الحماية الجزائية للبيانات الإسمية للمتعاقد في عقود التجارة الإلكترونية

د. طابي ليلى – جامعة باجي مختار – عنابة.

أ. ضيف نوال – جامعة باجي مختار –عنابة.

الملخص :

يقتضي التعامل عبر الأنترنت توافر أدنى حد من متطلبات الأمن، وهو ما اتجهت اليه أغلب التشريعات التجارية الإلكترونية ومن بينها المشرع الجزائري ،الذي سعى جاهدا نحو مواكبة التطورات التقنية الراهنة خاصة ما يتصل منها بالتعامل الإلكتروني في الميدان التجاري بإصدار جملة من التشريعات الهادفة الى تكريس الثقة في التجارة الإلكترونية ضمانا لحماية محل المعاملة التجارية و خصوصيات أطراف العلاقة الناشئة عن هذه المعاملات وأهمها المستهلك الإلكتروني خصوصا ما تعلق ببياناته الإسمية ذات الطابع المعلوماتي.

الكلمات المفتاحية: الوساطة الالكترونية، تسوية منازعات، التجارة الالكترونية، قانون الأونسيترال

Abstract :

Commercial business dealing via the internet requiers the availability of minimum security requirements which is what sought by Most contemporary legislation among them the algerian legislator who strove towards keeping up with current technological developments , especially those related to handling mail in the commercial field, by issuing a series of texts to devote confidence in e-commerce in order to ensure the protection of buiness tranactions acoross these media, especially those related to privacy of the parties in contractual relationship mostly e-consumer.

مقدمة:

ظهرت في أواخر القرن الماضي ما يسمى بثورة تكنولوجيا المعلومات هذه الأخيرة التي أفرزت تطورات لم يسبق لها مثيل في مختلف المجالات حيث أصبح الإنسان وفي اطار مواكبة التقدم العلمي مرغما على التعامل بما تمليه عليه قواعد التكنولوجيا الحديثة وصار استخدام الحاسب الآلي من سمات الحياة العصرية ومتطلبات الخدمات اليومية خاصة في مجال التعاملات الخدماتية على رأسها التجارة الإلكترونية التي يقصد بها المعاملات التجارية التي تتم باستخدام تكنولوجيا المعلومات وشبكات الاتصال الحديث كما عرفتها منظمة التعاون الاقتصادي على أنها جميع المعاملات التجارية التي تتم لبن الشركات أو الأفراد

وتقوم أساسا على التبادل الإلكتروني للبيانات وهذا من شأنه السماح للمستهلك بالولوج الى داخل الأسواق مما ساعد على تحقيق عائد اقتصادي أكبر من الذي حققه النشاط التجاري بشكله التقليدي .

ولكن في مقابل هذا التقدم التكنولوجي بزغ نوع من الإجرام المستحدث حمل في طياته خطورة بالغة على البيانات الشخصية للمستهلك كون أن مثل هذه التعاملات عبر شبكة الأنترنت تلزمه بوضع معلومات تتعلق بحياته الخاصة كبيانات اسمه ومقر اقامته و طبيعة عمله وغيرها من الخصوصيات.

وتستمد هذه الدراسة أهميتها من الضرورة الملحة التي تفرض عل التشريعات الوطنية وضع منظومة قانونية صارمة هدفها مواكبة التطورات العلمية من أجل توفير الحماية لخصوصيات في المستهلك مجال التجارة الإلكترونية باعتباره الطرف الضعيف في مثل هذه التعاملات.

ولقد دفعتنا عدة أسباب لتناول هذا الموضوع من بينها مكانة البيانات الشخصية في مجال البيئة الرقمية والتطورات التي تشهدها هذه الأخيرة مما سهل الإعتداء على تلك البيانات ،وكذلك محاولة دراسة جهود المشرع الجزائري في توفير الحماية الجزائية لبيانات المتعاقد في المعاملات التجارية الإلكترونية من خلال الوقوف على نقاط القوة والضعف في هذه الحماية ، وذلك الإجابة على الإشكالية التالية : "ما مدى كفاية الحماية الجنائية التي فرضها المشرع على بيانات المستهلك في مجال التجارة الإلكترونية؟

المبحث الأول: نطاق الحماية المقررة لبيانات المتعاقد الالكتروني

نظرا للتطور التكنولوجي الهائل في مجال المعلوماتية والاتصالات الحديثة وظهور اجهزة غاية في الدقة هدفها التواصل السريع وتسهيل التعاملات بين الأشخاص خاصة في مجال التجارة الإلكترونية، ومع ازدياد الحاجة الملحة لمثل هذه التعاملات نظرا للمزايا التي تؤديها جعل البعض يستغلها لارتكاب افعال اجرامية مستحدثة تستهدف بالدرجة الأولى البيانات الشخصية للمتعاقد في هذه التعاملات الإلكترونية مما جعل حرمة خصوصياته مهددة بالخطر، ومن ثمة كان لزاما على المشرع الجزائري مواكبة هذا الإجرام المستحدث بتوفير الحماية الجنائية لهذه البيانات من الإعتداء عليها باستحداث منظومة قانونية هدفها تأمين هذه المصالح من خلال تقريره لنصوص تجرم كل سلوك يشكل اعتداء عليها .

المطلب الأول: الحماية الجزائية لبيانات المتعاقد الالكتروني في ظل قانون العقوبات

لقد كرس المشرع الجزائري حماية لبيانات المستهلك الإلكتروني من خلال استحداثه للقسم السابع مكرر من الفصل الثالث من الباب الثاني من الكتاب ثالث لقانون العقوبات المتعلق بتجريم المساس بأنظمة المعالجة الآلية للمعطيات.

الفرع الأول: جريمة الدخول أو البقاء غير المصرح به في نظام المعالجة الآلية للمعطيات

هي من اهم جرائم المعطيات والجرائم المعلوماتية عموما ،ذلك ان اغلب جرائم المعطيات لا يمكن ارتكابها الابعد الدخول للنظام ولهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرى [1] وقد ساعد في انتشار هذه الظاهرة التطورات التكنولوجية في مجال الاتصالات وتنامي شبكات المعلوماتية.[2]

تقوم هذه الجريمة على سلوكين اجراميين احداهما ايجابي وهو الذي يتحقق بفعل الدخول وثانيهما سلوك سلبي يتحقق بالترك او الامتناع وهو الذي يتمثل في البقاء .

أولا: الدخول : ان فعل الدخول في هذه الجريمة لا يقصد به الدخول المادي الى المكان الذي يتواجد به الحاسوب ونظمه بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية الى النظام المعلوماتي اي الدخول المعنوي او الالكتروني.[3]

ومن استقراء نص المادة 394 مكرر يتضح بان المشرع الجزائري لم يحدد المقصود بالدخول غير المشروع الى نظم المعالجة الالية للمعطيات[23] غير أن مدلول كلمة الدخول يشير الى كل الأفعال التي تسمح بالولوج الى نظام معلوماتي والاحاطة او السيطرة على المعطيات والمعلومات التي يتكون منها.[4]

وقد أشار المؤتمر 15 للجمعية الدولية لقانون العقوبات المنعقد في البرازيل الى الدخول غير المرخص به الى الولوج دون ترخيص الى نظام او مجموعة نظم عن طريق انتهاك اجراءات الامن كما لم يحدد كل منهما وسيلة أو طريقة الدخول ، لذا فان الجريمة تقع باي وسيلة فقد يلجأ الجاني الى ادخال برنامج فيروس او يدخل عن طريق استخدام الرقم الكودي لشخص اخر عن طريق تجاوز نظام الحماية اذا كان ضعيفا ويستوي ان يتم الدخول مباشرة او عن طريق غير مباشر كما هو الحال في الدخول عن طريق شبكات الاتصال سواء كانت محلية او عالمية.[5]

ثانيا: البقاء: يعد البقاء الصورة الثانية للسلوك الذي عالجه المشرع الجزائري ضمن المادة 394 مكررو عده سلوك مستقل الى جانب الدخول حيث عبر عنه المشرع بقوله :".....او بقي ....." ، غير أن المشرع الجزائري لم يحدد المقصود بفعل البقاء الا أن الفقه يقصد به البقاء غير المشروع داخل النظام المعلوماتي وهو التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام او من له السيطرة عليه[6]

مما لاشك فيه ان البقاء داخل نظام الكمبيوتر بعد دخوله عن طريق الخطأ لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم ،فاتجاه ارادة الفاعل الى البقاء داخل هذا النظام على الرغم من معرفته انه غير مصرح له بالخول ، لا يختلف في جوهره عن الدخول غير المصرح به الى نظام الكمبيوتر .[7]

فالنتيجة الاجرامية في الحالتين واحدة وهي الوصول الى نظام غير مصرح للدخول اليه فالمصلحة التي يحميها القانون هي حماية نظام الكومبيوتر في الحالتين ، وقد يجتمع الدخول والبقاء غير المشروعين معا وذلك في الفرض الذي يكون فيه الجاني له الحق في لدخول الى النظام ويدخل اليه فعلا ضد ارادة من له حق السيطرة عليه ، ثم يبقى داخل النظام بعد ذلك ويتحقق في هذا الفرض الاجتماع المادي بجريمتي الدخول والبقاء غير المشروعين في النظام الآلي .[8]

ولا يتطلب فعل الدخول والبقاء غير المشروعين حدوث نتيجة اجرامية معينة ضارة لها وجودها المحدد في العالم الخارجي كالحصول على المعلومات او التلاعب فيها او اي شكل من الضرر ، بل يكفي ان يبدأ الجانب بتشغيل نظام المعالجة الآلية ومنذ اللحظة يبدأ هذا الأخير بالعمل اذ يتم ارسال اشارة كهربائية نحو وحدة المعالجة الآلية ومنذ هذه اللحظة يبدأ هذا الأخير بالعمل ، اذ يتم ارسال اشارة كهربائية نحو وحدة المعالجة الآلية المركزية وتقوم هذه الذاكرة بالبحث عن المعلومات التي تسمح بتشغيل النظام المسؤول عن البحث ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة والتي تقوم بمتابعة المراحل اللاحقة وبالتالي فان الدخول الى النظم الآلية بطريقة مباشرة يعد كافي لقيام جريمة الدخول غير المصرح به في قانون العقوبات الجزائري في حق الجاني لتكون هذه الجريمة من الجرائم.
الشكلية التي لا يلزم لتحقيقها تحقق نتيجة معينة منظورة اليها وفقا لمدلولها المادي.[9]

ولكن اذا نتج عن فعل الدخول او البقاء الغير المشروعين نتائج معينة يترتب على ذلك تشديد عقوبة هذه الجريمة وليست كل النتائج محل اعتبار المشرع بل هناك نتائج ثلاثة فقط يترتب عليها هذا الاثر القانوني وهو الحذف او تغيير معطيات او تخريب نظام المعالجة الآلية للمعطيات.[10]

ويعني مصطلح الحذف ازالة المعلومات الموجودة داخل نظام المعالجة الآلية وهو أقصى أنواع الضرر ويتضح من هذا اللفظ مدى جسامة الفعل لم يصل الى التغيير او الاعاقة بل امتد الى الازالة وهو الامر الذي دعى المشرع الى تشديد العقاب بشأنه.[11]

أما مصطلح التغيير فيشير الى احداث تعديلات فقط في المعلومات دون أن يصل الأمر الى حد ازالتها ، بحيث تظل المعلومة موجودة ولمن بدون معنى أو فائدة أو لها معنى ولكنها مغايرة للمعنى الاصلي الذي كانت عليه قبل التغيير[12] .

في حين يعني التخريب ممارسة افعال على نظام المعالجة الآلية للمعطيات من شأنها جعله غير قابل للاستخدام أو الاستعمال[13]، ولتحقق الظرف المشدد لابد من وجود علاقة سببية بين الدخول او البقاء وبين النتيجة المشددة فان حدثت هذه الأخيرة نتيجة لفعل اخر لا يقوم ظرف التشديد.[14]

أما بخصوص الركن المعنوي لهذه الجريمة في صورتها البسيطة فيتطلب توافر القصد الجنائي العام الذي يقوم على العلم أو الارادة أي علم الجاني بأن دخوله الى نظم المعالجة الآلية غير مشروع ولا يستند فيه الى حق قانوني ، وأن تتجه ارادته الى هذا الفعل وفي المقابل لم نجد ما يشير الى اشتراطه نية خاصة لقيام الجريمة ، أما عن الركن المعنوي للجريمة في صورتها المشددة ومن خلال قراءة المادة 394 مكرر من قانون العقوبات يتضح أن الظرف المشدد هو من الظروف المادية التي لا تغير من وصف الجريمة والتي تقوم بمجرد قيام الركن المادي اي ان المسؤولية عن الظرف المشدد هي مسؤولية مادية تقوم بمجرد توافر الركن المادي.[15]

أما عن العقوبات المقررة للجريمة في صورتها البسيطة نصت عليها المادة 394 مكرر و هي الحبس من ثلاثة أشهر الى سنة و غرامة من 50000 الى 100000 دج ، في حين قررت عقوبة الحبس من ستة أشهر الى سنتين و غرامة من 50000 الى 150000 دج هذا في حالة ما ترتب عن الدخول والبقاء غير المشروعين حذف او تغيير للمعطيات، أما اذا أدى الى تخريب النظام فتشدد الغرامة الى 100000الى 200000 دج ، كما رتب المشرع عقوبات تكميلية تتمثل في المصادرة و اغلاق المحل أو مكان الاستغلال اذا ارتكبت الجريمة بعلم مالكها.[16]

الفرع الثاني: جريمة التلاعب بمعطيات الحاسب الآلي

هي الجريمة المنصوص عليها في المادة 394 مكرر1 من قانون العقوبات ومن خلال قراءة نص هذه المادة يتضح وجود ثلاثة أنواع من السلوك الاجرامي وهو فعل الادخال ،فعل المحو، فعل التعديل ولا يشترط أن تقع هذه الافعال مجتمعة بل يكفي ان يقع احداها حتى تقوم الجريمة.

أولا: فعل الادخال: فعل الادخال هو الفعل الذي يتحقق بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية ام يوجد عليها معطيات من قبل ، ويتحقق الادخال كذلك في الفرض الذي يتمكن الحامل الشرعي لبطاقات السحب الممغنطة، والتي تسحب النقود من البنوك وتحدد من اجهزة الحاسب الآلي وذلك حين يستخدم رقمه الخاص السري حتى يسحب مبلغا من النقود اكثر من المبلغ الموجود في حسابه كذلك يتحقق هذا الفرض عند استخدام البطاقة المذكورة من قبل الحامل الشرعي في حالات سرقتها أو فقدانها أو تزويرها ، وكذلك عند ادخال برنامج غريب مثل فيروس حصان طروادة او عن طريق ادخال معلومات تؤدي الى اضافة جديدة.[17]

ثانيا : فعل التعديل: يقصد بتعديل المعطيات تغيير حالتها الموجودة بدون تغيير الطبيعة الممغنطة لها أو هو كل تغيير غير مشروع للمعلومات التي تتم عن طريق استخدام احدى وظائف الحاسب الآلي.[18]

ثالثا : فعل الازالة: تعرف الازالة بانها اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو عن طريق طمسها أي ضغط خصائص أخرى فوقها وهي مرحلة لاحقة على عملية ادخال المعطيات فالإزالة تفترض الوجود السابق لعملية الادخال، ويمكن للمسؤولين عن حفظ البيانات ولو بصورة مبسطة أن يغيروا و يتلفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلي، وذلك عن طريق اتلاف المعلومات أو محوها.[19]

والمشرع لم يشترط في هذه الجريمة تحقق نتيجة معينة كما يقوم الركن المعنوي فيها على القصد العام، وبخصوص العقوبات المقررة لهذه الجريمة فقد نصت عليها المادة 394 مكرر1 من قانون العقوبات و نصت المادة 394 مكرر 6 منها على العقوبات التكميلية.

المطلب الثاني: الحماية المقررة بموجب القوانين الخاصة

سنقوم في هذا المطلب بدراسة القانون الخاصة التي وضعها المشرع الجزائري لحماية البيانات الشخصية المتعلقة بالمتعاقد، هذا لفرض حماية على خصوصياته من الاعتداء عليها اثناء تعاملاته عبر شبكة الأنترنت في اطار التجارة الإلكترونية.

الفرع الأول: الحماية بموجب القانون المتعلق بالوقاية من تبيض الأموال وتمويل الارهاب ومكافحتهما

صدر القانون 05-01 المؤرخ في 2005/2/6 المتعلق بالوقاية من تبيض الأموال وتمويل الارهاب ومكافحتهما بعد تجريم المشرع الجزائري فعل تبيض الأموال وتمويل الإرهاب ومكافحتهما ، وقد جاء هذا القانون بنص يحمي المعطيات الشخصية حيث استعمل المشرع الجزائري و لأول مرة مصطلح المعطيات الشخصية حيث استعمل المشرع الجزائري لأول مرة مصطلح المعطيات الشخصية حيث استعمل المشرع الجزائري و لأول مرة مصطلح المعطيات الشخصية وذلك في نص المادة 26 منه والتي جاء فيها : "يتم التعاون وتبادل المعلومات المذكورة في المادة 25 من هذا القانون في اطار احترام الاتفاقيات الدولية والاحكام القانونية الداخلية المطبقة في مجال حماية الحياة الخاصة وتبليغ المعطيات الشخصية مع مراعاة ان تكون الهيئات الاجنبية المختصة خاضعة لنفس واجبات السر المهني مثل الهيئة المتخصصة " ، وقد قصد المشرع الجزائري المعلومات المتوفرة لدى الهيئة المتخصصة حول العمليات التي يبدو انها تهدف الى تبيض الاموال او تمويل الارهاب.[20]

الفرع الثاني: القانون المتعلق بمكافحة التهريب

أصدر المشرع الجزائري الامر رقم 05-06 المؤرخ في 2005/08/23 المتعلق بمكافحة التهريب ونص هذا القانون على حماية المعطيات الشخصية وقد نصت المادة 38 على انه :" مع مراعاة مبدا

المعاملة بالمثل، وفي اطار الاتفاقيات الثنائية ذات الصلة يمكن للجهات المؤهلة تبليغ الدول المعنية تلقائيا او بناءا على طلبها بالمعلومات المتعلقة بالنشاطات الدبرة او الجارية او المنجزة والتي تشكل قرينة مقبولة تحمل على الاعتقاد بارتكاب او احتمال ارتكاب جريمة تهريب في اقليم الطرف المعني " وقد قصد في مفهوم هذا القانون بالمعلومات وفقا لما ورد في المادة الثانية فقرة (ط) بان المعلومات هي كل المعطيات المعالجة او غير المعالجة المحللة او غير محللة و كل وثيقة او تقرير و كذا الاتصالات الخرى بمختلف اشكالها بما فيها الالكترونية والمعطيات المعالجة و بطبيعة الحال تكون المعالجة الية .[21]

الفرع الثالث: قانون الوقاية من الجرائم المحصلة بتكنولوجيا الاعلام والاتصال

نص المشرع الجزائري بموجب القانون 09- 04 المؤرخ في 2009/080/05 على قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، ويقصد في مفهوم هذا القانون وفقا لنص المادة 02 منه ان الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي جرائم المساس بأنظمة المعالجة المحددة في قانون العقوبات او اي جريمة اخرى ترتكب او يسهل ارتكابها من خلال نصوص قانون العقوبات لم يشر الى جرائم ترتكب عن طريق تقنية المعلومات او رسائل الاتصالات الالكترونية بصفة صريحة ماعدا نصه على جرائم ترتكب عن طريق تقنية المعلومات والتي ذكرها في سياق هذه المادة و بالتالي فنذهب الى ان المشرع الجزائري قد قصد الجرائم التقليدية التي ترتكب عن طريق نظم المعلومات وبطبيعة الحال يتعلق الامر بجرائم المساس بالمعطيات الشخصية للمستهلك الالكتروني.[22]

1- جريمة جمع او معالجة بيانات شخصية دون ترخيص :

تعتبر هذه الجريمة من الجرائم التي تنص عليها تشريعات حماية البيانات الشخصية في اطار مخالفة القائمين بالمعالجة للقواعد الشكلية المنظمة لعملهم والمحددة قانونا ، وتنشأ هذه الجريمة بمجرد مباشرة القائمين على معالجة البيانات الشخصية انشطة المعالجة في الاحوال التي لم يمنح فيها ترخيص من قبل الجهات المختصة المحددة قانونا ،كما تنشا كذلك في الاحوال التي يلغى فيها الترخيص او تنتهي مدته وتستمر جهة المعالجة بنشاطها.[23]

فيعاقب كل من يقوم بإجراء المعالجة الالكترونية للبيانات الشخصية دون اذن من اللجنة المختصة اذ نصت المادة 3 من القانون 09-04 على الحالات التي يمكن اللجوء فيها للمراقبة وتضمنت المادة 11 من المرسوم 15-261 مهام الهيئة و جهة منح الاذن.[24]

ويتحقق هذا االنشاط الإجرامي بجمع البيانات الشخصية من قبل مؤدي خدمات التصديق الإلكتروني دون الحصول على موافقة صاحب الشأن اذ يلزم لقيامها توافر عنصرين هما :

يتمثل العنصر الأول في السلوك الإجرامي المتمثل في جمع البيانات الشخصية خفية أو بصورة غير مشروعة أو معالجة بيانات شخصية تتعلق بشخص طبيعي[25]، كأن يقوم مؤدي خدمات التصديق الإلكتروني بحفظ معلومات شخصية بما يتجاوز الوقت المحدد المتفق عليه.[26]

أما العنصر الثاني يتمثل في عدم موافقة صاحب الشأن حيث يتضح أن القانون يتطلب موافقة صريحة لصاحب شهادة التصديق الإلكتروني يمنحها الى مؤدي خدمات التصديق الإلكتروني لقيام بجمع البيانات الشخصية الخاصة بطالب شهادة الإلكترونية .[27]

الفرع الرابع: الحماية المقررة بموجب القانون 04/15 الخاص بالتوقيع الالكتروني

جاء هذا القانون بحماية خاصة لبيانات المتعاقد الالكتروني اثناء التعاقد من خلال تجريم عدة سلوكات ماسة بالاعتداء على توقيعه الالكتروني من بينها :

1- جريمة حيازة او افشاء او استعمال بيانات انشاء توقيع الكتروني موصوف خاصة بالغير:

تناول المشرع هذه الجريمة في نص المادة 63 من هذا القانون و يقوم السلو ك الاجرامي في هذه الجريمة على ثلاثة صور تتمثل فمايلي :

أ- حيازة اداة انشاء توقيع الكتروني موصوف خاصة بالغير :

وهي حيازة برنامج او نظام معلوماتي لإعداد توقيع الكتروني خاصة بالغير دون موافقة صاحبه والحيازة المشروعة لهذا البرنامج او النظام المعلوماتي لا عقاب عليها طالما ان الشخص مرخص له بهذه الحيازة من الجهة المتخصصة بهدف توثيق هذه التوقيعات طالما لم يثبت ان نيته قد اتجهت الى استخراج توقيع الكتروني رغما عن ارادة صاحبة.[28]

اما الحيازة المعاقب عليها في هذا الصدد فهي حيازة البرامج او النظام المعلوماتي القادر على عمل التوقيع الالكتروني رغما عن ارادة صاحب الشأن والفرض ان حيازة الجاني على برنامج معلوماتي غير مشروعة اي غير مالكه ، وحيث يجب توفر شروط من اجل ممارسة نشاط تقديم خدمات التصديق والا عدت الحيازة للبرنامج او النظام المعلوماتي غير مشروع.[29]

ب- افشاء اداة انشاء توقيع الكتروني موصوفة خاص بالغير :

يكون افشاء اداة انشاء توقيع الكتروني بالتعدي على البيانات المشفرة او فض المعلومات المشفرة التي تخص اداة انشاء التوقيع الالكتروني والتي تكون مرتبطة بأجهزة او برامج معلوماتية معدة لتطبيق بيانات انشاء التوقيع الالكتروني ، ومحاولة الاطلاع على هذه البيانات وافشائها دون اخذ الاذن من طرفي العلاقة الذين اجريا عملية التوقيع الالكتروني التي يفترض فيها السرية ، واقرارا من المشرع

بأهمية هذه السرية التي تطلبها اداة انشاء التوقيع الالكتروني جرم الاعتداء عليها من خلال تجريم الاعتداء على هذه المصلحة بالإفشاء.[30]

ج – استعمال بيانات انشاء توقيع الكتروني موصوفة خاصة بالغير :

ويقصد ببيانات انشاء توقيع الكتروني "بيانات فريدة مثل الرموز او مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الالكتروني "، ووفقا لما جاء في نص المادة 02 الفقرة 03 من قانون 04/15 و غالبا ما تكون هذه البيانات التي تتعلق بالتوقيع الالكتروني مخزنة داخل الحاسوب الالي او قرص منفصلة مثل البيانات المتعلقة باسم صاحب التوقيع و مهنته وكافة بياناته الشخصية و كافة المعلومات بذلك التوقيع و التي يفترض سريتها.[31]

وبالرجوع الى هذه السلوكات نجد انها سلوكات لا تتطلب فيها تحقيق نتيجة اجرامية معينة ولا يتطلب فيها حدوث ضرر فعلي .

اما عن الركن المعنوي لهذه الجريمة فهي من الجرائم العمدية التي تشترط توافر الصد الجنائي العام بعنصريه العلم والارادة.[32]

ولقد قرر المشرع عقوبات لهذه الجريمة في نص المادة 68 من القانون 04/15 حيث العقوبة بحد ادنى متمثل في الحبس بثلاثة اشهر و حد اقصى محدد بثلاثة سنوات حبس، وحدد الغرامة من 100000 دج الى 500000 دج واعطى الحرية للقاضي في النطق بإحدى هاتين العقوبتين كأن تكون العقوبة حبس فقط او تكون غرامة فقط او يكون النطق بكلى العقوبتين اي الجمع بين الحبس و الغرامة معا .

2– جرائم الاعتداء على سرية بيانات التوقيع الالكتروني

نظم المشرع الجزائري الاعتداء على سرية بيانات التوقيع الالكتروني بتجريم جملة من الافعال تتمثل في:

أ– جريمة عدم الالتزام بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الالكتروني الممنوحة:

يتمثل الركن المادي لجريمة الاخلال بأحكام المادة 42 من قانون 04/15 من السلوك الاجرامي المتمثل في عدم حفاظ مؤدي خدمات التصديق الالكتروني على سرية البيانات المعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة، حيث يتضح ان السلوك الاجرامي لهذه الجريمة هو عدم الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة من قبل مؤدي خدمات التصديق الالكتروني التي عهدت اليه في اطار تأدية نشاطه ومن بين احد هذه الوسائل الافشاء الذي يعرف على انه كشف

السر للغير او اطلاعه عليه باي وسيلة كانت وفي غير الاحوال التي يوجب فيها القانون الافشاء او يجيزه.[33]

و لا يشترط لتحقيق فعل الافشاء العلانية لحدوثه ، حيث انه يحدث بمجرد اطلاع شخص عليه او عدة اشخاص، كما يجب ان يتم الافشاء دون رضا صاحب البيانات ذلك ان هذا الرضا في حالة وجوده يزيل عن الفعل صفة الاعتداء ويكون سببا لإباحة فعل افشاء البيانات وان يتم افشاء هذه البيانات للغير الذي لا يكون له الحق في الاطلاع عليها.[34]

اما بخصوص النتيجة الاجرامية فالمشرع لم يتطلب تحقق نتيجة معينة وانما يكفي لقيامها تحقق السلوك المادي ، كما يشترط توافر القصد الجنائي العام .

ولقد عاقب المشرع على هذه الجريمة بنص المادة 70 من القانون 04/15 بعقوبة الحبس من ثلاثة اشهر الى سنتين وبغرامة من 200000 الى 1000000دج او بإحدى هاتين العقوبتين .

ب – جريمة المساس بالبيانات الشخصية:

نظرا لأهمية التي تحملها البيانات الشخصية فإننا نجد معظم التشريعات تسارع لتوفير الحماية لها عن طريق وضع نصوص قانونية تجرم الاعتداء عليها لهذا فان المشرع الجزائري و كغيره سعى لتوفير الحماية لهذه البيانات وهذا ما نستشفه من نص المادة 71 من القانون 04/15 والتي تنص :" يعاقب بالحبس من ستة اشهر الى ثلاث سنوات و بغرامة من 200000 دج الى 1000000 دج او بإحدى هاتين العقوبتين كل مؤدي خدمات التصديق الالكتروني يخل بأحكام المادة 43 من هذا القانون ".

ويتمثل الركن المادي لهذه الجريمة من صورتين:

الصورة الأولى: جمع البيانات من قبل مؤدي خدمات التصديق دون الحصول على موافقة من صاحب الشأن

يتحقق النشاط الاجرامي لهذه الجريمة بجمع البيانات الشخصية من قبل مؤدي خدمات التصديق الالكتروني دون الحصول على موافقة صاحب الشأن اذ يلتزم لقيامها توافر عنصرين هما :

– **العنصر الأول:** يتمثل في جمع بيانات شخصية خفية او بصورة غير مشروعة او معالجة بيانات شخصية تتعلق بشخص طبيعي، كان يقوم مؤدي خدمات التصديق الالكتروني بحفظ معلومات شخصية بما يتجاوز الوقت المحدد المتفق عليه .[35]

– **العنصر الثاني** : يتمثل في عدم موافقة صاحب شهادة حيث يتضح ان القانون يتطلب موافقة صريحة لصاحب شهادة التصديق الالكتروني يمنحها الى مؤدي خدمات التصديق الالكتروني للقيام بجمع البيانات الشخصية الخاصة بطالب شهادة التصديق الالكترونية .[36]

الصورة الثانية: حفظ البيانات الشخصية من قبل مؤدي خدمات التصديق دون موافقة صاحب الشأن.

يتحقق النشاط الاجرامي بقيام مؤدي خدمات التصديق الالكتروني بحفظ معلومات شخصية بما يتجاوز الوقت المحدد والمتفق عليه في نص القانون و ذلك من اجل استعماله في اغراض اخرى وهذا ما جاء في نص المادة 43 من قانون 04/15 .

وتعد هذه الجريمة من جرائم السلوك التي لا تطلب تحقق نتيجة اجرامية معينة ، كما يأخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام بعنصريه العلم و الارادة.[37]

ويعاقب الجاني في هذه الجريمة وفقا لنص المادة 73 من قانون 04/15 بالحبس من ستة اشهر الى ثلاث سنوات و بغرامة من 200000 دج الى 1000000 دج او بإحدى هاتين العقوبتين .

ج- جريمة الكشف عن معلومات سرية مطلع عليها اثناء القيام بعملية التدقيق :

نصت على هذه الجريمة المادة 73 من القانون 04/15 حيث يقوم الركن المادي لهذه الجريمة على السلوك الاجرامي الذي يتمثل في ان يكشف الشخص المكلف بالتصديق على معلومات سرية اطلع عليها اثناء قيامه بالتدقيق .

ويتمثل السلوك الاجرامي لهذه الجريمة في ان يقوم الشخص بالكشف عن معلومات سرية اطلع عليها اثناء قيامه بالتصديق ولقد نص المشرع في القانون 04/15 على السلطات المكلفة بعملية التصديق الالكتروني في الباب الثالث الذي سماه بسلطات التصديق الالكتروني كما حدد مهام كل سلطة منها و هذه السلطات هي:

- السلطة الوطنية للتصديق الالكتروني
-السلطة الحكومية للتصديق الالكتروني
- السلطة الاقتصادية للتصديق الالكتروني

ومن خلال ما ورد في نص المادة 73 من القانون 04/15 نجد ان كل شخص تابع لهذه السلطات والتي تناط بها عملية التصديق و بحكم عملها قد يتحصل احد القائمين عليها على معلومات تتعلق بالتوقيع الالكتروني والذي يفترض فيها السرية من اجل حماية هذا الأخير هذه المعلومات لا يمكن الاطلاع عليها الا من قبل صاحب التوقيع او مقدم خدمات التصديق الالكتروني وذلك بشريطة عدم مساسه بمنظومة التوقيع الا بعد موافقة صاحب التوقيع كما هو وارد في نص المادة 43 من القانون 04/15، الا انه قد يقوم الشخص المكلف بالتصديق و بدون ترخيص بالاستلاء على منظومة التوقيع الالكتروني ويقوم بكشف المعلومات السرية سواء كان ذلك عن طريق النشر او عن طريق الافشاء والمشرع

لم يحدد ماهية المعلومات السرية التي يشكل لكشفها سلوك مجرم معاقب عليها فقد تتعلق هذه المعلومات بيانات الشخصية الخاصة بالموقع او الية انشاء توقيع الكتروني او بيانات التحقق من التوقيع الالكتروني سواء تعلقت بشهادة التصديق الالكتروني او بمؤدي خدمات التصديق .

تتحقق هذه الجريمة بمجرد كشف الشخص المكلف بالتصديق على المعلومات السرية، كما تقوم على القصد الجنائي بحيث لا تقوم الجريمة بطريق الخطأ.[38]

وقد اورد المشرع الجزائري على هذه الجريمة عقوبة الحبس من ثلاثة اشهر الى سنتين و غرامة من 20000 الى 200000 دج او بإحدى هاتين العقوبتين .

المبحث الثاني: آليات حماية بيانات المتعاقد في معاملات التجارة الإلكترونية

نظرا لأهمية البيانات الشخصية للمتعاقد الالكتروني والتي تعبر عن خصوصياته التي لا يجوز للغير الإطلاع عليها الا بإذن منه وبضوابط تحكمها القواعد القانونية و الأعراف الدولية في مجال التجارة الإلكترونية ، سارعت الدول إلى توفير حماية لهذه البيانات عن طريق فرض عدة آليات منها الوقائية التي توفر قبل وقوع الأفعال الإجرامية التي تشكل انتهاكا لتلك البيانات وهذا تجنبا لحدوث أي اعتداء عليها وكذلك آليات اجرائية تحمي تلك البيانات في المساس بها من قبل السلطات المختصة في حالة ما اذا اقتضت ضروريات التحقيق القضائي ذلك .

المطلب الأول: الآليات الوقائية لحماية بيانات المتعاقد الالكتروني

سنتناول في هذا المطلب الآليات الوقائية التي اوجدتها التشريعات في مجال التجارة الإلكترونية لحماية البيانات الشخصية للمتعاقد من الاعتداء عليها ، وهذا مواكبة للتطورات العلمية الحاصلة في مجال تكنولوجيا الاتصالات الحديثة و توفيرا لنوع من الثقة والأمان على هذه التعاملات الإلكترونية .

الفرع الأول: خدمات التأكد من الموقع الالكتروني

لقد ظهرت الخدمات التوكيدية التي هي احدى الخدمات الجديدة التي استحدثتها تقنية المعلومات وانشطة التجارة الالكترونية ، وتهدف هذه الخدمات الى تحسين جودة المعلومات ومحتواها لأغراض اتخاذ القرارات ، ومن خلال هذه الخدمات يضمن المراجع الخارجي جودة المعلومات ويساهم في اعدادها بدل من اصدار تقرير عن معلومات قائمة معدة من قبل ادارة المنشأة ، وهذا من اجل مساعدة مستخدميها في اتخاذ افضل القرارات .[39]

والخدمات التوكيدية هي عبارة عن الاليات والاجراءات الواجب اتباعها لتأمين الحصول على معلومات صحيحة وقد عرفها معهد المحاسبين القانوني الامريكي على موقعه عبر الانترنت

وبشكل يتماشى مع مهنة التدقيق على النحو التالي: " الخدمات التوكيدية عبارة عن خدمات مهنية تحسن من نوعية المعلومات او مداخلاتها والمرغوبة من قبل متخذي القرار.[40]

الخدمات التوكيدية يقوم بها المراجع الخارجي وتهدف الى اضفاء الثقة على موقع العميل على الانترنت حيث قدم كل من معهد المحاسبين الامريكي والمجمع الكندي للمحاسبين القانونيين في عام 1997 خدمة " الويب تروس سيل " لإضفاء الثقة على موقع العميل على الانترنت وما يحتويه من بيانات ومعلومات ، وتضيف هذه الخدمة ضمانا لأمن وسلامة الموقع الالكتروني الموجودة فيه ولكن بدون اضافة اي ضمانات لجودة السلعة او الخدمة المعروضة في ذلك الموقع وهناك خدمة لجودة السلعة او الخدمة المعروضة في ذلك الموقع وهناك خدمة اخرى الى جانب هذه الخدمة تدعى خدمة "سلي تروس " وهي خدمة اضفاء الثقة على نظم المعلومات الالكترونية .

وتهدف هذه الخدمات الى حماية البيانات الشخصية لمستخدمي شبكة المواقع التجارية من سوء الاستخدام ودعم امن وسلامة هذه البيانات .

ولفاعلية الخدمات التوكيدية يتعين توفير المقومات التالية :

– ضرورة التزام الموقع التجاري بمبادئ و معايير خدمة اضفاء الثقة في المواقع المعتمدة.

– ضرورة وجود شركة متخصصة تكون مسؤولة عن وضع ختم الثقة في الموقع التجاري وتوصيل تقرير المراجع عن الموقع للمستخدم اذا ضغط على ذلك الختم .

– قيام مراجع خارجي مؤهل بإعداد تقرير عن المواقع يفيد الالتزام بمبادئ ومعايير خدمة تأكيد الثقة في المواقع والقيام بتلك الاختبارات كل ثلاثة اشهر لتجديد ذلك الختم .[41]

الفرع الثاني: خدمة التوثيق الالكتروني

ان للتوثيق الالكتروني أهمية كبيرة في المجال الالكتروني وتكنولوجيا المعلومات اذ انه يعمل على خلق بيئة الكترونية امنة للتعامل عبر الانترنت فجهات التوثيق الالكتروني تقوم بدور الوسيط المؤتمن بين المتعاملين في التعاملات الالكترونية ومن اهم اختصاصاتها:

أولا : التحقق من صحة البيانات المتداولة عبر الشبكة

تلتزم جهات التوثيق الالكتروني بالتحقق من صحة البيانات المقدمة من الاشخاص المصدر لهم شهادات توثيق و صفاتهم المميزة والتي تمت المصادقة عليها وتضمينها في الشهادة و تستخلص هذه البيانات عادة من الأوراق المقدمة من المشترك كالهوية والشخصية و جواز السفر وغير ذلك من الاوراق الثبوتية المعترف بها .

يتم الحصول على هذه البيانات عبر الاتصال المباشر او بطريق ارسال المستندات الاثباتية بالبريد او الانترنت او بالهاتف ، والمكلف لا يكون مسؤولا الا عن القيد الصحيح في الشهادة للمعلومات المقدمة عن طريق الاشتراك من خلال الاوراق المسلمة وبطاقة التسجيل.[42]

يلتزم المكلف بخدمة التوثيق فقط بفحص هذه المعلومات ويقدر توافقها الظاهري مع المستندات المرسلة او المقدمة من خلال التسجيل الخاص بالعميل ويتفرع على هذا الالتزام التزامات اخرى عديدة اشارت اليها بعض التشريعات تتمثل فيما يلي :

– الحصول على المعلومات ذات الطابع الشخصي من الشخص نفسه او الغير بعد الموافقة الكتابية او الالكترونية للشخص المعني بموافقة صريحة .

– الحصول على المعلومات الضرورية واللازمة لإصدار الشهادة وحفظها .

– عدم استعمال المعلومات خارج اطار انشطة المصادقة مالم يحصل كتابيا او الكترونيا على موافقة الشخص المعني .

–يلتزم بالبيانات المقدمة له وذلك انه يجوز اضافة او حذف البيانات المقدمة له ذلك انه يجوز اضافة او حذف البيانات المقدمة له من قبل اصحاب الشأن او تعديل مضمونها لكي يصدر لهم شهادات تصديق وهذا ما يطلق عليه " معالجة البيانات الالكترونية "اذ يحظر عليه هذه المعالجة.[43]

– ضمان تحديث المعلومات المصدقة اي ان على سلطات المصادقة الحفاظ على صحة المعلومات المصادق عليها وان اقتضى الامر يوميا.

ثانيا : اصدار شهادة توثيقية الكترونية

شهادة التوثيق هي رسالة الكترونية تسلم من شخص ثالث موثوق ، وتكون لها وظيفة الربط بين شخص طبيعي او معنوي وتسمح بتحديد حائز المفتاح الخاص الذي يتطابق مع المفتاح العام المذكور فيها وتحتوي الشهادة على معلومات عن المتعامل (الاسم ، العنوان ، والممثل القانوني بالنسبة للشخص المعنوي واسم مصدر الشهادة والمفتاح العمومي للمتعامل والرقم التسلسلي وتاريخ تسليم الشهادة وتاريخ انتهاء صلاحيتها.[44]

ثالثا : الحفاظ على السرية

ان الحفاظ على السرية من جانب جهات التوثيق الالكتروني تدعم الثقة بين المتعاملين بالوسائل الالكترونية وخاصة وان معظم المعاملات الالكترونية تتم بين اشخاص لا يلتقون و لا يعرف بعضهم بعضا فلولا هذه الضمانات لما اقبل الاشخاص على ابرام العقود واتمام الصفقات.[45]

الفرع الثالث: نظام التشفير

التشفير هو احد فروع العلوم الرياضية كان في الماضي يستخدم في الاغراض الحكومية والعسكرية فقط قبل ان يصبح استخدامه الان في الحياة اليومية بدخول العالم عصر تكنولوجيات المعلومات واحتياجنا لمثل هذا العلم في نامين الشبكات والمعلومات والتشفير هو عملية تغيير في البيانات، ووصل تطوره الى حد امكن للمتخاطبين ضمان ان لا تفك رموز رسائلهم وتعاقداتهم سوى
من طرفهم باستخدام مفتاح فك التشفير او من الجهة التي تملك المفتاح المزود .[46]

والطريقة الشائعة للتشفير تتمثل في وجود مفتاحان المفتاح العام وهو معروف للكافة ومفتاح خاص يتوفر لدى الشخص الذي انشاه ،ويمكن بهذه الطريقة لأي شخص يملك المفتاح العام ان يرسل الرسائل المشفرة ولكن لا يستطيع ان يفك شفرة الرسالة الا الشخص الذي لديه المفتاح الخاص.[47]

وللتشفير اربع مستويات يمكن التمييز بينها على النحو الاتي :

1- الشبكة الافتراضية الخاصة : هي عبارة عن تبادل المعلومات والبيانات بشكل امن على جزء من شبكة الانترنت حيث تتم عن طريق تشفير جميع البيانات والمعلومات من نقطة ارسال الى نقطة الاستقبال

2- نظام "نت سكيب " للتأمين : يعمل هذا النظام على تشفير جميع الاتصالات بين احد برامج التصفح او الوافد لشبكة المعلومات او احد المواقع او مقار المعلومات على الشبكة ، فعندما يرغب احد المستهلكين في التعاقد الإلكتروني عبر الشبكة وعندما يقوم باختيار سلعة معينة يريد التعاقد على شراءها يطلب من الموقع او الصفحة المتعامل معها ان يدخل الى الطريق الامن لإتمام عملية التعاقد وعندما ينتقل الموقع الى المقر الامن يحدث التشفير لجميع قنوان الاتصال والارسال بين برنامج التصفح او نافذ شبكة المعلومات ومقر المعلومات او خادم الشبكة ويستطيع المتعاقد مع الشبكة التأكد من اتمام عملية التشفير عندما يلاحظ ان القفل المفتوح والمبين على الركن الايسر اسفل الشاشة قد تم اغلاقه بعد اختيار الدخول الى الطريق الامن.

ومن عيوب هذا النظام ان بطاقات الائتمان الخاصة بالمتعاقد عبر الانترنت يتم تخزينها لدى المنتج او البائع ولا يخفى على احد مدى الخطورة التي قد يتعرض لها المتعاقد عبر الانترنت اذا استولى احد المحتالين او البائع نفسه على ارقام بطاقة الائتمان وقام باستخدامها لحسابه الشخصي.[48]

3- نظام بروتوكول الاتصال الأمن : يعمل هذا النظام على تامين البيانات والمعلومات اثناء انتقالها بين احد نوافذ الشبكة واحد مقرات المعلومات ويختلف هذا النظام عن نظام "نت سكيب " للتامين في ان النظام الأول يقوم بحماية البيانات المنقولة ذاتها بينما النظام الثاني يقوم بحماية قنوات الاتصال وقد قامت

بعض المؤسسات العاملة في مجال الانترنت بضم النظامين السابقين بروتوكول نظام الأمن ونظام "نت سكيب " للتأمين ليعملا كلاهما بجانب بعض وذلك بغرض توفير اكبر قدر من نظم التأمين للمعاملات الالكترونية التي تتم عبر الانترنت.[49]

4- نظام تامين المعاملات الالكترونية :الهدف من انشاء هذا النظام هو تامين العمليات المالية التي تتم عبر شبكة الانترنت ، ويتطلب هذا النظام ان يفتح كل من المستهلك والمنتج حسابا بنكيا بأحد البنوك التي تستخدم هذا النظام كما يتطلب ايضا استخدام المنتج مقر المعلومات واستخدام المستهلك احد برامج تصفح نوافذ شبكة المعلومات وعند فتح المستهلك للحساب الخاص به يقوم البنك بإرسال كل من شهادة خاصة بالمستهلك مفتاحين للتشفير احدهما عام و اخر خاص ويستخدم احدهما في عملية التشفير و توقيع طلب الشراء ويستخدم الاخر للتوثيق وارسال بيانات عملية الدفع ثم يقوم البنك بتسليم كل من البائع والمشتري الشهادة الدالة على شخصية كل منهم على هيئة ملف من ملفات الحاسبات الالية ليتم بعد ذلك تبادل نسخة من تلك الشهادات بين البائع والمشتري اثناء المعاملة التجارية بصورة مشفرة بحيث لا يستطيع اي شخص من الخارج الاطلاع على تلك البيانات دون المنتج والمستهلك.[50]

الفرع الرابع: المراقبة الإلكترونية

تعرف المراقبة الالكترونية على انها تلك الإجراءات التي تتم عن طريق مراقبة الإتصالات الإلكترونية والتي تكشف في كثير من الأحيان عن أدلة الإلكترونية لإثبات جرائم الكترونية وقد عرف الفقه مراقبة الاتصالات الالكترونية على انها ذلك العمل الذي يقوم به المراقب

باستخدام التقنية الالكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء شخصا او مكانا ،او شيئا حسب طبيعته ، ولقد حدد المشرع الجزائري الحالات التي تسمح باللجوء الى المراقبة الالكترونية بموجب احكام المادة 04 من القانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وهي :

1- للوقاية من الافعال الموصوفة بجرائم الارهاب او التخريب و الجرائم الماسة بأمن الدولة.

2-وفي حالة توفر معلومات عن افعال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني .

3- لمقتضيات التحريات و التحقيقات القضائية ،عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية .

4- في اطار تنفيذ طلبات المساعدة القضائية.[51]

المطلب الثاني: الآليات الإجرائية لحماية البيانات الشخصية للمتعاقد الإلكتروني

أمام التطور التكنولوجي الذي تطورت معه أساليب تنفيذ الجرائم وصعب معه أمر محاربتها والقضاء عليها وجب على المشرع مسايرة التطور نفسه لمجابهة هذا النوع من الإجرام المستحدث الذي يهدد خصوصيات الأفراد ويمس بياناتهم الشخصية غير أن بعض الإجراءات المستحدثة للقيام بالكشف عن مثل هذا النوع الجرائم قد يشكل في حد ذاته اعتداء على تلك البيانات الشخصية في حالة القيام بها دون ضوابط قانونية حددها القانون .

الفرع الأول : تعريف الإجراءات التحري المستحدثة

نصت عليها المادة 65مكرر5 من قانون الإجراءات الجزائية .

أولا: تعريف اعتراض المراسلات

وقد عرفها المشرع في المادة 8من القانون رقم 2000 -03المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ،أهم التعاريف للمصطلحات المتعلقة بالمواصلات السلكية واللاسلكية ويقصد في هذا المفهوم كل المراسلات التي تتم بواسطة جهازي التلغراف والفاكس ، وجهاز الهاتف أو الرسائل القصيرة عن طريق الهاتف المحمول أو جهاز الإعلام الآلي عن طريق البريد الإلكتروني[52].

ثانيا: تسجيل الأصوات

يتمثل في تسجيل الأصوات في وضع الترتيبات التقنية من دون موافقة المعنيين من أجل التقاط تثبيت وتسجيل الكلام المتفوه به بصفة خاصة أو سرية.

الفرع الثاني : الضمانات القانونية للقيام بإجراءات التحري المستحدثة

حصر المشرع هذه الإجراءات في جرائم معينة من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات وذلك في حالة الجريمة المتلبس بها أو التحقيق الإبتدائي وذلك بإذن من وكيل الجمهورية أو قاضي التحقيق موجه لضابط الشرطة القضائية المختص على ان تكون مدة الإجراء محددة ويتم تدوين كل الإجراءات في محضر مع ذكر تاريخ وساعة بداية ونهاية الإجراء .

الخاتمة :

من خلال ماتم عرضه في موضوع دراستنا اتضح لنا بأن المشرع الجزائري قد قام بحماية البيانات الشخصية للمتعاقد في المعاملات التجارية الإلكترونية من خلال النصوص العامة المتعلقة بحماية المعطيات الإلكترونية في جرائم المعلوماتية وذلك في نصوص قانون العقوبات وكذا بعض القوانين الخاصة التي حمت البيانات الشخصية للأفراد عبر الشبكات الإلكترونية 09-04 المتعلق بالوقاية من الجرائم المتصلة

بتكنولوجيا الإعلام و الإتصال ، والقانون 15-04 المتعلق بالتوقيع الإلكتروني ، ولكنه لم يفرد قانون خاص بحماية المتعاقد الالكتروني بصفة عامة وبياناته الشخصية بصفة خاصة في اطار التجارة الإلكترونية.

الهوامش:

1. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الطبعة الاولى ،2008، ص156.
2. نهلا عبد القادر، المرجع السابق، ص158.
3. خليفة محمد، المرجع السابق، ص138.
4. نهلا عبد القادر، المرجع السابق، ص159.
5. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية –دراسة نظرية وتطبيقية – ، منشورات الحلبي الحقوقية ،بيروت ،الطبعة الأولى 2005،ص336.
6. نهلا عبد القادر، المرجع السابق ، ص 162.
7. مسعود ختير ، الحماية الجنائية لبرامج الكمبيوتر ،دار الهدى ،عين مليلة ، الجزائر ،2010، ص116.
8. أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة ، الجزائر ، الطبعة الثانية ،2007، ص 113.
9. رشيدة بوكر ،جرائم الإعتداء على نظام المعالجة الآلية في التشريع الجزائري والمقارن ، منشورات الحلبي الحقوقية ، بيروت ،الطبعة الأولى ، 2012،ص229.
10. محمد خليفة ، المرجع السابق ،ص160.
11. محمد خليفة، المرجع نفسه ،ص161.
12. رشيدة بوكر ،المرجع السابق ،ص230.
13. رشيدة بوكر ،المرجع نفسه ،ص241.
14. محمد خليفة ، المرجع السابق ،ص161.
15. رشيدة بوكر ، المرجع السابق ، ص241.
16. محمد خليفة ، المرجع السابق ،ص 171.
17. عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر والأنترنت في التشريعات العربية ، دار النهضة العربية ، الإسكندرية ، 2002، ص 496.
18. محمد خليفة ، المرجع السابق ، ص183.
19. عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر والأنترنت في التشريعات العربية ، المرجع السابق ،ص40.
20. أنظر المرسوم التنفيذي رقم 02-127 المؤرخ في 2002/4/7 والمتضمن انشاء خلية معالجة الإستعلام وتنظيمها وعملها ، المنشور في الجريدة الرسمية رقم 47 المؤرخ في 2006/07/19.
21. دنيا زاد ثابت ،الحماية الجنائية للحق في حرمة الحياة الخاصة في التشريع الجزائري والمقارن ، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم ، تخصص القانون الجنائي والعلوم الجنائية ،جامعة باجي مختار ، عنابة ، 2016، ص397 .
22. دنيا زاد ثابت ، المرجع نفسه ،ص ص 394،395.
23. بولين أنطونيوس أيوب ،الحماية القانونية للحياة الشخصية في مجال المعلوماتية –دراسة مقارنة –،الطبعة الأولى ،منشورات الحلبي الحقوقية ،لبنان ، 2009،ص414.
24. دنيا زاد ثابت ،المرجع السابق ،ص400.
25. بولين أنطونيوس أيوب ، المرجع السابق ، ص 414.

26. دنيا زاد ثابت ، المرجع السابق ، ص400.
27. دنيا زاد ثابت ، المرجع السابق ،ص400.
28. لالوش راضية ،أمن التوقيع الإلكتروني ، مذكرة ماجستير في القانون العام ،كلية الحقوق ، جامعة مولود معمري ، تيزي وزو ،2012،ص154.
29. لالوش راضية ،المرجع نفسه ،ص154.
30. بلحسني حمزة ، الحماية القانونية والفنية للتوقيع الإلكتروني في مجال البيئة الرقمية ،مجلة العلوم القانونية والإدارية ، العدد الحادي عشر ،2015، ص82.
31. لالوش راضية ، المرجع السابق ، ص 154.
32. حمزة بلحسني ،المرجع السابق ،ص84.
33. أسامة بن عمر محمد عيلان ،الحماية الجنائية لسر المهنة في الشريعة الإسلامية والقوانين الوضعية وتطبيقاتها في بعض الدول العربية ،مذكرة لنيل درجة الماجستير ، كلية الدراسات العليا قسم العدالة الجنائية ، جامعة نايف للعلوم الأمنية ، الرياض ، 2004، ص103.
34. صالح شنين ،الحماية الجنائية للتجارة الإلكترونية ، أطروحة لنيل شهادة الدكتوراه في القانون الخاص ، كلية الحقوق ،جامعة أبوبكر بلقايد ، تلمسان ، الجزائر ، 2003،ص120
35. خالد بن عبد الله بن معيض العبيدي ،الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية –دراسة تحليلية مقارنة– ،مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا ، الرياض ، 2009، ص99.
36. صالح شنين ، المرجع السابق ، ص 206.
37. عبد الفتاح بيومي حجازي ، مقدمة في التجارة الإلكترونية و العربية ، ص 277.
38. حمزة بلحسيني ، المرجع السابق ،ص 89.
39. نصيرة خلوي ، الحماية القانونية للمستهلك عبر الأنترنت –دراسة مقارنة – ،رسالة مقدمة لنيل شهادة الماجستير في القانون ،تخصص المسؤولية المهنية ،جامعة مولود معمري ، تيزي وزو ، كلية الحقوق ، 2013،ص158.
40. نعيم دهمش وظاهر القشي ، مدى ملائمة مهنة المحاسبة للتجارة الإلكترونية ، مجلة أربد للبحوث العلمية ، المجلد الثامن ،العدد الثاني ، جامعة اربد الأهلية ، عمان ، 2004، ص12.
41. نصيرة خلوي ، المرجع السابق ، ص 159.
42. نصيرة خلوي ،المرجع نفسه ، ص 159.
43. نصيرة خلوي ، المرجع نفسه ،ص 160.
44. وسيم شقيق الحجار ، الإثبات الإلكتروني ، الطبعة الأولى ، مكتبة ناشرون ،بيروت ،2002،ص217.
45. نصيرة خلوي ، المرجع السابق ،159.
46. محمد أمين الرومي،جرائم الكومبيوتر والأنترنت ،دار المطبوعات الجامعية ،الإسكندرية ، 2004،ص29.
47. عبد الفتاح بيومي حجازي ،جرائم الكمبيوتر والأنترنت في التشريعات العربية ، المرجع االسابق ،ص75.
48. عبد الفتاح بيومي حجازي،المرجع نفسه،ص84.
49. محمد أمين الرومي ، المرجع السابق ،ص32.
50. خلوي نصيرة،المرجع السابق،ص159.
51. دنيا زاد ثابت ،المرجع السابق ، ص 493.
52. بن ذياب عبد المالك ،حق الخصوصية في التشريع الجزائري ،مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص العلوم الجنائية ،جامعة الحاج لخضر ، باتنة ،الجزائر ،2013،ص 139.