جامعة محمد الصديق بن يحي – جيجل
كلية الحقوق والعلوم السياسية
قسم الحقوق

حماية البيانات الشخصية في مجال التجارة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر في القانون الخاص
تخصص: قانون خاص للأعمال

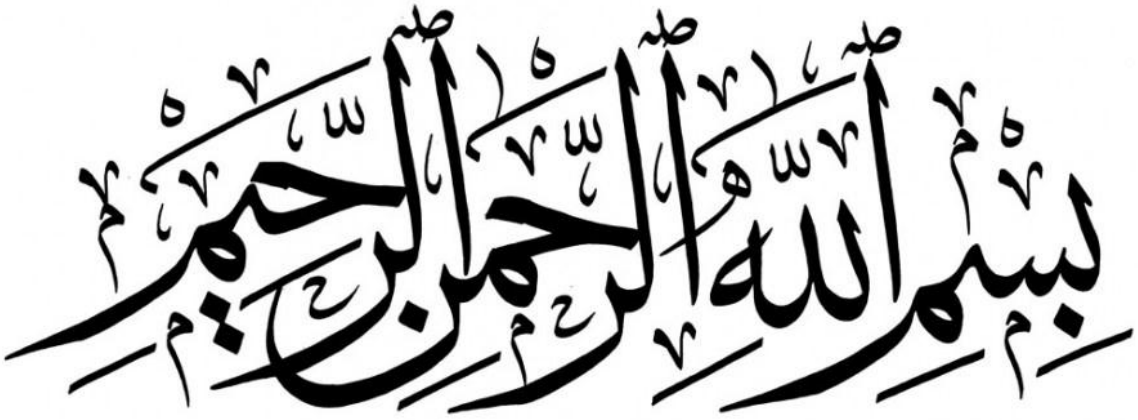
إعداد:
الطالبة: بودوشة أميرة
الطالبة: شاكر سميرة

إشراف :
أ/ بلجودي أحلام

لجنة المناقشة:

اللقب والاسم	الرتبة العلمية	الجامعة	الصفة
عبد الله ليندة	أستاذة مساعدة "أ"	محمد الصديق بن يحي– جيجل	رئيسا
بلجودي أحلام	أستاذة مساعدة "أ"	محمد الصديق بن يحي– جيجل	مشرفا ومقررا
نشناش مونية	أستاذة مساعدة "أ"	محمد الصديق بن يحي– جيجل	ممتحنا

السنة الجامعية 2016-2017


بسم الله الرحمن الرحيم

شكر وتقدير

نشكر الله عز وجل الذي أنعم علينا بنعمة العلم ويسر لنا إتمام هذا العمل المتواضع.

نتقدم بشكرنا وعرفاننا وبالغ امتناننا لأستاذتنا الكريمة " **بلجودي أحلام**" على توجيهاتها القيمة وصبرها علينا طيلة إنجاز هاته المذكرة.

كما نتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة على تقبلها مناقشة هاته المذكرة

كما نتقدم بالشكر لكافة هيئة التدريس بقسم الحقوق.

إلى كل من ساعدني من قريب أو بعيد في إنجاز هذا العمل.

.

أُمِيرَةَ، سَمِيرَةَ

إهداء

أهدي هذا العمل المتواضع إلى من قال الله سبحانه وتعالى في شانهما

"وقضى ربك ألا تعبدوا إلا أياه وبالوالدين إحسانا"

الوالدين الكريمين

إلى إخوتي وكل أفراد العائلة

إلى كل الأصدقاء

إلى كل من ساعدني في إنجاز هذا العمل من قريب أو بعيد

أميرة، سميرة

قائمة المختصرات

أولا: باللغة العربية

ص: ..... الصفحة

ص ص: ..... من الصفحة إلى الصفحة

ط: ..... الطبعة

د ط: ..... دون طبعة

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

ج ر:..... جريدة رسمية

ق. ع. ج:..... قانون العقوبات الجزائري

ق. م. ج:..... القانون المدني الجزائري

ثانيا: باللغة الأجنبية

P : .....Page

N° :.....Numéro

SSL : .....Secure Socket Layers

SET : .....Secure Electronic Transactions

مقدمة

ألقى التقدم العلمي والتكنولوجي الذي شهدته البشرية في العصر الحديث بظلاله ونتائجه على كافة جوانب الحياة والعلاقات بين الأفراد، وقد برزت هذه التكنولوجيا لتحدث ثورة حقيقية في كل مناحي الحياة اليومية كالتجارة والتعليم وغيرها، ومن أهم أدوات هذه التكنولوجيا ما يعرف بشبكة الأنترنت، والتي تعد من أحدث التقنيات التي شهدها العقد الأخير من القرن العشرين.

فالأنترنت بمثابة موسوعة علمية تقدم خدمات متنوعة في كافة أنحاء العالم وفي كل المجالات، وقد أثرت على نشاطات القطاعات الاقتصادية، وأحدثت الكثير من التغيرات في المفاهيم المعروفة الاقتصادية منها والقانونية، وقد استفادت النشاطات التجارية باعتبارها من أهم دعائم القطاع الاقتصادي من مزايا هذه التطورات التكنولوجية، وتمخض عن ذلك ميلاد التجارة الإلكترونية وبروزها إلى الساحة الدولية[1].

يقصد بالتجارة الإلكترونية المعاملات التي تتم باستخدام تكنولوجيا المعلومات وشبكات الاتصال، وقد عرفتها على المستوى الدولي، المنظمة العالمية للتجارة بأنها "عبارة عن عمليات إنتاج وترويج وبيع وتوزيع للمنتجات من خلال شبكة الاتصال"[2].

أما على المستوى الوطني فإن أغلب التشريعات لم تتضمن تعريفا للتجارة الإلكترونية منها التشريعات العربية، باستثناء البعض كالتشريع التونسي الذي عرفها في الفصل 02 من قانون المبادلات والتجارة الإلكترونية التونسي الصادر في 11 أوت 2000 بأنها "العمليات التجارية التي تتم عبر المبادلات الإلكترونية[3].

اكتست التجارة الإلكترونية أهمية كبيرة على الساحة الدولية، مع التوجه المتزايد للكثير من دول العالم نحو الاعتماد عليها في ممارسة نشاطاتها وأعمالها التجارية، نظرا لما تتميز

---

[1] صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013، ص1.

[2] كما عرفتها الجمعية الأمريكية للتجارة الإلكترونية تعريفا واسعا بأنها "مجموعة الاستعمالات لوسائل الاتصال".
أنظر: مرجع نفسه، ص1.

[3] مرجع نفسه، ص2.

من مزايا عديدة جعلت الإقبال عليها يتزايد وينمو يوما بعد يوم، حيث تمتاز بسهولة إنجاز العمليات التجارية في وقت قصير وبأقل جهد وأدنى تكاليف، إذ وفرت التقنيات الحديثة ميزة السرعة في التعاقد والتنفيذ وخفض تكاليف الاتصالات[1].

كما أن توفر معلومات متكاملة عن الأسواق في كافة أنحاء العالم، يتيح إمكانية مقارنة أسعار السلع والخدمات في الداخل والخارج وبالتالي زيادة المنافسة بين المؤسسات أما على المستوى الوطني فإن التجارة الالكترونية تؤدي إلى رفع درجة الانفتاح الاقتصادي من خلال دعم التجارة الخارجية والتنمية الاقتصادية والقطاعات التكنولوجية[2].

بالرغم من هذه المزايا والنقلة النوعية التي أفرزتها ثورة الاتصالات في العالم، إلا أن التجارة الإلكترونية لا تخلو من العيوب، التي أدت إلى ظهور مشاكل عملية وقانونية، تتمثل أساسا في صعوبة التأكد من هوية المتعاملين في التجارة الإلكترونية نظرا لغياب العلاقة المباشرة بين الأطراف، كما أن غياب التعامل الورقي يهدد مصالح العملاء والبنوك، نتيجة إمكانية حدوث تزوير في البيانات أو التلاعب بالفواتير والمستندات عند الطلب[3].

وتحمل التجارة الالكترونية العديد من التأثيرات الجانبية التي أبرزت مشاكل حقيقية ترتبط أساسا بمسألة الأمن المعلوماتي، فهناك الكثير من التهديدات المعلوماتية التي قد تطول البنى التحتية، والتي قد تشكل مخاطر حقيقية على الخصوصية[4]، حيث أن الواقع العملي أثبت عدم قدرة شبكات الاتصال على توفير الأمان المطلق لسرية ما ينقل عبرها من بيانات، وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة على المعلومات.

---

(1) صالح شنين مرجع سابق، ص3.

(2) كريمة صراع، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، تخصص استراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2013-2014، ص23.

(3) المرجع نفسه، ص25.

(4) يقصد بالخصوصية حق الشخص في أن يتحكم بالمعلومات التي تخصه، وقد جرى التعامل معها كحق لمنع إساءة إستخدام البيانات التي تعالج آليا أو إلكترونيا.

أنظر: منى تركي الموسوي، "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها"، مجلة العلوم الاقتصادية، كلية بغداد للعلوم الاقتصادية، العراق، عدد خاص، 2013، ص307.

فمنذ ظهور الأنترنت تزايدت عمليات نقل البيانات، وهو ما أثار معه مسألة كيفية توفير السرية لهذه البيانات وحمايتها، والصعوبة تتعلق بالنواحي الفنية الخاصة بتكنولوجيا المعلومات والبرمجيات وأنظمة التشغيل، فإذا كان هناك نقص في الأمان، فإن هذا يمهد الطريق للتدخل في خصوصيات الآخرين وكشف أسرارهم واختراق النظم المعلوماتية.

والخصوصية بصفة عامة هي مقياس غير موضوعي يختلف تعريفها وحدودها من شخص إلى آخر، فهناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان، مثل الاسم والعنوان ورقم الهاتف وغيرها، فهي معلومات تأخذ شكل بيانات تلزم الالتحاق بكل شخص طبيعي[1].

ولأن الحق في خصوصية المعلومات لا تتأتى إلا من خلال حماية البيانات نظرا للترابط القائم بينهما، ارتأينا أن تنصب الدراسة على موضوع حماية البيانات الشخصية في مجال التجارة الإلكترونية، خاصة وأن معظم المجتمعات الديموقراطية عملت على كفالة الخصوصية واعتبرته حقا دستوريا مستقلا بذاته.

وقد اعترف المؤسس الدستوري الجزائري بهذا الحق، وقرر له حماية خاصة، كما منح لصاحبه حق اللجوء إلى القضاء في حال الاعتداء على حياته الخاصة، وأكثر من ذلك فقد خص التعديل الدستوري لسنة 2016[2]، بالذكر حماية المعطيات ذات الطابع الشخصي في مجال المعلوماتية، واعتبرها من بين الضمانات الأساسية لحماية الحق في الخصوصية، حيث تنص المادة 46 منه، على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

---

[1] منى تركي الموسوي، المرجع السابق، ص.ص 4 – 5.

[2] مرسوم رئاسي رقم 96–843 مؤرخ في 7 ديسمبر 1996،يتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء 28 نوفمبر سنة 1996 في الجريدة الرسمية للجمهورية الجزائرية الديموقراطية ،جريدة رسمية عدد 76، صادر في 8 ديسمبر سنة 1996، المعدل و المتمم .

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطباع الشخصي حق أساسي يضمنه القانون ويعاقب عليه."

وتطبيقا لذلك نصت المادة 47 من القانون المدني[1] على الحقوق الملازمة للشخصية، كما جاء في المواد 303 و303 مكرر من قانون العقوبات[2] على أنه في حالة الاعتداء على البيانات الشخصية للشخص واستعمالها لأغراض لا تخص صاحبها تعتبر جريمة يعاقب عليها القانون.

وإن اختيار هذا الموضوع يرجع لأسباب عدة تعود أساسا إلى قلة الدراسات التي تناولته باللغة العربية وخاصة في الجزائر، ضف إلى ذلك غياب إطار تشريعي وتنظيمي متكامل[3] ينظم المعاملات التجارية الالكترونية بصفة عامة، وحماية البيانات الشخصية المتداولة من خلالها بصفة خاصة، بالرغم من انتشارها الواسع، وما نتج عنه من آثار سلبية على مصالح المتعاملين، وكذا الصعوبات الجمة التي يلقاها المتعامل في مجال التجارة الالكترونية في الجزائر، لتخطي ما قد يضر به بسبب الاعتداء على بياناته الشخصية.

وينطوي موضوع حماية البيانات الشخصية في مجال التجارة الالكترونية على أهمية بالغة من جوانب عدة نظرية وعملية، فمن الناحية العملية تظهر أهمية الموضوع في أن الواقع الذي نعيشه يؤكد تزايد التعامل عبر شبكة الأنترنت عن طريق تبادل المعلومات

---

[1] أمر رقم 75-58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج ر عدد 78، صادر في 30 ديسمبر 1975، المعدل والمتمم.

[2] أمر رقم 66-156 مؤرخ في 1 جوان 1966، يتضمن قانون العقوبات، ج ر عدد 102، صادر في 4 جوان 1966، المعدل والمتمم.

[3] ومع ذلك جاء القانون رقم 15-04 المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر عدد 06، الصادر في 10 فيفري 2015، كخطوة غاية في الأهمية في طريق بناء نصوص متكاملة تنظم التجارة الالكترونية، وهو لفتة مهمة من المشرع تعلن عن تبني فكرة المعاملات الالكترونية.

والمعطيات الشخصية، تستلزم هذه الأخيرة وجود وسائل تقنية وأخرى قانونية تمنع الوصول إليها بطريقة غير شرعية، والإحاطة بكل المخاطر التي قد تنجم عن العملية التجارية التي تتم عبر الوسائط الإلكترونية، بالإضافة إلى ضمان الحماية الكافية لهذه البيانات من العوائق الفنية والتقنية التي تمهد الطريق أمام مخترقي النظم المعلوماتية.

فمتى أحس المتعامل بأن بياناته الشخصية في مأمن من أيدي العابثين، فإنه يقدم على إجراء معاملاته إلكترونيا بكل ثقة وهذا لن يتحقق إلا من خلال توافر الوسائل التي يمكن من خلالها تحقيق أمن التجارة الإلكترونية وكذا خصوصيتها.

أما من الناحية النظرية فتكمن أهمية الموضوع في البحث عن أحكام خاصة تحمي البيانات الشخصية للمتعاملين في مجال التجارة الإلكترونية، والتعرف على مفاهيم قانونية جديدة تتعلق بالمعاملات المعالجة إلكترونيا، حتى ينتشر الفهم الصحيح والإدراك الجيد لخبايا مثل هذه المعاملات، خاصة وأن اللجوء إلى المعاملات الإلكترونية أصبح ضرورة في بعض الحالات لا خيار فيها.

ويطرح الموضوع محل الدراسة إشكالية عامة تنشأ من متغيرين متناقضين:

– الأول يتعلق بأهمية التجارة الإلكترونية، واعتبارها وسيلة لا يمكن الاستغناء عنها نظرا لما توفره من ازدهار للتجارة وتنمية للاقتصاد الوطني، مما يستوجب تحريرها من القيود والإجراءات التي قد تعيقها.

– أما المتغير الثاني فلا يتعلق بحداثة التجارة الإلكترونية، وانما في الوسائل المستخدمة فيها والتي يمكن ان تؤدي إلى الاعتداء على الحياة الخاصة، مما يستوجب تدخل المشرع لوضع الحلول القانونية لمختلف الإشكالات التي قد يثيرها التعامل عبر الوسائط الإلكترونية بصفة عامة، والأمن المعلوماتي بصفة خاصة.

ولذلك فإن الإشكال العام الذي يطرح في هذا الشأن يتعلق: بما مدى كفاية وفعالية الأحكام المقررة في التشريع الجزائري لحماية البيانات الشخصية في مجال التجارة

الإلكترونية، مع ما يفرضه الواقع العملي من الاتجاه نحو التوسع في استخدام التكنولوجيا في مجال المبادلات التجارية، خاصة الدولية منها؟

نظرا لخصوصية هذا الموضوع وأهميته وحداثته، وبهدف الإلمام بمختلف جوانبه ولبلوغ الغاية من الدراسة، اعتمدنا على المناهج التالية:

- **المنهج الوصفي:** الذي من خلاله بينا المفاهيم المتعلقة بحماية البيانات الشخصية في التجارة الإلكترونية.

- **المنهج التحليلي:** والذي استعنا به لتحليل بعض المواد القانونية المتعلقة بهذا الموضوع، فيما يتعلق بتحديد مدى كفاية النصوص المقررة في التشريع الجزائري

كما اعتمدنا على المنهج المقارن في حالات محددة، عند الإشارة إلى أحكام التشريعات المقارنة الأجنبية منها أو العربية، المتعلقة بموضوع الدراسة

ولأن مسألة حماية البيانات الشخصية في مجال التجارة الالكترونية تظهر على مستويين، مستوى وقائي، يتعلق بالعمل على تحقيق الأمن المعلوماتي، والآخر علاجي، يهدف إلى توفير الوسائل القانونية الكفيلة التي تمكن المعني من المطالبة بحقوقه في حالة وقوع تعدي على بياناته الشخصية، فقد تم تقسيم الدراسة إلى فصلين اثنين كما يلي:

الفصل الأول: تحت عنوان إجراءات أمن البيانات الشخصية في مجال التجارة الإلكترونية، والذي قسم بدوره إلى مبحثين، حيث خصص المبحث الأول منه لدراسة الوسائل التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية، في حين تضمن المبحث الثاني الوسائل القانونية لأمن البيانات الشخصية في مجال التجارة الإلكترونية.

أما الفصل الثاني فجاء تحت عنوان وسائل الحماية القانونية للبيانات الشخصية في مجال التجارة الإلكترونية، قسم هذا الأخير إلى مبحثين خصص المبحث الأول لدراسة وسائل الحماية الجزائية للبيانات الشخصية في مجال التجارة الإلكترونية، أما الثاني فقد تضمن وسائل الحماية المدنية للبيانات الشخصية في مجال التجارة الإلكترونية.

الفصل الأول

إجراءات أمن البيانات الشخصية في مجال التجارة الإلكترونية

المبحث الأول: الوسائل التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

المبحث الثاني: الوسائل القانونية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

إن من نتائج التعامل عبر الأنترنت ظهور وسائل غش واحتيال تتجاوز حدود الدول، تعرض الأطراف لمخاطر الاعتداء والاختراق من طرف القراصنة، الأمر الذي دفع مؤيدي التجارة الإلكترونية بشكل عام، إلى العمل على وضع إجراءات أمنية لحماية البيانات ذات الطابع الشخصي.

يعرف أمن البيانات بأنه حماية وتأمين لكافة الموارد المستخدمة في معالجة البيانات، حيث يتم تأمين هذه الأخيرة عن طريق إتباع إجراءات ووسائل حماية عديدة، تضمن في النهاية سلامة خصوصية الأطراف المتعاملة عبر الشبكة [1] .

ويعتبر أمن البيانات أحد عوامل نجاح التجارة الإلكترونية، من خلال استصحاب عنصري الثقة والأمان، إلى رغبة توفير الحماية القانونية والخصوصية المعلوماتية في بيئة التعامل الإلكتروني، بهدف حماية الأطراف من احتمال عمليات الاختراق.

ولتحقيق الأمن للبيانات الشخصية للأطراف، تم العمل على توفير وسائل تقنية تكفل الحماية اللازمة ضد جميع المخاطر التي قد تنجم عنها خسائر مادية ومعنوية للأطراف (المبحث الأول)، كما استجابت التشريعات لضرورات تحقيق الأمن المعلوماتي، من خلال تكريس مجموعة من الإجراءات القانونية في سبيل تحقيق هذا الغرض (المبحث الثاني).

[1] حسين محمد الحسن، الإدارة الإلكترونية، ط1، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2011، ص158.

المبحث الأول: الوسائل التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

بسبب زيادة الاختراقات المرتكبة عبر شبكة الأنترنت والتي تؤدي إلى المساس بخصوصية وسرية البيانات المتبادلة عبر شبكة الأنترنت والمرتبطة بالأشخاص، فإنه كان لابد من إيجاد وسائل تقنية تضمن أكبر قدر من الحماية والسرية للبيانات الشخصية، بعض هذه الوسائل عبارة عن أنظمة توفر حماية للبيانات وهي مخزنة (المطلب الأول)، والبعض الآخر منها عبارة عن برامج تحمي خصوصية وسرية البيانات أثناء تداولها (المطلب الثاني).

المطلب الأول: الأنظمة التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

تم منذ فترة البحث عن أنظمة تقنية يتم من خلالها تبادل البيانات بشكل آمن ومستقر، ومن نتائج هذا البحث التوصل إلى استخدام تشفير البيانات، وفي الحقيقة هذا النظام استخدم منذ القدم في تشفير الرسائل في الحروب خوفا من وقوعها في أيدي العدو[1] واستمر البحث على تطوير هذه التقنية تماشيا مع التطورات التكنولوجيا الحاصلة، مما أدى بالتشريعات العربية والأجنبية بالإقرار بشرعية التشفير التي تتم على البيانات الشخصية للأطراف المتعاملة في إطار التجارة الإلكترونية [2].

وسيتم التركيز على نظام التشفير باعتباره من أهم الوسائل التقنية لمنع الاعتداء على البيانات الشخصية في مجال التجارة الالكترونية، من خلال تحديد تعريف له (الفرع الأول) وضوابطه (الفرع الثاني)، وأخيرا دوره في حماية هذه البيانات (الفرع الثالث).

الفرع الأول: مفهوم نظام التشفير

بسبب أهمية الدور الذي يؤديه التشفير فيما يتعلق بحماية البيانات المعالجة الكترونيا فقد كانت الحاجة ماسة لتوضيح مفهومه، من خلال تعريفه وتحديد أنواعه.

---

[1] أنظر: محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية(دراسة مقارنة)، (د ط)، دار الثقافة للنشر والتوزيع، عمان، الاردن، 2011، ص158.

[2] لورنس محمد عبيدات، إثبات المحرر الالكتروني، ط1 ، دار الثقافة للنشر والتوزيع ، عمان، الاردن، 2009، ص135.

أولا- تعريف التشفير:

بالرغم من أن نظام التشفير هو نظام تقني بحث، إلا أن بعض التشريعات تعرضت لتعريفه كنظام أساسي تقوم عليه معاملات التجارة الالكترونية، كما اجتهد الفقه في وضع تعريفات معينة لهذا النظام.

1- التعريف الفقهي للتشفير:

عرف بعض الفقهاء التشفير بأنه عملية الحفاظ على سرية المعلومات الثابتة منها والمتحركة، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء، لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة [1].

في حين عرفه البعض الآخر بأنه عملية تحويل النص إلى رموز وإشارات غير مفهومة لمنع الغير من الاطلاع عليها، إلا الأشخاص المرخص لهم بالاطلاع على النص المشفر وفهمه، إذ تنصب عملية التشفير على القيام بتحويل النصوص العامة إلى نصوص مشفرة، مع إمكانية إعادة النص المشفر إلى شكله الاصلي بعد فك التشفير[2].

فالتشفير عبارة عن عملية رياضية يتم من خلالها تحويل النص المراد إرساله إلى رموز وإشارات غير مفهومة إلا بعد القيام بفك الشفرة وتحويل الرموز والإشارات إلى نص مقروء، من خلال استخدام مفاتيح التشفير العامة والخاصة[3].

2- التعريف التشريعي للتشفير:

أ- في القانون الجزائري:

لم يتضمن القانون رقم 15-04 المتعلق بالتصديق والتوقيع الالكترونيين، تعريفا للتشفير، واكتفى المشرع من خلال الفقرتين 8 و9 من المادة 02 من هذا القانون، بإعطاء

---

[1] عبد الفتاح محمود الكيلاني، المسؤولية المدنية الناشئة عن المعاملات الإلكترونية عبر الأنترنت، (د ط)، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2011، ص263.

[2] محمد فواز المطالقة، مرجع سابق ، ص159.

[3] المرجع نفسه، ص159.

تعريف غير مباشر للتشفير، من خلال تعريف كل من مفتاح التشفير الخاص ومفتاح التشفير العام ، حيث عرفت الفقرة 8 من المادة 2 مفتاح التشفير الخاص بأنه "هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي".

أما مفتاح التشفير العمومي "فهو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".

ويستنتج من خلال هاذين التعريفين أن التشفير الإلكتروني عملية أو تقنية تستخدم لحماية البيانات في إطار المعاملات الإلكترونية، بحيث يكون في شكل رموز غير مفهومة إلا لصاحبها، والذي يملك وحدة مفتاح فك التشفير.

ب- في القانون التونسي:

عرف المشرع التونسي التشفير وحدد مفهومه في الفصل الثاني من الباب الأول من القانون التونسي رقم 83 لسنة 2000 في شأن المبادلات والتجارة الالكترونية، حيث نص على أنه "استعمال رموز أو إشارات غير متداولة، تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها"[1].

ج- في القانون الفرنسي:

تضمنت المادة 27 من القانون الفرنسي 90 - 1170 الصادر بتاريخ 19 ديسمبر 1990 تعريف التشفير بأنه: "كل الأعمال التي تهدف إلى تحويل المعلومات أو إشارات واضحة باستخدام وسائل مادية أو معالجة آلية إلى معلومات أو إشارات غامضة

[1] قانون المبادلات والتجارة الالكترونية رقم 83-2000 الصادر في 9 أوت 2000 منشور في الموقع الالكتروني: Kaisdali/.over.blog.com/2014/03pdf-pdf-pdf.html.

للغير أو إلى إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض"[1]، وقد سمح هذا القانون للمشروعات الصغيرة والأفراد باستخدام التشفير بعد أن كان مقصورا على المجالات العسكرية والحكومية فقط[2].

ثانيا – أنواع التشفير:

تتعدد أنواع التشفير وتختلف باختلاف الوسيلة المستخدمة في عملية التشفير، كما تختلف أنواعه كذلك من حيث مستوى الاستخدام.

1 – التشفير من حيث الوسيلة المستخدمة:

تقسم أنواع التشفير حسب هذا المعيار إلى ثلاث أنواع تتمثل في:

أ – التشفير باستخدام المفتاح المتماثل:

يقصد بالمفتاح المتماثل المفتاح الذي يقوم على وجود مفتاح واحد من أجل تشفير البيانات وكذلك حل التشفير، وهو النظام المعروف بالسيمتري[3]، ذلك أن مصدر الرسالة والمرسل إليه يتعاملان بمفتاح تشفير واحد لفك رموز الرسالة التي لم توصل بعد، حيث يرسل المفتاح أولا بطريقة آمنة إلى المرسل اليه، ثم ترسل الرسالة مشفرة بطرق الاتصال العادية، وهذه الطريقة تستخدم مجموعة من الأرقام العديدة والمعقدة، التي تجعل من الصعب تزويرها[4].

وقد أخذ على هذا النظام أنه غير آمن، لأن مرسل المعاملة أو البيانات ومستقبلها لهما نفس المفتاح، وأنه لا يحتوي على صيغة من حيث أسلوب تبادل رموز هذه المفاتيح

---

(1) EYNARD Jessica, Les données personnelles (quelle définition pour un régime de protection efficace ?), Michalon Editeur, Paris, France, 2013, p273.

(2) راضية لالوش، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص98.

(3) عبد الفتاح محمود الكيلاني، مرجع سابق، ص365.

(4) عبد الفتاح بيومي حجازي، التجارة عبر الأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص45.

بين الأطراف، وأن استخدام ذات المفتاح من قبل المرسل والمرسل إليه لا يوفر الحماية اللازمة لتأمين البيانات[1].

ب- التشفير باستخدام المفتاح اللامتماثل:

إن طريقة استخدام المفتاح المتماثل لا يمكن أن تصلح لجميع عمليات التجارة الإلكترونية أي استخدام نفس المفتاح مع آلاف الزبائن، حيث يصبح المفتاح غير سري، ولهذا ظهر استخدام التشفير غير المتماثل، بحيث يقوم على وجود مفتاحين أحدهما مفتاح عام معلوم لبعض الجهات وسري بالنسبة للجمهور، ومفتاح خاص غير معروف لأي جهة غير الشخص الموجهة إليه البيانات لحل الشفرة[2].

ويتميز المفتاح العام عن المفتاح الخاص في كونه معروفا أو متاحا إلكترونيا لطرفين أو أكثر، غير أن هذا التمييز الذي يخص المفتاح العام لا يفصله عن المفتاح الخاص لأنهما مترابطان في عملهما، فإذا استعمل المفتاح الخاص لتشفير الرسالة فلا يمكن فك التشفير إلا بالمفتاح العام، كما أنه لو عرف أحد المفتاحين فلا يمكن معرفة الآخر حسابيا[3].

وعلى الرغم من أن هذا النظام أفضل وأكثر أمنا إلا أنه يحتاج إلى وقت أكثر في القيام بعملية التشفير وفكها، والتي يجب أن تتزامنا في الغالب، كما أنه لا يتمتع بدرجة عالية من الأمن، فمن المتوقع أن تتم عملية الاختراق إذا توفر ما يلزم من وقت ومال[4].

---

[1] عبد الفتاح محمود الكيلاني، مرجع سابق، ص377.

[2] خضر مصباح الطيطي، التجارة الإلكترونية والأعمال الإلكترونية،(د ط). دار الحامد للنشر والتوزيع، عمان، الأردن، 2008، ص 235.

[3] راضية لالوش، مرجع سابق، ص98.

[4] محمد فواز المطالقة، مرجع سابق، ص164.

ج- المزج بين نظامي المفتاح المتماثل والمفتاح اللامتماثل:

وهو خليط بين نظام التشفير المتماثل وغير المتماثل السابقين[1]، وفيه يتم تشفير الرسالة بمفتاح خاص، ثم تشفير المفتاح الخاص بمفتاح عام، وإرسال كل من الرسالة المشفرة والمفتاح الخاص المشفر إلى المرسل إليه باستخدام أي شبكة اتصالات[2].

ويمر هذا النظام بمجموعة من المراحل، والتي تبدأ بترميز البيانات باستخدام المفتاح المتماثل، وكذلك يتم استخدام المفتاح العام للمرسل إليه في تشفير هذا المفتاح المتماثل، يتم بعد ذلك إرسال كل من الرسالة المرمزة والمفتاح المشفر إلى المستقبل، هذا الأخير يحل التشفير باستعمال مفتاحه الخاص ليتحصل على المفتاح المتماثل في فك تشفير النص واسترجاع البيانات والمعلومات الاصلية[3].

ويهدف هذا النظام إلى تفادي عيوب النظامين السابقين، من خلال ضمان قدر كافي من الأمن والحماية للبيانات بأقل تكلفة وفي أقصر وقت ممكن، أي دون استخدام قدرات كبيرة لتحقيق درجة التشفير المطلوبة[4].

2- التشفير من حيث مستوى الاستخدام:

توجد عدة أنواع للتشفير من حيث الاستخدام فقد يكون التشفير على مستوى الإرسال (أولا) وقد يكون التشفير على مستوى التنقل أو التصفح (ثانيا) كما قد يكون التشفير على مستوى التطبيق (ثالثا) وأخيرا التشفير على مستوى الملفات (رابعا).

---

[1] عبد الفتاح محمود الكيلاني، مرجع سابق، ص367.

[2] عبد الفتاح بيومي حجازي، التجارة عبر الانترنت، مرجع سابق، ص46.

[3] سمية ديمش، التجارة الإلكترونية حقيقتها وواقعها في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم الاقتصادية، تخصص تحليل واستشراف اقتصادي، كلية العلوم الاقتصادية وعلم التسيير، جامعة منتوري، قسنطينة، 2011، ص85.

[4] عبد الفتاح بيومي حجازي، التجارة عبر الانترنت، مرجع سابق، ص46.

أ- التشفير على مستوى الإرسال:

يستخدم هذا النوع من التشفير لتأمين كل ما يمر عبر وصلات الاتصال عند نقطة الإرسال، ويتم حل الشفرة عند نقطة الاستقبال، ومن نماذج تطبيقاته ما يسمى بالشبكات الخاصة المؤمنة[1].

ب- التشفير على مستوى التصفح:

يستخدم هذا المستوى في تشفير البيانات التي يتم تداولها، وبالتالي يتم تشفير جميع الاتصالات بين نوافذ الشبكة أو المواقع الموجودة عليها، مما يؤدي إلى حماية البيانات أثناء انتقالها، ومن تطبيقات هذا النظام نظام (نيت سكيب) لتأمين المقاييس، وكذلك نظام تأمين برتوكول الاتصال، فبمجرد وصول المعلومات إلى مقر المعلومات يتم حل الشفرة، ويعد هذا النظام الأكثر انتشارا[2].

ج- التشفير على مستوى التنفيذ:

يستخدم كتطبيق خاص لتشفير البيانات، كما يتم استخدامه للتشفير الجزئي، ومن نماذج تطبيقاته نظام تأمين المعاملات الإلكترونية، وكذلك نظام المحفظة الإلكترونية[3].

د- التشفير على مستوى الملفات:

يتم التشفير هنا على مستوى الرسائل الإلكترونية والملفات التي يتم تداولها، حيث يتم تشفير البيانات التي تحتويها الرسائل باستخدام أسلوب المفتاح العام، ويتميز هذا النظام أو البرنامج بسهولة استخدامه، وفي نفس الوقت صعوبة الهجوم عليه، يقوم التشفير هنا على

---

[1] عبد الفتاح بيومي حجازي ،التجارة عبر الانترنت ،مرجع سابق، ص35.

[2] عبد الفتاح محمود الكيلاني، مرجع سابق، ص380.

[3] وتقوم المحفظة الالكترونية على استخدام بطاقة المعالجات الدقيقة، والتي تعبر عن قيم مالية تستخدم مباشرة في الدفع في حدود مبلغ محدد مدفوع مسبقا، فيتم تخزينها أو شحنها بالمبلغ المدفوع داخل البطاقة مزودة بذاكرة إلكترونية.
أنظر: أحمد سفر، أنظمة الدفع الإلكترونية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006، ص 82.

استخدام المفتاح الملائم لحل الشفرة، وأي تجربة لمفتاح آخر يعتبر من المهام المستحيلة التي لا يمكن أن تنجح[1].

الفرع الثاني: ضوابط التشفير

على اعتبار أن التشفير هو تحويل البيانات إلى رموز لا يتمكن أحد من قراءاتها إلا إذا قام باستخدام رموز التشفير، فهو يقوم على ضوابط يجب مراعاتها عند القيام بعملية التشفير، تتمثل في مشروعية تشفير البيانات (أولا) وكذلك احترام سرية البيانات المشفرة (ثانيا) كما يجب استخدام التشفير بواسطة السلطات المختصة (ثالثا).

أولا- مشروعية تشفير البيانات:

إن تقنية التشفير لم يتم إيجادها بداهة، بل كانت نتيجة عدة دراسات وأبحاث، حيث تبنت أغلب التشريعات التي قامت بوضع قوانين خاصة بالتجارة الإلكترونية والتوقيع الإلكتروني، نظام التشفير الإلكتروني وذلك بصفة مباشرة أو غير مباشرة[2].

ويقصد بمشروعية عملية التشفير أن يتم في إطار القانون، وبما تسمح به النصوص القانونية المطبقة، وبالرغم من أن المشرع الجزائري لم يتولى معالجة مبادئ التشفير في القانون 15-04 بشكل مباشر، حيث اكتفى بتعريف مفتاح التشفير العام والخاص فقط، بخلاف ما عليه الحال في التشريع التونسي ومشروع قانون التجارة الإلكترونية المصري، اللذين عالجا التشفير بشكل مباشر في نصوص خاصة بهما[3]، إلا أن هذا النص كاف على الأقل للقول بمشروعية عملية التشفير، وباعتراف المشرع الجزائري بجواز استعماله كآلية لحماية التوقيع الالكتروني.

---

[1] راضية لالوش، مرجع سابق، ص103.

[2] لورنس محمد عبيدات، مرجع سابق، ص137.

[3] عبد الفتاح بيومي حجازي، التجارة عبر الانترنت، مرجع سابق، ص38.

ثانيا – احترام سرية البيانات المشفرة:

اعتبر المشرع الاعتداء على البيانات المرسلة عبر الأنترنت اعتداء على خصوصية طرفي المعاملة، لأن البيانات التي يتم تبادلها بين الطرفين خاصة بهما، وتعبر عن إرادتهما في القيام بتصرف قانوني، فالاطلاع من قبل الغير على هذه البيانات من الممكن أن يؤدي إلى إلحاق الضرر بطرفي المعاملة باقتحام حريتهما والاعتداء على خصوصيتهما، بمعرفة البيانات التي تم كشفها بعد فك التشفير[1].

أكد المشرع على احترام سرية البيانات المعالجة الكترونيا، ومنها المشفرة، وعاقب كل من يقوم أو يحاول الاعتداء عليها سواء كان ذلك من خلال محاولة فك الشفرة أو الاطلاع على محتوى البيانات، وذلك بوضع نصوص في قانون العقوبات تعاقب من يقوم بانتهاك البيانات المشفرة وإفشاء سريتها[2].

ثالثا – استخدام التشفير بواسطة السلطات المختصة:

يتمثل الضابط الثالث في أن استخدام التشفير كتقنية في نطاق المعلومات والبيانات يجب أن يكون بواسطة الجهات المختصة التي يحددها القانون، والسبب في ذلك أن عمليات التشفير ترتبط بمعلومات هامة وسرية، سواء تعلق ذلك بالحكومة الإلكترونية، أو تعلق بالتجارة الإلكترونية للأفراد كتطبيق لهذه الحكومة الإلكترونية، أو تعلق بالأسرار الخاصة بالأفراد.

---

[1] محمد فواز المطالقة، مرجع سابق، ص161.

[2] حيث نصت المادة 394 مكرر 2 من الأمر رقم 66–156، المتضمن قانون العقوبات، المعدل والمتمم، على أنه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات بغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

2– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم...".

وسيكون لنا تفصيل في هذا الموضوع من خلال الفصل الثاني من هذه الدراسة.

لذلك فإن عمليات التشفير تتعلق بشكل أو بآخر باعتبارات ترتبط بالنظام العام، لذلك فإن الجهات المشرفة على عمليات التشفير يراعي فيها أن تكون جهات حكومية[1]، وهي في التشريع الجزائري السلطة الاقتصادية للتصديق الإلكتروني، تعين هذه الأخيرة من قبل السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية[2]. وتتولى السلطة الاقتصادية للتصديق الإلكتروني القيام –على الخصوص– بالمهام التالية:

– إعداد سياستها الاقتصادية والسهر على تطبيقها بعد أخذ الموافقة من السلطة الوطنية.

– نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة الوطنية.

– إرسال المعلومات للسلطة الوطنية دوريا أو بطلب منها.

– التحقق من مطابقة طالبي التراخيص مع سياسة التصديق أو عن طريق مكاتب تدقيق معتمدة.

– إصدار التقارير والإحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطها مع احترام مبدأ السرية.

– التحقق من مطابقة طالب التراخيص مع سياسة التصديق الالكتروني.

– إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني وعرضه على السلطة للموافقة عليه[3].

الفرع الثالث: دور التشفير في حماية البيانات ذات الطابع الشخصي للأفراد

تبرز أهمية التشفير من خلال القيام بحماية المعاملات والبيانات التي يتم تداولها من خلال شبكة الانترنت وذلك جراء استخدام أفضل أساليب التشفير[4].

وعن طريق هذه التقنية يمكننا توفير الحماية اللازمة وتجاوز الكثير من المخاطر، فبواسطتها نتجنب:

---

[1] عبد الفتاح بيومي حجازي، التجارة عبر الانترنت، مرجع سابق، ص41.

[2] أنظر المادة 29 من القانون 15–04، مرجع سابق.

[3] انظر المادة 30 من القانون 15–04، مرجع سابق.

[4] محمد فواز المطالقة، مرجع سابق، ص161.

- الاطلاع على المعلومات المحظورة السرية أو الشخصية.
- محاولة تعديل البيانات المنقولة بالشبكة.
- إعادة توجيه البيانات إلى وجهة أخرى.
- تغيير محتويات الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستفيدين.
- انتحال شخصية المستخدم الحقيقي.
- تعديل الحسابات المخزنة على الحسابات نفسها[1].

كما يعمل نظام التشفير على منع الغير من الدخول والتقاط رسائل البيانات التي يتم تبادلها من خلال شبكة الأنترنت، سواء كانت تتضمن أرقام بطاقات الائتمان، أو بعض البيانات الخاصة[2].

ويرفع التشفير الحماية ودرجات الأمان بشكل يحقق الثقة بها، ويشجع على استعمالها والدخول إلى عالم المعلوماتية دون خوف او تردد[3]، كما ويهدف التشفير إلى حماية البيانات وضمان وصولها للطرف الآخر غير مشوهة، فهو يسعى إلى وصول الرسالة سليمة من أي خلل واعتداء على البيانات[4].

المطلب الثاني: البرامج التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

إن أهم ما يهدد المعاملات التجارية الإلكترونية هو أمن البيانات وتأمين عملية تداولها عبر الأنترنت، الأمر الذي أدى إلى ضرورة وجود برامج تقنية تهدف إلى الحفاظ على سرية وخصوصية البيانات الشخصية من مخاطر القرصنة، ومن أهم هذه البرامج نجد

---

[1] يوسف واقد، النظام القانوني للدفع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011، ص98.

[2] لورنس محمد عبيدات، مرجع سابق، ص135-136.

[3] يوسف واقد، مرجع سابق، ص98.

[4] محمد فواز المطالقة، مرجع سابق، ص158.

بروتوكول الطبقات الأمنية (فرع أول)، بروتوكول المعاملات المالية الآمنة (فرع ثاني)، الجدران النارية (فرع ثالث).

الفرع الأول: بروتوكول الطبقات الأمنية

طور هذا البرنامج من طرف شركة نت سكيب [1](Net Scape) التي ساعدت على زيادة الثقة في التجارة الإلكترونية ومستوى الأمان فيها، حيث قامت معظم الشركات المنتجة لمتصفحات الأنترنت إلى الأخذ بها[2]، وفيما يلي سنعرض هذا البرنامج (أولا) وطريقة العمل به (ثانيا) وخطوات استخدامه (ثالثا).

أولا- تعريف بروتوكول الطبقات الأمنية (SSL):

SSL برنامج يحتوي على بروتوكول متخصص لنقل البيانات والمعلومات المخزنة بين جهازين، عبر شبكة الأنترنت بطريقة آمنة، حيث لا يمكن قراءتها إلا من طرف المرسل والمستقبل[3].

يتم استخدام بروتوكول SSL في عمليات التسوق الإلكتروني وتبادل المعلومات الحساسة، فعندما يظهر مفتاح أو قفل في أسفل شاشة المتصفح، فهذا يعني أن المتصفح قد أقام اتصال مشفر وآمن مع المستخدم، وأنه بالإمكان إرسال المعطيات أو البيانات الشخصية بأمان، كتفاصيل بطاقات الاعتماد[4].

ثانيا- طريقة عمل بروتوكول الطبقات الأمنية SSL:

يقوم برنامج SSL بربط المتصفح الموجود على جهاز العميل (المستخدم) بجهاز الخادم الخاص المراد الشراء منه، وهذا طبعا إذا كان مزودا بهذه التقنية أساسا، ويقوم هذا

---

[1] Net Scape هي شركة خدمات حاسوب أمريكية على خلفية مستعرض الويب، الذي طورته تحت اسم نث سكيب، والذي سيطر لفترة من الزمن، ثم فقد معظم حصته، أنظر: كريمة صراع، مرجع سابق، ص76.

[2] المرجع نفسه، ص77.

[3] إبراهيم بختي، دور الأنترنت وتطبيقاته في مجال التسويق، رسالة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2003، ص134.

[4] ناصر خليل، التجارة والتسويق الإلكتروني، (د ط)، دار أسامة للنشر والتوزيع، الأردن، 2009، ص223.

البرنامج بتشفير أي معلومة صادرة عن ذلك التصفح، وصولا إلى جهاز الخادم باستخدام بروتوكول الأنترنت[1].

إذ أن مهمة بروتوكول الطبقات الآمنة SSL هي تأمين اتصال أمن فقط، حيث لا يقوم بحماية المعلومات بعد تخزينها على المستخدم.

ثالثا – خطوات استخدام بروتوكول الطبقات الأمنية SSL:

تتم عمليات تبادل المعلومات باستخدام بروتوكول SSL وفقا للخطوات التالية:

1– يقوم الموقع بالتقدم إلى إحدى الهيئات المستقلة، التي تصدر شهادة رقمية تثبت هوية وصحة الموقع، وبعد تأكد الهيئة من نشاط وحسن سيرة هذا الموقع، تقوم بإصدار شهادة رقمية له تدون فيها معلومات خاصة بالموقع، مثل اسم الشركة وتاريخ إصدار وانتهاء الشهادة، وكذلك يتم إصدار المفتاح العام والخاص للموقع[2].

2– عند دخول زائر الموقع للصفحة الآمنة التي يدخل فيها البيانات والمعلومات للشراء، يقوم المتصفح المزود بهذا البرنامج بالجهاز الخادم الأمن للموقع الذي يطلب منه: الشهادة الرقمية مصدرها، تاريخ انتهائها للتأكد من مصداقية الموقع علما أن هذه الخطوات تتم بواسطة المتصفح لديك دون علمك أو تدخلك وبعد التأكد يقوم المتصفح بإعلامك بالتطابق أو عدمه وبعض الملاحظات إن وجدت[3].

3– بعد التأكد، يقوم المتصفح بإعلام الموقع بالتطابق أو عدمه، في حالة التطابق يصبح بالإمكان استخدام المفتاح لتشفير كافة المعلومات على قناة الاتصال التي تم إنشائها[4].

---

[1] كريمة صراع، مرجع سابق، ص77.

[2] المرجع نفسه، ص 77.

[3] المرجع نفسه، ص 78.

[4]. إبراهيم بختي، مرجع سابق، ص 135.

الفرع الثاني: بروتوكول المعاملات المالية الآمنة SET

بالإضافة إلى بروتوكول الطبقات الأمنية، ظهر ما يعرف ببروتوكول المعاملات المالية الآمنة، وسيتم التطرق إلى تعريف بروتوكول المعاملات المالية الآمنة (أولا) وأهدافه (ثانيا) وأخيرا طريقة عمله (ثالثا).

أولا- تعريف بروتوكول المعاملات الإلكترونية الآمنة SET:

SET عبارة عن بروتوكول تم تطويره من قبل الشركتين فيزا وماستر كارد، كطريقة آمنة لإجراء المعاملات والتحويلات المالية عبر الأنترنت والشبكات[1]، ووظيفته الأساسية هي توفير الأمان لمدفوعات البطاقات والتجار والبنوك[2].

تتضمن عملية الشراء وفقا لبروتوكول الحركات المالية الآمنة SET خمسة أطراف: حامل البطاقة، موفر المحفظة الإلكترونية، التاجر، معالج عمليات الدفع، بوابة الدفع.

حامل البطاقة هو شخص لديه حساب بطاقة ائتمانية لدى فيزا أو ماستر كارد، يستخدم هذا الشخص محفظة إلكترونية تحتوي شهادات رقمية لبروتوكول الحركات المالية الآمنة SET، وحامل البطاقة هو زبون في هذه العملية.

أما موفر المحفظة الإلكترونية فهو المؤسسة المالية التي تزود الزبائن بالأدوات التي تتيح بشكل آمن شراء البضائع والخدمات عبر الأنترنت ومن هذه الأدوات الشهادات الرقمية أو شهادات بروتوكول الحركات المالية الآمنة SET.

أما التجار فهم الشركات والأفراد الذين يعرضون البضائع والخدمات عبر الأنترنت، كي يتمكن هؤلاء التجار من التجاوب مع الحركات المالية التي يقوم بها الزبائن لابد لهم من الارتباط بعلاقة مع معالجي عمليات الدفع أو مؤسسات مالية معتمدة أخرى[3].

---

[1] خضر مصباح الطيطي، مرجع سابق، ص240.

[2] سمية ديمش، مرجع سابق، ص92.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، الطبيعة القانونية للعقد الإلكتروني، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص . ص165-166.

ومن أطراف هذه العملية كذلك معالج عمليات الدفع التي قام بها الزبائن، وأخيرا بوابة الدفع وهي الجهاز الذي يستغله معالج عمليات الدفع[1].

ثانيا – أهداف بروتوكول المعاملات المالية الآمنة SET:

يسعى بروتوكول المعاملات المالية الآمنة إلى تحقيق مجموعة من الأهداف تتمثل في: – ضمان الحفاظ على أمن البيانات (خصوصيتها، وسلاستها والتحقق من وصولها إلى الجهة المطلوبة أثناء إجراء الحركات المالية)[2].

– يرفع من مستوى موثوقية كافة المعطيات المرسلة إلكترونيا من خلال استخدام نظام خاص وسري.

– قيام هذا البروتوكول بتوثيق معطيات حامل بطاقة الاعتماد والتحقق من هوية المستخدم الحقيقي للبطاقة، والتأكد في نفس الوقت من موثوقية البائع عبر الأنترنت، وإمكانية القيام بالدفعات المالية له عن طريق طرف ثالث، كمؤسسة مالية مختصة.

– يستخدم بروتوكول SET أفضل تقنيات التصميم وإجراءات الأمن لحماية المستهلكين والباعة والشركات، التي تقوم بالتبادلات التجارية وإبرام العقود على الأنترنت[3].

ثالثا – طريقة عمل بروتوكول المعاملات المالية الآمنة SET:

1– يشترك الزبون لدى إحدى البنوك أو المؤسسات الائتمانية بغية الحصول على برنامج خاص ببروتوكول الحركات المالية الآمنة، وهو برنامج المحفظة الإلكترونية، التي تحتوي على البطاقة الائتمانية وشهادة إلكترونية[4].

---

[1] منير محمد الجنبيهي ، ممدوح محمد الجنبيهي، مرجع سابق، ص 167.

[2] إبراهيم بختي، التجارة الإلكترونية (مفاهيم واستراتيجيات التطبيق في المؤسسة)، (د ط)، ديوان المطبوعات الجامعية، الجزائر، 2008، ص79.

[3] ناصر خليل، مرجع سابق، ص225.

[4] سمية ديمش، مرجع سابق، ص92.

2- يقوم المستهلك بفتح حساب بطاقة ائتمان من نوع ماستر كارد أو فيزا كارد، أو لدى أي بنك آخر يصدر بطاقات ائتمان[1].

3- يزور المشتري موقع البائع الذي يتعامل ببروتوكول SET ويحدد حاجياته[2].

4- يتلقى المستهلك شهادة رقمية، وهي عبارة عن ملف رقمي يعمل كبطاقة اعتماد إلكترونية تستخدم في عمليات الشراء على الأنترنت، تحتوي الشهادة الإلكترونية على المفتاح المعلن وتاريخ الانتهاء، ولا ترسل هذه البيانات إلى المستهلك إلا بعد أن يتم تحويلها إلى المصرف ليتحقق من صلاحيتها، وصحة البيانات التي تحتويها[3].

5- يقوم المستهلك بتثبيت طلبيته على الأنترنت، ويتلقى متصفح الويب الطلب ويتأكد من هوية التاجر من خلال التحقق من صلاحية الشهادة الممنوحة له.

6- يرسل المتصفح الطلبية إلى التاجر، حيث يتم تشفير هذه الرسالة باستخدام المفتاح المعلن للبنك، والتي لا يمكن للتاجر قراءتها، بل ولا يمكنه استخدامها إلا مع هذا الطلب بالتحديد[4].

- يتحقق التاجر من هوية المستهلك من خلال التوقيع الإلكتروني الموجود على شهادته، ويمكن أن تتم هذه العملية بإرسال الشهادة إلى المصرف، أو فريق ثالث يقوم بعملية التحقيق.

8- يرسل التاجر الطلبية ضمن رسالة إلى المصرف متضمنة شهادته ومفتاح المصرف المعلن، ومعلومات الدفع الخاصة بالمستهلك والتي لا يستطيع التاجر فك تشفيرها.

---

[1] ناصر خليل، مرجع سابق، ص225.

[2] سمية ديمش، مرجع سابق، ص92.

[3] المرجع نفسه، ص 226.

[4] إبراهيم بختي، التجارة الالكترونية (مفاهيم واستراتيجيات التطبيق في المؤسسة)، مرجع سابق، ص 120.

9- يتحقق المصرف من هوية التاجر والرسالة التي أرسلها، ويقوم بمقارنة التوقيع الإلكتروني الموجود على الشهادة مع توقيع الرسالة، ويتحقق من الإجراءات الخاصة بالدفع المتضمنة في الرسالة.

10- يضع المصرف توقيعه الإلكتروني، ويقوم بإرسال الموافقة للتاجر، الذي يقوم بدوره بشحن الطلبية إلى الزبون[1].

الفرع الثالث: الجدران النارية

تحتوي معظم أنظمة التشغيل على برامج حماية (جدران نارية)، تدمج مع أنظمة التشغيل، يتم تثبيتها على أجهزة الحاسوب تقوم بمعالجة البيانات الشخصية للأطراف، وفي هذا الفرع سوف نتطرق إلى تعريف الجدران النارية (أولا)، أنواع الجدران النارية (ثانيا)، طرق الحماية باستخدام الجدران النارية (ثالثا).

أولا- تعريف الجدران النارية:

الجدران النارية عبارة عن مجموعة من الحاسبات الإلكترونية والبرمجيات المصاحبة معها، والتي تقوم بعملية فصل الشبكات الخاصة للشركة عن الشبكات العامة، حيث تقوم بعض هذه الجدران النارية، بعملية تصفية للبيانات التي تنتقل من شبكة الأنترنت العامة، إلى الشبكة المحلية الخاصة بالشركة، والمبنية على شبكات العمل للحاسوب، الذي يقوم بعملية الإرسال والاستقبال للطلبات أو البيانات، كما وتعرف أيضا الجدران النارية بأنها عبارة عن برمجيات هدفها الأساسي تأمين الحماية الكافية للبيانات، والقضاء على كل عمليات الاختراق والتدمير التي تتعرض لها ملفات خوادم الويب[2].

إن الهدف الرئيسي من الجدران النارية هو حماية المعطيات المخزنة على مخدم الويب أو أي مخدم آخر متصل بالأنترنت، من أي هجوم يقوم به العابثين والمخترقين من

---

[1] سمية ديمش، مرجع سابق، ص 100.

[2] المرجع نفسه ، ص94.

خارج الشركة، ويمكن إعداد الجدران النارية بحيث تتمكن من مراقبة أنماط معينة من البيانات، كالأوامر والتعليمات الغير مسموح بتنفيذها على المخدم، ومن الممكن حجب بيانات من مصادر معينة، كالمعلومات الآتية من دولة معينة أو من مستخدم معين[1].

وتبرر الحاجة لاستخدام الجدران النارية عندما يبدأ المخترقين بالدخول بغرض العبث أو التخريب، أو الاطلاع على ما ليسوا مخولين بالاطلاع عليه، ويتم منعهم من الدخول من خلال إيقاف الأوامر التي يرسلونها، ومع أن الجدار الناري يقوم بإيقاف محاولات قراصنة المعلومات غير الشرعية، إلا أنه يسمح بمرور الحركة الشرعية بدون عرقلة[2].

ثانيا – أنواع الجدران النارية:

هناك نوعان من الجدران النارية المتوفرة تتمثل في:

1 – الحائط المصفى:

يتم فيه التدقيق بكل حزمة بيانات تمر من حدود الشبكة، ويتفحص العناوين ويستطيع أن يقرر أي منها يمكن أن يمر، وبالمقابل فإنه سيمنع مرور المعلومات أو البيانات غير المسموح بها[3].

2 – الحائط المفوض:

يتميز هذا الحائط بمنع أي مرور مباشر لحركة المعلومات بين الشبكات الخارجية والشبكات المحمية، فإذا طلب أحد مستخدمي الشبكة المحمية صفحة موقع على الأنترنت فإن الحاسب المفوض المقدم للخدمة يحضر هذه الصفحة ثم يمررها لطالبها، بدون أن يكون هناك أي اتصال مباشر بين الحاسب الطالب لهذه الصفحة وشبكة الأنترنت[4].

---

[1] ناصر خليل، مرجع سابق، ص227.

[2] خضر مصباح الطيطي، مرجع سابق، ص248.

[3] عبد الفتاح محمود الكيلاني، مرجع سابق، ص372.

[4] المرجع نفسه، ص373.

وبذلك يشكل الحائط الناري خط الدفاع الأول للحماية من أي تهديد خارجي، ولكنه يحتاج إلى أنظمة أكثر تقنية في الشبكات المفتوحة[1].

ثالثا – طرق الحماية باستخدام الجدران النارية:

تقوم الجدران النارية بإدارة عملية النفاد إلى الموقع أو الشبكة، من خلال ثلاث طرق أساسية هي:

1– طريقة إتاحة العام وغلق الخاص:

ويقصد بهذه الطريقة وجود خادمين للملفات، أولهما توضع عليه البيانات العامة والتي ترغب الشركة في إتاحتها للمستخدمين في سهولة ويسر، ويوضع هذا الخادم خارج حائط المنع (جدار النار)، ويكون خادم الملفات الثاني هو الخادم الخاص بتطبيقات وقواعد بيانات الشركة أو المؤسسة، ويوضع بعد حائط المنع[2].

بالرغم من ارتفاع مستوى الحماية التي يوفرها هذا الأسلوب للنظم وقواعد البيانات الداخلية للمؤسسة أو الشركة، إلا أنه يترك التعامل في الخادم العام لمخاطر تقلل من فعالية هذا الأسلوب، حيث تجرى كافة المعاملات على الحاسب غير المؤمن، مما يمثل مخاطر للمشترين من كشف معلوماتهم[3].

2– طريقة حوائط المنع المزدوجة:

يحول هذا الجدار المزدوج دون وصول الطبقات المشكوك فيها من الأنترنت إلى الخادمين العام والخاص مباشرة، فيتم وضع خادم الملفات العام بعد الجدار الناري الأول ويوضع خادم الملفات الخاص بعد الجدار الناري الثاني، لترشيح وتصفية كل الرزم الداخلة

---

[1] عبد الفتاح محمود الكيلاني، مرجع سابق ، ص372.

[2] رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، ط 1، القاهرة، مصر، 1999، ص111.

[3] المرجع نفسه، ص ص111–112.

والخارجة من الشبكة، وبهذا يتم توفير حماية كاملة لجميع معلومات المؤسسة العامة منها والخاصة[1].

3- طريقة الفصل المطلق للخدمات:

يتم وفقا لهذه الطريقة الفصل التام بين كل من خادم الملفات العام وخادم الملفات الخاص، حيث يذهب دعاة هذا الأسلوب إلى أن يكون خادم الملفات الخاص حاسب مستقل بذاته، ويستخدم نظام تشغيل ذو درجة تأمين عالية، وبدون أي وظائف إضافية يمكن منها الدخول إلى الملفات الخاصة بالشركة[2].

يوفر هذا الأسلوب أعلى درجة تأمين للنظم الداخلية للمؤسسة أو الشركة، إلا أنه يؤدي إلى تعقيد تنفيذ المعاملات التجارية والمالية، والتي تتطلب تكامل النظم الداخلية للمؤسسة مع مقر معلومات الشركة، يناسب هذا الأسلوب المؤسسات والشركات التي لا تقوم بإجراء الدورة الكاملة للتجارة الإلكترونية[3].

وفي الأخير نخلص إلى أن الوسائل التقنية لأمن البيانات الشخصية عبارة عن أنظمة وبرامج تسمح بحجب المعلومات والبيانات ومنع الدخول غير المرخص إليها، بهدف حماية طرفي المعاملة الإلكترونية والحفاظ على خصوصية وسرية البيانات، أمام تزايد جرائم الاختراق والاحتيال المرتكبة عبر شبكة الأنترنت، وعلى الرغم من فعاليتها كوسائل وقائية تمنع دخول القراصنة ومخترقي النظم المعلوماتية إلا أنها لا تكفي لوحدها، بل يجب البحث عن الوسائل القانونية التي تضمن سلامة البيانات الشخصية، وهذا ما سنتطرق إليه من خلال المبحث الثاني.

---

[1] سمية ديمش، مرجع سابق، ص94.

[2] رأفت رضوان، مرجع سابق، ص113.

[3] المرجع نفسه، ص114.

المبحث الثاني: الوسائل القانونية لأمن البيانات الشخصية في مجال التجارة الإلكترونية

تغيرت العديد من المفاهيم والنصوص القانونية في العصر الحديث بتغير تقنيات توثيق التصرفات القانونية، تبعا لتطورها في مجال نظم التكنولوجيا الحديثة، الأمر الذي دفع بالعديد من الدول في كل مرة في سبيل مواكبة هذه التطورات، إلى إدخال تعديلات على تشريعاتها الداخلية والخاصة بالتجارة الإلكترونية.

ولعل ظهور التوقيع الإلكتروني كمصطلح جديد في نظام المعالجة الإلكترونية كان تلبية إلى حاجة المتعاملين إلى إضفاء حماية على المعاملات الإلكترونية، وتبادل البيانات عبر هذه الوسائل (المطلب الأول)، ولتحقق من صحة هذا الأخير في ظل غياب علاقة مباشرة بين المتعاملين في التجارة الالكترونية، والتي تتم عبر الوسائط الإلكترونية، ولضمان توفر عنصري الثقة والأمان، كان لابد من إيجاد نظام يحافظ موثوقية على سرية وأمن التوقيع الالكترونية والبيانات التي يحملها، فظهر ما يعرف بالتصديق الإلكتروني (المطلب الثاني).

المطلب الأول: مفهوم التوقيع الإلكتروني

تباينت الجهود الدولية التي سعت إلى تنظيم المعاملات التي تتم عبر الوسائط الالكترونية وقطاع الاتصال، في تحديد مفهوم التوقيع الإلكتروني، الذي أصبح عنصر مهما يعتمد عليه في مجال التجارة الإلكترونية، فالتوقيع الإلكتروني يلعب دورا أساسيا في حماية البيانات ذات الطابع الشخصي لذا سيدرس في هذا المطلب تعريف التوقيع الإلكتروني (الفرع الأول)، صور التوقيع الإلكتروني (فرع ثاني)، وأخيرا شروط الاعتماد على التوقيع الإلكتروني كوسيلة لحماية البيانات ذات الطابع الشخصي (فرع ثالث).

الفرع الأول: تعريف التوقيع الإلكتروني

أعطت معظم التشريعات تعريف للتوقيع الإلكتروني لكونه منظومة جديدة وعليه سيتم التطرق من خلال هذه الجزئية إلى تعريف التوقيع الإلكتروني كما جاء في بعض التشريعات (أولا) ثم التعريف الفقهي للتوقيع (ثانيا).

أولا: التعريف التشريعي للتوقيع الإلكتروني:

حظي التوقيع الإلكتروني بتعريف من طرف العديد من التشريعات، سواء على المستوى الدولي أو على المستوى الداخلي.

1- تعريف التوقيع الإلكتروني على المستوى الدولي:

أ- تعريف التوقيع الإلكتروني في قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني لسنة 2001:

بتاريخ 2001/07/05 قامت لجنة الأمم المتحدة للقانون التجاري الدولي وفي دورتها الرابعة والثلاثون، بوضع قانون ينظم التوقيع الإلكتروني، وتحديد الجهة المختصة به، إضافة إلى تحديد واجبات صاحب التوقيع، والغاية التي ينظمها التوقيع من الطرف الذي يعول عليه، إضافة إلى تنظيم خدمات التوثيق والتصديق الإلكتروني[1].

حيث عرفت المادة الثانية منه التوقيع الإلكتروني بأنه "بيانات في شكل إلكتروني مدرجة برسالة مضافة إليها أو مرتبطة بها منطقيا، بحيث يمكن أن تستخدم لبيان هوية الموقع بالنسبة إلى هذه الرسالة، ولبيان موافقته على المعلومات الواردة في رسالة البيانات[2].

ويلاحظ على هذا التعريف أنه لم يقم بتحديد أنواع التوقيع الإلكتروني المستخدم، تاركا لدول إصدار تشريعات خاصة بتحديد أنواع التوقيع وكيفية استخدامه، للدلالة على شخصية الموقع والتزامه بالمحرر الإلكتروني[3].

---

[1] قانون اليونسترال النمودجي بشأن التوقيعات الالكترونية لسنة 2001،منشورات الامم المتحدة 2002،المنشور في الموقع الالكتروني:

www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf/

« Le terme signature électronique désigne des données sous formes électronique contenues dans un message de données ou jointes ou logiquement associes au dit message, permit être pour identifier la signature dans le cadre du message de données et indique qu'il épreuve l'information qui est contenue ».

[2] لورنس محمد عبيدات، مرجع سابق، ص125.

[3] المرجع نفسه، ص125.

ب- تعريف التوقيع الإلكتروني في التوجيه الأوروبي بشأن التوقيعات الإلكترونية لسنة 1999:

إن أول نص أوروبي عالج موضوع التوقيع الإلكتروني هو التوجيه الأوروبي رقم 1999/93 الخاص بالتوقيع الإلكتروني، حيث نصت المادة الثانية منه على أن التوقيع الإلكتروني هو: "عبارة عن معلومات في شكل إلكتروني، ترتبط أو تتصل منطقيا بمعطيات إلكترونية أخرى وتستخدم كوسيلة لإقرارها"، ويميز التوجه الأوروبي بشأن التوقيع الإلكتروني بين التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم[1].

2- تعريف التوقيع الإلكتروني في القوانين الداخلية:

أ- تعريف التوقيع الإلكتروني في القانون الجزائري:

بالرجوع إلى القانون الجزائري نجد أن المشرع اعتمد مصطلح التوقيع الإلكتروني لأول مرة في نص المادة 327 فقرة 2 من القانون المدني والتي تنص على: ...يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه.

نستخلص من المادة السالفة الذكر أن المشرع الجزائري في القانون المدني لم يعط تعريف محدد للتوقيع الإلكتروني، على خلاف المرسوم التنفيذي رقم 07-162 الملغى[2].

وبصدور القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، حدد المشرع تعريفا للتوقيع الإلكتروني في الفقرة الأولى من المادة 02 منه التي جاء فيها: "...1- التوقيع الإلكتروني: بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق...".

---

[1] ثروت عبد الحميد، التوقيع الإلكتروني (ماهية، مخاطر وكيفية مواجهتها مدى حجيته في الإثبات)، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص49.

[2] المادة 3 من المرسوم التنفيذي رقم 07-162،مؤرخ في 30 ماي 2007 ، يعدل ويتمم المرسوم التنفيذي رقم 01-123، مؤرخ في 9 ماي 2001 ، والمتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات السلكية واللاسلكية بما فيها اللاسلكية الكهربائية وعلى مختلف المواصلات السلكية واللاسلكية ، ج ر عدد 37، صادرة في 07 جوان 2007،(ملغى).

وفي نص المادة السابعة من ذات القانون ميز المشرع بين التوقيع الإلكتروني الموصوف والتوقيع الإلكتروني العادي، حيث عرف التوقيع الإلكتروني الموصوف على أنه "التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

1-أن ينشأ على أساس شهادة التصديق الإلكتروني 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 وسائل تكون تحت التحكم الحصري للموقع.

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

فالتوقيع الإلكتروني الموصوف هو ذلك التوقيع الذي يشهد بصحته مقدم خدمات التصديق الإلكتروني[1]، الذي يكون معتمد من السلطة الاقتصادية المكلفة باعتماد ومراقبة التصديق الالكتروني[(2)]

في حين وضع تعريف صريح وواضح للتوقيع الإلكتروني العادي في المادة 2 فقرة 1 من القانون 15-04، و هو ذلك التوقيع الإلكتروني الذي يتم إنشائه دون أن يتضمن أحد المتطلبات القانونية المنصوص عليها في المادة 7 أعلاه.

ب- تعريف التوقيع الإلكتروني في القانون الفرنسي:

عرف المشرع الفرنسي التوقيع الإلكتروني في المادة 1316 الفقرة الرابعة من القانون المدني الفرنسي رقم 230 لسنة 2000 : "يتمثل في استخدام وسيلة أمنية لتحديد هوية صاحبه بحيث تضمن صلة بالتصرف الذي وقع عليه ويفترض أمان هذه الوسيلة ما لم يوجد

[1] علاء محمد نصيرات ،حجية التوقيع الالكتروني في الاثبات (دراسة مقارنة)، (د ط)، دار الثقافة لنشر والتوزيع، عمان، الأردن، 2005، ص 145.

[(2)] المادة 30 من القانون 15-04، مرجع سابق.

دليل عكسي وذلك بمجرد وضع التوقيع الإلكتروني الذي بموجبه تتحدد شخصية الموقع، وتضمن سلامة التصرف وذلك بالشروط المحددة بمرسوم من مجلس الدولة[1].

ج- تعريف التوقيع الإلكتروني في التشريع الأردني:

جاء تعريف التوقيع الإلكتروني في قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، في المادة الثانية كما يلي: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة، في رسالة معلومات أو مضافة عليها أو مرتبطة بها، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره، من أجل توقيعه ويفرض الموافقة على مضمونه[2].

ثانيا- التعريف الفقهي للتوقيع الإلكتروني:

تعددت التعريفات الفقهية للتوقيع الإلكتروني، فقد عرفه جانب من الفقه بأنه "عبارة عن حروف أو أرقام، أو رموز، أو إشارات، لها طابع منفرد، تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، ويتم اعتماده من الجهة المختصة[3].

ويراه البعض بأنه "عبارة عن مجموعة من الأرقام التي تنجم عن عملية حسابية مفتوحة باستخدام الرمز السري الخاص[4].

وعرفه البعض الآخر بأنه "تعبير شخص عن إرادته في الالتزام بتصرف قانوني معين، عن طريق تكوينه لرموز سرية، يعلمها هو وحده تسمح بتحديد هويته".

---

(1) ELISABETH MATHIEU-Marieu, Les Services et financier en ligne, Editeur Revue Banque, Paris, France, 2005, p 196.

(2) علاء محمد نصيرات، مرجع سابق، ص29.

(3) إلياس ناصيف، العقود الدولية العقد الإلكتروني في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص242.

(4) عمر خالد زريقات، عقود التجارة الإلكترونية (عقد البيع عبر الأنترنت)، دار حامد للنشر والتوزيع، (د ط)، عمان، الأردن، 2007، ص236.

والملاحظ أن التعريفات المقدمة للتوقيع الإلكتروني متشابهة، وإن اختلفت في بعض الألفاظ المستخدمة، فكلها تؤكد على أن التوقيع الإلكتروني لكي يكون صحيحا ومنتجا لآثاره القانونية، لابد أن يعبر تعبيرا أكيدا على هوية الموقع، وأن يصدر صحيحا من الموقع، وهذا الأمر لا يأتي إلا بسيطرة الموقع على عناصر التوقيع[1].

الفرع الثاني: صور التوقيع الإلكتروني

للتوقيع الإلكتروني صور وأشكال متعددة تختلف فيما بينها من حيث درجة الثقة والائتمان التي تقدمها ،وكذلك من حيث الإجراءات والشروط المتبعة في إنشائها وإصدارها ومن بينها التوقيع الرقمي (أولا)، التوقيع بالقلم الإلكتروني (ثانيا)، التوقيع باستخدام الخواص الذاتية (ثالثا)، التوقيع بالرقم السري في البطاقات البلاستيكية (رابعا).

أولا- التوقيع الرقمي:

يعتبر التوقيع الرقمي من أهم صور التوقيع الإلكتروني نظرا لما يتمتع به من قدرة فائقة على تحديد هوية أطراف العقد تحديدا دقيقا ومميزا، إضافة لما يتمتع به أيضا من درجة عالية من الثقة والأمان في استخدامه وتطبيقه[2].

يقوم هذا التوقيع على وسائل التشفير الرقمي الذي يعتمد على خوارزميات أو معدلات حسابية رياضية لضمان سرية البيانات والاتصالات بطريقة آمنة، عبر تحويله إلى شكل غير مفهوم إلا من صاحب العلاقة، حيث يتم التوقيع الإلكتروني باستعمال مفتاح معين لتشفير الرسالة الإلكترونية، ثم يعمد مستقبل تلك الرسالة إلى فك التشفير بمفتاح آخر للحصول على المعلومات المرسلة، فإذا ظهرت الرسالة بعد فك التشفير بصورة واضحة ومقروءة، كان توقيع المرسل صحيحا[3]، وتتمثل مهمة التشفير هنا في الحفاظ على أمن وسرية البيانات الموجودة على المحرر الموقع.

---

[1] إلياس ناصيف، مرجع سابق، ص236.

[2] لورنس محمد عبيدات، مرجع سابق، ص144.

[3] فراح مناني، العقد الالكتروني وسيلة اثبات حديثة في القانون المدني الجزائري ، دار الهدى للطباعة والنشر،(د ط) الجزائر، 2009 ، ص152.

ويمكن القول أن التوقيع الرقمي بهذه الطريقة، يحقق أعلى درجات الثقة والأمان للمحرر، ويحافظ على كمال العمل القانوني وبقائه بصورته الأولى منزها من العبث والتحريف، كما أنه يحقق الارتباط بين المحرر والتوقيع الوارد عليه، يسهل التوقيع الرقمي التحقق من هوية الموقع كونه على جهة التصديق موثوقة، كما أنه يعبر بطريقة واضحة عن إرادة صاحب الالتزام بالتصرف القانوني وقبوله لمضمونه.

ويضمن التوقيع الرقمي سرية المحرر حيث لا يمكن الاطلاع عليه إلا ممن أرسل إليه وباستخدام المفتاح العام للمرسل[1].

وبالرغم من المزايا التي يحملها التوقيع الرقمي، وما يحققه من ثقة وأمان لمحتوى المحرر، بحيث يجعله بمنأى من عمليات الاحتيال والقرصنة والاختراق، إلا أنه وبفضل التقدم العلمي والتكنولوجي أن يكون بالإمكان القيام بعمليات احتيال وتزوير، عن طريق كسر المفتاح الخاص برسالة البيانات [2]، والتوصل إلى اكتشاف المفاتيح الخاصة مصدر الموثوقية والأمان وتغيير مضمون رسالة البيانات[3].

وفي سبيل تحقيق أقصى درجة من الأمان وتأمين رسالة البيانات من خطر الاختراق واللصوصية، يقترح البعض ضرورة أن يملك الشخص زوج من المفاتيح الخاصة، عندما يريد أن يقوم بتوقيع رسالة بيانات وتشفيرها[4].

ثانيا – التوقيع بالقلم الإلكتروني:

تقوم هذه الطريقة على استخدام قلم إلكتروني حساس يمكنه الكتابة على الكمبيوتر عن طريق برنامج يسيطر على هذه العملية[5]، فهي طريقة مشابهة لما يعرف بالماسح

---

[1] إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته الجوانب القانونية لعقد التجارة الإلكترونية، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2008، ص27.

[2] المرجع نفسه، ص64.

[3] عمر خالد زريقات، مرجع سابق، ص261.

[4] ثروت عبد الحميد، مرجع سابق، 4ص65.

[5] نضال إسماعيل برهم، غازي أبو عرابي، أحكام عقود التجارة الإلكترونية، (د ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص175.

الضوئي، والذي يتم عن طريق تصوير ونقل التوقيع اليدوي إلى المحرر المراد استخدامه، ويقوم هذا النوع من التوقيع بأداء وظيفتين:

– التقاط إمضاء العميل الذي يتم كتابته بقلم إلكتروني حساس، في مرجع مخصص لذلك، على شاشة الحاسب أو أي مكان يخصص له[1].

– التعرف على دقة التوقيع وصحته، من خلال نظام برمجي يقارن التوقيع الموجود مع التوقيع المخزن، حيث تعتمد هذه المقاربة على الخصائص البيولوجية، ويتم تحديد الدقة المطلوبة للتوقيع تبعا لأهمية نوع المعاملة[2].

غير أن استعمال هذه الصورة للتوقيع في الشكل الإلكتروني يتسبب في العديد من الإشكالات التي لم تجد طريقها إلى الحل حتى الآن، وهي مسألة إثبات الصلة بين التوقيع ورسالة البيانات أو المحرر[3]، إذ بإمكان المرسل إليه الاحتفاظ بنسخة من التوقيع الذي وضعه على أحد المحررات الإلكترونية، ومن ثم يعيد وضعها على أي محرر آخر، وهذا قد ينشأ عنه انعدام الثقة والأمان في هذه الصورة من التوقيع الإلكتروني[4].

ثالثا – التوقيع باستخدام الخواص الذاتية (البيومتري):

يتم التوقيع في هذه الصورة عن طريق استعمال إحدى الخواص الذاتية للشخص[5]، والتي تعتمد على التطور العلمي القائم على دراسة بصمات اليد أو قرنية العين أو نبرات الصوت أو أبعاد الوجه، وذلك من خلال الخصائص الفزيائية والطبيعية والسلوكية التي يتميز بها الأشخاص عن بعضهم البعض[6].

---

[1] علاء محمد نصيرات، مرجع سابق، ص34.

[2] نضال إسماعيل برهم، غازي أبو عرابي، مرجع سابق، ص175.

[3] ثروت عبد الحميد، مرجع سابق، ص55.

[4] إلياس ناصيف، مرجع سابق، ص246.

[5] علاء محمد نصيرات، مرجع سابق، ص32.

[6] عمر خالد زريقات، مرجع سابق، ص256.

وتعتمد هذه الصورة من صور التوقيع الإلكتروني على حجية علمية، هي أن لكل شخص صفات ذاتية خاصة به تختلف من شخص إلى آخر، تتميز بالثبات النسبي مما يؤدي إلى توافر الثقة في أن التوقيع بأحد تلك الخواص قد تم عن طريق الموقع ذاته.

يتم التوقيع بالخواص الذاتية بالتقاط صورة دقيقة لصفة جسدية للشخص الذي يريد استعمال الإمضاء البيومتري، ثم يتم تخزينها بطريقة مشفرة في ذاكرة الحاسب الآلي، حيث تتم برمجته على أساس ألا يصدر أوامر بفتح القفل المغلق، إلا بعد أن يطابق هذه البصمة المبرمجة في ذاكرته[1]، وذلك بهدف توفير الاستخدام القانوني فقط للأشخاص المصرح لهم بذلك، وبالتالي منع أي استخدام غير قانوني أو غير مرخص لأي معلومات أو بيانات سرية أو شخصية موجودة في نظم المعلومات الخاصة بإحدى الجهات[2].

يؤخذ على هذا التوقيع بالرغم من دقته والأمان والثقة المتوفرة بأنه ليس بعيد عن التزوير[3]، فيمكن أن تأثر مميزات الشخص بإدخال أي من المؤثرات أو التعديلات عليها، مما يؤدي لافتقادها الأمن والسرية[4].

ونرى أن هذه المآخذ لا تقلل من الثقة الواجب إعطاؤها لهذا النوع من التوقيع الإلكتروني، فكما أن التزوير وارد في هذه الصورة فهو وارد أيضا في التوقيع التقليدي، هذا بالإضافة إلى أن شأن هذه الصورة في ذلك –أي إمكانية التزوير– شأن جميع أنواع التوقيع الإلكتروني، من احتياجها لتكنولوجيا تؤمن استخدامها عبر الشبكة وتحول دون التلاعب بإعادة النسخ والاستعمال[5].

---

[1] إيمان مأمون أحمد سليمان، مرجع سابق، ص 256–257.

[2] بشار محمود دودين، محمد يحي المحاسنة، الإطار القانوني للعقد المبرم عبر شبكة الأنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص253.

[3] إيمان مأمون أحمد سليمان، مرجع سابق، ص 257.

[4] عمر خالد زريقات، مرجع سابق، ص256.

[5] إيمان مأمون أحمد سليمان، مرجع سابق، ص257.

رابعا – التوقيع بالرقم السري في البطاقات البلاستيكية

تعد هذه الصورة للتوقيع في الشكل الإلكتروني هي الأكثر شيوعا لدى الجمهور، ولا يتطلب استخدامها الكثير من العناء أو خبرة معينة، بل يمكن لأي شخص أن يستخدمها، كما أنها لا تستلزم أن يمتلك الشخص جهاز حاسب آلي أو أن يكون الجهاز متصل بالأنترنت[1].

تكمن دقة هذا النظام في أنه يشتمل على رقم سري متميز وفريد بصاحبه، وبالتالي لو عثر على البطاقة فلا يستطيع أي شخص استخدامها ما لم يكن على علم بالرقم السري، وهذا نادرا ما يحدث إلا بإهمال من قبل حامل البطاقة، الذي يمكنه تفادي ذلك عن طريق مخاطبة البنك بوقف العمل بهذه البطاقة، لذلك فإن هذه البطاقة والرقم السري قد يحقق وظائف التوقيع بكفاءة عالية أكثر من الإمضاء والختم والبصمة، على الرغم من أن الرقم السري ينفصل عن صاحبه[2].

تتميز هذه الصورة من صور التوقيع الإلكتروني بالإضافة إلى سهولتها وبساطتها بقدر كبير من الأمان والثقة[3]، بيد أنها لا تخلو من العيوب لذلك كانت موضع انتقاد خاصة إذا حدث، وهو فرض نادر ولكنه قائم، أن شخصا حصل على البطاقة الممغنطة والرقم السري الخاص بصاحبها، وأجرى عمليات سحب أو شراء قبل أن ينتبه صاحب البطاقة لفقدها، فلا مناص من خصم هذه المبالغ من حساب العميل صاحب البطاقة[4].

الفرع الثالث: شروط الاعتماد على التوقيع الإلكتروني كوسيلة لحماية البيانات ذات الطابع الشخصي

حددت المادة 7 من القانون رقم 15-04 السالف الذكر الشروط التي يجب توافرها في التوقيع الإلكتروني الموصوف حتى يحقق الوظيفة المناط بها ، في حين انها لم تحدد

---

[1] ثروت عبد الحميد، مرجع سابق، ص56.

[2] علاء محمد نصيرات، مرجع سابق، ص36.

[3] ثروت عبد الحميد، مرجع سابق، ص47.

[4] المرجع نفسه، ص49.

شروط التوقيع الالكتروني العادي لذلك ينبغي الرجوع بشأنها الى القواعد العامة في نص المادة 323 مكرر 1 والمادة 327 من ق م ج .

تتمثل شروط التوقيع الالكتروني الموصوف في:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

- أن يرتبط بالموقع دون سواه.

- أن يمكن من تحديد هوية الموقع.

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

- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

- أن يكون مرتبط بالبيانات الخاصة به، بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات.

ومن ما جاء في نص المادة 07 السالفة الذكر، يمكن أن نجمل شروط التوقيع الإلكتروني الموصوف في ثلاث نقاط أساسية تتمثل في:

أولا- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره:

يتطلب هذا الشرط أن يكون التوقيع الإلكتروني مميزا لصاحبه عن غيره، مثله مثل التوقيع التقليدي، على اعتبار أن التوقيع روح الورقة المحررة[1]، فالتوقيع الإلكتروني باعتباره علامة تميز الموقع عن غيره فلا يتصور وجود مجموعة من النسخ عنه، حيث أنه إذا تم إصدار التوقيع فلا يمكن إصدار نفس التوقيع لشخص آخر، وإلا أدى ذلك إلى ضياع حقوق الغير، بالتالي محو السمة الأساسية التي يتمتع بها التوقيع الإلكتروني ألا وهي الأمان[2].

---

[1] لورنس محمد عبيدات، مرجع سابق، ص129.

[2] سهيلة طمين، الشكلية في عقود التجارة الإلكترونية، رسالة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، الجزائر، 2011، ص52.

فالتوقيع الإلكتروني يعمل على تحديد شخص الموقع والبيانات الأساسية عنه، وبهذا يتميز الموقع عن غيره من الموقعين وتتحدد هويته، لا سيما وأن أدوات إنشاء التوقيع الإلكتروني سواء كانت رموز أو أرقام سرية أو خصائص بيولوجية، فإنها تؤدي إلى توفير خاصية التمييز والانفراد للشخص صاحب العلاقة، وذلك لعدم إمكانية إنشاء مثل هذا التوقيع من قبل أي شخص آخر[1] وهذا من شأنه توفير حماية وخصوصية للبيانات الموجودة على المحرر الموقع.

ثانيا – سيطرة صاحب التوقيع على منظومة التوقيع:

إن هذا الشرط يتطلب أن يكون صاحب التوقيع الإلكتروني منفردا به، بحيث لا يستطيع أي شخص معرفة فك رموز التوقيع الخاص به أو الدخول عليه، سواء عند استعماله لهذا التوقيع أو عند إنشائه، وبالتالي فإن التوقيع الإلكتروني يجب أن يتم عبر وسائل تخضع خضوع كامل للسيطرة المباشرة لصاحب التوقيع[2]، وذلك حفاظا على سلامة البيانات الموقعة إلكترونيا وحتى لا يتم التنصل من الاعتراف بها من قبل الشخص الموقع[3].

ثالثا – ارتباط التوقيع الإلكتروني بالمحرر ارتباطا وثيقا:

ارتباط التوقيع بالمحرر بمعنى أن يتصل التوقيع الإلكتروني بالمحرر الكتابي اتصالا مباشر[4]، بحيث لا يمكن الفصل بينهما، وهذا الارتباط يحقق كفاءة التقنيات المستخدمة في تأمين البيانات الموجودة على المحرر الإلكتروني ومنها مفاتيح التشفير العام والخاص، أو الخواص البيولوجية للإنسان التي من المستحيل أن تتشابه مع شخص آخر، وبهذا فإن أية

---

[1] عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، ط1، دار وائل للنشر والتوزيع، عمان، الأردن، 2010، ص56.

[2] محمد مأمون سليمان، التحكيم الإلكتروني، دار الجامعة الجديدة، (د ط)، الإسكندرية، مصر، 2011، ص232.

[3] عبير ميخائيل الصفدي الطوال، مرجع سابق، ص57.

[4] ناهد فتحي الحموري، الأوراق التجارية الإلكترونية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2010، ص87.

محاولة من قبل الغير للاطلاع على المحرر وإحداث أي تغيير أو تعديل عليه سيكون قابلا للكشف، كونه سيؤدي إلى إحداث تعديل على التوقيع الموضوع على المحرر[1].

وعليه فإن الارتباط المادي والمباشر للتوقيع بالمحرر المتعلق به يضمن سلامة المحرر والمعلومات المدونة بداخله من أية محاولات للتلاعب أو التزوير أو التعديل أو التحريف.

المطلب الثاني: التصديق الإلكتروني

يعد التصديق الإلكتروني من أهم الوسائل والعمليات المستخدمة في تأمين التوقيع الإلكتروني وحمايته من مخاطر القرصنة، وإساءة استخدام البيانات الشخصية المتعلقة بالغير في أنشطة غير مشروعة عبر شبكة الأنترنت، وكدا التحقق من صحة التوقيع ونسبته للموقع، ويتولى عملية التصديق الإلكتروني طرف محايد ومستقل مرخص من قبل الدولة، ويخضع لمراقبة جهات مختصة حددها المشرع في القانون 15-04.

وسيتم التطرق في هذا المطلب إلى مفهوم شهادة التصديق الإلكتروني في (الفرع الأول)، وإلى الجهة المختصة بإصدار شهادة التصديق الإلكترونية في (الفرع الثاني)، وإلى دور التصديق الإلكتروني في ضمان أمن البيانات الشخصية وذلك في (الفرع الثالث).

الفرع الأول: مفهوم شهادة التصديق الإلكتروني

نظرا لخطورة المعاملات الإلكترونية، يحتاج المتعاملين في هذا المجال الإلكتروني إلى إضفاء نوع من السرية في البيانات المتبادلة إلكترونيا، فهم في حاجة لشهادة التصديق الإلكتروني للتأكد من شخصية الموقع والتأكد من أن كافة البيانات صحيحة، ونظرا لأهمية شهادة التصديق الإلكتروني، لأنها توفر الثقة والأمان لدى المتعاملين في التجارة الإلكترونية، ارتأينا تحديد مفهوم شهادة التصديق الإلكتروني، من خلال تعريفها (أولا)، وبيان أنواعها (ثانيا).

[1] عبير ميخائيل الصفدي الطوال، مرجع سابق، ص57.

أولا- تعريف شهادة التصديق الإلكتروني:

لقد عرف المشرع الجزائري شهادة التصديق الإلكتروني في المادة 2 فقرة 7 من قانون 15-04 بأنها "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

ونلاحظ من خلال هذا التعريف أن المشرع حدد الغاية والهدف من وراء إصدار هذه الشهادة، والمتمثلة في إثبات نسبة التوقيع الإلكتروني إلى شخص معين، وبالتالي تحديد شخصية الموقع وتأكيد موافقته على مضمون المحرر، بالإضافة إلى التحقق من صحة البيانات التي تحتويها الشهادة.

أما قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية فقد عرفها في المادة 2 منه بأنها "رسالة بيانات أو سجل آخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع"[1] واعتبر هذا التعريف أن الشهادة وثيقة يؤكد بها شخص وقائع معينة، والغرض منها بيان وجود صلة ما بين شخصية الموقع وبيانات إنشاء التوقيع، والمعبر عنها بالمفتاح الخاص.

أما التوجه الأوروبي رقم 1999/93 فقد عرف شهادة التصديق الإلكترونية في مادته الثالثة بأنها "تلك التي تربط بين التوقيع وبين شخص معين وتؤكد شخصية الموقع"[2].

ثانيا- أنواع شهادة التصديق الإلكتروني:

تختلف أنواع شهادات التصديق الإلكتروني بحسب مستويات الأمن في اختيار التكنولوجيا المناسبة في التصديق الإلكتروني لمنحها فعالية قانونية أكثر، حيث ميز المشرع في القانون 15-04 بين شهادة التصديق الإلكترونية الموصوفة والعادية.

1- شهادة التصديق الإلكتروني الموصوفة:

عرف المشرع الجزائري الشهادة الإلكترونية الموصوفة في القانون رقم 15-04 في مادته 15 بأنها شهادة تتوفر فيها المتطلبات الآتية:

---

[1] عبير ميخائيل الصفدي الطوال، مرجع سابق، ص 99.

[2] إيمان مأمون أحمد سليمان، مرجع سابق، ص 321.

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

– أن تمنح للموقع دون سواه، ويتم منح هذه البطاقة بصفة شخصية لصاحبها دون غيره.

– ويجب أن تتضمن أيضا وعلى وجه الخصوص إشارة واضحة، تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة، يتبين من خلالها أن هذه الشهادة صادرة بصفتها شهادة موصوفة.

– تحديد هوية الطرف الثالث الموثوق، أو مؤدي خدمات التصديق الإلكتروني المرخص له لشهادة التصديق الإلكتروني، وكذا البلد الذي يقيم فيه.

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

– التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني، أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني.

2– شهادة التصديق الإلكتروني العادية:

عرف المشرع الجزائري شهادة التصديق الإلكتروني في الفقرة 7 من المادة 2 من القانون 15–04 بأنها "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع"، ومن خلال هذا التعريف يؤكد المشرع على الطابع الالكتروني الذي يجب أن تصدر فيه الشهادة..

ولم يتطرق لتعريف شهادة التصديق الإلكتروني البسيطة كما فعل في نص المادة 3 الفقرة 9 من المرسوم التنفيذي رقم 07– 162[1] الذي تم إلغاؤه.

[1] مرسوم تنفيذي رقم 07–162، المتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات السلكية واللاسلكية بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، مرجع سابق.

ثالثا – شهادة التصديق الأجنبية:

عالجت المادة 12 من قانون اليونسترال النموذجي بشأن التوقيع الالكتروني[1] مسألة الشهادات والتوقيعات الأجنبية، وقد تضمن القانون المذكور مجموعة من القواعد في هذا الخصوص، تتمثل في:

– وفقا للقاعدة الأولى فإنه لا اعتبار للمكان الجغرافي الذي صدرت منه شهادة التصديق الإلكتروني، أو تم فيه التوقيع الإلكتروني، طالما أن كل منهما ساري المفعول لم يوقف أو يلغى، لأن الشهادة أو الموقع في التوقيع الإلكتروني سوف يتم الاعتراف به من الجهة الأجنبية، والهدف من ذلك تيسير المعاملات الدولية، لا سيما التجارة الإلكترونية الدولية[2].

– أما القاعدة الثانية فتعني مساواة الأثر القانوني للشهادة في الدولة التي صدرت فيها مع الشهادة الأجنبية التي صدرت من دولة أخرى، بمعنى أن الشهادة الأجنبية تعامل مع الشهادة الوطنية، مرتبة ذات الأثر القانوني أي المعاملة بالمثل[3].

– وجاءت القاعدة الثالثة لتكرس مساواة الأثر القانوني للتوقيع الإلكتروني في الدولة التي صدر فيها، في داخل الدولة الأخرى الوطنية، متى كان التوقيع الأجنبي يعادل ذات الثقة للتوقيع في الدولة المطلوب استخدام التوقيع فيها[4].

– والقاعدة الرابعة، إذا كانت شهادة التصديق الإلكتروني الأجنبية لها قوة إثبات تعادل المعمول بها في الدولة الأجنبية، فإنه يتم مراعاة المعايير الدولية المعمول بها.

– والقاعدة الأخيرة أن أطراف المعاملة الإلكترونية قد يتفقون على استخدام شهادات تصديق بغض النظر عما هو منصوص عليه في القاعدة (1، 2، 3)، وفي هذه الحالة اتفاق

---

[1] قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001، مرجع سابق .

[2] عبد الفتاح بيومي حجازي، التجارة عبر الانترنت، مرجع سابق، ص 305.

[3] المرجع نفسه، ص 307.

[4] قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية لسنة 2001، مرجع اسابق.

الأطراف هو المطبق عبر الحدود، ولا يعطل الاتفاق إلا إذا كان غير صحيح قانونا، أو متعارض مع قانون الدولة المطلوب إعماله فيها[1].

وقد نص المشرع الجزائري على شهادة التصديق الأجنبية في المادة 63 من القانون 15-04، حيث نصت على: "تكون لشهادات التصديق الإلكتروني التي يمنحها مؤدي خدمات التصديق الإلكتروني المقيم في البلد الأجنبي، نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الإلكتروني المقيم في الجزائر، بشرط أن يكون مؤدي الخدمات الأجنبي هذا قد تصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها السلطة."

وما يفهم من نص المادة أن المشرع الجزائري ساوى من حيث القيمة القانونية بين شهادات التصديق الوطنية التي تقوم بإصدارها جهات تصديق جزائرية، وبين تلك الشهادات التي يقوم بإصدارها مقدمي خدمات أجنبية، وهذا بشرط أن تكون اتفاقية بين الجزائر وهذا البلد الأجنبي الصادر منه الشهادة.

الفرع الثاني: الجهة المختصة بإصدار شهادة التصديق الإلكترونية

تعتمد التجارة الإلكترونية في إجراءاتها على شبكة اتصال مفتوحة، كما أن غالبية العقود التي تتم بين أطرافها تعتبر عقود مبرمة بين غائبين، مما استلزم وجود طرف ثالث محايد، يتمثل في أفردا أو شركات مستقلة تقوم بإصدار شهادات التصديق الإلكتروني.

وسيتم التطرق من خلال هذا الفرع إلى تعريف الجهة المختصة بإصدار شهادة التصديق الإلكتروني (أولا)، ودور الجهة المختصة في إصدار شهادة التصديق الإلكتروني (ثانيا) والتزامات مقدم خدمات التصديق الالكتروني(ثالث).

---

[1] مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الأنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2011، 2012، ص ص 241-242.

أولا- تعريف الجهة المختصة بإصدار شهادة التصديق الإلكتروني:

عرف المشرع الجزائري مؤدي خدمات التصديق الإلكتروني في الفقرة 12 من المادة 2 من القانون 15-04 على أنه " شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني."

ويلاحظ أن المشرع لم يميز بين الشخص الطبيعي أو المعنوي في ممارسة خدمات التصديق الإلكترونية وعليه يمكن أن يكون مؤدي خدمات التصديق الإلكتروني شخصا معنويا كما يمكن أن يكون شخصا طبيعيا.

ولتقديم خدمات التصديق الالكتروني يشترط القانون 15-04 مجموعة من الشروط الشكلية والموضوعية، حددتها المواد من 33 إلى 40 منه، وتتمثل أساسا في الحصول على الترخيص من الهيئة الاقتصادية للتصديق الالكتروني، على أن يتمتع بقدرة مالية كافية، وبمؤهلات وخبرة في مجال تكنولوجيات الاتصال والاعلام[1].

ثانيا- التزامات مقدم خدمات التصديق الإلكتروني:

يقع على عاتق مقدم خدمات التصديق الإلكتروني مجموعة من الالتزامات تتعلق بمزاولة النشاط، بالإضافة إلى الالتزامات المتعلقة بتأمين وحماية البيانات.

1- الالتزامات المتعلقة بمزاولة النشاط:

من بين التزامات مؤدي خدمات التصديق الالكتروني والمتعلقة بمزاولة النشاط، الالتزام بالحصول على ترخيص مسبق بمزاولة النشاط المهني من الجهة المختصة، قبل الشروع في أي عمل يدخل في حدود الترخيص، حيث من واجبات مزود خدمات التصديق أن يكون مرخص من قبل مراقب خدمات التصديق[2].

---

[1] أنظر المادة 34 من القانون 15-04، المتعلق بالتوقيع والتصديق الالكترونيين، مرجع سابق.

[2] مخلوفي عبد الوهاب، مرجع سابق، ص 231.

كما أن المشرع الجزائري أخضع نشاط تأدية خدمات التصديق الإلكتروني إلى الترخيص وهذا حسب المادة 33 من القانون 15-04 "يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني."

ومن بين الالتزامات كذلك الالتزام بعدم إفشاء سرية البيانات الإلكترونية المسلمة إليه، حيث تنص المادة 42 من القانون 15-04 "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية الممنوحة"

وبالتالي فإن بيانات التوقيع الإلكتروني وكل المعلومات التي يقدمها دوي الشأن لمؤدي خدمات التصديق الإلكتروني تبقى سرية، ولا يجوز للأعوان الذين قدمت إليهم بحكم عملهم أن يقوموا بإفشائها للغير أو استخدامها لغير الغرض المخصص لها.

2- الالتزام بتأمين وحماية البيانات:

أولى قانون اليونسترال النموذجي بشأن التوقيعات الإلكترونية مقدم خدمات التصديق الإلكتروني، مجموعة من العوامل تعطي الثقة للأشخاص للتعامل بالطرق الإلكترونية، حيث نص في المادة 10 من نفس نص القانون على توفير العوامل التالية:

- الموارد المالية والبشرية.

- جودة نظم المعدات والبرمجيات.

- إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات[1].

وقد تبنى المشرع الجزائري المبدأ ذاته في القانون 15-04، حيث جاء في المادة 34 منه، على أنه: "يجب على كل طالب ترخيص لتأدية خدمة التصديق الإلكتروني أن يستوفي الشروط الآتية:

[1] مخلوفي عبد الوهاب، مرجع سابق، ص 232.

– أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي.

– أن يتمتع بقدرة مالية كافية.

– أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال، للشخص الطبيعي أو المسير للشخص المعنوي.

– ألا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني".

الفرع الثالث: دور التصديق الإلكتروني في ضمان تأمين البيانات

نظرا لأهمية شهادة التصديق الإلكتروني وخطورة المعلومات التي تتضمنها والتي يعتمد عليها الغير لإتمام تعاملاتهم، فإن دور التصديق الإلكتروني جد مهم، بحيث يوفر الثقة للمتعاملين الذين يبرمون مختلف تعاملاتهم عبر شبكات الأنترنت، بحيث يضمن صحة البيانات والمعلومات والتوقيعات في مختلف المعاملات الإلكترونية.

وتظهر أهمية التصديق الالكتروني في تأمين البيانات، من خلال النقاط التالية:

أولا– التحقق والتأكد من صحة البيانات:

ألزم المشرع الجزائري بموجب القانون 15–04 مؤدي خدمات التصديق الإلكتروني قبل منح شهادة التصديق الإلكتروني بالتحقق من تطابق بيانات الإنشاء مع بيانات التحقق من التوقيع، وذلك بعد التحقق من هوية طالب الشهادة سواء كان بصفة شخصية بالنسبة للشخص الطبيعي أو بالنسبة للممثل القانوني، فيقوم مؤدي خدمات التصديق الإلكتروني بحفظ البيانات في سجل خاص، يدون فيه هوية وصفة الممثل القانوني وحدود استعمال صلاحياته[1].

[1] انظر: المادة 44 من القانون 15–04، المتعلق بالتوقيع والتصديق الالكترونيين، مرجع سابق.

ثانيا – حماية البيانات:

وضع المشرع التزام على عاتق مؤدي خدمات التصديق الإلكتروني يتمثل في وضع متطلبات فنية وتقنية مؤمنة تتفق مع حماية التوقيع الإلكتروني والبيانات.

وتتمثل هذه المتطلبات الفنية في الأجهزة المستعملة وتكون خاصة ومهيأة لإنشاء توقيع إلكتروني موصوف، ومن هذه المتطلبات تشغيل العاملين المتخصصين على تلك الأجهزة، والعمل وفق منظومة متكاملة لعناصر التوقيع الإلكتروني، كل ذلك بهدف حماية وحفظ البيانات والمعلومات المرتبطة بشهادة التصديق الإلكتروني[1].

كما ويتمثل الالتزام الرئيسي لهذه الجهات في قيامها بالتحقق من هوية الشخص الموقع، حيث تقوم بإصدار شهادة توثيق إلكترونية تفيد التصديق على التوقيع الإلكتروني في تعاقد معين، تشهد بموجبها بصحته ونسبته إلى من صدر عنه، ويجب على مقدم خدمة التوثيق ممارسة عناية معقولة لضمان صحة كل البيانات ذات الصلة بالشهادة، كما يجب تحديد الأهلية القانونية للمتعاقد، وكذلك التحقق من سلطات هذا الشخص واختصاصاته الوظيفية[2].

ثالثا – حفظ بيانات شهادة التصديق الإلكتروني:

على مؤدي خدمات التصديق الإلكتروني الالتزام بتحويل كل المعلومات المتعلقة بشهادة التصديق الإلكتروني الموصوفة إلى السلطة الاقتصادية من أجل حفظها وهذا بعد انتهاء صلاحيتها، حيث جاء في المادة 47 من القانون 15-04 أنه: "يجب على مؤدي خدمات التصديق الإلكتروني، تحويل المعلومات المتعلقة بشهادة التصديق الالكتروني الموصوفة بعد انتهاء صلاحيتها إلى، السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها".

---

[1] محمد مأمون سليمان، مرجع سابق، ص 255.

[2] إيمان مأمون أحمد سليمان، مرجع سابق، ص 314.

في حين لا يحق لمؤدي خدمات التصديق الإلكتروني حفظ أو نسخ بيانات إنشاء التوقيع الإلكتروني[1]، كما أنه ملزم بالحفاظ على البيانات والمعلومات ذات الطابع الشخصي التي تم جمعها وعدم نقلها إلى الخارج، إلا في حالة وجود اتفاق يقضي بذلك حيث نص المشرع الجزائري في المادة 5 من القانون 15-04: "يجب أن تتواجد على التراب الوطني كل البيانات والمعلومات ذات الطابع الشخصي التي تم جمعها من طرف مؤدي خدمات التصديق الالكتروني، أو الطرف الثالث الموثوق أو سلطات التصديق الالكتروني، وكذلك قواعد البيانات التي تحتويها، ولا يمكن نقلها خارج التراب الوطني إلا في الحالات التي ينص عليها التشريع المعمول به."

رابعا – إصدار المفاتيح الإلكترونية:

تتولى هذه الجهات إصدار المفاتيح الإلكترونية، سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الإلكترونية، أو المفتاح العام الذي يتم بواسطة فك هذا التشفير، وبالتالي تضمن هذه الجهات أن المفتاح العام هو المناظر، حيث تتحقق من تطابقه وصلاحيته[2].

كما تقوم هذه الجهة بإصدار التوقيع الرقمي، حيث يقوم طالب التوثيق بتقديم البيانات اللازمة إلى جهة التوثيق، ثم يتم إصدار المفتاح الخاص بصاحب طلب حق التوقيع الذي استخدمه في التوقيع، ولا يمكن استخدامه إلا من جهاز حاسب آلي واحد فقط، وذلك حتى يتم التأكد من أن التوقيع الرقمي صادر من صاحبه، لذا يتعين على الموقع بالمفتاح الخاص أن يحتفظ به سرا ولا يطلع عليه أحد، أما المفتاح العام فتحتفظ به عادة جهة تصديق، حيث تقوم بإرساله بالبريد الإلكتروني إلى كل من يرغب في التعامل مع صاحب التوقيع الإلكتروني، وبذلك يمكن التحقق من صحة التوقيع، ويجب على جهة التصديق أن تنقل

---

[1] انظر: المادة 48 من القانون 15-04، المتعلق بالتوقيع والتصديق الالكترونيين، مرجع سابق.

[2] إيمان مأمون أحمد سليمان، مرجع سابق، ص 316.

التوقيع الإلكتروني بمفتاحه الخاص بطريقة آمنة موثوق بها، دون احتفاظ بصورة من التوقيع بمفتاحه الخاص[1].

وفي الأخير نخلص إلى أن الوسائل القانونية لأمن البيانات الشخصية تجعل المعاملات الإلكترونية أكثر موثوقية، بالإضافة إلى تمتعها بالأمان والثقة لدى مستخدميها وحمايتها من التقليد والتزوير.

ونظم المشرع الوسائل القانونية لأمن البيانات الشخصية في مجال التجارة الإلكترونية في القانون المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين من خلال جهات مختصة تسهر على حماية البيانات الشخصية للأطراف.

والواضح أن أمن البيانات مصلحة من المصالح الجديرة بالحماية ،كونها عنصر أساسي تقوم عليه التجارة الإلكترونية، وإزاء هذه الأهمية وجب توفير وسائل تقنية وقانونية بهدف بث الثقة والأمان في المعاملات التي تتم عبر الوسائط الإلكترونية، حيث لجأ التقنيون إلى حمايتها من المخاطر التي قد تتعرض لها من تزوير، وتخريب، وإتلاف، وسرقة وتشويه إضافة إلى منع الدخول إليها أو تعديلها أو استخدامها استخداما غير مشروع، باستعماله تقنيات التشفير وبروتوكولات الحماية، كم اعتبر المشرع الجزائري التصديق الالكتروني من أهم الآليات التي تسمح بتأمين التوقيع الالكتروني وبعث الثقة فيه.

والملاحظ مما تقدم أن إصدار المشرع الجزائري للقانون المتعلق بالتوقيع والتصديق الالكترونيين يعتبر خطوة مهمة في طريق إرساء قواعد التجارة الالكترونية بصفة عامة، ويظهر واضحا أهميتهما في بعث الثقة الكاملة في المعاملات الالكترونية، كما لا يمكن تجاهل دورهما الفعال في حماية البيانات ذات الطابع الخاص، من خلال نسبة التوقيع لصاحبه، ومنع استعماله من قبل الغير.

[1] محمد مأمون سليمان، مرجع سابق، ص 253.

وعلى الرغم من النجاعة الظاهرة لهذه الإجراءات في حماية وحفظ المعلومات وصحة البيانات، إلا أن يد العابثين يمكن أن تطالها وتنزع منها قوتها كأدوات حفظ وحماية، حيث أصبح من السهل فك الشفرة أو تقليدها والدخول إلى المواقع المشفرة والاطلاع على البيانات المحجوبة، الأمر الذي يدفعنا إلى القول بأن هذه الحماية القبلية وعلى مختلف أشكالها لا تستطيع لوحدها الحد من ظاهرة القرصنة، لأنها ما هي إلا إجراءات وتدابير وقائية الهدف منها منع وقوع فعل الاعتداء أكثر من كونها إجراءات تقف في وجه من تسول له نفسه التعدي على حقوق غيره، حيث أن بيئة التجارة الإلكترونية وحماية البيانات والأسرار المتعلقة بأطراف المعاملة تحتاج إلى الجزاء الرادع مثل احتياجها للإجراء الإحترازي، ولهذا تضمنت معظم التشريعات الجزائية عقوبات سالبة للحرية وغرامات مالية كبيرة تم توقيعها بحق المعتدين على أي حق من حقوق المتعاملين في إطار البيئة الرقمية بشكل عام، والبيانات الشخصية بصفة خاصة، الأمر الذي يدفعنا إلى البحث عن هذه الوسائل وهذا ما ستتم دراسته في الفصل الثاني، بالإضافة إلى جزاءات مدنية تسمح للمتضرر الحصول على التعويضات اللازمة.

الفصل الثاني

وسائل الحماية القانونية للبيانات الشخصية في مجال التجارة الالكترونية

المبحث الأول: وسائل الحماية الجزائية للبيانات الشخصية في مجال التجارة الإلكترونية

المبحث الثاني: وسائل الحماية المدنية للبيانات الشخصية في مجال التجارة الالكترونية

إن تفاقم الاعتداءات على البيانات الشخصية في مجال التجارة الإلكترونية، خاصة في حالة ضعف الحماية الفنية، استدعى تدخلا تشريعيا لتوفير وسائل تكفل الحماية القانونية للبيانات الشخصية في مجال التجارة الإلكترونية.

إذ أن خصوصية جرائم الاعتداء على الخصوصية عن طريق الانترنت، أبرزت مشكلة المكافحة الإجرائية للجريمة المعلوماتية، الأمر الذي دفع المشرع إلى مواكبة هذا التطور الذي لحق الجريمة المعلوماتية، بتعديل بعض المواد في قانون الإجراءات الجزائية، وإصدار قوانين خاصة وجديدة في مجال الإجراءات، كما أنه استحدث جرائم بموجب تعديله لقانون العقوبات بالقانون 04-15[1] تجريم بعض الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات بهدف توفير الحماية الموضوعية (المبحث الأول)، كما قام بتفعيل المسؤولية المدنية لمقدمي خدمات التصديق الإلكتروني والوسطاء في مجال الخدمات الإلكترونية في حالة الإخلال ببنود العقد الذي يجمعهم مع أطراف المعاملة الإلكترونية، أو في حالة القيام بفعل غير مشروع يمس أمن البيانات الشخصية (المبحث الثاني).

[1] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 08 جوان 1966 والمتضمن قانون العقوبات، ج ر عدد 71، صادر في 10 نوفمبر 2004.

المبحث الأول: وسائل الحماية الجزائية للبيانات الشخصية في مجال التجارة الالكترونية

تتميز الجريمة المعلوماتية بصعوبة ارتكابها نظرا لخصوصيتها، كما أن آثارها ليست محصورة في نطاق إقليمي محدد، بالإضافة إلى أنها تستهدف محلا من طبيعة خاصة، وهي البيانات التي يحتوي عليها نظام المعالجة الآلية للمعطيات، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة هذه الجريمة.

تماشيا مع خصوصية هذه الجرائم وضع المشرع قواعد في قانون الإجراءات الجزائية، واستتبعها بقواعد أخرى في القانون المتعلق بالوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال (المطلب الأول)، كما أنه حاول التصدي لها من خلال نصوص موضوعية تجرم الأفعال الماسة بأنظمة المعالجة الية للمعطيات (المطلب الثاني).

المطلب الأول: إجراءات المتابعة في الجرائم الماسة بأمن البيانات الشخصية في مجال التجارة الإلكترونية

إذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين متعودة على التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية، فإن المشكلات الإجرائية التي تواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية تبدأ من طبيعة البيئة الافتراضية، فضلا عن إمكانية إخفائها عن طريق التلاعب بالبيانات ومحو الدليل من مسرح الجريمة، لهذا يحتاج هذا النوع من الجرائم إلى إجراءات خاصة في البحث والتحري (الفرع الأول)، فضلا عن ضرورة وجود هيئات خاصة بمتابعة هذا النوع من الجرائم (الفرع الثاني).

الفرع الأول: خصوصية إجراءات المتابعة في جرائم الاعتداء على البيانات الشخصية الالكترونية

إن خصوصية إجراءات المتابعة في الجرائم الماسة بأمن البيانات الشخصية تظهر من خلال توسيع صلاحيات الضبطية القضائية(أولا) ومراقبة الاتصالات الإلكترونية (ثانيا)، كما أنها تستدعي تفتيش النظم المعلوماتية (ثالثا) وحجز المعطيات المعلوماتية (رابعا).

أولا- توسيع صلاحيات الضبطية القضائية:

إن لسلطة الضبط القضائي[1] دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها[2]، في نطاق إقليمي محدد يسمى بدائرة الاختصاص الإقليمية، ويتحدد هذا الأخير بمعالم الجريمة أو بصفة عضو الضبطية القضائية والجهة التي ينتمي إليها، وقد يمتد هذا الاختصاص إلى كافة دائرة المجلس القضائي[3]، كما يمكن أن يمتد إلى كامل التراب الوطني في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[4].

بحيث منح المشرع لضباط الشرطة القضائية على اختلاف الجهات التي ينتمون إليها اختصاصا وطنيا لمباشرة صلاحياتهم في البحث والتحري، ويشترط لتمديد هذا الاختصاص أن تكون الجريمة ماسة بالأنظمة المعلوماتية، وأن يتم العمل تحت إشراف النائب العام لدى المجلس القضائي المختص، كما يجب إعلام وكيل الجمهورية المختص إقليميا[5].

كذلك يمتد اختصاص الضبطية القضائية إلى كامل التراب الوطني إذا كانوا بصدد مراقبة أشخاص توافرت ضدهم مبررات مقبولة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ومن بينهم المجرمين المعلوماتيين، باعتبار أن هذا الشكل من الجرائم يجد مجال المعلوماتية فضاء خصبا للممارسة النشاط الإجرامي[6].

---

[1] عرف المشرع الجزائري الضبط القضائي على أنه مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها بتحقيق قضائي، المادة 3/12 من الأمر رقم 66-155، مؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، ج ر عدد 48، صادر في 10 جوان 1966، المعدل والمتمم.

[2] مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص46.

[3] أمال حابت، "الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري"، مداخلة مقدمة ضمن أشغال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد يومي 16، 17 نوفمبر 2015، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، ص5.

[4] المادة 7/16 من الأمر 66-155، يتضمن قانون الإجراءات الجزائية، المعدل والمتمم، مرجع سابق.

[5] أمال حابت، مرجع سابق، ص5.

[6]، المرجع نفسه ، ص6.

ومبرر تمديد الاختصاص الاقليمي لضباط الشرطة القضائية يرجع إلى طبيعة الجريمة المرتكبة في حد ذاتها، والتي ترتكب في الغالب في العالم الافتراضي، الذي لا يعترف بالحدود الجغرافية، ولا يقيم لها اعتبارا.

ثانيا – مراقبة الاتصالات الإلكترونية:

عرف المشرع الجزائري الاتصالات الإلكترونية في نص المادة 2 من القانون رقم09-04 المتعلق بالجرائم الماسة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها: "تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة اي وسيلة إلكترونية"[1].

إن إجراء المراقبة الإلكترونية جديدا على المنظومة القانونية الإجرائية الوقائية، فقد نص عليه المشرع في قانون الإجراءات الجزائية في الفصل المتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ولكن يتم تطبيقه على مجموعة من الجرائم محددة على سبيل الحصر في المادة 65 مكرر 5 من ق.إ.ج[2]، وبالتالي يمكن اعتراض مراسلات في إطار تحريات الشرطة القضائية أو تحقيقات قضائية في الجرائم المذكورة في هذه المادة والتي كانت من بينها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

وبالنص على هذا الإجراء في القانون 09-04 فإن المشرع قد أعطى تصريحا للجهات القضائية باستعماله تطبيقا لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[3] وكذا في إطار تنفيد طلبات المساعدة القضائية الدولية المتبادلة لجمع الأدلة الخاصة

---

[1] القانون 09-04،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما، مؤرخ في 5اوت 2009،ج ر عدد 47،صادر في 16 اوت 2009.

[2] المادة 65 مكرر5 من 66-155، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، إذا اقتضت ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...

[3] المادة 4 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، مؤرخ في 05 أوت 2009، ج ر عدد 47، صادر في 16 أوت 2009.

بالجريمة في الشكل الإلكتروني، بشرط المحافظة على سرية البيانات المبلغة، وعدم استعمالها في غير ما هو موضح في الطلب[1].

ثالثا – تفتيش المنظومة المعلوماتية:

الأصل في القانون أن الإذن بالتفتيش إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جناية أو جنحة واقعة بالفعل، وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية[2].

نص المشرع الجزائري على إجراءات التفتيش في نص المادة 44 من ق.إ.ج، التي تفرض على ضابط الشرطة القضائية، عند انتقاله إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة، لا يكون إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق، مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش[3].

والمشرع في المادة 5 من القانون رقم 09-04 أحال إلى أحكام التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وإن اختلف التفتيش في مجال الجرائم المعلوماتية من حيث مضمونه عن التفتيش العادي، بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 44 من ق.إ.ج، مع مراعاة أحكام الفقرة الأخيرة من المادة 05 السالفة، لأننا بصدد جرائم معلوماتية، والتي تسمح للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

---

[1] المادة 09 من القانون 09-04، المرجع نفسه.

[2] طارق إبراهيم الدوسقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص396.

[3] المادة 45 من الأمر 66-156، المتضمن قانون العقوبات، المعدل والمتمم، مرجع سابق.

وإن السماح باللجوء إلى الأشخاص المؤهلين، كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسوب لإجراء عمليات التفتيش على المنظومة المعلوماتية وجمع المعطيات المتحصل عليها والحفاظ عليها، وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات، يسمح بجعل التفتيش أكثر دقة، ولكن المشرع لم يبين لنا طبيعة العمل الذي يقوم به هؤلاء الأشخاص، هل يدخل في إطار ما يعرف بالخبرة، وتطبق عليه النصوص القانونية المتعلقة بها،[1] أم أنه إجراء ذو طبيعة خاصة يدمج مباشرة في أعمال الشرطة القضائية.

والواضح أن هذا الإجراء جاء بسبب تيقن المشرع الجزائري بعدم تخصص ضباط الشرطة القضائية في مجال المعلوماتية، بالشكل الذي يسمح بمواكبة التكنولوجيات الحديثة والمعقدة في مجال القرصنة المعلوماتية وبرامج الإعلام الآلي.

كما ونص المشرع على حالات اللجوء إلى تفتيش المنظومة المعلوماتية، وهي نفسها الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية للاتصالات.

وقد نص القانون 09-04 على إجراء التفتيش على المنظومة المعلوماتية عن بعد كإجراء جديد، بحيث يمكن الدخول إليها دون إذن صاحبها، بالدخول ولو عن بعد في الكيان المنطقي للحاسوب، للتفتيش عن الأدلة في المعلومات التي يحتوي عليها هذا الأخير، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها[2].

رابعا- حجز المعطيات المعلوماتية:

إن الحجز هو إجراء مقرر في القواعد العامة بموجب المادة 42 فقرة 3 من ق.إ.ج حيث يمكن لضباط الشرطة القضائية حجز كل الأشياء والوثائق التي استعملت في الجريمة أو شكلت نتيجة لها عندما تكون هذه المضبوطات ضرورية لكشف الحقيقة، وبالتالي فإن

---

[1] أنظر: المواد 143 إلى 156 من الأمر 66-155، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، مرجع سابق.

[2] آمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)"، مداخلة مقدمة ضمن أشغال الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد يوم 29 مارس 2017، مركز جيل البحث العلمي، الجزائر العاصمة، ص77.

الدعائم الرقمية (الإلكترونية) مثل الأقراص المضغوطة، الهواتف النقالة يمكن وضعها في أحراز حسب ما نص عليه قانون الاجراءات الجزائية.

ولخصوصية الوسائل المستعملة في ارتكاب الجرائم في العالم الافتراضي، فقد خص المشرع الضبط في هذا المجال بأحكام منفردة، جاءت في المادة 06 من القانون 09-04 حيث أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوظائف في أحراز يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

كما أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض في التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[1].

وإذا استحال إجراء الحجز لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية او الى نسخها ،الموضوعة تحت تصرف الاشخاص المرخص لهم باستعمال هذه المنظومة[2]

الفرع الثاني: الجهات المختصة في مجال جرائم الاعتداء على البيانات الشخصية الإلكترونية

نظرا لخصوصية إجراءات المتابعة في جرائم الاعتداء على البيانات الشخصية استحدث المشرع جهات مختصة للنظر في هذه الجرائم ومتابعتها، تتمثل في الهيئة الوطنية

---

[1] آمنة أمحمدي بوزينة، مرجع سابق، ص 78.

[2] المادة 7 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، مرجع سابق.

للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال ومكافحتها (أولا) والفروع المختصة بالنظر في الجرائم الماسة بالمعالجة الآلية للمعطيات (ثانيا).

أولا- الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال:

يتم التطرق من خلال هذه الجزئية إلى تحديد الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال ودورها في الوقاية من الجرائم المعلوماتية.

1- الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال:

تعد الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال ومكافحتها المستحدثة بموجب المادة 13 من القانون 09-04،[1] سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل[2].

تتشكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من لجنة مديرة، وثلاثة مديريات ومركز للعمليات التقنية، وملحقات جهوية[3].

كما يتمثل أعضاءها في الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا، تحت رئاسة الوزير المكلف بالعدل[4].

---

[1] تنص المادة 13 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، على أنه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته..."

[2] المادة 2 من المرسوم الرئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53 ، صادرة في 08 أكتوبر 2015.

[3] المادة 6 من المرسوم الرئاسي 15-261، المرجع نفسه.

[4] المادة 7 من المرسوم الرئاسي 15-261، المرجع نفسه.

والملاحظ في تشكيلة اللجنة أنها تتشكل من أعضاء أغلبهم متخصصين في المجال الأمني والقضائي، ما دام عمل اللجنة يتعلق بالجرائم المتصلة بتكنولوجيا الاتصال والإعلام، وهو ما يجعل عمل اللجنة أكثر فعالية سواء في مجال الوقاية أو المكافحة.

2- دور الهيئة الوطنية في الوقاية من جرائم الاعتداء على البيانات الشخصية الإلكترونية:

تتمثل بعض مهام الهيئة الوطنية في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية، وتشكل اعتداء على البيانات الشخصية لأطراف المعاملة الإلكترونية[2].

كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية، في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، وضمان مراقبة الاتصالات الإلكترونية[3].

أما فيما يخص مجال تطبيق الوقاية من هذه الجرائم، ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.[4]

---

[1] المادة 14 من القانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، مرجع سابق.

[2] المادة 2 من القانون 09-04، المرجع نفسه.

[3] المادة 4 من المرسوم الرئاسي 15-261، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[4] المادة 3 من القانون 09-04، مرجع سابق.

إن إنشاء هذه الهيئة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك مجال الجزائي من أجل تحسين حماية خصوصية متعاملي شبكة الأنترنت وتشديد العقوبات على أي تقصير في هذا المجال.[1]

ثانيا- الجهات المختصة بالنظر في الجرائم الماسة بالمعالجة الآلية للمعطيات

يتم التطرق من خلال هذه الجزئية إلى تحديد الطبيعة القانونية للأقطاب القضائية المتخصصة من حيث تشكيلتها ، ودورها في نظر جرائم الاعتداء على البيانات الشخصية.

1- مدى اعتماد نظام الأقطاب المتخصصة في المسائل الجزائية:

أدرجت الأقطاب القضائية المتخصصة في الجزائر ضمن المادة 24 من القانون المتعلق بالتنظيم القضائي، والتي ألغيت في قرار المجلس الدستور المتعلق بمراقبة مطابقة القانون العضوي للتنظيم القضائي[2]، حيث أصدر المجلس الدستوري بعد إحالة مشروع القانون العضوي عليه رأيا بعدم مطابقة هذا النص لأحكام الدستور، حيث اعتبر أن المشرع عند إقرار إمكانية إنشاء هيئات قضائية مسماة "أقطاب قضائية متخصصة في نص المادة 24 من القانون العضوي، يكون قد تجاوز مجال اختصاصه من جهة، وأن تنازله عن صلاحيات إنشاء هذه الهيئات للتنظيم، يكون قد أخل بالمبدأ الدستوري القاضي بتوزيع مجالات الاختصاصات من جهة أخرى.[3]

وعليه فالقارئ لنص المادة 24 الملغاة التي تنص على أنه: "يمكن إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم..."، يلاحظ أن المشرع وفر إمكانية إنشاء أقطاب قضائية متخصصة لدى المحاكم وليس محاكم قائمة بذاتها، وعلى هذا

---

[1] آمنة أمحمدي بوزينة، مرجع سابق، ص79.

[2] رأي رقم 01 / ر.ق.ع/م د/05، مؤرخ في 17 جوان 2005، يتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي للدستور، البند الثاني من الموضوع المتعلق بفحص المادة 24 من القانون العضوي محل الإخطار، ج ر عدد 51، صادرة في 20 جويلية 2005.

[3] محمد بكرارشوش، "الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري"، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، العدد 14، 2006، ص312.

الأساس فإن موقف المجلس الدستوري جاء دفاعا على أحكام الدستور المادة 6/140[1] التي تخول للسلطة التشريعية إنشاء هيئات قضائية بموجب قانون عادي، وليس بموجب قانون عضوي.

وبعد رأي المجلس الدستوري صدر النص خاليا من أي عبارة تشير إلى الأقطاب القضائية المتخصصة لاسيما نص المادة 13 من القانون العضوي رقم 05-11 التي تضمنت أحكام تنظيم المحكمة في شكل أقسام ولم يشر إلى القطب.[2]

وعليه فالفروع الجزائية المتخصصة لا تمثل جهات قضائية قائمة بذاتها داخلة في هيكل التنظيم القضائي الجزائي، وإنما هي عبارة عن تخصص في المحاكم الجزائية.[3]

2- الفروع الجزائية المتخصصة:

عالج المشرع الاختصاص النوعي للفروع الجزائية المتخصصة بالمواد 37، 40، 329 من ق.إ.ج، وهي نفسها النصوص التي تحدد الاختصاص الإقليمي المحلي لكل من وكيل الجمهورية، قاضي التحقيق والمحكمة في الظروف العادية، لكن يتم توسيع هذا الاختصاص ليشمل اختصاص إقليمي لجهات قضائية أخر عندما يتعلق الأمر بجرائم مذكورة على سبيل الحصر، ومن بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[4]، حيث جاءت كالتالي:

1- وكيل الجمهورية: نصت المادة 2/37 من ق.إ.ج على أنه: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم...".

---

[1] المادة 140 من المرسوم الرئاسي رقم 96-438، يتعلق بإصدار نص تعديل الدستور ، مرجع سابق.

[2] المادة 13 من القانون رقم 05-11، مؤرخ في 17 يوليو 2005، يتعلق بالتنظيم القضائي، ج ر عدد 51، صادرة في 20 يوليو 2005.

[3] محمد بكرارشوش، مرجع سابق، ص311.

[4] المرجع نفسه، ص320.

2- قاضي التحقيق: حيث جاء في المادة 40 الفقرة 2 من ق.إ.ج أنه: "يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...".

3- المحكمة كفرع جزائي متخصص: تناولت المادة 329 الفقرة 5 من ق.إ.ج مسألة تحديد الاختصاص النوعي لها، حيث جاء فيها: "يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...".

كما أشارت هذه النصوص إلى أن مسألة تمديد الاختصاص لكل من وكيل الجمهورية وقاضي التحقيق والمحكمة المختصة تعود إلى التنظيم، وهو ما تجسد بالفعل في سنة 2006 بموجب المرسوم التنفيذي رقم 06-348[1] الذي نص في المادة الأولى منه، على أن هذا المرسوم جاء تطبيقا لأحكام المواد 37، 40 و329 من ق.إ.ج والتي خولته تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى، موضحة ذلك على سبيل التدقيق في جرائم معينة لاسيما منها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

المطلب الثاني: تعدد جرائم الاعتداء على البيانات الشخصية في مجال التجارة الإلكترونية

بالرغم من أن النظم القانونية في بعض الدول توفر الحماية الخاصة للبيانات الشخصية في مجال التعاملات الإلكترونية، إلا أنه يتصور أن يتم التعدي على هذه البيانات والمعلومات بأي صورة، نظرا لطبيعة التعاملات الإلكترونية وإمكانية الاطلاع على البيانات والدخول إليها في أي مكان، ولهذا تفطن المشرع الجزائري لحماية هذا الحق من الاعتداء وذلك بتعديل قانون العقوبات بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006،

[1] مرسوم تنفيذي 06-348، مؤرخ في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر عدد 63، صادر في 08 أكتوبر 2006.

بحيث جرّم من خلاله الاعتداء على الحياة الخاصة للأشخاص (الفرع الأول)، كما جرّم من خلال القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين العديد من الجرائم الماسة بالتوقيع الالكتروني، في سبيل بث الثقة والأمان في المعاملات الالكترونية، كما أن المشرع الجزائري أورد بعض الأحكام الجزائية المتعلق بمخالفة البنوك لقواعد الأمن المقررة في المجال المصرفي (الفرع الثاني).

الفرع الأول: الجرائم المقررة في القواعد العامة

في سبيل تحقيق حماية جنائية خاصة للبيانات الشخصية الإلكترونية، يمكن تطبيق بعض العقوبات المقرر للجرائم تقليدية في إطار قانون العقوبات، بحيث حظر المشرع الاعتداء على الحياة الخاصة للأفراد (أولا)، بالإضافة إلى ذلك يمكن تطبيق العقوبات الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، في حالة إذا أدت ارتكاب هذه الجرائم بالمساس بالبيانات الشخصية (ثانيا).

أولا- الجرائم التقليدية:

تتمثل هذه الجرائم في جرائم الاعتداء على الحياة الخاصة للأفراد والمنصوص عليها في المواد 303، 303 مكرر، 303 مكرر 1 من قانون العقوبات، والمتمثلة في:

1- جريمة المساس بحرمة الحياة الخاصة:

يعتبر المساس بالحياة الخاصة عند التعدي على المعلومات سواء كانت صحيحة أو مشوهة، وقد نص المشرع الجزائري على هذه الجريمة في نص المادة 303 مكرر، 303 مكرر 1 من قانون العقوبات، ولقيام هذه الجريمة يتطلب توافر ركنين أحدهما مادي والآخر معنوي.

أ - الركن المادي:

تعد جريمة المساس بحرمة الحياة الخاصة للأشخاص كل تعمد بأي تقنية أو وسيلة تمس بالشخص في الحالات التالية:

– التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية أو نقل صورة شخص في مكان خاص بغير إذن صاحبها أو رضاه.

– كل من احتفظ بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليهما.

فبالنسبة لالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة سرية ،فكل من استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة مهما كانت نوعيتها، ومهما كانت نوعية المحادثات التي جرت في مكان خاص أو عن طريق الهاتف، يعد مرتكبا لهذه الجريمة[1].

إلى جانب ذلك جرّم المشرع التقاط أو تسجيل أو نقل صورة شخص في مكان خاص بغير إذن صاحبها أو رضاه، أي التقاط الصورة وتثبيتها في أجهزة التصوير أو إرسالها إلى مكان آخر[2].

كما تتحقق هذه الجريمة بإيداع أو استعمال أو الاحتفاظ، فكل من سمح بأن توضع في متناول الجمهور أو الغير تعد جريمة يعاقب عليها القانون.

ولقد اشترط المشرع الجزائري لقيام هذه الجريمة عدم رضا الضحية عن القيام بهذه الأفعال، وقد اعتبرها جنحة ويعاقب على الشروع فيها، إلا أن صفح الضحية يخلص الجاني من المسؤولية الجنائية[3].

ولهذا يجب في مجال التجارة الإلكترونية التأكد من صحة المعلومات المدخلة، فإذا كانت غامضة أو فيها انتحال لصفة أو اسم الغير بدون وجه حق، تقوم جريمة الاعتداء على خصوصية المعلومات والمراسلات التي تتم عبر الانترنت بشكل غير مشروع[4].

---

[1] صالح شنين، مرجع سابق، ص200.

[2] المرجع نفسه، ص200.

[3] المادة 303 مكرر من الأمر 66–156، المتضمن قانون العقوبات، المعدل والمتمم، مرجع سابق.

[4] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، (د ط)، منشأة المعارف، الإسكندرية، مصر، 2009، ص342.

ب- الركن المعنوي:

جريمة المساس بحرمة الحياة الخاصة جريمة عمدية، تتخذ صورة القصد الجنائي العام المتمثل في العلم والإرادة، وبالتالي يجب أن يعلم الجاني أن من شأن فعله أن يشكل جريمة، ويجب أن تتجه إرادته نحو تلك الأفعال الإجرامية، ولا عبرة بالدوافع لارتكاب هذه الجريمة[1].

فإن لم يكن يعلم أن مصدرها غير مشروع، ولم يكن يعلم أن محتوى التسجيل أو الوثائق التي يستعد لإعلام الجمهور أو الغير بها أو استخدامها، فلا تقوم الجريمة ولا تثبت المسؤولية في جانبه[2].

ج- العقوبة المقررة لهذه الجريمة:

نظرا لخطورة هذه الجريمة على الحياة الخاصة للأفراد فقد قرر لها المشرع عقوبة تقدر بالحبس من ستة أشهر إلى 3 سنوات وبغرامة من 50.000دج إلى 300.000دج.[3]

ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة ويضع صفح الضحية حدا للمتابعة الجزائية.

2- جريمة الاعتداء على حرمة المراسلات:

تدعيما للحماية الدستورية التي قررها المشرع لحرمة المراسلات، نص أيضا في قانون العقوبات على حماية هذا العنصر من عناصر الحياة الخاصة للأشخاص، وذلك في نص المادة 303 مكرر السالفة الذكر.

---

[1] صالح شنين، مرجع سابق، ص200.

[2] صفية باشتان، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة مقدمة لنيل شهادة دكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، السنة 2012 ، ص408.

[3] المادة 303 مكرر من الأمر رقم 66-156، المتضمن قانون العقوبات، المعدل والمتمم، مرجع سابق.

ولقد اكتفى المشرع لقيام هذه الجريمة القيام بعملتي فض واتلاف الرسائل أو المراسلات الموجهة إلى الغير، فهذه الجريمة تتحقق في صورتين تتمثل بفض أو فتح الرسائل أو المرسلات وإفشاء ما تحتويه من أسرار للغير، كما يشترط لقيام هذه الجريمة نية الإضرار بالغير بفعل الفتح أو اتلاف رسائل أو مراسلات الغير حسب نص المادة 303 "... وذلك بسوء نية"، مما يستبعد مسؤولية الشخص الذي يفتح رسالة ويطلع على محتواها ظنا منه أنها موجهة إليه، إلا أنه ملزم بإثبات حسن نيته[1].

ولتوقيع العقوبات المقررة لهذه الجريمة في مجال البيانات الشخصية الالكترونية، فإنه يشترط في البيانات والمعلومات التي يتم إفشاؤها أن تتعلق بالشخص صاحب المعاملة الإلكترونية، وإفشاء هذه المعلومات يعني نقلها وإطلاع الغير عليها، بعد أن كان العلم بها قاصرا على أصحابها[2].

فجريمة التعدي على حرمة المراسلات والاطلاع على الأسرار وإفشاؤها أو اتلافها، يتم باستدعاء المعلومات، وفتح السجلات الإلكترونية والاطلاع عليها، من خلال شاشة الكمبيوتر، أو أي جهاز الكتروني آخر[3].

ولأن سرية المراسلات تدخل في نطاق حماية حرمة الحياة الخاصة، فإن توقع عليها ذات العقوبات المشار إليها في نص المادة 303 من قانون العقوبات، وهي الحبس من شهر واحد إلى سنة وبغرامة من 25.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية.

---

(1) صفية باشتان، مرجع سابق، ص416

(2) عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني (دراسة تأصيلية مقارنة)، (د ط)، دار الكتب القانونية، القاهرة، مصر، 2007، ص507.

(3) خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للطباعة والنشر والتوزيع، (د ط)، الإسكندرية، مصر، 2008، ص72.

ثانيا – الجرائم المستحدثة:

تخص هذه الجرائم أنظمة المعالجة الآلية للمعطيات[1]، استحدثها المشرع بموجب القانون 06-22 المعدل والمتمم للقانون 66-156 المتضمن قانون العقوبات، وتعتبر هذه النصوص القانونية من أهم الأحكام الجزائية التي تقرر حماية خاصة للبيانات الشخصية الالكترونية، في حالة إذا ما وقع الاعتداء عليها، وتتمثل هذه الجرائم في:

1- جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي:

تعد جريمة الدخول والبقاء غير المشروع من أهم جرائم المعطيات والجرائم المعلوماتية بصفة عامة، ذلك أن أغلب جرائم المعطيات لا يمكن ارتكابها إلا بعد الدخول إلى النظام، ولهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف الجرائم الأخرى[2]، وقد نص عليها المشرع الجزائري في نص المادة 394 مكرر من ق.ع.ج، وحتى تقوم هذه الجريمة يجب أن يتوفر ركينها المادي والمعنوي.

أ- الركن المادي:

يعد السلوك الإجرامي من أهم عناصر السلوك المادي ويأخذ صورتي الدخول والبقاء[3]، وينصرف مصطلح الدخول في إطار المعلوماتية ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي، ويتحقق الدخول غير المشروع إلى الجهاز بالوصول إلى المعلومات والبيانات المخزنة داخل نظام الكمبيوتر، دون رضا المسؤول عن هذا النظام[4].

---

(1) يعرّف نظام المعالجة الآلية للمعطيات بأنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية".
أنظر: أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للنشر والتوزيع، الجزائر، 2007، ص102.

(2) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، (د ط)، دار الفكر الجامعي، القاهرة، مصر، 2007، ص306.

(3) المرجع نفسه، ص306.

(4) خالد ممدوح إبراهيم، أمن المستندات الإلكترونية، (د ط)، الدار الجامعية، مصر، 2008، ص148.

أما فعل البقاء غير المشروع داخل النظام المعلوماتي، فيقصد به التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام ومن له السيطرة عليه، كما يتحقق الركن المادي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به[1].

ب- الركن المعنوي:

جريمة الدخول أو البقاء غير المشروع في صورتهما البسيطة أو المجردة من الجرائم العمدية تقوم على القصد الجنائي العام، ولا تتطلب قصدا خاصا، وعلى ذلك يجب أن يشمل علم الجاني كل واقعة تدخل في تكوين جريمة الدخول وبالبقاء، فيتعين أن ينصب علمه إلى أن فعله ينصب على نظام للمعالجة الآلية للمعطيات والبيانات[2].

ج- العقوبة المقررة لهذه الجريمة:

نص المشرع الجزائري على عقوبة هذه الجريمة في نص المادة 394 مكرر من ق.ع.ج "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

وقد أشار المشرع في هذه المادة على تجريم فعل الشروع في هذه الجريمة وذلك بقوله في نص المادة 394 مكرر "أو يحاول ذلك".

2- جريمة التلاعب في أنظمة المعالجة الآلية للمعطيات:

يقصد بالتلاعب في بيانات أنظمة المعالجة الآلية للمعطيات إدخال معطيات جديدة غير صحيحة أو تعديل أو محو معطيات كانت قائمة، ويشترط أن تكون هذه المعطيات في

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص161.

[2] عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص316.

النظام لمعالجتها، أي غير منفصلة عن النظام[1]، وقد نص عليها المشرع الجزائري في المادة 394 مكرر 1 من ق.ع.ج.

وحتى تقوم هذه الجريمة يجب أن يتوفر ركنين أحدهما مادي والآخر معنوي.

أ- الركن المادي:

ويتمثل الركن المادي في هذه الجريمة في التلاعب ببيانات أنظمة المعالجة الآلية للمعطيات، عن طريق الإدخال أو الإزالة أو التغيير، ولا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني أحدها فقط لكي يتوفر الركن المادي.

يتحقق الإدخال بإضافة معطيات جديدة إلى النظام[2]، أما المحو فيتحقق بإزالة جزء من معطيات مسجلة في الحاسب الآلي، أو إضافة جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، بخلاف التعديل الذي يتحقق بتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى[3].

ولقد وردت الأفعال السابقة على سبيل الحصر، فهذه الجريمة لا تتحقق بغيرها ،فحتى ولو وقع الاعتداء على معطيات المواقع، فلا يخضع لنص جريمة التلاعب، لأنها لا تتحقق بإدخال ومحو وتغيير المعطيات[4].

ب- الركن المعنوي:

يتمثل الركن المعنوي في هذه الجريمة في القصد الجنائي العام، ولا يشترط توافر القصد الجنائي الخاص، إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على المعطيات بالإدخال أو التعديل أو المحو، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في

---

(1) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص189.

(2) آمال قارة، مرجع سابق، ص120-121.

(3) عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية)، (د ط)، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص ص93-95.

(4) صالح شنين، مرجع سابق، ص91.

المعطيات[1]، وبالتالي فإنه إذا توافر القصد الجنائي العام بعنصريه العلم والإرادة إلى جانب الركن المادي، تقع جريمة الاعتداء العمدي على المعطيات، وتوقع على مرتكب الجريمة العقوبة المقررة لها[2].

ج- العقوبة المقررة لهذه الجريمة:

حددت المادة 394 مكرر 01 من ق.ع.ج العقوبات المطبقة على هذا النوع من الجرائم بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من50.000 دج إلى150.000 دج.

3- جريمة التعامل في معطيات غير مشروعة:

جرّم المشرع مجموعة من الأفعال تصب كلها في التعامل في معطيات صالحة لأن ترتكب بها إحدى جرائم المعطيات، كما قام بتجريم أشكال من التعاملات في المعطيات التي يتم الحصول عليها من إحدى الجرائم، فكل المعطيات غير مشروعة سواء كانت صالحة لأن ترتكب بها جريمة أو كانت متحصلة من جريمة[3]، نص عليها المشرع في المادة 394 مكرر 2 من ق.ع.ج، وهذه الجريمة تتكون من ركنين مادي ومعنوي.

أ- **الركن المادي:** يتكون الركن المادي في جريمة التعامل في معطيات غير مشروعة صورتين أولهما تتمثل في التعامل في معطيات صالحة لارتكاب الجريمة والثانية هي التعامل في معطيات متحصلة من جريمة[4].

أ-1- التعامل في معطيات صالحة لارتكاب جريمة:

تجرم المادة 394 مكرر 2 من ق.ع.ج في البند الأول منها، مجموعة من الأفعال الخطرة التي لو تركت بدون تجريم لأدت إلى حدوث جرائم أخرى، هذه الأفعال تشمل كافة أشكال التعامل الواقعة على المعطيات، والتي تسبق عملية استعمال هذه المعطيات في ارتكاب الجريمة، فالمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل

---

(1) آمال قارة، مرجع سابق، ص125.

(2) صالح شنين، مرجع سابق، ص92.

(3) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص193.

(4) المرجع نفسه، ص200.

إلى يد الجاني فيرتكب بها جريمته، وهذه المراحل تبدأ من تصميم هذه المعطيات والبحث فيها وتجميعها، وصولا إلى جعلها في متناول الغير، وذلك بتوفيرها أونشرها أو الاتجار فيها.

ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداهما فقط، وهذه الأفعال هي التصميم والبحث والتجميع والتوفير (الوضع تحت التصرف أو العرض) والنشر والاتجار[1].

أ-2- التعامل في معطيات متحصلة من جريمة:

يقوم الركن المادي لهذه الجريمة بالحيازة أو الإفشاء أو النشر أو الاستعمال لأي غرض كان للمعطيات المتحصل عليهما من إحدى هذه الجرائم المعلوماتية، وتتحقق الحيازة بسيطرة الحائز على البيانات، ويستوي أن تكون حيازة البيانات بقصد محوها أو تعديلها أو استعمالها تحت أي شكل، فيجب بداية ثبوت واقعة حيازة الجاني لهذه البيانات حتى يتسنى له محوها أو تعديلها أو استعمالها[2].

ويتمثل الإفشاء في فعل إفشاء البيانات للغير الذي لا يكون من حقه الاطلاع عليها فإذا كان فعل الإفشاء لشخص من حقه الاطلاع على هذه البيانات فإن الركن المادي لا يعد متوافرا وبالتالي لا تتحقق الجريمة[3].

أما النشر فيتحقق بإذاعة البيانات الشخصية محل الجريمة وتمكين الغير من الاطلاع عليها وذلك عن طريق مختلف الوسائل التي يتصور النشر بهامهما كانت طبيعتها.

وإذا كانت حيازة المعطيات وإفشاؤها ونشرها أمورا خطيرة، فإن الأخطر من ذلك كله هو القيام باستعمال هذه المعطيات، ويشمل هذا التجريم كل استعمال للمعطيات مهما كان

---

[1] محمد خليفة، "خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها"، مداخلة مقدمة ضمن أشغال الملتقى الدولي الأول حول التنظيم القانوني للأنترنت والجريمة الالكترونية، المنعقد يومي 27 و 28 أفريل 2009، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 8 ماي 1945 قالمة ، ، ص 384.

[2] صالح شنين، مرجع سابق، ص94.

[3] محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، (د ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص102.

الهدف منه ومهما كان نوعه[1].

ب- الركن المعنوي:

جريمة التعامل في معطيات غير مشروعة عمدية، ويستفاد ذلك من عبارة المادة 394 مكرر2 "عمدا وعن طريق الغش".

وهذه الجريمة في صورتها الأولى، التعامل في معطيات صالحة لارتكاب جريمة، تتطلب قصدا خاصا، هو قصد الإعداد والتمهيد، أما في صورتها الثانية، التعامل في معطيات متحصلة من جريمة، فيكفي لقيامها توافر القصد الجنائي العام[2].

ج- العقوبة المقررة لهذه الجريمة:

نصت المادة 394 مكرر2 من ق.ع.ج على هذه الجريمة بالحبس من شهرين إلى ثلاث سنوات وبغرامة من مليون (1.000.000دج) إلى خمسة ملايين دينار جزائري (5.000.000دج) كل من يقوم عمدا وعن طريق الغش.

الفرع الثاني: الجرائم المقررة في القانون المتعلق بالتوقيع والتصديق الاكترونيين

بالإضافة إلى نصوص قانون العقوبات، باعتبار المجال العادي لتجريم الأفعال وتوقيع العقوبات، أورد المشرع الجزائري نصوص خاصة يمكن أن تطبق في مجال الحماية الجزائية للبيانات الشخصية الالكترونية، ويتعلق الأمر أساسا بالجرائم المقررة المتعلقة بالتوقيع والتصديق الالكترونيين.

والملاحظ أن المشرع الجزائري لم يخص التوقيع الإلكتروني بحماية جنائية خاصة، ولكنه تدارك هذا الأمر بصدور قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، وذلك لخصوصية هذه الجرائم، وتتعدد جرائم الاعتداء على التوقيع الالكتروني، ولكن ما يهمنا في هذه الدراسة، هي تلك التي تمس بالبيانات الشخصية الالكترونية، والتي يمكن

---

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، مرجع سابق، ص210.

[2] محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مرجع سابق، ص385.

إجمالها في حيازة بيانات إنشاء التوقيع الإلكتروني (أولا)، إفشاء بيانات التوقيع الإلكتروني(ثانيا)، واستعمال بيانات إنشاء التوقيع الإلكتروني(ثالثا).

أولا- جريمة حيازة بيانات إنشاء التوقيع الإلكتروني:

يمكن أن يتم الاعتداء على التوقيع الإلكتروني عندما يتم صنع أو حيازة برنامج لإعداد التوقيع الإلكتروني وتقوم هذه الجريمة بتوفر كل من الركن المادي والركن المعنوي.[1]

فالركن المادي يتمثل في صور عديدة وهي صناعة نظام معلوماتي أو برنامج لإعداد توقيع إلكتروني، أو حيازتهما بغرض إعداد توقيع إلكتروني دون موافقة صاحبه[2]، بحيث قد يكون الجاني شخص طبيعي أو اعتباري مرخص وغير مرخص له بإعداد التوقيع الإلكتروني، لأن مناط التجريم هنا أن يتم عمله رغما عن إرادة صاحبه، أما الوسيلة المستعملة في ذلك فهي مجموعة من الأجهزة والأدوات التي يختلس بها الجاني معلومات عن التوقيع القائمة بالفعل، أو يقوم بصناعة برنامج جديد للقيام بعمله غير المشروع[3]، مع العلم أنه لكي تقوم الجريمة يجب أن يكون للنظام القدرة على عمل التوقيع الإلكتروني.

والملاحظ أن المشرع الجزائري قد منح اختصاص إنشاء التوقيع الالكتروني حكرا لمؤدي خدمات التصديق الالكتروني، التي لا يمكنها مباشرة عملها إلا بعد الحصول على الترخيص، وفقا للأشكال القانونية المقررة[4]، بل وإنه لا يمكنها جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة[5]، أي حتى وإن كان هذا الشخص مرخص له بإعداد التوقيع الإلكتروني، فإذا قام بذلك دون موافقة صاحبه عد الفعل جريمة.

---

(1) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، (د ط)، دار الفكر الجامعي، الاسكندرية، مصر، 2002، ص607.

(2) المادة 68 من القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مرجع سابق.

(3) عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص ص161-162.

(4) المادة 35 الفقرة 03، من القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مرجع سابق.

(5) المادة 43 من القانون 15-04، المرجع نفسه.

أما الركن المعنوي فهو أن يكون اتجاه إرادة الجاني إلى صنع أو حيازة برنامج لإعداد التوقيع الإلكتروني، هو الاعتداء على التوقيع الإلكتروني ليحقق غرضه.[1]

وقد قرت لهذه الجريمة عقوبة تتمثل في الحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار جزائري (1.000.000دج) أو بإحدى هاتين العقوبتين فقط[2].

كما يعاقب في المادة 71 من القانون نفسه "بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار جزائري (1.000.000دج) أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".

ثانيا- جريمة إفشاء بيانات التوقيع الإلكتروني:

يتضح من نص المادة 42 من القانون 15-04 والتي نصت على أنه: "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة"، ينص المشرع على التزام مؤدي خدمات التصديق الالكتروني احترام سرية بيانات التوقيع الالكتروني، بحيث يشكل أي إفشاء لهذه البيانات، الكن المادي لهذه الجريمة، كما يمنع تقوم هذه الجريمة أيضا باستعمال هذه البيانات لأغراض أخرى، غير الغرض الذي قدمت من أجله[3].

كما يتطلب لقيام هذه الجريمة، إلى جانب الركن المادي توفر الركن المعنوي القصد العام دون الخاص، والمتمثل في اتجاه إرادة الجاني إلى إفشاء بيانات التوقيع الإلكتروني أو

---

[1] صالح شنين، مرجع سابق، ص170.

[2] المادة 70 من القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مرجع سابق.

[3] المادة 42 الفقرة 02 من القانون 15-04، المرجع نفسه.

إساءة استخدامها مع علمه بذلك، وقبول النتائج المترتبة على هذا السلوك الإجرامي، الذي لا يتصور وقوعه بطريق الخطأ[1].

ونظرا لخطورة إفشاء بيانات التوقيع الإلكتروني عاقب المشرع على القيام بهذه الجريمة بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مائتي ألف دينار إلى مليون دينار أو بإحدى هاتين العقوبتين[2].

كما ويعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من عشرين ألف دينار إلى مائتي ألف دينار جزائري أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق[3].

ثالثا- جريمة استعمال بيانات إنشاء التوقيع الإلكتروني:

تنشأ هذه الجريمة من خلال الفقرة 03 من نص المادة 61 من القانون 15-04 والتي تنص على أنه "لا يجوز لصاحب شهادة التصديق الإلكتروني عند انتهاء صلاحيتها أو عند إلغائها، استعمال بيانات إنشاء التوقيع الموافقة لها، من أجل توقيع أو تصديق هذه البيانات نفسها من طرف مؤدي آخر لخدمات التصديق الإلكتروني".

ويتطلب لقيام هذه الجريمة توفر ركن مادي، يتمثل في استعمال بيانات إنشاء التوقيع الإلكتروني من طرف صاحب الشهادة نفسه، كما أنه قد يتحقق الركن المادي، باستعمال أو إساءة استعمال البيانات الخاصة بإنشاء التوقيع الإلكتروني دون رضا صاحب شهادة التصديق الإلكتروني، من طرف شخص غير مرخص له باستخدام هذه البيانات، وفي الغالب يكون هذا الشخص ذو درجة عالية من العلم والحرفية في مجال المعلوماتية[4].

---

[1] صالح شنين، مرجع سابق، ص170.

[2] المادة 72 من القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مرجع سابق.

[3] المادة 73 من القانون 15-04، المرجع نفسه.

[4] عامر محمود الكسواني، التجارة عبر الحاسوب، (د ط)، دار الثقافة للنشر التوزيع، عمان، الأردن، 2008، ص181.

ويعاقب على هذه الجريمة بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000دج).[1]

مع الإشارة إلى أنه سبق وأن صدر القانون 15-03 المتعلق بعصرنة العدالة ونص في مادته 17 على جريمة الاستعمال غير القانوني للعناصر الشخصية المتصلة بإنشاء التوقيع الإلكتروني والذي يتعلق بشخص آخر، وقرر له عقوبة وتنص هذه المادة على أنه "يعاقب بالحسب من سنة (1) إلى خمسة (5) سنوات وبغرامة تتراوح بين مائة ألف دينار (100.000دج) إلى خمسمائة ألف دينار (500.000دج) كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بشخص آخر[2].

كذلك نص في مادته 18 على جريمة حيازة شهادة إلكترونية منتهية الصلاحية أو تم إلغائها، وتنص المادة على أنه "يعاقب بالحبس من سنة (01) إلى خمس (5) سنوات وبغرامة تتراوح بين مائة ألف دينار (100.000دج) إلى خمسمائة ألف دينار (500.000دج) كل شخص حائز شهادة إلكترونية يواصل استعمالها رغم علمه بانتهاء صلاحيتها أو إلغائها"[3].

وبالإضافة إلى هذه الجرائم هناك نصوص جزائية خاصة أخرى في مجال حماية البيانات الشخصية الالكترونية، حيث تلزم البنوك فيما يتعلق بواجباتها المرتبطة بتحقيق الأمن في مجال أنظمة الدفع بحفظ سرية المعطيات الشخصية التي تتحصل عليها من زبائنها[4].

---

[1] المادة 68 من القانون 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، مرجع سابق.

[2] أمر رقم 15-03، مؤرخ في 1 فيفري 2015، يتعلق بعصرنة قطاع العدالة، ج ر عدد 6، صادر في 10 فيفري 2015.

[3] المادة 18 من القانون 15-03، المرجع نفسه.

[4] حيث تنص المادة 10 من النظام رقم 05-07، مؤرخ في 25 ديسمبر 2005، يتضمن أمن أنظمة الدفع، ج ر عدد 37، صادر في 04 جوان 2006، على أنه:" "يتعين على المشاركين في نظام الدفع ضمان سرية وصحة المعلومات التي تمر عبر أنظمة الدفع ".

والحقيقة أن الالتزام بحفظ السر المصرفي التزام عام يقرر على البنوك والمؤسسات المالية بموجب المادة 117 من الأمر 03-11 المتعلق بالنقد والقرض[1]، والمعدل والمتمم، وهو من الالتزامات الأساسية التي تقوم عليها المهنة المصرفية، بالنظر إلى حساسية المعلومات التي قد يتحصل عليها البنك بمناسبة تقديم خدمات بنكية الكترونية، وبالرغم من ذلك فإنه فيما يتعلق بتوقيع الجزاء الجنائي أحل قانون النقد والقرض إلى النص العام الواردة في قانون العقوبات، وبالرجوع إلى المادة 301 و303 مكرر من هذا القانون نجد المشرع يقرر عقوبة تقدر بالحبس من شهر إلى ستة أشهر، وبغرامة من 500 إلى 5000 دج.

والملاحظ أن هذه العقوبة تمتاز بالخفة مقارنة بالعقوبات في جرائم أخرى، وكان الأجدر بالمشرع البنكي أن يقرر نص خاص في قانون النقد والقرض، يتلاءم وخطورة الدور الذي تؤديها البنوك والمؤسسات المالية، بحيث يميز بين العقوبات المقررة على المستخدمين كشخص طبيعي، والعقوبات المقرر على البنك كشخص معنوي.

من خلال دراستنا لجرائم الاعتداء على البيانات الشخصية في مجال التجارة الإلكترونية تبين لنا أنها جرائم تتسم بالخطورة، نظرا لخصوصيتها وعدم إمكانية حصرها، فقد عمل المشرع الجزائري لسد الفراغ القانوني على تعديل قانون العقوبات، وقد عاقب على الشروع في الجريمة وجعل صفح الضحية جائز أمام المتابعة، إلا أن هذه الحماية متواضعة وغير كافية، فقد اقتصرت على جرائم قلة، ولهذا يجب على المشرع مراعاة الأبعاد المستقبلية لمواكبة التطورات الحاصلة، كما أن تعدد النصوص المجرمة في هذا الإطار وتناثرها قد يشكل عائقا كبيرا أمام القاضي أثناء تكييفه للأفعال المرتكب

[1] أمر رقم 03-11، مؤرخ في 23 أوت 2033، يتعلق بالنقد والقرض، ج ر عدد 52، صادر في 27 أوت 2011، المعدل والمتمم.

المبحث الثاني: وسائل الحماية المدنية للبيانات الشخصية في مجال التجارة الإلكترونية

بالرجوع إلى طبيعة النشاط المسند لأطراف المعاملة الإلكترونية، نجد أنه ينطبق بشأنها أحكام المسؤوليتين العقدية والتقصيرية متى توافرت أركانهما وشروطهما، فنظرا لوجود علاقة تتمثل في العقد المبرم بين هذه الأطراف، والذي يرتب التزامات متبادلة في مواجهة كل طرف فإن هذه العلاقة تخضع لأحكام المسؤولية العقدية، أما في حالة عدم وجود علاقة تعاقدية فإنها تخضع لأحكام المسؤولية التقصيرية، فالأولى هي جزاء لعدم الوفاء بالالتزامات التعاقدية (المطلب الأول) والثانية نتيجة لعمل غير مشروع (المطلب الثاني).

المطلب الأول: دعوى المسؤولية العقدية الناتجة عن التعدي على البيانات الشخصية في مجال التجارة الإلكترونية

تمثل المسؤولية العقدية جزاء على مخالفة الشخص لأحد الالتزامات التعاقدية الملقاة على عاتقه بموجب العقد الإلكتروني، الذي يفرض التزامات في ذمة المتعاقدين ويرتب الجزاء بحسب الواجب الذي حدث الإخلال بشأنه، ومن خلال هذا المطلب يتم التطرق إلى أركان قيام المسؤولية العقدية وفقا للقواعد العامة (الفرع الأول)، ثم حالات قيام المسؤولية العقدية لوسطاء الأنترنت في حال وقوع تعدي على البيانات الشخصية الالكترونية(الفرع الثاني).

الفرع الأول: أركان قيام المسؤولية العقدية وفقا للقواعد العامة

تقوم المسؤولية العقدية نتيجة الإخلال بالالتزام التعاقدي، ويستوجب هذا الأخير وجود عقد صحيح لم يقم أحد الطرفين بتنفيذ التزامه المتعلق به، والعقد الصحيح كما عرفه المشرع الجزائري في المادة 54 من القانون المدني، "اتفاق يلتزم بموجبه شخص أو عدة أشخاص نحو شخص أو عدة أشخاص آخرين بمنح أو فعل أو عدم فعل شيء ما"، يترتب على العقد إنشاء التزامات تقع على كاهل كل من طرفيه وقد تكون ملزمة لجانب واحد، والقوة الملزمة للعقد تقضي بأن يقوم كل طرف بتنفيذ التزامه التعاقدي[1].

---

[1] محمد صبري السعدي، مصادر الالتزام (النظرية العامة للالتزامات)، الكتاب الأول، المصادر الإرادية والإرادة المنفردة، (د ط)، دار الكتاب الحديث، الجزائر، 2003، ص310.

فإذا طبقنا ذلك المبدأ بصفة عامة ومجردة على العقد الإلكتروني، نجد أنه لا يختلف في جوهره عن هذا المعنى، ولا يخرج عن كونه تبادل التعبير الإرادي بين شخصين على إحداث الأثر القانوني المقصود من العقد حسب طبيعته، ولكن بالنظر لكون العقد الإلكتروني يتم "عن بعد"، فإن الطابع المميز له والذي يعطيه ذاتيته المختلفة عن العقد العادي يكمن في الطريقة المستخدمة في انعقاده، أي الوسيلة القانونية التقنية التي يتم عن طريقها إبرام العقد الإلكتروني، وإتمام اقتران الإيجاب والقبول بين شخصين لا يجمعهما مجلس عقد واحد[1].

ويعرف العقد الإلكتروني بأنه التقاء إيجاب صادر من الموجب بشأن عرض مطروح بطريقة إلكترونية سمعية أو مرئية أو كليهما عبر شبكة الاتصالات والمعلومات، باستخدام التبادل الإلكتروني للبيانات، بقبول مطابق له صادر من الطرف المقابل بذات الطرف، بهدف تحقيق عملية أو صفقة معينة يرغب الطرفان في إنجازها[2].

فالمسؤولية العقدية إذن جزاء لعدم قيام أحد الطرفين بتنفيذ التزامه، تؤدي إلى تعويض الطرف الآخر عما أصابه من ضرر، ولعدم وجود نصوص خاصة بالمسؤولية العقدية الالكترونية، جعل دراستنا هذه تستند إلى القواعد العامة في القانون المدني، وحسب هذه الأخيرة فإنه يشترط لقيام المسؤولية العقدية توافر ثلاث أركان تتمثل في الخطأ (أولا) الضرر (ثانيا) والعلاقة السببية (ثالثا).

أولا- الخطأ العقدي:

يقصد بالخطأ عدم قيام المدين بتنفيذ التزامه التعاقدي أو التأخر في تنفيذه، ويستوي في ذلك أن يكون عدم التنفيذ أو التأخر فيه عن عمد أو إهمال من المدين[3].

---

[1] نزيه محمد الصادق المهدي، "انعقاد العقد الإلكتروني"، مداخلة مقدمة ضمن أشغال مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية – الحكومة الإلكترونية)، المنعقد في 19 و 20 ماي، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، 2009، ص188.

[2] خالد ممدوح إبراهيم، إبرام العقد الإلكتروني (دراسة مقارنة)، (د ط)، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص52.

[3] محمد صبري السعدي، مرجع سابق، ص336.

وينبغي ملاحظة أن عدم تنفيذ الالتزام التعاقدي يشمل عدم التنفيذ الكلي وعدم التنفيذ الجزئي والتأخير في التنفيذ، وقد نصت المادة 176 ق.م.ج على ذلك: "إذا استحال على المدين أن ينفذ الالتزام عينا حكم عليه بتعويض الضرر الناجم عن عدم تنفيذ التزامه، ما لم يثبت أن استحالة التنفيذ نشأت بسبب لا يد له فيه، ويكون الحكم كذلك إذا تأخر المدين في تنفيذ إلتزامه".

يقتضي الخطأ العقدي وجود نوعين من الالتزامات التزام بتحقيق نتيجة والالتزام ببدل عناية، ويتحمل الدائن الذي يطالب بالتعويض عبء إثبات عدم التنفيذ، فإذا كان الالتزام بتحقيق نتيجة فعلى الدائن إثبات عدم تحقيق هذه النتيجة التي استهدفها، أما إذا كان الالتزام ببذل عناية وجب عليه إثبات أن المدين لم يبدل العناية التي يبدلها الشخص العادي[1].

ونظرا لخصوصية العقد الإلكتروني فإن الإثبات يقتضي أن يتم عبر المستند الإلكتروني والتوقيع الإلكتروني، فالمستند الإلكتروني تتبلور فيه حقوق طرفي التعاقد فهو المرجع للوقوف على ما اتفق عليه الطرفان وتحديد التزاماتها القانونية، والتوقيع الإلكتروني هو الذي يضفي حجية على هذا المستند الإلكتروني[2].

ثانيا – الضرر:

يعد الضرر الركن الثاني في المسؤولية العقدية، وهو ركن لا غنى عنه، وذلك لأنه لا يكفي أن يرتكب المدين خطأ عقديا حتى تقوم مسؤوليته العقدية، وإنما يجب أن يترتب على عدم تنفيذ للالتزام العقدي ضرر يلحق الدائن[3].

وبالتالي فإمه حتى تقوم المسؤولية عن العقد الإلكتروني لا يكفي أن يكون هناك خطأ عقدي فقط، وإنما يجب أن يكون هناك ضرر لحق بالمتعامل الإلكتروني جراء هذا الخطأ[4]

---

[1] محمد صبري السعدي، مرجع سابق، ص337.

[2] خالد ممدوح إبراهيم، إبرام العقد الإلكتروني (دراسة مقارنة)، مرجع سابق، ص57.

[3] خليل أحمد حسن قدادة، الوجيز في القانون المدني الجزائري، الجزء الأول، ط2، ديوان المطبوعات الجامعية، الجزائر، 2008، ص151.

[4] ندى معيزي، النظام القانوني للتصديق الإلكتروني، مذكرة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون العلاقات الدولية الخاصة، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2016، ص340.

وعبء إثبات الضرر يقع على عاتق الدائن، لأنه المدعى في دعوى المسؤولية ويشترط في الضرر أن يكون مباشرا ومتوقعا، ولا يهم أن يكون الضرر واقعا أي حالا فالمهم أن يكون الضرر محقق غير احتمالي[1].

والضرر قد يكون ماديا أو أدبيا، فالضرر المادي هو الذي يصيب الشخص في ماله او جسمه نتيجة خطأ المدين، وهو الأكثر وقوعا في نطاق المسؤولية العقدية[2]، أما الضرر الأدبي هو الذي يصيب الإنسان في مصلحة غير مادية، ومثاله الضرر الذي يصيب الإنسان في عاطفته، ومنه أيضا الضرر الذي يصيب الإنسان في سمعته، كالذي يترتب عن السب والقذف ويشمل التعويض عن الضرر المعنوي حسب نص المادة 182 مكرر من ق.م.ج كل مساس بالحرية أو الشرف أو السمعة.

وهذا النوع من الضرر يقع كثيرا في المسؤولية التقصيرية على خلاف وقوعه في المسؤولية العقدية لأن طبيعة العقد تقتضي أن يكون إبرامه على شيء ذي قيمة مالية، غير أنه قد يكون للدائن مصلحة أدبية في تنفيذ العقد ويترتب على إخلال المدين بالتزامه ضرر أدبي[3].

ثالثا- علاقة السببية بين الخطأ والضرر:

لا يكفي أن يكون هناك خطأ وضرر، بل يجب أن يكون الضرر الذي أصاب الدائن نتيجة لخطأ المدين، وبمعنى آخر أن يكون الخطأ هو السبب في الضرر وهذا ما يعبر عنه بعلاقة السببية.

ويقع على الدائن إثبات رابطة السببية بين خطأ المدين والضرر، ويستطيع المدين إثبات أن الضرر وقع بسبب أجنبي أو بخطأ الدائن، أي يثبت أن الضرر الذي أصاب الدائن لم يكن نتيجة لعدم الوفاء بالتزامه التعاقدي بل يرجع إلى سبب لا يد له فيه[4].

---

[1] المادة 182مكرر من الأمر 75-58، المتضمن القانون المدني، المعدل والمتمم، مرجع سابق.

[2] محمد صبري السعدي، مرجع سابق، ص341.

[3] المرجع نفسه، ص341.

[4] المرجع نفسه، ص344.

الفرع الثاني: حالات قيام المسؤولية العقدية بسبب التعدي على البيانات الشخصية الالكترونية

كما وسبق توضيحه فإن المسؤولية العقدية لا تتقرر إلا في حالة وجود عقد صحيح، وفي مجال التعدي على البيانات الالكترونية، وفي مجال التعاقدات الالكترونية، فإنها تتم إما مع مؤدي خدمات التصديق الالكترونية، أو مع وسطاء في مجال الأنترنت، وبالتالي تقوم المسؤولية العقدية لكليهما في حالة وجود اخلال بالالتزامات المتضمنة في العقد المبرم مع الزبون، والتي تؤدي إلى المساس بالبيانات الشخصية.

ولذلك سيتم توضيح الحالات التي تي تقوم فيها المسؤولية العقدية لمؤدي خدمات التصديق الالكتروني (أولا)، والحالات التي تقوم فيها مسؤولية الوسطاء في مجال الأنترنت (ثانيا).

أولا- المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني:

بالرغم من أن المشرع الجزائري من خلال نصوص القانون 15-04 ركزّ على أحكام المسؤولية الجزائية التي تترتب على عاتق مؤدي خدمات التصديق الالكتروني، في حالة مخالفته للالتزامات المقررة على عاتقه، إلا أنه ما دام إصدار شهادة التصديق الإلكترونية يتم في إطار تعاقدي، بين مؤدي خدمة التصديق الإلكتروني كطرف، وطالب الشهادة من أصحاب التوقيع الإلكتروني كطرف ثاني، فإن ذلك من شأنه أن يثير مسؤوليته المدنية عموما ومسؤوليته العقدية خصوصا، إذا ما توافرت شروطها وفقا للقواعد العامة، وتقوم المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني بسبب التعدي على البيانات شخصية في مجال التجارة الإلكترونية في الحالات التالية:

1- عدم الحفاظ على البيانات والمعلومات الممنوحة له:

تقوم مسؤولية مؤدي خدمات التصديق الإلكتروني اتجاه صاحب الشهادة في حالة عدم الحفاظ على البيانات والمعلومات الممنوحة له، حيث يلتزم بموجب 42 من القانون

15-04 بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة له، فإذا قام بإفشاء هذه المعلومات والبيانات فإنه يكون مسؤولا عن الضرر الناتج عن إخلاله بالتزامه الناشئ بموجب العقد.

2- الحصول على البيانات دون موافقة صاحبها:

يقع على مؤدي خدمات التصديق الالكترونية التزامات بعدم تجميع البيانات الشخصية دون إذن صاحبها، حيث تنص المادة 43 من القانون 15-04 على أنه: "لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة"، فإذا ما حصل وخالف مثل هذا الالتزام، يكون مسؤولا في مواجهة صاحب التوقيع استنادا إلى أحكام المسؤولية العقدية.

3- استعمال البيانات لأغراض أخرى:

تقوم المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني عند الإخلال بالالتزام المنصوص عليه في الفقرة الثانية من المادة 43 من القانون 15-04 التي تنص على أنه: "لا يمكن مؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى" فإذا قام مؤدي خدمات التصديق الالكتروني بما يخالف هذا النص، بجمع بيانات ليست لها علاقة بموضوع الشهادة، فإنه يكون قد ارتكب خطأ يوجب مساءلته، إذا ثبت وقوع ضرر لصاحب البيانات.

4- الاحتفاظ ببيانات التوقيع الإلكتروني أو نسخها:

يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن حفظ أو نسخ بيانات إنشاء توقيع الشخص الذي منحت له شهادة التصديق إذا ثبت خطأ، وهذا ما نصت عليه المادة 48 من القانون 15-04 "لا يمكن لمؤدي خدمات التصديق الإلكتروني حفظ أو نسخ بيانات إنشاء توقيع الشخص الذي منحت له شهادة التصديق الإلكتروني

الموصوفة"، فإذا أخل بهذا الالتزام تثبت مسؤوليته العقدية اتجاه صاحب شهادة التصديق الإلكتروني.

ومما سبق فإن مسؤولية مؤدي خدمات التصديق الإلكتروني تقوم تلقائيا بمجرد ثبوت الحالات المنصوص عليها أعلاه، وهي مسؤولية عقدية تقوم عند عدم تنفيذ مؤدي خدمات التصديق الإلكتروني للالتزامات الواردة في العقد الذي يربطه بالموقع صاحب الشهادة، أو التأخير في تنفيذ التزامه.

ثانيا- مسؤولية وسطاء الأنترنت في مجال الخدمات الإلكترونية:

وسطاء الأنترنت هم مجموعة من الأشخاص ينحصر دورهم في تمكين المستخدم من الدخول إلى شبكة الانترنت والتجول فيها والاطلاع على ما يريدون، فهم يتولون تقديم الخدمات الوسيطة في الأنترنت[1]، ولما كان هؤلاء الوسطاء يرتبطون مع غيرهم بعقود فإنه يترتب على الإخلال ببنود هذا الأخير قيام المسؤولية العقدية، والوسيط في مجال الانترنت قد يقتصر دوره على تزويد الزبون بخدمة الأنترنت، وقد يتعدى ذلك ليوفر للزبون خدمات الكترونية متنوعة، لذلك سنميز بين:

1- المسؤولية العقدية لمزود خدمات الأنترنت:

عرف المشرع الجزائري في المادة 2 البند "د" من القانون 09-04 مقدمي خدمات الأنترنت بأنه أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية، أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمات الاتصال المذكورة أو لمستعمليها.

تقوم مسؤولية مزود خدمة الأنترنت في مجال إخلاله ببنود عقد الاشتراك المبرم بينه وبين عملائه، ومن أهم الحالات التي تقوم فيها مسؤوليته العقدية مايلي:

---

[1] عبد الهادي كاظم ناصر، المسؤولية المدنية لوسطاء الأنترنت، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، العراق، المجلد الثاني، العدد الثاني، ديسمبر 2009 ، ص228.

– الاخلال بالتزامه في المحافظة على سرية المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء، حيث تنص المادة 14 من المرسوم التنفيذي رقم98–257 وكيفيات إقامة خدمات الأنترنت واستغلالها،[1] على أنه :"يلتزم مقدم خدمات الأنترنت خلال ممارسة نشاطه بما يأتي: – .....

– المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة، وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون....".

– عدم اتخاذ الإجراءات الكفيلة بضمان حماية وسرية المعلومات والبيانات ذات الطابع الشخصي، التي يحوزها عن زبائنه أو يعالجها ويدرجها في وحدة التعرف على المشتركين، حيث تنص المادة 23 البند 2.2 من المرسوم التنفيذي 02–189 المعدل والمتمم[2]، على أنه :"يتخذ صاحب الرخصة الإجراءات الكفيلة بضمان حماية وسرية المعلومات والبيانات ذات الطابع الشخصي التي بحوزتها عن زبائنه أو يعالجها أو يدرجها في وحدة التعرف على المشتركين أو شريحة الدفع المسبق أو اللاحق SIM أو USIM وذلك مع احترام الأحكام القانونية والتنظيمية المعمول بها".

---

[1] تنص المادة 14 من المرسوم التنفيذي رقم 98–257، مؤرخ في 25 أوت 1998، يتضمن شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، ج ر عدد 63، صادرة في 26 أوت 1998.

[2] المادة 23 البند.3.2 من المرسوم التنفيذي رقم 02–186، المؤرخ في 26 ماي 2002، المتضمن الموافقة على سبيل التسوية على رخصة إقامة شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM واستغلالها مؤرخ في 7 مارس وتوفير خدمات المواصلات اللاسلكية للجمهور الممنوحة لشركة "اتصالات الجزائر للهادف النقال"، شركة ذات أسهم، ج ر عدد 38، مؤرخ في 29 ماي 2002، المعدل والمتمم.

وقد عدلت هذه المادة بموجب الملحق 01 من المرسوم التنفيذي رقم 17–108، المؤرخ في 07 مارس 2017، المتضمن الموافقة على تجديد رخصة لإقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور الممنوحة لشركة "اتصالات الجزائر للهاتف النقال"، شركة ذات اسهم، ج ر عدد 17، صادر في 15 مارس 2017.

كما يلتزم مزود خدمة الأنترنت اتجاه عملائه بمقتضى العقد بمراقبة مضمون المعلومات والبيانات المعروضة عبر أدواته الفنية[1]، وفي حال الإخلال بهذا الالتزام تقوم المسؤولية العقدية ويلزم بتعويض الضرر الحاصل عنه.

2- المسؤولية العقدية لمؤدي الخدمات الإلكترونية:

مؤدي الخدمات الإلكترونية هو شخص طبيعي أو معنوي يوفر لعملائه الوسائل التقنية التي تسمح لهم بالحصول على الخدمات الالكترونية التي يرغبون فيها، والحصول على حاجاتهم من المعلومات والخدمات المتاحة عبر شبكة المعلومات.

يرتبط مؤدي الخدمات الإلكترونية مع عملائه بعقد الاشتراك يعرف بعقد الدخول إلى الأنترنت، وهو عقد يلتزم بموجبه مؤدي الخدمات الإلكترونية بتمكين المستخدمين من الدخول إليها من الناحية الفنية، من خلال تزويده بالوسائل الفنية التي تؤمن هذا الدخول[2].

يعد عقد الدخول إلى الشبكة عقدا رضائيا، إذ ينعقد بمجرد التقاء إرادة المتعاقدين وتتجلى هذه الإرادة من خلال التوقيع على سند كتابي والشائع أن يبرم عقد الاتصال بالشبكة إلكترونيا[3].

تثور مسؤولية المورد في الحالات التي يتضمن فيها عقد الدخول الى الشبكة الذي يبرمه مع عملائه شرط يوجب على المورد المسؤولية عن مراقبة مضمون المعلومات والبيانات المعروضة عبر أدواته الفنية، ويعد هذا الشرط من الشروط المشددة لمسؤولية المورد والذي يلتزم بمقتضاه، فضلا عن التزامه الأصلي وهو توفير الأدوات الفنية التي تكفل للعميل الدخول إلى الشبكة، أن يوفر الوسائل الفنية التي من شأنها أن تقوم بمراقبة محتوى المعلومات والبيانات التي تمر عبر تقنياته، وبمنع التعدي على هذه البيانات من قبل الغير،

---

[1] إلياس ناصيف، مرجع سابق، ص263.

[2] عبد المهدي كاظم ناصر، مرجع سابق، ص231.

[3] المرجع نفسه، ص232.

ومن تم يعد مسؤولا اتجاه عملائه في حالة وقوع خطأ يشكل اعتداء على البيانات الشخصية[1].

المطلب الثاني: دعوى المسؤولية التقصيرية الناتجة عن التعدي على البيانات الشخصية الإلكترونية

تنشأ المسؤولية التقصيرية في الحالات التي لا يوجد فيها عقد عكس المسؤولية العقدية التي توجب وجود علاقة عقدية بين الطرفين، وتترتب المسؤولية التقصيرية نتيجة المخالفات التي تتم لنصوص قانونية، وتقوم المسؤولية التقصيرية عن التعدي على البيانات الشخصية الالكترونية بموجب النص العام الوارد في القانون المدني، وهو نص المادة 124 من القانون المدني الجزائري، التي جاء فيها: " كل فعل أيا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"، فلقيام هذه المسؤولية لابد من وجود خطأ يسبب ضررا للغير، من خلال بث المعلومات عن طريق شبكة الأنترنت، وبالتالي فالمسؤولية التقصيرية تقوم على نفس أركان المسؤولية العقدية، من خطأ وضرر وعلاقة سببية، باستثناء أن الخطأ الذي يكون موجب للمسؤولية العقد يكون بسبب الإخلال بواجب قانوني وليس عقدي.

وسنتناول في هذا المطلب حالات قيام المسؤولية التقصيرية بسبب التعدي على البيانات الشخصية الالكترونية(الفرع الأول) والتعويض في المسؤولية التقصيرية الإلكترونية (الفرع الثاني).

الفرع الأول: حالات قيام المسؤولية التقصيرية بسبب التعدي على البيانات الشخصية الالكترونية

في نطاق المعاملات الإلكترونية وإعمالا للقواعد العامة في المسؤولية المدنية التقصيرية تقوم مسؤولية مقدمي خدمات التصديق الإلكتروني (أولا) اتجاه الأشخاص الذين

[1] عبد المهدي كاظم ناصر، مرجع سابق، ص236.

أصابهم الضرر من صدور هذه الشهادة دون أن يكونوا متعاقدين معه، كما تقوم المسؤولية التقصيرية لوسطاء الأنترنت في حالات معينة(ثانيا).

أولا- المسؤولية التقصيرية لمقدم خدمات التصديق الإلكتروني:

قد لا تكون مسؤولية مقدم خدمات التصديق الإلكتروني عقدية، وهذا بالطبع عند عدم وجود علاقة عقدية بين مؤدي خدمات التصديق من طرف، والمتضررين من طرف آخر، أو في حالة فسخ العقد أو إلغائه، وهم الغير، ويندرج تحت هذا الوصف أي شخص لا تربطه علاقة مباشرة بعقد ما مع جهة التصديق، فالقانون هو المصدر المباشر والرئيسي لالتزامات جهة التصديق، فإن أي إهمال أو تقصير يسجله على صعيد تلك الالتزامات من شأنه أن يقيم مسؤولية مقدم الخدمات وفقا لأحكام المسؤولية المدنية التقصيرية[1].

ويمكن في الإجمال تحديد الحالة التي تقوم فيها المسؤولية التقصيرية لمؤدي خدمات التصديق الالكتروني، بسبب التعدي على البيانات الشخصية الإلكترونية بما في حالة الإخلال بالحكم الوارد في نص المادة 47 من القانون 09-04 الذي جاء فيه: "يجب على مؤدي خدمات التصديق الإلكتروني تحويل المعلومات المتعلقة بشهادات التصديق الإلكتروني الموصوفة بعد انتاء صلاحيتها إلى السلطة الاقتصادية للتصديق الإلكتروني من أجل حفظها".

ففي حالة انتهاء صلاحية شهادة التصديق الإلكتروني يجب على مؤدي خدمات التصديق الإلكتروني تحويل المعلومات المتعلقة بها إلى السلطة الاقتصادية للتصديق الإلكتروني لحفظها، وفي حالة مخالفة ذلك وإعادة استعمال هذه الشهادة وعدم إلغائها يكون مقدم خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن ذلك، إذ تقوم المسؤولية

---

[1] محمد حاتم البايات، "المسؤولية المدنية عن الخطأ في المعاملات التي تتم عن طريق الوسائط الإلكترونية"، مداخلة مقدمة ضمن أشغال مؤتمر المعاملات الالكترونية (التجارة الالكترونية- الحكومة الالكترونية)، المنعقد يومي 19 و 20 ماي 2009، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، ص140.

التقصيرية اتجاهه إذا قام باستعمال أو حفظ هذه الشهادة لإنشاء توقيع آخر لشخص آخر غير صاحب الشهادة.

كما تقوم المسؤولية التقصيرية لمقدم خدمات التصديق بصفة عامة عن كل إفشاء للبيانات المتحصل عليها بموجب عقد ملغى أو باطل، أو إعادة استعمال هذه البيانات لأغراض أخرى.

ثانيا – المسؤولية التقصيرية لوسطاء الأنترنت:

ونميز في هذا الصدد بين مسؤولية مزود خدمات الأنترنت ومقدم الخدمات الإلكترونية:

1 – المسؤولية التقصيرية لمزود خدمات الأنترنت:

يتولى مزود خدمات الأنترنت عملية تخزين البيانات وحفظها لمصلحة عملائه، وتقوم مسؤوليته كلما تخطى دوره أو ارتكب خطأ ألحق ضررا بالغير ممن لا يرتبط معه بعقد اشتراك،[1] وقد كان المشرع البحريني أكثر وضوحا عند تصديه لمعالجة مسؤولية مزود خدمات الأنترنت، إذ نصت المادة 19 من قانون التجارة الإلكترونية لسنة 2002 "تنتفي مسؤولية وسيط الشبكة مدنيا أو جنائيا عن أية معلومات واردة في شكل سجلات إلكترونية تخص الغير، إذا لم يكن هو مصدر هذه المعلومات أو اقتصر دوره على مجرد توفير إمكانية الدخول عليها، وذلك إذا كانت المسؤولية قائمة على:

- إفشاء أو نشر أو بث أو توزيع هذه المعلومات أو أية بيانات تتضمنها.
- التعدي على أية حق من الحقوق الخاصة بتلك المعلومات"[2].

[1] إلياس ناصيف، مرجع سابق، ص266.

[2] عبد المهدي كاظم ناصر، مرجع سابق، ص239.

وبالتالي فإن قيام مزود خدمات الأنترنت بإفشاء أو نشر المعلومات الخاصة والشخصية، أي التعدي على هذه البيانات باستعمالها في غير الغرض المخصص لها، خطأ يرتب مسؤولية تقصيرية على عاتقه.

2- المسؤولية التقصيرية لمؤدي الخدمات الإلكترونية:

وفيما يتعلق بالمسؤولية التقصيرية لمؤدي الخدمات الإلكترونية فإنها تقوم على ارتكابه خطأ بمخالفته للقواعد العامة التي تفرض عليه ضرورة احترام حقوق الغير وعدم الإضرار بهم، كما هو الأمر في حالة بثه لمعلومات تشكل اعتداء على الحياة الخاصة للغير، أو تمس بسمعته أو شرفه، أو في حالة بثه لمعلومات خاطئة أو ناقصة[1]، وبالتالي فإن جميع الأفعال المجرمة التي يمكن أن تقع من مؤدي الخدمات الإلكترونية تصلح أساسا لقيام مسؤوليته التقصيرية في مواجهة الغير الذي لحق به ضرر مادي أو معنوي من جراء هذه المخالفات والذي لم يرتبط معه بعلاقة عقدية[2].

3- المسؤولية التقصيرية الناشئة عن أعمال القرصنة الالكترونية:

تستهدف القرصنة الإلكترونية وبشكل خاص التحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة والشخصية أو تغييرها والتأثير على سلامتها أو حتى إتلافها، وتعتبر القرصنة عملية دخول غير مصرح به من طرف أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي، بحيث تكون لهم القدرة على تجاوز إجراءات وأنظمة الحماية التي اتخذت لحماية تلك الشبكات الإلكترونية[3].

فالقرصنة الإلكترونية تستهدف وبشكل خاص المعلومات المخزنة داخل الكمبيوتر أي الوصول من خلال ثغرات في نظام الحماية الخاص، وبالتالي يقوم قراصنة الأنترنت بنشر

---

[1] إلياس ناصيف، مرجع سابق، ص270.

[2] عبد المهدي كاظم ناصر، مرجع سابق، ص249.

[3] فتيحة ليتيم، نادية ليتيم، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الثاني عشر، 2015. ص242.

معلومات وتعطيل مواقع لشركات وإيقافها عن العمل، فقد حصل اختراق شركات نفط عملاقة وتسريب أسماء موظفيها وحساباتهم، وبالتالي فالقراصنة يقومون بالعبث بالبيانات وذلك بتغييرها أو إنشاء بيانات وهمية في مراحل الإدخال أو الإخراج أو التخزين[1].

وقد أثبت الواقع العملي حجم الأضرار الكبيرة التي قد تلحق بالشركات والأفراد وحتى بأجهزة تابعة للدولة بسبب هذه العمليات المشروعة، لدا فمن البديهي أن تقوم مسؤولية القائم بهذه الأفعال، في حالة تم اكتشاف هويته، بالتعويض عن هذه الأضرار.

الفرع الثالث: التعويض في المسؤولية التقصيرية الإلكترونية

إذا تعرض الغير للضرر نتيجة الاعتداء غير المشروع على البيانات الشخصية الالكترونية، فإنه يستحق تعويضا، ويكون التعويض عينيا أو بمقابل، فالتعويض العيني ينصب على إزالة الضرر وإعادة الحال لما كان عليه قبل وقوع الفعل الضار، ويتمثل التعويض العيني في دعاوى المسؤولية بوقف الاعتداء على الحياة الخاصة، ومن أمثلة ذلك الأمر بوقف بث وبنشر المعلومة، وقد يتخذ التعويض العيني صورة حق الرد والتصحيح، ويجب على الموقع الإلكتروني الذي تثبت مسؤوليته الالتزام بنشر الرد أو التصحيح.

وقد يكون التعويض بمقابل، والذي يكون في الغالب على شكل مبلغ نقدي يدفعه محدث الضرر للمتضرر، ويهدف إلى إصلاح الضرر الذي وقع على المتضرر، ويشمل التعويض النقدي في المسؤولية التقصيرية، كلا من الأضرار المادية والأدبية، والأضرار المباشرة و غير المباشرة[2].

---

[1] فتيحة ليتيم، نادية ليتيم، المرجع السابق، ص ص242 – 247.

[2] محمد ابراهيم عرسان أبو الهيجاء، علاء الدين عبد الله الخصاونة، "المسؤولية التقصيرية لمزودي خدمات الأنترنت عن المحتوى غير المشروع، دراسة في التوجيه الخاص بالتجارة الالكترونية لسنة 2000 والقانون الفرنسي"، مجلة الشريعة والقانون"، جامعة الإمارات العربية المتحدة، العدد 42 الصادر في أفريل 2010، ص 31، المنشور في الموقع الالكتروني: Platform.almanhal.com/article/preview.aspx ?id=617.

فالضرر المادي الذي يجوز التعويض عنه وفقا لأحكام المسؤولية التقصيرية يتحقق إما بالإخلال بمصلحة مالية له، ويشترط في الضرر المادي أن يكون محققا، أي يكون وقع بالفعل أو حتمي الوقوع في المستقبل[1].

أما التعويض عن الضرر الأدبي يشمل ما لحق المتضرر من ضرر أدبي بسبب المساس بسمعته التجارية وإظهاره بمظهر يسهل انخداعه وفي عدم الثقة فيه، وقد استقرت أحكام القضاء الفرنسي على الأخذ بمبدأ التعويض عن الضرر الأدبي الناشئ عن المسؤولية التقصيرية[2]، وهو المبدأ الذي أخذ به المشرع الجزائري فيما بعد ضمن نصوص القانون المدني.

وتجدر الإشارة إلى أن دعاوى المسؤولية الجزائية والمدنية كوسائل مقررة لصاحب البيانات، تمكنه من حماية حقه، تثير إشكالات في التطبيق، في حالة قيام نزاع يتعدى حدود الدولة الواحدة، فيما يتعلق بتحديد القانون الذي سيحكم هذا النوع من النزاع، وقد استقرت التشريعات على إخضاع العقود الإلكترونية لقانون إرادة المتعاقدين، أي القانون الذي يحدده طرفا العقد سواء كان بشكل صريح أو ضمني ليكون واجب التطبيق على العقد، أما في حال عدم تحديد القانون واجب التطبيق على العقد وعدم التمكن من تحديد إرادة المتعاقدين الضمنية فتظهر سلطة القاضي في البحث عن القانون الأنسب بين القوانين الوطنية.

وحسب نص المادة 18 من القانون المدني الجزائري في حالة وجود إرادة واضحة بين المتعاقدين يطبق القانون المختار، أما إذا لم يفصح الأطراف على اختيار تطبيق قانون معين يطبق قانون الموطن المشترك أو الجنسية المشتركة، وفي حال تعذر ذلك يطبق قانون محل إبرام العقد.

أما فيما يتعلق بالمسؤولية الجزائية فالأصل هو تطبيق مبدأ إقليمية قانون العقوبات الجزائري، إلا في حالة وجود اتفاقيات دولية خاصة في هذا الشأن.

---

[1] عبد الفتاح محمود الكيلاني، مرجع سابق، ص459.

[2] المرجع نفسه، ص460.

وفي الأخير يمكن القول فيما يتعلق بالوسائل المقررة لحماية البيانات الشخصية الالكترونية، أن المشرع أولى العناية أكثر لدعوى المسؤولية الجزائية، من خلال إفراد نصوص خاصة بها، حاول من خلالها مراعاة الخصوصية التي تتميز بها الجرائم المرتكبة في هذا الشأن، في حين تجاهل تماما الخصوصية التي تميز المسؤولية المدنية الناتجة بسبب الأخطاء العقدية أو التقصيرية التي قد تمس بالبيانات الشخصية الالكترونية، بالرغم من أن المعني في كثير من الحالات تمكينه من جبر الضرر الذي لحق به ووقف الاعتداء، أكثر من توقيع الجزاء العام الممثل في العقوبة الجزائية.

لذلك يتعين على المشرع، أن يسارع إلى تبني سياسة موسعة ومحكمة تستهدف بوضع نصوص قانونية تتلاءم وطبيعة هذا النوع من الاعتداءات، من خلال وضع مدونة تتناسب والتطورات التي يعرفها المجال التكنولوجي بصفة عامة.

الخاتمة

من خلال دراستنا لموضوع حماية البيانات الشخصية في مجال التجارة الإلكترونية تبين لنا أن تداول البيانات عبر الوسائط الإلكترونية يحمل مخاطر عدة تتعلق أساسا بأمن هذه البيانات، واحتمالية الاعتداء عليها، وهو ما يقلل من ثقة المتعاملين في مجال التجارة الإلكترونية، مما دفع إلى البحث عن الوسائل التقنية التي توفر الحماية اللازمة لهذه البيانات، بما يحول دون وقوع أي تعدي عليها، كما استلزم الأمر البحث عن الوسائل القانونية التي تمكن المتضرر من صد أي اعتداء على بياناته الشخصية الالكترونية، والمتمثلة أساسا في الدعوى الجزائية والدعوى المدنية.

ومن خلال البحث والدراسة حول المسائل المتعلقة بحماية البيانات الشخصية في مجال التجارة الالكترونية، توصلنا إلى جملة من النتائج التالية:

- ظهور بوادر اهتمام المشرع الجزائري بتنظيم بالتجارة الإلكترونية، بإصدار القانون 15-04 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، والذي كرّس أحكاما غاية في الأهمية تدعم مصداقية التوقيع الالكتروني وحجيته القانونية.

- إصدار القانون 09-04، والذي كان من أهم مضامنه إنشاء الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال، والتي تناط بها مهام معينة أهما تفعيل التعاون القضائي ومنح المساعدة التقنية، بالإضافة لتنسيق عمليات الوقاية من الجرائم.

- السماح باتخاذ إجراءات خاصة في مرحلة المتابعة الجزائية تتلاءم وطبيعة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، والتي يمكن أن تدرج ضمنها الجرائم الماسة بالبيانات الشخصية الالكترونية، من خلال استحداث نظام المراقبة الالكترونية، وتوسيع صلاحيات الضبطية القضائية.

- استحداث جرائم خاصة بالاعتداء على أنظمة المعالجة الآلية للمعطيات ضمن أحكام قانون العقوبات الجزائري، مما يستبعد تطبيق العقوبات المقررة للجرائم التقليدية على تلك المرتكبة في العالم الافتراضي.

– تعديل المشرع الجزائري لقانون الإجراءات الجزائية، بتمديد اختصاص المحاكم الجزائية، في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وذلك لخطورة هذه الجرائم وصعوبتها لأنها تتم عبر الشبكة الإلكترونية.

– تحديد الالتزامات المقررة على عاتق مؤدي خدمات التصديق الالكتروني فيما يتعلق بعملها الأساسي المتمثل في منح شاهدة التصديق الالكتروني، وأيضا بعض التزامات مزود خدمات الأنترنت فيما يتعلق بالمحافظة على سرية المعطيات الشخصية.

بالرغم من أنه من الواضح من خلال نصوص القانون الجزائري أن المشرع يتجه نحو تكريس نصوص خاصة بالتعامل في المجال الافتراضي، إلا أنه يمكن تسجيل بعض النقائص، أهمها:

– شمولية الجرائم الماسة بالمعالجة الآلية للمعطيات، بحيث قررت عقوبة واحدة على جريمة عامة، قد تتضمن عدة أفعال مادية، مما يثير الشك حول ملائمة العقوبات المقررة لكل فعل.

– صعوبة إثبات الركن المادي في الجرائم الإلكترونية، والذي يتطلب نصوصا خاصة تفصيلية، خاصة في ظل مبدأ شرعية العقوبات.

– على الرغم من الدور الذي تلعبه الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال ومكافحتها، خاصة وأن المشرع قد اعتبرها هيئة إدارية مستقلة، إلا أن اختصاصاتها جاءت في إطار التعاون الدولي والتنسيق الداخلي، وتدريب الأعوان المكلفين بالتحقيق في هذا النوع من الجرائم، في حين لم يمنح لها أي اختصاص قضائي أو قمعي، كما هو الحال بالنسبة للسطات الإدارية المستقلة الأخرى.

– عدم وجود نصوص خاصة بالمسؤولية المدنية الالكترونية، تتلاءم وطبيعة الأخطاء المرتكبة في العالم الافتراضي، وبالخصوص تلك التي تشكل اعتداء على البيانات الشخصية.

وفي سبيل تجاوز كل هذه النقائص نتقدم بالاقتراحات التالية:

– ضرورة وضع قانون متكامل بخصوص حماية المعاملات الإلكترونية بصفة عامة، يعالج كافة جوانبها، لسد الفراغ التشريعي في هذا المجال.

– الحرص على تحديث أنظمة الحماية تبعا لتطورات الجريمة الإلكترونية، وضرورة تطوير برمجيات آمنة للحد من الاختراقات والاعتداءات الماسة بالبيانات الشخصية في التعاملات الإلكترونية.

– تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم، وذلك بالتعاون مع التقنيين من أصحاب الخبرة في هذا المجال.

– إعادة تنظيم الجرائم المتعلقة بالمعالجة الآلية للمعطيات، من خلال الفصل بين مختلف الجرائم من حيث أركانها والعقوبات المقررة عليها، وتقرير عقوبات خاصة بالاعتداء على البيانات الشخصية الالكترونية، وتحديد أركانها بدقة، خاصة الركن المادي منها.

– تدريس مواد المعلوماتية والجرائم الماسة بها في الكليات والمعاهد القضائية، لنشر ثقافة المعلوماتية بين مختلف المستويات، لرفع درجة الوعي لدى المتعاملين، من أجل تجنب المخاطر التي يمكن أن يتعرضوا لها بسبب هذا التعامل.

– ضرورة سن تشريعات تحفظ حقوق المتعاملين عبر شبكة الأنترنت، وخاصة الطرف الضعيف، لتحقيق الثقة والأمان بين المتعاملين.

قائمة المراجع

أولا- باللغة العربية:

I- الكتب:

1. إبراهيم بختي، التجارة الإلكترونية (مفاهيم واستراتيجيات التطبيق في المؤسسة)، (د ط)، ديوان المطبوعات الجامعية، الجزائر، 2008.
2. أحمد سفر، أنظمة الدفع الإلكترونية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2006.
3. إلياس ناصيف، العقود الدولية العقد الإلكتروني في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.
4. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للنشر والتوزيع، الجزائر، 2007.
5. إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته الجوانب القانونية لعقد التجارة الإلكترونية، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2008.
6. بشار محمود دودين، محمد يحي المحاسنة، الإطار القانوني للعقد المبرم عبر شبكة الأنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006.
7. ثروت عبد الحميد، التوقيع الإلكتروني (ماهية، مخاطر وكيفية مواجهتها مدى حجيته في الإثبات)، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2007،.
8. حسين محمد الحسن، الإدارة الإلكترونية، ط1، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2011.
9. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني (دراسة مقارنة)، (د ط)، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
10. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، (د ط)، الدار الجامعية للطباعة والنشر والتوزيع، الإسكندرية، مصر، 2008.

11. خالد ممدوح إبراهيم، أمن المستندات الإلكترونية، (د ط)، الدار الجامعية، مصر، 2008.
12. خضر مصباح الطيطي، التجارة الإلكترونية والأعمال الإلكترونية،(د. ط). دار الحامد للنشر والتوزيع، عمان، الأردن، 2008.
13. خليل أحمد حسن قدادة، الوجيز في القانون المدني الجزائري، الجزء الأول، ط2، ديوان المطبوعات الجامعية، الجزائر، 2008.
14. رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، ط 1، القاهرة، مصر، 1999.
15. طارق إبراهيم الدوسقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.
16. عامر محمود الكسواني، التجارة عبر الحاسوب، (د ط)، دار الثقافة للنشر التوزيع، عمان، الأردن، 2008.
17. عبد الفتاح بيومي حجازي، التجارة عبر الأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2008.
18. عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية)، (د ط)، دار الفكر الجامعي، الإسكندرية، مصر، 2008.
19. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، (د ط)، دار الفكر الجامعي، الاسكندرية، مصر، 2002.
20. عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني (دراسة تأصيلية مقارنة)، (د ط)، دار الكتب القانونية، القاهرة، مصر، 2007.
21. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، (د ط)، دار الفكر الجامعي، القاهرة، مصر، 2007.

22. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، (د ط)، منشأة المعارف، الإسكندرية، مصر، 2009.
23. عبد الفتاح محمود الكيلاني، المسؤولية المدنية الناشئة عن المعاملات الإلكترونية عبر الأنترنت، (د. ط)، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2011.
24. عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، ط1، دار وائل للنشر والتوزيع، عمان، الأردن، 2010.
25. علاء محمد نصيرات، حجية التوقيع الإلكتروني في الإثبات (دراسة مقارنة)،(د. ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.
26. عمر خالد زريقات، عقود التجارة الإلكترونية (عقد البيع عبر الأنترنت)، (د ط)، دار حامد للنشر والتوزيع، عمان، الأردن، 2007.
27. فراح مناني، العقد الإلكتروني، وسيلة إثبات حديثة في القانون المدني الجزائري، (د ط)، دار الهدى للطباعة والنشر، الجزائر، 2009.
28. لورنس محمد عبيدات، إثبات المحرر الالكتروني، ط1 ، دار الثقافة للنشر والتوزيع ، عمان، الاردن، 2009.
29. محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، (د ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006.
30. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.
31. محمد صبري السعدي، مصادر الالتزام (النظرية العامة للالتزامات)، الكتاب الأول، المصادر الإرادية والإرادة المنفردة، (د ط)، دار الكتاب الحديث، الجزائر، 2003.
32. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية (دراسة مقارنة)، (د. ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

33. محمد مأمون سليمان، التحكيم الإلكتروني، (د ط)، دار الجامعة الجديدة، الإسكندرية، مصر، 2011.

34. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، الطبيعة القانونية للعقد الإلكتروني، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

35. ناصر خليل، التجارة والتسويق الإلكتروني، (د ط)، دار أسامة للنشر والتوزيع، الأردن، 2008.

36. ناهد فتحي الحموري، الأوراق التجارية الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

37. نضال إسماعيل برهم، غازي أبو عرابي، أحكام عقود التجارة الإلكترونية، (د ط)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

38. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

II- الرسائل والمذكرات الجامعية:

أ- رسائل الدكتوراه:

1. إبراهيم بختي، دور الأنترنت وتطبيقاته في مجال التسويق، رسالة دكتوراه، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2003.

2. صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012-2013.

3. صفية باشتان، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة مقدمة لنيل شهادة دكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، السنة 2012.

4. عبد الوهاب مخلوفي، التجارة الإلكترونية عبر الأنترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 2011، 2012.

ب- المذكرات:

ب1- مذكرات الماجستير:

1. راضية لالوش، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.
2. سمية ديمش، التجارة الإلكترونية حقيقتها وواقعها في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم الاقتصادية، تخصص تحليل واستشراف اقتصادي، كلية العلوم الاقتصادية وعلم التسيير، جامعة منتوري، قسنطينة، 2011.
3. سهيلة طمين، الشكلية في عقود التجارة الإلكترونية، رسالة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، الجزائر، 2011.
4. كريمة صراع، واقع وآفاق التجارة الإلكترونية في الجزائر، مذكرة مقدمة لنيل شهادة الماجستير في العلوم التجارية، تخصص استراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، 2013-2014.
5. مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.
6. يوسف واقد، النظام القانوني للدفع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011.

ب2- مذكرات الماستر:

- ندى معيزي، النظام القانوني للتصديق الإلكتروني، مذكرة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق، تخصص قانون العلاقات الدولية الخاصة، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2016.

III- المقالات:

1. عبد الهادي كاظم ناصر، "المسؤولية المدنية لوسطاء الأنترنت"، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، العراق، المجلد الثاني، العدد الثاني، ديسمبر 2009، ص. ص224-268، متاح على الموقع الإلكتروني:
iasj.net/iasj?func=fulltext&aId=13003
2. فتيحة ليتيم، نادية ليتيم، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد الثاني عشر، 2015، ص. ص 237-253، متاح على الموقع الإلكتروني:
http://fdsp.univ-biskra.dz/index.php
3. محمد إبراهيم عرسان أبو الهيجاء، علاء الدين عبد الله الخصاونة، "المسؤولية التقصيرية لمزودي خدمات الأنترنت عن المحتوى غير المشروع، دراسة في التوجيه الخاص بالتجارة الالكترونية لسنة 2000 والقانون الفرنسي"، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد 42 الصادر في أفريل 2010، ص. ص 19-84، متاح على الموقع الإلكتروني:
http://platform.almanhal.com/Article/Preview.aspx?ID=617
4. محمد بكرارشوش، "الاختصاص الإقليمي الموسع في المادة الجزائية في التشريع الجزائري"، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، العدد 14، 2006، ص ص 305-326، متاح على الموقع الإلكتروني:
https://revues.univ-ouargla.dz/index.php/numero-14-2016-dafatir/2833-2016-01-26-09-18-39

5. منى تركي الموسوي، "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها"، مجلة العلوم الاقتصادية، كلية بغداد للعلوم الاقتصادية، العراق، عدد خاص، 2013، ص. ص 303-356، متاح على الموقع الإلكتروني:
iasj.net/iasj?func=fulltext&aId=72783

IV- المداخلات:

1. أمال حابت، "الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري"، مداخلة مقدمة ضمن أشغال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16، 17 نوفمبر 2015، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة.
2. آمنة أمحمدي بوزينة، "إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)"، مداخلة مقدمة ضمن أشغال الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، يوم 29 مارس 2017، مركز جيل البحث العلمي، الجزائر العاصمة.
3. محمد حاتم البايات، "المسؤولية المدنية عن الخطأ في المعاملات التي تتم عن طريق الوسائط الإلكترونية"، مداخلة مقدمة ضمن أشغال مؤتمر المعاملات الالكترونية (التجارة الالكترونية- الحكومة الالكترونية)، يومي 19 و 20 ماي 2009، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، متاح على الموقع الإلكتروني:
http://slconf.uaeu.ac.ae/papers/PDF%201%20&%202%20arabic/805-847.pdf
4. محمد خليفة، "خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها"، مداخلة مقدمة ضمن أشغال الملتقى الدولي الأول حول التنظيم القانوني للأنترنت والجريمة الالكترونية، المنعقد يومي 27 و 28 أفريل 2009، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 8 ماي 1945- قالمة.
5. نزيه محمد الصادق المهدي، "انعقاد العقد الإلكتروني"، مداخلة مقدمة ضمن أشغال مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية – الحكومة الإلكترونية)، المنعقد في

19 و 20 ماي 2009، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، متاح على الموقع الإلكتروني:
http://slconf.uaeu.ac.ae/papers/PDF%201%20&%202%20arabic/185-255.pdf

IV- النصوص القانونية:

أ- الدساتير:

1- مرسوم رئاسي رقم 96-438 مؤرخ في 07 ديسمبر 1996، يتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء 28 نوفمبر سنة 1996 في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، جريدة رسمية عدد 76، صادر في 08 ديسمبر سنة 1996، المعدل والمتمم.

ب- النصوص التشريعية:

1. أمر رقم 66-155، مؤرخ في 8 جوان 1966، يتضمن قانون الإجراءات الجزائية، ج ر عدد 48، صادر في 10 جوان 1966، المعدل والمتمم.
2. أمر رقم 66-156 مؤرخ في 1 جوان 1966، يتضمن قانون العقوبات، ج ر عدد 102، صادر في 4 جوان 1966، المعدل والمتمم.
3. أمر رقم 75-58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج ر عدد 78، صادر في 30 ديسمبر 1975، المعدل والمتمم.
4. أمر رقم 03-11، مؤرخ في 23 أوت 2033، يتعلق بالنقد والقرض، ج ر عدد 52، صادر في 27 أوت 2011، المعدل والمتمم.
5. قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 08 جوان 1966 والمتضمن قانون العقوبات، ج ر عدد 71، صادر في 10 نوفمبر 2004.
6. قانون رقم 05-11، مؤرخ في 17 يوليو 2005، يتعلق بالتنظيم القضائي، ج ر عدد 51، صادرة في 20 يوليو 2005.

7. قانون رقم 09-04، مؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، ج ر عدد 47، صادر في 16 أوت 2009.
8. أمر رقم 15-03، مؤرخ في 1 فيفري 2015، يتعلق بعصرنة قطاع العدالة، ج ر عدد 6، صادر في 10 فيفري 2015.
9. قانون رقم 15-04 المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر عدد 06، الصادر في 10 فيفري 2015.

ج- النصوص التنظيمية

ج1- المراسيم الرئاسية:

- مرسوم رئاسي رقم 15-261، مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53 ، صادرة في 08 أكتوبر 2015.

ج2- المراسيم التنفيذية:

1. مرسوم تنفيذي رقم 98-257، مؤرخ في 25 أوت 1998، يتضمن شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، ج ر عدد 63، صادرة في 26 أوت 1998.
2. مرسوم تنفيذي رقم 02-186، مؤرخ في 26 ماي 2002، يتضمن الموافقة على سبيل التسوية على رخصة إقامة شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM واستغلالها مؤرخ في 7 مارس وتوفير خدمات المواصلات اللاسلكية للجمهور الممنوحة لشركة "اتصالات الجزائر للهادف النقال"، شركة ذات أسهم، ج ر عدد 38، مؤرخ في 29 ماي 2002، المعدل والمتمم.

3. مرسوم تنفيذي 06-348، مؤرخ في 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر عدد 63، صادر في 08 أكتوبر 2006.

4. مرسوم تنفيذي رقم 07-162، مؤرخ في 30 ماي 2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 9 ماي 2001، والمتعلق بنظام الاستغلال المطبق على كل أنواع الشبكات السلكية واللاسلكية الكهربائية بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37، صادر في07 جوان2007، (ملغى).

5. مرسوم تنفيذي رقم 17-108، مؤرخ في 07 مارس 2017، يتضمن الموافقة على تجديد رخصة لإقامة واستغلال شبكة عمومية للمواصلات اللاسلكية الخلوية من نوع GSM ولتوفير خدمات المواصلات اللاسلكية للجمهور الممنوحة لشركة "اتصالات الجزائر للهاتف النقال"، شركة ذات اسهم، ج ر عدد 17، صادر في 15 مارس 2017.

د- أنظمة بنك الجزائر:

- نظام رقم 05-07، مؤرخ في 25 ديسمبر 2005، يتضمن أمن أنظمة الدفع، ج ر عدد 37، صادر في 04 جوان 2006.

هـ- آراء المجلس الدستوري:

- رأي رقم 01 / ر.ق.ع/م د/05، مؤرخ في 17 جوان 2005، يتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي للدستور، البند الثاني من الموضوع المتعلق بفحص المادة 24 من القانون العضوي محل الإخطار، ج ر عدد 51، صادرة في 20 جويلية 2005.

ثانيا – باللغة الفرنسية:

I- Les Ouvrages :

1. Eynard Jessica, Les données personnelles (quelle définition pour un régime de protection efficace ?), Michalon Editeur, Paris, France, 2013.
2. Elisabeth Mathieu –Marie, Les Services et financier en ligne, Editeur Revue Banque, Paris, France, 2005.

ثالثا – المواقع الالكترونية:

1. www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf
2. kaisdali.over.blog.com/2014/03 pdf-pdf-pdf-html.
3. platform.almanhal.com/preview.aspx ?id=617.
4. iasj.net/iasj?func=fulltext&aId=13003
5. http://slconf.uaeu.ac.ae/papers/PDF%201%20&%202%20arabic/805-847.pdf
6. http://slconf.uaeu.ac.ae/papers/PDF%201%20&%202%20arabic/185-255.pdf
7. iasj.net/iasj?func=fulltext&aId=72783
8. http://fdsp.univ-biskra.dz/index.php
9. https://revues.univ-ouargla.dz/index.php/numero-14-2016-dafatir/2833-2016-01-26-09-18-39

فهرس الموضوعات

العنوان **الصفحة**

شكر وعرفان

الإهداء

قائمة المختصرات

مقدمة 1

الفصل الأول: إجراءات أمن البيانات الشخصية في مجال التجارة الإلكترونية 8

المبحث الأول: الوسائل التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية 10

المطلب الأول: الأنظمة التقنية لأمن البيانات الشخصية في مجال التجارة الإلكترونية 10

الفرع الأول: مفهوم نظام التشفير 10

أولا- تعريف التشفير 11

1- التعريف الفقهي للتشفير 11

2- التعريف التشريعي 11

أ- في القانون الجزائري 11

ب- في القانون التونسي 12

ج- في القانون الفرنسي 12

ثانيا- أنواع التشفير 13

1- التشفير من حيث الوسيلة المستخدمة 13

أ- التشفير باستخدام المفتاح المتماثل 13

ب- التشفير باستخدام المفتاح اللامتماثل 14

ج- المزج بين نظامي المفتاح المتماثل والمفتاح اللامتماثل 15

2- التشفير من حيث مستوى الاستخدام 15
أ- التشفير على مستوى الإرسال 16
ب- التشفير على مستوى التصفح 16
ج- التشفير على مستوى التنفيذ 16
د- التشفير على مستوى الملفات 16
الفرع الثاني: ضوابط التشفير 17
أولا- مشروعية تشفير البيانات 17
ثانيا- احترام سرية البيانات المشفرة 18
ثالثا- استخدام التشفير بواسطة السلطات المختصة 18
الفرع الثالث: دور التشفير في حماية البيانات ذات الطابع الشخصي للأفراد.. 19
المطلب الثاني: البرامج التقنية لأمن البيانات الشخصية في مجال التجارة
الإلكترونية 20
الفرع الأول: بروتوكول الطبقات الأمنية 21
أولا- تعريف بروتوكول الطبقات الأمنية (SSL) 21
ثانيا- طريقة عمل بروتوكول الطبقات الأمنية SSL 21
ثالثا- خطوات استخدام بروتوكول الطبقات الأمنيةSSL 22
الفرع الثاني: بروتوكول المعاملات المالية الآمنة SET 23
أولا- تعريف بروتوكول المعاملات الإلكترونية الآمنة SET 23
ثانيا- أهداف بروتوكول المعاملات المالية الآمنة SET 24
ثالثا- طريقة عمل بروتوكول المعاملات المالية الآمنة SET 24
الفرع الثالث: الجدران النارية 26
أولا- تعريف الجدران النارية 26
ثانيا- أنواع الجدران النارية 27

1- الحائط المصفى 27
2- الحائط المفوض 27
ثالثا- طرق الحماية باستخدام الجدران النارية 28
1- طريقة إتاحة العام وغلق الخاص 28
2- طريقة حوائط المنع المزدوجة 28
3- طريقة الفصل المطلق للخدمات 29
المبحث الثاني: الوسائل القانونية لأمن البيانات الشخصية في مجال التجارة الإلكترونية 30
المطلب الأول: مفهوم التوقيع الإلكتروني 30
الفرع الأول: تعريف التوقيع الإلكتروني 30
أولا: التعريف التشريعي للتوقيع الإلكتروني 31
1- تعريف التوقيع الإلكتروني على المستوى الدولي 31
أ- تعريف التوقيع الإلكتروني في قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني لسنة 2001 31
ب- تعريف التوقيع الإلكتروني في التوجه الأوروبي بشأن التوقيعات الإلكترونية لسنة 1999 32
2- تعريف التوقيع الإلكتروني في القوانين الداخلية 32
أ- تعريف التوقيع الإلكتروني في القانون الجزائري 32
ب- تعريف التوقيع الإلكتروني في القانون الفرنسي 33
ج- تعريف التوقيع الإلكتروني في التشريع الأردني 34
ثانيا- التعريف الفقهي للتوقيع الإلكتروني 34
الفرع الثاني: صور التوقيع الإلكتروني 35
أولا- التوقيع الرقمي 35

ثانيا– التوقيع بالقلم الإلكتروني 36
ثالثا– التوقيع باستخدام الخواص الذاتية (البيومتري) 37
رابعا– التوقيع بالرقم السري في البطاقات البلاستيكية 39
الفرع الثالث: شروط الاعتماد على التوقيع الإلكتروني كوسيلة لحماية البيانات ذات الطابع الشخصي 39
أولا– ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره 40
ثانيا– سيطرة صاحب التوقيع على منظومة التوقيع 41
ثالثا– ارتباط التوقيع الإلكتروني بالمحرر ارتباطا وثيقا 41
المطلب الثاني: التصديق الإلكتروني 42
الفرع الأول: مفهوم شهادة التصديق الإلكتروني 42
أولا– تعريف شهادة التصديق الإلكتروني 43
ثانيا– أنواع شهادة التصديق الإلكتروني 43
1– شهادة التصديق الإلكتروني الموصوفة 43
2– شهادة التصديق الإلكتروني العادية 44
ثالثا– شهادة التصديق الأجنبية 45
الفرع الثاني: الجهة المختصة بإصدار شهادة التصديق الإلكترونية 46
أولا– تعريف الجهة المختصة بإصدار شهادة التصديق الإلكتروني 47
ثانيا– التزامات مقدم خدمات التصديق الإلكتروني 47
1– الالتزامات المتعلقة بمزاولة النشاط 47
2– الالتزام بتأمين وحماية البيانات 48
الفرع الثالث: دور التصديق الإلكتروني في ضمان تأمين البيانات 49
أولا– التحقق والتأكد من صحة البيانات 49
ثانيا– حماية البيانات 50

ثالثا– حفظ بيانات شهادة التصديق الإلكتروني 50
رابعا– إصدار المفاتيح الإلكترونية 51

الفصل الثاني: وسائل الحماية القانونية للبيانات الشخصية في مجال التجارة الالكترونية 54

المبحث الأول: وسائل الحماية الجزائية للبيانات الشخصية في مجال التجارة الالكترونية 56
المطلب الأول: إجراءات المتابعة في الجرائم الماسة بأمن البيانات الشخصية في مجال التجارة الإلكترونية 56
الفرع الأول: خصوصية إجراءات المتابعة في جرائم الاعتداء على البيانات الشخصية الالكترونية 56
أولا– توسيع صلاحيات الضبطية القضائية 57
ثانيا– مراقبة الاتصالات الإلكترونية 58
ثالثا– تفتيش المنظومة المعلوماتية 59
رابعا– حجز المعطيات المعلوماتية 60
الفرع الثاني: الجهات المختصة في مجال جرائم الاعتداء على البيانات الشخصية الإلكترونية 61
أولا– الهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال 62
1– الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال 62
2– دور الهيئة الوطنية في الوقاية من جرائم الاعتداء على البيانات الشخصية الإلكترونية 63

ثانيا– الجهات المختصة بالنظر في الجرائم الماسة بالمعالجة الآلية
للمعطيات 64
1– مدى اعتماد نظام الأقطاب المتخصصة في المسائل الجزائية ... 64
2– الفروع الجزائية المتخصصة 65
المطلب الثاني: تعدد جرائم الاعتداء على البيانات الشخصية في مجال
التجارة الإلكترونية 66
الفرع الأول: الجرائم المقررة في القواعد العامة 67
أولا– الجرائم التقليدية 67
1– جريمة المساس بحرمة الحياة الخاصة 67
أ– الركن المادي 67
ب– الركن المعنوي 69
ج– العقوبة المقررة لهذه الجريمة 69
2– جريمة الاعتداء على حرمة المراسلات 69
ثانيا– الجرائم المستحدثة 71
1– جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي 71
أ– الركن المادي 71
ب– الركن المعنوي 72
ج– العقوبة المقررة لهذه الجريمة 72
2– جريمة التلاعب في أنظمة المعالجة الآلية للمعطيات 72
أ– الركن المادي 73
ب– الركن المعنوي 73
ج– العقوبة المقررة لهذه الجريمة 74
3– جريمة التعامل في معطيات غير مشروعة 74

أ- الركن المادي 74
ب- الركن المعنوي 76
ج- العقوبة المقررة لهذه الجريمة 76
الفرع الثاني: الجرائم المقررة في قانون التوقيع والتصديق الإلكترونيين 76
أولا- جريمة حيازة بيانات إنشاء التوقيع الإلكتروني 77
ثانيا- جريمة إفشاء بيانات التوقيع الإلكتروني 78
ثالثا- جريمة استعمال بيانات إنشاء التوقيع الالكتروني 79
المبحث الثاني: وسائل الحماية المدنية للبيانات الشخصية في مجال التجارة الإلكترونية 82
المطلب الأول: دعوى المسؤولية العقدية الناتجة عن التعدي على البيانات الشخصية في مجال التجارة الإلكترونية 82
الفرع الأول: أركان قيام المسؤولية العقدية وفقا للقواعد العامة 82
أولا- الخطأ العقدي 83
ثانيا- الضرر 84
ثالثا- علاقة السببية بين الخطأ والضرر 85
الفرع الثاني: حالات قيام المسؤولية العقدية بسبب التعدي على البيانات الشخصية الإلكترونية 86
أولا- المسؤولية العقدية لمؤدي خدمات التصديق الإلكتروني 86
1- عدم الحفاظ على البيانات والمعلومات الممنوحة له 86
2- الحصول على البيانات دون موافقة صاحبها 87
3- استعمال البيانات لأغراض أخرى 87
4- الاحتفاظ ببيانات التوقيع الإلكتروني أو نسخها 87
ثانيا- مسؤولية وسطاء الأنترنت في مجال الخدمات الإلكترونية 88

1- المسؤولية العقدية لمزود خدمات الأنترنت 88
2- المسؤولية العقدية لمؤدي الخدمات الإلكترونية 90
المطلب الثاني: دعوى المسؤولية التقصيرية الناتجة عن التعدي على البيانات
الشخصية الالكترونية 91
الفرع الأول: حالات قيام المسؤولية التقصيرية بسبب التعدي على البيانات
الشخصية الالكترونية 91
أولا- المسؤولية التقصيرية لمقدم خدمات التصديق الإلكتروني 92
ثانيا- المسؤولية التقصيرية لوسطاء الأنترنت 93
1- المسؤولية التقصيرية لمزود خدمات الأنترنت 93
2- المسؤولية التقصيرية لمؤدي الخدمات الالكترونية..... 94
3- المسؤولية التقصيرية الناشئة عن أعمال القرصنة الالكترونية 94
الفرع الثالث: التعويض في المسؤولية التقصيرية الإلكترونية..... 95
الخاتمة..... 98
قائمة المراجع 102
فهرس الموضوعات 114

من إعداد الطالبتين:	عنوان المذكرة:	إشراف الأستاذة:
- بودوشة أميرة - شاكر سميرة	**حماية البيانات الشخصية في التجارة الالكترونية**	بلجودي أحلام

الملخص:

من أهم المسائل التي يثيرها التعامل في مجال التجارة الإلكترونية مسألة حماية البيانات الشخصية، لذلك عملت الكثير من الشركات والهيئات العالمية على البحث عن الإجراءات التقنية اللازمة لتوفير الأمن والأمان لهذه البيانات بمنع الاعتداء عليها، كما كرست العديد من التشريعات الوطنية وسائل قانونية لحماية حقوق المتضرر في حال وقوع الاعتداء عليها تتمثل في الدعوى الجزائية والدعوى المدنية.

Résumé :

La protection des données personnelles est l'une des questions soulevées dans le domaine du commerce électronique (E-commerce). Ainsi, plusieurs sociétés et organismes de recherche internationaux ont pris des mesures techniques nécessaires à garantir la sécurité de ces données contre toute intrusion. De même, plusieurs législations nationales ont consacré des moyens légaux pour la protection des droits de tout utilisateur victime d'atteinte à ses données personnelles. Ces moyens consistent en l'instance pénale et l'instance civile.