قصد، وذلك من حيث اعتراض خط سير البيانات دون وجه حق ويتم ذلك بالوسائل الفنية، لقطع عملية البث

[1]- مريم مسعود أحمد، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04 ، مذكرة لنيل شهادة الماجستير، تخصص القانون الجنائي، كلية الحقوق ، جامعة قاصدي مرباح، ورقلة، 2013، ص. 81.

[2]- عمارة فوزي، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة دار العلوم الإنسانية، كلية الحقوق، والعلوم السياسية، جامعة منتوري، قسنطينة،عدد 33 /2010، ص.236.

[3]- سعيداني نعيم، مرجع سابق، ص. 177.

والإرسال غير عمومية لبيانات الكمبيوتر إلى داخل منظومة الكمبيوتر، بما في ذلك ما ينبعث من منظومة كمبيوتر من موجات كهرومغناطيسية تحمل معها بيانات[1].

عرف المشرع الجزائري في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية، بأنه اعتراض تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات تكون على شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض.

أولا: السلطة المختصة بإصدار إذن الاعتراض

بالنسبة للقانون الفرنسي والمصري تعتبر السلطة القضائية هي المختصة عموما بإصدار هذا الإذن ويعد ذلك ضمانة لأزمة مشروعية الاعتراض على الاتصالات السلكية واللاسلكية، حيث أنها ضمانة ضد تعدي أجهزة الدولة على حرمة الحياة الخاصة بالتالي استلزم المشرع صدور الإذن بالاعتراض من قاضي التحقيق المختص أو من القاضي الجزائي، وحرمان النيابة العامة من إصدار هذا الإذن، وذلك للحد من سلطة هذه الأخيرة منعا لأي تعسف، ولكن في حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها وتبين لها ضرورة اعتراض المحادثات التلفونية للمتهم كان عليها طبقا لنص المادة 206 إجراءات مصري أن تحصل على إذن من القاضي الجزائي بمراقبة المحادثات التلفونية. بحيث لا يشترط أن يقوم قاضي التحقيق أو النيابة العامة في حالة صدور إذن من القاضي الجزائي بتنفيذ أمر الاعتراض بل لهما أن يعهدا ذلك لمأمور الضبط القضائي[2].

خالف المشرع الجزائري ذلك، وذلك في نص المادة[3] 65 مكرر 5، والذي يتضح من خلالها أنه يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عçن طريق وسائل الاتصالات السلكية واللاسلكية، أو وضع ترتيبات تقنية دون موافقة المعنيين، وذلك من أجل التقاط صور شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عامة، وتتم

[1]- خالد ممدوح إبراهيم،،فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.261.

[2]- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.174.

[3]- راجع نص المادة 65 مكر 5 من ق. إ. ج. ج .

هذه العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، أما في حالة فتح تحقيق قضائي تتم العمليات بناء على إذن من قاضي التحقيق وتحت رقابته مباشرة.

استحدث المشرع الجزائري نصوص قانونية تتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، حيث تضمنت عدة أحكام منصوص عليها في المواد 65 مكرر5 إلى 65 مكرر 10.

ثانيا: تسبيب الإذن القضائي الصادر باعتراض الاتصالات الالكترونية

يجب أن يكون الإذن مسببا أي متضمنا الأسباب التي تستدعي إجراء عملية اعتراض المراسلات، بمعنى أن تكون هذه الأسباب مبنية على تحريات جدية يتخذ منها أسبابا لإجراء عملية اعتراض المراسلات، فلوكيل الجمهورية أن يصدر الإذن باعتراض الاتصالات الإلكترونية بناء على ما يكتشف له من خلال العمليات المأذون بها تحت مراقبته مباشرة، والسبب في ذلك يرجع إلى أن هذا الإجراء يمس حريات الأفراد، فهو استثناء على القاعدة العامة والمتمثلة في حرمة الحياة الخاصة للأشخاص وحقهم في سرية مراسلاتهم واتصالاتهم.

المبحث الثاني

الحماية الجنائية الإجرائية للمحررات الإلكترونية في مرحلة المحاكمة

تعد مرحلة المحاكمة من أهم إجراءات الدعوى باعتبارها مرحلة حاسمة، إذ تعتبر عملية تقدير الأدلة جوهر الحكم، وليس باستطاعة القاضي إدراك الدليل والوصول إليه إلا بعد ممارسة سلطته التقديرية للأدلة محل الوقائع، فتتوقف سلامة الحكم على سلامة تقدير الأدلة، فسلطة القاضي الجنائي في قبول وتقدير الدليل الالكتروني يتحدد على أساس طبيعة النظام الإجرائي السائد الذي تتبناه مختلف التشريعات المقارنة وموقفها من حجية الدليل الالكتروني أمام القضاء، والذي يعتبر كباقي الأدلة يتم تقديره من طرف القاضي الجنائي، فهو على خلاف القاضي المدني أين لا يجوز له أن يستمد قناعته بما يقدمه له الأطراف في الدعوى من أدلة، وإنما عليه أن يكلف نفسه عناء البحث عن الدليل ذات الأثر في تكوين عقيدته، فهو يستعين بأي دليل يراه لازما سواء في مضمونه أو في كيفية تقديمه، كاستعانته بالشاهد المعلوماتي والخبرة التقنية أثناء المحاكمة، ويكمن ذلك خاصة في المسائل التي تتطلب استيعاب بعض النقاط التي لا يستطيع الإلمام بها أو التي تستعصي عليه فهمها، عن طريق تقديم الخبير التقني للتقرير الذي يعد البينة والدليل في الكشف والتثبت من محتوى المحررات الالكترونية، بالتالي على القاضي أن يراعي خصوصية هذه الأدلة العلمية الثابتة فلا حرية له في مناقشتها وإنما يناقش فقط الظروف والملابسات التي وجد فيها الدليل وطريقة الحصول عليه، بحيث أن قواعد الإثبات الجنائي تخضع لمبدأ المشروعية ذلك أن القاضي الجنائي ليس له مطلق الحرية في تكوين عقيدته من الأدلة غير المشروعة التي يتحصل عليها، فيقتضي عند إصداره للحكم أن يكون مبنيا على يقينية صحة ما ينتهي إليه من أدلة لا مجرد الظن والاحتمال، فنقص خبرة القاضي الجنائي في التعامل مع الجرائم الالكترونية ذات الطبيعة الفنية والعلمية المعقدة، يؤدي به إلى إخضاع الدليل إلى التقييم الفني من قبل خبراء المعلوماتية من أجل البحث عن مصداقيته وعدم التشكيك في قيمته، فهي مسألة فنية حتى وإن لم يتعرض ذلك الدليل إلى العبث فإن القاضي الجنائي لا يمكنه التشكيك في مدى حجيته ما لم يثبت عدم وجود أية علاقة تثبت أن الدليل المتحصل عليه له صلة مباشرة بالجريمة المرتكبة، بالتالي سنتعرض في هذا المبحث إلى سلطة القاضي الجنائي في

الاستعانة بالدليل المباشر أمام المحكمة **(المطلب الأول)** لنتناول سلطة القاضي في تقدير الدليل الإلكتروني **(المطلب الثاني)**.

المطلب الأول

سلطة القاضي الجنائي في الاستعانة بالدليل المباشر أمام المحكمة

تتمثل الأدلة القولية في الجرائم الماسة بالمحرر الالكتروني أساسا في الشهادة، فيمكن أن يصدر عن الحاسب الآلي معطيات تشبه الأدلة القولية التي يدلي بها الشاهد المعلوماتي[1]، أو التي يتم كتابتها فتصبح شهادة مدونة بصورة إلكترونية، ومخزنة على ذاكرة الحاسوب الرئيسية أو على دعائم خزن ثانوية، إذ يمكن أن تكون مخزنة بصورة محررات إلكترونية نصية متضمنة لشهادة أو اعتراف، أو مخزنة بشكل معطيات صوتية يمكن سماعها باستخدام الحاسوب[2].

تنصرف الخبرة كدليل إثبات إلى رأي الخبير الفني أو التقني إذا ما عرضت أثناء المناقشة، فالخبير يأخذ حكم الشاهد ويجوز استدعائه لسماع شهادته ومناقشته في التقرير الذي أعده وتقدم به، غير أن الخبير يختلف عن الشاهد من حيث الوقائع التي يشهد بها، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها، أما الخبير فشهادته فنية أي تنصرف إلى إيضاح مسألة تستعصي عن فهمها من قبل المحقق، ويترتب على ذلك أنه لا يجوز سماع الخبير كشاهد إذا كان إجراء الخبرة قد وقع باطلا، وسنتطرق في هذا المطلب إلى سلطة القاضي الجنائي في الاستعانة بالشاهد المعلوماتي **(الفرع الأول)**، ثم إلى سلطة القاضي الجنائي في الاستعانة بالخبير المعلوماتي أو الرقمي **(الفرع الثاني)**.

[1]- كانت بدايات الأخذ بنظام الشهادة الالكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبولها لنظام الشهادة طالما كانت هناك أسباب في القانون تدعوا إليه، للمزيد من التفاصيل أنظر في ذلك: خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.262

[2] - جميل عبد الباقي صغير، الانترنت والقانون الجنائي، مرجع سابق، ص.209.

الفرع الأول

سلطة القاضي الجنائي في الاستعانة بالشاهد المعلوماتي أثناء المحاكمة

لا يتقيد القاضي في نظام الأدلة الإقناعية للجرائم الالكترونية مثل الشهادة بأي نظام إثبات معين، وإنما يترك له حرية الإثبات وفقا لسلطته التقديرية في تقدير الدليل، ويترتب على ذلك، أن للقاضي الجنائي قبول أي دليل يمكن أن يتولد منه، وأنه هو الذي يقدر قدرته في الإثبات على قدر اقتناعه به، و تعد عملية الحصول على الأدلة الجنائية الرقمية من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، مما يستوجب الحال عند الاستعانة بالشاهد المعلوماتي أن يكون صاحب تخصص في نظم المعلومات، وأن تكون لديه معلومات كافية ومهمة حول كيفية الولوج داخل أنظمة المعالجة الآلية للمعطيات، وعليه سنتناول المقصود بالشاهد المعلوماتي في جرائم المحررات الالكترونية **(أولا)** ثم التزامات الشاهد المعلوماتي **(ثانيا).**

أولا: المقصود بالشاهد المعلوماتي في جرائم المحررات الالكترونية

يعتبر نطاق الإفشاء بالمعلومات الجائز والمطلوب من الشاهد المعلوماتي الإدلاء بها من المسائل المتعلقة بالدعاوى الجزائية في مجال المعلوماتية، أكثر المسائل إشكالية نظرا لوجود نظام خاص بها، وثمة أعمال لا تتصل بالشاهد بذاته بل ربما لا تتصل بشخص طبيعي وقد تكون متصلة بنظام إلكتروني، أو نحوه، كما أن الشاهد يعلم الكثير وجزء مما يعلم واقع ضمن إطار الخصوصية والسرية[1].

يعتبر الشاهد في الجريمة المعلوماتية بأنه ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد اسم الشاهد المعلوماتي وذلك تمييزا عن الشاهد التقليدي[2].

---

[1]- . محمد فالح رشدان العواني، مرجع سابق، ص.82.

[2] - خالد محمد المهيري، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، دار الغرير، دبي،2005، ص.508. محمد فالح رشدان العواني، مرجع سابق، ص.82. هلالي عبد الله أحمد، التزام الشاهد في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000، ص.23.

نص المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون 09-04 ، على أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[1].

قد يكون الشاهد المعلوماتي بهذا المفهوم واحدا وهذا من عدة طوائف أهمها:

ـ مشغلو الحاسب الآلي: هم الخبراء الذين لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به، واستخدام لوحة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج[2].

ـ المحللون: المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظم معين وتحليلها إلى وحدات منفصلة واستنساخ العلاقات الوظيفية منها، كما يقوم كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات[3] .

ـ المبرمجون: هم الأشخاص المتخصصون في كتابة أوامر البرامج[4]، ويمكن تقسيمهم إلى فئتين:

الفئة الأولى: هم مخططو برامج التطبيقات ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة موثوقة لتحقيق هذه المواصفات.

الفئة الثانية: هم مخططو برامج النظم ويقومون باختيار وتعديل وتصحيح برامج الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها[1].

---

[1] ـ المادة 5 /ب من القانون09 -04 السالف الذكر.

[2] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009، ص.79.

[3] ـ هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، مرجع سابق، ص.23.

[4] ـ عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، مرجع سابق، ص.612.

ـ مهندسو الصيانة والاتصالات: هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

ـ مديرو النظم: هم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[2].

يجب على الشاهد في الجرائم الالكترونية عامة وجرائم المحررات الالكترونية خاصة أن يقوم بتزويد سلطات التحقيق بجميع البيانات والمعلومات التي يعلمها، والتي تفيد في كشف الحقيقة وهو ملزما في ذلك، ومن العناصر الجوهرية التي يجب على الشاهد أن يخبر بها سلطات التحقيق البيانات والمعلومات المخزنة على الجهاز الالكتروني، وأن يقوم بطباعتها متى أمكن ذلك، ويجب على الشاهد الإفصاح عن كلمات المرور السرية التي يعلم بها، وعن الشفرات الخاصة بالبرامج والأنظمة[3].

ثانيا: التزامات الشاهد المعلوماتي

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله[4]، وذلك بصورة دقيقة ومحددة، وأن يتوخى الصدق والأمانة بحيث لا يقدم بيانات أو معلومات كاذبة أو مزورة[5]، فإذا كانت المعلومات مشفرة أو تحوي رموز، فعلى الشاهد المعلوماتي فك هذه الرموز وتلك الشفرات وتحويلها إلى اللغة المفهومة عند طلب سلطات التحقيق ذالك[6]، وبصدد التزام الشاهد

---

[1] ـ هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، مرجع سابق، ص.23.

[2] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي، مرجع سابق، ص.264. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال الجرائم المعلوماتية، دار الفكر العربي، القاهرة، ص.616. خالد محمد المهيري، مرجع سابق، ص.509.

[3] ـ يوسف خليل يوسف العفيفي، الجرائم الالكترونية في التشريع الفلسطيني، رسالة ماجستير، كلية الشريعة والقانون، جامعة غزة، 2013، ص.126.

[4] ـ عبد العال الديري، محمد صادق إسماعيل، الجرائم الالكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص.315.

[5] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.266.

[6] ـ عبد الله سيف الكينوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، رسالة ماجستير، كلية الدراسات العليا والبحث العلمي، جامعة الشارقة، 2012، ص.112.

بطبع الملفات الخاصة بالبيانات والإفصاح عن كلمات السر و الكشف عن مفاتيح الشفرات[1]، برز هناك اتجاهان:

الاتجاه الأول:

يرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات المخزنة، أو الإفصاح عن كلمات المرور السرية أو الشفرات الخاصة بالبرامج المختلفة، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[2].

الاتجاه الثاني :

يرى أنصار هذا الاتجاه أنه من بين الالتزامات التي يتحمل الشاهد القيام بها، هي طبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، حيث يرى اتجاه في الفقه الفرنسي، أن القواعد العامة في مجال الإجراءات تحتفظ بسلطاتها في مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم[3].

تفرض بعض التشريعات المقارنة على الشاهد المعلوماتي التزاما قانونيا يتمثل في تقديمه كافة المعلومات اللازمة للولوج إلى نظام الحاسوب، والتعاون مع سلطة التحقيق في هذا المجال.

حددت المادة 331 من قانون الإجراءات الجزائية الفرنسي واجبات الشاهد في الشهادة بخصوص الوقائع المستندة إلى المتهم أو بخصوص شخصية هذا الأخير أو أخلاقياته[4]، لذلك

---

[1] ـ خالد مرزوق سراج العتيبي، مرجع سابق، ص.105.

[2] ـ عبد العال الديربي، مرجع سابق، ص.316.

[3] ـ عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، مرجع سابق، ص.382.

[4] -Article 331 du C.P.P.F , Modifié par la loi n° 2019-222 du 23mars 2019- art 63(v), dispose que : « ***Les témoins doivent, sur la demande du président, faire connaître leurs nom, prénoms, âge, profession, leur domicile ou résidence, s'ils connaissaient l'accusé avant le fait mentionné dans l'arrêt de renvoi, s'ils sont parents ou alliés, soit de l'accusé, soit de la partie civile, et à quel degré. Le président leur demande encore s'ils ne sont pas attachés au service de l'un ou de l'autre...***

Les témoins déposent uniquement, soit sur les faits reprochés à l'accusé, soit sur sa personnalité et sur sa moralité. » .

ليس من واجب الشاهد في الجريمة الإلكترونية طبع ملفات البيانات المخزنة في ذاكرة الحاسوب، أو الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج[1].

نص المشرع المصري في المادة 99 من قانون الإجراءات الجنائية المصري، على أن لسلطة التحقيق أن تأمر الشخص الذي يحوز شيء ترى ضبطه أو الاطلاع عليه أن يسارع بتقديمه، فإذا امتنع يجوز معاقبته بالعقوبة المقررة للامتناع عن الشهادة على أن يعفى من هذه العقوبة في الحالات التي يجوز له فيها الامتناع عن الشهادة قانونا[2].

نص المشرع الجزائري في المادة 10من القانون09- 04[3] المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تلزم مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية، لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها، كما يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، كما نص في المادة 19من المرسوم الرئاسي رقم 15-261[4] على إمكانية الاستعانة بأي خبير أو أي شخص يمكن أن يساعدها في أعمالها.

يمكننا القول مما سبق انه نتيجة قصور أحكام الشهادة في الحصول على الدليل الالكتروني، فإن أغلبية الفقهاء يرون ضرورة البحث عن وسيلة قانونية جديدة تحقق ما لم تستطع فكرة الالتزام بأداء الشهادة أن تؤديه، وهذه الوسيلة هي "الالتزام بالإعلام في الجريمة المعلوماتية"، وقد تستعمل بعض الدول وسائل للضغط على الشهود بهدف حملهم على التعاون الايجابي مع

[1] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.84.

[2] ـ راجع نص المادة 99 من قانون الإجراءات الجزائية المصري المعدل بالقانون 95 لسنة 2003 الصادر بالقانون رقم 150 لسنة 1950على موقع: http://laws.jp.gov.eg/

[3] ـ القانون 09- 04 السالف الذكر.

[4] ـ مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8أكتوبر سنة 2015 ، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، ص.16.

سلطات التحقيق، حيث يسأل الشاهد الذي يخفي الشفرة أو كلمة السر أو الذي يعطي أوامر خاطئة عن جريمة شهادة الزور، لأنه يعوق سير العدالة أو يسأل باعتباره شريكا في الجريمة موضوع المحاكمة[1]، كما أن جل القوانين المقارنة اتفقت حول الإجراءات التي تتخذ بحق الشاهد الذي يمتنع عن تقديم معلومات للسلطات المختصة تفيد رجال القضاء في الكشف عن الدليل الذي يسهم في القبض على الجاني، خصوصا إذا كانت المعلومات المتوافرة لديه هي معلومات قيمة فإن هذا الشاهد يستحق العقاب كجزاء يفرض عليه.

الفرع الثاني

سلطة القاضي الجنائي في الاستعانة بالخبرة التقنية أثناء المحاكمة

تكتسي الخبرة أهمية بالغة في مجال الجريمة الإلكترونية، نظرا أن النظم المعلوماتية تحتاج لخبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها، بالتالي يستوجب الحال عند الاستعانة بالخبير المعلوماتي أو الرقمي أن تتوفر لديه الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية، فلا يكفي مجرد حصوله على درجة علمية معينة وإنما يجب أن يكون متدربا على جميع أنواع الأدلة الرقمية وفحصها وتحليلها.

تزداد أهمية الخبرة في الجرائم عموما بل ربما تصبح ضرورية وحتمية في مجال الجريمة الالكترونية، والتي تحتاج عادة البحث وتدقيق أمور تقنية لاسيما مع تعدد أنواع الحاسبات وشبكات الاتصال وما يتصل بها، لذا يمكن القول أنه لا مناص في أغلب الأحوال من الاستعانة بأصحاب الخبرة الفنية المتميزة والمتخصصة في مجال النظام المعلوماتي، بل يكون نجاح التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها مرهونا بكفاءة هؤلاء الخبراء.

[1] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.85.

أولا: المقصود بالخبرة التقنية في استخلاص الدليل ذات الطابع الفني

تعرف الخبرة التقنية بأنها تلك الأدلة التي تنبعث من رأي الخبير الفني بناءا على معايير علمية، ويدور حول تقدير دليل مادي أو قولي قائم في الدعوى، والخبرة هي تقدير فني لواقعة معينة على أسس علمية[1]، وتعتبر الخبرة أحد أهم الوسائل في جمع الأدلة، يلجأ إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات.

تغير المفهوم السائد حديثا حول مفهوم الخبرة نظرا إلى التطور التقني في أنظمة المعالجة الآلية للمعطيات، بالتالي أصبحت للخبرة التقنية مكانة لها ضمن وسائل الإثبات أمام القضاء، فلا يمكن أن نتصور رفضها من طرف القضاء في القضايا المتعلقة بتقنية المعلومات، خاصة عندما يتعلق الأمر بجرائم المحررات الالكترونية، لأن القاضي أو المحقق في بعض الأحيان لا تتوفر لديه الخبرة الفنية والتقنية للكشف عن دليل ذات طابع فني، يمكنه من معرفة كيفية التفاعل مع هذه الأدلة الرقمية في إثبات الجرائم الالكترونية وكشف أنماطها[2]، فالغالبية العظمى من منسوبي أجهزة العدالة الجنائية لا يدركون شيئا عن الحاسب الآلي وتقنياته المتطورة ولغاته المتنوعة، خاصة عندما يواجه قاعدة خطيرة تتمثل في حداثة موضوع هذه الجرائم التي تتخذ من العالم الافتراضي مخبأ لها[3]، مما يستدعي من القضاء اللجوء إلى انتداب الخبراء لإجراء الكشف والتثبت من محتوى المحررات الالكترونية، ومن ثم تقدير التقرير الذي يعد كقيمة علمية دقيقة وكبينة ودليل يسهم في إثبات التهمة أو نفيها، لكن لا يعني أن هذا التقرير يلزم القاضي بالأخذ به في إصدار حكمه، لأن الدليل العلمي ليس آلية معدة لقبوله من طرف القضاء، وإنما للقاضي السلطة التقديرية في استبعاده أو الأخذ به وذلك حسب الظروف والملابسات المحيطة بذلك الدليل.

[1] - جميل عبد الباقي الصغير، مرجع سابق، ص.19.

[2] - خالد بن مرزوق بن سراج العتيبي، مرجع سابق، ص.65.

[3] - خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص.296.

ثانيا : دور الخبرة في الجرائم الماسة بالمحررات الالكترونية

إذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق، فهي أوجب في مجال استخلاص الدليل الالكتروني لإثبات الجرائم الماسة بالمحررات الالكترونية، حيث تتعلق بمسائل فنية غاية في التعقيد يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات[1].

يبرز دور الخبرة في الجرائم الماسة بالمحررات الالكترونية في:

ـ الكشف عن الدليل الإلكتروني الذي يمكن الاستناد إليه في إثبات شروع المجرم المعلوماتي في جريمته.

ـ إجراء الاختبارات التكنولوجية والعلمية على الدليل الالكتروني لاختباره والتحقق من مصدره.

- تحديد الخصائص الفريدة للدليل الالكتروني.

ـ إصلاح الدليل الالكتروني وإعادة تجميعه من المكونات المادية للنظام المعلوماتي.

- عمل نسخة أصلية من الدليل الالكتروني للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

- جمع الآثار المعلوماتية الرقمية من النظام المعلوماتي.

- استخدام الخوارزميات للتأكد من أن الدليل لم يتم العبث به أو تبديله.

- تحريز الدليل المعلوماتي لإثبات أنه أصيل وموثوق به.

- تحديد الخصائص المميزة لكل جزء من الأدلة المعلوماتية مثل المحرر الالكتروني.

- الوصف الدقيق للحاسب وأنظمته المختلفة، وأجهزته الطرفية، التأكد من عدم تأثير أعمال الاستدلال والتحقيق على الغير[2].

---

[1] - علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، محور القانون الجنائي، من 26-28 أفريل 2003، ص.285.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.302. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لإعمال التحقيق الابتدائي في الجرائم المعلوماتية، مرجع سابق، ص.235. خالد بن مرزوق بن سراج العتيبي، مرجع سابق، ص.69.

اهتم المشرع الجزائري وذلك نظرا لأهمية الخبرة في مجال التحقيق في الجريمة المعلوماتية حينما أشار في المادة 05 /ب من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه: **" يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها"**، يلاحظ أن المشرع الجزائري أنه ومن خلال هذه المادة أجاز للسلطات المكلفة بالتفتيش، ومن أجل الحصول على أية أدلة ضرورية في إنجاز المهام المنوطة بها، أن تكلف أي شخص له خبرة في النظام المعلوماتي من أجل المساعدة على تجميع وتحصيل المعلومات المتعلقة بمحل البحث.

ثالثا: شروط صحة أعمال الخبرة

حرصت أغلب التشريعات على تنظيم الخبرة ووضع شروط وضوابط لها:

1- شروط خاصة بتعيين الخبير:

حدد المشرع الجزائري بموجب المادة 144[1] من قانون الإجراءات الجزائية طرق اختيار الخبراء، وذلك عن طريق الجدول الذي أعدته المجالس القضائية بعد أخذ رأي النيابة العامة دون التقيد بترتيب معين، ويكون تحديد الأوضاع التي يجري بها قيد الخبراء، أو شطب أسمائهم بقرار من وزير العدل، كما أجاز المشرع الجزائري وبصفة استثنائية اختيار خبراء من غير المقيدين في أي من الجداول، لكن بشرط مبني بقرار مسبب مثل عدم وجود الخبرة التقنية المطلوبة، كما أجاز المشرع الجزائري للقاضي في نص المادة 147من قانون الإجراءات الجزائية الحرية في ندب خبير واحد أو عدة خبراء، وأضافت المادة 146[2] من نفس القانون

[1] - تنص المادة 144 من ق.إ.ج.ج على أنه:" **يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل، ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسو مقيدين في أي من هذه الجداول".**

[2] - تنص المادة 146 من نفس القانون على أنه: " **يجب أن تحدد دائما في قرار ندب الخبراء مهمتهم التي لا يجوز أن تهدف إلا إلى فحص مسائل ذات طابع فني".**

تحديد مهمة الخبراء التي لا يجوز أن تهدف إلا إلى فحص مسائل ذات طابع فني، كما أنه لم يحدد من خلال هذه النصوص طبيعة شخص الخبير إن كان شخصا طبيعيا أو معنويا.

أ- شرط أداء اليمين من طرف الخبير التقني:

نص المشرع الجزائري في المادة 145 من قانون الإجراءات الجزائية الجزائري بأنه يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي، كما يؤدي الخبير الذي يختار من خارج الجدول قبل فترة مباشرة مهمته اليمين السابق بيانها أمام قاضي التحقيق أو القاضي المعين من الجهة القضائية، كما أجاز المشرع الجزائري أداء اليمين بالكتابة، في حالة قيام مانع لأسباب يتعين ذكرها بالتحديد، ويرفق الكتاب المتضمن ذلك بملف التحقيق.

ب - تقرير الخبير وميعاده وشكله:

نص المشرع في نص المادة 148 معدلة من قانون الإجراءات الجزائية الجزائري[1] على أنه إذا لم يودع الخبراء تقاريرهم في الميعاد المحدد لهم، جاز في الحال أن يستبدل بهم غيرهم وعليهم إذ ذاك أن يقدموا نتائج ما قاموا به من أبحاث، كما عليهم أيضا أن يردوا في ظرف ثماني وأربعين ساعة جميع الأوراق والوثائق والأشياء التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم، وعلاوة على ذلك فمن الجائز أن تتخذ ضدهم تدابير تأديبية قد تصل إلى شطب أسمائهم من جدول الخبراء.

ج - القواعد الفنية التي تحكم عمل الخبير في مجال جرائم المحررات الالكترونية:

تتمثل القواعد الفنية التي تحكم عمل الخبير أن يتوافر لدى الخبير الإمكانيات والقدرات العلمية والفنية في مجال التخصص، كما يجب أن ينصرف رأي الخبير إلى الوقائع اللازم إصدار رأيه الفني بشأنها، وبالتالي نتطرق أولا إلى أساليب عمل الخبير في جرائم المحررات الالكترونية، ثم إلى الشروط التي يجب توافرها في عمل الخبير أثناء تأديته لمهامه المنوطة له.

[1]- راجع نص المادة 148 معدلة من ق.إ.ج.ج السالف الذكر.

1 ـ أساليب عمل الخبير في جرائم المحررات الالكترونية:

يتعين على الخبير التقني أثناء تأدية المهام الموكلة له إتباع أسلوبين هما:

ـ القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كجرائم النسخ، ثم يقوم بعملية تحليل رقمي لها، وذلك لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها، وأخيرا التوصل لمعرفة بروتوكول الانترنت"IP"[1]، الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع.

ـ القيام بتجميع وتحصيل لمجموعة المواقع الذي لا تشكل موضوعها جريمة في ذاته، ولكن الجرائم التي تقع من جراء تتبع موضوعات هذه المواقع، كما هو الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية[2] إلى غير ذلك من الموضوعات[3].

2 ـ الشروط الواجب توافرها في الخبير أثناء تأديته لمهامه:

يتحدد اختيار الخبير في مجال جرائم المحررات الالكترونية بنوعية الجريمة المرتكبة، وذلك نظرا أن الحواسيب الآلية وشبكة الاتصال ذات نماذج متعددة، بالتالي لا يوجد خبير لديه معرفة متعمقة مع كافة أنواع الحاسبات وبرامجها وشبكاتها، كما أنه ليس هناك خبير قادر على التعامل مع أنواع الجرائم التي تكون هذه الوسائل الالكترونية محلا لارتكابها أو أداة لها[4].

يتعين على الخبير في مجال الأدلة الالكترونية الجزائية أثناء تأديته لمهمته، أن يكون لديه العلم والخبرة والمهارة التي تمكنه من أداء مهمته على الوجه الأمثل و هي كما يلي:

---

[1] - IP :Internet Protocol

[2] ـ القنابل المنطقية أو الزمنية هي عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى بهدف تدمير وتخريب وتغيير برامج ومعلومات وبيانات الحاسوب في لحظة محددة، فهذه القنابل تضل ساكنة ودون فاعلية وبالتالي غير مكتشفة لمدة قد تطول أو تقصر يحددها مؤشر موجود في برنامج القنبلة، وهذا المؤشر لا يقتصر على المدة الزمنية وإنما قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة من داخل برنامج أو ملف معين، وذلك حسب الرمز الذي يحدده برنامج القنبلة، فإذا حل الميعاد أو توافرت هذه الشروط، بدأ البرنامج في القيام بمهامه التخريبية، ومن الأمثلة على القنابل المنطقية والزمنية في أنظمة الحاسوب هو قيام أحد المبرمجين الفرنسيين بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالجهة التي كان يعمل بها، تتضمن أمرا بتفجيرها بعد ستة أشهر من تاريخ فصله مما ترتب عليه تدمير كافة بياناتها، للمزيد راجع في ذلك: خالد عياد الحلبي، مرجع سابق، ص.ص. 86-87.

[3] ـ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.301.

[4] ـ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2001، ص.392.

1- نظم الحاسب الآلي بمكوناته المادية البرامجية.

2- وسائل وبرامج وطرق فحص نظم الحاسب الآلي[1] كبرامج كشف وإزالة الفيروسات، وبرامج استرجاع المحررات وإصلاح التالف منها وإظهار المخفي منها، وبرامج فك الشفرات وكلمات السر.

3- وسائل وبرامج نسخ البرامج والملفات، وعمل نسخ من القرص الصلب طبق الأصل.

4 - كيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث. .

5- كيفية تفسير الملاحظات والربط بين الأشياء واستخلاص نتائج دلالة علمية فنية قضائية[2].

6- التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها[3].

يمكن القول مما سبق أن الخبرة في مجال الجرائم المعلوماتية لها صلة وثيقة بأنظمة الحاسب الآلي وشبكات الاتصال المرتبطة بالتخصصات العلمية والفنية الدقيقة، ومع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها، بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم، فأهمية الاستعانة بالخبير في مجال الجرائم الماسة بالمحررات الالكترونية تظهر خاصة عند غياب الخبير، إذ لا يمكن كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب الفنية والتكنولوجية التي ارتكبت بواسطتها هذه الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه.

[1]- أتاح استخدام الحاسب الآلي في وقتنا المعاصر إنجاز العديد من الأعمال عن طريق نظام تبادل رسائل البيانات الموقعة توقيعا إلكترونيا عبرها، وتحميلها على دعامات غير ورقية ومن ثم استرجاعها على ورق مكتوب، فبفضل هذا النظام تعمل العديد من المنشآت التجارية التي تنشط في مجال التجارة الدولية إلى تحسين العملية الإنتاجية والإدارية بين وحدات الإعمال وبعض القطاعات راجع في ذلك:

BOCHURBERG Lionel, internet et commerce électronique, 2e edition, DELMAS, Paris, 2001, p196.

[2] - محمد نافع فالح رشدان العدواني، مرجع سابق، ص.90.

[3] - عبد الله حسين علي محمود، مرجع سابق، ص.395.

المطلب الثاني

سلطة القاضي الجنائي في تقدير الدليل الالكتروني

لا يمكن لسلطة القاضي الجزائي في تقدير الدليل أن تتوسع في شأنها إلى حيث يمكن القول أن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الالكتروني، فضلا عن ذلك فإن هذا الدليل يتمتع من حيث قوته بقيمة إثباتيه قد تصل إلى حد اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل[1].

يعتبر الدليل الالكتروني مشروعا من حيث الوجود على اعتبار أن المشرع لا تعهد عنه سياسة النص على قائمة أدلة الإثبات، وذلك فمسألة قبول الدليل الالكتروني لا ينال منها سوى مدى اقتناع القاضي بها، إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي[2].

تكمن حرية القاضي الجنائي في قبول الأدلة مسألة قانونية لا مجال لأعمال سلطة القاضي التقديرية فيها، حيث أن أغلب التشريعات حسمت هذه المسألة بتحديدها للنموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى ما توافرت شروط هذا النموذج طبقا لمبدأ الشرعية الإجرائية، وجب على القاضي إخضاعه لعملية قبوله، أما حرية القاضي الجنائي في تقدير الأدلة فمسألة تتعلق بقيمة الدليل لإثبات الحقيقة، وهي مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة، حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة[3]، وعلى ذلك لا بد من تحديد ماهية الدليل الإلكتروني وذلك بتعريفه وتحديد خصائصه وأنواعه وتبيان مكانته بين أدلة الإثبات الجنائي وذلك في **(الفرع الأول)**، ثم بيان نطاق سلطة القاضي الجنائي في قبول الدليل الالكتروني من خلال ضوابط وأطر معينة،

[1] - محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الالكتروني، مجلة الحقوق، جامعة الكويت، العدد 2، 2012، ص.530.

[2] - هدى طالب علي، مرجع سابق، ص.132.

[3] - نضال ياسين الحاج حمو، دور الدليل الالكتروني في الإثبات الجنائي، دراسة تحليلية، مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد الأول، السنة 5، العدد19، جامعة المملكة، 2013، ص.197.

(الفرع الثاني)، ثم سنتعرض في **(الفرع الثالث)** إلى حجية الدليل الإلكتروني في الإثبات الجنائي، وذلك على النحو التالي:

الفرع الأول

ماهية الدليل الالكتروني في الإثبات الجنائي

أثر التطور الذي لحق بالوسائل الالكترونية تأثيرا كبيرا على الأدلة المتحصلة منها وعلى إجراءات الحصول عليها، فهذا التطور جعل أكثر هذه الأدلة يتميز بطبيعة غير مرئية، بحيث يصعب الوصول إليها[1]، فالدليل الالكتروني يستمد طبيعته من ذات العمليات الالكترونية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة[2]، فالتلاعب بالمحررات الالكترونية لا يمكن كشفه بالطرق التقليدية وإنما قد يحتاج إلى الأدلة الالكترونية، والذي يستدعي استخدام تقنيات علمية فنية متطورة في إجراءات التحقيق من حيث إتباع إجراءات ذات طبيعة تقنية وفنية، وبالتالي في الوقت الحاضر يعد الدليل الالكتروني من الأدلة التي يعتمد عليها في إثبات الجريمة، وقد يبنى القاضي الجزائي حكمه على هذا الدليل، كما أن وسائل الإثبات الجزائي التقليدي كالشهادة والخبرة فإنها في أغلب الأحوال تحتاج إلى إثباتها بواسطة الدليل الإلكتروني، باعتبار أن المحررات الإلكترونية أداة من أدوات حفظ الأدلة الجزائية بصورة إلكترونية، بالتالي سنتناول مفهوم الدليل الإلكتروني في الإثبات الجنائي **(أولا)**، ثم سنتعرض إلى أنواع الدليل الإلكتروني **(ثانيا)**، ثم إلى المراحل التي يمر بها الدليل الالكتروني في الإثبات الجنائي **(ثالثا)**.

---

[1] ـ وهذا عكس الجرائم التقليدية، فجمع التحريات في واقعة معينة تخضع لسيطرة أجهزة العدالة والدليل فيها مرئي ومقروء، عكس الجريمة المعلوماتية التي تتم دون رؤية دليل الإدانة، وحتى في حالة وجود الدليل يمكن للجاني طمس الدليل أو محوه وفي حضور أجهزة العدالة غير المتخصصة، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق الإبلاغ عنها، راجع في ذلك: عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.24.

ـ كما أن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية وهي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة، راجع في ذلك : جميل عبد الباقي صغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص.15.

[2] ـ خالد ممدوح إبراهيم، التقاضي الالكتروني، مرجع سابق، ص.323.

أولا: مفهوم الدليل الالكتروني في الإثبات الجنائي

قابل التطور التكنولوجي في مجال تكنولوجيا المعلومات إلى إعادة تطوير الإجراءات الخاصة بالجرائم الالكترونية وخاصة في مجال المحررات الالكترونية، وذلك عن طريق أدلة إثبات خاصة وغير تقليدية عما هو منظم في قوانين الإجراءات الجنائية الحالية، نظرا للدور المهم الذي تلعبه الأدلة الالكترونية في الإثبات.

يعتبر الدليل الالكتروني الوسيلة الرئيسية للإثبات الجنائي في جرائم الانترنت وخاصة الجرائم المتعلقة بالمحررات الالكترونية، كما يوصف بأنه نوع متميز مقارنة بأنواع الدليل الجزائي، فهو مفهوم حديث ظهر مع ظهور الحواسيب الالكترونية وتقنية الانترنت ووجود الجرائم الالكترونية.

يتطلب بيان مفهوم الدليل الالكتروني إلى تعريف الدليل الالكتروني وموقف الفقه حول مكانة الدليل الالكتروني بين وسائل الإثبات الجنائي، ثم بيان خصائصه وأنواعه وأهميته في الإثبات الجنائي.

1 ـ تعريف الدليل الالكتروني:

يعرف جانب من الفقه القانوني بأنه **:" الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة[1]، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة، أو الصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[2].**

[1] ـ محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004، ص.969.

[2] ـ مشار إليه لدى : ممدوح عبد الحميد عبد المطلب، قواعد اعتماد الدليل الرقمي للإثبات في جرائم الإرهاب الالكتروني، بحث منشور في مركز بحوث شرطة الشارقة، شعبة العدالة الجنائية، 2007، ص10، عائشة بن قارة مصطفى، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، مصر، 2012، ص.50، ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر،2012، ص.88. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات

عرفه آخرون في نفس سياق هذا التعريف بأنه: **" الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا، أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور أو أشكال أو أصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو ألإدانة فيها"**[1].

يلاحظ على هاذين التعريفين أنهما يقصران مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي، ولا شك أن ذلك فيه تضييق لدائرة الأدلة الالكترونية، فهي كما يمكن تستمد من الحاسب الآلي فمن الممكن أن يتحصل عليها من أية آلة أخرى، فضلا عن ذلك أن الدليل الالكتروني فيما يخص المخرجات من الوسائل الالكترونية الأخرى، لا تكون لها حجية الدليل الالكتروني في الإثبات الجنائي ما دامت أنها نشأت في عالم افتراضي، وبالتالي هذا التعريف لا يدعم حجية المخرجات الالكترونية بصفة عامة في المسائل الجزائية.

عرف البعض الآخر بأنه: **" المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية، وهي معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة"**[2]، فهو الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة، فهو يتطلب الاستعانة بالأجهزة والمعدات الإلكترونية وباستخدام برامج ونظم خاصة، والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة إلكترونية.

الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول للأدلة والعلوم الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، ص.13.

[1] - مشار إليه لدى: عبد الناصر محمد محمود فرغلي، مرجع سابق، ص.13.

[2]- مشار إليه لدى: طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية، المنعقد في28،29 أكتوبر2009 والذي نظمته أكاديمية الدراسات العليا، طرابلس، ص.5.

2- موقف الفقه حول مكانة الدليل الالكتروني بين وسائل الإثبات الجنائي:

حتى يمكن بيان مكانة الدليل الالكتروني ضمن وسائل الإثبات الجنائي لا بد أن نبين رأي الفقه في ذلك، فلقد تباينت آراء الفقه حول مكانة الدليل الالكتروني بين أدلة الإثبات الجنائي فانقسم إلى اتجاهين:

- الاتجاه الأول:

يرى أن الدليل ما هو إلا مرحلة متقدمة من الأدلة المادية الملموسة، التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان، فهي إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات أو الراسم، وذلك بالاستعانة بجميع ما ابتكره العلم من أجهزة مختبريه ووسائل التقنية العالية ومنها الحاسب الآلي محور الدليل الالكتروني[1]، وإما أن تكون مخرجات غير ورقية، وإما أن تكون إلكترونية، كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الالكترونية غير التقليدية، وإما أنها تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به، أو الإنترنت بواسطة الشاشات أو وحدة العرض المرئي[2].

- الاتجاه الثاني:

يرى أن الدليل الالكتروني له طبيعته الخاصة التي تميزه عن غيره من أنواع الأدلة الجنائية الأخرى، ومن ثم يعد الدليل الالكتروني إضافة جديدة لأنواع الأدلة الجنائية الأخرى[3].

يلاحظ أن الاتجاه الثاني من الفقه الجنائي هو الاتجاه الأقرب إلى تحديد مكانة الدليل الالكتروني بين أدلة الإثبات الجنائي، نظرا أن الدليل الالكتروني يتمتع بخصائص تميزه عن باقي الأدلة الجنائية الأخرى، وذلك أن الدليل الالكتروني هو دليل فني ذو طبيعة تقنية خاصة نظرا إلى البيئة التي يستخلص منها، وهو العالم الافتراضي المبني على الكيفية المعنوية غير

[1] - محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص.235

[2] - أحمد هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص.14. نضال ياسين الحاج حمو، مرجع سابق، ص.185.

[3] - هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، مرجع سابق، ص.22.

الملموسة، فهذه الخصائص العلمية والمواصفات القانونية يؤهله ليقوم بوصفه إضافة جديدة تضاف إلى أنواع الأدلة الجنائية.

3 ـ أهمية الدليل الالكتروني في الجرائم الواقعة على المحررات الالكترونية:

يكتسي الدليل الرقمي أهمية كبرى ودور أساسي في معرفة كيفية حدوث الجريمة، ولتأكيد ذلك لا بد أن يحتوي التحقيق الجنائي الرقمي على هذا الدليل، ويجب أن يكون الأشخاص المسئولين عن التعامل على استعداد تام لمثل هذه الأمور غير الاعتيادية، ويكونوا على دراية وفهم واطلاع بالأمور التقنية وألاعيبها وكيفية التعامل معه[1]، فتظهر أهمية الدليل الالكتروني في دور التقنية التي تقوم على كشف الدليل الالكتروني، وهذا ما يقضي الاهتمام بهذا الأمر من ناحيتين :

الأولى: هي ضرورة الاهتمام بتقنية البرامج التي تتعامل مع الدليل الالكتروني، وهذا من ناحية اكتسابه، أو التحفظ عليه، وتحليله، وتقديمه.

الثانية: هي أن هذه البرامج في حد ذاتها يجب أن تكون مقبولة من مستخدميه في الحصول على هذا الدليل، فإطلاق الصفة الالكترونية على الدليل تعني بالضرورة وجود توافق بيته وبين بيئته، فلا وجود لدليل الكتروني خارج بيئته التقنية والالكترونية[2].

يعتبر الإثبات بالدليل الالكتروني الجزائي أهمية كبيرة في مجال جرائم المحررات الالكترونية خاصة والجريمة الالكترونية عامة، فهو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة لتطبيق حكم القانون عليها بإثبات حصول الجريمة من الناحية الواقعية بركنيها المادي والمعنوي، ونسبتها إلى المتهم، وقد ازدادت أهمية الدليل الالكتروني وفقا للسياسة الحديثة التي تهدف إلى توقيع العقاب الجزائي وفقا لشخصية المتهم، وعلى ذلك فإن الدليل الإلكتروني يفيد في أمرين:

[1] ـ عبد الناصر محمد محمود فرغلي، محمد سيف سعيد المسماري، مرجع سابق، ص.13.

[2] ـ فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، 2010، ص.649.

الأول: التقدير القانوني للجريمة من حيث ارتكابها ونسبتها إلى المتهم من أجل تطبيق العقوبات.

الثاني: التقدير الاجتماعي للمتهم من حيث ظروفه الشخصية وخطورته[1].

4 ـ خصائص الدليل الالكتروني:

يتميز الدليل الجنائي الالكتروني ذات الطبيعة الالكترونية في الإثبات الجنائي عن الدليل الجزائي التقليدي بالخصائص التالية:

أ ـ الطبيعة التقنية للأدلة الالكترونية الجنائية:

يعتبر الدليل الالكتروني من قبيل الأدلة ذات طبيعة تقنية وفنية وكيفية معنوية غير ملموسة[2]، بمعنى أنه ليس دليلا ماديا، وعليه يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات ومعدات وأدوات الحاسبة الآلية واستخدام نظم برامجية حاسوبية[3]، وبالتالي هذه العملية لا تعدوا كونها عملية نقل تلك المجالات المغناطيسية أو الكهربائية من طبيعتها الالكترونية على الهيئة التي يمكن الاستدلال بها على معلومة معينة[4].

ـ الأدلة الرقمية أدلة علمية:

يعتبر الدليل الالكتروني من قبيل الأدلة الفنية أو العلمية، وهو من طائفة ما يعرف بالأدلة المستمدة مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية، على ضوء ما يتم الوصول إليه من برامج وأجهزة وبرامج تقنية، وهو من طائفة الأدلة المستمدة من الآلة[5]، كما أن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية، وهذه الآثار بدورها إنما هي عبارة عن

[1] ـ عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت، مرجع سابق، ص.56.

[2] ـ عبد الناصر محمد محمود فرغلي، محمد سيف سعيد المسماري، مرجع سابق، ص.14.

[3] ـ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004،ص.234. طارق محمد الجملي، مرجع سابق، ص.6.

[4] ـ ممدوح عبد الحميد عبد المطلب، قواعد اعتماد الدليل الرقمي للإثبات في جرائم الإرهاب الالكتروني، مرجع سابق، ص.90.

[5] ـ محمود أمين البشري، نفس المرجع، ص.237.

نبضات إلكترونية غير مرئية بالعين المجردة[1]، فلا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية علمية جد متطورة، كما أنه لا يمكن الحصول على الدليل الرقمي أو الإطلاع على فحواه باستخدام الأساليب العلمية، وتفيد هذه الخاصية أيضا حين قيام رجال الضبط القضائي والاستدلال أو سلطات التحقيق أو المحاكمة بالتعامل مع الدليل الرقمي سعيا وراء إثبات الحقيقة، حيث يجب أن تبنى عملية البحث هنا على أسس علمية، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة[2].

- الأدلة الرقمية متطورة ومتنوعة بطبيعتها:

تعتبر الأدلة الرقمية متطورة بطبيعتها الديناميكية الفائقة السرعة بحيث تنتقل من مكان لآخر عبر شبكات الاتصال، متعدية لحدود الزمان والمكان وهذا نظرا أن البيئة الالكترونية غالبا ما تكون مؤلفة من شبكة منتشرة حول العالم، ومرتبطة بعضها البعض عن طريق شبكة الانترنت، بحيث تتيح الفرصة أمام مجرمي المعلوماتية المساس بالمحررات الالكترونية عن طريق الولوج عن بعد إلى البيانات الالكترونية المخزونة في أي مكان في العالم[3]، فالدليل الالكتروني يمكنه أن يسجل تحركات الفرد، بحيث يمكن من خلالها رصد المعلومات عن الجاني وتحليلها في ذات الوقت كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه[4]، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

نجد أيضا أن الدليل الالكتروني متنوع فهو يظهر بطريقة علنية في هيئات مختلفة الأشكال، كأن يكون إما بيانات غير مقروءة كما هو الأمر في حالة المراقبة عبر الشبكات والملقمات أو الخوادم، وقد يكون الدليل الالكتروني مفهوما للأشخاص كما كان وثيقة معدة بنظام المعالجة

[1] - جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص.115.

[2] - فتحي محمد أنور عزت، مرجع سابق، ص.648.

[3] - جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص.115.

[4] - ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، عدد رقم 4، المحور الأمني والإداري، الإمارات العربية المتحدة، دبي، 2003، ص.650.

TCP: بروتوكول نقل البيانات عبر الانترنت .

الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الالكتروني، وهذه الخاصية تستوجب مواكبة التطور في عالم التكنولوجيات[1] .

ب ـ صعوبة حذف الأدلة الالكترونية والتخلص منها:

يمكن الجاني استخراج نسخ من الأدلة الجزائية الالكترونية مطابقة للأصل ولها القيمة العلمية والحجية الثبوتية، الشيء الذي لا يتوفر في الأنواع الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل[2]، وما يزيد من صعوبة حذف الأدلة الالكترونية أنه يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها، وإظهارها بعد اختفائها، مما يؤدي إلى صعوبة الخلاص منها، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغائها أو محوها، سواء كانت محررات أو غيرها[3]، ويعتبر أيضا نشاط الجاني في سبيل محو الدليل الذي يدينه دليلا أيضا، وهذا لأن فعله هذا أي محاولته لإخفاء الدليل يتم تسجيله في الحاسب الآلي، ويمكن استخلاصه كدليل إدانة ضده[4]، كما أنها تمتاز بالسعة التخزينية العالية، فالذاكرة الداخلية للحاسوب يمكن تخزين مكتبة صغيرة في سعة واحدة.

يترتب على هذه الخاصية التي يتمتع بها الدليل مسائل هامة في القانون، أبرزها على الإطلاق مسألة التخلص منه، وهو الموضوع المعاقب عليه بمقتضى القانون، فمثلا إن إعداد برمجيات يتم التعويل عليها من مرتكبي جرائم الحاسوب عامة والانترنت خاصة، مهمتها هي التخلص من الأدلة بإزالة محتويات الحاسوب والبرمجيات التي يستخدمها هؤلاء في ارتكاب جرائمهم، حتى لو تضمنت إمكانية التخلص من الأدلة في جريمة معينة، فإذا أثبت الخبير التقني مثلا أن مرتكب الجريمة استخدم مثل هذه البرمجيات، فإنه يمكن إدانة مرتكب الجريمة

[1] ـ فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، مرجع سابق، ص.652.

[2] ـ عمر محمد بن يونس، الإثبات الجنائي عبر الانترنت، جامعة عين شمس، مصر، 2010، ص.45. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مرجع سابق، ص.6.

[3] ـ ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص.649.

[4] ـ عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.63.

بالنصوص التي تجرم مثل هذه الأفعال، ويعني ذلك أن الإلغاء أو الحذف للدليل الالكتروني هو في الحقيقة واقعة إخفاء له من قبل مرتكب الجريمة[1].

يتضح من خلال ما سبق أن الدليل الالكتروني يعتبر كأفضل دليل لإثبات جرائم المحررات الإلكترونية، فقد تعاظم دور الإثبات العلمي مع ظهوره، فهو يعد تطبيق من تطبيقات الدليل العلمي بل أكثر منه حجية في الإثبات، فهو يساعد القاضي على التقليل من الأخطاء القضائية إلى درجة أكبر نحو الحقيقة، بالتالي لا يمكنه أن ينازع في قيمة ما يتمتع به من قوة استدلالية قد استقرت بالنسبة له وتأكدت له من الناحية العلمية، ولا يعتبر هذا انتقاصا من سلطته التقديرية في تكوين اقتناعه من هذه الأدلة.

ثانيا: أنواع الدليل الالكتروني

يصعب الحصول على الدليل المادي في الجرائم المعلوماتية مقارنة بالجرائم التقليدية نظرا للبيئة غير المادية التي تتم فيها الجريمة، وهي في الغالب الحاسب الآلي أو شبكة الإنترنت، بحيث يمكن للجاني أن يعبث في بيانات الحاسب الآلي أو برامجه، أو في المحررات الالكترونية الموجودة فيه أو المرسلة عبر الانترنت، ويمكن محو الأدلة في ظرف قياسي قبل وصولها إلى يد القضاء[2]، فالدليل الالكتروني له عدة صور وأشكال، وتعد المحررات الالكترونية إحدى أهم

[1]- تكمن الخطورة في أولئك الذين يعملون داخل المؤسسات أكثر من العاملين خارجها، في شأن الجريمة المعلوماتية، وذلك لقدرة الموظفين بالداخل على إخفاء دليل الجريمة، فضلا عن أنها تكون أشد إيذاء بالجهة التي يعملون بها، ورغم استخدام المؤسسات والشركات والجهات الحكومية لحواجز حماية وتشفير، وتوقيعات إلكترونية، وأشكال أخرى من وسائل حماية المعلومات أو أنظمة حمائية أخرى عديمة القيمة، كما أن هناك فرصا أكبر أمام هؤلاء الموظفين لارتكاب جرائمهم دون اكتشاف أمرهم، سواء بالدخول إلى بنك المعلومات السرية والأسرار التجارية بغرض بيعها أو استخدامها في مؤسسة جديدة، للمزيد راجع في ذلك: عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2007، ص.110.

[2] - يفرض جانب من الفقه أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسئولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية، وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في تحقيق هذه الجرائم وينبغي عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية، وحتى يتم ذلك يرى هذا الجانب ضرورة الاستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها وشرح هذه الأدلة و أبعادها أمام المحاكم، للمزيد راجع في ذلك: محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص.52.

أنواع الأدلة الإلكترونية في مجال الإثبات الالكتروني الذي انعكس بدوره على الأدلة الجنائية الإلكترونية، والتي يمكن تقسيمها إلى الأنواع الأساسية التالية:

أ ـ الأدلة الالكترونية المتعلقة بجهاز الكمبيوتر وشبكاته:

تعتبر الأدلة الالكترونية المتعلقة بجهاز الكمبيوتر وشبكاته بأنها فعل غير مشروع على أجهزة الكمبيوتر، سواء وقع هذا الأمر على المكونات المادية له أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الكمبيوتر كالطابعة.

ب ـ الأدلة الالكترونية المتعلقة بالشبكة العالمية للمعلومات:

تعد الأدلة الالكترونية المتعلقة بالشبكة العالمية للمعلومات فعل غير مشروع قانونا ويقع على أي وثيقة أو نص موجود بالشبكة، مثل قرصنة المعلومات وسرقة أرقام بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج وغيرها، فهذه الجرائم تتطلب اتصالا بالإنترنت على عكس جرائم الحاسب الآلي التي قد يتصور حدوثها سواء كان هناك اتصال بالانترنت أم لا[1].

ج ـ الأدلة الالكترونية المتعلقة بالشبكة الدولية للمعلومات:

هو ذلك الفعل غير المشروع قانونا يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل جرائم الدخول غير المشروع لمواقع يمنع الدخول إليها، واستخدام عناوين غير حقيقية للولوج إلى الشبكة العالمية للمعلومات وغيرها[2].

د ـ الأدلة الالكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:

هي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، بحيث لا يعتبر استخدام الكمبيوتر أو الشبكة العالمية للمعلومات أو الانترنت في هذه الجرائم من طبيعة الفعل الإجرامي، بل تستخدم

[1] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع السابق، ص.72.

[2] ـ ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص.88.

كوسيلة مساعدة لارتكاب الجريمة، ففي هذه الحالة يحتفظ جهاز الحاسب الآلي بآثار إلكترونية يمكن أن تستخدم للإرشاد عن الفاعل[1].

يلاحظ من خلال هذا أن التنوع في الدليل الالكتروني بأنه ليس هناك وسيلة واحدة للحصول عليه وإنما تتعدد وسائل التوصل إليه، وفي كل الأحوال يضل الدليل المستمد منه رقميا حتى وإن أتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسسا على طابع افتراضي مبني على أهمية الدليل الالكتروني ذاته، وضرورته لكي يحدث التواصل بين القانون والدليل المذكور ـ نتيجة لنقص توافر الإمكانيات الالكترونية في المحاكم ـ يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلا أصليا، كذلك قسم الدليل الالكتروني لقسمين:

1 ـ أدلة أعدت لتكون وسيلة إثبات:

أ ـ المحررات التي تم إنشاؤها بواسطة الحاسوب تلقائيا، وتعتبر هذه المحررات من مخرجات الحاسوب التي لم يساهم الأفراد في إنشائها، مثل سجلات الهاتف وفواتير البطاقة البنكية[2].
ب ـ المحررات التي تم حفظ جزء منها بالإدخال وجزء تم انتشائه بواسطة الحاسوب مثل رسائل غرف المحادثة المتبادلة على الإنترنت ورسائل البريد الالكتروني[3].

2 ـ أدلة لم تعد لتكون وسيلة إثبات:

نشأ هذا النوع من الدليل الالكتروني من دون إرادة الفرد، وله أثر يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى بالبصمة الالكترونية، وتتجسد في الآثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسلة منه، أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسوب وشبكة الانترنت[4].

[1] ـ عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.73.

[2] ـ عبد الناصر حمد محمود فرغلي، محمد عبيد سيف المسماري، مرجع سابق، ص.13.

[3] ـ خالد عياد الحلبي، مرجع سابق، ص.24.

[4] ـ عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، مرجع سابق، ص.64.

ثالثا: المراحل التي يمر بها الدليل الالكتروني في الإثبات الجنائي

يجب على الدليل الرقمي في عملية التحقيق الجنائي حتى يتم اعتباره دليل رقمي معتمد من قبل القضاء أن يمر على المراحل التالية التي تكمن فيما يلي:

1 ـ مرحلة جمع الأدلة :

يتم في هذه المرحلة جمع كل الأدلة التي تم العثور عليها في مسرح الجريمة، والاحتفاظ بها عن طريق إرسالها إلى المختبر الجنائي، وأثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أي نوع من البيانات يمكن من خلالها الحصول على دليل جنائي رقمي، وعليها الحفاظ على النظام الرقمي وكامل القيم الرقمية ليتم تحديد الضرورية منها لاستخلاص الدليل لاحقا، كما يستلزم أيضا نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة، إلى الحاسب الخاص بالمختبر الجنائي الرقمي للاعتماد عليها، بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه.

2 ـ مرحلة فحص الأدلة:

يتم في هذه المرحلة القيام بالفحص والتحليل لجميع الآثار المرتبطة والمستمدة من مسرح الجريمة، ويشمل ذلك القيم الرقمية لتحديد نوع الدليل، حيث يتم الفحص في محتويات الوثائق والملفات والمسارات واستعادة المحتويات التي تم حذفها، ويجب أن يتم الفحص بالصيغة العلمية عن طريق استخدام البرامج والتطبيقات الخاصة بتحليل نظام الملفات والمسارات.

يهدف من وراء قيام عملية الفحص والتحليل إلى استنباط ثلاثة أنواع من الأدلة:
ـ دليل الإدانة، دليل البراءة، دليل محايد، وهذا الأخير يعتبر دليل غير مرتبط لا بالإدانة ولا بالبراءة، بل يستعان به في إثبات أنه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته، أو الاستعانة به كدليل[1].

[1] ـ ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص.125.

3 ـ مرحلة تحليل ومراجعة الأدلة:

تمثل هذه المرحلة في تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة.

4 ـ مرحلة القيام بتقرير بجميع الإثباتات الرقمية المستخرجة من الأدلة:

يتم من خلال هذه المرحلة إعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإيضاحية المصورة، أو المسجلة وغيرها لاعتمادها ثم تسلم إلى جهة الحكم والقضاء[1].

نخلص القول أن الدليل الجنائي الإلكتروني هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزتها وملحقاتها وشبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء، فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم الاعتداء على المحررات الالكترونية بهدف إثباتها ونسبتها إلى مرتكبيها، إلا أن الطبيعة الفنية الخاصة للدليل الإلكتروني قد تمكن من العبث بمضمونه على نحو يمكن للمجرم المعلوماتي العبث في المحررات المخزنة في الحاسب الآلي، أو التي يتم إنشائها أو إرسالها واستلامها عن طريق وسائل الاتصال الحديثة، وأن هذه المحررات لا يتم ضبطها إلا من طرف من لديه دراية بالأمور الفنية في الجريمة المعلوماتية، فالطبيعة الفنية المعقدة لهذه الجرائم أضفى عليها نوعا من الخصوصية في كل مراحل التحقيق الجنائي، بدءا من مرحلة جمع الأدلة إلى غاية مناقشتها أمام المحكمة، ويعتبر من الأمور التي تقف عائقا أمام الحصول على الدليل الالكتروني في مجال الجرائم الماسة بالمحررات الالكترونية، هو عدم ظهور الدليل المادي لهذا النوع المستحدث من الجرائم، فالدليل الالكتروني يكون عبارة عن نبضات إلكترونية غير مرئية تنساب عبر شبكات الحاسب الآلي، أين لا يمكن قراءتها إلا من خلال شاشة الحاسب الآلي، مما يمكن الجناة ويسهل عليهم إخفاء الأدلة المتحصلة من الوسائل الإلكترونية والقائمة ضدهم، عن

[1] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.150.

طريق محوها وإتلافها وتدميرها في زمن قصير جدا بحيث لا تستطيع جهات التحقيق من كشف جرائمهم إذا ما علمت بها، خاصة أن أغلب الأجهزة التي تقوم بالتحقيق ليست لديها المهارات والخبرة الفنية فيما يتعلق بكيفية التعامل مع هذه التقنيات الحديثة ونظمها وأساليب ارتكابها، مما يجعل فرصة الحصول على الدليل الالكتروني ضئيلة بالمقارنة مع الجرائم التقليدية.

الفرع الثاني

الضوابط التي تحكم قبول القاضي الجنائي للدليل الإلكتروني

يشترط لقبول القاضي الجنائي الدليل الالكتروني توافر عدة شروط كضرورة أن يتم الحصول على دليل رقمي مشروع ومقبول، بمعنى أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن **(أولا)**، ضرورة مناقشته إلى أن يتم اقتناع القاضي به على نحو يقين **(ثانيا)**، ويمكن تفصيل هذه الشروط كالآتي :

أولا : مشروعية الدليل الالكتروني

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة، ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته[1].

تعد مشروعية الدليل الالكتروني ضمانا كبيرا للحرية الفردية، إذ يترتب على استخدام وسائل غير مشروعة للحصول على الأدلة الرقمية بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجنائية، ومن أمثلة الطرق غير المشروعة استخدام الإكراه المادي أو المعنوي، أو الغش ضد الجاني في الجرائم المعلوماتية، من أجل فك الشفرة الخاصة بالدخول إلى النظام والوصول إلى الأدلة المتحصلة من الوسائل الالكترونية[2]، وأخذا بمبدأ المشروعية قرر المشرع

[1] - هلالي عبد اللاه أحمد، حجية مخرجات الكمبيوتر في المواد الجنائية، مرجع سابق، ص.104.

[2] - علي محمود علي حمودة، مرجع سابق، ص.38.

الدولي قاعدة يجب عدم إغفالها وإلا أصبح الحكم الصادر في الدعوى باطلا، وهي عدم قبول الأدلة المتحصل عليها خلافا لأحكام القانون أو لحقوق الإنسان المعترف بها دوليا، مثل الأدلة المتحصلة تعذيب أو معاملة مهينة أو لا إنسانية، طبقا لما نصت عليه المادة (7/69) من نظام المحكمة الجنائية الدولية[1].

يوجد نوعان للدليل الالكتروني من حيث المشروعية:

أ ـ مشروعية وجود:

بمعنى أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي، أي أن يعترف به من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز فيها القانون للقاضي الاستناد إليه في تكوين عقيدته، ويعتبر نظام الإثبات السائد في الدولة هو المعيار الذي يتحدد على أساسه سلطة القاضي في قبول الدليل الرقمي.

ب ـ مشروعية الحصول على الدليل الالكتروني:

يقصد بها أنه لقبول الدليل الالكتروني يجب الحصول عليه بطريقة مباشرة، أي أن الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن، ومشروعية الحصول على الدليل الالكتروني تستلزم توفر صفة القائم بالتفتيش، ومدى مشروعية التفتيش عن الدليل الالكتروني وضبطه في الوسط الافتراضي[2].

ثانيا: أن يكون الدليل الالكتروني محلا للمناقشة

يقصد بمناقشة الدليل الجنائي أن القاضي لا يمكن أن يؤسس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى الجنائية لها[3].

---

[1] ـ أحمد عبد الحكيم عبد الرحمان شهاب، نور عزم الليل بن مارني، شروط قبول الأدلة الالكترونية أمام القضاء الجنائي الفلسطيني، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07 ، عدد02، 2018، ص.177.

[2] ـ خالد عياد الحلبي، مرجع سابق، ص.246.

[3] ـ نضال ياسين الحاج حمو، دور الدليل الالكتروني في الإثبات الجنائي، دراسة تحليلية، مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد الأول، السنة 5، العدد19، جامعة المملكة ، كلية الحقوق، ص.203.

يطبق نفس الأمر بالنسبة لمخرجات الحاسب الآلي بوصفها أدلة إثبات، إذ ينبغي أن تطرح في جلسة المحاكمة، وأن يتم مناقشتها في مواجهة الأطراف، وهذا يعني أن مخرجات الحاسب الآلي سواء أكانت مطبوعات، أم بيانات معروضة على شاشة الحاسب الآلي، أو بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، كل ذلك سيكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[1].

يعتبرمناقشة حجية مخرجات الحاسب الآلي[2] في قوانين ذات الصياغة اللاتينية ـ الذي اقتصرنا الدراسة عليه فقط أين يسود مبدأ حرية الإثبات والاقتناع ـ بأن حجية هذه المخرجات لا تثير صعوبات سواء بالنسبة لمدى حرية تقديم مخرجات الحاسب الآلي لإثبات جرائم الحاسوب، أم بالنسبة لمدى حرية القاضي الجنائي في تقدير مخرجات الحاسب الآلي باعتباره أدلة إثبات في المواد الجنائية، ففي فرنسا مثلا نجد أنه إذا كانت الدراسات الفقهية التي تتعلق بتطور قانون الإثبات في المواد المدنية والتجارية قد تعددت، بهدف معرفة ما إذا كانت المحررات الموضوعة على دعامة مغناطيسية، لها نفس القيمة الدافعة المعطاة للمحررات المكتوبة تطبيقا لمبدأ هيمنة الكتابة، والذي يسمح بعمل أرشيف للنسخ الموثوق به والتي يمكن اللجوء إليه كأدلة إثبات غير مادية في المواد المدنية والتجارية، فإن مشكلة حجية المخرجات الكمبيوترية على المستوى الجنائي لا تبدوا ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة[3].

[1] ـ عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، مرجع سابق، ص.246.

[2] ـ المخرجات إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات أو الراسم، وإما أن تكون مخرجات لا ورقية أو إلكترونية، حيث تتزايد في الآونة الأخيرة كميات المعلومات المنتجة على أوعية لا ورقية أو غير مطبوعة كالأشرطة والأقراص الممغنطة أو الضوئية، وأسطوانات الفيديو والمصغرات الفيلمية وغيرها من الأشكال الالكترونية غير التقليدية التي تتوافر عن طريق الوصول المباشر حيث يقوك المستخدم بإدخال البيانات ويحصل على المخرجات في نفس الوقت. للمزيد راجع في ذلك: محمد فهمي طلبة وآخرون، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، موسوعة دلتا كمبيوتر، القاهرة، 1991، ص.331.

[3] ـ هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ورقة مقدمة إلى مؤتمر القانون والكمبيوتر والانترنت، المجلد الأول، ط3، من 1-3 مايو 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص.747.

تنطبق هذه الأحكام على كافة الأدلة المتولدة عن الحاسب الآلي، وتشمل أيضا شهود الجرائم الالكترونية، الذين تكون أقوالهم قد سبق الاستماع إليها في مرحلة التحقيق الابتدائي، فإنه يجب أن تعيد المحكمة سماع أقوالهم من جديد أمامها مرة أخرى إلا إذا حال عارض دون ذلك[1].

نخلص مما سبق أن القاضي الجنائي ليس له أن يأخذ بالأدلة الالكترونية المتحصل عليها في الدعوى الجنائية، أو نفيها إلا إذا طرحت خلال المحاكمة وفي حضور جميع أطراف الخصومة للمناقشة، ولا يختلف الأمر بالنسبة لمخرجات الحاسب الآلي، فهي أيضا تعد كأدلة إثبات يجب أن تطرح للمناقشة أثناء الجلسة.

ثالثا: وجوب يقينية الأدلة الالكترونية

يشترط في الأدلة المستخرجة من المنظومة المعلوماتية والإنترنت، أن تكون غير قابلة للشك حتى يمكن الحكم بموجبها بالإدانة ذلك أنه لا مجال لدحض قرينة البراءة، أو افتراض عكسها، إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين لا الشك والاحتمال[2]، وذلك لأنه إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة من اليقين تتساوى ابتداء في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ افتراض البراءة[3]، يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية من الوصول إلى يقينية هذه المخرجات عن طريق المعرفة:

- المعرفة الحسية التي تدركها الحواس من خلال معاينته هذه المخرجات وفحصها.
- المعرفة العقلية من خلال ما يقوم به من استقراء واستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها لم ينتهي القاضي إلى الجزم بنسبة الفعل أو الجريمة المعلوماتية إلى المتهم المعلوماتي، كان المتعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي، ليصل في الأخير إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه استنادا إليها[4]

[1] - نضال ياسين الحاج حمو، مرجع سابق، ص.203.

[2] - علي حسن محمد الطوالقة، مرجع سابق، ص.190.

[3]- جمال إبراهيم الحيدري، ضوابط اعتبار المخرجات الالكترونية أدلة إثبات في القضايا الجزائية، مكتبة السنهوري، بغداد، 2012، ص.55.

[4] - هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص.91

يتوقف تكامل هذا اليقين في ضمير القاضي على قدرة الأدلة المطروحة فيها المخرجات الالكترونية على توصيل القاضي إلى هذه المرحلة، بحيث أنه إذا استطاع القاضي إدراكها فإنه في هذا الفرض تتطابق حالة الذهن والعقل مع حالة الواقع والحقيقة، وعلى العكس من ذلك يتباعد مصطلح اليقين في حالة تشكك القاضي وعدم قدرة أدلة الدعوى ومن بينها الأدلة الناتجة عن الأجهزة الالكترونية بطبيعة الحال على توصيلة إلى تلك المرحلة من اليقين[1].

الفرع الثالث

حجية الدليل الالكتروني في الإثبات الجنائي

لا يكفي مجرد الحصول على الدليل الالكتروني للاعتداد به كدليل كاملا للإدانة أو البراءة، وهذا نظرا للطبيعة التقنية التي يتميز بها، فهو يثير مسألة الشك في مصداقيته كدليل يقدم أمام القضاء، نظرا أنه يمكن العبث بمضمونه على نحو يحرف الحقيقة التي يسعى القضاء جاهدا في الوصول إليها، دون أن يكون في مقدرة غير المتخصصين إدراك ذلك العبث، وإما أن نسبة الخطأ أو عدم النزاهة في إجراءات الحصول عليه واردة في هذا النوع من الأدلة.

حظيت حجية الدليل الالكتروني اهتمام فقهي وتشريعي، فسنتناول حجية الدليل الالكتروني في الفقه **(أولا)**، ثم سنتطرق إلى حجية الدليل الالكتروني في التشريع اللاتيني الذي يعتمد على نظام الإثبات الحر، دون الخوض في الأنظمة الأخرى نظرا أن أغلبية التشريعات أخذت بالصياغة اللاتينية كالمشرع الجزائري والفرنسي والمصري والقوانين الأخرى التي تأثرت به كالقانون الإيطالي والإسباني وقوانين أمريكا اللاتينية، وغيرها من القوانين الذي يسود فيها نظام الإثبات الحر**(ثانيا)**، وذلك على النحو التالي:

أولا: حجية الدليل الالكتروني في الفقه

اختلف الفقه الجنائي حول حجية الدليل الالكتروني نظرا لاختلاف أنظمة الإثبات الجنائي الذي أثر على موقف الفقه منه، الأنظمة اللاتينية تعتنق الأنظمة القانونية ذات الصبغة اللاتينية

[1] - جمال إبراهيم الحيدري، مرجع سابق، ص. 57.

نظام الإثبات الحر، حيث أن القاضي في هذا النظام يمتلك سلطة واسعة في قبول الدليل أو رفضه، فهو يعتمد في ذلك على اقتناعه الشخصي بذلك الدليل المعروض عليه والذي يبني عليه حكمه الذي استوحاه من الأدلة المطروحة أمامه للمناقشة في الدعوى الجنائية، فله السلطة التقديرية بالاعتداد به أو رفضه.

لعل أبرز القوانين التي اعتنقت نظام الإثبات الحر والتي منحته قيمة وحجية مساوية للدليل الجنائي التقليدي، يأتي على رأس هذه النظم القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الألماني والاسباني والايطالي، وكذلك القوانين المتأثرة بالنزعة الاشتراكية الحديثة، كالقانون الصيني لأنها قريبة من صياغة القانون الفرنسي، وأخيرا القوانين العربية كالقانون المصري والتونسي والجزائري بصفة عامة قوانين شمال إفريقيا، فهذه القوانين تتشابه في الصياغة، فمصادر القانون فيها واحدة وأصولها العامة متحدة والإصلاحات القانونية فيها متشابهة، وكذلك الأسلوب والصياغة متحدان أو على الأقل متقاربان، ونظام الإثبات الحر أو نظام الأدلة المعنوية هو السائد في هذه النوعية من القوانين[1]، فالفقه الفرنسي يدرس مسألة قبول الأدلة الجنائية الرقمية أمام القضاء الجنائي ضمن مجال أوسع، وهو مسألة قبول الأدلة الناتجة عن الأجهزة الإلكترونية الأخرى غير أجهزة الحاسب الآلي، فقد قضت محكمة النقض الفرنسية في قرار صادر بتاريخ 28أفريل1978،أن أشرطة التسجيل الممغنطة التي يكون لها قيمة في الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي، ومنه فالتسجيل الصوتي إلكترونيا بواسطة أجهزة خاصة بذلك، لا يحتمل الخطأ ويصعب التلاعب به، ويمكن للخبراء الفنيين أن يكتشفوا أي تلاعب أو محاولة إتلافه بواسطة وسائل تقنية عالية الكفاءة[2].

نلاحظ أنه في فرنسا كل الدراسات الفقهية التي تتعلق بتطور قانون الإثبات في المواد المدنية والتجارية، قد تعددت بهدف معرفة ما إذا كانت المحررات الموضوعة على دعامة مغناطيسية لها ذات القيمة القانونية للمحررات المكتوبة، ومع ذلك فإن مشكلة الدليل الالكتروني على

[1] ـ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، 2000، ص.114.

[2] ـ مشار إليه لدى :علي حسن محمد الطوالقة، مرجع سابق، ص.199.

النطاق الجنائي لا تبدو ملحة أو عاجلة في نظر الفقه الفرنسي، لأن الأساس هناك هو حرية تقديم وحرية القاضي الجنائي في تقدير الأدلة[1].

ثانيا: حجية الدليل الالكتروني في التشريعات المقارنة

اختلفت الأنظمة المقارنة في تقديرها لحجية الدليل الالكتروني، وهذا الاختلاف راجع إلى اختلاف نظم الإثبات الجنائي في الأنظمة المقارنة، فالأنظمة التي تأخذ بمبدأ حرية الإثبات وحرية القاضي في تقدير الأدلة، لا يوجد فيها ما يمنع من الاعتماد على الدليل الالكتروني في المسائل الجنائية، فمن بين التشريعات المقارنة التي أقرت وكرست لهذا المبدأ نذكر منها:

1 ـ القانون الفرنسي:

اعترف المشرع الفرنسي في قانون الإجراءات الجزائية مبدأ حرية الإثبات الجنائي صراحة بمقتضى المادة 427 [2]، حيث نص على أنه ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناءا على اقتناعه الشخصي .

2 ـ القانون المصري:

تعرض الفقه الجنائي في مصر وبالاستناد إلى مبدأ الإثبات الحر، إلى مسألة حجية هذا النوع من الأدلة على الرغم من خلو التشريع الإجرائي من التعرض لها، وأشار إلى أنه يمكن الاستناد إلى هذا الدليل في إثبات أو نفي الجريمة، وتكون له قوة القرائن في الإثبات[3]، إذ نصت المادة 291 من قانون الإجراءات الجنائية المصري على أنه: **"للمحكمة أن تأمر ولو من تلقاء نفسها**

[1]- نضال ياسين الحاج حمو، مرجع سابق، ص.198.

[2] - Article 427 du C.P.P.F , dispose que **: «** ***Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.***

***Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui* ».**

[3] - سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، بيروت، 2013، ص.367.

أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة"[1]، وعلى ذلك يكون للمحكمة أن تستند إلى الدليل الالكتروني لإثبات وقوع الجريمة أو نفيها.

3 ـ موقف المشرع الجزائري:

أقر المشرع الجزائري مبدأ حرية الإثبات الجنائي حيث منح للقاضي الحرية المطلقة في تقدير الأدلة لبناء حكمه، فله أن يأخذ بها أو يطرحها بناء على تقدير قيمة الأدلة المعروضة عليه استنادا للمنطق وللعقل، وهذا في نص المادة 212 من قانون الإجراءات الجزائية الجزائري، حيث نص على أنه: " **يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص**[2]**".**

بالمقابل أوجب المشرع الجزائري القاضي أن يضمن أحكامه الأسباب التي بني عليها، وأن يبني قراره على إظهار الأدلة والواقعة المستوجبة للعقوبة والظروف التي أحاطت بها، وذلك في الفقرة الثانية من نفس المادة أين نص على أنه: **" لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".**

نلاحظ أن المشرع الجزائري منح وأجاز للقاضي إثبات الجرائم بكافة طرق الإثبات، واستثنى في ذلك الأحوال التي ينص فيها القانون إثباتها دليلا معينا، وأجاز للقاضي الجنائي سلطة تقدير الدليل والحرية في تكوين اقتناعه الخاص من أي دليل يطمئن إليه، بشرط أن لا تكون هذه الأدلة التي يستند عليها القاضي في تقرير حكم البراءة أو الإدانة متناقضة بين بعضها البعض، بحيث يجب أن تؤسس قناعته على درجة عالية من الثقة، بالتالي فإن المشرع الجزائري اعتبر الدليل الرقمي الجنائي مثله مثل بقية الأدلة الجنائية الأخرى، والسلطة التقديرية التي يتمتع بها تمتد لتشمل جميع الأدلة الجنائية بما فيها الأدلة الرقمية.

نخلص مما سبق أن أغلب التشريعات الجنائية التي تبنت نظام الإثبات الحر استقرت وكرست هذا المبدأ، فأجازت الإثبات في المسائل الجنائية بكافة صور الأدلة أيا كان نوعها أو

[1] ـ المادة291 من قانون الإجراءات الجنائية المصري على موقع: http://laws.jp.gov.eg/

[2] ـ المادة 212 من قانون الإجراءات الجزائية الجزائري السالف الذكر.

طبيعتها، وجعل الأدلة متساوية في قيمتها مقبولة من حيث المبدأ خاضعة لتقدير المحكمة ومدى اقتناعها بها، وعلى ذلك فإن اختلاف دور القاضي الجنائي عن دور القاضي المدني يرجع أساسا إلى أن القانون الجنائي اعتنق مبدأ حرية الإثبات على عكس القانون المدني، فهو يعتبر نتيجة ضرورية لمبدأ الاقتناع القضائي، فالإثبات في الدعوى الجنائية يرد على وقائع مادية ولا يرد على تصرفات قانونية.

بالتالي فإن الاعتراف القانوني بالأدلة الالكترونية مع احتمالية ظهور أنماط جديدة لجميع الجرائم وخاصة في قطاع المعلومات المعالجة بواسطة الكمبيوتر، أدى بمعظم الدول إلى الاتجاه على الإقرار بحجية قانونية للمحررات الالكترونية من ملفات ومستخرجات الحاسب الآلي، والرسائل الالكترونية ذات الطبيعة الالكترونية المحضة وليس الطبيعة المادية لها.

خلاصة الباب الثاني

يتمثل الطابع الخاص الذي تتميز به الجرائم الإلكترونية عامة وجرائم المحررات الإلكترونية خاصة، أن محلها يكون غير مادي وأن إثبات هذه الجرائم يحيطها كثير من الصعوبات، والتي تتمثل أساسا في صعوبة اكتشاف هذه الجرائم باعتبارها جرائم فنية تتطلب تقنية معينة وخبرة في مجال التكنولوجيات الحديثة، إضافة إلى كونها أيضا لا تترك في الغالب أثرا ماديا ملموسا يمكن ضبطه، خاصة أنها في الغالب جريمة عابرة للحدود، فضلا عن أن المجرم المعلوماتي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات والتي تساعده على ارتكاب جرائمه.

تتعرض المحررات الإلكترونية بوصفها معلومات ذات قيمة مالية إلى مخاطر تهددها ومحلا للاعتداء عليها، طالما كانت هذه المعلومات قابلة للانتقال وقابلة للتملك والاستئثار ولها قيمته اقتصادية، مما أدى ذلك إلى اعتبارها محلا للحماية القانونية ويجب معاملتها معاملة المال، فأغلب التشريعات تعتمد بخصوص بعض الجرائم الماسة بالمحررات الإلكترونية على النصوص التقليدية كجريمة التزوير أو الاحتيال أو السرقة، بالتالي فإن اعتماد الحماية الجنائية من خلال هذه النصوص وتطبيق المبادئ المستقرة في القانون الجنائي عليها يعد مساسا مباشرا لمبدأ الشرعية، فالقاضي لا يستطيع أن يجرم أفعال لم ينص عليها التشريع حتى ولو كانت هذه الأفعال خطيرة على الجانب الاقتصادي، وهذا ما أقدمت عليه أغلب التشريعات الوطنية من خلال إعادة النظر بالتشريعات القائمة وذلك بتعديل بعض نصوصها بما يتماشى مع هذا النوع من الجرائم هذا من جهة، ومن جهة أخرى أدى اتساع نطاق الجريمة الالكترونية إلى ظهور عدة أنماط إجرامية مستحدثة وخاصة مع تعدد صور الأفعال الماسة بالمحرر الالكتروني، والذي يرتبط بالتقنيات الحديثة التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، كجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، وجريمة إتلاف المحرر الإلكتروني، مما أدى بأغلب الدول إلى إصدار تشريعات مستقلة للإحاطة بجميع الجرائم الإلكترونية.

تختلف مرحلة المحاكمة عن مرحلة التحقيق الابتدائي، فإجراءات التحقيق الابتدائي هي الإجراءات التي تسبق مرحلة المحاكمة وذلك للكشف عن الوقائع التي تعرض على سلطات التحقيق، ففي مرحلة التحقيق الابتدائي تثير جرائم المحررات الإلكترونية العديد من الصعوبات خاصة حول مدى قابلية نظم الحاسب الآلي والإنترنت للتفتيش والضبط والمعاينة، كما أن أغلب التشريعات بخصوص إجراءات جمع الأدلة تتم في إطار النصوص التقليدية، مما يترتب على ذلك أن سلطات التحقيق تواجه العديد من المشكلات في ضبط الأدلة المتعلقة بهذه الجرائم، لإضفاء قواعد وإجراءات خاصة لإجراء التفتيش والمعاينة والضبط في بيئة هذه الجرائم، فالتفتيش في جرائم المحررات الإلكترونية إما أن يكون عن المكونات المادية لوسائل التقنية الحديثة كالحاسب الآلي والإنترنت، وإما أن يكون عن المكونات المعنوية مثل البيانات والمعلومات وكل البرامج المعنوية التي تستخدم أنظمة الاتصال الحديثة، وذلك بهدف البحث عن الأدلة الموجودة عند معاينة مسرح الجريمة، وكل ما يفيد في كشف الحقيقة في الجرائم الماسة بالمحررات الإلكترونية، ومن أهم الإجراءات التي يسفر عنها التفتيش هي ضبط كل ما يتعلق بهذه الجرائم، بحيث تحرز وتحفظ وتثبت في محضر التفتيش والتي يمكن استخدامها فيما بعد أثناء المحاكمة كدليل إدانة ضد مرتكب الجريمة التي تمس بالمحررات الإلكترونية، بالتالي فالتعامل مع هذا النوع المستحدث من الجرائم استدعى تدخل مختلف التشريعات الوطنية، إما بتعديل النصوص القائمة حتى تتماشى مع الطبيعة الخاصة بجرائم المحررات الإلكترونية، وإما باستحداث نصوص خاصة مستقلة للإحاطة بها.

يستعين القاضي الجنائي في استخلاص الدليل المباشر بالشاهد المعلوماتي الذي لديه معلومات جوهرية للولوج لنظم المعالجة الآلية للمعطيات، بحيث يقوم هذا الأخير بتقديم للقاضي معلومات تحصل عليها عن طريق طبع البيانات المخزنة في ذاكرة الحاسب الآلي، أو الإفصاح عن كلمات المرور السرية، كما يمكن للقاضي الاستعانة أيضا بالخبرة التقنية في مسألة ما تخص القضية المعروضة أمامه، عن طريق تقديم الخبير التقني لتقارير وآراء ونتائج تحصل عليها من خلال تطبيق معايير علمية وأصول فنية دقيقة، ومن ثم عرضها

على القاضي لتكوين قناعته القضائية تجاهها، فلا بد أن يكون الدليل الذي يقوى على إثبات جرائم المحررات الإلكترونية من طبيعة إلكترونية هو أيضا.

تخضع المحررات الإلكترونية كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة، حيث يسود مبدأ حرية القاضي في تكوين عقيدته ولا يجوز تقييده بأي من القرائن والافتراضات، فيجب على القاضي الجزائي عند تقديره للأدلة الالكترونية في مجال الإثبات الجنائي، التمييز بين القيمة القاطعة للدليل أين لا يحق له مناقشة الحقائق العلمية الثابتة، وبين الظروف والملابسات التي وجد فيها هذا الدليل، أين يمكن أن يستند إليها في تكوين عقيدته بمعنى أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة، والكشف عنها دون أن يتقيد في ذلك بإتباع وسائل معينة للكشف عنها، كما له مطلق الحرية في تقدير أدلة الدعوى فله أن يأخذ بها أو يطرحها حسب عقيدته، فلا يلزم نفسه بإتباع الطرق المعروفة في الإثبات إلا إذا ألزمه القانون بذلك صراحة.

يمكن استخلاص الدليل الإلكتروني في أية مرحلة من مراحل الدعوى، فقد يتوصل إليه رجال الضبط الجنائي أو في التحقيق الابتدائي أو القاضي الجزائي، وهذا يعتمد على مقدار معرفتهم وقدرتهم ومهارتهم في التعامل مع الأنظمة المعلوماتية، فالقاضي الجزائي خول له القانون الاستعانة بأي دليل يؤدي إلى تكوين عقيدته واقتناعه بشكل مطمئن دون أن يكون ملزما ببيان أسباب ذلك، فمن غير المقبول أن يتخلى القاضي عن حقه إذا رأى لأي سبب من الأسباب أن لا يأخذ بتقرير الخبير عند استعانته به في المسائل الفنية البحتة.

فلكي يكون للأدلة الإلكترونية حجية في مجال الإثبات الجنائي أمام القضاء الجنائي يجب أن يكون قد تم الحصول عليها بطريقة مشروعة، وذلك من خلال احترام الضوابط القانونية التي يجب أن تتخذ في استخلاص الدليل الإلكتروني، بالإضافة إلى شرط يقينية الأدلة بحيث يجب أن تكون على درجة عالية من الثقة أين يمكن طرح هذه الأدلة للمناقشة أمام جميع الأطراف، فعدم مراعاة هذه الشروط قد تهدر قيمة الدليل وتشوب قضائه بالبطلان، ويؤدي إلى استبعاد الدليل الرقمي مباشرة وعدم قبوله.

خاتمة

خاتمة

لم يعد مفهوم المحرر مقتصرا على نوع الدعامة المرتبطة به والتي حرر من خلالها، فبعدما كان سابقا يرتبط هذا المفهوم بالدعامة الورقية، تغيرت البيئة التي قد ينشأ فيها هذا المحرر أو يتم نداوله فيها بفضل التطورات المستحدثة في الوسائل التكنولوجية الحديثة، بالتالي أصبح المحرر ذا طبيعة الكترونية يحتاج إلى دعامة إلكترونية، وحتى تواكب التطورات الحاصلة في تكنولوجيا المعلومات وتقنيات الاتصال وما نتج عنها من مكانة للمحررات الالكترونية ضمن وسائل الإثبات، والتي أصبحت واقعا مفروضا لا سبيل للتحكم فيه إلا بالاعتراف به وتنظيمه، لجأت هذه الدول وفي غياب نصوص قانونية صريحة إما إلى تعديل قوانينها الداخلية، أو إصدار قوانين خاصة بما يتلاءم مع حجية المحررات الالكترونية في الإثبات لتستجيب لهذه التطورات العالمية، والاعتراف بها في إبرام التصرفات القانونية والاستناد لها كأدلة للإثبات.

ركزت أغلب التشريعات المقارنة في تنظيمها للتعاملات الالكترونية على وضع البنية القانونية المنظمة لهذه التعاملات، والتي تتمثل أساسا في الاعتراف بالمحررات الالكترونية ومساواتها بالمحررات الكتابية التقليدية، فالمساواة الوظيفية بين المحررات في شكلها الإلكتروني بالمحررات بشكلها الورقي التقليدي يجب توافر مجموعة من الشروط التقنية والفنية، ومن ثم معادلتها بها في مجال الإثبات، وإضفاء الحماية القانونية عليها وبالتالي مساواتها من حيث القيمة القانونية، وتتلخص هذه الشروط في العناصر الأساسية في المحرر الإلكتروني وهي الكتابة الإلكترونية والتوقيع الإلكتروني، وسلامة المحتوى وثباته، ودون الاعتداد بنوع الدعامة التي تحملها مادام يمكن الاحتفاظ بها والرجوع إليها كلما دعت الحاجة إلى ذلك، فتحوز المعلومات التي تكون على شكل محرر إلكتروني حجية في الإثبات، على أن يؤخذ في تقدير هذه الحجية جدارة الطريقة التي استخدمت في إنشاء أو تخزين المحرر الالكتروني، والطريقة التي استخدمت في المحافظة على سلامة المعلومات، والطريقة التي حددت بها هوية منشئها أو لأي عمل آخر يتصل بالأمر.

يتعين حل مسألة تأمين المحرر الالكتروني من كل تعدي قد يمس ويؤثر على صحته، إيجاد نظام قانوني يتصدى لكل العوائق التشريعية والتقنية في حماية المحرر الالكتروني وتجريم الأفعال التي تهدد سلامته، وبالتالي استمرار المعاملات الالكترونية وزيادة الثقة فيها، ولغرض تأمين الحماية والثقة في التعامل بالمحررات الإلكترونية تم اعتماد نظام التصديق الإلكتروني، حيث يعتبر بمثابة وسيلة تحفظ سرية البيانات والمعلومات التي يتم تبادلها خلال التعامل بهذا النوع من المحررات، ومن خلال هذا النظام أيضا يمكن التأكيد على هوية الأطراف وصحة توقيعهم وهذا ما توفره لهم جهة التصديق الإلكتروني، من خلال إصدار شهادة التصديق الإلكتروني، كما يسعى المتخصصون بأمن المعطيات للحفاظ على خصوصية البيانات المتناقلة عبر شبكات الاتصال الحديثة، تأمين سرية المحررات الإلكترونية باستخدام تقنية التشفير، والذي يعتبر أفضل وسيلة لمنع الغير من الإطلاع على المحرر الالكتروني ومنع التقاط الرسائل أو المعلومات، ومن ثم منع وصولها مشوهة للطرف الآخر.

تؤكد أغلب التشريعات المقارنة المحافظة على سلامة البيانات والمعلومات الواردة في المحرر الإلكتروني دون أن يلحقها أي تغيير في شكلها الأصلي الذي نشأت به، وعليه لا بد من إمكانية الاحتفاظ بالسجل الإلكتروني بنفس الشكل والمواصفات التي تم بها إنشاء المحرر أو إرساله أو تسلمه عند إنشائه، كما حرصت عن طريق الاستعانة بخبراء تقنيات الحوسبة والاتصال إلى وضع أنظمة قانونية تحمي هذه المحررات من الجانب التقني، حيث نصت هذه الأنظمة على تدابير وقائية تتمثل في استخدام برامج تشفير متطورة، ومنح شهادات التصديق الالكتروني يعتبر وسيلة أمنة تهدف إلى التحقق من صحة المحرر الالكتروني وعدم التلاعب بها ويبعث في نفوس الأفراد الثقة والأمان، والاعتماد عليها كدليل مسبق عند صدور التصرف القانوني في وقت لا نزاع فيه يتم نسبته إلى جهات مستقلة ومحايدة معتمدة من الدولة، تكون إما هيئة عامة أو هيئة خاصة تقوم على التوسط بين المتعاملين إلكترونيا .

لا يستكمل المحرر الإلكتروني مقوم وجوده إلا عندما يكون مدعما بإمضاء إلكتروني، فاقتران الكتابة بالتوقيع الإلكتروني يترتب عليه الاعتراف بهذه المحررات الإلكترونية

وإسباغ الحجية عليها ومساواتها بالمحررات التقليدية، والذي يجعل القاضي يحكم بحجيتها بالإثبات في النزاع المعروض عليه دون أن يكون له سلطة تقديرية في ذلك، سيما أن الثقة بالتوقيع الإلكتروني له درجة مصداقية عالية بالمقارنة بالتوقيع العادي على المحررات، فهو يتميز بأنه لديه القدرة على تحديد هوية الشخص الموقع، وقدرته على التعبير عن إرادة الموقع في الموافقة على نفس مضمون المحرر، وذلك من خلال الاستعانة بسلطات التصديق الإلكتروني .

تنفرد الجرائم الماسة بالمحررات الالكترونية بخصائص تميزها عن الجرائم التقليدية، وتتمثل خصوصا بطابعها العابر للحدود وارتكابها في العالم الافتراضي وهي صعبة الاكتشاف نظرا لانعدام الآثار التقليدية لها، بالإضافة إلى ضعف مستوى القائمين على مكافحتها، وذلك بالنظر إلى التطور المتسارع في ارتكابها، أضف إلى ذلك أن المجرم المعلوماتي يتميز بسمات خاصة كالمهارة والمعرفة والذكاء وعدم استعماله للعنف، فلا يحتاج إلى مجهود كبير لارتكابها مقارنة بالمجرم التقليدي، وبالتالي لا بد من ضمانات قانونية كافية تكفل حمايتها، بالإضافة إلى إحاطتها بإجراءات أمنية إلكترونية ووقائية في نفس الوقت تمنع مسبقا المجرم المعلوماتي من استغلال واختراق المحررات الالكترونية.

يثير تطبيق أحكام الجرائم التقليدية على جرائم المحررات الإلكترونية إشكالات عديدة وخصوصا من حيث تحديد أركان هذه الجريمة، فإذا كان تحديد أركان الجريمة التقليدية واضحا في الركن المادي والمعنوي والركن الشرعي، فإن تطبيق هذا التحديد على الجرائم الماسة بالمحررات الالكترونية يشكل صعوبة كبيرة وذلك بالنظر لخصوصية هذه الجريمة، فمثلا تحديد القصد الجنائي مع تحديد السلوك الإجرامي والنتيجة الإجرامية والعلاقة السببية بينهما هو أمر بالغ الصعوبة في ضل الطابع العالمي للجريمة الالكترونية، وعليه فلا بد من تقنين قواعد جديدة لمكافحة الجرائم الالكترونية عامة والجرائم الواقعة على المحررات الالكترونية بصفة خاصة، آخذة بعين الاعتبار الطبيعة الخاصة لهذه الجرائم.

سهلت تقنية المعلومات ارتكاب الكثير من الجرائم المستحدثة فمثلا جريمة الدخول والبقاء غير المشروع تعتبر صور من صور الجريمة الالكترونية، والتي لا بد من تطوير أساليب

حماية المحررات الالكترونية مسبقا كإجراء وقائي وذلك باستحداث أساليب التخزين وحمايتها بوسائل متطورة حتى لا يمكن لأي شخص من الولوج إليها بسهولة.

لحماية المحررات الالكترونية وتأمينها من كل أشكال وصور الاعتداء الماسة التي تقع عليها عن طريق وسائل الاتصال الحديثة، باتت هناك ضرورة إعادة النظر في النصوص الجنائية الموضوعية والإجرائية، لأن هذه النصوص أضحت عاجزة عن توفير الحماية اللازمة لها، فهذه التشريعات الحالية لا تعكس النقاط السلبية الموجود حاليا في نظم تكنولوجيا المعلومات الحديثة والتي هي في تطور مستمر.

تستلزم إجراءات الاستدلال في جرائم المحررات الالكترونية على وجه التحديد المعرفة بالنظام المعلوماتي ومعرفة طرق ارتكاب المجرم المعلوماتي لسلوكه الإجرامي، فالطبيعة الخاصة للدليل الالكتروني يحتاج إلى تغيير الكثير من المفاهيم المتعارف عليها حول الإجراءات وطرق الحصول عليها، فالدليل الإلكتروني هو الدليل الذي يتم الحصول عليه بطريقة إلكترونية وقانونية من أنظمة الأجهزة المحمولة، والحواسيب الآلية وتطبيقاتها وبرامجها المختلفة وشبكات الاتصال الإلكترونية، وذلك باستخدام معدات فنية في تحليل وتفسير النتائج المتحصل عليها وتقديمها للقضاء كبينة إثبات، مما دفع بأغلب التشريعات إلى تدارك هذا الأمر الواقع عن طريق استحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية، فالطبيعة الإلكترونية التي يتميز بها هذا النوع المستحدث من الجرائم يحيلنا إلى مسألة سلطة القاضي في قبول هذا الدليل، ومدى مشروعيته ومصداقيته إعمالا لمبدأ السلطة التقديرية للقاضي الجزائي الذي يشكل جوهر أي حكم.

يعترض إثبات الجرائم الماسة بالمحررات الإلكترونية ونظرا لبعدها الدولي بعض الصعوبات، من حيث أن المجرم المعلوماتي يرتكب جريمة النفاذ إلى أنظمة المعالجة الآلية للمعطيات في بلد ما، ويتم التلاعب بمضمون ومحتوى المحررات الالكترونية في بلد آخر وتسجل النتائج في بلد ثالث، بالإضافة إلى الصعوبات التي تتعلق باستحداثه أنواع وأساليب جديدة في نشاطه الإجرامي، خاصة مع تمكن مرتكبيها بالتقنيات الجديدة غير المسبوقة في مجال تكنولوجيا المعلومات والاتصالات، والتي يسرت لهم ارتكاب هذه الأنشطة داخل حدود

الدولة وخارجها، كما أن الاستخدام المتزايد لوسائل الاتصال الحديثة شكل مخاطر أمنية يصعب التنبؤ بها، والتي تهدد معظم دول العالم خاصة في الدول المتقدمة التي وضعت جل معاملاتها وبياناتها الخاصة والعامة في بيئة شبكات إلكترونية، فللتعامل مع هذا النوع المستحدث من الجرائم كان لزاما على تشريعات الدول أن تواكب ذلك وأن تأخذ في حساباتها التقدم العلمي والتكنولوجي، وأن تقوم بتطوير الوسائل اللازمة من أجل الحد من هذه السلوكيات التي أخذت بالاتساع والتزايد، دون قوانين ردعية بالشكل الذي تؤمن معه متطلبات هذا التطور، مما استدعى توجه المنظمات والمؤتمرات الدولية إلى الانشغال بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها، وذلك بضرورة التدخل بتعديل بعض النصوص القائمة أو وضع نصوص جديدة تتلاءم وطبيعة الجرائم الالكترونية.

فتطويع هذه النصوص الجنائية التي تتعلق بجرائم المحررات الإلكترونية في صورها التقليدية كالسرقة والنصب والتزوير، وتعديل هذه النصوص من أجل توفير نوع من الحماية ومن أجل أن تتلاءم مع الطبيعة الالكترونية لها لم يكتب لها النجاح، والعلة في ذلك أن الأخذ بها يعني تشويه مبادئ وأصول هامة ومستقر في القانون الجنائي، وعلى رأسها مبدأ الشرعية الجنائية في شقيه الموضوعي والإجرائي، والذي يتفرع منها مبدأ التفسير الضيق ومبدأ حظر القياس في علة التجريم، فأدلة الإثبات التقليدية قد لا تقوى على إثبات هذا النوع المستحدث من الجرائم، الأمر الذي أستوجب إعادة النظر في مسألة الإثبات على ضوء الأدلة الجديدة التي تعد الوسيلة الأصل لإثبات الجرائم التي ترتكب بالوسائل الالكترونية أو التي تقع على هذه الوسائل، بالإضافة إلى أن الوسائل الفنية التي قد تستخدم في تنفيذ هذه الجرائم المستحدثة كثيرة ومعقدة في الوقت الحالي، ولا يمكن التنبؤ بالوسائل التي يمكن أن يفرزها التطور التكنولوجي مستقبلا، مما أدى إلى صعوبة مسايرة التطور المتسارع من قبل سلطات التحقيق.

يستلزم أيضا التحقيق في مجال الجرائم الماسة بالمحررات الإلكترونية العمل على تطوير إجراءات المعاينة والتفتيش والضبط، وذلك من خلال وضع ضوابط إجرائية لها تعمل على تحقيق الفاعلية المطلوبة للأجهزة الأمنية وسلطات التحقيق في كشف غموض

الجريمة وضبط فاعليها والتحقيق معهم وتقديمهم للقضاء، إلا أن غالبية النصوص القانونية لا تزال عامة ولم تتناول الجرائم الإلكترونية بصفة خاصة، سيما أن اختلاف أركان وشروط الجرائم الإلكترونية عن أركان وشروط الجرائم التقليدية، يترتب عليه عدم إمكانية تطبيق هذه النصوص على هذه الجرائم مما يصعب مهمة التحقيق في هذا النوع المستحدث من الجرائم، بالتالي فإنه يحتاج إلى تطوير هذه الإجراءات لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها.

فتطبيق القانون الجنائي الإجرائي على جرائم المحررات الإلكترونية أثار صعوبات إجرائية، تكمن أساسا في صعوبة تفتيش ومعاينة وضبط هذه الجرائم وجمع الأدلة المتعلقة بها، سيما وأنها تتعلق ببيانات معالجة إلكترونية وكيانات غير ملموسة، بالتالي استدعى من الناحية الفنية إعداد برامج تدريب وتأهيل لجهات التحري والتحقيق على نحو يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة.

يتكون الدليل الالكتروني من بيانات ومعلومات غير ملموسة، مما يتطلب إدراكها استخدام برامج حاسوبية ومعدات إلكترونية ونظم خاصة، فهو يحتاج إلى بيئة تقنية حتى يتكون فيها، فلا بد أن لا يخرج الدليل الالكتروني عما توصل إليه الدليل العلمي، فبعض الخصائص التي يتميز بها، أكسبته طابعا مميزا جعلته الأفضل لإثبات الجرائم الالكترونية مثل جرائم الاعتداء على نظم المعالجة الآلية، لأنه من طبيعة الوسط الذي ارتكبت فيه، فتقدير هذا الدليل يخضع للاقتناع الشخصي للقاضي الجنائي مثله كل الأدلة المادية المثبتة لقيام جريمة واقعة على المحررات الالكترونية، فللقاضي الجنائي له حرية تقدير الأدلة الجنائية وتكوين قناعته، ويبني حكمه على أي دليل متى اطمأن إليه ولو كان مستمد من محاضر الاستدلالات فهي مسألة موضوعية تتعلق بقيمة ذلك الدليل، أما حرية القاضي الجنائي في قبول الدليل الإلكتروني فهي مسألة قانونية لا مجال لإعمال سلطة القاضي التقديرية فيها.

تعتبر الإجراءات الجنائية هي مصدر الأدلة التي تؤسس عليها المحكمة اقتناعها بالإدانة، فلا يكون البحث عن الدليل الإلكتروني بأية وسيلة كانت وإنما يتعين أن تكون هذه الوسائل

مشروعة، وبالتالي يتوقف قبول هذه الأدلة على مشروعية الإجراءات التي تم وفقها الحصول عليها، فشرط تمتع المحرر الالكتروني بقوة إثبات قانونية لا بد من توفر شرط مشروعية الدليل الالكتروني، من إجراءات التحري والتحقيق في الحصول على الدليل الرقمي، وشرط مناقشة الأدلة الرقمية المتحصل عليها من ارتكاب الجرائم الماسة بالمحرر الالكتروني بالجلسة، وأن يخضع تقييم ذلك الدليل الالكتروني إلى تقدير القاضي الجزائي بأن يصل في تقديره واقتناعه به إلى درجة اليقينية.

نجد أنه من الناحية العملية القاضي لا يملك الحرية عند تقديره القيمة العلمية القاطعة للدليل العلمي، فهو يقوم على أسس علمية دقيقة ولا يحق له مناقشة الحقائق العلمية الثابتة، فهو دليل إثبات ينظر إليه القاضي على ضوء الظروف والملابسات المحيطة بذلك الدليل، وإنما يناقش ما تضمنته المحررات الإلكترونية من بيانات ومعطيات، أين يكون الدليل فيها قد تعرض للمحو أو التدمير أو التلاعب فيه سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات، بالتالي فإن القاضي في هذه الحالة وللتثبت وكشف محتوى المحرر، فإنه يلجأ إلى الاستعانة بتقرير الخبرة التقنية التي تعد البينة والدليل.

فالاستعانة بالخبراء التقنيين في مجال المعلوماتية له دور كبير في أعمال الاستدلال والتحقيق في الجريمة المعلوماتية، فهي تحتاج لبحث وتدقيق في أمور تقنية دقيقة ويعود ذلك إلى طبيعة تلك الجرائم وطبيعة المجرم المعلوماتي وطبيعة الأدلة، فالخبير التقني يفرض نفسه كوسيلة لا يمكن الاستغناء عنها في فهم طبيعة وأنشطة الجرائم الالكترونية في مختلف مراحله.

نجد أيضا أن التحقيق يتميز في مجال جرائم المحررات الإلكترونية بأن له طابعه الخاص من حيث الإجراءات، مقارنة بالتحقيق في جرائم المحررات التقليدية، فهو يعتمد على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية، بالتالي يستدعي ذلك تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع متطلبات هذه التقنية الجديدة وخصوصيتها، سيما أن إجراءات التحقيق فيها يجب أن يكون من قبل محققين لديهم المهارة المعرفية والخبرة الضرورية بمكونات الحاسب الآلي ونظمه، ويكون ملما بأهم تقنيات أمن

المعلومات وأدوات وأساليب ارتكابها وهذا لا يتحقق إلا من خلال العمل على تدريب محققين متخصصين في هذا المجال.

أغلب التشريعات سواء الوطنية أو الدولية والتي تعتمد على حرية الإثبات، تعتمد على قبول أي دليل يمكن طرحه أمام القضاء، بالتالي فإنه لا إشكال في قبول مخرجات الحاسب الآلي والانترنت كدليل أمام القضاء الجنائي والاستعانة بها في إثبات الجريمة الالكترونية، طالما أن ضبط هذه الأدلة جاء وفقا لإجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير، فسلطة القاضي الجنائي في تقدير الدليل الإلكتروني يحكمها مبدأ عام هو مبدأ حرية القاضي في تكوين قناعته، وذلك من حيث حريته في أن يستند على أي دليل إلكتروني يطمئن إليه هذا من جهة، ومن جهة أخرى إلى حريته في تقدير الدليل الإلكتروني المعروض عليه.

وفي ظل الجهود التي بذلت على المستوى الوطني وعلى مستوى الدولي فإن الصعوبات التي أفرزتها الجرائم الإلكترونية تبقى بعيدة كل البعد عن الآمال التي يطمح إليها، ويرجع ذلك أساسا إلى غياب إستراتيجية واضحة في التعامل مع هذا النوع المستحدث من الجرائم، لاسيما في الدول التي لم تدرك خطورة الوضع ولم تبادر إلى تعديل تشريعاتها بما يتماشى مع الطبيعة التقنية لهذه الجرائم.

قائمة المراجع

قائمة المراجع

أولا: باللغة العربية

1 ـ الكتب :

1- إبراهيم الدسوقي أبو الليل، الحجية القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003.

2- إبراهيم يوسف حسان، التوثيق الإلكتروني ومسئولية الجهات المختصة به، دار الراية، عمان، 2009.

3- أبو هبة نجوى، التوقيع الالكتروني، دار النهضة العربية، القاهرة، 2002.

4- أبو زيد محمد محمد، تحديث قانون الإثبات، مكانة المحررات الالكترونية بين الأدلة الكتابية، دار النهضة العربية، القاهرة، 2002 .

5- أحمد الفضل، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2008.

6- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2000 .

7- أحمد المهدي، الإثبات في التجارة الإلكترونية، دار الكتب القانونية، مصر، 2004.

8 ـ أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010.

9- أحمد عبد العال أبو قرين، أحكام الإثبات في المواد المدنية والتجارية في ضوء الفقه والتشريع والقضاء، الطبعة الثالثة، دار النهضة العربية، القاهرة، 2006 .

10- أسامة أحمد المناعسة وآخرون، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، عمان، 2013 .

11- أسامة أبو حسن مجاهد، خصوصية التعاقد عبر الإنترنت، دار النهضة العربية، القاهرة، 2008 .

12- أسامة أحمد شوقي المليجي، استخدام مستخرجات التقنيات الحديثة وأثره على قواعد الإثبات المدني، دار النهضة العربية، القاهرة، 2000 .

13- أسامة سمير حسن، الاحتيال الالكتروني، الجنادرية، عمان، 2011.

14- أسامة عبد العليم الشيخ، مجلس العقد الإلكتروني وأثره في عقود التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2013.

15- الصالحين محمد العيش، الكتابة الرقمية طريقا للتعبير عن الإرادة ودليلا للإثبات، منشأة المعارف، الإسكندرية، 2008.

16- الغريب فيصل سعيد، التوقيع الالكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005.

17- الياس ناصيف، العقد الالكتروني في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009 .

18- الكسواني عامر محمود، التجارة عبر الحاسوب، دار الثقافة ، عمان، 2008.

19- أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2004.

20- أيمن عبد الله فكري، الجرائم الالكترونية، مكتبة القانون والاقتصاد، الرياض، 2015.

21- إيمان مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، 2008 .

22- إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2008.

23- برهم نضال إسماعيل، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2005 .

24- بشار محمد دودين، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، دار الثقافة ، عمان، 2006.

25- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2011.

26- ثروت عبد الحميد، التوقيع الالكتروني، مكتبة الجلاء الجديدة، المنصورة، 2002.

27- جمال إبراهيم الحيدري، ضوابط اعتبار المخرجات الالكترونية أدلة إثبات في القضايا الجزائية، مكتبة السنهوري، بغداد، 2012

28- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002.

29- ـــــــــــــــ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.

30- ـــــــــــــــ، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2012 .

31- ـــــــــــــــ، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2012.

32- ـــــــــــــــ، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار الفكر الجامعي، القاهرة، 2001.

33- حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، دار الفكر والقانون، المنصورة، 2015.

34- حسن طاهر داود، الحاسب وأمن المعلومات، الإدارة العامة للطباعة والنشر، الرياض، 2000 .

35- حسن عبد الباسط جميعى، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000 .

36- حسن عمر المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دار وائل للنشر والتوزيع، عمان، 2003 .

37- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت، دار النهضة العربية، القاهرة، 2009.

38- خالد حسن أحمد، الحجية القانونية للمستندات الإلكترونية بين الفقه الإسلامي والقانون الوضعي، مركز الدراسات العربية، القاهرة، 2016 .

39- خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، 2014.

40 - خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2007.

41- ــــــــــــــ، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2008.

42- ــــــــــــــ، أمن المعلومات، الدار الجامعية، الإسكندرية، 2008 .

43 - ــــــــــــــ، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية، 2008.

44- ـــــــــــــــ، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

45 - ـــــــــــــــ، التوقيع الإلكتروني، الدار الجامعية، الإسكندرية، 2010.

46- خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2007.

47- خاد مصطفى فهمي، إبرام العقد الالكتروني في ضوء التشريعات العربية والمنظمات الدولية، دار الجامعة الجديدة، مصر، 2007.

48- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان،2011.

49- داود سليمان علي الحمادي، أحكام جريمة التزوير المعلوماتي، دار النهضة العربية، القاهرة، 2016.

50- رحيمة صغير ساعد نمديلي، العقد الإداري، دار الجامعة الجديدة،الإسكندرية، 2007.

51- زياد خليف العنزي، المشكلات القانونية لعقود التجارة الالكترونية، دار وائل ، عمان، 2010.

52- سامي جلال الفقي، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، القاهرة، 2001.

53- سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دار الكتب القانونية، مصر، 2008 .

54- سعيد السيد قنديل، التوقيع الالكتروني، دار الجامعة الجديدة، الإسكندرية، 2006.

55- سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق، منشورات الحلبي الحقوقية، بيروت، 2010.

56- سليمان احمد محمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007.

57- سمير حامد عبد العزيز الجمال، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة، دار النهضة العربية، القاهرة، 2004.

58- ـــــــــــــــــــــــــ، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006 .

59- سمير عبد السميع الأودن، العقد الإلكتروني، منشأة المعارف، الإسكندرية، 2005.

60- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

61- صفاء فتوح جمعة، العقد الإداري الالكتروني، دار الفكر والقانون، المنصورة، 2014 .

62- طارق سرور، ذاتية جرائم الإعلان الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001 .

63- طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2007 .

64- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010.

65- عامر محمود الكسواني، التجارة عبر الحاسوب، دار الثقافة، عمان، 2008.

66- عاطف عبد الحميد حسن، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2008.

67 - عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002.

68 - عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، 2007.

69- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002 .

70- ـــــــــــــــــــ، التوقيع الإلكتروني في النظم المقارنة، دار الفكر الجامعي، الإسكندرية، 2003 .

71- ـــــــــــــــــــ، مقدمة في التجارة الإلكترونية العربية، شرح قانون المبادلات والتجارة الإلكترونية التونسي، دار الفكر الجامعي، الإسكندرية، 2004 .

72- ـــــــــــــــــــ، الحكومة الإلكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، 2004.

73- ـــــــــــــــــــ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2005.

74- ـــــــــــــــــــ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.

75- ـــــــــــــــــــ، الحكومة الالكترونية ونظامها القانوني، دار الكتب القانونية، مصر، 2007.

76- ـــــــــــــــــــ، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، 2008.

77- ـــــــــــــــــــ، نحو صياغة عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2009.

78- عبد العادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة، 2005.

79- عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، بيروت، 2010 .

80- ـــــــــــــــ، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني، دار الثقافة، عمان، 2002.

81 - ـــــــــــــــ، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، مكتبة دار الثقافة، عمان، 1997.

82- عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، دار وائل، عمان، 2010 .

83- عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض، 2012.

84 - عبد التواب مبارك، الدليل الإلكتروني أمام القاضي المدني، دار النهضة العربية، القاهرة، 2006.

85- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.

86 - علي بن هادى البشري، جرائم الحاسب الآلي، دار العلوم، الرياض، 1998.

87- علي حسن محمد الطوالقة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الجديدة، الأردن، 2004.

88- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2004.

89- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، عمان، 2011.

90- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية و الأجنبية، دار الجامعة الجديدة ، الإسكندرية، 2009.

91- ـــــــــــــــــ، التحكيم الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2009.

92- عصمت عبد المجيد بكر، دور التقنيات الحديثة في تطور العقد، دار الكتب العلمية، بيروت، 2015.

93- علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002.

94 - علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات، دار الثقافة، الأردن، 2005.

95 - ـــــــــــــــــ، التحكيم الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2009.

96- عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي و أبعادها الدولية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1995.

97- عمر خالد زريقات، عقد البيع عبر الإنترنت، دار الحامد، عمان، 2007 .

98- عمر ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الالكتروني، دار وائل، عمان، 2010.

99- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، 2006.

100- عمر أبو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دار النهضة العربية، القاهرة، 2010.

101- عيسى غسان ربضي، القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة، عمان، 2009.

102- فتحي محمد أنور عزت، جرائم العصر الحديث، دار الفكر والقانون، المنصورة، 2010.

103- فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، 2005 .

104- فضالة حسن موسى، التنظيم القانوني للإثبات الالكتروني، دار السنهوري، بيروت، 2016.

105- لزهر سعيد، النظام القانوني في عقود التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2012 .

106- لورنس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة ، عمان، 2005.

107- ماجد محمد سليمان أبا الخيل، العقد الالكتروني، مكتبة الرشد، الرياض، 2009.

108- محمد أحمد العابدين، الورقة الرسمية والعرفية في الإثبات، منشأة المعارف، الإسكندرية، 2002.

109- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، الأردن،2011.

110- محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

111- ـــــــــــــــ، المستند الالكتروني، دار الفكر الجامعي، الإسكندرية، 2007.

112- محمد السعيد رشدي، التعاقد بوسائل الاتصال الحديثة، منشأة المعارف، الإسكندرية، 2008 .

113- محمد السيد عمران، الطبيعة القانونية لعقود الخدمات، دار الثقافة الجامعية، الإسكندرية، 1992.

114- محمد المرسى زهرة، الحماية المدنية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2008 .

115- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.

116- ـــــــــــــــ، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

117- محمد إبراهيم عرسان أبو الهيجاء، التحكيم بواسطة الإنترنت، دار الثقافة، الأردن، 2002.

118- محمد أحمد العابدين، الورقة الرسمية والعرفية في الإثبات، منشأة المعارف، الإسكندرية، 2002.

119- محمد دباس الحميد، حماية أنظمة المعلومات، دار حامد، عمان، 2005 .

120- محمد حسام محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، دار النهضة العربية، القاهرة، 1993.

121- ـــــــــــــــــــ،الحجية القانونية للمصغرات الفيلمية، دار الثقافة، القاهرة، 1988.

122- ـــــــــــــــــــ، الإطار القانوني للمعاملات الإلكترونية، دار الثقافة، القاهرة، 2002.

123- محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.

124 - ـــــــــــــــــــ، المسئولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.

125 - محمد جمال خالد رستم، التنظيم القانوني للتجارة والإثبات الالكتروني في العالم، منشورات الحلبي الحقوقية، بيروت، 2006 .

126- محمد سعد خليفة، مشكلات البيع عبر الإنترنت، دار النهضة العربية، القاهرة، 2004 .

127- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، 2006.

128 - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، الطبعة الثانية، 2009.

129- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة ، الإسكندرية، 2004.

130- محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، دار الجمهورية للصحافة القاهرة، 2010.

131- محمد محمد سادات، حجية المحررات الإلكترونية الموقعة إلكترونيا في الإثبات، دار الجامعة الجديدة ، الإسكندرية ، 2011 .

132- محمد مدحت عزمي، المعاملات التجارية الإلكترونية "الأسس القانونية و التطبيقات"، مركز الإسكندرية للكتاب، الإسكندرية، 2009.

133- محمد فواز المطالقة ، الوجيز في عقود التجارة الإلكترونية"دراسة مقارنة" ، دار الثقافة للنشر و التوزيع، عمان، 2008 .

134- محمد نصر محمد، الوسيط في الجرائم المعلوماتية، مركز الدراسات العربية، الجيزة، 2015.

135- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001 .

136- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، الطبعة الثانية، 2009.

137- محمد فهمي طلبة وآخرون، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، موسوعة دلتا كمبيوتر، القاهرة، 1991.

138- مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، القاهرة، 2005.

139- مصطفى موسى العجارمة، التنظيم القانوني للتعاقد عبر شبكة الانترنت، دار الكتب القانونية، القاهرة، 2010.

140- مصطفى يوسف كافي، الإدارة الإلكترونية، دار رسلا ن، دمشق، 2011.

141- مناني فراح، العقد الإلكتروني، وسيلة إثبات حديثة في القانون الجزائري، دار الهدى، عين مليلة، 2009 .

142- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004.

143- ـــــــــــــــــــــــــــــــ، الطبيعة القانونية للعقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2005 .

144- ـــــــــــــــــــــــــــــــ، ممدوح محمد الجنبيهي، تزوير التوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006 .

145- ـــــــــــــــــــــــــــــــ، ممدوح محمد الجنبيهي، البنوك الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2005.

146- نائلة عادل فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005 .

147- ناهد فتحي الحمودي، الأوراق التجارية الالكترونية، دار الثقافة، الأردن، 2010.

148- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2007.

149- نبيل صقر ومكاري نزيهة، الوسيط في القواعد الإجرائية و الموضوعية للإثبات في المواد المدنية، دار الهدى، الجزائر، 2009.

150- نضال سليم برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة، الأردن، 2005.

151- نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، 2006.

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

153- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات في القانون الأردني، دار وائل للنشر والتوزيع، 2007 .

154- ـــــــــــــــ، الإثبات الالكتروني في المواد المدنية والمصرفية، دار الثقافة، عمان، 2012.

155- هالة جمال الدين محمد محمود، أحكام الإثبات في عقود التجارة الإلكترونية، دار النهضة العربية، القاهرة، 2012.

156- هبة ثامر محمود عبد الله، عقود التجارة الإلكترونية "دراسة مقارنة"، منشورات زين الورقية، بغداد، 2011 .

157- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994.

158- هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1997.

159- ـــــــــــــــ، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1999.

160- ـــــــــــــــ، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2011.

161- هدى حامد قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

162- ـــــــــــــــ، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، 2000.

163- زياد خليف العنزي، المشكلات القانونية لعقود التجارة الالكترونية، دار وائل للنشر والتوزيع،عمان، 2010.

164- وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات و المعلومات، دار المطبوعات الجامعية، الإسكندرية، 2005.

165- يحيى بكوش، أدلة الإثبات في القانون المدني، الشركة الوطنية للنشر والتوزيع، الجزائر،1981.

2 ـ الرسائل والمذكرات الجامعية:

أ ـ رسائل الدكتوراه:

1- بلقاسم حامدي، إبراهيم العقد الإلكتروني، رسالة لنيل شهادة دكتوراه في العلوم، فرع قانون الأعمال، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2015 .

2- باطلي غنية، الجريمة الالكترونية، أطروحة لنيل شهادة الدكتوراه، القانون الخاص، كلية الحقوق، جامعة باجي مختار، عنابة، 2015.

3- تامر محمد سليمان الدمياطي، إثبات التعاقد الالكتروني عبر الانترنت، رسالة لنيل شهادة دكتوراه في الحقوق، كلية الحقوق، قسم القانون المدني، جامعة عين شمس، مصر، 2009 .

4- حمودي ناصر، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، رسالة لنيل شهادة دكتوراه في العلوم، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2009 .

5- خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.

6- عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، مصر، 1998.

7- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم الانترنت، أطروحة دكتوراه، كلية الحقوق،الجامعة الإسلامية في لبنان، لبنان، 2004.

8- محمد إبراهيم عرسان أبو الهيجاء، القانون الواجب التطبيق على عقود التجارة الإلكترونية، رسالة لنيل شهادة دكتوراه، معهد البحوث والدراسات العربية، قسم الدراسات القانونية، المنظمة العربية للتربية و الثقافة و العلوم، جامعة الدول العربية، القاهرة، 2004.

9 ـ محمد عبد الله محمد العوا، المسئولية الجنائية الناشئة عن جرائم الأموال عبر الانترنت، أطروحة دكتوراه، جامعة الإسكندرية، مصر، 2012.

10- مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الإنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012.

11- نور خالد عبد المحسن العمد الرزاق، حجية المحررات والتوقيع الالكتروني في الإثبات عبر شبكة الانترنت، رسالة لنيل شهادة دكتوراه في الحقوق، كلية الحقوق، جامعة عين شمس، مصر، 2009.

12- زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية ، جامعة أبو بكر بلقايد، تلمسان، 2013 .

ب ـ مذكرات الماجستير:

1- أراميس عائشة، الإثبات في العقود الإلكترونية المبرمة عبر الإنترنت، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق، جامعة الجزائر، 2007.

2- بن غرابي سامية، عقود التجارة الإلكترونية ومنهج تنازع القوانين ، مذكرة لنيل درجة الماجستير في القانون، فرع قانون التعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2009.

3- حابت أمال، استغلال خدمات الإنترنت، مذكرة لنيل درجة الماجستير في الحقوق، فرع قانون الأعمال،كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2004 .

4- داديار حميد سلمان، دور السندات المستخرجة عن طريق الإنترنت لإثبات المسائل المدنية، رسالة ماجستير، كلية القانون، جامعة صلاح الدين،2005.

5- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012.

6 - محمد نافع فالح رشدان العدواني، حجية الدليل الالكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2015.

7- لما عبد الله صادق سلهب، مجلس العقد الإلكتروني، أطروحة ماجستير في القانون، كلية الدراسات العليا، جامعة النجاح الوطنية في نابلس، فلسطين، 2008 .

8 - عبد الله سيف الكينوب، الأحكام الإجرائية لجريمة الاحتيال المعلوماتي، رسالة لنيل شهادة ماجستير في القانون العام، كلية الدراسات العليا والبحث العلمي، جامعة الشارقة، 2012.

9 - يوسف خليل يوسف العفيفي، الجرائم الالكترونية في التشريع الفلسطيني، قسم القانون العام، رسالة ماجستير في القانون العام، كلية الشريعة والقانون، جامعة غزة، 2013.

10- عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009.

3 - المقالات والمداخلات:

أ - المقالات:

1- أحمد عبد الحكيم عبد الرحمان شهاب، نور عزم الليل بن مارني، شروط قبول الأدلة الالكترونية أمام القضاء الجنائي الفلسطيني، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 07 ، عدد 02، 2018، ص.ص.171-197.

2- باطلي غنية، حجية المستند الإلكتروني، المجلة الجزائرية للعلوم القانونية الاقتصادية والسياسية، جامعة الجزائر، كلية الحقوق، عدد3، سبتمبر 2011 ، ص.ص.165-195.

3- حامد شاكر محمود الطائي، حجية المراسلات التجارية في ضل التطور التقني الحديث ، مجلة الحقوق،، جامعة المستنصرية،،المجلد1، 2017 ، ص.ص.1-46.

4 - حسين بن محمد المهدي، القوة الثبوتية للمعاملات الإلكترونية، مجلة البحوث القضائية، عدد7، جويلية2007 ، ص. ص.7-76 ، على موقع: www.ysc.org.ye

5 - حنان مليكه، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري "دراسة مقارنة"، مجلة جامعة دمشق للعلوم الاقتصادية و القانونية، المجلد 26، عدد2/2010، ص.ص.549-572، على موقع: www.damascusuniversity..sy

6- خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة دهوك، العراق، المجلد 7، العدد36/ 2018، ص.ص.80- 125.

7- رامي وشاح، الصعوبات التي تعترض الإثبات عبر الوسائل التكنولوجية الحديثة، مجلة جامعة الأزهر، غزة ، سلسلة العلوم الإنسانية، المجلد 11، عدد 1، 25جوان2009، ص. ص.225-262.

8- زيد حمزة مقدم، النظام القانوني للتوثيق الإلكتروني، مجلة الشريعة والقانون والدراسات الإسلامية، العدد24، أوت 2014، ص.ص.127- 176على موقع:
http://dspace.iua.edu.sd

9- صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالى، المجلد الخامس، العدد02، 2016، ص.ص.255-290.

10- طه السيد أحمد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق، مجلة الشريعة والقانون،جامعة الإمارات العربية المتحدة، العدد28، المجلد1، 2013، ص.ص.191- 381.

11- عبد العزيز المرسي حمود، مدى حجية المحرر الإلكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، عدد11،السنة11، أفريل2002، ص.ص.19-39 .

12- عماد حسن سليمان، القيمة القانونية للإثبات بالتوقيع الالكتروني، مجلة القانون للدراسات والبحوث القانونية، جامعة ذي قار، كلية القانون، العراق، المجلد2، العدد1، 2009، ص.ص. 58-68.

13- عمر لطيف كريم العبيدي، التقاضي الإلكتروني وآلية التطبيق، مجلة جامعة تكريت للحقوق، السنة الأولى1 ، المجلد 3 ، الجزء 1، مارس2017، ص.ص. 509- 452.

14- كاظم محمد عطيات، محمد رضوان هلال، كيفية التعامل التقني والآمن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيدة الدليل المستخلص، المجلة العربية الدولية للمعلوماتية، السعودية، المجلد 3، العدد5 ، 2015. ص.ص.43-55.

15- محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الالكتروني، مجلة الحقوق،، جامعة الكويت، الكويت ،العدد 2، السنة الثالثة، 2012، ص.ص. 563،515.

16- محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15 ، العدد 30، الرياض، جامعة نايف العربية للعلوم الأمنية، 2000، ص.ص.317- 380.

17- محمد أمين الخرشة، نايف عبد الجليل الحمايدة، الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، مجلة جامعة الأزهر،غزة، سلسلة العلوم الإنسانية، 2014، المجلد 16، العدد1، ص.ص.319- 350.

18- محمد محمد سادات، أثر تنوع التوقيعات الالكترونية على حجية العقود العرفية الإلكترونية في القانون الجزائري، مجلة صوت القانون، جامعة خميس مليانة، الجزائر، العدد7، الجزء الثاني، 2017، ص.ص.144-183.

19- نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الإنسانية والاجتماعية، المجلد15، العدد13، أفريل 2017، ص.ص.299-335.

20- نضال ياسين الحاج حمو، دور الدليل الالكتروني في الإثبات الجنائي، دراسة تحليلية، مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد الأول، السنة 5، العدد19،2013، ص.ص.170- 234.

21- يعيش تمام شوقي، خليفة محمد، نظام المعالجة الآلية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مجلة جيل الأبحاث القانونية المعمقة، العدد 25، السنة الثالثة، ماي2018، ص.ص.11-25.

ب- المداخلات:

1- أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-29 أكتوبر 2009، ص.ص.1-20.

2- أحمد شرف الدين، حجية الكتابة الإلكترونية على دعامات ورقية في الإثبات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث

والدراسات بأكاديمية شرطة دبي، الإمارات العربية المتحدة، 26-28 أفريل2003، ص.ص.13-26.

3- الصالحين محمد العيش، مدى قبول الدليل الكتابي الرقمي في إثبات المعاملات التجارية الالكترونية، المؤتمر الدولي الثاني لقانون الانترنت، جامعة الدول العربية، مالطا من 27 إلى 31نوفمبر2006، ص.ص.1- 31، على موقع: www.iefpedia.com

4- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المقام من طرف غرفة تجارة وصناعة دبي في 12/10 ماي2003، ص.ص.483-573.

5- خالد ممدوح إبراهيم،، عقود التجارة الالكترونية، أوراق عمل مؤتمر التجارة الالكترونية وأمن المعلومات "الفرص والتحديات"، القاهرة، نوفمبر2008، منشور بموقع مركز العدالة للتحكيم والاستشارات: www.aladalacenter.com

6 - طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية، 28- 29 أكتوبر2009، أكاديمية الدراسات العليا، طرابلس، ص.ص.1-33.

7 - عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي، من 26 إلى 28 أفريل 2003، ص.ص.234-253.

9- عبد الله بن إبراهيم بن ناصر، العقود الالكترونية ، دراسة فقهية تطبيقية مقارنة، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون، المجلد 5، الإمارات العربية المتحدة، 10-12ماي 2003 ، ص.ص.2119-2151 .

10- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12إلى 14 نوفمبر،2007، ص.ص. 1-46 .

11- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي، 2003، ص.ص.1-73، على موقع: www.arablawinfo.com

12- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ، الفترة 1-3 ماي 2000، المجلد الأول، الطبعة الثالثة، 2004، ص.ص.559-623.

13- غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، الإمارات العربية المتحدة، مؤتمر قانون الكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، 1- 3 ماي 2000، المجلد الأول، الطبعة الثالثة، 2004، ص.ص.143-174.

14- فتوح عبد الله محمد الشاذلي، المواجهة التشريعية للجرائم المستحدثة، مؤتمر الأمن والسلامة، المنعقد من طرف وزارة الداخلية بدولة الإمارات العربية المتحدة، أبو ظبي، الفترة منن 5إلى 8 أكتوبر 2003، ص.ص. 467- 489.

15- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والانترنت،جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، من 1إلى 3ماي2000، المجلد الثالث، ص.ص.1033-1082.

16- محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور المعاملات المدنية، دبي، الإمارات العربية المتحدة، المجلد الثاني، 26-28 أفريل2003، ص.ص.359 -378.

17- كمال أحمد الكركي، التحقيق في جرائم الحاسوب، المؤتمر العلمي الأول حول الجوانب القانونية والقانونية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة ، 26-28 أفريل 2003، ص.ص435 -440، على موقع: http://www.f-law.net/law/threads/

18- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، 26-28أفريل 2003، ص.ص.1-18، على موقع: https://drive.google.com/file/d/0B9VPnsUnYmSaRjVCbGtneFE2NGM/view

19- محمد حسام محمود لطفي، الجرائم الواقعة في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر1993، ص.ص.448- 491.

20- محمد فريد هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، مؤتمر القانون والكمبيوتر والانترنت، المنعقد من 1 إلى 3 فيفري 2000 ، المجلد الثاني، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص.ص.401- 506 .

21- محمود عبد الله، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات العربية المتحدة، 26-27 أفريل 2003، ص.ص.591- 631 .

22- ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، عدد رقم 4، المحور الأمني والإداري، الإمارات العربية المتحدة، دبي، 26- 27 أفريل2003، على موقع: https://www.f-law.net/law/archive/index.php/f-85.html

23- محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من 25إلى 28 أكتوبر1993، ص.ص.452 -488.

24- موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، من 28 إلى 29 أكتوبر 2009، ص.ص.1-24، على موقع: www.iefpedia.com

25- هدى حامد قشوش، الإتلاف غير العمدي لبرامج وبيانات الحاسب الإلكتروني، مؤتمر القانون والكمبيوتر والانترنت، المنعقد من 1 إلى 3 فيفري 2000 ، المجلد الثاني، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة،2004، ص.ص.887-905.

26- ــــــــــــــــ، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المقام من طرف غرفة تجارة وصناعة دبي في 12/10 ماي2003، ص.ص. 599- 613 .

27- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مؤتمر القانون والكمبيوتر والانترنت، المنعقد من 1 إلى 3 فيفري 2000 ، المجلد الثاني، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص.ص.713- 787 .

28- وسيم الحجار، أهمية مساواة السند الإلكتروني بالسند الورقي وإصدار تشريع يكفل ذلك ويضع له ضوابط ، ورقة عمل الندوة العلمية ، جامعة الدول العربية، مجلس وزراء العرب، المركز العربي للبحوث القانونية والاقتصادية ، بيروت، الفترة من 4-6 أوت 2009، على موقع: https://carjj.org/sites/default/files/symp-rec-edoc-hajjar.doc.

29- يان الياسون، جرائم الفضاء الإلكتروني، مؤتمر الأمم المتحدة الثالث عشر بشأن منع الجريمة والعدالة الجنائية، الدوحة، 12- 19 أفريل 2015، على موقع :
https://www.un.org/ar/events/crimecongress2015/cybercrime.shtml

30- يونس عرب، جرائم الكمبيوتر والإنترنت، مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-12 فيفري2002، ص.ص.1-12، على موقع:
http://www.uomisan.edu.iq/library/admin/book/52524504996.pdf

4 - النصوص القانونية:

I- النصوص التشريعية :

1- قانون رقم 05- 02 مؤرخ في 06 فيفري 2005، يعدل ويتمم الأمر رقم 75- 59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري ،جريدة رسمية عدد37، صادر في 07جويلية 2007،(معدل ومتمم).

2- قانون رقم 05- 10 مؤرخ في 20 جوان 2005، يعدل ويتمم الأمر رقم 75-58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، جريدة رسمية عدد 44، صادر في 20جوان 2005.، (معدل ومتمم).

3 - قانون رقم 09- 04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة الرسمية عدد 47، صادر في 16 أوت 2009.

4- قانون رقم 14-01 مؤرخ في 4 فيفري2014، يعدل ويتمم الأمر رقم 66-156 يتضمن قانون العقوبات، جريدة رسمية عدد 07، صادر في 16فيفري 2014، (معدل ومتمم).

5- قانون رقم 15-03 مؤرخ في 01 فيفري،2015 يتعلق بعصرنة العدالة، جريدة رسمية عدد 06 ، صادر في 20 فيفري 2015.

6- قانون رقم 15-04 مؤرخ في 01 فيفري2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 06، صادر قي 20 فيفري2015.

7- قانون رقم17-07 مؤرخ في 27 مارس 2017، يعدل ويتمم الأمر رقم 66-155 يتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 20، صادر بتاريخ 29 مارس 2017.

8 - قانون رقم 18-05 مؤرخ في 10ماي2018، يتعلق بالتجارة الإلكترونية، جريدة رسمية عدد28، صادر في 18ماي2018.

II-النص التنظيمي:

- مرسوم تنفيذي رقم 07- 162 مؤرخ في 30 ماي 2007 يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 ماي 2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

III - الوثائق الدولية :

1- قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16ديسمبر 1996، على الموقع:
https://www.uncitral.org/pdf/arabic/texts/electcom/ml-ecomm-a_ebook.pdf

2- اتفاقية بودابست الصادرة بتاريخ 23 نوفمبر 2001، على موقع:
https://rm.coe.int/budapest-convention-in-arabic/1680739173

3- قواعد الأونسترال الموحد بشأن التوقيعات الإلكترونية لسنة 2001، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 12ديسمبر2001، متوفر عبر الموقع المنشور باللغتين العربية والانجليزية:

http://www.uncitral.org.stabl/ml-elecsig-a.pdf

4 - القانون العربي الاسترشادي الموحد للمعاملات والتجارة الإلكترونية، صادر بقرار مجلس وزراء العدل العرب رقم 812/د ، صادر بتاريخ 19نوفمبر 2009، على موقع:

https://www.carjj.org/legal-terms/4671/print

IIII- النصوص التشريعية للدول الأجنبية:

1- القانون المدني التونسي على موقع: http://www.legislation.tn/

2- قانون الإجراءات الجنائية المصري على موقع: http://laws.jp.gov.eg/

3- قانون عدد 83 لسنة 2000 المؤرخ في09-09-2000 المتعلق بالمبادلات والتجارة الإلكترونية التونسي المنشور بالرائد الرسمي للجمهورية التونسية المؤرخ في 11أوت 2000، على موقع: http://www.legislation.tn/

4- قانون رقم 82 لسنة 2002 بإصدار قانون حقوق الملكية الفكرية متوفر على موقع:

http://www.egypo.gov.eg/page.aspx?id=27

5- قانون رقم 02 لسنة 2002 بشأن المعاملات والتجارة الالكترونية الإماراتي، على موقع:

https://www.dc.gov.ae/

6- قانون رقم 15- 2004 خاص بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، متوفر على موقع:

www.mcit.gov.eg/Ar/Media_Center/Press.../1158

7- قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015، على موقع:

http://www.cbj.gov.jo/

ثانيا: باللغة الفرنسية

I - OUVRAGES :

1- Abbas JABER, Les infractions commises sur Internet, L'Harmattan, Paris, 2009 .

2-Arnaud-François fausse, la signature électronique transaction et confiance sur internet, DUNOD, Paris, 2001.

3- Alain Bensoussan, L'informatique et le droit, Tome 2, HERMES, Paris, 1995.

4-Alain Bensoussan, Informatique, télécoms, Internet, Francis, LEFEBVRE, Paris, 1997.

5- BOCHURBERG Lionel, internet et commerce électronique, 2e édition, DELMAS, Paris, 2001.

6 -Florence Mas, La conclusion des contrats du commerce électronique, Paris, 2005.

7- HUET Jérôme, vers une consécration de la preuve et la signature électronique, DALLOZ, Paris, 2000.

8- Jacques Larrieu, Droit de l'internet, Ellipses, Paris, 2010.

9 - Marie Pierre Fenoll Trousseau et Gérard Haas, Internet et

protection des données personnelle, LITEC, Paris, 2000.

10 - Michel Bibent, Le Droit du traitement de l'information, Nathan, Paris, 2000.

11 - OLIVIER D'AUZON, Le droit du commerce électronique, puits fleuri, Paris, 2004

12 - PIETTE-COUDOL Thierry, la signature électronique, édition LITEC, Paris, 2001.

13- Roger Merle et André Vitu, Traité de droit criminel, tome1, 7emeédition, Cujas, Paris, 2000.

14 - RENARD Isabelle, vive la signature électronique, DALLOZ, Paris, 2002.

15- R Bisciari, Les contrats et la preuve dans l'environnement électronique, UGA, Bruxelles, 2004.

16 - THIEFFRY Patrick, commerce électronique, droit international et européen, LITEC, Paris, 2002.

17-Thibault Verbiest, La protection juridique du cyberconsommateur, LITEC, Paris, 2002.

18 -Verbiest Thibauult et wéry Etienne, Le droit de l'internet et de la société de l'information, Larcier, Bruxelles, 2001.

19- Xavier linant de bellefonds, Alain Hollande, Pratique du droit de l'informatique et de l'internet, 6emeédition, Delmas, Paris, 2008.

II - ARTICLES :

1 - CAPRIOLI Eric, Le juge et la preuve électronique , sur le site : https://www.caprioli-avocats.com/fr/

2 - CAPRIOLI Eric, les moyens juridiques de lute contre la cyberciminalité, Revue 46 risque n° 51, septembre 2002, sur le site : https://www.caprioli-avocats.com/fr/

3 - Éric Labbé, La multiplicité des normes encadrant le contrat électronique : l'influence de la technologie sur la production des normes , sur le site : https://www.lex-electronica.org/auteur-e-s/labbe-eric/

4 - GAUTRAIS Vincent, Droit du commerce électronique et normes applicable, Revue de droit des affaires,1997 internationales, p.p.547-584, sur le site : https://www.iblj.com/abstract.htm

5 - MICHEL Jaccard, Problèmes juridiques liés à la sécurité des transactions sur le réseau , sur le site : http://www.signelec.com/content/se/articles/article_michel_jaccard_html.

6 - SEDALLIAN Valérie, Preuve et signature électronique , article disponible sur le site : http://juriscom.net/chr/2/fr20000509.htm.

7- Yann padova, un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénale, Article disponible sur le site : https://criminocorpus.org/fr/

III - Textes juridiques:

A- Directives:

1- Directive 1999/93/CE du parlement européen et du Conseil, du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

2- Directive 97/7CE du parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance, *J.O* n°L144 DU 04 Juin 1997.

B -Textes législatifs:

1- Code civil Français, sur le site:

https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070

2- Code pénal français, sur le site:

https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070

3- Code de procédure pénale français, sur le site:
https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071

4- Loi n° 90- 1170 du 29 décembre 1990 sur la réglementation des télécommunications, *J.O.R.F* n°303 du 30 décembre1990.

5- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *J.O.R.F.*n°62 du 14mars 2000.

6- Loi n° 2001-1062, du 15 novembre 2001portant code de procédures pénales, *J.O.R.F* du 16 novembre2001.

7- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *J.O.R.F* n° 43 du 22juin 2004.

C - Texte réglementaire:

- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, Modifié par Décret n° 2017 du 28septembre 2017.

الفهرس

الفهرس

ملخص :

ساهم التطور الكبير في تكنولوجيا الاتصالات والمعلومات في ازدياد نسبة التعامل بالمحررات الإلكترونية الذي كان له دورا ايجابيا في تحسين أداء الخدمة للمتعاملين، سيما أن التحول إلى تعميم استعمالها أصبح يأخذ حيزا مهما في التعاملات الالكترونية، بالتالي لا بد وأن يسبقه تنظيم تشريعي يكفل الضوابط والشروط اللازمة لإضفاء المصداقية عليها، ويعزز الثقة في هذه المحررات الصادرة عبر هذه الوسائل، لأن الأمر يزداد تعقيدا في ظل تنامي وتزايد ظاهرة الإجرام المعلوماتي، بالتالي أصبح أمنها له أهمية كبرى في تحقيق استقرار النظام القانوني لهذه المعاملات، مما أدى بنا إلى ضرورة البحث في مدى فاعلية الآليات القانونية التي اعتمدتها التشريعات المقارنة في ضمان الأمن القانوني للمحررات الإلكترونية، الأمر الذي يترتب عليه بالضرورة العمل على البحث عن آخر ما توصل عليه في مجال الحماية التقنية، وسن وتطبيق التشريعات بشكل يتناسب مع هذا النوع المستحدث من الجرائم التي تتعلق بالاعتداء عليها، لا سيما التركيز على الإطار الرئيسي الذي يتيح لهذه التشريعات تبني أفضل تقنية من أجل تطبيق نصوصه بشكل ملائم، يواجه التحديات التي تفرضها هذه الجرائم على القوانين الجنائية التقليدية الحالية بشقيها الموضوعي والإجرائي، على اعتبار أن هذا النوع من الجرائم له طبيعته الخاصة تميزها عن باقي الجرائم.

Résumé :

Les progrès importants réalisés dans les technologies de l'information et de la communication, ont grandement contribué à l'augmentation du pourcentage des traitements des fichiers électroniques, qui ne cesse de jouer un rôle positif quand à l'amélioration des performances des clients en matière de services d'un coté, de l'autre coté la cybercriminalité qui est un phénomène de plus en plus complexe.

Sa sécurisation étant d'une importance capitale pour la stabilité du système juridique des transactions à travers tous les pays, doit conduire à priori, à revoir et d'examiner l'efficacité des mécanismes juridiques adoptés par la législation comparée, afin de parvenir à sécuriser juridiquement les documents électroniques, ceci implique nécessairement à rechercher les dernières conclusions en matière de protection technique, ainsi que la promulgation d'une législation compatible avec ce type d'infractions liées à des voies de fait.

La concentration particulière sur le cadre principal permettra à une telle législation d'adopter la meilleure technologie afin d'appliquer ses dispositions dans un cadre juridique approprié, et parvenir à relever tous les défis posés par ces crimes aux lois pénales traditionnelles existantes, tant sur le fonds que sur la procédures applicables.