جامعة ابن خلدون – تيارت–
كلية الحقوق والعلوم السياسية
قسم الحقوق

مقدم ضمن متطلبات نيل شهادة الماستر في الحقوق
تخصص: علاقات مهنية

الموضوع:

الحماية القانونية للعقد المبرم عبر الأنترنت

من إعداد الطالبتين:
– سي مرابط زينـــب
– غلام الله بنت الشيخ

إشراف الدكتور:
– بلقنيشي حبيب

أعضاء لجنة المناقشة

أعضاء اللجنة	الرتبة	الصفة
د. بن عمارة محمد		رئيسا
د. بلقنيشي حبيب		مشرفا مقررا
د. هروال نبيلة هبة		عضوا مناقشا

السنة الجامعية: 2016م/ 2017م

أتقدم بكلمة شكر وعرفان للدكتور بلقنيشي الحبيب الذي أشرف على عملي هذا والذي تم بفضل الله وبفضل نصائحه وتوجيهاته القيمة وأتقدم أيضا بالشكر والتقدير لأول من أخد بأناملي الصغيرة لتعلم أبجديات اللغة العربية معلمتي عابد رقية وإلى من زرع في نفسي روح العمل الجماعي والتعاون أستاذي الفاضل بختي.

إهداء

أهدي ثمرة عملي المتواضع إلى روحي أبي وأمي الغالية

وإلى بناتي عائشة ورشا وإلى إخوتي وأخواتي

وإلى كل من ساهم في انجاز هذا العمل من قريب أو من بعيد

وإلى كل الأهل والأصدقاء

زينب

إهداء

إلى روح أبي العزيز رحمه الله وأسكنه فسيح جناته

إلى النبع الذي ارتويت منه دعاءا وبركات روح جدتي الطاهرة

إلى التي أعانتني بدعائها أمي الحنون حفظها الله

إلى إخوتي وزوجاتهم وأخواتي وأزواجهم والأبناء

إلى كل الأهل والأقارب والأحباب

إلى كل من ساعد في إنجاز هذا العمل المتواضع من قريب أو من بعيد.

غلام الله

مُقَدِّمَةٌ

مقدمـــــة:

شهد العالم أواخر القرن العشرين تطورا هائلا في تقنيات الاتصال الحديثة وثورة في تكنولوجيا المعلومات كان من ابرز نتائجها أن أصبح العالم قرية صغيرة تتبادل فيه المعلومات عبر مختلف أنحائه في ظرف قصير وبأقل جهد بفضل ما يطلق عليه الشبكة العالمية للمعلومات أو الانترنت التي ساهمت في إحداث تحولات وإدخال تغيرات على المجتمع في مختلف مناحي حياته الاجتماعية والثقافية والاقتصادية وحتى القانونية، ومن ذلك أنه أصبح يتم إبرام المعاملات والصفقات والعقود التجارية بطريقة الكترونية عبر تبادل البيانات والمعطيات والمعلومات بشكل مستندات رقمية حلت محل سابقتها العادية الورقية مستخدمين في ذلك ومعتمدين على الحاسوب الآلي وعلى المواقع التجارية الإلكترونية الموجودة على مستوى الشبكة الدولية أو عن طريق البريد الإلكتروني.

لقد واجهت عملية إبرام العقود الكترونيا في بادئ الأمر صعوبات وعراقيل كما واجهت العديد من التحديات فقد كان من الصعوبة بمكان تحديد هوية الأشخاص المتعاقدين والتحقق من توافر إرادتيهما وسلامتها من كل ما يشوبها من عيوب، وحتى التأكد مما إذا كانت هناك جدية في هذا التعاقد من عدمها وكذا التعرف على حقيقة مضمونه وكيفيات إثباته.

كل هذه الأسباب مجتمعة دفعت بالدول والحكومات ومختلف المنظمات العالمية وغير العالمية، الحكومية وغير الحكومية إلى العمل على وضع تشريعات وقوانين تكفل الحفاظ على عملية التعاقد الإلكتروني وضمان استمراريتها وديمومة العمل بها، كونها أضحت تشكل مظهرا من مظاهر التطور التكنولوجي في التعاملات التجارية ورهانا وتحديا مستقبليا، والاهم من ذلك البحث عن التشريعات والقوانين والآليات والوسائل التي تضمن حماية هذه العقود من أي خرق أو تزوير أو إخلال بمضمونها ومحتواها والغاية منها ، وكذا الفصل في المنازعات التي تنجر عن التعامل بها، الأمر الذي دفعنا في الأخير إلى التساؤل عن طرح الإشكال التالي:

إشكالية البحث:

باعتبار أن قانونية المعاملات لا تكون إلا بوجود عقد يوثق العملية، فان المعاملة الإلكترونية تخضع لما يسمى بالعقد الإلكتروني، إلا أن الإشكال الذي يطرح نفسه هو: **ما هي السبل والآليات التي تكفل الحماية القانونية للعقد المبرم عبر الانترنت؟**

يعتبر العقد الإلكتروني موضوع الساعة فأصبح من الموضوعات الهامة يفرضه الواقع والمستقبل حيث كثر الإشكال حول مدى إحلال العقد الإلكتروني محل العقد العادي فهو يكتسي أهمية بالغة من الناحية العلمية والعملية.

إن الأهمية العلمية والقانونية للبحث فإنها تساعد المتعاملين في هذا المجال إلى توعيتهم بالآثار القانونية للتعامل عبر الوسيلة الحديثة وما هي الحماية المقررة لهذا النوع من العقود؟ وتقديم الأطر القانونية الملائمة لتنظيم هذه المعاملات الإلكترونية بالشكل الذي يحقق الثقة والأمان القانوني للطرفين المتعاقدين عبر الانترنت.

تكمن الأهمية العملية لموضوع البحث في ارتباطه بعقود أصبح التعامل بها يزداد يوما بعد يوم مما يستدعي إيجاد أساليب لحماية هذه العقود فالتعامل من خلال شبكة الاتصالات الإلكترونية في صورة عقود دولية أصبح من الأمور المفروضة على الدول والأفراد بالنظر إلى ما تحققه من قيمة مادية واقتصادية وما توفره من جهد ووقت من الانتقال والسفر من بلد إلى آخر.

إن الاهتمام الوطني والدولي بهذا النوع من العقود أصبح متزايدا نظرا لأهميتها الكبيرة في حياة الأفراد والدول خاصة في إطار ما يعرف بالتجارة الرقمية أو الإلكترونية.

نظرا لحداثة هذا النوع من العقود وأهميته أصبحت الحاجة ملحة لظهور دراسات قانونية حول ماهية هذا الموضوع المستجد في القانون لمعرفة مدى الاستجابة لمعطيات الحداثة وتكنولوجيا المعلومات وما ينجم عنه من إشكاليات ومنازعات وكيفية التصدي لذلك من خلال سن قوانين لحماية المتعاملين في إطاره.

كما يرجع السبب كذلك إلى نقص الثقافة القانونية لدى المتعاملين في التجارة الإلكترونية خاصة في الدول النامية، وكذا يرجع السبب لاختيار هذا الموضوع إلى الشغف لمعرفة كل ما هو جديد خصوصا فيما يتعلق بالجانب القانوني.

من بين الصعوبات في هذا الموضوع هو الصبغة الفنية التي يتسم بها هذا البحث حيث يتحتم الإلمام بالجوانب الفنية لتقنيات الاتصال الحديثة، وكذا حداثة الموضوع وتشعبه مما يستوجب التطرق إلى فروع القانون المختلفة كالقانون المدني القانون التجاري القانون الدولي الخاص بالإضافة اللجوء إلى الاتفاقيات الدولية والقوانين النموذجية والتوجهات الأوروبية، إضافة إلى قلة المراجع القانونية المتخصصة في الموضوع.

تقتضي الدراسة لهذا الموضوع الاعتماد على العديد من المناهج.

المنهج التحليلي الوصفي: وهذا من خلال التطرق إلى ماهية العقد الإلكتروني (تعريفه – مهامه– أنواعه – أدواته –كيفية إبرامه ومما يتكون....)

المنهج المقارن: يتجلى ذلك من خلال عرض ومقارنة وتحليل مختلف التشريعات والاتفاقيات والتوجيهات الصادرة بشان التجارة الإلكترونية وتأثرها في ظل المعاملات الإلكترونية.

لمعالجة الموضوع قسمنا هذا البحث إلى فصلين يسبقهما فصل تمهيدي ينتهي بخاتمة وذلك كما يلي:

الفصل التمهيدي: وتطرقنا فيه إلى ماهية العقد الإلكتروني وذلك من خلال تعريفه وخصائصه وما يميزه عن باقي العقود وكذا أركانه وكيفية إبرامه، أما في الفصل الأول فتحدثنا عن الحماية المدنية للعقد الإلكتروني وهذا من خلال مبحثين.

المبحث الأول تكلمنا فيه عن الكتابة الإلكترونية من خلال التعريفات التي شملتها وكذا شروطها وأهدافها وحجيتها في الإثبات، أما المبحث الثاني فتطرقنا فيه إلى التوقيع الإلكتروني من خلال تعريفه وصوره وأهدافه وما هي آليات حمايته، أما بالنسبة للفصل الثاني تناولنا فيه الحديث عن الحماية الجنائية للعقد الإلكتروني وهذا من خلال مبحثين.

المبحث الأول تعرضنا لتطور الحماية الجنائية وتجريم الاعتداء غير المشروع لمواقع التعاقد على الصعيد الدولي والصعيد الداخلي في المطلب الأول وتجريم الاعتداء غير المشروع لمواقع التعاقد عبر الانترنت في المطلب الثاني وجريمة التلاعب ببيانات نظام معالجة المعطيات في المطلب الثالث

أما المبحث الثاني فتناولنا بالدراسة العقوبات المقررة لكل جريمة ونطاق تطبيقها وهذا بالتعرض إلى العقوبات الأصلية في المطلب الأول والعقوبات التكميلية في المطلب الثاني وأخيرا نطاق تطبيق العقوبة في المطلب الثالث.

أما الخاتمة فتضمنت أهم ما توصلنا إليه من نتائج في دراستنا لهذا الموضوع.

الفصل التمهيدي

ماهية العقد الإلكتروني وانعقاده

الفصل التمهيدي: ماهية العقد الإلكتروني وانعقاده

كون العقد الإلكتروني أصبح ظاهرة عصرية ناجم عن استخدام الوسائل التقنية الإلكترونية بما فيها التكنولوجيا الحديثة مما تحتم اتجاه الأبحاث القانونية إلى محاولة تنظيم هذه الظاهرة العصرية وما يتلاءم واندماج الوسائل التقنية في الجوانب القانونية اندماجا متوازنا يحدد كيفية استخدامها في مجال العقود والمعاملات التجارية[1].

هذا ما يؤدي بنا إلى تحديد ماهية هذا النوع من العقود من خلال تحديد مفهومه وكذا خصائصه وما يميزه عن بقية العقود في (المبحث الأول) والتطرق إلى كيفية انعقاد العقد الإلكتروني في (المبحث الثاني).

المبحث الأول: ماهية العقد الإلكتروني

يتم التطرق في هذا المبحث إلى تحديد مفهوم العقد الإلكتروني سواء من خلال التعاريف التي وردت في المواثيق الدولية أو من خلال التعاريف الفقهية وكذلك الإلمام بأهم الخصائص التي يتميز به هذا العقد.

المطلب الأول: مفهوم العقد الإلكتروني وخصائصه

لا يمكن إعطاء تعريف موحد للعقد الإلكتروني، فهو يرتبط ارتباطا وثيقا بالتجارة الإلكترونية، ورغم عدم اختلافه عن العقد التقليدي من حيث أركانه وشروط صحته إلا أن له خصائص تجعله يتميز عن باقي العقود الأخرى وهذا ما سوف نتطرق إليه من خلال هذا المطلب.

الفرع الأول: تعريف العقد الإلكتروني

أ-التعريف الوارد في المواثيق الدولية:

أ-1: التعريف الذي جاء به القانون النموذجي للأمم المتحدة حول التجارة الإلكترونية[2] في المادة الثانية "بتبادل البيانات الإلكترونية l'échange de données informatique"، حيث نصت هذه المادة بأنه يراد بمصطلح تبادل البيانات الإلكترونية نقل المعلومات من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات.

[1] – عتيق حنان، مبدأ سلطان الإرادة في العقود الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون، جامعة البويرة، 2012، ص 04.

[2] – غول نجاة، العقد الإلكتروني، مذكرة لننيل شهادة الماستر، جامعة خميس مليانة، 2013-2014، ص 13.

ورأت لجنة الأمم المتحدة للقانون التجاري الدولي بأن هذا التعريف ينصرف إلى كل استعلامات المعلومات الإلكترونية ويشمل بذلك إبرام العقود والأعمال التجارية المختلفة وعليه فإن العقد الإلكتروني حسب هذا قانون هو العقد الذي يتم التعبير فيه عن الإرادة بين المتعاقدين باستخدام الوسائل المحددة في المادة الثانية وهي: نقل المعطيات من كمبيوتر إلى كمبيوتر آخر وفقا لنظام عرض موحد.

نقل الرسائل الإلكترونية باستعمال قواعد عامة أو قواعد قياسية، النقل بالطريق الإلكتروني للنصوص باستخدام الانترنيت، أو عن طريق استعمال تقنيات أخرى كالتلكس أو الفاكس.

أ-2 :التعريف الوارد في الوثائق الأوربية:

نصت المادة 2 من التوجيه رقم97 -07 الصادر في 20 ماي1997[1] الصادر عن البرلمان الأوربي والمتعلق بالتعاقد عن بعد وحماية المستهلكين في هذا المجال، بأنه يقصد بالتعاقد عن بعد: "كل عقد يتعلق بالبضائع أو الخدمات أبرم بين مورد ومستهلك في نطاق نظام بيع أو تقديم الخدمات عن بعد نظمه المورد الذي يستخدم لهذا العقد تقنية أو أكثر للاتصال عن بعد لإبرام العقد أو تنفيذه"، وعرفت تقنية الاتصال عن بعد في نفس النص بأنها: "كوسيلة بدون وجود مادي ولحظي للمورد وللمستهلك يمكن أن تستخدم لإبرام العقد بين طرفيه"، فهذا التوجيه قد عرف العقود عن بعد التي تشمل في مفهومها العقود الإلكترونية.

ب- التعريف الوارد في منظمة التجارة العالمية wto:

عرفت منظمة التجارة العالمية[2] بأن التجارة الإلكترونية "عبارة عن عملية إنتاج وترويج وبيع وتوزيع منتوجات من خلال شبكة اتصال و لم يقصرها على الانترنيت فقط".

ومن هذا التعريف يتضح أن التجارة الإلكترونية تستعمل جميع الأنظمة الناشئة عن العلاقات ذات الطابع التجاري، سواءً كانت تعاقدية أم لم تكن، ولكن يعاب على هذا التعريف أنه قصر الأنشطة التجارية على المنتجات غير الخدمات، ومن ثمة لا يدخل في نطاق هذا التعريف الخدمات.

[1]- غول نجاة، مرجع سابق، ص 14.

[2]- منظمة التجارة العالمية هي إحدى المنظمات التي تهتم بالتجارة الإلكترونية وتعمل على تحرير التجارة العالمية وتضم عضويتها أكثر من 13 دولة في العالم.

ج-التعريف الفقهي للعقد الإلكتروني

الفقه أورد[1] عدة تعريفات للعقد الإلكتروني، فمنهم من اعتبر أن "العقد الإلكتروني هو العقد الذي يتم إبرامه عبر الانترنيت"، وبذلك يكون قد عرف العقد بناء على وسيلة إبرام العقد الإلكتروني في شبكة الانترنيت متجاهلا الوسائل الأخرى لإبرامه مثل التلكس والفاكس .

ومن من عرف أن العقد الإلكتروني: "هو كل اتفاق يتلاقى فيه الإيجاب بالقبول على شبكة دولية مفتوحة للاتصال عن بعد، وذلك بوسيلة مسموعة مرئية، وذلك بفضل التفاعل بين الموجب والقابل".

ويستقرا من هذا التعريف اشترط وسيلة مسموعة مرئية، لكي يعتبر العقد الكترونيا، إلا أنه يمكن إبرام العقود الإلكترونية بدون استعمال الوسائل المسموعة أو المرئية، مثل التعاقد عبر البريد الإلكتروني الذي يكون فيه التعبير عن الإرادة بواسطة الكتابة، ومع ذلك يعتبر العقد الكترونياً.

ومن التعاريف ما يكتفي بأن يكون العقد مبرما ولو جزئيا بوسيلة الكترونية لاعتباره عقدا الكترونيا.

فمنه القائل:" أن العقد الإلكتروني هو الاتفاق الذي يتم انعقاده بوسيلة الكترونية كليا أو جزئيا، أصالة أو نيابة"

ومن التعاريف ما شمل جميع الوسائل الإلكترونية، لكنه اشترط لكي يعتبر العقد الكترونيا أن تكتمل كافة عناصره عبر الوسيلة الإلكترونية، حتى إتمامه، معتبرا أنه:" كل عقد يتم عن بعد باستعمال وسيلة الكترونية، وذلك حتى إتمام العقد.

وهو نفس الاتجاه[2] الذي سارت عليه اللجنة التي شكلت في مصر لتنظيم التجارة الإلكترونية، إذ عرفت عقود التجارة الإلكترونية بأنها تنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري آخر، أو بين مشروع ومستهلك، وذلك باستخدام تكنولوجيا المعلومات والاتصال، غير انه يجب التركيز في تعريف.

العقد الإلكتروني على خصوصيته التي تتمثل بصفة أساسية في الطريقة التي ينعقد بها ومن دون إغفال صفة عامة فيه، باعتباره ينتمي إلى طائفة العقود التي تبرم عن بعد.

---

[1]- عبد الفتاح بيومي الحجازي، النظام القانون لحماية التجارة الإلكترونية، الكتاب الأول، دار الفكر الجامعي، 2002، ص 47.

[2]- أحمد خالد العاجولي، التعاقد عن طريق الانترنت، دراسة مقارنة، المكتبة الوطنية، عمان، الأردن، طبعة 2002، ص 123.

الفرع الثاني: خصائص العقد الإلكتروني

العقد الإلكتروني يتميز بخصائص تميزه عن غيره من العقود ومن بين هذه الخصائص[1]:

أولا: العقد الإلكتروني عقد يبرم عن بعد: العقد الإلكتروني يبرم عن بعد عبر تقنيات الاتصال المختلفة وهي تلك العقود التي تبرم بين طرفين يتواجدان في أماكن متباعدة، وهذا باستعمال وسيلة أو أكثر من وسائل الاتصال عن بعد.

ثانيا: العقد الإلكتروني عقد تجاري:من خصائص العقد الإلكتروني بالطابع التجاري ولذلك يطلق عليه عادة تسمية عقد التجارة الإلكترونية E-Commerce، وغالبا يكون في عقود البيع أو تقديم الخدمات أو القرض أو سواها من العقود.

ثالثا: العقد الإلكتروني عقد مبرم بوسيلة الكترونية: يتم إبرام العقد الإلكتروني عبر شبكة الاتصال الإلكترونية، فهو من حيث الموضوع أو الأطراف لا يختلف عن باقي العقود التقليدية ولكن الاختلاف يكمن في طريقة حيث يتم بوسائط الكترونية الورقية ليظهر ما يسمى بالكتابة الإلكترونية التي تقوم على دعائم الكترونية.

رابعا: العقد الإلكتروني عقد عابر للحدود: ذلك لأن الطابع العالمي لشبكة الانترنت[2] وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم يسهل العقد بين طرف في دولة وطرف آخر في دولة أخرى، بل تتعداها لتشمل أنحاء العالم.

المطلب الثاني: تمييز العقد الإلكتروني عن باقي العقود

إن العقد الإلكتروني يعد مميزا عن الصورة التقليدية للتعاقد وعليه نتطرق إلى أهم الخصائص التي يتميز بها وذلك على النحو التالي:

الفرع الأول: تمييز العقد الإلكتروني عن العقد التقليدي

رغم أن العقد التقليدي والعقد الإلكتروني يتفقان في أنهما ينعقدان باتفاق إرادتي المتعاقدين، إلا أن الأول يتم تبادل الإيجاب والقبول في مجلس عقد واحد، وهذا ما لا يتوافر في العقد الإلكتروني حيث أن

[1]- غول نجاة، مرجع سابق، ص 19.

[2]- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، طبعة 2005، ص 44.

الانفصال المكاني في التعاقد الإلكتروني يجعله يكتسي ميزة خاصة[1]، بالإضافة إلى ظهور طرق الدفع الإلكترونية والتي حلت محل النقود العادية مما أدى إلى ظهور مجموعة من الخدمات البنكية الإلكترونية[2].

الفرع الثاني: تمييز العقد الإلكتروني عن العقود المبرمة عن بعد

أ- يختلف التعاقد الإلكتروني عن التعاقد بواسطة الهاتف، لان شبكة الانترنت لا تقتصر خدماتها على نقل الصوت فقط وإنما في نفس الوقت الصورة والحركة والكتابة وأيضا بشكل آني وتفاعلي.

ب-أما التعاقد الإلكتروني والتعاقد عن طريق التلفاز فيتشابهان في أن الرسالة المنقولة هي نفسها بالنسبة لكافة العملاء إذ تتم بالصوت والصورة، إلا أن التعاقد في النوع الأول يكون الإعلام فيه عن طريق الإذاعة المرئية المسموعة ويتم إبلاغ القبول عبر الاتصال بالتليفون، أما في العقد الإلكتروني فيظل قائما 24 ساعة

ويكون الاستعلام عن التفاصيل من خلال تصفح صفحات موقع الانترنت، والتعبير عن القبول يتم عبر التبادل الإلكتروني للبيانات أو عن طريق البريد الإلكتروني، أو بالضغط على عبارة الموافقة عن طريق لوحة مفاتيح الكمبيوتر[3].

المبحث الثاني: انعقاد العقد الإلكتروني

ينعقد العقد الإلكتروني عن بعد بدون حضور مادي للمتعاقدين ويتم التعبير عن الإرادة عبر تقنيات الاتصال عن بعد، فلابد من تلاقي الإرادتين بأن يصدر الإيجاب أولا ثم يعقبه القبول وغالبا ما سبق انعقاد العقد الإلكتروني مرحلة التفاوض، بالإضافة إلى توافر الأركان التي يتطلبها إبرام العقد[4].

المطلب الأول: التراضي

يتطلب انعقاد العقد الإلكتروني كغيره من العقود توافق إرادتي المتعاقدين، وهذا ما نصت عليه المادة 59 من القانون المدني: "يتم العقد بمجرد تبادل الطرفان التعبير عن إرادتهما المتطابقتين دون الإخلال

[1]- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، طبعة 2006، ص 67.
[2]- خالد ممدوح إبراهيم، المرجع نفسه، ص 55، 56.
[3]- خالد ممدوح إبراهيم، المرجع نفسه، ص 68، 69.
[4]- غول نجاة، مرجع سابق، ص 30.

بالنصوص القانونية"، إذا لابد من تلاقي الإرادتين بان يصدر الإيجاب أولا ثم يعقبه القبول وغالبا ما يسبق انعقاد العقد الإلكتروني مرحلة التفاوض.

الفرع الأول: التفاوض الإلكتروني

لابد أن يسبق[1] العقد الإلكتروني كغيره من العقود مرحلة المساومة والتفاوض، ولهذه المرحلة أهميتها في العقد لأنها تهيئ لإعداد العقد إعداداً جيدا يحول دون قيام المنازعات بين الطرفين في المستقبل.

لا يختلف عقد التفاوض في تعريفه عن أي عقد آخر فهو تصرف قانوني بين طرفين بهدف ترتيب أثر قانوني معين ولا يتطلب لوجوده وصحته سوى توفر الشروط المقررة للعقود بصفة عامة.

يظل عقد التفاوض عقدا رضائيا حتى ولو كان العقد النهائي المراد إبرامه في نهاية المطاف عقداً شكليا ومن ثمة فإن عقد التفاوض الإلكتروني يتم بتوافق القبول مع الإيجاب على الدخول في العملية التفاوضية.

الفرع الثاني: تلاقي الإرادتين في العقد الإلكتروني (التراضي)

يتطلب انعقاد العقد الإلكتروني كسائر العقود توافق إرادتي المتعاقدين على إحداث أثر قانوني المقصود من العقد ويتحقق هذا التوافق بتبادل التعبير وفقا لإرادتين متطابقتين وهو التراض الذي يكفي لوجود العقد طبقا بتوافر الأركان الأخرى ويتم التعبير عن إرادة التعاقد إيجابا وقبولا، كما نصت عليه أحكام المادة 59 من القانون المدني: "يتم العقد بمجرد تبادل الطرفان التعبير عن إرادتهما المتطابقتين دون الإخلال بالنصوص القانونية".

لم يتطرق المشرع الجزائري إلى التعبير عن الإرادتين في العقد الإلكتروني، واكتفى إلى تطبيق القواعد العامة التي تخضع لها العقود التقليدية[2]، إلا أن ظهور الوسائل الجديدة للتعبير عن الإرادة جعلت التساؤلات تطرح في الآونة الأخيرة حول المشروعية في إبرام العقود الإلكترونية ولهذا يلزمنا التطرق أولا توافق الإرادتين عن طريق الإيجاب والقبول ثم صور التعبير عنها بالوسائل الإلكترونية.

[1]- غول نجاة، مرجع سابق، ص 33.

[2]- خالد ممدوح إبراهيم، مرجع سابق، ص 284، 285.

أ- **الإيجاب الإلكتروني**: الإيجاب بصورة عامة هو تعبير عن الإرادة الصادر، عن أحد المتعاقدين والموجه إلى الطرف الآخر، يقصد إحداث أثر قانوني، والإيجاب في العقد الإلكتروني هو التعبير عن إرادة الراغب في التعاقد عن البعد، حيث يتم من خلال شبكة دولية للاتصالات[1].

ب-**القبول الإلكتروني**:إن القبول هو الإرادة الثانية في العقد التي تظهر بصورة جازمة باتة معبرة عن موقف الطرف الآخر الذي وجه إليه الإيجاب، فالعقد لا يتم إلا باكتمال عقد الرضا، وفيما يتعلق بالقبول

المطلب الثاني: المحل، السبب والشكلية

إضافة إلى ركن التراضي يستلزم لانعقاد العقد الإلكتروني توافر ركنين: المحل والسبب بالإضافة إلى الشكلية المتطلبة.

الفرع الأول: ركن المحل

محل الالتزام هو الشيء الذي يلتزم به المدين القيام به، ويشترط في محل العقد بصفة عامة، انو يكون موجودا أو ممكن الوجود، معينا أو قابلا للتعيين، وان يكون مشروعا، ويخضع المحل في العقود الإلكترونية لنفس هذه الشروط[2].

الفرع الثاني: ركن السبب

السبب هو الغرض المباشر الذي يقصد الملتزم الوصول إليه من وراء التزامه، ويشترط أن يكون السبب كركن من الأركان المكون للعقد بصفة عامة – والعقد الإلكتروني بصفة خاصة-، مشروعا وغير مخالف للنظام العام والآداب العامة، وهذا ينطبق كذلك على العقود المبرمة عبر تقنيات الاتصال الحديثة، وبما أن مفهوم الآداب العامة يتطور من زمن لآخر، ويختلف من دولة لأخرى، وعليه فإن ما يعتبر مناقضا للآداب العامة في دولة، قد لا يكون كذلك في دولة أخرى، وبالتالي فإن السبب كركن من أركان العقد، لا يثير أي إشكال في العقود المبرمة عبر وسائل الاتصال الحديثة، وتبقى النظرية العامة كافية لتنظيمه في إطار التعاقد الإلكتروني[3].

[1]- غول نجاة، مرجع سابق، ص 34.

[2]- غول نجاة،، المرجع نفسه، ص 52.

[3]- سمير عبد العزيز جمال، التعاقد عبر تقيات الاتصال الحديثة، دراسة مقارنة، طبعة 1، القاهرة، 2006، ص 184.

الفرع الثالث: ركن الشكلية

الأصل في العقود هي الرضائية، أي كفاية مجرد الرضا لقيام العقد وفي ذلك تنص المادة 59 من القانون المدني الجزائري (يتم العقد بمجرد أن يتبادل الطرفان التعبير عن إرادتهما المتطابقتين دون الإخلال بالنصوص القانونية)، والعقد الشكلي هو ذلك العقد الذي لا يتم بمجرد تراضي المتعاقدين، بل يجب لإتمامه زيادة على ذلك، إتباع شكل خاص يعينه القانون، وأكثر ما يكون هذا الشكل ورقة رسمية يدون فيها العقد والأصل العام أن العقود تكون رضائية، لان الأطراف لهم الحرية في اختيار شكل معين لإبرام العقد، أي يكفي تطابق الإيجاب مع القبول لانعقاد العقود بصفة عامة، وهو ما ينطبق على العقد الإلكتروني، غير أن القانون قد يتطلب شكل محدد، كأن يشترط أن يكون العقد مكتوبا، وتكون الكتابة في هذه الحالة، ليست لإثبات العقد وإنما لانعقاده[1].

والمشرع الجزائري أشار إلى مسالة الإثبات بالكتابة من خلال المادة 323 مكرر1 حيث أنه أبقى على القواعد الخاصة المتعلقة بالشكلية بالطرق التقليدية وبالتالي استبعاد الشكلية التي تقوم على الوسائل الإلكترونية الحديثة.

[1]- غول نجاة، مرجع سابق، ض 54.

الفصل الأول

الحماية المدنية للعقد المبرم عبر الانترنت

أتاح التطور التقني في وسائل الاتصال الحديثة إبرام العقود عبر شبكة الانترنت مما أدى إلى ظهور نوع جديد من الكتابة والتوقيع اللذين يتميزان بالطابع الإلكتروني، حيث يتم تبادل رسائل البيانات عبر شبكة الانترنت وتحميلها على دعامات الكترونية، وهذا ما يثير التساؤل حول التحديات التي تواجه إثبات العقود الإلكترونية؟ وما هي آليات الحماية القانونية المقررة لهما، وسنجيب على هذه الأسئلة من خلال تقسيم هذا الفصل إلى مبحثين كما يلي:

المبحث الأول: الكتابة الإلكترونية.

المبحث الثاني: التوقيع الإلكتروني.

المبحث الأول: الكتابة الإلكترونية

أصبح تطور تقنيات المعلومات ظاهرة لا يمكن إغفالها أو إهمالها على المستوى القانوني على نحو يستدعي ضرورة أن يواكب القانون هذا التقدم، مما قاد رجال القانون إلى إعادة التفكير في النظام المعمول به لإثبات التصرفات القانونية الذي يعتمد على مبدأ أولوية الكتابة الورقية والتوقيع الخطي، وسنتناول الكتابة الإلكترونية من خلال تقسيم هذا المبحث إلى ثلاثة مطالب كما يلي:

المطلب الأول: ماهية الكتابة الإلكترونية.

المطلب الثاني: مبدأ التعادل الوظيفي بين الكتابة التقليدية والكتابة الإلكترونية.

المطلب الثالث: حجية الكتابة الإلكترونية في الإثبات.

المطلب الأول: ماهية الكتابة الإلكترونية

نعني بالمفهوم التقليدي للكتابة ذلك المفهوم الذي يحصر الكتابة في طابع مادي بحت سواء من حيث الدعامة التي تدون عليها (الورق) أو من حيث الأداة التي تكتب بها، وهو مفهوم بلا شك يتعارض مع استخدام التقنيات الحديثة التي تتسم بطابع غير مادي، إلا إذا تم ترويضه وحصره في أضيق نطاق ممكن وإضفاء بعض المرونة عليه بشكل يجعله يستوعب هذه التقنيات الجديدة[1].

[1]- كميني خميسة، منصور عزالدين، الإثبات بالكتابة في الشكل الإلكتروني، مذكرة تخرج لنيل شهادة المدرسة العليا للقضاء، دفعة 16، 2005-2006، ص 01.

الفرع الأول: مفهوم الكتابة الإلكترونية

لما كانت الكتابة هي العنصر الأول في المحرر العرفي سواء أكانت في الشكل التقليدي أم الإلكتروني يكون لزاما علينا التعرض إلى مفهومها. ولذلك نحدد ماهيتها على النحو التالي:

أولا: مفهوم الكتابة لدى لجنة الأمم المتحدة للقانون التجاري الدولي

توصل الفريق العامل الرابع التابع للجنة الأمم المتحدة للقانون التجاري الدولي[1]، والمكلف بالعمل التحضيري بشأن التجارة الإلكترونية بعد وضعه الدليل القانوني الخاص بقبول التحويلات الإلكترونية للأموال سنة 1978 وتوصية 1985 المتعلقة بالقيمة القانونية للسجلات الحاسوبية إلى وضع قانونين:

سمي الأول: بقانون اليونسترال النموذجي بشأن التجارة الإلكترونية والمعتمد رسميا من قبل اللجنة العامة للأمم المتحدة بموجب القرار 162/51 الصادر بتاريخ 16 ديسمبر 1996.

أما الثاني فهو قانون اليونسترا النموذجي بشأن التوقيعات الإلكترونية الصادر عن الجمعية العامة للأمم المتحدة بموجب القرار رقم80/56 المؤرخ في 12 ديسمبر 2001، وتلتها اتفاقية الأمم المتحدة المتعلقة بالخطابات الإلكترونية في العقود الدولية سنة 2005.

وقد جاء في القانونين النموذجيين بصدد تعريف المصطلحات أن رسالة البيانات هي:"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 الإلكترونية ،أو البريد الإلكتروني، البرق، أو التلكس، أو النسخ البرقي".

والبيانات هي معلومات الكترونية يمكن من خلالها الوصول إلى نتائج محددة، فهي عبارة عن كلمات أو أرقام أو رموز أو حقائق أو إحصائيات منفصلة عن بعضها، لكن بمجرد وضعها في منظومة معينة يمكن معالجتها آليا وتوصل إلى إعطاء النتائج أو المعلومات التي تستفاد منها وهذه البيانات هي التي تشكل لنا الكتابة في لغة الكمبيوتر[2].

---

[1] – وتسمى الأونيستيرال: وهي لجنة أنشئت بموجب القرار رقم 255 المؤرخ في 1966/12/17 الصادر عن الجمعية العامة للأمم المتحدة تتشكل من 60 دولة منتخبة في الجمعية العامة مع مراعاة تنظيم الأقاليم الجغرافية والأنظمة الاقتصادية القانونية المختلفة مهمتها عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية.

[2] – كميني خميسة، منصور عزالدين، مرجع سابق، ص 04.

ثانيا: مفهوم الكتابة الإلكترونية في التشريع الجزائري

لم يختلف التشريع الجزائري عن غيره، وجاء مواكبا للمستجدات القانونية التي نادت بها لجنة الأمم المتحدة للقانون التجاري الدولي، إذ عُدّلت وتممت أحكام القانون المدني المتعلقة بالإثبات بموجب القانون رقم: 05-10 المؤرخ في 20 يونيو 2005 أين أضيفت المادتين: 323 مكررو 323 مكرر 1 وعدلت المادة 327.

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".

أما المادة 323 مكرر 1 فنصت: "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".

الفرع الثاني: أهمية الكتابة الإلكترونية وشروطها

إن استلزام الكتابة من الناحية القانونية جاء لما تتميز به من تثبيت للمعلومات والأفكار على دعامة ما لفترة طويلة جدا من الزمن لذا فهي تستلزم توفر عدة شروط.

أولا: أهمية الكتابة الإلكترونية

جاءت الكتابة على رأس أدلة الإثبات لما تتميز به عن باقي الأدلة من الثبوت والاستقرار فلا تخضع للنسيان والتقادم فهي ثابتة بثبات الدعامة المثبتة عليها، بالتالي يؤدي ذلك إلى اعتبار الكتابة هي الأفضل والأسهل لإثبات الالتزام[1].

هذا ما جعل المشرع المصري يتوج الكتابة المرتبة الأولى في وسائل الإثبات فيما يتعلق بالتصرفات القانونية، أما باقي الوسائل من الشهادات والقرائن...فليس لها ذات القوة بل قوتها محدودة[2] نظرا لأهمية الكتابة فقد اشترطت بعض الاتفاقيات الدولية المتعلقة بالتحكيم على ضرورة أن يكون شرط التحكم مكتوبا سواء في عقد اتفاق أو غير ذلك.

[1]- بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة لنيل درجة الدكتوراه، جماعة باتنة، 2014-2015، ص 186.

[2]- مصطفى أحمد إبراهيم نصر، وسائل إثبات العقود الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص 17.

تأكيدا لأهمية الكتابة يلزم عدم قصرها كونه وسيلة وشكل معين أو على مادة معينة وذلك حتى تستوعب كل ما يستجد من وسائل تقنية حديثة ذلك يتحقق بتغيير وتعديل بعض النصوص القانونية كي تستوعب الوسائل الحديثة المستمرة دون توقف.

ثانيا: الشروط الواجب توافرها في الكتابة الإلكترونية

هناك جملة من الشروط التي يجب أن تستجمعها الكتابة حتى يمكن الاعتداد بها قانونا وبالتالي تأدية دورها في الإثبات، وبالرجوع إلى استقراء نص المادة 323 مكرر من التقنين المدني الجزائري وما اشترطه الفقه والقضاء في الكتابة التقليدية والقوانين النموذجية ودليل لجنة الأمم المتحدة للقانون التجاري الدولي يمكن حصر أهم شروط الكتابة الإلكترونية في أن تكون الكتابة (ذات دلالة تعبيرية واضحة ومفهومة موقعة وموثوقة وأخيرا محفوظة ويمكن استرجاعها) [1].

أ. ذات دلالة تعبيرية واضحة ومفهومة

يعني ذلك أن يكون المستند المتضمن الكتابة المراد جعلها ناطقا بما فيه ليتسنى فهمه واستيعابه وإدراك محتواه[2].

هذا الشرط نصت عليه المادة 323 مكرر بقولها: "...ذات معنى مفهوم"، وهو شرط مألوف إلا أن هذا الإشكال لم يكن مطروحا حينما كانت الدعامة ورقية، وذلك لسببين أولهما هو أن هذه الطريقة مألوفة، وثانيها أن الكتابة المستعملة فيها تكتب برسوم وأشكال تقرأ مباشرة ولا تحتاج لوسيط أو نظام أو برنامج معين لقراءتها فيكفي النظر إليها بالعين المجردة لفك معانيها وبالتالي الوصول إلى دلالتها والقول ما إذا كانت متعلقة بمصدر الحق المراد إثباته أم لا، أما اليوم فالأمر اختلف فالدعامة أصبحت الكترونية أي غير مادية، والتدوين عليها أصبح يخضع لقواعد خاصة وكذا الوصول إليها لقراءتها وفهمها.

ب. التوقيع:

جاء في نص المادة 323 مكرر"...بشرط التأكد من هوية الشخص..."، وبالعودة إلى القانون النموذجي للجنة الأمم المتحدة للقانون التجاري الدولي نجده في مادته الثامنة (8) ينص انه إذا استخدمت

[1] – بلقاسم حامدي، مرجع سابق، ص 185.

[2] – حسن عبد الباسط جمعي، إثبات التصرفات التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، 2000، ص 20.

طريقة لتعيين هوية الشخص والتدليل عليه فإن ذلك يعد توقيعا على رسالة البيانات، وعليه فإن شرط التوقيع لازم للاعتداد بحجية الكتابة الإلكترونية في الإثبات.

كما جاء في نص المادة 6 من القانون رقم 15-04 المحدد للقواعد العامة للتوقيع والتصديق الإلكترونيين بنصها "يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع واثبات قبوله مضمون الكتابة في الشكل الإلكتروني"[1].

ج. إمكانية الحفظ والاسترجاع:

بالرجوع إلى نص المادة 323 مكرر نجد أن المشرع الجزائري اشترط أن تكون الكتابة معدة ومحفوظة في ظروف تضمن سلامتها بنصها: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وان تكون معدة ومحفوظة في ظروف تضمن سلامتها".

أما شرط الاسترجاع فهو مرتبط بالشرط السابق ومعناه إمكانية الإطلاع على المعلومات الواردة في رسالة البيانات على نحو يتيح استخدامها عند الحاجة بالرجوع إليها لاحقا بعد إعدادها وحفظها وإرسالها، وهذا بطبيعة الحال يستلزم حفظ النظام أو البرنامج الذي اعتمد في إنشاء وحفظ وتخزين البيانات وذلك لأنه النظام المؤهل لقراءة ما جاء في المحرر الإلكتروني[2].

المطلب الثاني: مبدأ التعادل الوظيفي بين الكتابة التقليدية والكتابة الإلكترونية

للتطرق لهذا المبدأ علينا بتحديد معناه ثم نتائج تطبيق هذا المبدأ وأخيرا ضمان تطبيق المبدأ وعدم المفاضلة العملية بين شكلي المحررات الإلكترونية.

الفرع الأول: عرض مبدأ التعادل الوظيفي بين الكتابة الإلكترونية والورقية

بالرجوع إلى نص المادة 323 مكرر من التقنين المدني نجدها تنص على أنه: "يعتبر الإثبات في الشكل الإلكتروني كالإثبات بالكتابة على الورق..."، ومعنى ذلك أن التشريع لا يفرق بين القوة الثبوتية للكتابة في الشكل التقليدي والكتابة في الشكل الإلكتروني، طالما استطاعت أن تؤدي الوظيفة أو المهمة التي يتطلبها

[1] – جريدة رسمية عدد 06 المتضمن القانون رقم 04/15 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.
[2] – بلقاسم حامدي، مرجع سابق، ص 186.

المشرع وهي تمييز شخص مصدرها وتحديد هويته، وأن يتم تدوينها وحفظها في ظروف تضمن بقائها على حالتها وقت الإصدار دون تغيير أو تحوير[1].

الفرع الثاني: نتائج تطبيق المبدأ

رغم سهولة المبدأ القاضي بعدم المفاضلة بين المحررات الإلكترونية والمحررات التقليدية من حيث المفهوم النظري، إلا انه قد تطرح مسائل عدة في الموضوع وخاصة في ظل تشريعنا الحالي الذي نظم الموضوع بصفة عامة دون تحديد لبعض التفاصيل، ولعل من أهم المسائل التي تطرح: حالة وجود دليل كتابي ورقي وآخر الكتروني لإثبات الواقعة نفسها بأيهما يأخذ القاضي؟

دور القاضي في الترجيح بين أنواع الكتابة:

إن الاعتراف بالكتابة الإلكترونية كطريق من طرائق الإثبات انه قد يثار نزاع مفاده الترجيح بين نوعي الكتابة[2] ومثاله أن متعاقدين تبادلا الإيجاب والقبول عبر وسيط الكتروني وليكن البريد الإلكتروني، ولم يكتفيا بذلك بل قاما بإرسال الإيجاب والقبول عبر البريد العادي، لكن يختلفان مع ما ورد في البريد الإلكتروني، وكل يتمسك بالدليل الذي لصالحه فبأيهما يأخذ القاضي؟

بالنظر في القانون المقارن نجد المشرع الفرنسي قد أورد مادة تخص الموضوع، ونص في الفقرة الثانية من المادة 1316 أنه: "إذا لم يكن هناك نص أو اتفاق بين الأطراف يحدد أسس أخرى، فانه على القاضي مستخدما كل الوسائل أن يفصل في التنازع القائم بين الأدلة الكتابية عن طريق ترجيح السند الأقرب إلى الاحتمال، أيا كانت الدعامة المستخدمة في تدوينه". وهذا النص غير موجود مثله في التقنين الجزائري إلا انه يمكن القول بإعمال المنطق انه للفصل بين تنازع شكلي الكتابة يمكن المرور على الخطوات التالية[3]:

أ-التأكد أولا من مدى توافر شروط المادة 323 مكرر 1:

ويكون بالنظر في مسألة نجاعة التقنية المستخدمة في الكتابة والتوقيع الإلكترونيين، بتحديد ما إذا كان من الممكن التأكد من هوية الشخص الذي أصدرها، وكذا إن كان المحرر قد أعد وحفظ في ظروف تضمن سلامته.

---

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 28.

[2]- ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2007، ص 16.

[3]- كميني خميسة، منصور عزالدين، المرجع نفسه، ص 28.

ب–التأكد من وجود أو عدم وجود اتفاق يرجح شكل كتابة عن الآخر:

فإن اتفق الأطراف على الشكل المراد اعتماده فالمحكمة ملزمة بإتباع إرادة الأطراف كون العقد شريعة المتعاقدين وإن لم يوجد اتفاق وعارض كل واحد من الأطراف عن مضمون الكتابة التي يحتج بها الطرف الآخر، فهنا لابد أن ترجح المحكمة السند الأقرب إلى الاحتمال، دون النظر إلى الدعامة المستخدمة في تدوينه.

ج– ترجيح السّند الأقرب إلى الاحتمال أيا كان وعاؤه:

رغم أن المشرع الجزائري لم ينص صراحة عن ذلك كما فعل نظيره الفرنسي، إلا انه يمكن القول أن القاضي الجزائري في حالة وجود محرر ين احدهما إلكتروني والآخر تقليدي، يرجح الكتابة الأقرب للاحتمال ويستبعد الأخرى، أي أن معيار الأخذ بأحد المحررين ليس الشكل الذي ورد فيه بل مدى اقترابه إلى التصديق في الظروف الوارد فيها[1].

المطلب الثالث: حجية العقود الإلكترونية بين الأطراف وفي مواجهة الغير

بالرجوع إلى التقنين المدني نجد أن المشرع نص على هذه الحجية بموجب المادتين 327 و328، نصت المادة 327 على أنه: "يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه، ما لم ينكر صراحة ما هو منسوب إليه، أما ورثتها وخلفه فلا يطلب منهم الإنكار، ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخطأ والإمضاء أو البصمة هو لمن تلقوا منه هذا الحق، ويعتد بالتوقيع الإلكتروني وفقا لشروط المذكورة في المادة 323 مكرر 1".

ونصت المادة 328 على أنه: "لا يكون العقد (المحرر) العرفي حجة على الغير في تاريخه إلا منذ أن يكون له تاريخ ثابت...". وسوف نتعرض إلى حجية العقود الإلكترونية بين الأطراف (الفرع الأول) وحجيتها ما بين الغير (الفرع الثاني).

الفرع الأول: حجية العقود الإلكترونية بين الأطراف

تطبيقا لمبدأ التعادل الوظيفي بين المحررات الإلكترونية والتقليدية[2] مع مراعاة الخصوصية التي يتمتع بها كل من الشكلين، فإنه يتضح من نص المادة 327 المذكورة أعلاه: أن المحررات العرفية تعتبر دليلا كاملا

[1]– كميني خميسة، منصور عزالدين، مرجع سابق، ص 30.

[2]– المرجع نفسه، ص 42.

وذات حجية مطلقة غير أن هذه الحجية تتعلق بمدى اعتراف الخصم بتوقيعه أوخط يده أو بصمة إصبعه أو إنكاره إياها، أو تصريح الوارث أو الخلف بالعلم أو عدم العلم بما نسب لمن تلقى عنه الحق.

أ. حجية المحرر العرفي من حيث صدوره ممن وقع عليه:

طبق النصوص القانون المدني المتعلقة بالإثبات فالمحرر العرفي لا يكون حجة إلا إذا لم ينكره الشخص المنسوب إليه إنكارا صريحا، أي أنها موقوفة على اعتراف من وقعه بصحة هذا التوقيع وذلك بعدم إنكاره[1]، فإن أُعترِف بها أو أكدت كان المحرر العرفي ذو حجية مطلقة بين أطرافه، لا يجوز إثبات عكس ما ورد فيه إلا بالكتابة، إما أن أنكر من نسب إليه المحرر أو نفى الوارث أو الخلف علمه بذلك قبل مناقشة موضوع المحرر العرفي فهنا يفقد المحرر حجيته مؤقتا في الإثبات إلى غاية الفصل في أمر الإنكار أو الادعاء بالجهالة، ويمكن في كل الأحوال دفع كل ذي مصلحة بأن المحرر المحتج به مزور.

ب. حجية المحرر العرفي من حيث صحة الوقائع الثابتة فيه:

إذا ثبت صدور المحرر العرفي من الشخص المنسوب إليه سواء باعترافه به أو لثبوت ذلك بعد الإنكار، كان للمحرر حجيته من حيث مضمونه، على أن ثبوت نسبة التوقيع للموقع أو الخط له لا يمنع من الطعن في مضمون المحرر نفسه، فمثلا لو كان مضمون المحرر يتعلق بعقد بيع بين شخصين وأن البائع قد قبض الثمن وأن المشتري تسلم المبيع فإن هذه البيانات يفترض جديتها وحقيقتها وأن ذكرها في المحرر قرينة على صحتها، ولصاحب التوقيع أن يثبت صوريتها أو أنه لم يقبض الثمن، لكن لا يجوز إثبات ذلك إلا بالكتابة تطبيقا لقاعدة لا يجوز نقض الكتابة إلا بالكتابة، وفي هذه الحالة لا يكفي الإنكار بل يقع عليه عبء إثبات العكس[2].

الفرع الثاني: حجية المحررات الإلكترونية بالنسبة للغير

المحرر العرفي يعد حجة بما دون فيه ليس على أطرافه وإنما على الغير أيضا، والغير بصفة عامة هو كل شخص لم يكن طرفا في المحرر، ويجوز أن يسري في حق التصرف القانوني الذي تضمنه المحرر ومن ثمة يصح أن يحتج به عليه. على أن هذا المفهوم يضيق فيما يخص تاريخ المحرر، وهو ما سنتعرض له في النقاط التالية:

[1] – محمد حسن قاسم، التعاقد عن بعد، قراءة تحليلية في التجربة الفرنسية، دار الجامعة الجديدة للنشر، 2005، ص 156.

[2] – المرجع نفسه، ص 170.

أ. حجية المحرر العرفي بالنسبة إلى الغير من حيث صدوره ممن وقعه:

يعتبر المحرر العرفي بالنسبة إلى صدوره ونسبته إلى الموقع حجة على الغير، فهو حجة بالنسبة إلى الخلف العام (الوارث والموصي له بجزء من التركة)، والخلف الخاص والدائن، والموقع وحده له أن ينكر نسبة المحرر له[1]، فإن اعترف به أو سكت عنه أصبح حجة عليه وعلى الغير ولا يبقى سبيل أمامهم سوى الطعن فيه بالتزوير، وإذا احتج بالمحرر بعد وفاة صاحب التوقيع فلا يطلب من الوارث أو الخلف إنكار التوقيع بل الحلف يمينا بأنهم لا يعلمون أن الخط أو التوقيع أو البصمة هي لمن تلقى عنه المحرر.

ب. حجية المحرر العرفي بالنسبة إلى الغير من حيث صحة الوقائع الثابتة به:

بثبوت صدور المحرر العرفي من صاحب الخط أ والتوقيع أو البصمة يكون ذا حجية من حيث مضمونه في مواجهة أطراف المحرر وكذا الغير، مع الإشارة إلى أن ثبوت نسبة التوقيع للموقع أو الخط له لا يمنع من الطعن في مضمون المحرر نفسه، ويعامل هنا الغير كأطراف العقد فلهم الدفع بصورية العقد المضمن في المحرر، ولهم الدفع ببطلان العقد لعدم مشروعية المحل أو السبب أو لعدم استفاء الشكل الذي تطلبه القانون، ولهم الدفع بانقضاء الالتزام بالوفاء به، أي أن لهم ما كان للسلف من دفوع[2]، وخلاصة القول أن الوقائع الثابتة بالمحرر العرفي ذات حجية بالنسبة إلى الغير مثلهم في ذلك كمثل أطراف المحرر فيما عدا التاريخ فله شأن آخر.

ج. حجية المحرر العرفي بالنسبة إلى الغير من حيث صحة تاريخه:

رأينا أن المحررات العرفية لها حجية على الناس كافة فيما يتعلق بما تتضمنه من بيانات، بينما لا يعتبر التاريخ الذي تحمله حجة على الغير إلا إذا كان ثابتا طبق النص المادة 328 مدني، فبالنسبة لطرفي المحرر يكون المحرر حجة بكافة البيانات الواردة فيه بما في ذلك تاريخه[3]، أما بالنسبة للغير فإن التاريخ ليس حجة إلا منذ أن يكون ثابتا وذلك حماية للغير من غش يحتمل قيام السلف به بتقديم التاريخ أو تأخيره وهو غش يصعب على الغير إثباته.

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 46.

[2]- عبد الرزاق أحمد الصنهوي، الوسيط في شرح القانون المدني، ج2، منشأة المعارف بالإسكندرية، طبعة 2004، ص 271.

[3]- كميني خميسة، منصور عزالدين، المرجع نفسه، ص 46.

المبحث الثاني: التوقيع الإلكتروني

لقد صاحب التقدم التكنولوجي والتقني ظهور وسائط حديثة يمكن استخدامها في تدوين البيانات ولكن بشكل الكتروني سميت "بالدعامة الإلكترونية" ونظرا لعدم ملائمة التوقيع التقليدي مع الدعامة الإلكترونية، ظهر مؤخرا التوقيع الذي لا يمكن القول انه بديل للتوقيع التقليدي، وإنما جاء ليتلاءم مع طبيعة الدعامة الإلكترونية وسمي بالتوقيع الإلكتروني، الذي ظهرت له تعريفات سواء وطنية أو دولية، بالإضافة إلى ما يتمتع به من خصائص وشروط ووظائف تجعله يتفوق بكثير على التوقيع التقليدي[1].

وهذا ما سوف يتم التطرق إليه من خلال التعرض إلى ماهية التوقيع الإلكتروني من خلال مفهومه القانوني والفقهي بالإضافة إلى صوره ووظائفه وشروطه في (المطلب الأول) ودوره في الإثبات (المطلب الثاني)، والحماية المقررة له في (المطلب الثالث).

المطلب الأول: ماهية التوقيع الإلكتروني

لأن الواقع العملي قد اتجه إلى إدخال طرق ووسائل حديثة في التعامل لا تتفق مع فكرة التوقيع بمفهومها التقليدي وإزاء انتشار نظم المعالجة الإلكترونية للمعلومات التي بدأت تغزو الشركات والإدارات والبنوك، اعتمادا على هذه الآلات، إذ أصبح التوقيع التقليدي يستحيل تكيفه مع النظم الحديثة، فقد تم الاتجاه نحو بديل للتوقيع التقليدي وهو التوقيع الإلكتروني، فما هو مفهومه؟ وما هي ميزاته وشروطه؟ وما هي الوظائف التي يؤديه؟

كل هذه التساؤلات سوف يتم الإجابة عليها على النحو التالي:

الفرع الأول: تعريف التوقيع الإلكتروني

أولا: تعريف التوقيع الإلكتروني تشريعا وفقها

من خلال هذه النقطة نتطرق إلى تعريف التوقيع الإلكتروني من قبل المنظمات الدولية، ثم التشريعات المقارنة وكذا المحاولات الفقهية لتعريفه، وأخيرا موقف المشرع الجزائري وذلك على النحو التالي:

[1]- زينب غريب، إشكالية التوقيع الإلكتروني وحجيته في الإثبات، رسالة لنيل دبلوم الماستر في القانون الخاص، الرباط، 2009-2010، ص 11.

أ. تعريف التوقيع الإلكتروني من قبل المنظمات الدولية:

تطرقت أكثر من منظمة لتعريف التوقيع الإلكتروني من خلال قوانين التجارة الإلكترونية أومن خلال قوانين خاصة بالتوقيع الإلكتروني، ونورد فقط تعريف منظمة الأمم المتحدة عن طريق لجنتها للتجارة الدولية (اليونسترال) والاتحاد الأوروبي كمثال لمنظمة إقليمية[1].

1-**تعريف التوقيع الإلكتروني في قواعد اليونسترال الموحدة بشأن التوقيعات الإلكترونية:** جاء في المادة الثانية من قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية ودليل الاشتراع لسنة 2001 بصدد تعريف المصطلحات أن: "التوقيع الإلكتروني: يعني بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا[2]، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".

2- تعريف التوقيع الإلكتروني في توجيهات الاتحاد الأوروبي: عرضت اللجنة الأوروبية مشروع التوجه الأوروبي حول إطار قانون عام للتوقيع الإلكتروني لمجلس وزراء المجموعة الأوروبية الذي وافق عليه البرلمان الأوروبي في 13 ديسمبر 1999.

وقد عرفت المادة الثانية منه التوقيع الإلكتروني انه: "بيان أو معلومة معالجة الكترونيا، ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى (كرسالة أو محرر)، والتي تصلح وسيلة لتمييز الشخص وتحديد هويته".

ب.تعريف التوقيع الإلكتروني في التشريعات المقارنة:

نتطرق إلى تعريف القانون الفرنسي ثم القانون المصري، وذلك في النقاط التالية:

1- تعريف التوقيع الإلكتروني في التشريع الفرنسي: عرّف المشرّع الفرنسي إثر تعديل وتتميم أحكام الإثبات سنة 2000 التوقيع الإلكتروني في الفقرة الثانية من المادة 4/1316بانه:"التوقيع الذي ينتج عن استخدام أية وسيلة مقبولة موثوق بها لتحديد هوية الموقع وتكفل اتصال التوقيع بالعمل أو المستند المرتبط به"، مع العلم أن الفقرة الأُولى من المادة المذكورة كانت قد عرفت التوقيع بالمعنى العام بنصها:

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 12.

[2]- زينب غريب، مرجع سابق، ص 19.

"التوقيع الذي يحدد شخصية (هوية) من هو منسوب إليه والذي يفصح عن قبوله بمضمون المحرر الذي يرتبط به، وبالالتزامات الواردة فيه"[1].

2- تعريف التوقيع الإلكتروني في التشريع المصري: عرفت المادة الأولى فقرة "أ" من القانون المصري2004/15 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات التوقيع الإلكتروني بأنه: "ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرد، يسمح بتحديد شخص صاحب التوقيع، ويميزه عن غيره"[2].

ج: التعريف الفقهي للتوقيع الإلكتروني:

انقسم الفقه في تعريفه للتوقيع الإلكتروني إلى اتجاهين، اتجاه يركز على كيفية نشوء التوقيع الإلكتروني واتجاه ثان نظر إليها من زاوية الوظائف التي يؤديها التوقيع الإلكتروني، وجمع آخرون بين الاثنين، ومثالها أن التوقيع الإلكتروني هو: "مجموعة من الإجراءات والوسائل التي يتيح استخدامها عن طريق الرموز أو الأرقام إخراج رسالة الكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة الكترونيا يجرى تشفيرها باستخدام خوارزم المفاتيح واحد معلن والآخر خاص بصاحب الرسالة"[3].

وقد عُرِّف أيضا أنه: "مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته"، وعرف انه: "استخدام معادلات خوارزمية متناسقة تتم معالجتها من خلال الحاسب الآلي تنتج شكلا معينا يدل على شخصية صاحب التوقيع"، وعرف أنه: "مجموعة من الرموز أو الأرقام أو الحروف الإلكترونية تدل على شخصية الموقع دون غيره".

وأخيرا يلاحظ من التعريفات السابقة أن الفقه يحاول تعريف التوقيع الإلكتروني من خلال التركيز على كيفية إنشاء التوقيع أو من خلال التركيز على الوظيفة التي يؤديها التوقيع في الحياة العملية تاركا المجال لظهور أنواع جديدة من أشكال التوقيع الإلكتروني مثله مثل التعريفات التشريعية[4].

---

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 15.

[2]- بلقاسم حامدي، مرجع سابق، ص 212.

[3]- علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 30.

[4]- كميني خميسة، منصور عزالدين، المرجع نفسه، ص 17.

بعد تطرقنا إلى مختلف التعريفات التشريعية سواء منها المتعلقة بالمنظمات أو التشريعات الداخلية المقارنة، وكذا بعض التعريفات الفقهية، نرى موقف المشرع الجزائري في النقطة الموالية:

د – موقف المشرع الجزائري فيما يخص تعريف التوقيع الإلكتروني:

تنص المادة 2/327 من التقنين المدني المعدل والمتمم على أنه: "...يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه".

كما نصت المادة 2 من القانون رقم 15-04 المحددة للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على أنه: "التوقيع الإلكتروني بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى تستعمل كوسيلة توثيق".

ومن جهة أخرى لم يخص المشرع التوقيع بشروط منفردة، واكتفى بربطها بالشروط المتعلقة بالكتابة الإلكترونية وكأن التوقيع والكتابة لهما نفس الوظيفة، وتتمثل هذه الشروط في:

أ – إمكانية التأكد من هوية الشخص.

ب– معدة ومحفوظة في ظروف تضمن سلامتها.

واستنادا إلى التعريفات التي أشرنا إليها بمناسبة الكلام عن تعريفات التشريعات المقارنة، يمكن القول أن التشريع الجزائري لم ينص على شيء مهم كشرط لابد من توافره وهو ارتباط التوقيع الإلكتروني بالمحرر ارتباطا منطقيا، وربما أن المشرع اعتبر ذلك شرط بديهي، وخاصة انه نص في المادة 323 مكرر على إمكانية تحديد هوية الشخص الذي أصدر الكتابة، وهو من أهم وظائف التوقيع الإلكتروني، ولا يهم إن كان متصلا بالكتابة الإلكترونية أم لا، بالإضافة أن مسألة الترابط بينهما هي مسألة تقنية يمكن أن المشرع تركها لتقدير قاضي الموضوع.

لكن الشيء الذي سيصعب المهمة أكثر أن المشرع لم ينص صراحة على اشتراط إمكانية اكتشاف أي تعديل أو تغيير حدث بعد وضع التوقيع الإلكتروني كمعيار لمدى نجاعته، ويمكن أن يلجأ هنا أيضا قاضي الموضوع لعبارة "معدة ومحفوظة في ظروف تضمن سلامتها "لاستنباط ما إذا كانت التقنية المستعملة تحقق الأمان الكافي للاعتداد بالتوقيع الإلكتروني أم لا[1].

[1]– كميني خميسة، منصور عزالدين، مرجع سابق، ص 17.

الفرع الثاني: صور التوقيع الكتروني

أوجدت التقنيات الحديثة صورا عديدة من التوقيعات الإلكترونية لمحاولة استيفاء التوقيع الإلكتروني للشروط اللازم توافرها في التوقيع التقليدي وبالتالي اعتماده والاعتداد به قانونا.

هذه الصور هي التوقيع البيومتري الذي يعتمد على الصفات والخصائص الجسدية والسلوكية للشخص، والتوقيع بالقلم الإلكتروني، والتوقيع الكودي أو السري والتوقيع الرقمي الذي يعتمد على التشفير وربطه بمفاتيح خاصة لفك الشفرة.

أولا: التوقيع البيومتري

يتم التوقيع البيومتري بأحد الخواص المميزة لكل شخص[1]، أي استخدام هويته، لذا يطلق عليه التوقيع بالخواص الذاتية، تعتمد هذه الصورة على حقيقة علمية هي أن لكل شخص صفات ذاتية خاصة به تختلف من شخص إلى آخر تتميز بالثبات النسبي، فالصفات الجسدية أو البيومترية التي يعتمد عليها التوقيع البيومتري متعددة من أهمها: البصمة الشخصية، بصمة شبكية العين، بصمة الصوت، بصمة الشفاه، خواص اليد البشرية، التوقيع الشخصي...،يؤخذ على هذا التوقيع أنه بالرغم من دقته والأمان والثقة المتوافرة به إلا أنه ليس بعيدا عن التزوير فيمكن تسجيل بصمة الصوت ثم إعادة بثها، طلاء الشفاه بمادة معينة تجعلها مطابقة للبصمة الأصلية كذلك تزوير بصمة العين بتقليدها عن طريق بعض أنواع العدسات اللاصقة... بل إن هناك إمكانية خضوع الذبذبات الحاملة للصوت أو الصورة للنسخ وإعادة الاستعمال مما يؤدي لافتقادها للأمن والسرية.

ثانيا: التوقيع بالقلم الإلكتروني

التوقيع بالقلم الإلكتروني هو طريقة حديثة من طرق التوقيع البيومتري ويتم هذا التوقيع بقيام الشخص بالتوقيع على شاشة جهاز الحاسب الآلي باستخدام قلم الكتروني خاص، يستوجب جهاز حاسب آليا ذا مواصفات خاصة تمكنه من أداء مهمته في التقاط التوقيع من شاشته.

هذه الصورة يتم حفظ صورة التوقيع الشخص بذاكرة الحاسب الآلي، وعندما يرسل مستند الكتروني موقع بخط يده عن طريق القلم الإلكتروني يتم المضاهاة بين التوقيع المرسل والتوقيع المخزن بذاكرة الحاسب،

[1]- بلقاسم حامدي، مرجع سابق، ص 213.

يتم التحقق من صحة التوقيع بالاستناد إلى حركة القلم الإلكتروني والأشكال التي يتخذها من انحناءات أو التواءات وغير ذلك من سمات خاصة بالتوقيع الخاص بالموقع[1].

ثالثا: التوقيع عن طريق البطاقة المقترنة بالرقم السري (التوقيع الكودي)

غالبا ما يرتبط التوقيع السري بالبطاقات البلاستيكية والبطاقات الممغنطة[2] وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية، ويتم توقيع التعاملات الإلكترونية وفقا لهذه الطريقة باستخدام مجموعة من الأرقام أو الحروف أو كليهما يختارها صاحب التوقيع لتحديد شخصيته ولا تكون معلومة إلا له ولمن يبلغه به، وتسمى هذه الطريقة بالانجليزية اختصارا "PIN"، ينتشر استعمال التوقيع السري أو الكودي في عمليات المصارف والدفع الإلكتروني حيث تحرص البنوك على تنظيم عملية الإثبات بمقتضى اتفاق مع حامل البطاقة في العمل.

رابعا: التوقيع الرقمي

التوقيع الرقمي عبارة عن: "أرقام مطبوعة تسمى"HASH" لمحتوى المعاملة التي يتم التوقيع عليها بالطريقة ذاتها أي باستخدام الأرقام"، يتم الحصول على التوقيع الرقمي عن طريق تحويل المحرر المكتوب والتوقيع الوارد التشفير عليه من نمط الكتابة العادية إلى معادلة رياضية باستخدام مفاتيح سرية وطرق حسابية معقدة "لوغاريتمات".

إن التوقيع الرقمي يحقق أعلى درجات الثقة والأمان لعدة أمور هي[3]:

- باستخدام التوقيع الرقمي يتحقق الارتباط بين المستند الكتابي والتوقيع الوارد عليه.
- يضمن عدم إمكان التدخل في مضمون التوقيع أو مضمون المحرر الذي يرتبط به.
- يؤدي إلى التحقق من هوية الموقع، وأن الرسالة الموقعة منه تنسب إليه، فلا يمكن للموقع إنكار أن المستند الموقع منه لا ينسب إليه، ويرجع ذلك إلى الارتباط التام بين المفتاح العام والخاص.
- يعبر بطريقة واضحة عن إرادة صاحبه للالتزام بالتصرف القانوني وقبوله لمضمونه، بذلك فهو يحقق كافة الشروط التي يتطلبها القانون في المحرر لكي يصلح أن يكون دليلا كتابيا كاملا.

---

[1]- بلقاسم حامدي، مرجع سابق، ص 214.

[2]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 21.

[3]- بلقاسم حامدي، المرجع نفسه، ص 215.

- يضاف إلى ما سبق أن التوقيع الرقمي يحقق سرية المعلومات التي تتضمنها المحررات الإلكترونية حيث لا يمكن قراءة تلك المحررات إلا ممن أرسلت إليه وباستخدام المفتاح العام للمرسل.

- لضمان الأمان في عملية التشفير الخاصة بالتوقيع الإلكتروني فقد وجدت الحاجة إلى طرف ثالث في عملية التجارة الإلكترونية يكون محل ثقة طرفي العقد والذي يتمثل في هيئة مختصة يكون لها سلطة توثيق التوقيع الإلكتروني، لذا يتم تسجيل التوقيع الرقمي لدى جهات متخصصة في إصداره بناءً على طلب العملاء[1].

- يجب عدم الخلط بين أمرين هما: تشفير التوقيع وتشفير الرسالة، فإذا كانا يتفقان على أنه يمكن تشفيرهما إلا أن الفارق هو أن تشفير الرسالة الإلكترونية يشملها بأكملها بما في ذلك التوقيع.

خلاصة القول هي أن هذه الصور تتباين فيما بينها من حيث درجة الثقة وذلك بحسب الإجراءات المتعبة في إصدارها وتأمينها والتقنيات التي تتيحها ولا شك أن هذه التقنيات في تطور مستمر يضمن الحفاظ على الحقوق.

الفرع الثالث: وظائف التوقيع الإلكتروني وشروطه

بعد أن تطرقنا إلى مفهوم التوقيع الإلكتروني والتعريف التشريعي والفقهي له ولاحظنا أن الكثير من التشريعات عرفت التوقيع من خلال الوظائف التي يؤديها، لذا نلخص الوظائف فيما يلي:

أولا: وظائف التوقيع الإلكتروني

أ. تحديد شخصية أو هوية الشخص الموقع:

وهو الشخص الملتزم بالتوقيع وهذا من أساسيات التوقيع إذ أن الغاية من التوقيع هو نسبة ما ورد في المحرر أو السند للشخص الموقع. وإن معظم الفقه يرى أن التواقيع الإلكترونية يتم بواسطتها تحديد هوية الموقع، إذا ما روعيت وسائل الأمان المتبعة كما أن التوقيع يستطيع تأدية هذه الوظيفة باختلاف نوع التواقيع الإلكترونية المستخدمة[2].

[1]- ثروت عبد الحميد، التوقيع الإلكتروني، مكتبة الجلاء الجديدة بالمنصورة، 2001، ص 63.

[2]- زينب غريب، مرجع سابق، ص 217.

كما أشار المشرع الجزائري إلى سلطات التصديق الإلكتروني في الفصل الثاني من الباب الثالث من القانون رقم 15-04، ولقد عرف المشرع الجزائري الموقع في المادة 3 مكرر بأنه: "شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله ويضع موضع التنفيذ جهاز إنشاء التوقيع الإلكتروني".

كما عرف المشرع الجزائري في نفس المادة مصطلح الشهادة الإلكترونية بأنها: "وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع" ويعني بها التحقق من هوية الشخص الموقع من خلال الشهادة الإلكترونية.

ب. التعبير عن إرادة الشخص الموقع مضمون السند (المحرر):

فالتوقيع الإلكتروني الموثق والمؤمن والصادر وفق الضوابط الفنية والتقنية قرينة على أن الشخص الموقع قد وافق على مضمون المحرر الإلكتروني والبيانات الواردة فيه[1] ما لم يثبت خلاف لذلك، بالتالي فإن التوقيع الإلكتروني له وظيفة هامة في التعبير عن إرادة الشخص الموقع بالالتزام والقبول بما ورد في المحرر الإلكتروني وأن قيام الشخص الموقع بالتوقيع الإلكتروني على المحرر متى كان التوقيع موثقا ومؤمنا حسب الأصول يعتبر أداة للتعبير عن رضا الشخص الموقع بما ورد في المحرر الإلكتروني.

كما نصت المادة 6 من القانون 15-04 المذكور أعلاه على أن:" يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع واثبات قبوله مضمون الكتابة في الشكل الإلكتروني"، فالتوقيع الإلكتروني باستخدام إحدى صور التوقيع الإلكتروني المشار إليها سلفا يعني أنه يؤدي الوظيفة ذاتها التي يؤديها التوقيع التقليدي وهي التعبير عن رضا الموقع بما ورد في السند.

ج. **إثبات سلامة العقد:**

لا يقصد بذلك أن التوقيع يضفي الحجية على سلامة العقد وصحته وحجيته، إنما قرينة تقبل إثبات العكس على سلامة محتوى العقد وصحته وعدم المساس بمضمونه أو العبث به، إذ أنه حتى لو ثبتت سلامة العقد من خلال استخدام التوقيع الإلكتروني المؤمن والمشفر والذي يضمن عدم العبث بمحتوى العقد فإن من الممكن إثبات عدم حجية المحرر الإلكتروني أو بطلانه.

[1]- بلقاسم حامدي، مرجع سابق، ص 217.

في الأخير يمكن القول أن التوقيع الإلكتروني يستطيع أن يؤدي دوره في الإثبات خاصة أن وسائل الأمان في مجال العقود الإلكترونية مهمة صعبة وشاقة[1].

ثانيا: شروط التوقيع الإلكتروني

حتى يكون للتوقيع الإلكتروني أثر قانوني فيجب توافر بعض الشروط التي تضمن قيامه بالدور المنوط بالتوقيع بصفة عامة، وبالتالي فإذا لم تتوافر في التوقيع الإلكتروني هذه الشروط فإنه لا يكون له أثر قانوني في الإثبات، إن الشروط الواجب توافرها في التوقيع الإلكتروني نصت عليها كل القوانين التي نظمت حجية التوقيع الإلكتروني في الإثبات[2].

فقانون اليونسترال النموذجي للتوقيع الإلكتروني والصادر عام 2001 فقد أورد شروطا فوفقا للمادة 1/6 منه يشترط للاحتجاج بالتوقيع الإلكتروني أن يكون موثوقا به، وقد أوضحت المادة 3/6 من ذات القانون أن التوقيع يكون موثوقا به إذا توافرت به أربعة شروط وهي[3]:

- أن تكون بيانات إنشاء التوقيع الإلكتروني مرتبطة بالشخص الموقع.
- أن تكون بيانات إنشاء التوقيع الإلكتروني خاضعة لسيطرة الشخص الموقع.
- إمكان اكتشاف أي تغيير في التوقيع الإلكتروني.
- أن يكون الغرض من التوقيع تأكيد سلامة المعلومات التي يتعلق بها وإمكان اكتشاف أي تغيير يجري بتلك المعلومات بعد التوقيع عليها.

كما أقر التوجيه الأوربي اتفاقات الإثبات التي بموجبها يتفق أطرافها على شروط قبول التوقيعات الإلكترونية في الإثبات[4]، وقد أوضحت المادة 2/2 الشروط التي يتعين توافرها في التوقيع المعزز وهي:

- أن يرتبط فقط بالشخص الموقع.
- أن يسمح بتحديد شخصية أو هوية الشخص الموقع.

---

[1]- ضياء أمين مشيمش، التوقيع الإلكتروني، دراسة مقارنة، المنشورات الحقوقية، 2003، ص 155.

[2]- بلقاسم حامدين مرجع سابق، ص 218.

[3]- إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، 2008، ص 278.

[4]- المرجع نفسه، ص 281.

- أن يتم بوسائل يستطيع الشخص الموقع من خلالها الاحتفاظ به والسيطرة عليه بشكل حصري.
- أن يرتبط ببيانات تخرجه في شكل يسمح بإمكانية كشف كل تعديلات لاحقة على هذه البيانات.

أما المشرع الجزائري فقد اعتمد التوقيع الإلكتروني لأول مرة في نص المادة 2/327 من القانون المدني المعدلة بالقانون 10/05والتي تنص على: "...يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر..." وذلك من أجل إضفاء الحجية على المحررات الإلكترونية بصفة عامة والتوقيع الإلكتروني بصفة خاصة حتى يمكن الاعتداد به في الإثبات، وسوف نتطرق في هذا المجال إلى نقطتين للتحدث على هذه الشروط:

أ. التوقيع الإلكتروني الأمن:

نصت عليه المادة 2/1 من المرسوم الفرنسي رقم 272 لسنة 2001 على المقصود بالتوقيع الإلكتروني الآمن الذي يطلق عليه التوجيه الأوروبي مصطلح التوقيع الإلكتروني المتقدم بأنه: "التوقيع الإلكتروني الذي يحقق الشروط الآتية:

- أن يكون خاصًا بالشخص الموقع.
- أن يتم إنشاؤه بوسائل تقع تحت سيطرة الشخص الموقع وحده.
- أن يرتبط بالمحرر ارتباطا وثيقا بحيث أن كل تعديل في المحرر أو السند بعد ذلك يتم اكتشافه".

أما المشرع الجزائري فقد أورد الشروط الواجب توافرها في التوقيع الإلكتروني المؤمن في المادة 3 مكرر بقوله أن: التوقيع الإلكتروني المؤمن: "هو توقيع الكتروني يفي بالمتطلبات الآتية:

- أن يكون خاصا بالموقع.
- أن يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية.
- أن يضمن مع الفعل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه".

وقد نصت المادة 7 من القانون رقم 15-04 المذكور أنفا على المتطلبات التي يجب توافرها في التوقيع الإلكتروني الموصوف بنصها: "التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوافر فيه المتطلبات الآتية:

1. أن ينشا على أساس شهادة تصديق الكتروني موصوفة.

2. أن يرتبط بالموقع دون سواه.

3. أن يمكن من تحديد هوية الموقع.

4. أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

5. أن يكون منشأ بواسطة تكون تحت التحكم الحصري للموقع.

6. أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات".

ب. **أداة إنشاء التوقيع الإلكتروني الآمنة:**

أورد المشرع الجزائري تعريفا لأداة إنشاء التوقيع الإلكتروني المؤمن وسماها بجهاز مأمون لإنشاء توقيع الكتروني في المادة 3 مكرر فعرفه بأنه: "جهاز إنشاء توقيع الكتروني يفي بالمتطلبات المحددة" فاستعمل المشرع عبارة المتطلبات المحددة يعني الشروط التي تتعلق بحماية البيانات والمعطيات لإنشاء التوقيع، لكنه لم يحصر هذه الشروط حتى تتماشى والتكنولوجيات المستجدة[1].

الشروط التي تطلبها المرسوم والتوجيه الأوروبي هي أربعة، الثلاثة الشروط الأولى منها تتعلق بالوسائل التقنية لحماية معطيات إنشاء التوقيع، والشرط الأخير يهدف إلى أن يتضمن أداة إنشاء التوقيع ألا تكون عائقًا على أن يعلم الموقع علما تاما بمضمون المحرر قبل التوقيع عليه، وأن لا تؤدي أداة التوقيع لتغيير في المحرر الموقع.

الشروط الثلاثة التي تتعلق بحماية معطيات إنشاء التوقيع هي:

- لا يمكن أن يتم إنشاء بيانات التوقيع أكثر من مرة وأن تكون سريتها مكفولة.
- أن لا يمكن استنباط بيانات التوقيع أو تقليدها.
- أن يتم حماية بيانات التوقيع بواسطة الشخص الموقع ضد أي استعمال من لغير.

[1]- بلقاسم حامدي مرجع سابق، ص 220.

أما الشرط الرابع هو أن لا تؤدي أداة إنشاء التوقيع إلى حدوث أي تغيير في مضمون المحرر الموقع وأن لا تكون هذه الأداة عائقا في إمكانية معرفة الشخص الموقع التامة بمضمون المحرر قبل أن يقوم بالتوقيع عليه[1].

كما نص الفصل الثاني من- الباب الثاني من القانون 15-04 المذكور أعلاه عن آليات إنشاء التوقيع الإلكتروني الموصوف والتحقق منه في المواد 10-11-12-13-14.

كل هذه الشروط السابقة تهدف إلى أن يكون التوقيع الإلكتروني نظيرا وظيفيا للتوقيع التقليدي حتى يمكن للتوقيع الإلكتروني أن يتمتع بالحجية ويتمتع بنفس الآثار القانونية(2).

ج. شهادة التصديق المعتمدة:

إن الشرط الثالث من شروط تمتع التوقيع الإلكتروني بالحجية هو أن يتم التحقق من هوية الشخص الموقع من خلال شهادة تصديق الكتروني معتمدة، وقد تطلب هذا الشرط تقريبًا في جل القوانين المهتمة بهذا الأمر.

نصت المادة 15 من التوجيه الأوروبي على أن التوقيع الإلكتروني الذي يتمتع بحجية مساوية لحجية التوقيع الخطي من أحد شروطه أن يكون مبينا على شهادة تصديق معتمدة[2].

أما بخصوص القانون الجزائري فقد نصت المادة 3 مكرر من المرسوم 162/07 والشهادة الإلكترونية الموصوفة وأعطت كلا المصطلحين تعريفًا: فالشهادة الإلكترونية هي: "وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع". وأما الشهادة الإلكترونية الموصوفة هي":شهادة الكترونية تستجيب للمتطلبات المحددة".

كما أشارت المادة 15 في الباب الثالث – الفصل الأول في المادة 15 منه من القانون رقم 15-04 المذكور أعلاه عن شهادة التصديق الإلكتروني الموصوفة بنصها: " شهادة التصديق الإلكتروني الموصوفة هي شهادة تصديق الكتروني تتوفر فيها المتطلبات الآتية:

1. أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق الكتروني، طبقا لسياسة التصديق الإلكتروني الموافق عليها.

[1]- بلقاسم حامدي مرجع سابق، ص 220.

[2]- المرجع نفسه، 221.

2. أن تمنح للموقع دون سواه.

3. يجب أن تتضمن على الخصوص:

أ- إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق الكتروني موصوفة.

ب- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني وكذا البلد الذي يقيم فيه.

ج-اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته.

د- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني.

ه- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني.

و- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني.

ز- رمز تعريف شهادة التصديق الإلكتروني.

ح-التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني.

ط-حدود استعمال شهادة التصديق الإلكتروني عند الاقتضاء.

ي-حدود قيمة المعاملات التي قد تستعمل من اجلها شهادة التصديق الإلكتروني عند الاقتضاء.

ك-الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر عند الاقتضاء.

المطلب الثاني: دور التوقيع الإلكتروني في الإثبات ونطاق حجيته

قد يبدو لأول وهلة أن التوقيع الإلكتروني يعجز عن أداء الوظائف المنوطة بالتوقيع التقليدي، أي تحديد هوية الشخص الموقع والتعبير عن رضائه بمضمون المحرر ويرجع ذلك إلى الوسيلة التي يتم بها، فالتوقيع الإلكتروني[1] لكونه منفصلا عن شخصية صاحبه ووجوده ضمن المحرر على وسيط الكتروني لا يحقق نفس

[1]- بلقاسم حامدي مرجع سابق، ص 221.

ضمانات التوقيع التقليدي، إذ يمكن للقراصنة اختراق أنظمة المعلومات والتقاط صورة التوقيع أوفك شفرته ثم استخدامه بدون علم صاحبه، وكذا ظهور حالات عديدة لتزوير بطاقات الائتمان.

بالإضافة إلى الفيروسات التي تهدد بإتلاف الملفات المحفوظة مما يؤدي إلى اضطراب التعامل. كل ذلك يدعو إلى التشكيك في التوقيع الإلكتروني وفي أدائه لدوره مما يعرقل في إعطائه قيمته القانونية. لهذا الغرض سنقسم هذا المطلب إلى فرعين كالآتي:

الفرع الأول: دور التوقيع الإلكتروني

التوقيع بصفة عامة عنصر أساسي لحجية الدليل المعد للإثبات، فالمحرر دون توقيع ليس له حجية ملزمة للقاضي وبوجه عام يمكن القول أن التوقيع له ثلاثة أدوار رئيسية وهي:

أولا: أن التوقيع وسيلة لتحديد هوية الشخص الموقع

مفاد ذلك، أن التوقيع يمكن من تحديد شخصية الموقع وتمييزه عن غيره، كما يتيح تحديد سلطة الشخص الموقع للتوقيع، فالشخص الموقع قد يكون هو الطرف الأصيل في التعاقد وقد لا يكون كذلك كما لو كان وكيلا أو وليا أو وصيا على القاصر أو ممثلا عن الشخص المعنوي، ففي جميع هذه الحالات يجب على الشخص الموقع أن يحدد هويته كما يوضح سلطته في التوقيع.

ثانيا: أن التوقيع تعبير عن رضاء الشخص الموقع بمضمون المحرر

فعندما يضع الشخص الموقع توقيعه على المحرر فهو يعبر عن التزامه بمضمون المحرر وإقراره له[1]، وقد جرت العادة على وضع التوقيع في آخر المحرر، حتى يكون منسجا على جميع البيانات الواردة بالمحرر وآمنا بعدم الإضافة به بعد التوقيع دون علم الشخص الموقع.

ثالثا: أن التوقيع دليل على الحضور الجسدي للشخص الموقع

التوقيع بالإمضاء دليل على الحضور الجسدي لصاحبه وإقراره لما ورد بالمحرر، هناك مسألة أخرى تتصل بالحضور الشخصي للموقع وهي مسألة تحديد أهلية الشخص الموقع، إذ أن الحضور الشخصي لطرفي

[1]- سعيد السيد قنديل، التوقيع الإلكتروني ماهيته صوره حجيته في الإثبات، دار الجامعة الجدية، 2004، ص 50.

العقد من التحقق من أهلية كل طرف للتعاقد، وهذا الأمر غير متوفر بالعقد الإلكتروني بالتالي تتواجد احتمالية أن يكون أحد أطراف التعاقد غير ذي أهلية[1].

الفرع الثاني: نطاق حجية التوقيع الإلكتروني

إن معظم التشريعات التي أولت اهتماما كبيرا بالتوقيع الإلكتروني، ولم تعارض استخداماته في المعاملات الإلكترونية بين الأشخاص في جميع المستويات جعلت له حجية تتماشى وتحقيق الأثر القانوني المراد من التوقيع.

يمكن القول أن القانون النموذجي جاء لوضع الأسس والقواعد العامة التي تحكم التوقيع الإلكتروني في جميع المجالات المعلوماتية (تجارية، إدارية، مدنية...) حيث نص في المادة الأولى منه والمعنونة ب: "نطاق الانطباق" على ما يلي: "ينطبق هذا القانون حيثما يستخدم توقيعا الكترونيًا في سياق أنشطة تجارية وهو لا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلكين"[2].

وبالرجوع إلى التوجيه الأوروبي نجده يحد العلاقة العقدية بين المورد أو المهني في مجال البيع أو أداء الخدمات، كما تضمن التوجيه الأوروبي حماية المستهلك وبذلك فإن نطاق تطبيق التوقيع الإلكتروني وحجيته تكون في المعاملات الإلكترونية التي تهدف إلى حماية المستهلك، مع العلم أن عبارة "مستهلك" تستخدم في المجال الاقتصادي بوجه عام والتجاري بوجه خاص، ما يفيد أن نطاق تطبيق التوجيه الأوروبي في بدايته كان في الأنشطة التجارية، إلا أنه سرعان ما أصبح مرجعا أساسيا للدول الأعضاء التطبيقية في شتى المجالات التي تستلزم إدراج التوقيع الإلكتروني لإثبات المبادلات الإلكترونية بوجه عام.

ويعتبر المشرع الفرنسي الذي تأثر بالتوجيه الأوروبي وكان لزاما عليه تعديل النصوص القانونية المتعلقة بقواعد الإثبات تأثرا، إذ صدر المرسوم رقم 2001-741 المنظم للتعاقد عن بعد، وكان التعرض لذلك بوجه عام أي في نطاق المعاملات جميعها (التجارية، المدنية والإدارية) وسرعان ما تدخل المشرع الفرنسي بإدراج نصوص المرسوم في تقنين الاستهلاك الفرنسي[3].

بينما المشرع الجزائري فقد اعتد بالتوقيع الإلكتروني في نطاق جميع المعاملات، ذلك أنه أخذ بمبدأ التكافؤ الوظيفي بين الإثبات التقليدي والإثبات الإلكتروني، وباعتبار أن نص المادة 327 من القانون المدني

[1]- زينب غريب، مرجع سابق، ص 43.

[2]- بلقاسم حامدي مرجع سابق، ص 223.

[3]- شحاتة غريب شلقاني، التعاقد الإلكتروني في التشريعات العربية، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2008، ص 20.

هي التي جاءت بالمبدأ، وبحكم أن القانون المدني هو الشريعة العامة، فإنه لا خلاف في قبول استعمال التوقيع الإلكتروني في نطاق المعاملات بشتى أنواعها.

وكنتيجة فإن نطاق حجية التوقيع الإلكتروني يكون في شتى المعاملات المدنية والتجارية والإدارية، ما لم يتعارض مع وجود أحكام خاصة تقيد ذلك، وبحسب الشروط التي يوليها المشرع اهتماما وتركيزا من أجل ضبط تلك الحجية.

المطلب الثالث: الحماية القانونية للتوقيع الإلكتروني

إن حماية التوقيع الإلكتروني هو مطلب جميع المتعاملين بواسطة الوسائط الإلكترونية، ذلك أن كل طرف متعاقد الكترونيا يسعى من خلال معاملاته تلك أن ترتب جميع آثارها القانونية في مواجهة الأطراف الأخرى وكذا في مواجهة الغير، كما أن جميع الدول التي عالجت منظومة التوقيع الإلكتروني في تشريعاتها اقتداء بالمجهودات الدولية في ذلك أصبح متطلبها الأساسي والجوهري هو البحث عن حماية حقيقية للتوقيع الإلكتروني[1].

الفرع الأول: ضوابط حماية التوقيع الإلكتروني

لم تضع التشريعات سواء الأجنبية أو العربية ضوابط معينة من أجل حماية التوقيع الإلكتروني ولعل السبب في ذلك هو كون الضوابط مرتبطة باستمرار مع التقنية القائمة، إلا أن من التشريعات التي ذكرت بعض الضوابط الأساسية والمرتبطة بنشاط الموقع طالب الحماية لتوقيعه، وهو الشيء الذي سوف يدعونا للتطرق الى تلك الضوابط مع مقارنة مدى الأخذ بها من طرف التشريعات[2].

أولا: اتخاذ احتياطات ضبط منظومة التوقيع الإلكتروني

يقصد بهذه الشروط ضرورة توافر ضوابط ومواصفات معينة تتعلق بكيفية حصول التوقيع الإلكتروني – الخاص بصاحب التوقيع– حتى يمكن الحفاظ على مصداقيته لدى الطرف الآخر الذي سيوقع له على وثائق الكترونية تكون حجة في الإثبات فيما بعد، ولذلك يمكن الحصول على التوقيع الإلكتروني بإتباع خطوات محددة وهي:

1. اللجوء إلى جهة مختصة ومرخص لها بإصدار الشهادات التي تتعلق بالتوقيع الإلكتروني.

[1]– بلقاسم حامدي مرجع سابق، ص 226.

[2]– المرجع نفسه، ص 227.

2. يتم ذلك مقابل مالي سنويا، لقاء مراجعة الأوراق وإصدار منظومة التوقيع ثم التصديق على الشهادة.

3. تصدر شهادة التوقيع الإلكتروني ومعها المفتاح العام والخاص للمستخدم الجديد[1].

4. يقوم صاحب التوقيع بإرسال رسالته الإلكترونية، وتشفير الرسالة باستخدام المفتاح العام والخاص وتكون كذلك موقعة بتوقيعه الإلكتروني.

5. يقوم المستقبل للرسالة –وحسب برنامج خاص– بإرسال نسخة من التوقيع الإلكتروني إلى الهيئة التي أصدرت شهادة التوقيع وذلك للتأكد من صحة التوقيع وأنه مطابق أم لا.

6. تقوم أجهزة الحاسب الآلي المتخصصة – لدى هيئة التصديق– بمراجعة قاعدة البيانات الخاصة بها والتصديق على صحة التوقيع، ثم تعاد النتيجة والمعلومات الخاصة بالشهادة إلى الأجهزة لدى الهيئة مرة أخرى.

7. تقوم هيئة التصديق بإرسال المعلومات والنتيجة إلى المستقبل مرة أخرى وذلك حتى يتأكد من صحة وسلامة رسالة المستقبل وذلك عن طريق استخدام مفتاحه الخاص إن كان التشفير قد تم بطرق المفتاح العام، أو بواسطة الرقم العام للمرسل ويجيب المرسل إليه على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية.

كل هذه الخطوات وإن كانت ليست بصيغة مباشرة، اعتمدها المشرع الجزائري بحيث أشار الى تعريف بعض المصطلحات بشكل عام وجعلها مرتبة بترتيب ينطبق على الخطوات المذكورة سابًقا.

هذه المصطلحات مدرجة ضمن المادة 3 مكرر والتي هي:

1. التوقيع الإلكتروني المؤمن.
2. الموقع.
3. معطيات إنشاء توقيع الكتروني
4. جهاز مأمون لإنشاء توقيع الكتروني.
5. معطيات فحص التوقيع الإلكتروني.

[1]– بلقاسم حامدي مرجع سابق، ص 227.

6. جهات فحص التوقيع الإلكتروني.

7. الشهادة الإلكترونية.

8. الشهادة الإلكترونية الموصوفة.

9. مؤدي خدمات التصديق الإلكتروني.

10. أهلية مؤدي خدمات التصديق الإلكتروني.

بالإضافة للشروط الفنية التي يتعين إرفاقها بطلب الترخيص بصدور منظومة التوقيع الإلكتروني، فإن هناك شروط[1] أخرى يلزم بها صاحب التوقيع الإلكتروني المزمع إصداره والذي يتولى بعد ذلك إبرام الصفقات ضمن منظومة التجارة الإلكترونية ومن هذه الشروط:

1. اتفاق أطراف العقد على الوسائل الفنية التي تسهل عملية الاتصال بينهما عبر شبكة الانترنيت.

2. شروط أمان تتعلق بضمان سلامة التعامل بين أطراف العقد الإلكتروني، وذلك كتحديد نوع الرسالة التي يمكن اعتمادها في العلاقات التجارية المتبادلة بينهما.

3. يجب على التاجر الإلكتروني أن يحتفظ بأرشيف الكتروني ضمن ملف خاص داخل الحاسب الآلي الخاص به.

وتفصيل ذلك أن القوانين التقليدية تلزم التاجر بأن يحتفظ بدفاتره التجارية لمدة زمنية معينة وتعاقبه جزائيًا على عدم الاحتفاظ بهذه السجلات، فقواعد غرفة التجارة الدولية تحبذ هذا التصرف، كما أن القانون النموذجي أشار إلى ضرورة حفظ الوثيقة الإلكترونية بمعرفة شخص ثالث، وكما فعل أيضا المشرع الجزائري الذي أشار إلى ضرورة الاحتفاظ بأرشيف الكتروني في تعريفه للتوقيع الإلكتروني المؤمن في المادة 3 مكرر من نفس المرسوم

ثانيا: إعلام جهة التصديق بالاستعمالات غير المشروعة للتوقيع الإلكتروني

من شروط التوقيع الإلكتروني أن يفصح صاحب التوقيع لمزود خدمة التصديق أو ما يسمى بمؤدي خدمات التصديق الإلكتروني حسب المشرع الجزائري (وهي الجهة التي تصدر الشهادة الرقمية بصحة

[1]- بلقاسم حامدي مرجع سابق، ص 228.

توقيعه الإلكتروني) وبأي استعمال غير مشروع لهذا التوقيع الذي صدر عنه، والسبب في ذلك أن مؤدي خدمات التصديق الإلكتروني يعطي شهادة رقمية للطرف الآخر في المعاملة مفادها أن التوقيع المراد بها صحيح، الأمر الذي يرتب آثارا تضمن حق الطرف الأخير، ولذلك لو تم استعمال هذا التوقيع بطريقة غير مشروعة وصادق مؤدي خدمات التصديق الإلكتروني على ذلك لا اعتبر شريكا في المسؤولية الجزائية – متى كان يعلم بذلك الاستعمال غير المشروع– فضلا عن مسؤوليته المدنية في حالة العلم[1].

إن قانون اليونيسترال بشأن التوقيع الإلكتروني لم يضع الضوابط المتعلقة بالحماية في مواجهة إحدى الأطراف دون الطرف الآخر بل جعل المسؤولية في تجاوز تلك الضوابط لكل بحسب خروجه عن السلوك الواجب قانونا.

أما المشرع الجزائري عندما أشار في تعريفه لمؤدي خدمات التصديق الإلكتروني في مفهوم المادة 8/8 من القانون رقم 2000-03 المؤرخ في 05 أوت 2000بأنه: "كل شخص في يسلم شهادات الكترونية او يقدم خدمات أخرى في مجال التوقيع الإلكتروني".

وكما أشار أيضا عندما عرف أهلية مؤدي خدمات التصديق الإلكتروني بأنه: "...يقدم خدمات مطابقة لمتطلبات نوعية خاصة". لم يحدد الضوابط بشكل مباشر بل تستنتج من خلال عبارتي: (يقدم خدمات أخرى في مجال التوقيع الإلكتروني) و(يقدم خدمات مطابقة لمتطلبات نوعية خاصة) لأن مؤدي خدمات التصديق الإلكتروني ملزم بالتحري لدقة التوقيع الإلكتروني وبأنها مطابقة بفعل ضوابط معينة قبل إصدار شهادة البيانات الرقمية الخاصة بالتوقيع الإلكتروني.

كما نصت المادة 12 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على أن: مؤدي خدمات التصديق الإلكتروني "شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوف، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني...".

جل التشريعات تضع مسؤولية الحفاظ على محتوى العقد الإلكتروني الموقع، وتلزم كل طرف له علاقة سواء مباشرة أو غير مباشرة به، فهو سلوك لابد منه، فغالبا ما يقع على ثلاث أطراف رئيسية وهي:

[1]- بلقاسم حامدي مرجع سابق، ص 229.

أ- سلوك الموقع:

لقد ألزم المشرع في قانون اليونيسترال النموذجي بشأن التوقيعات الإلكترونية الموقع بأن يمارس عناية معقولة لاجتناب أي استخدام البيانات إنشاء توقيعه استخداما غير مأذون به[1]، كما أن المشرع أكد على أن إخلال الموقع عن الوفاء بما سبق ذكره يرتب تحمل هذا الأخير التبعات القانونية.

أما المشرع الجزائري فقد عرف الموقع بأنه: "شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله ويضع موضع التنفيذ جهاز إنشاء التوقيع الإلكتروني"

يستفاد من هذا التعريف أن الموقع إذا عمل بخلاف ذلك مثل عدم الوفاء وعدم الالتزام بما هو مدون في المحرر الذي وقعه ترتب عليه تحمل التبعات القانونية[2].

كما عرفت الموقع المادة 2/2 من القانون 15-04 المذكور أعلاه على أن "الموقع شخص طبيعي يحوز على بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله".

ب- سلوك مقدم خدمات التصديق:

لقد أوجب المشرع في قانون اليونيسترال النموذجي بشأن التوقيع الإلكتروني بأن يوفر مقدم خدمات التصديق خدمات لتأييد التوقيع الإلكتروني وإعطائه مفعولا قانونيا بصفته توقيعا، وأن من بين التزاماته أن يتصرف وفقا للتأكيدات التي يقدمها وأن يمارس العناية لضمان دقة واكتمال مقاصده الجوهرية ذات الصلة بالشهادة طيلة فترة سريانها، وأكد على أن إخلال مقدم خدمات التصديق[3] عن الوفاء بما سلف ذكره يرتب تحمل هذا الأخير تبعات قانونية.

في حين أشار المشرع الجزائري لسلوك مقدم خدمات التصديق الإلكتروني بعبارة "...يقدم خدمات مطابقة لمتطلبات نوعية خاصة"، أي بأن يلتزم بتصرفاته وفقا لما تمليه عليه مهنته وإلا فسيترتب عليه تحمل التبعات القانونية، وهذا ما شارت إليه مواد الفرع الثاني من الفصل الثالث للقانون رقم 15-04.

[1]- المادة 8 من قانون اليونستيرال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

[2]- بلقاسم حامدي، مرجع سابق، ص 223.

[3]- المرجع نفسه، ص 229.

ج- سلوك الطرف المعول:

المشرع في قانون اليونيسترال أوجب على الطرف المعول اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني كما ألزمه باتخاذ خطوات معقولة إذا ما كان التوقيع مؤيدا بشهادة.

يعتبر ضابط إعلام جهة التصديق بالاستعمالات غير المشروعة للتوقيع الإلكتروني من بين الضوابط القانونية والعملية التي يحتاجها كل تشريع في الدول التي أخذت بمنظومة التوقيع، ذلك أن عدم إعلام جهة التصديق بالاستعمال غير المشروع يعتبر تأكيدا ورضا من صاحب التوقيع على سلامة المعاملة الإلكترونية المبرمة وبذلك يتحمل جميع الآثار المترتبة عن تلك المعاملة[1].

ثالثا: صدق المعطيات المقدمة لجهة التصديق

حينما حدد قانون اليونيسترال سلوك الموقع في المادة 8 فإنه أراد أن يحدد الالتزامات التي على عاتق الموقع وفق مفاهيم عامة ومن بين هذه الالتزامات: استخدام الوسائل التي يوفرها له مقدم خدمة التصديق، وبذل جهده لأن يقدم كلما يؤكد صدق المعطيات المقدمة لجهة التصديق.

وهو ما أراده المشرع الجزائري كذلك من وراء تعريفه للموقع، وهو صدق المعلومات، أي أن يكون التوقيع الحاصل وغير المشروع ليس لحسابه الخاص أو ليس لحساب الشخص الطبيعي أو المعنوي الذي يمثله، وأنه لم يوضع موضع تنفيذ جهاز إنشاء التوقيع الإلكتروني، بالتالي له الحق في استعمال جميع طرق الإثبات ليثبت صدق المعطيات التي يقدمها لمؤدي خدمات التصديق الإلكتروني[2].

وبذلك يمكن القول أن صدق المعطيات المقدمة لجهة التصديق يرتب تواجد منظومة التوقيع الإلكتروني سليمةً ومرتبة لجميع آثارها القانونية حين استخدامها من طرف الأشخاص ذوي الصلة.

رابعا: حق التعويض في حالة المخالفة

إن الحق في التعويض جراء الإخلال بالالتزام المترتب في ذمة صاحبه هو حق يستأثر به كل متضرر من ذلك الإخلال، وفي إطار المسؤولية العقدية فإن الموقع الذي يدلي لجهة التصديق بمعلومات غير صحيحة أو يخل بما ترتب في ذمته من التزامات قانونية يكون ملزما بالتعويض عن الضرر اللاحق وربما الأمر في هذا الشأن وفي منظومة التوقيع الإلكتروني لا يحتاج إلى نصوص تقر ذلك الحق لأنه في الأصل مكرس في القواعد

[1]- بلقاسم حامدي، مرجع سابق، ص 230.

[2]- المرجع نفسه، ص 230.

العامة لكافة التشريعات الوطنية للدول، غير أننا وعند ذكرنا لبعض التشريعات التي أقرت الحق في التعويض فإن ذلك لا يعني عدم أحقية المتضرر في التعويض إذا ما لم تقره القوانين الخاصة المتعلقة بمنظومة التوقيع بل أن ذلك الحق محفوظ بموجب القواعد العامة في إطار المسؤولية العقدية.

فبالرجوع إلى قانون اليونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 فإنه حدد تبعات سلوك الموقع وسلوك مقدم خدمات التصديق الإلكتروني في حالة إخلال كل طرف بالالتزامات الملقاة على عاتقه والذي يفهم أيضا من خلال عرض المشرع الجزائري لمفهوم ما يقصد بالموقع ومؤدي خدمات التوقيع الإلكتروني واهلية مؤدي خدمات التوقيع الإلكتروني على أن كل من الموقع ومؤدي (مقدم) خدمات التوقيع الإلكتروني يتحمل التبعات القانونية لتخلفه عن الوفاء بالاشتراطات أو بالتزاماته، ولقد ترك تحديد التبعية القانونية للنصوص القانونية في إطارها المدني أو الجزائي[1]، لذا الموقع يتوجب عليه اتخاذ الاحتياطات اللازمة لمنع الاستعمال غير المشروع لعناصر التشفير أو المعلومات الشخصية التي تتعلق بتوقيعه والتزامه بالإعلام عن أي استعمال غير مشروع لبيانات إمضاءه وكذا تحري الصدق في كافة البيانات التي يدلي لمزود خدمة المصادقة الإلكترونية.

كما أن لمزود الخدمة مسؤولية إذا تسبب بخطئه في ضرر للغير الذي وثق بحسن نيته في الضمانات المقدمة، وأنه قد يتحمل مسؤوليته في إطار المسؤولية التقصيرية إذا ما كان هناك وجود علاقة بين الخطأ والضرر بموجب رابطة السببية.

وقد تم التطرق إلى مسؤولية مؤدي خدمات التصديق الإلكتروني وصاحب شهادة التصديق الإلكتروني في القسم الثاني في الفصل الثالث من الباب الثالث من القانون 15-04 المذكور آنفا.

تبقى أن الضوابط في جملتها عادة ما ترتبط بجوانب تقنية لها آثار قانونية إذا ما نص عليها المشرع كون تلك الضوابط تضمن في النصوص التشريعية الالتزامات على عاتق الأطراف المشاركين المتدخلين في منظومة التوقيع الإلكتروني وفي عالم المبادلات الإلكترونية.

[1]- بلقاسم حامدي، مرجع سابق، ص 231.

الفرع الثاني: أنماط حماية التوقيع الإلكتروني

إن حماية منظومة التوقيع الإلكتروني لها جانبين احدهما تقني والآخر قانوني.

أولا: الحماية القانونية

أما الحماية القانونية فهي مرتبطة بأنماط وأشكال الحماية، هذه الأخيرة التي نسقيها من حامل المسؤولية في حد ذاته والتي أقرها المشرع من أجل وضع حصانة للتوقيع الإلكتروني بما يضمن عدم المساس به، ومن ثم جعله جديرًا بالثقة والأمان، وأن يتم تحقيق ثلاثي أبعاد العلاقة الإلكترونية وهي: السرعة ، الثقة، والائتمان[1].

تتعدد أنماط الحماية بحسب ما أقرته التشريعات وتدارسه الفقه إلى حماية مدنية، تجارية، وأخرى جزائية (والتي سوف نتناولها في الفصل الثاني).

بناءً على ذلك فإنه يتم التعرض إلى أنماط الحماية بحسب نمط المسؤولية وأساسها فيما يلي:

أ. الحماية المدنية للتوقيع الإلكتروني:

لقد نصت جل التشريعات على الحماية المدنية لأي تصرف خارج عن الأطر القانونية بناءً على إحدى أسس المسؤولية إما عقدية أو تقصيرية، غير أن المتمعن في مفهوم الحماية يجد أنها تتماشى وفق طرح زمني، أي حماية لاحقة وأخرى سابقة.

1- الحماية السابقة: إن الحماية كمفهوم عام[2] يرتبط أكثر بالإجراءات والتقنيات والوسائل المتوفرة التي تستهدف وضع حصانة للتوقيع الإلكتروني كمنظومة قائمة بذاتها ، فالحماية أساسها في جميع المستويات تحدد وتضبط الوسائل الكفيلة بالحفاظ على التوقيع الإلكتروني في شكله واستمراريته وترتيبه للآثار والاعتداد في ذاته وفي مضمون المحرر الموقع، ويمكن القول بأن الحماية السابقة لا تتطلب خطأ قائما رتب الضرر، إنما يكفي أن تكون هناك إخلال بالتزام لم يرتب ضرار بعد، من هنا فإن الضرر محتمل الوقوع وليس واقعا.

---

[1]- بلقاسم حامدي، مرجع سابق، ص 231.

[2]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 33.

المشرع الجزائري أشار للمتطلبات التي من شأنها ضمان التوقيع الإلكتروني المؤمن أن من بينها عبارة":يضمن مع الفعل المرتبط به، صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه" فهذه العبارة سابقة ومشترطة لوقوع التوقيع أي أنها تسبق التوقيع وأثرها يأتي بعد عملية التوقيع الإلكتروني، فالمشرع هنا لم يحدد التبعة القانونية لتخلف الموقع بالاشتراطات ولكن وضع الاشتراط لتوقع الإخلال بالشرط، فهذا الأخير الذي يرتب التبعة القانونية، بالتالي يكون المشرع قد حمل الموقع مسؤولية عقدية إن عمل بالاشتراط ويحمله مسؤولية تقصيرية إن أهمل الاشتراط.

2- الحماية اللاحقة: إن مناط هذه الحماية هو جبر الضرر الحاصل نتيجة الخطأ المرتكب من طرف المتدخل في منظومة التوقيع الإلكتروني بأي صورة من الصور، وتعتبر مرجعية الحماية اللاحقة هي المسؤولية، هذه الأخيرة التي تقوم بمجرد توافر الخطأ والضرر والعلاقة السببية.

كما تعتبر المسؤولية المدنية التي تستهدف جبر الضرر أهم مرجع للحماية، غير أن القائلين بعدم وجود حماية لاحقة لا مبرر لهم إذا ما تم اعتمادهم عن مصطلح الحماية فبحسب ذلك أن جبر الضرر إحدى نتائج الحماية كون أن أساس الحماية اللاحقة في هذا الشأن هو عدم ترتيب منظومة التوقيع الإلكتروني المعتدى عليها لأثارها اتجاه أطراف التعاقد، وهي حماية للموقع من الالتزامات الواقعة على عاتقه بموجب العلاقة العقدية التي تم كسرها والدخول إليه[1].

ب.الحماية التجارية للتوقيع الإلكتروني:

إن مبدأ التعويض أو جبر الضرر كما هو معلوم نصت عليه جميع التشريعات في دول العالم في الشريعة العامة، بذلك فإن مناط الحماية التجارية في أصله يعود إلى الحماية المدنية التي سلف وأن تطرقنا إليها[2].

إن في دراستنا للحماية التجارية يكون من خلال تطبيق بعض القواعد الخاصة التي تتضمنها التشريعات عند ممارسة عمل تجاري أو بمناسبة نشاط تجاري أو بحكم طبيعة العلاقة إذا كانت تجارية. يمكن التطرق إلى الحماية التجارية من خلال بعض المبادئ نذكر منها:

1- طبيعة الأشخاص المتعاقدة: إن العلاقة العقدية الإلكترونية في مجال النشاطات التجارية إما أن تكون بين التجار فيما بينهم بأن تكون بين التاجر كأحد الأعوان الاقتصاديين وعون اقتصادي آخر أو بين

[1]- بلقاسم حامدي، مرجع سابق، ص 232.

[2]- المرجع نفسه، ص 232.

تاجر ومستهلك، وقد عنيت معظم التشريعات التي أقرت بحماية المستهلك اهتمام كبيرا بالمستهلك، إذ صدر في التشريع الفرنسي المرسوم رقم 741-2001 والذي ينظم التعاقد عن بعد اين تم ادخال النصوص القانونية الواردة في هذا المرسوم في تقنين الاستهلاك الفرنسي رقم 949-93 الصادر في 26 جويلية 1996 ، كما أن التوجيه الأوروبي الصادر في 20 ماي 1997 أكد في مادته 2 على حماية المستهلك في إبرام العقد وتنفيذه لاسيما في الالتزام بإعلام المستهلك والالتزام بالمطابقة وكذا أكد التوجيه على حماية المستهلك من الاعتداء على بطاقة الدفع المستخدمة من طرفه.

فطبيعة الشخص المتعاقد تحدد طبيعة الحماية الواجبة، فالمستهلك بصفته هذه فقد خصه المشرع بحماية خاصة بإدراجه نصوصًا خاصة كما أن المشرع فيض له الجمعيات التي تهدف إلى حماية المستهلك والتي تنشط في كافة دول العالم[1].

2- طبيعة العلاقة: إن المستهلك في علاقته مع العون الاقتصادي يهدف إلى تحقيق إشباع حاجاته بأسس الطرق وبأبخس الأثمان، ربحا للوقت والأموال غير أن ذلك يجعل من طبيعة العلاقة تحدد مدى توافر تلك الحماية من عدمها، فالعمل التجاري بحسب الشكل يجعل من المستهلك يمارس العمل التجاري وله ضمانات الإثبات فيما لحقه من ضرر في مواجهة التاجر أو العون الاقتصادي، كما أن العمل التجاري بحسب الموضوع يوفر للمستهلك نفس الضمانات، غير أن العمل التجاري بالتبعية يوفر الضمانات لاسيما في الإثبات لأطراف العلاقة العقدية أي التجار وفقا لتوافر شروط اعتباره فطبيعة العلاقة وكذا طبيعة الأشخاص توفر حماية للمستهلك من حيث الإثبات للعلاقة العقدية أو نفيها، وكذا مرجعية تقييم التعويض.

3- مرجعية التعويض: إن مرجعية التعويض في الاعتداء على منظومة التوقيع الإلكتروني تركز على جانبين هما: ما فات من كسب وما لحق من خسارة، فالعون الاقتصادي إذا ما لحقه ضرر من جراء: سواء إخلال المتعامل معه الكترونيا كالبنوك الإلكترونية أو نتيجة اختراق وكسر سرية بيانات التوقيع، فإن تقديم التعويض وأساسه يكون بناء على المعطيات المعاملاتية التجارية التي يبرمها في ذات الظروف الزمنية والمكانية، كما يؤخذ بعين الاعتبار ما فاته من كسب عن ذلك إضافة إلى ما لحقه من ضرر وفقا للقواعد العامة.

[1]- شحاتة غريب شلقاني، مرجع سابق، ص 19.

بذلك فإن مرجعية التعويض في الحماية التجارية تجمع بين تعويض الضرر وفقا للقواعد العامة في الشريعة العامة (جبر الضرر) وبين التعويض عن خصوصية العلاقة التي تمتاز بالسرعة والثقة والائتمان (ما فاته من كسب)

ثانيا: الحماية التقنية

حاول أهل العلم في مجال المعلوماتية تطوير الأنظمة والوسائل المستعملة في إصدار وتخزين ونقل المحررات الإلكترونية ومن أهمها في الوقت الحالي نجد نظام التشفير والبصمة الإلكترونية، بالإضافة إلى ما اشترطته التشريعات التي اعتمدت أنظمة التوقيع الإلكتروني من إجراءات لابد من اتباعها وتتمثل في أنظمة المصادقة وإصدار شهادات بذلك[1].

أ. نظام التشفير

في الوقت الراهن أصبحت تقنيات تشفير الرسائل الإلكترونية في مقدمة الوسائل الحديثة في مجال توفير الأمن وسلامة وسرية المعلومات والمعاملات المتبادلة عن بعد عبر الانترنت. ولا تقتصر هذه التقنيات على أداء وظائف حماية البيانات فقط بل يمتد دورها إلى المساهمة في تدعيم وسيلة الإثبات الإلكتروني من خلال تحديد هوية مرسل المحرر والموافقة على مضمونه وتوقيع ذوي الشأن إلكترونيًا والتأكد من سلامته[2].

1- ماهية التشفير: نظرا لأهمية التشفير في مجال المعلومات الإلكترونية، اهتم المشرع الفرنسي بتعريف خدمات التشفير المادة 1/28 من القانون رقم 90-1170الصادر في 29 ديسمبر 1990 بشان تنظيم الاتصالات عن بعد بأنها: أي خدمات تهدف إلى تحويل معلومات أو رموز واضحة إلى معلومات أو رموز غير مفهومة بالنسبة للغير وذلك عن طريق اتفاقات سرية أو تنفيذ عكس هذه العملية بفضل وسائل مادية أو برامج مخصصة بهذا الغرض".

في ذات الاتجاه يشير قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية إلى أن التشفير هو: "فرع الرياضيات التطبيقية الذي يعني بتحويل الرسالة إلى أشكال تبدو غير مفهومة ثم إعادتها إلى أشكالها الأصلية"[3].

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 33.

[2]- طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، لبنان، طبعة 1، 2001، ص 19.

[3]- بلقاسم حامدي، مرجع سابق، ص 239.

أما قانون التوقيع الإلكتروني المصري فلقد جاء خاليا من الإشارة لتحديد المقصود بالتشفير، إلا أن اللائحة التنفيذية للقانون المذكور قد عالجت ذلك الأمر حيث أوردت في المادة 9/1 تعريف للتشفير الإلكتروني بأنه "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة."

يتضح من التعريفات السابقة، أنها تركز على عملية تحويل البيانات من حالتها المقروءة إلى صيغة رقمية غير مفهومة للغير، من هنا يمكن القول بوجه عام، إن فكرة نظام التشفير تقوم على إخفاء المعلومات عليها معتمدًا على عملية رياضية أو معادلات خوارزمية يتم تحويل النص المراد تحويله إلى رموز وإشارات لا يمكن فهمها باستخدام التشفير، ويستفاد مما تقدم أن عملية التشفير تتألف من ثلاثة عناصر مترابطة[1] وهي:

1. المعلومات التي سيتم تشفيرها.
2. خوارزمية التشفير التي ستطبق على المعلومات، وخوارزمية فك التشفير التي تعيدها إلى حالتها الأصلية.
3. المفاتيح وهي سلسلة أو أكثر من الرموز تستند إلى صيغ رياضية معقدة في شكل خوارزميات.

2- أهداف التشفير: يمكن القول بوجه عام أن هدف التشفير يتمثل في تحقيق عدد من مظاهر أمن المعلومات وهي:

- **سرية البيانات:** وذلك بالاحتفاظ بالمعلومات في صيغة مخفية من أي شخص.

- **التوثيق:** حيث تعمل من ناحية على تحديد هوية الأطراف، أما ما يخص المعلومات المستلمة فينبغي أن تطابق المعلومات الأصلية المرسلة.

- **عدم الإنكار:** بتدخل طرف ثالث موثوق به (مقدم خدمات التصديق) يكفل التحقق من صحة التوقيعات وسلامة المعاملة.

[1]- بلقاسم حامدي، مرجع سابق، ص 293.

مما سبق يوفر استخدام تقنيات التشفير أعلى قدر ممكن من الأمن والحماية لمستخدمي الانترنت، وأصبحت تقنية التشفير من الدعائم الأساسية للتعاملات الإلكترونية مما أدى إلى اكتساب الأخيرة لثقة المستهلك وحازت على اطمئنانه كنوع جديد من التعاملات المالية[1].

3- طرق التشفير: نحاول في ما يلي بيان طرق أو أنظمة التشفير في إيجاز من خلال التعرض لنظامي: التشفير المتماثل والتشفير غير المتماثل وذلك على النحو التالي:

أولا: التشفير المتماثل: يعد هذا النوع من أنواع التشفير المستخدمة[2]، ففيه يستخدم كل من المرسل والمستقبل المفتاح السري ذاته في تشفير الرسالة وفك تشفيرها، ويتفق الطرفان في البداية (حال إنشاء المفتاح) على كلمة المرور التي سيتم استخدامها، ويمكن أن تحوي هذه الكلمة حروفا، أرقاما أو رموزا وعقب ذلك تحول برمجيات التشفير كلمة المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها، ويشمل العدد الثنائي مفتاح تشفير الرسالة، ويعتمد مفهوم التشفير المتمثل على معيار(DES) الذي اعتمدته البنوك لتشغيل آلات الصرف الآلي (ATM).

ويكمن ضعف هذا النوع من التشفير في تبادل المفتاح السري نفسه بين الأطراف دون أمان وهو ما أدى إلى تراجع استخدام هذا النوع من التشفير لعدم تلبيته لرغبات وطموحات المتعاقدين في تأمين المعاملات بصورة مرضية.

ثانيا: التشفير اللامتماثل: جاء هذا النوع من التشفير[3] لتجنب مشكلة التبادل غير الآمن للمفاتيح في التشفير المتماثل، فهو استخدام مفتاح واحد، يستخدم التشفير اللامتماثل زوجًا من المفاتيح تربط بينهما علاقة رياضية أحدهما مفتاح خاص، والثاني مفتاح عام، وقد اصطلح على تسمية هذا النظام ب:" نظام التشفير بالمفتاح العام" وقد يشار إليه بصفة عامة ب:" تقنية شفرة المفتاح العام.

[1]- بلقاسم حامدي، مرجع سابق، ص 240.

[2]- زينب غريب، مرجع سابق، ص 12.

[3]- المرجع نفسه، ص 14.

ب.البصمة الإلكترونية:

ظهرت البصمة الإلكترونية بمناسبة ظهور التوقيع الإلكتروني وبوجه التحديد التوقيع الرقمي وهي نوع من أنواع التشفير وتسمى التشفير باتجاه واحد فتؤخذ الرسالة المراد تشفيرها وتحور للحصول على ما يسمى المفتاح الشفرة (Hash Key) الأصلية منه، ولهذا السَّبب سمي هذا الأسلوب بأسلوب التشفير باتجاه واحد، وهو يستخدم في الأنظمة التي تحتاج فيها للتحقق من صحة معلومات ما دون الحاجة لمعرفة فحوى هذه المعلومات، وذلك لأن تشفير نفس الرسالة بنفس الخوارزمية ينتج مفتاح الشفرة نفسه في كل مرة.

فهو يستخدم للتحقق من عدم التلاعب ببيانات أو ملفات معينة، فمثلا إذا حصلنا على بيانات من أحدهم فإن هنالك احتمالا بأن هذه البيانات قد تم التلاعب بها عمدا أو أنها أصيبت بفيروس ما، أوانها حدث بها تغيير غير متعمد أثناء تنزيلها من الإنترنت بسبب عطل ما في الاتصال، فنحن بحاجة هنا لطريقة ما نتأكد فيها من تطابق نسخة البيانات التي لدينا مع البيانات الأصلية.

وعليه فالبصمة الإلكترونية أو التشفير باتجاه واحد يستخدم في التوقيع الرقمي للتأكد من صحة البيانات المنقولة عن طريق وسيط الكتروني[1].

ج. توثيق المستندات الإلكترونية:

من أهم عقبات التعاقد[2] في مجال التجارة الإلكترونية هي إمكانية التنصل من الالتزامات والدفع بتزوير المحررات الإلكترونية، وإنكار التوقيعات الصادرة بين المتعاملين في الانترنت أو عبر الشبكات عموما والادعاء أن التوقيع غير مطابق لهوية الموقع، مما أدى إلى اعتماد وسيط أو طرف ثالث لحل مشكلة تحديد الهوية في الشبكات الإلكترونية وهي سلطات المصادقة ووسيلة عملها هي إصدار شهادات التصديق الإلكترونية. ونوضحها على النحو التالي:

1- سلطات المصادقة: وهي جهات توثيق الكترونية، حكومية أم خاصة مهمتها: توثيق المستندات الإلكترونية وإصدار المفاتيح واعتماد أنظمة التشفير، وتحديد هوية المتعاملين في الانترنت وتحديد مدى أهليتهم للتعاقد وأهم ما في الأمر أنه يناط لها مهمة إصدار التوقيعات الإلكترونية، وشهادات التوقيع الإلكترونية لنسبة التوقيع للموقع والترخيص بإصدارها لهيئات تعمل تحت إشرافها، وفي سبيل ذلك تمسك هيئات التوثيق الإلكتروني سجلات الكترونية يتم فيها قيد التوقيعات الإلكترونية وما هو قائم ، وما أبطل

[1]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 34.

[2]- محمد أمين الرومي، المستند الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2007، ص 166.

أو ألغي، أو عدل منها، وعلى سبيل المثال قد أوجد التشريع التونسي سنة 2004 الوكالة الوطنية للمصادقة الإلكترونية وأعطاها صبغة إدارية ومتعها بالشخصية المعنوية، ومن أهم صلاحياتها الإشراف على جميع الجهات العاملة في مجال التوثيق، ومن مهامها الأصيلة: تحديد مواصفات منظومة إحداث الإمضاء وإبرام اتفاقيات الاعتراف المتبادل مع الأطراف الأجنبية، وكذا إصدار وتسليم وحفظ شهادات المصادقة الإلكترونية الخاصة للأعوان العموميين المؤهلين للقيام بالمبادلات الإلكترونية ويمكن أن يتم ذلك مباشرة أو عبر مزودي خدمات مصادقة الكترونية عموميين، وقد اعتمدت مصر نفس النظام سنة 2004 بإنشائها هيئة تنمية صناعة تكنولوجيا المعلومات[1] التابعة لوزير الاتصالات وتكنولوجيا المعلومات.

وعليه فهذه السلطات تمثل ضمانة ومرجعية يمكن اللجوء إليها للتأكد من صحة ورودها من الموقع، وكذا استرجاع المحرر فيما بعد، بالإضافة أنها تعتبر كخبير في المجال مما يسهل عمل السلطة القضائية حين طرح إشكالية صحة الكتابة الإلكترونية من جهة ومدى ورودها من الموقع بإثبات السيطرة الفعلية للموقع على منظومة التوقيع أثناء توقيع المحرر فهي تضمن أمن المعاملات[2].

وقد نص المشرع الجزائري على سلطات التصديق الإلكتروني في الباب الثالث في الفصل الثاني من القانون رقم 15-04 المذكور أعلاه.

2- شهادة التصديق الإلكترونية: وتسمى كذلك شهادة التوثيق[3] وهي سجل الكتروني معلوماتي صادر عن سلطة توثيق معتمدة تحتوي على معلومات الشخص الذي يحملها والجهة المصدرة، وتاريخ صلاحيتها، والمفتاح العام للشخص، وهي بمثابة الهوية التي يصدرها شخص محايد للتعرف عن الشخص الذي يحملها وتصادق على توقيعه الإلكتروني خلال فترة معينة وتصادق كذلك على المعاملات التي يجريها عبر الشبكات المفتوحة كالانترنت فهي سجل موقع من قبل سلطة التعريف توفر تأكيدا مستقلا حول الصفات المميزة للشخص الذي قدمها والذي يستخدم توقيع الكتروني، وعليه فهي تحدد السلطة التي أصدرتها وتحدد بالتدقيق هوية صاحب الشهادة وفيها معلومات حول المفتاح العام، وكذا بدء سريان الشهادة ونهاية استخدامها.

[1]- محمد أمين الرومي، مرجع سابق، ص 166.

[2]- كميني خميسة، منصور عزالدين، مرجع سابق، ص 35.

[3]- المرجع نفسه، ص 35.

وعليه للتأكد من أن التوقيع الإلكتروني صحيح لابد أن يصدر التوقيع خلال فترة سريان الشهادة، وأن تكون الشهادة معتمدة من طرف سلطة مرخص لها بإصدارها، وهي أساسا سلطة المصادقة أو إحدى الهيئات التي رخصت لها هذه الأخيرة بإصدار هذه الشهادات، وقد نص المشرع الجزائري على سلطات التصديق الإلكتروني في الباب الثالث من الفصل الثاني من القانون رقم 15-04 المذكور آنفا.

الفصل الثاني

الحماية الجنائية للعقد المبرم عبر الانترنت

نظرا لتعدد الجرائم الواقعة على شبكة المعلوماتية مثل السرقة والنصب والتزوير وخيانة الأمانة وكذا الإتلاف العمدي لشاشات الحاسوب والبرامج الموجودة عليه، وكذا الاعتداءات العمدية على سير نظام المعالجة الآلية للمعطيات وسلامتها داخل النظام فقد عنت مختلف التشريعات في قوانينها الجزائية بتجريم كافة الاعتداءات التي تقع على النظم المعلوماتية وما تحتويه من بيانات لحماية جميع التصرفات التي تبرم على مواقع الشبكة العنكبوتية. فكيف تطورت الحماية الجنائية لهذه النظم وكيف يتم تجسيدها؟ فسنتعرض لتطور الحماية الجنائية على الصعيد الدولي وتجريم الدول للاعتداء غير المشروع لمواقع التعاقد عبر الانترنت في المبحث الأول، وفي المبحث العقوبات المقررة لكل جريمة ونطاق تطبيقها.

المبحث الأول: تطور الحماية الجنائية وتجريم الاعتداء غير المشروع لمواقع التعاقد

لقد قامت جميع دول العالم بتطوير تشريعاتها خاصة تلك المتعلقة بالحماية الجنائية للنظام المعلوماتي وخاصة عندما أصبح الاعتداء عليه يشكل خطرا على خصوصية الأشخاص ولعل أول الدول الرائدة في هذا المجال والتي بدأت تندد بخطورة هذه الجريمة هي الولايات المتحدة الأمريكية وتبعتها بعض الدول الأخرى والتي قامت بتجريم هذا الاعتداء في جميع صوره سواء كان هذا التعدي في صورة الدخول أو البقاء غير المشروع فيه أو أي تدمير لنظام المعالجة الآلية من محو للبيانات وتعليمات البرنامج أو إعاقة عمله، فسنتعرض لتطور الحماية الجنائية على الصعيد الدولي في المطلب الأول وتجريم الاعتداء على مواقع التعاقد في المطلب الثاني، وجريمة التلاعب ببيانات نظام معالجة المعلومات في المطلب الثالث.

المطلب الأول: تطور الحماية الجنائية

إن الطابع الدولي الذي تكتسيه الجرائم المطبقة على النظام المعلوماتي بصفتها بجرائم عالمية أدى بكل دولة على سن قوانين جنائية لمكافحة جرائم التعدي على النظام، خاصة تلك المتعلقة بالعقود المبرمة عبر الانترنت والتي أصبحت تربط بين أطراف المعمورة كلها، فاختصرت المسافات والحواجز المكانية الزمانية.

الفرع الأول: تطور الحماية الجنائية على الصعيد الدولي

تعد **الولايات المتحدة الأمريكية** من أوائل الدول التي انتهت لهذه المشكلات وحاولت علاجها من خلال سن التشريعات ابتداء بقانون تقرير الأشخاص عام 1970 وقانون سياسة الاتصالات السلكية واللاسلكية في 10 أكتوبر 1984[1].

[1]- بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2016، ص 69.

حيث أصدر الكونغرس الأمريكي، قانونا يسمى بالتحايل المعلوماتي، وفي سنة 1985، تم إصدار قانون الغش والتعسف الذي تناول الجرائم الخاصة على الأنظمة المعلوماتية للحكومة الفيدرالية، وقانون سرية المخابرات الإلكترونية في 8 فيفري 1996. ناهيك عن قانون الاتصالات الذي تضمن نصوصا خاصة تهدف إلى تقييد حرية القصر في الدخول للمواقع الإلكترونية قصد الإطلاع على الصور والأفلام المخلة بالآداب العامة المنتشرة على شبكة الانترنيت كما قامت هيئة الأمم المتحدة بمجهودات طائلة في هذا المجال حيث كانت الانطلاقة من المؤتمر السابع المنعقد في ميلانو 1985 والتي أشارت إلى مسألة الخصوصية واختراقها للبيانات الشخصية واعتماد ضمانات لحماية سريتها وفي سنة 1990 انعقد مؤتمر هافانا[1] والذي جاء بمجموعة من المبادئ ومنها:

- تحديد القوانين الجنائية الوطنية.
- تطوير أمن الحاسب الآلي.
- اعتماد إجراءات تمنع كافة الموظفين والوكالات المسؤولة بمنع الجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
- تلقين آداب الكمبيوتر كجزء من مفردات الاتصال والمعلومات.
- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم. واحدث هذه التشريعات هو قانون التوقيع الإلكتروني الصادر سنة 2000، أما اتفاقية الأمم المتحدة لنفس السنة فتنص على مكافحة سوء استعمال تكنولوجيا المعلومات لأغراض إجرامية فقد أكدت على ضرورة تعزيز التعاون والتنسيق بين الدول[2]، كما عقدت الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية أيام 17-19 أفريل 2010 بالبرازيل حيث ناقشت فيه الدول الأعضاء الجريمة

الحاسوبية وكذا استخدام المجرمين وسائل العلم والتكنولوجيا في جرائمهم وهذا تأكيدا لخطورتها والتحديات التي تطرحها، أضف إلى ذلك المؤتمرات التي عقدتها بعض الأطراف أيام 18-22 أكتوبر 2010 بفيينا لمكافحة الجريمة المنظمة واستعمال تكنولوجيا المعلومات لأغراض إجرامية وكذا السلطات المختصة بمكافحة الجرائم الحاسوبية[3].

[1]- د.شيماء عبد الغني محمد عطا الله الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الأزاريطة 2007، ص114.

[2]- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2013، ص93.

[3]- صغير يوسف، المرجع نفسه، ص95.

أما على مستوى الاتحاد الأوربي:

تعد **فرنسا** من بين الدول التي تنبهت لهذه المشكلة ، فحاولت علاجها من خلال تشريعاتها وكان ذلك ابتداء من 6 جانفي 1978، إذ **أصدرت** قانون المعلومات والحقوق الشخصية ليعقبه صدور مرسوم في 25 /1981/12 يوحد بعض المخالفات المرتبطة بمجال المعلوماتية لمد سلطان قانون العقوبات لحماية المال المعلوماتي فقام وزير العدل سنة 1985 باقتراح قانون تحت عنوان الجرائم في المادة المعلوماتية لكن هذه المحاولة باءت بالفشل آنذاك وفي سنة 1986 تقدم النائب Godfrain jacques مع نواب آخرون إلى الجمعية الوطنية باقتراح مشروع عن قانون الغش المعلوماتي وذلك من خلال تعديل بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف والإخفاء وكذلك العدوان على المال المعلوماتي[1]. لتصدر في عام 1988 قانون لحماية نظم المعالجات الآلية للبيانات، كما أصدرت قانونا جديدا عدل بعض أحكام قانون 1988 وذلك في سنة 1994، حيث أدمج هذا القانون في قانون العقوبات الفرنسي .

وقد قامت بعض الدول الأخرى بتعديل قانونها الجنائي مثل **فنلندا** والتي قامت بتعديل القوانين الخاصة بها فأصبح للقاضي الحق في إصدار أوامر لمراقبة اتصالات الحاسوب الآلي وتسجيلها والتعامل معها أما **هولندا** فقد أعطت للقاضي حق التصنت على الشبكات و**اليابان** قامت بسن قوانينها لتستوعب المستجدات الإجرامية المتعلقة بجرائم الانترنت[2].

وكذلك **المجر** و**بولندا** أما **كندا** فقامت بتعديل قانونها الجنائي سنة 1985 ليشمل جرائم الحاسب الآلي والانترنت وكذا تحديد العقوبات المطبقة على المخالفات الحاسوبية وجرائم التدمير والدخول غير المشروع على المعاملات الإلكترونية ووضح القانون صلاحيات جهات التحقيق وخول للمأمور حق تفتيش أنظمة الحاسوب الآلي والتعامل معها وضبطها وذلك بعد حصوله على أمر قضائي. ومن بين الاتفاقيات الدولية في هذا المجال هي:

اتفاقية بودابست المنبثقة عن اتفاقيات المجلس الأوربي والتي شهدت الميلاد في 23 نوفمبر 2001 لمكافحة جرائم الانترنت والتي أصبحت تهدد الأشخاص والممتلكات[3] كما تهدف هذه الاتفاقية إلى التعاون والتضامن الدولي لمحاربة هذه الجريمة ومحاولة الحد منها فقامت بتحديد الحد الأدنى المشترك بين هذه الجرائم وإمكانية استكمال القائمة في القوانين الداخلية كما يأخذ بعين الاعتبار الممارسات غير المشروعة والأكثر

[1] – أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة ابن عكنون، الجزائر، دفعة 2003، ص38

[2] – بعرة سعيدة، مرجع سابق، ص70.

[3] - صغير يوسف، مرجع سابق، ص 99.

حداثة لا سيما تلك المرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد وقد صنفت الاتفاقية الجرائم في خمسة عناوين في القسم الأول منها حيث بدأت بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم ثم الانتهاكات الممارسة بواسطة الحاسوب الآلي ولقد وضعت مجموعة من الشروط لكي تأخذ هذه الأفعال وصف الجريمة[1] ومن بينها:

- أن ترتكب الجرائم المذكورة دون وجه حق.

- أن ترتكب الجرائم المذكورة بطريقة عمدية من أجل إقرار المسؤولية الجنائية.

أما في **الوطن العربي**:

فقد بدأت الدول فيه تتحرك لمواجهة الجرائم الناشئة عن استخدام شبكة الانترنيت بسن قوانين خاصة بذلك، أو بتعديل وإضافة مواد لقوانينها العقابية القائمة.

ومن بين الدول العربية التي تصدت لهذه الظاهرة **سلطنه عمان** وذلك بإصدار المرسوم رقم 2001/72، والذي تضمن تعديل بعض أحكام قانون العقوبات ومنها جرائم الالتقاط غير المشروع للمعلومات أو البيانات[2]، الدخول غير المشروع على أنظمة الحاسب الآلي، التجسس والتنصت على البيانات والمعلومات، انتهاك خصوصيات الغير أو التعدي على حقوقهم في الاحتفاظ بأسرارهم وتزوير بيانات وثائق مبرمجة أيا كان شكلها، إتلاف، تغيير، محو للبيانات والمعلومات، التعدي على برامج الحاسب الآلي، نشر واستخدام برامج الحاسب الآلي كما أصدرت **تونس** سنة 2000 قانونا في هذا المجال وكذلك **إمارة دبي** عام 2002 صدر قانون التجارة الإلكترونية رقم 2 خاص بالمعاملات الإلكترونية والتوقيع الإلكتروني والحماية المقررة لها في نطاق إمارة دبي فقط[3].

الفرع الثاني: تطور الحماية الجنائية على الصعيد المحلي (الجزائر)

إن **الجزائر** ليست بمنأى عن الثورة المعلوماتية فقد حاول المشرع الجزائري أن يتدارك الأمر ويقوم بتعديل قانون العقوبات فأصدر قانون 15-04 المؤرخ في 10 فيفري 2015 لمواجهة بعض أشكال الإجرام الجديد والحد من هذه الظاهرة المستحدثة من أجل توفير حماية جنائية للأنظمة المعلوماتية.

[1] - د. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الأزاريطة 2007، ص 118.

[2] - بعرة سعيدة، مرجع سابق، ص69.

[3] - بعرة سعيدة، المرجع نفسه، ص70.

المطلب الثاني: تجريم الاعتداء غير المشروع لمواقع التعاقد عبر الانترنت

من أجل حماية العقد المبرم عبر الانترنت فقد جرمت جميع أفعال التعدي أو أي سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها سواءً كان هذا التعدي في صورة الدخول أو البقاء غير المشروع أو أي تدمير لنظام المعالجة الآلية من محو للبيانات وتعليمات البرنامج أو إعاقة عمله، وعلى ذلك كيف تمت حماية نظام المعالجة الآلية للمعطيات من الاعتداء؟ وهذا ما سنتطرق إليه من خلال تحقق جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية على الرغم من صعوبة اكتشافها لأن معظمها أو جميعها تكتشف بمحض الصدفة فهي لا تترك أي أثر خارجي بصورة مرئية فلا جثث فيها ولا آثار دماء ولا اقتحام من أي نوع فهي جرائم فكر لا جرائم عنف[1] وكذلك صعوبة إثباتها لأن الجاني يدمر كل ما يعتبر دليلا يمكن أن يدينه.

الفرع الأول: تجريم الدخول غير المشروع على نظام المعالجة الآلية للمعطيات في مختلف التشريعات

من بين التشريعات التي جرمت الدخول غير المشروع على نظام المعالجة الآلية للمعطيات:

أ- المجتمع الأوربي:

لقد شعر المجتمع الأوربي بخطورة الجرائم الواقعة على النظام ولذلك عملت اللجنة الأوربية بشأن مشاكل الجريمة وكذا الخبراء على إعداد مشروع اتفاقية تتعلق بجرائم المعلوماتية وقد أعلن المجلس الأوربي مشروع هذه الاتفاقية مع الأخذ بعين الاعتبار الطابع الدولي الغالب لمثل هذه الجرائم وقد حدد المشروع الإجراءات التي يتعين على الدول المتعاقدة اتخاذها سواء على المستوى الداخلي أو المستوى الدولي فعلى المستوى الداخلي وجه المشروع الدول المتعاقدة على أن تجرم أفعال الاعتداء على سرية وتكامل بيانات النظام والاتصال به وحدد أيضا أفعال الدخول العمدي غير المشروع على النظام بصورة كلية أو جزئية وأعطى الدول المتعاقدة خيار أن تضيف شرطا للعقاب وهو أن يكون الدخول باختراق إجراءات تأمين النظام أو بنية الحصول على بيانات معينة أو لأي غرض آخر غير مشروع[2].

لقد نصت على جريمة الولوج أو الدخول غير القانوني دون حق في المادة الثانية :"يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبار جريمة الولوج

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت مذكرة ماجستير، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2013، ص 15.

[2] – د.شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 97.

جريمة جنائية وفقا لقانونها الداخلي كما يمكن أن ترتكب هذه الجريمة من خلال انتهاك إجراءات أمنية بنية الحصول على بيانات الحاسوب أو بحاسوب آلي يكون متصلا عن بعد بحاسوب آخر.

ب- تجريم الدخول غير المشروع في الولايات المتحدة الأمريكية:

أصدرت الولايات المتحدة الأمريكية القانون الفدرالي بشأن الاعتداء على نظام المعالجة الآلية واستغلاله حيث يعاقب كل شخص يدخل عمدا على النظام بدون تصريح أو يتجاوز التصريح الممنوح له ويحصل بأي وسيلة كانت على معلومات أو بيانات سرية حددت الولايات المتحدة الأمريكية أنه لا يجوز الكشف عنها مثل اختراق أحد العسكريين لنظام وزارة الدفاع وقيامه بنشر ملفاتها السرية على مواقع الانترنت[1].

ج- تجريم الدخول غير المشروع في التشريع الفرنسي:

أراد المشرع الفرنسي مواجهة الإجرام المعلوماتي من خلال قانون العقوبات الجديد حيث يعاقب على الدخول بطريق الغش أو التدليس على نظام المعالجة الآلية للبيانات أو إبقاء الاتصال به بطريقة غير مشروعة سواء كان هذا الدخول بطريقة مباشرة أو غير مباشرة وقد شدد المشرع العقوبة إذا ترتب على نشاط الجاني إلغاء أو تعديل للمعطيات، أو تشغيل النظام كما يمكن أن تقع هذه الجريمة على نظام غير مفتوح للجمهور، بحيث يجوز لفئة معينة من الأشخاص الدخول إليه أو أن يكون النظام مفتوحا للجمهور ولكن يجوز له الدخول إلى جزء معين منه، وبرغم ذلك يقوم الجاني بالدخول إلى بيانات محظورة[2].

فقام المشرع الفرنسي بتعديل قانون العقوبات عام 1994 مستخدما مصطلح الغش المعلوماتي، وفي عام 2004 أضاف جريمة أخرى وهي جريمة التعامل في وسائل المكتب أي الوسائل التي تصلح لأن ترتكب بها جريمة الدخول أو البقاء المصرح بهما وجريمة التلاعب بالمعطيات أو الإعاقة لأنظمة المعالجة الآلية، وتشدد العقوبة في حالة محو أو تعديل لهذه المعطيات[3].

---

[1]- د مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ص37-38.

[2]- دحمان صبايحية خديجة، جرائم السرقة والاحتيال عبر الانترنت، دراسة مقارنة، مذكرة لنيل شهادة ماجستير، كلية العلوم الإسلامية، جامعة الجزائر، 2013، ص.....

[3]- **د**.شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 98.

شروع أو أي تدمير لنظام المعالجة الآلية من محو للبيانات وتعليمات البرنامج أو إعاقة عمله، فكيف تمت حماية نظام المعالجة الآلية للمعطيات من الاعتداء؟ وهذا ما سنتطرق إليه من خلال تحقق جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية فعلى الرغم من صعوبة اكشافها لأن معظمها أو جميعها تكتشف بمحض الصدفة فهي لا تترك أي أثر خارجي بصورة مرئية فلا جثث فيها ولا آثار دماء ولا اقتحام من أي نوع فهي جرائم فكر لا جرائم عنف وكذلك صعوبة إثباتها لأن الجاني يدمر كل ما يعتبر دليلا يمكن أن يدينه.

د- تجريم الدخول غير المشروع في القانون العربي النموذجي:

بناءا على قرار مجلس وزراء العرب فقد تم إصدار القانون الجزائي الموحد كقانون عربي نموذجي والذي جرم مجموعة من الأفعال المرتبطة بإساءة تقنية المعلومات، كما نصت المادة 461 و464 على وجوب حماية الحياة الخاصة للأفراد وأسرارهم من خطر المعالجة الآلية[1] لمن بين هذه الجرائم جريمة الاختراق ممثلة في الدخول أو البقاء غير المشروع في النظام المعلوماتي بأي وسيلة تقنية كانت ويتحقق هذا الدخول متى دخل الجاني إلى النظام المعلوماتي كله أو جزء منه دون وجه حق أي دون موافقة صاحب النظام أو من له حق السيطرة عليه[2].

ه- تجريم الدخول غير المشروع في القانون الجزائري:

وقد تفطن المشرع الجزائري إلى ذلك من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 حيث أصبحت المعلوماتية من وسائل ارتكاب الجريمة ضد الأشخاص والأموال فخصص في القسم السابع منه لجرائم المساس بأنظمة المعالجة الآلية للمعلومات[3]، فجرم بذلك فعل الدخول أو البقاء غير المشروع داخل النظام ألمعلوماتي في المادة 394 مكرر فيقصد هنا بفعل الدخول هو الدخول المعنوي إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية وليس الدخول المادي[4] تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به أو عن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقطً وقام بتعديل آخر

[1]- صغير يوسف، مذكرة ماجستير بعنوان الجريمة المرتكبة عبر الأنترنت، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، دفعة 2013، ص101.

[2]- د، مدحت عبد الحليم رمضان الحماية الجنائية للتجارة الإلكترونية دار النهضة العربية القاهرة، ص41-42.

[3]- قانون العقوبات المادة 394 مكرر.

[4]- دحمان صبايحية خديجة،، مرجع سابق، ص 92.

في القانون 15-04 المؤرخ في 10فيفري 2015[1].كما أورد المشرع الجزائري ظرفين لتشدد عقوبة الدخول غير المشروع إلى النظام المعلوماتي أوله حذف أو تغيير المعطيات.

و**الظرف الثاني** هو تخريب نظام اشتغال المنظومة كالشروع في جريمة الدخول غير المصرح به وذلك بقوله " **أو يحاول ذلك**".

أولا: أركان جريمة الدخول أو البقاء غير المشروع

1- الركن المادي: استشعر المشرع في دول عديدة الحاجة إلى إدخال تشريعات جديدة تحمي النظام ألمعلوماتي وذلك لتعرضه للاختراق من قبل أشخاص غير مرخص لهم بالدخول أو البقاء فيه من جهة وقصور القواعد التقليدية من جهة أخرى فقد يشكل الدخول إلى النظام أول حلقة في مشروع إجرامي أوسع، فحاولنا التعريف بجريمة الدخول غير المشروع إلى النظام ونتائجه.

2- الركن المعنوي: إن جريمة الدخول أو البقاء داخل النظام وكذا التجول والبقاء داخله لا يجرمان إلا إذا تم بطريق الغش.

ثانيا: تحقق جريمة الدخول غير المشروع ونتائجه

تقع جريمة الدخول غير المشروع إلى النظام بمجرد إتيان النشاط المؤثم أي الدخول في النظام أو البقاء فيه بعد الدخول بطريقة عرضية وغير مقصودة وأكثر التقنيات استخداما لارتكاب هذه الجريمة هو استخدام البرامج الظاهرة والمخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة، فإن كل إدارات تشغيل البيانات والحاسبات بطريقة آمنة والتي تخضع للتحكم والسيطرة من طرف مستخدميها، تقتضي وجود برامج يمكنها تخطي حواجز الحماية الفنية لمنظومات الحاسوب في حالة اختلال وظائفه أو توقفه عن العمل وأشهرها برنامج super zap[2] إذ يسمح استخدامه بالوصول إلى سائر أجزاء نظام معلومات الحاسوب فهو بمثابة المفتاح العمومي في حالة الطوارئ لفتح الأبواب والمنافذ المغلقة.

إن هذا البرنامج يشكل أداة بالغة الفعالية شديدة الخطر على أمن البرامج والبيانات المخزنة وهذا لأنها تسمح لمستخدميها بالتغلغل في النظام حتى ولو كان محميا بشكل دقيق، إذ تمكن الجاني من أداء أية مهام غير مصرح بها.

[1]- القانون 15-04 المؤرخ في 10فيفري 2015 تحت عنوان.....الجريدة الرسمية رقم 06.

[2]- أمال قارة، مرجع سابق، ص42.

ثالثا: نتائج الدخول غير المشروع إلى النظام.

- إفقاد صاحب الحق السيطرة على النظام.
- مسح الملفات كلها أو بعضها أو تبديلها بشكل جزئي.
- إضافة بيانات أو معلومات جديدة أو نسخ الملفات الموجودة به.
- الإخلال بسير النظام أو إيقاف عمله والإضرار به.
- التنصت على النظام ونقل المعلومات التي تصل إليه إلى نظام آخر[1].

الفرع الثاني: البقاء غير المشروع في نظام المعالجة الآلية

يعرف على أنه "**التواجد داخل نظام المعالجة الآلية دون ترخيص من صاحب الحق في السيطرة على هذا النظام**" أو البقاء فيه بعد الدخول إليه عرضا وبطريق الخطأ وهناك فرض آخر وهو الدخول إلى النظام بطريق مشروع ولكنه يستمر بعد الوقت المحدد لبقائه فيه خاصة إذا كان وقت البقاء مقابل مبلغ مالي يدفع لصاحب النظام فيقوم الجاني بسرقة وقت الآلة.

ويتمثل في علم الجاني بخطورة فعل البقاء والتجول داخل النظام الخاص بالغير ومع ذلك تنصرف إرادته لهذا الفعل مع توفر نية الغش فيقوم الجاني بخرق الجهاز الرقابي الخاص بحماية النظام، ويستوي الحال إذا كان الفعل صادرا ممن يحمل بطاقة معينة أو شفرة من مالك النظام أو عن طريق السرقة والتزوير فهذا كافيا لتوفر القصد الجنائي الخاص، وينتفي في حالتين:

1. إذا سبق للجاني الاشتراك للدخول إلى النظام وانتهت مدة صلاحيته ودخل بطريق الخطأ معتقدا أن تاريخ صلاحيته لم ينتهي بعد فينتفي القصد الجنائي لأن هذا يعد جهلا بالواقع.
2. إذا دخل الجاني إلى النظام بطريق الخطأ فلا يسأل عن الجريمة أما إذا بقي داخل النظام مع إدراكه لذلك واستمر فيه فإن المسؤولية تقوم عليه ولا يعتد بالباعث الذي دفع الجاني على ارتكاب الجريمة سواء كان بنية الحصول على أي نفع أو بنية الإضرار بالغير أو لمجرد المزاح فالعبرة هي توافر عنصري العلم والإرادة[2].

[1] – د مدحت عبد الحليم رمضان الحماية الجنائية للتجارة الإلكترونية دار النهضة العربية، القاهرة، ص 118.

[2] – بوتماني فاطمة الزهراء، الحماية القانونية للعقد المبرم عبر الانترنت، مذكرة لنيل شهادة الماستر،..... ص49.

أولا: تحقق البقاء غير المشروع في نظم المعالجة الآلية

تعتبر جريمة البقاء غير المشروع في النظام من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرميه معينة، وتقوم الجريمة إذا دخل شخص بطريق الخطأ إلى النظام ولكنه استمر داخله أو أن يقوم بطبع نسخة من المعلومات في حين أنه كان مسموح له بالإطلاع عليها فقط، وتتحقق الجريمة أيضا إذا وجد الشخص نفسه داخل النظام بشكل مشروع لكنه يبقى داخله بعد المدة المحددة له بالبقاء فتتحقق جريمة البقاء غير المشروع لتوافر القصد الجنائي لأنها من الجرائم العمدية بغض النظر عن الباعث حتى وإن كان الجاني يريد أن يثبت للمسئولين عن وجود ثغرات في أنظمتهم المطبقة أو بدافع من حب الاستطلاع والفضول فإن هذا لا ينفي القصد الجنائي[1].

وعلى أية حال فإنه لا يلزم توافر قصد من نوع خاص لوقوع الجريمة بل يكفي توافر القصد الجنائي العام أي أن يعلم الجاني بدخوله في النظام الخاص بالغير. ويظهر فعل البقاء من خلال العمليات التي تتم داخل النظام.

ثانيا: الوسائل التي ترتكب بها جريمة الدخول أو البقاء غير المشروع للنظام

1-الدخول إلى الحاسب الآلي بواسطة بطاقة تشغيل خاصة بشخص آخر: قد يتمكن الجاني من الحصول على بطاقة للدخول إلى حاسب آخر للحصول على خدمات مقتصرة على حاملي هته البطاقة فقط ويحصل بذلك عليها عن طريق السرقة مستخدما في ذلك الرقم السري للولوج إلى نظام المعطيات المتواجد بحاسوب آخر.

2-**الدخول إلى الحاسب الآلي بواسطة خط الهاتف:** في هذه الحالة يتمكن الجاني من الوصول إلى نظام الحاسوب عن طريق العبث بالخط الهاتفي المربوط عليه هذا النظام فيقوم بإعطاء أوامر لحاسوب آخر بغية تحقيق أغراض شخصية ومثال ذلك ما قام به عمال شركة الهاتف الفرنسية حيث كان هذا الخط موصول بأجهزة عارضة للألعاب الإلكترونية وتمكنوا من الحصول على جوائز تقدمها الشركة للفائزين في هذه الألعاب[2].

3-الدخول من الحاسوب إلى حاسوب آخر: قد يتمكن الجاني من الدخول إلى نظام آخر من أنظمة الحاسوب بالاتصال عن بعد بهذا النظام والتوصل إلى معرفة كلمة السر للدخول إلى النظام كله أو

[1] - د.شيماء عبد الغني محمد عطا الله الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الأزاريطة 2007 ص 126 ص127.

[2] -د. شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 108-109.

جزء منه كما أن الجاني هنا يستطيع أن يتمكن من الدخول إلى النظام من مرورا من جهاز ثالث وقد يقوم بذلك من خارج البلاد.

الفرع الثالث: الاعتداء العمدي على نظام المعالجة الآلية

لقد نصت المادة الثالثة من القانون النموذجي العربي غلى معاقبة كل شخص يقوم بفعل إعاقة تشغيل نظم معالجة البيانات بفعل التعطيل بأي وسيلة كانت كتسريب الفيروسات أو توقيف تشغيل نظام المعالجة الآلية للمعطيات، كما جرمت اتفاقية بودابست الاعتداء على سلامة النظام في المادة الخامسة منها مجسدة في صورة الإعاقة بما في ذلك تعطيل، إتلاف أو طمس البيانات والتي يجب أن تكون جسيمة وبدون وجه حق ولتحقق هذه الجريمة يجب توافر الأركان الثلاثة الشرعي، المادي والمعنوي.

أولا: الركن الشرعي

إن المشرع الجزائري قد نص على هذه الجريمة في المادة 394 مكرر فقرة 03 بأنه:" وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة مالية من50.000 إلى 150.000دج" وما يلاحظ أن المشرع الجزائري أتى بمصطلح عام يدل على هذه الجريمة وهو "التخريب" الذي يطال نظام المعالجة الآلية للمعطيات[1].

ثانيا: الركن المادي

يكمن الركن المادي في فعل توقيف نظام المعالجة الآلية للمعطيات عن أداء عمله أو في فعل إفساد نشاطه أو تعييب وظائفه كما أنه لا يشترط أن يقع فعل التعطيل أو الإفساد على كل عناصر النظام بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية مثل الجهاز أو المعنوية مثل البرامج والمعطيات وتأخذ صور الاعتداء العمدي ما يلي:

1- فعل التعطيل (العرقلة أو الإعاقة): لم يشترط المشرع أن يتم فعل التعطيل بوسيلة معينة فقد تكون تلك الوسيلة مادية إذا وقعت على أجهزة النظام أو القيام بتخزينها كقطع شبكات الاتصال بها أو كسرها، وقد تكون تلك الوسيلة معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات ويحدث ذلك إما :

[1]- تمم الفصل الثالث بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 (ج.ر 71 ص 11و12) ويتضمن المواد من 394 مكرر إلى 394 مكرر 7.

- بإدخال برنامج فيروسي.
- استخدام قنابل منطقية.
- إشباع إمكانيات الدخول.
- جعل النظام يتباطأ في أدائه لوظائفه.

– استخدام بطاقات الوقف: وهي بطاقات تسمح بوقف تنفيذ البرنامج بالمرور بمختلف الفيروسات المعلوماتية والقنابل المنطقية، فيقوم الجاني بنشاط يؤدي إلى توقيف النظام أو الامتناع عن التدخل وعرقلة سير نشاطه[1].

وقد ترد الإعاقة على برنامج من البرامج التي يحتويها النظام وليس على كل نظام الجهاز. فالمشرع الفرنسي يرى أنه لا يعد من قبيل إعاقة النظام إضراب العمال عن أداء وظائفهم والذي يتسبب في توقف النظام عن العمل، فلا يسري في ذلك وصف السلوك المؤثم في جريمة إعاقة النظام إلا إذا حدث أثناء الإضراب تخريب للأجهزة الخاصة بالعمل عندئذ يمكن القول بجريمة الإعاقة مع الإتلاف وبالتالي نتواجد أمام تعدد في الجرائم يتم حله بتطبيق العقوبة الأشد.

كما يمكن أن تقع الجريمة أيضا إذا قام المضربون بمنع العمال غير المضربين من استخدام الأجهزة وبالتالي أدى ذلك إلى تخريبها وتعطلها، كما أنه لا يعتبر من قبيل النشاط المعاقب عليه أن يحدث إخلال بعقد من عقود صيانة الأجهزة أو عدم توريد قطع غيار لتلك الأجهزة بما يؤدي إلى الإخلال بسيرها[2].

أ– البرامج الخبيثة: هنا يقوم الجاني بتصميم عدة برامج للاعتداء على نظام المعالجة الآلية ومن أبرز هذه البرامج القنابل المنطقية والزمنية– حصان طروادة وفيروس الدودة.

ب– القنابل المنطقية والزمنية: عبارة عن برنامج أو جزء منه ينفذ في لحظة معينة أو فترة زمنية محددة ويتم وضعه في الشبكة المعلوماتية لتغيير حالة محتوى النظام فهي عبارة عن برامج محمية تبقى ساكنة وغير فعالة وغير مكتشفة لمدة أشهر أو سنوات ولهذا يصعب تعقب الجاني وتقفي أثره.

تحدد هذه المدة عن طريق مؤشر زمني يحتويه البرنامج فينشط عند حلول أجله. يرتبط مؤشر التفجير في هذه القنابل المنطقية بشروط منطقية معينة داخل نظام التشغيل أو داخل الملف ويختلف مؤشر التفجير من قنبلة إلى أخرى فقد يكون بإدخال أو عدم إدخال بيانات معينة إلى نظام المعلومات أو بمجرد الاتصال بمستخدمي هذا النظام بوجود قنبلة بداخله فتؤدي إلى تفعيله[3].

---

[1]– أمال قارة، مذكرة تخرج ماستر بعنوان الجريمة الإلكترونية، ابن عكنون، الجزائر، دفعة2003، ص47.

[2]– د.شيماء عبد الغني محمد عطا الله الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الأزاريطة 2007 ص128.

[3]– د،عطا الله فشار ، المرجع السابق، ص50

ج- القنابل الزمنية: يتم إدخال قنبلة زمنية لتثير حدثا في لحظة معينة حيث تكون مبرمجة برمجة دقيقة محددة بالتاريخ، اليوم والساعة والثانية فينجم عنها شل عمل النظام عند البدء في تشغيله أو عند استخدام أحد برامج التطبيق.

د- فيروس الدودة: هو برنامج يستطيع ان يقوم بنسخ تنفيذية من نفسه في برامج أخرى كباقي الفيروسات فهو في حد ذاته برنامج تشغيل ينتقل من حاسوب إلى آخر ومن شبكة لأخرى عن طريق الوصلات التي تربط بينهما فتتكاثر كالبكتيريا وتقوم بإنتاج نسخ أخرى من هذا الفيروس الذي يغزو الشبكة للتقليل من كفاءتها فيبدأ في الانتشار ليقوم بالتخريب الفعلي للملفات والبرامج ونظم التشغيل ويتميز هذا البرنامج بقدرته الفائقة على تعطيل وإيقاف نظام الحاسب الآلي وكذا إفساد البرامج والمعطيات المعلوماتية.

2/ فعل الإفساد أو التعييب: يقصد به كل فعل يجعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بإعطائه نتائج مخالفة للنتائج المفترض الحصول عليها وهذا باستعمال برامج وتقنيات متعددة. إن جريمة التعييب أو الإفساد تفترض علم الجاني أن ما يقوم به يتم دون موافقة ورضا صاحب الحق في السيطرة على نظام المعالجة الآلية للمعطيات ولهذا فتعتبر هذه الجريمة من الجرائم العمدية والتي تقوم بالقصد الجنائي العام وبناءا عليه إذا قام المتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات لم يسأل عن هذه الجريمة[1].

ومن الناحية النظرية يمكن التمييز بين فعل التعطيل، التوقيف، الإفساد أو التعييب غير أنه من الناحية العملية فكثيرا ما يتطابقان وهذا للتشابه الكبير بين فعل التعطيل أو الإفساد وجريمة التخريب أو الإتلاف العادية لاشتراكهما في عدة جوانب وللتفرقة بينهما يجب أن ننظر في الوسائل التي أدت إلى ارتكاب كل جريمة على حدى.

موقف المشرع الفرنسي: يرى المشرع الفرنسي أن جريمة الإعاقة أو إفساد عمل نظام التشغيل أو الإرسال ينصرف إلى كل عمل من شأنه إرباك نظام المعالجة الآلية للبيانات ويستوي أن يؤدي نشاط الجاني إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شأنها الإخلال بالسير الحسن للنظام كالاعتداء المادي على النظام أو نشر فيروس به ويستوي لدى المشرع الوسيلة المستخدمة ولا يشترط أن تكون الإعاقة أو الإفساد كليا بل يمكن أن يؤدي النشاط إلى إعاقة أو إفساد جزئي للنظام.

[1]- بوتماني فاطمة الزهراء، مذكرة تخرج بعنوان الحماية القانونية للعقد المبرم عبر الانترنت، ص54.

ا/تقنيات الإفساد والتعييب:

– **التلاعب في المدخلات:** ويكون ذلك في أولى مراحل تشغيل النظام أي مرحلة إدخال البيانات لمعالجتها وتحويلها إلى لغة مقروءة كأن يقوم الجاني بإدخال معلومات مختلفة أو محرفة كما يلجأ أيضا إلى تغيير مسار البيانات الصحيحة المدخلة أو منع إدخال بيانات وثائق معينة ومن أبرز صور **التلاعب في البرامج:**

– */ إدخال تعديلات غير مرخص بها على البرامج المستخدمة ويتم ذلك أثناء مرحلة التنفيذ أين تتم بعض التعديلات الثانوية على البرامج من تصحيح لبعض الأخطاء التي لم يتم اكتشافها من قبل حيث يقوم الجاني بإدخال تغييرات غير مرخص بها على البرامج والتي تسمح بارتكاب جرائم الاعتداء ويعرف ذلك ب**حيلة أو خدعة التقريب**[1].

ب/ برنامج حصان طروادة :le cheval de Troie

حيث يقوم هذا الفيروس بتغيير غير محسوس في البرنامج أو المعطيات فيتم الإفساد عن طريق إتلاف أو تخريب العناصر المادية لنظام المعالجة الآلية للمعطيات. أول ما ظهر هذا البرنامج في الولايات المتحدة الأمريكية في نهاية السبعينيات عبر اللوحات الإلكترونية ويعرف باسم ZAXOON وهو عبارة عن ألعاب تسلية في ظاهره ثم يبدأ تدريجيا في محو أقراص النظام المعلوماتي .[2]

– برنامج FILER والذي يقوم بتنظيم بيانات الملفات وهو في حقيقة الأمر يقوم بمحوها.

– الركن المعنوي

إن جريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات هي جريمة قصدية عمدية حيث يتخذ فيها الركن المعنوي صورة القصد الجنائي العام بعنصريه العلم والإرادة فيكفي أن يعلم الجاني بأن وجوده بالنظام هو ضد إرادة صاحب الحق في السيطرة عليه وبدون رضاه وبالرغم من ذلك فإن إرادته تتجه لفعل التعطيل أو الإفساد. إضافة إلى القصد الجنائي العام فيجب أن تتوفر نية الغش لدى الجاني فهذا لا يعني ضرورة توفر قصد الإضرار بالغير بل حتى ولو كان بدافع الفضول.

[1] – أمال قارة، **مذكرة** تخرج بعنوان الجريمة المعلوماتية، جامعة بن عكنون، الجزائر ص48.

[2] – د.مدحت عبد الحليم رمضان، المرجع السابق، ص 55.

المطلب الثالث: جريمة التلاعب بنظام المعالجة الآلية

يقع النشاط الإجرامي في جريمة التلاعب بنظام المعالجة الآلية على موضوع محدد وهو المعطيات أو المعلومة المعالجة آليا والتي تبلورت وأصبحت مجرد إشارات ورموز وليس المعلومة في حد ذاتها باعتبارها أحد عناصر المعرفة بل يقتصر المحل في هذه الجريمة على المعلومات المعالجة آليا والموجودة داخل النظام باعتبارها جزء لا يتجزأ من النظام بكله فما هي الأفعال المجرمة التي تمارس على نظام المعالجة الآلية ؟

وما هي العقوبات المقررة لها؟ سوف نجيب على هذا التساؤل في المطالب الآتية.

الفرع الأول: الأفعال المجرمة التي تمارس على نظام المعالجة الآلية

يتمثل النشاط الإجرامي في هذه الجريمة في إحدى الأفعال التالية:

- الإدخال L'intrusion.
- المحو l'effacement
- التعديل la modification

و هذه الأفعال الثلاثة تأخذ **صورة التلاعب العمدي بالمعطيات داخل النظام** فيتحقق الركن المادي لهذه الجريمة بمجرد صدور إحدى هذه الأفعال الثلاث فلا يشترط أن تصدر كل هذه الأفعال مجتمعة معا .

أولا: فعل الإدخال (L'intrusion)

يقصد بفعل الإدخال إضافة معلومات جديدة على الدعامة الخاصة بها سواء كانت خالية أو تحتوي على معلومات ومعطيات سابقة ومثال ذلك أن يستخدم الجاني بطاقات السحب الآلي مستعملا في ذلك الرقم السري الخاص بالشخص ويقوم بسحب أموال طائلة من حساب المعني أو عن طريق الاستخدام التعسفي لبطاقات الائتمان فيقوم الجاني بتسديد مبالغ أكثر من المبالغ المحددة له. وأخيرا يمكن القول أن فعل الإدخال يتحقق في كل حالة تستخدم فيها بطاقات السحب أو الائتمان بطريقة تعسفية سواء من صاحبها الشرعي أو غيره وخاصة في حالات السرقة ، الفقد أو التزوير، أو استخدام بطاقة ائتمان منتهية الصلاحية أو ملغاة من طرف البنك نتيجة لفسخ العقد بين البنك وصاحب البطاقة.

الاستخدام غير المشروع لبطاقة الائتمان من قبل موظف البنك إذ يتواطأ مع العميل حامل البطاقة سيء النية ويقوم باستخراج بطاقة سليمة بناءا على معلومات مزورة ويقوم بعملية شراء بمبالغ طائلة يعتبر البنك مسؤولا عنها دون إمكانية تحصيل قيمتها من حامل البطاقة لاستحالة الاستدلال عليه[1].

[1] – دحمان صبايحية خديجة ، مرجع سابق، ص 70، ص 71.

كما يتحقق فعل الإدخال عن طريق إدخال برامج خبيثة حاملة للفيروسات فيقوم الجاني بإضافة معلومات جديدة على المعلومات الأصلية[1].

- **موقف المشرع الفرنسي:**

لقد جرم المشرع الفرنسي كل عملية إدخال البيانات في قانون العقوبات وذلك بعقاب كل من أدخل بسوء نية بيانات في نظام معالجة البيانات أو قام بسوء نية بإلغاء أو تعديل هذه البيانات في نظام المعالجة الآلية أو أي محو أو تعديل البيانات المثبتة فيه وكل ما من شأنه أن يسبب خللا في نظام عمل الجهاز حيث تكون وتيرة عمله بصورة بطيئة أو مضطربة فتبتعد عن الصورة المعتادة كما تتحقق الجريمة عندما يقوم المتهم بأي عمل يؤدي إلى إرباك سير النظام فلا يؤدي نفس الوظيفة المعتادة له، فيصبح بذلك عاجزا عن العمل بصفة كلية أو جزئية[2].

تطبيقا لذلك قضت المحكمة الفرنسية بتوافر جريمة الإخلال بسير النظام من طرف المتهم الذي قام بإرسال رسائل كثيرة إلى أحد الأجهزة الخاصة بإحدى الشركات المنافسة موهما هذا الجهاز أن الرسائل تصل إليه من أجهزة متعددة، وتتضمن طلابيات شراء من الشركة وقد كانت تلك الطلبيات غير جدية وكان هدفه هو ملء الأجهزة الخاصة بالشركة حتى تصبح عاجزة عن تلقي طلبات جديدة وبالتالي الإضرار بالشركة، فقضت المحكمة الفرنسية آنذاك بتوافر الجريمة .

ومن التطبيقات القضائية على جريمة إدخال بيانات غير مصرح بها ما قامت به المتهمة التي كانت تعمل في إحدى شركات المحاسبة حيث قامت بإدخال بيانات غير صحيحة تتعلق بمعدل احتساب الضريبة على القيم المنقولة وقد أدى ذلك إلى إرباك العمل بما كانت تزمع الشركة القيام من أعمال المحاسبة داخل الشركة وقد كان واضحا أن قصد المتهمة كان منصرفا إلى تحقيق تلك الغاية.

لا تقوم الجريمة استنادا إلى الخطأ غير العمدي فإذا نسب إلى المتهم أنه في أثناء تجاربه على النظام حدث هناك إغلاق للنظام وإضاعة البيانات المبرمجة فيه فإن الجريمة لا تقوم رغم ذلك لانتفاء القصد الجنائي[3].

ومن هنا يتضح لنا أن المشرع الفرنسي لا يحمي النظام من الناحية المادية ولكنه يوفر الحماية للمعلومات الموجودة بالنظام وهذا ما عبر عليه بالقرصنة المعلوماتية فوفر الحماية ضد أي نشاط إجرامي يؤدي إلى تحقق نتائج غير تلك المراد تحقيقها. فالجريمة هنا من الجرائم العمدية التي تقوم بالقصد الجنائي العام

[1]- أمال قارة، مذكرة تخرج حول الجريمة المعلوماتية، نفس المرجع، ص52.

[2]- د.شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 198.

[3]- د.شيماء عبد الغني محمد عطا الله، نفس المرجع ص 130، ص 134.

حيث يتعين أن يعلم الجاني بطبيعة نشاطه وأن تتجه إرادته إلى الإدخال أو إحدى الأفعال الثلاث وأن يعلم أنه يعتدي على حقوق الغير بهذا الفعل فنص المشرع الفرنسي في قانون العقوبات بعقابه كل من أدخل بسوء نية بيانات في نظام معالجة البيانات أو قام بسوء نية بإلغاء أو تعديل هذه البيانات.

من الواضح أن موقف المشرع الفرنسي يتسم بالبساطة والمنطق فلم يغرق في التفاصيل كما فعل المشرع الأمريكي حيث نص على الجرائم دون أن يحدد الجهة التي يتبع لها نظام معالجة البيانات حيث أمعن في التفاصيل واهتم بحماية الأنظمة الخاصة بالأمن القومي والاتحادية وربما يعود هذا لكون القوانين الاتحادية تهتم بالأمور المتعلقة بالأمن القومي وعلاقات الولايات المتحدة الأمريكية مع المجتمع الدولي وبهذا فقد ترك المشرع الاتحادي كامل الحرية للولايات المتحدة الأمريكية في وضع القوانين المحلية المناسبة في هذا المجال[1].

ثانيا: فعل المحو "l'effacement"

يتمثل فعل المحو في إزالة جزء من المعطيات الموجودة داخل النظام ونقله وتخزينه في الذاكرة أو تحطيم تلك المعلومات بمحوها كليا أو جزئيا ويتم ذلك باستخدام برامج غريبة للتلاعب بالمعطيات ومنها **برنامج المحاة**.la gomme d'effacement [2].

ثالثا: التعديل : la modification

يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى فقد يقوم المتهم بتعديل المحتوى المادي للبيانات المبرمجة وذلك بإضافة ، حذف أو تغيير البيانات ذاتها، والملاحظ في جريمة التعديل أنها تتداخل مع جريمة الدخول إلى النظام والبقاء به فغالبا ما تقع الجريمة حتى ولو كان الفاعل مسموحا له بالدخول إلى النظام فيستوي أن يكون مسموحا له أو غير مسموح له بالدخول إلى النظام ولذا قضي بوقوع الجريمة من المحاسب في ذات الشركة التي يعمل بها إذا قام بتعديل البيانات بدون وجه حق[3].

إن أفعال المحو التعديل والإدخال لا يشترط أن تقع بطريق مباشر إذ يمكن أن تتحقق بطريق غير مباشر سواء عن بعد أو بواسطة شخص آخر ولقد وردت هذه الأفعال على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر.

الفرع الثاني: المساس العمدي بالمعطيات خارج النظام

لقد وفر المشرع الجزائري الحماية الجنائية للمعطيات في حد ذاتها وذلك من خلال المادة 394 مكرر 2 ويستوي أن تكون هذه المعطيات داخل نظام المعالجة الآلية أو قد تمت معالجتها لأن محل الجريمة هنا

[1]- مدحت عبد الحليم رمضان، مرجع سابق، ص 92.

[2]- أمال قارة، المرجع السابق، ص53.

[3]- د.شيماء عبد الغني محمد عطا الله، مرجع سابق، ص137-136.

المعطيات في حد ذاتها سواء كانت مخزنة على أشرطة ، أقراص أو تلك المعالجة آليا أما الفقرة الثانية من نفس المادة فجرمت جميع أفعال الحيازة، الإفشاء، النشر والاستعمال مهما كان غرضها (المنافسة غير المشروعة، الجوسسة، الإرهاب.....)[1].

الركن المعنوي: يتمثل في القصد الجنائي العام مع توفر نية الغش.

المبحث الثاني: العقوبات المقررة لكل جريمة ونطاق تطبيقها

لقد نصت جميع التشريعات على عقوبات أصلية وأخرى تكميلية لردع جريمة الاعتداء غير المشروع لمواقع التعاقد عبر الانترنت وطبقا لنص المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة على الجرائم الماسة بالأنظمة المعلوماتية بشتى صوره يجب أن تكون رادعة وسالبة للحرية ولمواجهة هذا النوع من الإجرام الحديث، قام المشرع الجزائري في نص المادة 394 مكرر ق.ع على عقوبات تطبق على الشخص الطبيعي والشخص المعنوي بناءا على مبدأ مسائلة الشخص المعنوي الواردة في المادة 12 من نفس الاتفاقية.

المطلب الأول: العقوبات الأصلية المقررة لكل جريمة

أ/ العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع في النظام:

نظرا لكثرة الاعتداءات على نظام المعالجة الآلية للمعطيات وخطورتها خاصة تلك المتمثلة في جرائم الدخول والبقاء غير المشروع فإن المشرع قام بعدة تعديلات لمواجهة هذه الأخيرة ومن بينها:

1/ العقوبات الأصلية المطبقة على الشخص الطبيعي:

لقد وضع المشرع الجزائري تدرجا داخل النظام العقابي يحدد الخطورة الإجرامية لهذه التصرفات فتأتي في الدرجة الأولى جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة والمشددة ثم جريمة المساس العمدي بالمعطيات.

أولا: عقوبات جريمة الدخول أو البقاء غير المشروع في (الصورة البسيطة):

وفقا لنص المادة 394 مكرر فقرة 01على أنه:"**يعاقب بالحبس من ثلاثة(03) أشهر إلى سنة وبغرامة مالية من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك**"[2].

أما المشرع الفرنسي فعاقب على جريمة الدخول أو البقاء غير المشروع في النظام بالغش في **المادة 323 من قانون العقوبات الفرنسي يعاقب بالحبس بسنتين وثلاثون ألف أورو.**

[1] – د.عطا الله فشار، الجريمة المعلوماتية في التشريع الجزائري، محاضرة، كلية الحقوق والعلوم السياسية، جامعة الجلفة، ص 493.

[2] – الأمر رقم 66-156 المتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.

ثانيا: الصورة المشددة: لقد شدد المشرع الجزائري العقوبة إذا نجم عن فعل الدخول أو البقاء غير المشروع في النظام تخريب لنظام اشتغاله، حذف أو تغيير لمعطيات المنظومة في نص المادة 394 مكرر/02-03 بقوله:" **تضاعف العقوبة إذا ترتب على ذلك حذف وتغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 06 أشهر إلى سنتين والغرامة من 500.000 دج إلى 1500.000 دج**[1].

أما إذا توفرت ظروف التشديد المتمثلة في حذف، تعديل أو تغيير في النظام فقد تضاعف العقوبة بالحبس ثلاث سنوات **وغرامة مالية مقدرة ب 45000 أورو**[2].

ب/العقوبات المقررة لجريمة الاعتداء العمدي على المعطيات.

لقد عنت معظم التشريعات التي جرمت التلاعب ببيانات نظام المعالجة الآلية دون وجه حق بعقوبات أصلية في حق مرتكبيها وذلك متى تحققت الجريمة بكامل أركانها ، الركن المادي والمتمثل في فعل الإدخال، المحو أو التعديل والركن المعنوي والمتمثل في علم الجاني بخطورة ما يقوم به وانصراف إرادته لذلك الفعل ومن بينها:

* **التشريع الجزائري:** لقد نصت المادة 394 مكرر2 ق.ع.ج بالحبس من ستة 06 أشهر إلى ثلاث سنوات حبس وبغرامة مالية من 500.000 دج إلى20.000.00 دج على أفعال التلاعب من إدخال محو أو تعديل أما العقوبة المقررة في لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة، إفشاء، نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية فتكون العقوبة الحبس من شهرين غلى ثلاث 03 سنوات وغرامة من 1000000 دج إلى 5000000 دج. وعلى الرغم من تشديد العقوبة على الشخص الطبيعي إلا أن الجريمة تأخذ وصف الجنحة.

-المشرع الفرنسي: لقد عاقب المشرع الفرنسي على هذه العقوبة بخمس سنوات حبس وغرامة مالية بـــ 75000 أورو هذا بالنسبة للشخص الطبيعي. أما الشخص المعنوي فقد تصل الغرامة إلى خمسة أضعاف الغرامة المقررة للشخص الطبيعي وفق نص المادة 323-03.

أما **بالنسبة للشخص المعنوي:**

وطبقا لنص المادة 394 مكرر 4 والمادة 177 مكرر 1 من قانون العقوبات الجزائري فتقدر العقوبة بغرامة مالية تعادل 5 خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وهذا لأن المادة

[1]- نفس الأمر 66-156 لمتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.

[2]- مختارية بوزيدي ماهية الجريمة الالكترونية، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، ص 07.

394 مكرر 4 تشمل جميع العقوبات المقررة للشخص المعنوي والمنصوص عليها في القسم السابع من قانون العقوبات الخاص بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

أما في التشريع الفرنسي فتقدر العقوبة بغرامة مالية قد تصل إلى خمسة أضعاف الغرامة المقررة للشخص الطبيعي[1].

المطلب الثاني: العقوبات التكميلية

أ/ العقوبات التكميلية المقررة لجريمة الدخول أو البقاء غير المشروع في النظام.

1- العقوبات المطبقة على الشخص الطبيعي:

لقد كانت العقوبة التكميلية الوحيدة في القانون الفرنسي القديم هي مصادرة وسائل ارتكاب الجريمة وبعد عدة تعديلات أضاف المشرع الفرنسي عقوبات تكميلية أخرى من بينها:

- الحرمان من الحقوق السياسية والمدنية والعائلية مدة لا تتجاوز 5 سنوات.
- الحرمان من حق تولي الوظائف العامة أو أي نشاط مهني أو اجتماعي تكون الجريمة قد ارتكبت بسببه أو بمناسبته.
- مصادرة الأشياء التي استخدمت أو كان من شانها أن تستخدم في ارتكاب الجريمة عدى الأشياء محل المطالبة بالرد.
- غلق المؤسسة أو المشروعات التي ساهمت في ارتكاب الجريمة مدة لا تتجاوز 5 خمس سنوات.
- الحرمان من إصدار الشيكات مدة لا تتجاوز 05 سنوات إلا تلك التي تسمح للساحب بسحب أموال من المسحوبة عليه أو إذا كانت مقبولة للدفع[2].
- الحرمان من التعامل في الأسواق العامة مدة لا تتجاوز خمس سنوات.
- نشر الحكم وإعلانه.

والملاحظ أن المشرع الفرنسي قد تبنى مبدأ المسؤولية الجنائية **للشخص المعنوي** فحدد الأشخاص المعنوية التي يمكن أن تسأل جنائيا سواء كانت أشخاصا معنوية عامة أو خاصة باستثناء الدولة شريطة أن ترتكب الجريمة لحسابه ومن طرف أعضائه أو ممثليه دون التأثير على المسؤولية الجنائية للشخص الطبيعي فيحكم على الشخص المعنوي بالغرامة المالية إلى جانب العقوبات التكميلية المطبقة على الشخص الطبيعي ما عدا تلك المتعلقة بشخصه.

[1] – أمال قارة، مرجع سابق، ص 67.

[2] – مدحت عبد العليم، مرجع سابق، ص 48.

أما **في القانون الجزائري** فقد نص المشرع في المادة 394 مكرر 03 على العقوبات التكميلية وفي المادة 394 مكرر 06: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه[1].

أ/ جريمة الدخول والبقاء غير المشروع (الصورة البسيطة)

- **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة مع مراعاة حقوق الغير حسن النية.
- **إغلاق المواقع:** والأمر يتعلق بالمواقع (les sites) التي تكون محلا للجريمة.
- **إغلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد تمت بعلم مالك المحل أو مكان الاستغلال مثل إغلاق المقهى الإلكتروني الذي ترتكب منه الجريمة مع عناصر العلم لدى مالكها فبذلك يتخذ المالك صفة الشريك في الجريمة[2].

الظروف المشددة:

وفقا لنص المادة 394 مكرر/2-3 تشدد عقوبة الدخول والبقاء غير المشروع داخل النظام إذا نتج عن هذا الدخول أو البقاء إما حذف أو تغيير للمعطيات فتضاعف العقوبة المقررة في الفقرة الأولى من المادة 394 مكرر وفي حال تخريب النظام تكون العقوبة من ستة أشهر إلى سنتين وغرامة مالية من 50.000دج إلى 150.000 دج.

وتضاعف العقوبات أيضا إذا استهدفت الجريمة الدفاع الوطني، الهيئات والمؤسسات الخاضعة للقانون العام وهذا ما جاء به نص المادة 394 مكرر 3.

ب/ العقوبات التكميلية المطبقة على الشخص المعنوي:

أما إذا كان مرتكب الجريمة شخص معنوي فإن العقوبة تختلف وهذا نظرا لخصوصية الشخص المعنوي فمن غير الممكن تطبيق عقوبة الحبس أو السجن عليه.و تجسيدا لمبدأ مساءلة الشخص المعنوي سواء كان فاعلا أصليا أو شريكا أو متدخلا وأن ترتكب الجريمة بواسطة أحد أعضائه أو ممثليه فإن المشرع الجزائري قد أقر في التعديل الخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي من خلال المادة 18 مكرر من القانون 15/04 والذي ينص على:" العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:

[1]- الأمر 66-156 لمتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.

[2]- عطا الله فشار، الجريمة المعلوماتية في التشريع الجزائري كلية الحقوق والعلوم السياسية، جامعة الجلفة، ص 495.

– الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة".

- واحدة أو أكثر من العقوبات التالية:

– حل الشخص المعنوي

– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.

– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 خمس سنوات.

– مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها[1].

– نشر أو تعليق حكم الإدانة.

– الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته[2].

أما تطبيق عقوبة الغرامة المالية في المادة **394 مكرر فقرة 4 قانون العقوبات الجزائري والمادة 177 مكرر 1** منه وذلك بالحكم على الشخص المعنوي بغرامة مالية تعادل 05 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

تقوم المسؤولية الجزائية للشخص المعنوي على أساس المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

المطلب الثالث: نطاق تطبيق العقوبة

نظر الخطورة الجرائم التي تطال النظام المعلوماتي وما ينجر عنها من أضرار فإن جل التشريعات وسعت من نطاق العقوبة ليشمل كلا من الأفعال والأشخاص ومن بين هذه الأفعال كل أعمال البدء في التنفيذ أما فيما يخص الأشخاص فتضم جميع المشاركين في العمال التحضيرية للجنح المرتكبة ضد النظام المعلوماتي[3]. وهذا ما سنتعرض إليه في الفرعين التاليين:

[1]– أمال قارة، مرجع سابق، ص 94.

[2]– عطا الله فشار، الجريمة المعلوماتية في التشريع الجزائري كلية الحقوق والعلوم السياسية، جامعة، الجلفة، ص 496، ص 497.

[3]– بوتماني فاطمة الزهراء، الحماية القانونية للعقد المبرم عبر الانترنت، مذكرة تخرج ماستر، جامعة محمد آكلي، بويرة، ص68.

الفرع الأول: الشروع في جرائم الاعتداء العمدي على نظام المعالجة الآلية للمعطيات

لقد جرمت الاتفاقية الدولية للإجرام المعلوماتي كل أفعال الشروع في هذه الجريمة وذلك من خلال المادة 11و نص عليه المشرع الجزائري في المادة 394 مكرر7 من قانون العقوبات :"**يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها**"

أي أن المشرع الجزائري يعاقب على الجرائم المنصوص عليها في المادة 394 مكرر01 ق.ع.ج وهذا لتغطية أكبر قدر من الغش المعلوماتي. كما أن المشرع قد أضفى وصف الجنحة على هته الجرائم ولا عقاب على الشروع في الجنح إلا بنص. أما من خلال نص المادة 394 مكرر5 :" **كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها**"

فقد تبنى المشرع فكرة الاتفاق الجنائي حيث جعل للشروع في الجريمة نفس عقوبة الجريمة التامة[1].

أولا: أركان الشروع.

طبقا للقواعد العامة للقانون الجزائري لا عقاب على الشروع في الجنح إلا بنص، وهذا تطبيقا لنص المادة 31 من ق.ع.ج وتجسيدا لنص المادة 394 مكرر 07 ق.ع.ج تتمثل أركان الشروع في الركن المعنوي (القصد الجنائي) والركن المادي.

1-الركن المادي:

يتكون الركن المادي في جريمة المساس بالأنظمة المعلوماتية من عنصرين هما:

أ- **البدء في التنفيذ:**

في بادئ الأمر يجب الإشارة إلى أن البدء في التنفيذ يختلف عن الأفعال التحضيرية والتي تعتبر أفعال مادية غير معاقب عليها. لكن المشرع الجزائري يعاقب عليها باعتبارها جرائم مستقلة وقائمة بذاتها[2]. فأخضع بذلك كل الأعمال التحضيرية التي تتم في إطار اتفاق جنائي للعقوبة غير أن الأعمال المرتكبة من طرف شخص منفرد غير مشمولة بالنص[3].

---

[1]- د. عطا الله فشار، المرجع السابق، ص 499.

[2]- بوتماني فاطمة الزهراء، مرجع سابق، ص 69.

[3]- دحمان صبايحية خديجة، مذكرة تخرج للطالبة جرائم السرقة والاحتيال عبر الانترنت، كلية العلوم الإسلامية، جامعة الجزائر، 2013، ص 95.

يعاقب على أفعال الشروع التي تمس بمعلومات النظام كمحاولة تغييرها أو محوها أو أي تبادل للمعلومات الهامة لارتكاب الجريمة كالإعلان عن كلمة المرور Mot De Passe أو رمز الدخول[1] Code d'accès.

ب- عدم إتمام الجريمة لظروف خارجة عن إرادة الفاعل:

لكي يكتمل الشروع في جريمة المساس بالنظام المعلوماتي يجب أن يتوفر عنصر ثاني إلى جانب البدء في التنفيذ ويتمثل في وقت التنفيذ في إحدى صوره التالية:

-**الشروع الناقص:** وهو عدول إيجابي عن إتمام الجريمة بشكل اختياري أو إجباري فمثلا إذا بدأ الجاني في التلاعب في البيانات ثم عدل عن فعله فإن الجريمة لا تتحقق ولا يتم توقيع العقوبة.

-الشروع التام:

يقوم الجاني باستعمال كل الطرق والوسائل لتحقيق الجريمة كإدخال برنامج فيروسي لتخريب نظام المعالجة الآلية لكن الجريمة لا تتحقق لأن النظام محمي بتدابير أمنية.

- **الجريمة المستحيلة:** يقوم الجاني بكل النشاط اللازم لتحقيق الجريمة لكن دون جدوى ولا يصل إلى تحقيق النتيجة الإجرامية المرجوة ومن أمثلة ذلك استخدام الجاني لشفرة غير صحيحة للدخول إلى النظام إلا أن صاحب الشفرة يكون قد أنهى تعاقده مع المؤسسة المالكة للنظام.

تعد جريمة الشروع جريمة قصدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة إذ يكون الجاني على علم بخطورة ما يقوم به وما ينجر عنه من عواقب وعلى الرغم من ذلك تنصرف إرادته إلى إتمام الجريمة[2].

الفرع الثاني: الاتفاق الجنائي الخاص للاعتداء على نظام المعالجة الآلية للمعطيات

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وأخذ به المشرع الجزائري في المادة 394 مكرر5 من قانون العقوبات والتي نصت على الاتفاق الجنائي للجنح المنصوص عليها في المواد 394 مكرر و394 مكرر1 والتي تمثل خروجا عن القواعد العامة في العقاب التي تقضي به في الجرائم التامة أو تلك التي تقف عند الشروع[3].

---

[1]- د-عطا الله ، المرجع السابق، ص 499.

[2]- بوتماني فاطمة الزهراء، مرجع سابق، ص 70.

[3]- د.عطا الله فشار ، المرجع السابق، ص 498.

نص المادة 394 مكرر5 من ق.ع:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ، يعاقب بالعقوبات المقررة بالجريمة ذاتها".

وهنا يتضح لنا أن هناك شروطا يجب أن تتوفر في القصد الجنائي وهي:

1- أن يكون اتفاق الجنائي في صورة جماعة لأنه عادة ما ترتكب هذه الجرائم في إطار مجموعات سواء كانت شركة ، مؤسسة أو جماعة من الأفراد قد يعرف بعضهم البعض وقد لا يعرف أحدهم لأخر.

2- يجمع أعضاء الجماعة الهدف الإجرامي وفعل المشاركة.

3- توفر القصد الجنائي والمتمثل في علم وإرادة الجماعة الإجرامية في تحقيق النشاط الإجرامي المتمثل في الاعتداء على النظام المعلوماتي.

عقوبة الاشتراك في القصد الجنائي:

الاشتراك في القصد الجنائي حيث عاقب عليه المشرع الجزائري بعقوبة الجريمة المحضر لها فإن تعددت الجرائم توقع عقوبة الجريمة الأشد[1].

لقد تم تجريم كل أفعال التعدي ضد أي تلاعب بالبيانات والمعطيات من إدخال، محو وتعديل وذلك عن طريق تخصيص عقوبات أصلية وأخرى تكميلية ويستوي إن كان هذا الاعتداء الحاصل من شخص طبيعي أو شخص معنوي كما قام المشرع أيضا بتجريم هذه الشروع في هذه الجنح وكذلك الاتفاق الجنائي[2] الذي يخص التحضير لأي جريمة من جرائم الاعتداء على نظام المعالجة الآلية للبيانات فوضع لها نفس عقوبة الجريمة التامة وفي حالة تعدد الجرائم أخذ المشرع الجزائري بمعيار الجريمة الأشد.

[1]- د.عطا الله فشار ، المرجع السابق، ص 499.

[2]- بوتماني فاطمة الزهراء، مرجع سابق، ص71.

خـــاتمـــة

خاتمـــة:

من خلال دراستنا للحماية القانونية للعقد المبرم عبر الانترنت مجسدة في الحماية المدنية ومتمثلة في الكتابة الإلكترونية، التوقيع الإلكتروني والتشفير أنها تقوم بحماية البيانات أو المعلومات والمعطيات التي يتبادلها المتعاقدان عبر الانترنت فهي عبارة عن حماية وقائية للعقد لا غير أما الحماية الجنائية والتي تحمي نظام المعالجة الآلية بتجريم الاعتداء على السير الحسن للنظام وإحلال عمله فقامت بسن قوانين وضعية للتصدي لهاته الجرائم وردعها وهذا ما دفع بالمشرع الجزائري لأن يقوم بتجريم الاعتداء على النظام المعلوماتي بكل صوره من حلال التعديل الأخير لقانون العقوبات في القسم السابع منه تحت طائلة جرائم المساس بالأنظمة المعلوماتية من خلال المواد 494 مكرر و494 مكرر 1 إلى غاية مكرر 7 وقد ترتب عن هذه الجرائم جزاءات للشخص الطبيعي وأخرى للشخص المعنوي دون الإخلال بمسؤولية الشخص الطبيعي من مرتكبي الجرائم من موظفيه أعضائه أو ممثليه وتتمثل هذه الجزاءات في عقوبات أصلية وأخرى تكميلية تخص جميع أشكال التعدي على النظام المعلوماتي بكل صوره من أفعال الدخول أو البقاء غير المشروع للنظام والاعتداء العمدي على سير نظام المعالجة الآلية فإذا كان هذا الاعتداء غاية في حد ذاته فهو ينصب على المعطيات تحت جريمة التلاعب ببيانات نظام معالجة المعطيات أما إذا كان هذا الاعتداء مجرد وسيلة فهو ينصب على النظام المعلوماتي فقط.

فقد عاقب المشرع الجزائري أيضا على جريمة الشروع في الجريمة والاتفاق الجنائي وفي حالة تعدد الجرائم فقد أخذ بمعيار تطبيق عقوبة الجريمة الأشد.

غير أنه على الرغم من المجهودات الجبارة التي يقوم بها المشرع الجزائري في هذا المجال إلا أن نصوصه تبقى ناقصة ولهذا ارتأينا جملة من التوصيات والاقتراحات:

-إنشاء واستحداث قانون جنائي مختص بالجريمة المعلوماتية مستقل عن قانون العقوبات.

-تكوين خلية بحث وتحري مختصة في مكافحة هته الجرائم كالضبطية القضائية وفرق شرطة متخصصة وتزويدها بالوسائل المادية والتقنية اللازمة لذلك.

الارتقاء بالجهاز القضائي من خلال تكوين قضاة عن طريق دورات تدريبية متخصصة في الجرائم المعلوماتية وإذا اقتضى الأمر الاستعانة بخبراء تقنيين محلفين ومعتمدين لدى المحكمة أو المجلس مختصين في مجال المعلوماتية.

-تكثيف سن المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال.

-إضفاء وصف الجناية على الجرائم المرتكبة على النظام وكل أفعال التعدي بدلا من وصف الجنحة وهذا لخطورة تأثيرها على الأشخاص والممتلكات فهي تمس المال المعلوماتي للأفراد وبياناتهم الشخصية وأسرارهم.

-ضرورة تضافر الجهود الدولية والتعاون والتنسيق بين أعضاء المجتمع الدولي لمواجهة هذه الجرائم من خلال إبرام اتفاقيات تعاون وتسليم المجرمين.

-القيام بمؤتمرات ودورات تحسيسية تمس جميع الفئات من العمر خاصة المراهقين باعتبارهم الأكثر على استخدام شبكة الانترنيت ضمن حملات توعية بخطورة هذا النوع الجديد من الإجرام.

وفي الأخير تجدر بنا الإشارة إلى أن هذه الحماية تبقى غير كافية لتغطية جميع تعاملاتنا عبر الحاسوب خاصة تلك المتعلقة بإبرام العقد عبر الانترنت لسرعة قيام هذه الجرائم فهي متجددة ومتطورة بتطور التكنولوجيات والوسائل الحديثة المستخدمة.

قائمة المصادر والمراجع

أولا: الكتب

1. أحمد خالد العاجولي، التعاقد عن طريق الانترنت، دراسة مقارنة، المكتبة الوطنية، عمان، الأردن، طبعة 2002.
2. إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، 2008.
3. حسن عبد الباسط جمعي، إثبات التصرفات التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة، 2000.
4. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، طبعة 2005.
5. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، طبعة 2006.
6. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة.
7. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية دار الجامعة الجديدة الأزاريطة 2007.
8. سعيد السيد قنديل، التوقيع الإلكتروني ماهيته صوره حجيته في الإثبات، دار الجامعة الجدية، 2004.
9. سمير عبد العزيز جمال، التعاقد عبر تقيات الاتصال الحديثة، دراسة مقارنة، طبعة 1، القاهرة، 2006.
10. شحاتة غريب شلقاني، التعاقد الإلكتروني في التشريعات العربية، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2008.
11. ضياء أمين مشيمش، التوقيع الإلكتروني، دراسة مقارنة، المنشورات الحقوقية، 2003.
12. طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، لبنان، طبعة 1، 2001.
13. عبد الرزاق أحمد الصنهوي، الوسيط في شرح القانون المدني، ج2، منشأة المعارف بالإسكندرية، طبعة 2004.
14. عبد الفتاح بيومي الحجازي، النظام القانون لحماية التجارة الإلكترونية، الكتاب الأول، دار الفكر الجامعي، 2002.
15. علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات، دار الثقافة للنشر والتوزيع، عمان، 2005.

16. محمد أمين الرومي، المستند الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2007.
17. محمد حسن قاسم، التعاقد عن بعد، قراءة تحليلية في التجربة الفرنسية، دار الجامعة الجديدة للنشر، 2005.
18. مصطفى أحمد إبراهيم نصر، وسائل إثبات العقود الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.
19. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2007.
20. ثروت عبد الحميد، التوقيع الإلكتروني، مكتبة الجلاء الجديدة بالمنصورة، 2001.

ثانيا: المذكرات ورسائل الماجستير

1. أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة ابن عكنون، الجزائر، دفعة 2003.
2. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2016.
3. بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة لنيل درجة الدكتوراه، جماعة باتنة، 2014-2015.
4. بوتماني فاطمة الزهراء، الحماية القانونية للعقد المبرم عبر الانترنت، مذكرة لنيل شهادة الماستر.
5. دحمان صبايحية خديجة، جرائم السرقة والاحتيال عبر الانترنت، دراسة مقارنة، مذكرة لنيل شهادة ماجستير، كلية العلوم الإسلامية، جامعة الجزائر، 2013.
6. زينب غريب، إشكالية التوقيع الإلكتروني وحجيته في الإثبات، رسالة لنيل دبلوم الماستر في القانون الخاص، الرباط، 2009-2010.
7. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2013.
8. عتيق حنان، مبدأ سلطان الإرادة في العقود الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون، جامعة البويرة، 2012.
9. غول نجاة، العقد الإلكتروني، مذكرة لننيل شهادة الماستر، جامعة خميس مليانة، 2013-2014.
10. كميني خميسة، منصور عزالدين، الإثبات بالكتابة في الشكل الإلكتروني، مذكرة تخرج لنيل شهادة المدرسة العليا للقضاء، دفعة 16، 2005-2006.

ثالثا: الملتقيات والمؤتمرات

1- عطا الله فشار، الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا أكتوبر 2009، محاضرة، كلية الحقوق والعلوم السياسية، جامعة الجلفة.

2-مختارية بوزيدي ماهية الجريمة الالكترونية، أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد بالجزائر العاصمة، مارس 2017، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر.

ثالثا: النصوص القانونية

- جريدة رسمية عدد 06 المتضمن القانون رقم 04/15 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.
- جريدة رسمية عدد 71 المتضمن القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات.
- القانون المدني رقم 05-10 المؤرخ في 20 يونيو 2005 المعدل والمتمم.
- الأمر رقم 66-156 المتضمن قانون العقوبات المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.
- قانون اليونستيرال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001.

فهرس المحتويات

فهرس المحتويات

كلمة شكر

إهداء

مقدمة ..... أ

الفصل التمهيدي: ماهية العقد الإلكتروني وانعقاده

المبحث الأول: ماهية العقد الإلكتروني 05

المطلب الأول: مفهوم العقد الإلكتروني وخصائصه 05

الفرع الأول: تعريف العقد الإلكتروني 05

الفرع الثاني: خصائص العقد الإلكتروني 08

المطلب الثاني: تمييز العقد الإلكتروني عن باقي العقود 08

الفرع الأول: تمييز العقد الإلكتروني عن العقد التقليدي 08

الفرع الثاني: تمييز العقد الإلكتروني عن العقود المبرمة عن بعد 09

المبحث الثاني: انعقاد العقد الإلكتروني 09

المطلب الأول: التراضي 09

الفرع الأول: التفاوض الإلكتروني 10

الفرع الثاني: تلاقي الإرادتين في العقد الإلكتروني (التراضي) 10

المطلب الثاني: المحل، السبب والشكلية 11

الفرع الأول: ركن المحل 11

الفرع الثاني: ركن السبب 11

الفرع الثالث: ركن الشكلية 12

الفصل الأول: الحماية المدنية للعقد المبرم عبر الانترنت

المبحث الأول: الكتابة الإلكترونية 14

المطلب الأول: ماهية الكتابة الإلكترونية 14

الفرع الأول: مفهوم الكتابة الإلكترونية 15

الفرع الثاني: أهمية الكتابة الإلكترونية وشروطها 16
المطلب الثاني: مبدأ التعادل الوظيفي بين الكتابة التقليدية والكتابة الإلكترونية 18
الفرع الأول: عرض مبدأ التعادل الوظيفي بين الكتابة الإلكترونية والورقية 18
الفرع الثاني: نتائج تطبيق المبدأ 19
المطلب الثالث: حجية العقود الإلكترونية بين الأطراف وفي مواجهة الغير 20
الفرع الأول: حجية العقود الإلكترونية بين الأطراف 20
الفرع الثاني: حجية المحررات الإلكترونية بالنسبة للغير 21
المبحث الثاني: التوقيع الإلكتروني 23
المطلب الأول: ماهية التوقيع الإلكتروني 23
الفرع الأول: تعريف التوقيع الإلكتروني 23
الفرع الثاني: صور التوقيع الكتروني 27
الفرع الثالث: وظائف التوقيع الإلكتروني وشروطه 29
المطلب الثاني: دور التوقيع الإلكتروني في الإثبات ونطاق حجيته 35
الفرع الأول: دور التوقيع الإلكتروني 36
الفرع الثاني: نطاق حجية التوقيع الإلكتروني 37
المطلب الثالث: الحماية القانونية للتوقيع الإلكتروني 38
الفرع الأول: ضوابط حماية التوقيع الإلكتروني 38
الفرع الثاني: أنماط حماية التوقيع الإلكتروني 45

الفصل الثاني: الحماية الجنائية للعقد المبرم عبر الانترنت

المبحث الأول: تطور الحماية الجنائية وتجريم الاعتداء غير المشروع لمواقع التعاقد 55
المطلب الأول: تطور الحماية الجنائية 55
الفرع الأول: تطور الحماية الجنائية على الصعيد الدولي 55
الفرع الثاني: تطور الحماية الجنائية على الصعيد المحلي (الجزائر) 58
المطلب الثاني: تجريم الاعتداء غير المشروع لمواقع التعاقد عبر الانترنت 59
الفرع الأول: تجريم الدخول غير المشروع على نظام المعالجة الآلية للمعطيات

في مختلف التشريعات 59
الفرع الثاني: البقاء غير المشروع في نظام المعالجة الآلية..... 63
الفرع الثالث: الاعتداء العمدي على نظام المعالجة الآلية 65
المطلب الثالث: جريمة التلاعب بنظام المعالجة الآلية 69
الفرع الأول: الأفعال المجرمة التي تمارس على نظام المعالجة الآلية 69
الفرع الثاني: المساس العمدي بالمعطيات خارج النظام 71
المبحث الثاني:العقوبات المقررة لكل جريمة ونطاق تطبيقها 72
المطلب الأول: العقوبات الأصلية المقررة لكل جريمة..... 72
المطلب الثاني: العقوبات التكميلية 74
المطلب الثالث: نطاق تطبيق العقوبة 76
الفرع الأول: الشروع في جرائم الاعتداء العمدي على نظام المعالجة الآلية للمعطيات 77
الفرع الثاني: الاتفاق الجنائي الخاص للاعتداء على نظام المعالجة الآلية للمعطيات 78
خاتـــمة 81
قائمة المصادر والمراجع..... 84

الملاحق