Journal Sharia and Law

Volume 2016
Number 66 *Year 30, Issue No. 66 April 2016*

Article 6

April 2016

Crimes Against Electronic Signatures In Saudi Law

Osama Ghanem Alobaidy
(J.S.D) Institute of Public Administration Riyadh, Kingdom of Saudi Arabia, obaidyo@ipa.edu.sa

Crimes Against Electronic Signatures In Saudi Law

Cover Page Footnote

Dr. Osama Ghanem Alobaidy (J.S.D) Institute of Public Administration Riyadh, Kingdom of Saudi Arabia
obaidyo@ipa.edu.sa

التوقيع الإلكتروني وجرائم الاعتداء عليه في النظام السعودي*

د. أسامة بن غانم العبيدي*

ملخص البحث

أدت ثورة الاتصالات والمعلومات والتطور التقني الكبير في استخدام الحاسب الآلي وشبكة الإنترنت إلى تطور كبير في التعاملات والتجارة الإلكترونية والتوقيع الإلكتروني، وهو توقيع يستخدم في العقود الإلكترونية المبرمة عبر شبكة الإنترنت، فأصبحت معظم التعاملات المالية والتجارية تتم بواسطة الكتابة الإلكترونية والمحررات الإلكترونية.

لذلك ظهر بديل عن التوقيع الخطي التقليدي توقيع إلكتروني يتوافق مع طبيعة التصرفات القانونية والعقود التي تتم باستخدام وسائل التقنية الحديثة.

ويتناول هذا البحث جرائم الاعتداء على التوقيع الإلكتروني في النظام السعودي، وقد بينا في المبحث الأول ماهية التوقيع الإلكتروني وخصائصه وعيوبه، كما تناولنا في المبحث الثاني صور التوقيع الإلكتروني وآليات حمايته وجهات تصديقه. كما تناولنا في المبحث الثالث الجرائم المتصلة بالتوقيع الإلكتروني والعقوبات المقررة في النظام السعودي للجرائم المتصلة بالتوقيع الإلكتروني.

* أجيز للنشر بتاريخ ١٨/ ٥/ ٢٠١٤.

* أستاذ القانون المشارك – معهد الإدارة العامة – الرياض – المملكة العربية السعودية.

إشكالية البحث:

يهدف هذا البحث إلى دراسة موضوع جرائم الاعتداء على التوقيع الإلكتروني في النظام السعودي وإبراز ماهية التوقيع الإلكتروني وخصائصه وعيوبه وصوره وآليات حمايته وجهات تصديقه إضافة إلى العقوبات المقررة في النظام السعودي للجرائم المتصلة بالتوقيع الإلكتروني.

خطة البحث:

يشتمل هذا البحث على ثلاثة مباحث:

المبحث الأول: ماهية التوقيع الإلكتروني.

المبحث الثاني: صور التوقيع الإلكتروني وآليات حمايته.

المبحث الثالث: الجرائم المتصلة بالتوقيع الإلكتروني والعقوبات المقررة في النظام السعودي للجرائم المتصلة بالتوقيع الإلكتروني.

منهج البحث:

يعتمد هذا البحث على أسلوب الدراسة التحليلية لنصوص القوانين والأنظمة المقارنة مع الاستناد إلى المراجع العلمية ذات العلاقة.

المقدمة

نتج عن التطور الهائل في نظم الاتصالات والمعلومات تأثير كبير على القواعد والقوانين التقليدية. فالتعاملات والتوقيعات الإلكترونية تتميز بميزات خاصة تختلف عن التعاملات التقليدية ولا تتلاءم معها القوانين التقليدية.

وقد أدى هذا التطور في تقنية الاتصالات والمعلومات إلى إحداث تغييرات في العديد من المفاهيم القانونية كمفهوم الكتابة والمحرر والتوقيع، إذ أوجدت هذه التقنية أشكالاً جديدة للكتابة والمحرر والتوقيع تتميز جميعها بالطابع الإلكتروني. ومع انتشار العقود الإلكترونية والتجارة الدولية، استوجب ذلك من المشرعين في الدول المختلفة وضع الأطر والقواعد التي تكفل التعرف على أشخاص المتعاملين أثناء تبادلهم للمعلومات، والتحقق من شخصيتهم وهويتهم منعاً لإفشاء أسرارهم والتعامل غير المشروع في التصرفات والعقود الإلكترونية التي تتم فيما بينهم.

لذلك ظهر التوقيع الإلكتروني بديلاً عن التوقيع التقليدي كأحد الضمانات التي يتحقق منها من شخصية المتعاقدين. ولكن قبول التوقيع الإلكتروني في التعاملات الإلكترونية كحجة في الإثبات أثار جدلاً كبيراً في الفقه والقضاء وخاصة قبل صدور قوانين التعاملات الإلكترونية.

وقد ازدادت الجرائم الواقعة على التوقيع الإلكتروني بشكل كبير مما يشكل تهديداً لاستخدامات التوقيع الإلكتروني في المجالات المختلفة وبشكل خاص في مجال التجارة الإلكترونية.

ولذلك سنبين في هذا البحث ماهية التوقيع الإلكتروني وخصائصه وعيوبه، ونوضح صوره وآليات حمايته وجهات تصديقه إضافة إلى الجرائم المتصلة بالتوقيع الإلكتروني والعقوبات المقررة في النظام السعودي للجرائم المتصلة بالتوقيع الإلكتروني.

المبحث الأول :
ماهية التوقيع الإلكتروني
المطلب الأول:
تعريف التوقيع الإلكتروني

عرف بعض الفقهاء التوقيع الإلكتروني بأنه "مجموعة من الإجراءات والوسائل يتبع استخدامها عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونياً يجري تشفيرها باستخدام زوج من المفاتيح، واحد معلن والآخر خاص بصاحب الرسالة"(١).

كما عرفه فقهاء آخرون بأنه " مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته"(٢). وعرفه البعض الآخر بأنه " علامة أو رمز متمايز يعود على شخص بعينه، من خلاله يعبر الشخص عن إرادته ويؤكد حقيقة البيانات المتضمنة في المستند الذي وقعه(٣).

كما عرفه آخرون بأنه "مجموعة من الرموز أو الأرقام أو الحروف أو الإشارات أو الأصوات، مؤلفة على شكل بيانات إلكترونية تتصل بمحرر إلكتروني، تهدف إلى تحديد هوية الموقِّع وإعطاء اليقين بموافقته على مضمون هذه

(١) أحمد شرف الدين ، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة إلى مؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية ، ٢٠٠٠م . ص ٣ . انظر أيضاً عيسى غسان ربضي ، القواعد الخاصة بالتوقيع الإلكتروني ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠٠٩م . ص ٤٨ وما بعدها .

(٢) عيسى غسان ربضي ، المرجع السابق . ص ٥٥ .

(٣) عادل رمضان الأبيوكي ، التوقيع الإلكتروني في التشريعات الخليجية ، دراسة مقارنة ، المكتب الجامعي الحديث ، الإسكندرية ، ٢٠٠٩م . ص ١٥ وما بعدها .

الرسالة [٤] وعرفه آخرون بأنه " عناصر متفردة خاصة بالموقِّع تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، توضع على محرر إلكتروني لتحديد شخص الموقِّع وتمييزه عن غيره، وتعبر عن موافقته على مضمون المحرر" [٥].

وقد عرف القانون المدني الفرنسي التوقيع الإلكتروني بأنه "التوقيع الضروري لإتمام التصرف القانوني الذي يميز هوية من وقعه، ويعبر عن رضائه بالالتزامات التي تنشأ عن هذا التصرف. وعندما يكون إلكترونياً فيجب أن يتم باستخدام وسيلة آمنة لتحديد هوية الموقِّع وضمان صلته بالتصرف الذي وقّع عليه" [٦] .

وعرف المشرع الأمريكي التوقيع الإلكتروني بأنه "أي صوت أو رمز أو إجراء إلكتروني مرتبط أو متعلق منطقياً بسجل وينفذ أو يعتمد من الشخص الراغب في توقيع السجل" [٧].

أما المشرع المصري فقد عرف التوقيع الإلكتروني على أنه " ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقِّع ويميزه عن غيره [٨].

أما المنظم السعودي فقد عرف التوقيع الإلكتروني بأنه " بيانات إلكترونية، مدرجة في تعامل إلكتروني، أو مضافة إليه، أو مرتبطة به منطقياً تستخدم لإثبات هوية الموقِّع وموافقته على التعامل الإلكتروني، واكتشاف أي تعديل يطرأ على هذا

(٤) عادل الأبيوكي ، المرجع السابق . ص ١٥ .
(٥) ثروت عبدالحميد، التوقيع الإلكتروني، دار الجامعة الجديدة ، القاهرة ، ٢٠٠٧م . ص ٤٧ وما بعدها.
(6) Unif. Electronic Transactions Act, 7A . ULA.23 (2002) .
(٧) المادة (١) ، فقرة (ج) من القانون المصري رقم (١٥) لعام ٢٠٠٤م الخاص بتنظيم التوقيع الإلكتروني.
(٨) المادة (١) ، القانون المصري رقم (١٥) لعام ٢٠٠٤م الخاص بتنظيم التوقيع الإلكتروني .

التعامل بعد التوقيع عليه "[٩].

أما المشرع الإماراتي فقد عرف التوقيع الإلكتروني بأنه "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقياً برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة[١٠].

ونرى أن التعريف الأفضل للتوقيع الإلكتروني هو " مجموعة من الإجراءات التقنية التي تتيح تحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع مرتبطاً به " فهذا التعريف يركز على أهمية قيام التوقيع الإلكتروني بالوظائف التقليدية للتوقيع وهي تحديد هوية الشخص، والتعبير عن قبوله بالتصرف القانوني.

المطلب الثاني:
خصائص التوقيع الإلكتروني:

١- يتكون التوقيع الإلكتروني من عناصر متفردة وسمات خاصة بالموقِّع تتخذ شكل أرقام أو حروف أو إشارات أو رموز أو غيرها.

٢- أنه يحدد شخصية الموقِّع ويميزه عن غيره.

٣- أنه يعبر عن رضاء الموقِّع بمضمون المحرر [١١].

٤- التوقيع الإلكتروني يتصل برسالة إلكترونية وهي عبارة عن معلومات

(٩) المادة (١) ، فقرة (١٤) نظام التعاملات الإلكترونية السعودي ، الصادر بقرار مجلس الوزراء رقم (٨٠) وتاريخ ٧/ ٣/ ١٤٢٨هـ .

(١٠) المادة (١) ، القانون الاتحادي الإماراتي رقم (١) لعام ٢٠٠٦م بشأن المعاملات والتجارة الإلكترونية.

(١١) سعيد السيد قنديل ، التوقيع الإلكتروني ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٦م . ص٥١ وما بعدها . انظر أيضاً عادل رمضان الأبيوكي ، التوقيع الإلكتروني في التشريعات الخليجية (دراسات مقارنة) المرجع السابق . ص ٣١ وما بعدها .

يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسيلة إلكترونية.

٥- التوقيع الإلكتروني يحقق أغراض ووظائف التوقيع التقليدي متى كان صحيحاً وأمكن إثبات نسبته إلى موقعه.

٦- أنه يحقق الأمان والخصوصية والسرية في نسبته للموقع، بالنسبة للمتعاملين مع أنواعه وخاصة مستخدمي شبكة الإنترنت وعقود التجارة الدولية. ويتم ذلك عن طريق إمكانية تحديد هوية الموقِّع وبالتالي حماية المؤسسات من عمليات تزوير التوقيعات [١٢].

المطلب الثالث:
وظائف التوقيع الإلكتروني:

أولاً: تحديد هوية الموقِّع:

التوقيع علامة شخصية تكشف عن هوية صاحبه، وذلك بأن يدل التوقيع الموجود على المحرر أنه ينسب لشخص معين بذاته، فتصبح الورقة الموقعة منسوبة إليه، أما بالنسبة للتوقيع الإلكتروني، فلا يختلف كثيراً عن التوقيع التقليدي فهو يقوم بذات الوظيفة من خلال استخدام وسائل وإجراءات موثوق بها. تتمثل في استخدام أنظمة مختلفة مثل التوقيع باستخدام القلم الإلكتروني أو البصمة الإلكترونية أو استخدام نظام التشفير بأنواعه، حيث تسمح هذه الوسائل بتحديد هوية الأشخاص الذين أوجدوا هذه الوثائق من خلال الربط بين هويتهم

(١٢) ثروت عبدالحميد ، التوقيع الإلكتروني ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٧م . ص ٣٥ وما بعدها . انظر أيضاً ممدوح محمد علي مبروك ، مدى حجية التوقيع الإلكتروني في الإثبات . دار النهضة العربية، ٢٠٠٩م . ص ٨ وما بعدها .

والنصوص والرسائل التي يتبادلونها [١٣].

والتوقيع الإلكتروني يقوم بهذا الدور، بشكل رموز أو أرقام أو حروف أو إشارات تدل على شخصية الموقِّع، وتميزه عن غيره [١٤].

وهكذا فإن التوقيع، إلكترونياً كان أم كتابياً، يؤدي هذه الوظيفة وإنما يقع الاختلاف في كيفية وضع التوقيع على المحرر. ففي حين ينشأ التوقيع بالشكل الكتابي على محررات مادية ذات طبيعة ورقية تماثل الشكل الذي تم به التصرف القانوني، وذلك بالحضور المادي لأطراف التصرف ومقابلتهم وجهاً لوجه في مجلس واحد، لذا كان من الضروري أن يأتي التوقيع أيضاً مادياً على ذات المحررات الورقية. أما حين يتم إبرام العقود والتصرفات إلكترونياً باستخدام وسائل الاتصالات الحديثة ودون رؤية الأشخاص لبعضهم البعض، ظهر التوقيع الإلكتروني الذي يوضع على المحرر باستخدام الأجهزة الإلكترونية [١٥].

لذلك يمكن أن نقول أن المهم في التوقيع هو أن يكون مميزاً لشخصية صاحبه ويعبر عن هويته، وإرادته في الالتزام بمضمون المحرر، ولا أهمية لشكل التوقيع لأن الشكل غير مقصود بذاته.

ويمكن القول أن التوقيع الإلكتروني له القدرة على تحديد هوية الشخص

(١٣) لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠٠٩م . ص ١٥٠ وما بعدها. انظر أيضاً فيصل سعيد الغريب، المنظمة العربية للتنمية الإدارية ، القاهرة ، ٢٠٠٥م ، ص ٢٢٢ وما بعدها . انظر أيضاً عادل الأبيوكي ، التوقيع الإلكتروني في التشريعات الخليجية ، المرجع السابق . ص ٢٦ وما بعدها .

(١٤) عادل الأبيوكي ، المرجع السابق . ص ٢٦ .

(١٥) ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص ٣٧ وما بعدها . انظر أيضاً عبدالرحمن عبدالله السند ، الأحكام الفقهية للتعاملات الإلكترونية ، (الحاسب الآلي وشبكة المعلومات " الإنترنت") ، دار الوراق للطباعة والنشر ، ط ٣ ، ٢٠٠٦م . ص ١٤٦ وما بعدها .

الموقِّع في حال تدعيم التوقيع الإلكتروني بوسائل تدعم الثقة به للقيام بوظائفه[١٦].

ثانياً : التعبير عن رضا الموقِّع:

يدل التوقيع العادي على رضا الموقِّع بما هو مدون في المحرر وقبوله بما جاء فيه. لأن وضع التوقيع على مستند معين أو وثيقة معينة يعني انصراف مضمون الوثيقة أو المستند إلى شخص الموقِّع [١٧].

وذات الشيء ينطبق على التوقيع الإلكتروني فيستفاد رضاء الموقِّع وقبوله الالتزام بمجرد وضع توقيعه إلكترونياً على البيانات التي تحتويها المحررات الإلكترونية. فعندما يأخذ التوقيع الإلكتروني (Electronic Signature) شكل أرقام سرية أو رموز معينة ومحددة تحفظ في حيازة صاحبها، ولا يعلمها غيره، فإذا تم استخدام الأرقام، أي وقع لها صاحبها، فإن مجرد توقيعه هذا يدل على موافقته على المعلومات والبيانات التي قام بالتوقيع عليها، واتجاه إرادته إلى الالتزام بها [١٨].

ويعتبر رضا الموقِّع صحيحاً بتوافر الأهلية وهي قدرة الشخص على إبرام التصرفات القانونية. فيجب لتوافر الرضا أن تكون لدى الموقِّع أهلية قانونية كاملة. كما يجب أن يخلو الرضا من أي من عيوب الإرادة. فيجوز لصاحب التوقيع متى ما كانت إرادته معيبة بأحد عيوب الإرادة وهي الغلط، والتدليس، والاستغلال، والإكراه، أن يطلب إبطال التصرف الصادر منه [١٩].

(١٦) عيسى غسان ربضي ، القواعد الخاصة بالتوقيع الإلكتروني ، المرجع السابق . ص ٦٦ وما بعدها .

(١٧) فيصل الغريب ، التوقيع الإلكتروني وحجيته في الإثبات ، المرجع السابق . ص ٢٢٣ وما بعدها .

(١٨) لورنس عبيدات ، إثبات المحرر الإلكتروني ، المرجع السابق . ص ١٤٢ وما بعدها . انظر أيضاً خالد عبدالتواب عبدالحميد ، تطور مفهوم الدليل الكتابي في ضوء التقنيات الحديثة ؛ دراسة مقارنة ، مجلة البحوث الأمنية ، العدد ٤٤ ، ٢٠٠٩ م . ص ١٩٥ .

(١٩) إلا أن الواقع العملي يثير عدداً من المشكلات في هذا الشأن وخصوصاً فيما يخص طريقة الإثبات ، إذ إن من الصعب على صاحب التوقيع أن يثبت وقوعه في غلط أو تدليس على سبيل المثال . انظر لورنس

المطلب الرابع:
عيوب التوقيع الإلكتروني:

على الرغم من إيجابيات التوقيع الإلكتروني والتي سهلت العديد من العمليات التجارية والشخصية إلا أن هناك بعض الجوانب السلبية التي تعتريه. ويمكن أن نورد بعض عيوب التوقيع الإلكتروني على النحو التالي:

أولاً : إساءة استعمال التوقيع الإلكتروني:

قد تتم إساءة استعمال التوقيع الإلكتروني، ومثال ذلك استعمال البطاقة البنكية، حيث قد يستعمل الغير هذه البطاقة لسحب مبالغ مالية لا يحق له الحصول عليها، كأن يحصل شخص ما على بطاقة بنكية عن طريق السرقة أو الاحتيال ويستخدمها في سحب مبالغ مالية أو دفع فواتير مستحقة عليه [٢٠]. كما أن التوقيع الإلكتروني معرض للتزوير وخاصة من الأشخاص الذين يتوافر لديهم معرفة جيدة باستخدامات الحاسب الآلي، إذ قد يستطيعون الدخول إلى منظومات التوقيع الإلكترونية باستخدام برامج خاصة والاحتيال على تلك النظم وفك شفرات التوقيع الإلكتروني ومن ثم استخدامها في أغراض احتيالية عن طريق نسخها أو تزويرها ووضعها على محرر مزور [٢١].

ثانياً: ارتفاع تكلفة التوقيع الإلكتروني:

بعض صور التوقيع الإلكتروني وخصوصاً التوقيع البيومتيري Biometric)

عبيدات، المرجع السابق . ص ١٥٣ . انظر لورنس عبيدات ، المرجع السابق . ص ١٥٣ . انظر أيضاً عادل الأبيوكي ، المرجع السابق . ص ٢٩ وما بعدها .

(٢٠) محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، بدون تاريخ . ص ٢٤٢ . انظر أيضاً عادل رمضان الأبيوكي ، التوقيع الإلكتروني في التشريعات الخليجية ، المرجع السابق . ص ٣٧ وما بعدها .

(٢١) محمد عبيد الكعبي ، المرجع نفسه ، ص ٢٤٠ . انظر أيضاً عادل الأبيوكي ، المرجع نفسه ، ص٣٨.

(Signture وتطبيقاتها عالية التكلفة مما يشكل عقبة أمام انتشار استخدام التوقيع الإلكتروني نظراً لاستخدامها تقنيات حديثة مكلفة لا يستطيع الشخص العادي وحتى بعض المؤسسات تحملها مما يحد من انتشار استخدام التوقيع الإلكتروني[٢٢].

المبحث الثاني:
صور التوقيع الإلكتروني وآليات حمايته:

يتخذ التوقيع الإلكتروني صوراً مختلفة بحسب الطريقة أو الأسلوب الذي يتم به، خاصة وأن القوانين التي نظمت هذا التوقيع لم تنص على شكل معين له، وتركت تحديد شكله والطريقة التي يتم بها إلى التطور الحاصل في التقنية وما قد ينشأ عنها، ولكن هذه القوانين حددت الضوابط العامة التي يجب أن يتوافر عليها هذا التوقيع.

وسنتناول في هذا المبحث أهم صور التوقيع الإلكتروني في المطلب الأول ثم آليات حمايته في المطلب الثاني ثم جهات تصديقه في المطلب الثالث.

المطلب الأول:
صور التوقيع الإلكتروني:

أولاً : التوقيع بالقلم الإلكتروني (Pen – Op):

من صور التوقيع الإلكتروني التي يمكن استخدامها في توثيق التصرفات القانونية التي تبرم على الوسائط الإلكترونية التوقيع باستخدام القلم الإلكتروني (Pen – Op) وهو عبارة عن قلم إلكتروني حسابي يمكن باستخدامه في الكتابة

(٢٢) عادل الأبيوكي ، المرجع نفسه ، ص ٣٧ . انظر أيضاً ممدوح محمد مبروك ، مدى حجية التوقيع الإلكتروني في الإثبات ، المرجع السابق . ص ١٧٥ وما بعدها .

على شاشة الحاسب الآلي الخاص بالموقِّع. ويتم ذلك باستخدام برنامج هو المسيطر والمحرك لهذه العملية، ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من التوقيعات، الأولى وهي خدمة التقاط التوقيع (Signature Capture Service) والثانية وهي خدمة التحقق من صحة التوقيع (Signature Capture Service)[٢٣]. حيث يتلقى البرنامج أولاً بيانات العميل عن طريق بطاقته الخاصة التي يتم وضعها في الآلة، وتظهر بعد ذلك التعليمات على الشاشة، ثم تظهر بعد ذلك رسالة إلكترونية تطلب توقيعه باستخدام قلم على مكان محدد داخل شاشة الحاسب الآلي (Monitor)، ويقوم هذا البرنامج بقياس خصائص معينة للتوقيع من حيث الحجم والشكل والنقاط والخطوط والالتواءات [٢٤]. ويطلب البرنامج من الشخص الضغط على مفاتيح معينة تظهر له على الشاشة تفيد بالموافقة أو عدم الموافقة على هذا التوقيع.

ومتى تمت الموافقة يتم تشفير البيانات الخاصة بالتوقيع وتخزينها باستخدام البرنامج، ثم تأتي مرحلة التحقق من صحة التوقيع، عن طريق مقارنة المعلومات مع التوقيع المخزن ويتم إرسالها إلى برنامج الحاسب الآلي الذي يحدد فيما إذا كان التوقيع صحيحاً أم مزوراً [٢٥].

وتوفر هذه الصورة من صور التوقيع الإلكتروني مزايا كثيرة، لمرونتها، وسهولة استخدامها حيث يتم بواسطتها تحويل التوقيع التقليدي إلى الشكل

(٢٣) ممدوح محمد مبروك ، مدى حجية التوقيع الإلكتروني في الإثبات ، المرجع السابق . ص١٤ وما بعدها. انظر أيضاً عبدالفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني ، (دراسة تأصيلية مقارنة)، دار الكتب القانونية ، القاهرة ، ٢٠٠٧م . ص ٣٠ وما بعدها .

(٢٤) ثروت عبدالحميد ، المرجع السابق . ص ٥١ . وما بعدها . انظر أيضاً عبدالفتاح بيومي حجازي، المرجع السابق . ص ٣٢ وما بعدها .

(٢٥) منير الجنبيهي ، ممدوح الجنبيهي ، التوقيع الإلكتروني وحجيته في الإثبات ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٤م . ص ١٠ وما بعدها .

الإلكتروني باستخدام أنظمة معالجة المعلومات [٢٦].

ورغم مزايا هذه الصورة، إلا أنها لا تتمتع بأي درجة من درجات الأمان التي يمكن أن تحقق الثقة في التوقيع.

ويعود ذلك إلى أن المرسل إليه يستطيع أن يحتفظ بنسخة من صورة التوقيع ويعيد نسخها ولصقها على أي وثيقة من الوثائق المحررة على الوسائط الإلكترونية ويدعي أن واضعها هو صاحب التوقيع الفعلي. الشيء الذي يحتاج إلى إثبات الصلة بين التوقيع بهذه الصورة والمحرر.

ولهذا السبب فإن هذا النوع من التوقيع الإلكتروني لا يعتد به في استكمال عناصر الدليل الكتابي المعد للإثبات [٢٧].

ثانياً : التوقيع الرقمي (Digital Signature):

من الصور الأخرى للتوقيع الإلكتروني التي تستخدم في إبرام التصرفات القانونية باستخدام الوسائط الإلكترونية وخاصة تلك التعاملات التي تتم عبر شبكة الإنترنت صورة التوقيع الرقمي. ويقصد بالتوقيع الرقمي بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة، والذي يسمح للمرسل إليه إثبات مصدرها، والتأكد من سلامة مضمونها، وتأمينها ضد أي تحريف أو تعديل [٢٨].

ويتم ذلك باستخدام مفاتيح سرية (Encryption Keys) وطرق حسابية

(٢٦) ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص ٥٠ وما بعدها .
(٢٧) عيسى غسان ربضى ، القواعد الخاصة بالتوقيع الإلكتروني ، المرجع السابق . ص ٦١ وما بعدها .
(٢٨) ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص ٦١ . انظر أيضاً محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت (دراسة مقارنة) ، المرجع السابق . ص٢٣٨ وما بعدها .

معقدة ومعادلات رياضية (لوغاريتمات) تتحول بواسطتها المعاملة من رسالة ذات كتابة عادية مقروءة ومفهومة إلى معادلة رياضية أو رسالة رقمية غير مقروءة وغير مفهومة، ما لم يتم فك تشفيرها ممن يملك مفتاح فك الشفرة والمعادلات الخاصة بذلك[٢٩].

وينشأ التوقيع الرقمي ويتحقق من صحته باستخدام التشفير، وبناءً على ذلك فإذا رغب الموقِّع بإرسال رسالة بيانات عبر البريد الإلكتروني (E-mail) مثلاً فإنه يقوم بإعداد ملخص الرسالة باستخدام برنامج تشفير وباستخدام المفتاح الخاص وإرسالها للشخص المتلقي، الذي يستخدم المفتاح العام للتحقق من صحة التوقيع الرقمي (Verification)، ثم ينشئ المرسل إليه ملخص رسالة باستخدام ذات برنامج التشفير ويقارن بين ملخص الرسالتين، فإذا كانتا متطابقتين (Identical) فهذا يدل على أن الرسالة وصلت بشكل سليم ودون أن يحصل لها تعديل أو تحريف، (Alteration or Change)، أما إذا حصل تعديل أو تحريف في الرسالة فسيكون ملخص الرسالة التي أفشاها المستلم مختلفة عن ملخص الرسالة التي أنشأها الموقِّع [٣٠].

(٢٩) ثروت عبدالحميد ، المرجع السابق . ص ٦١ .

(٣٠) يوجد نوعان من المفاتيح : مفتاح عام ومفتاح خاص ، المفتاح العام يسمح لكل شخص مهتم القيام بقراءة رسالة البيانات عبر الإنترنت ، لكن بدون أن يدخل أي تعديل عليها ، لأنه لا يملك المفتاح الخاص بها، فإذا وافق على مضمونها وملخصها ، ورغب في الالتزام بها ، وضع توقيعه عليها عن طريق المفتاح الخاص به، ثم يقوم بإعادة رسالة البيان إلى مصدرها مرفقاً بها توقيعها في ملف ، ثم يقوم بإعادة رسالة البيانات إلى مصدرها مرفقاً بها توقيعه في ملفه ، ولا يستطيع التاجر إجراء أي تعديل به ، بسبب عدم امتلاكه المفتاح الخاص بالموقِّع . ويعني ذلك ، أنه بوضع التوقيع على رسالة البيانات ، تقفل الرسالة بشكل كامل ، ولا يستطيع أي طرف التعديل فيها أو المساس بها بأي شكل من الأشكال إلا بالاستخدام المتزامن للمفتاحين الخاصين بصاحب رسالة البيانات وبصاحب التوقيع . انظر خالد ممدوح إبراهيم ، حجية البريد الإلكتروني في الإثبات ، دراسة مقارنة ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٨م . ص ٢١٤ . انظر أيضاً ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص ٦٢ وما بعدها .

وهذه الطريقة للتوقيع الإلكتروني تحقق أعلى درجات الثقة والأمان للمحرر، وتضمن تحديد هوية الأطراف بدقة، كما يعبر بشكل صريح وواضح عن إرادة صاحب الارتباط بالتصرف القانوني وقبوله لمضمونه، وتتوافر بالتالي كافة الشروط التي يتطلبها المشرع في المحررات لكي تكون لها الحجية في الإثبات. ولكن عيب التوقيع الرقمي هو في إمكانية سرقة هذه الأرقام أو معرفتها من قبل الغير، والتصرف فيها بشكل غير مشروع، وخاصة مع التقدم والتطور التقني وازدياد عمليات الاحتيال والقرصنة، ومحاولة بعض الأشخاص فك الشفرة (Code) والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني والقيام بنسخها، ومن ثم إعادة استخدامها بعد ذلك لأغراض غير مشروعة [٣١].

ثالثاً: التوقيع البيوميتري (Biometric Signature):

تقوم هذه الصورة على اعتماد الصفات والخواص الفيزيائية والطبيعية والسلوكية للأفراد والتي تختلف من شخص لآخر. ومن هذه الخواص البصمة الشخصية (Finger Printing)، مسح العين البشرية أو ما يعرف ببصمات قزحية العين (Retina Scanning)، وخواص اليد البشرية (Hand Gesmetry)، وبصمة نبرة الصوت(Voice Recognition)، والتعرف على الوجه البشري (Face Recognition)، وغير ذلك من الصفات الجسدية والسلوكية[٣٢].

(٣١) من سلبيات التوقيع الرقمي احتمال تعرضه للضياع أو السرقة ، ولكن يمكن الرد على هذا بأن التوقيع التقليدي هو عرضة أيضاً للتقليد والتزوير ، وسرية الرقم تكفي للدلالة على صدور الرقم عن صاحبه بحسب الأصل وعميل البنك ملزم بسرية الرقم السري للبطاقة حسب الاتفاق مع البنك ، وإذا تسرب لآخرين فهو مسؤول عن ذلك . ولذلك فإن العميل ملزم بالمحافظة على الرقم السري للبطاقة . إلا أن مسؤولية صاحب التوقيع الإلكتروني تنتفي عند قيامه بالإبلاغ عن سرقة أو فقدان البطاقة، وذلك بالنسبة لجميع العمليات المنفذة بعد الإبلاغ . انظر ممدوح محمد مبروك ، مدى حجية التوقيع الإلكتروني ، المرجع السابق . ص ١٥ وما بعدها . انظر أيضاً عبدالفتاح بيومي حجازي ، النظام القانوني للتوقيع الإلكتروني (دراسة تأصيلية مقارنة) ، المرجع السابق . ص ٣٥ وما بعدها . انظر أيضاً سعيد السيد قنديل ، التوقيع الإلكتروني ، المرجع السابق . ص ٧٣ وما بعدها .

(٣٢) إبراهيم الدسوقي أبوالليل ، الجوانب القانونية للتعاملات الإلكترونية ، مجلس النشر العلمي ، جامعة الكويت ، الكويت ، ٢٠٠٣م . ص ١٥٩ . انظر أيضاً ممدوح محمد مبروك ، مدى حجية التوقيع الإلكتروني في الإثبات . المرجع السابق . ص ١٢ وما بعدها .

وعند استخدام أي من هذه الخواص يتم أولاً الحصول على صورة للشكل وتخزينها داخل الحاسب الآلي حتى يمكن الرجوع إليها عند الحاجة، وهذه البيانات الذاتية يتم تشفيرها حتى لا يتمكن أي شخص من الوصول إليها ومحاولة تعديلها أو العبث بها، وفي ذات الوقت السماح للأشخاص المصرح لهم باستخدامها(٣٣). ولما كانت الخواص المميزة لكل شخص، كالبصمة الشخصية وبصمة العين وبصمة الصوت، تختلف عن تلك العائدة لغيره، فإن التوقيع البيوميتري يعتبر وسيلة يمكن الوثوق بها والاعتماد عليها لتمييز الشخص وتحديد هويته نظراً لارتباط الخصائص الذاتية به، وهو ما يتيح استخدامها في إقرار التصرفات القانونية التي تبرم باستخدام وسيلة إلكترونية(٣٤).

إلا أن ما يعيب هذه الصورة إمكان مهاجمتها ونسخها من قبل قراصنة الحاسب الآلي عن طريق فك شفرتها، إضافة إلى أنها ذات تكلفة عالية نسبياً، مما حد من انتشارها إلى درجة كبيرة، وجعلها قاصرة على بعض الاستخدامات المحدودة.

لذا فإن تأمين الثقة في التوقيع البيوميتري يتطلب استخدام منظومة بيانات مؤمنة للتوقيع الإلكتروني بحيث تضمن انتقاله دون إمكانية التلاعب فيه، إضافة إلى توافر الضوابط الفنية والشروط والمتطلبات القانونية اللازمة للاعتماد عليه كحجة في الإثبات(٣٥).

(٣٣) إبراهيم الدسوقي أبوالليل ، المرجع السابق . ص ١٥٩ . انظر أيضاً ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص٦٠ وما بعدها .
(٣٤) ثروت عبدالحميد ، التوقيع الإلكتروني ، المرجع السابق . ص٦٠ وما بعدها .
(٣٥) سعيد السيد قنديل ، التوقيع الإلكتروني ، المرجع السابق . ص ٧٠ وما بعدها . انظر أيضاً محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، مرجع السابق . ص ٢٣٨ وما بعدها.

المطلب الثاني:
آليات حماية التوقيع الإلكتروني:

يتطلب قيام مستخدم ما بالدخول لموقع ما للقيام بتعاملات إلكترونية مثلاً باستخدام شبكة الإنترنت، ضرورة تأمين تلك التعاملات في حالة استخدام التوقيع الإلكتروني.

وكلما كان الإجراء المتبع يحقق الثقة بين المتعاملين زادت كمية المعاملات الإلكترونية والتجارة الإلكترونية، حيث يقع على عاتق القائم على موقع التجارة الإلكترونية التوثق من صحة الطلب، والذي يتطلب التحقق من أن من يخاطبه هو فعلاً من سجل اسمه أو عنوانه الإلكتروني أو غير ذلك من البيانات والمعلومات التي تتطلبها المواقع التجارية على شبكة الإنترنت. ويكتسب هذا الأمر أهمية كبيرة في ضوء الزيادة الكبيرة في جرائم الاختراق والاحتيال الإلكتروني المرتكبة باستخدام شبكة الإنترنت. ومن هنا تأتي أهمية التشفير (Encryption)، لمنع مرتكبي جرائم الاختراق والاحتيال الإلكتروني من ارتكاب جرائمهم ضد هذه التعاملات الإلكترونية [٣٦]. والذي دفع بعض الجهات لإيجاد تقنيات لحماية أمن المعلومات عامة وأمن التجارة الإلكترونية خاصة، من خلال استخدام تقنية التشفير لضمان خصوصية تعاملات الأطراف ومنع أية تعديات عليها.

(٣٦) وتقوم هذه المواقع على شبكة الإنترنت بالتحقق من شخصية الشخص المخاطب من حيث توفير تقنيات التعريف بالشخص، ابتداء من كلمة السر(Password) إضافة إلى بصمة الصوت (Voice Recognition)، إضافة إلى تقنية التشفير . انظر عيسى غسان ربضى ، القواعد الخاصة بالتوقيع الإلكتروني ، المرجع السابق. ص ١٧٧ وما بعدها . انظر أيضاً خالد مصطفى فهمي ، النظام القانوني للتوقيع الإلكتروني ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٧م . ص ١٠٠ وما بعدها . انظر أيضاً لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، المرجع السابق . ص ١٣٣ وما بعدها .

أولاً : المقصود بالتشفير:

لم يتطرق المنظم السعودي للمقصود بالتشفير في نظام التعاملات الإلكترونية السعودي. إلا أن المشرع المصري عرفه في مشروع قانون التجارة الإلكترونية بأنه" تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها". كما عرفه المشرع التونسي في الفقرة (٥) من المادة (٣) من قانون المبادلات والتجارة الإلكترونية التونسي بأنه "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها"[٣٧].

أما بالنسبة لباقي التشريعات العربية التي تعاملت مع التجارة الإلكترونية، فقد تطرقت إلى تقنية التشفير بشكل غير مباشر وذلك من خلال تطرقها للتوقيع الإلكتروني الذي يعتمد بشكل أساسي على عملية التشفير.

أما الفقه فقد عرف البعض التشفير بأنه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها [٣٨].

ومن خلال التعريف السابق نجد أن التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهم محتواها إلا بواسطة فك الشفرة وتحويل الرموز والإشارات إلى نصوص مقروءة ومفهومة

(٣٧) عيسى غسان ربضى ، القواعد الخاصة بالتوقيع الإلكتروني ، المرجع السابق. ص ١٧٨ وما بعدها. انظر أيضاً لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، المرجع السابق . ص ١٣٥ وما بعدها .

(٣٨) عبدالفتاح حجازي ، النظام القانوني لحماية التجارة الإلكترونية ، دار الفكر الجامعي ، الإسكندرية، ٢٠٠٢م . ص ٢٠٣ . انظر أيضاً خالد مصطفى فهمي ، المرجع السابق . ص ١٠١ .

باستخدام مفاتيح التشفير العامة والخاصة، فهذه العملية لا تتم إلا إذا كان مستقبل الرسالة يملك مفتاح التشفير الذي يحول الإشارات والرموز إلى النص الأصلي(٣٩).

ثانياً :ضوابط التشفير:

١- **إباحة تشفير البيانات والمعلومات التي يتم كتابتها أو التعامل فيها باستخدام الوسائل الإلكترونية:** حيث إن غالبية التشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات. وأصدرت تلك الدول قوانين خاصة بالتجارة الإلكترونية لتتعامل مع التشفير. فنجد على سبيل المثال لا الحصر أن القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية تعامل معه بشكل مباشر من خلال نصوص خاصة، وأجاز استخدامه في المراسلات الإلكترونية وفي التعاملات الإلكترونية التجارية عبر شبكة الإنترنت.

كما أكد قانون المبادلات والتجارة الإلكترونية التونسي على أهمية حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها من أي اعتداء عليها سواء تم ذلك باستخدام عناصر التشفير الشخصية الخاصة بتوقيع من غير طرفي العلاقة لاستخدام التشفير في ارتكاب جرائم احتيالية أو سرقة مفاتيح التشفير التي تفك النص المشفر وترجعه إلى النص الأصلي باستخدام مفاتيح التشفير الخاصة (٤٠).

(٣٩) عبدالفتاح حجازي ، المرجع السابق . ص ٢٠٣ . انظر أيضاً لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، المرجع السابق . ص ١٣٧ وما بعدها .

(٤٠) مدحت عبدالحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م . ص ٣١ وما بعدها . انظر أيضاً لورنس محمد عبيدات ، إثبات المحرر الإلكتروني، المرجع السابق . ص ١٣٦ وما بعدها .

وقد عالجت التشريعات العربية الخاصة بالتجارة الإلكترونية عملية التشفير بطريقة غير مباشرة كما أوضحنا سابقاً من خلال التوقيع الإلكتروني وذلك باستثناء المشرع التونسي الذي تعامل مع عملية التشفير بشكل مباشر من خلال نصوص خاصة به منعاً لاختلاف التفاسير والاجتهادات الفقهية بشأنها [٤١].

٢- **الحق في الحفاظ على سرية البيانات والمعلومات المشفرة**: ويتطلب ذلك الاعتراف بحق أصحابها في سرية تلك البيانات والمعلومات وتجريم الاعتداء عليها. فقد اعتبر مشروع قانون التجارة الإلكترونية المصري أن الاعتداء على البيانات المرسلة بين طرفي العقد عبر شبكة الإنترنت هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بين طرفي العلاقة، لأن تلك البيانات والمعلومات تتميز بالخصوصية والسرية وتعبر عن إرادة الطرفين بالقيام بتصرف قانوني. واطلاع الغير على هذه البيانات والمعلومات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة والاعتداء على خصوصيتهم بمعرفة البيانات التي تم كشفها بعد فك التشفير [٤٢].

وقد وضع المشرع المصري نصوصاً في قوانين التجارة الإلكترونية تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة وإفشائها، سواء كان ذلك بشكل مباشر، أو عن طريق النص على أن أي اعتداء يقع على التجارة الإلكترونية يعد مخالفاً لأحكام القوانين وبالتالي يعاقب العقوبة المقررة [٤٣].

(٤١) مدحت عبدالحليم رمضان، المرجع السابق . ص ٣١ . انظر أيضاً لورنس محمد عبيدات ، المرجع السابق . ص ١٣٧ .

(٤٢) عبدالفتاح حجازي ، المرجع السابق ، ص ٢٠٤ . انظر أيضاً لورنس محمد عبيدات ، المرجع السابق. ص ١٣٨ .

(٤٣) مدحت عبدالحليم رمضان ، المرجع السابق . ص ٣٢ . انظر أيضاً لورنس محمد عبيدات ، المرجع السابق . ص ١٣٨ وما بعدها .

٣- اعتبار استخدام التشفير وسيلة يعتد بها قانوناً في تحرير البيانات والمعلومات من قبل الجهات المختصة: كأثر لإقرار المشرع للنص المشفر وحجيته في إثبات التصرفات القانونية فإنه يعتبر من المحررات الإلكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من قام بمخالفة الاتفاق المبرم بين الطرفين [٤٤].

ثالثاً : الهدف من التشفير:

تبرز أهمية التشفير في منع الغير من مستخدمي شبكة الإنترنت من الدخول إلى البيانات والمعلومات والحفاظ على سريتها وخصوصيتها للأطراف باستخدام وسائل إلكترونية رقمية أو رموز معينة عوضاً عن الكتابة التقليدية التي لا يعرفها إلا أطراف التعامل التجاري بما لا يسمح باستخدامها من قبل الغير.

فاستخدام التشفير تحقق أكبر درجة من الأمن والحماية لمستخدمي شبكة الإنترنت نتيجة لاستعمال أفضل طرق التشفير والتي يصعب فكها [٤٥].

رابعاً : طرق التشفير:

يتم التشفير من خلال استعمال المفاتيح الخاصة في عملية تشفير الرسالة. وفك تشفيرها. ويتم ذلك بتحويل الرسائل إلى أشكال تظهر وكأنها لا يمكن فهمها وبالتالي إعادة النص إلى ما كان عليه في السابق. ويتم الاستعانة بمفتاحين مختلفين مرتبطين بشكل حسابي لإنشاء التوقيع الإلكتروني، لتحويل البيانات والمعلومات ثم تثبيتها مرة أخرى بنظام التشفير الغير متماثل ولا يستطيع الغير لو

(٤٤) عبدالفتاح حجازي ، المرجع السابق . ص ٢٠٤ . انظر أيضاً لورنس محمد عبيدات ، المرجع السابق. ص ١٣٨ .

(٤٥) عبدالفتاح حجازي ، المرجع السابق . ص ٢٠٥ . انظر أيضاً خالد مصطفى فهمي ، المرجع السابق. ص ١٠١ وما بعدها .

عرفوا مفتاح الشفرة العام اكتشاف المفتاح الخاص بالموقِّع واستخدامه في التعرف على محتوى الرسالة [٤٦]. والمفتاح الخاص يكون معروفاً لدى جهة واحدة فقط أو شخص واحد وهو المُرسِل، ويُستخدم لتشفير الرسالة وفك شفرتها. أما المفتاح العام فعادة ما يكون معروفاً لدى أكثر من جهة أو شخص.

ويؤدي فك الشفرة إلى إفشاء البيانات والمعلومات وانتشارها وبالتالي الإضرار بأصحابها وبالغير. ويجب بالتالي على المشرعين أن ينصوا على عقاب من يقوم بفك الشفرة وفض المعلومات المشفرة نظراً للأضرار الكبيرة التي تترتب على هذا الفعل [٤٧].

المبحث الثالث:
الجرائم المتصلة بالتوقيع الإلكتروني
والعقوبات المقررة لها في النظام السعودي:

تدخل الجرائم المتصلة بالتوقيع الإلكتروني ضمن الجرائم المعلوماتية [٤٨]. ونتيجة لظهور تقنية التوقيعات الإلكترونية، واستخدامها في التعاملات الإلكترونية، ظهرت الجرائم المتعلقة بهذا النوع من التوقيعات، وصدرت الأنظمة والقوانين في دول العالم لتنظيمها، ومن هذه الأنظمة نظام التعاملات الإلكترونية والذي نص على أنه من أهدافه " منع إساءة الاستخدام والاحتيال في التعاملات

(٤٦) عبدالفتاح حجازي ، المرجع السابق . ص ٢٠٤ . انظر أيضاً خالد مصطفى فهمي ، المرجع السابق. ص ١٠١ وما بعدها .

(٤٧) عبدالفتاح حجازي ، المرجع السابق . ص ٢٠٥ . انظر أيضاً لورنس محمد عبيدات ، المرجع السابق. ص ١٣٩ وما بعدها .

(٤٨) وقد عرف نظام مكافحة الجرائم المعلوماتية السعودي الجريمة المعلوماتية بأنها " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام " . انظر المادة (١) ، الفقرة (٨)، نظام مكافحة الجرائم المعلوماتية السعودي ، الصادر بالمرسوم الملكي رقم (م/ ١٧) وتاريخ ٨/ ٣/ ١٤٢٨هـ.

والتوقيعات الإلكترونية" [٤٩]. وتهدف الحماية الجنائية في مجال المعلوماتية بشكل عام إلى الحد من وقوع الجرائم المعلوماتية، مما يؤدي إلى ما يأتي:

١. المساعدة على تحقيق الأمن المعلوماتي.
٢. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
٣. حماية المصلحة العامة، والأخلاق، والآداب العامة.
٤. حماية الاقتصاد الوطني[٥٠].
٥. إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بوساطة سجلات إلكترونية يُعوِّل عليها.
٦. إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.
٧. تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي، للاستفادة منها في جميع المجالات، كالإجراءات الحكومية، والتجارة، والطب، والتعليم، والدفع المالي الإلكتروني.
٨. إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية.
٩. منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية[٥١].

(٤٩) المادة (٢)، نظام التعاملات الإلكترونية السعودي.
(٥٠) المادة (٢)، نظام مكافحة الجرائم المعلوماتية السعودي.
(٥١) المادة (٢)، نظام التعاملات الإلكترونية السعودي، الصادر بالمرسوم الملكي رقم (م/١٨) وتاريخ ١٤٢٨/٣/٨هـ.

وسنقوم فيما يلي ببيان بعض الصور المجرمة ذات الصلة بالتوقيع الإلكتروني ثم نتناول العقوبات المقررة نظاماً لهذه الجرائم في النظام السعودي.

المطلب الأول:

الجرائم المتصلة بالتوقيع الإلكتروني:

أولاً: جريمة الدخول غير المصرح به على منظومة توقيع إلكتروني:

وتتحقق هذه الجريمة بالدخول إلى منظومة توقيع إلكتروني، والتي عرفها نظام التعاملات الإلكترونية السعودي بأنها " منظومة بيانات إلكترونية معدة بشكل خاص لتعمل مستقلة أو بالاشتراك مع منظومة بيانات إلكترونية أخرى لإنشاء توقيع إلكتروني"(٥٢). وقد جرم المنظم السعودي فعل "الدخول على منظومة توقيع إلكتروني لشخص آخر دون تفويض صحيح، أو نسخها، أو إعادة تكوينها، أو الاستيلاء عليها(٥٣).

الركن المادي لهذه الجريمة:

ويتحقق الركن المادي لهذه الجريمة في حالتين:

أ- الدخول بأية وسيلة كانت على منظومة توقيع إلكتروني لشخص آخر دون تفويض صريح. وفي هذه الحالة يتحقق قيام الركن المادي بمجرد الدخول، ولا يتطلب الأمر إحداث نتيجة إجرامية وفق مدلولها المادي.

ب- الدخول بأية وسيلة كانت على منظومة توقيع إلكتروني لشخص آخر

(٥٢) المادة (١) ، الفقرة (١٥) ، نظام التعاملات الإلكترونية السعودي ، الصادر بالمرسوم الملكي رقم (م/ ١٨) وتاريخ ٨/ ٣/ ١٤٢٨هـ.

(٥٣) المادة (٢٣) ، الفقرة (٨) ، نظام التعاملات الإلكترونية .

دون تفويض صحيح. وينتج عن ذلك نسخ للمنظومة، أو إعادة تكوينها أو الاستيلاء عليها [٥٤].

الركن المعنوي لهذه الجريمة:

يتحقق الركن المعنوي في جريمة الدخول غير المصرح به على منظومة توقيع إلكتروني على توافر القصد الجنائي العام بركنيه العلم والإرادة. فيجب أن تتجه إرادة الجاني إلى فعل الدخول، أو البقاء غير المشروع إلى منظومة توقيع إلكتروني وأن يعلم أنه ليس من حقه الدخول أو البقاء في هذه المنظومة[٥٥].

ويتحقق القصد الجنائي سواء في الدخول أو البقاء غير المشروع بغض النظر عن الباعث، فإذا كان قصد المتهم من الدخول إلى نظام معين هو أن يثبت للجهة التي يقوم باختراقها أن هناك ثغرات في أنظمتها المطبقة، فإن ذلك يعتبر من قبيل البواعث التي لا تنفي توافر القصد الجنائي. وجريمة الدخول إلى منظومة توقيع إلكتروني أو البقاء فيه هي جريمة عمدية، فيجب أن يعلم الجاني بأنه يدخل إلى موقع لا يجوز له الدخول فيه وأن تتجه إرادته إلى ذلك. ومن ثم لا تتوافر إذا كان الدخول أو البقاء قد تم عن طريق الخطأ[٥٦].

(٥٤) وهذه الحالة أشد من سابقتها ، حيث يترتب عليها نتيجة جرمية تتمثل في نسخ لمنظومة التوقيع الإلكتروني، أو إعادة تكوينها أو الاستيلاء عليها. انظر عبدالمحسن الخنين ، المرجع السابق ، ص٧٦ وما بعدها.

(٥٥) وتطبيقاً لذلك ، قضى بوقوع الجريمة من أحد المتخصصين في علوم الحاسب الآلي أراد أن يثبت لأحد البنوك في الولايات المتحدة قدرته الفنية على اختراق أنظمة البنك . انظر مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية ، القاهرة ، ٢٠٠١م . ص ٥٣ وبعدها .

(٥٦) جميل عبدالباقي الصغير ، الإنترنت والقانوني الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠١م . ص١٣٤.

ثانياً: جريمة تقديم معلومات خاطئة عمداً عن التوقيع إلى أي من الأطراف التي وثقت بهذا التوقيع:

الركن المادي للجريمة:

يتحقق الركن المادي لهذه الجريمة بارتكاب السلوك الإجرامي والذي يتمثل في تقديم معلومات خاطئة عمداً عن التوقيع الإلكتروني إلى أي من الأطراف الذين وثقوا بذلك التوقيع. والمعلومات الخاطئة هي المعلومات الكاذبة التي لا تعبر عن الحقيقة، ويستوي في المعلومات الخاطئة أن تكون معالجة أو غير معالجة، أي سواء قد دخلت ضمن نظام معلوماتي أو لم تدخل بعد، وهذا ما يعني إمكانية الإدلاء بهذه المعلومات قبل معالجتها(٥٧).

الركن المعنوي للجريمة:

أما الركن المعنوي لهذه الجريمة فهذه الجريمة عمدية، يتمثل ركنها المعنوي في القصد الجنائي بعنصريه العلم والإرادة، ويتحقق ذلك بعلم الجاني بأن هذا السلوك مجرم، مع علمه بأنه يقدم معلومات خاطئة عن التوقيع الإلكتروني إلى أي من الأطراف الذين وثقوا بذلك التوقيع مع انصراف إرادته إلى هذا السلوك(٥٨).

ثالثاً: جريمة تزوير التوقيع الإلكتروني:

يمثل تزوير التوقيع الإلكتروني صورة لا تقل أهمية عن التزوير التقليدي في المحررات الورقية. وتتجه التشريعات المقارنة في تجريم تزوير التوقيع الإلكتروني إلى وضع نصوص عامة بتحريم هذا التزوير، ومن ثم يمتد حكم هذه النصوص

(٥٧) عادل رمضان الأبيوكي ، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة) ، المكتب الجامعي الحديث ، القاهرة، ٢٠٠٩م . ص ٤٧ وما بعدها .

(٥٨) عبدالفتاح حجازي ، النظام القانوني للتوقيع الإلكتروني، المرجع السابق ، ص ٥٧١ وما بعدها.

ليشمل التزوير الحاصل في كافة صور هذه المستندات.

ونرى أن أهمية تجريم التزوير في التوقيع الإلكتروني تتمثل في أن فكرة المحرر في جرائم التزوير التقليدية لا تلتقي مع فكرة المستند الإلكتروني، الشيء الذي يجعل من هذا التجريم ضرورة لحماية هذا المستند[٥٩].

وقد جرم المنظم السعودي فعل تزوير سجل إلكتروني، أو توقيع إلكتروني، أو شهادة تصديق رقمي، أو استعمال أي من ذلك مع العلم بتزويره[٦٠].

الركن المادي للجريمة:

يتمثل الركن المادي لهذه الجريمة في سلوك الجاني المتمثل في فعل تغيير الحقيقة، والذي يكون محله التوقيع الإلكتروني. ويحصل التزوير بأي طريقة كانت، فطرق التزوير ليست محصورة بصورة معينة، بل تشمل كل طريقة يصدق عليها مسمى التزوير، يمكن أن يكيف مرتكبها على ارتكابه جريمة تزوير. ونرى أن هذا القول يتماشى مع طبيعة الجرائم المستحدثة، فقد ظهرت أنماط من التزوير لا تطالها النصوص التقليدية. وقد نص قانون التوقيع الإلكتروني المصري على أنه " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنية، أو بإحدى هاتين العقوبتين كل من:

- أتلف أو غيب توقيعاً أو وسيطاً أو محرراً إلكترونياً، أو زور شيئاً من ذلك بطريقة الاصطناع أو التعديل أو التحوير أو بأي طريق آخر.

(٥٩) أشرف توفيق شمس الدين ، الحماية الجنائية للمستند الإلكتروني ، دراسة مقارنة ، دار النهضة العربية، ط١ ، القاهرة ، ٢٠٠٦م . ص ١٠٤ وما بعدها .

(٦٠) المادة (٢٣) ، الفقرة (٦) ، نظام التعاملات الإلكترونية السعودي.

- استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك[٦١].

وأساس الركن المادي في جريمة تزوير التوقيع الإلكتروني هو تغيير الحقيقة، وقد حدد المشرع المصري صور هذا التزوير بأن نص على وقوعه بطريق "الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

وفي رأينا فإن المشرع المصري قد وجد أن محاولة حصر هذه الطرق يعد أمراً غير ممكن، لتعدد صور تغيير الحقيقة واختلافها وتجددها بما لا يمكن معه حصرها، ولهذا السبب استخدم عبارة " أو بأي طريق آخر ".

وينصب تغيير الحقيقة الذي تقوم به جريمة التزوير على التغيير الذي يمس بشكل مباشر حقاً أو مركزاً قانونياً فيجعله غير مطابق للواقع. لذا فإنه لو كان التغيير في الحقيقة لا يمس إلا مركز المتهم أو حقوقه فلا تزوير ولا تقع الجريمة أيضاً حتى لو كان التغيير يمس مركزاً قانونياً أو حقاً للغير إذا تم ذلك برضائه لكون هذا الرضاء يعني أنه هو الذي قام بتعديل مركزه القانوني أو حقوقه قبل المتهم. فإذا كان التغيير الواقع في المحرر قد قام به من له الحق في إثبات بيانات هذا المحرر بداية فلا يقع التزوير وطالما لم يتعلق بالمحرر حق للغير، وهو ما ذهب إليه قضاء محكمة النقض المصرية[٦٢].

والتزوير المعلوماتي يتصور طبقاً لذلك في مخرجات الحاسب الآلي أي البيانات والمعلومات والتوقيعات الإلكترونية الصادرة منه على أن يتم وضعها

(٦١) المادة (٢٣) ، قانون التوقيع الإلكتروني المصري.
(٦٢) راجع في ذلك حكم محكمة النقض الجنائي المصرية جلسة ٣٠/ ١٠/ ١٩٣٠م ، مجموعة القواعد القانونية – ج٢ ، رقم ٨٠ ، ص ٧٥ .

على دعامة مكتوبة أو مسجلة ذات كيان مادي يمكن إدراكه بحاسة من الحواس. إلا أن الفقه قد ذهب إلى تعريف التزوير في نطاق المعلومات بأنه تغيير الحقيقة بأية وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق أو إحداث نتائج قانونية معينة(٦٣).

وعرف قانون العقوبات الفرنسي الجديد التزوير بأنه " كل تغيير بطريق الغش في الحقيقة ويكون من شأنه إحداث ضرر، ويرتكب بأي طريقة" (٦٤).

ولم يشترط المشرع الفرنسي في القانون الصادر عام ١٩٩٤م ضرورة أن يحدث التغيير للحقيقة بوسيلة معينة، حيث أجاز أن يحدث تغيير الحقيقة بأي وسيلة كانت ويستوي أن يحدث تغيير الحقيقة على محرر أو دعامة، أو سند طالما أن هذه الدعامة من الممكن أن يكون لها أثر في إفشاء حق أو كل ما من شأنه إحداث نتائج قانونية معينة.

والمشرع الفرنسي رغم محاولته إعطاء مرونة أكبر في تحديد الركن المادي بقوله إن التزوير هو " تغيير الحقيقة "، فإن ما نص عليه المشرع الفرنسي هو أقرب للوصف منه إلى تحديد الفعل الذي يقوم به التزوير. ففعل اصطناع التوقيع أو الوسيط أو المحرر الإلكتروني لا ينطوي على تغيير الحقيقة في مستند قائم، وإنما قد لا يكون للمستند الذي اصطنعه الجاني نظير، فإرسال رسالة إلكترونية مصطنعة تتضمن إيجاباً غير صحيح منسوباً لآخر، لا يعد تغييراً للحقيقة(٦٥).

(٦٣) أشرف شمس الدين ، المرجع السابق ، ص ١٦٦ وما بعدها. انظر أيضاً هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، مكتبة الآلات الحديثة ، أسيوط ، ١٩٩٤م . ص١٧٩ وما بعدها .

(٦٤) هشام رستم ، المرجع السابق . ص ١٨٠ وما بعدها .

(٦٥) عبدالفتاح حجازي ، المرجع السابق . ص ٥٤٢ وما بعدها .

وبينما لم يحدد المشرع المصري طبيعة البيان الذي يصلح أن يكون محلاً للتزوير، فإن القانون الفرنسي تطلب أن يكون من شأن التزوير إحداث ضرر في إثبات حق أو واقعة لها آثار قانونية.

ويكون التزوير في نطاق المعلومات بتغيير الحقيقة في الشرائط أو المحررات التي تمثل مخرجات الحاسب الآلي طالما حدث تغيير الحقيقة في بيانات الحاسب الآلي نفسه. وهو ما سار عليه قانون العقوبات الفرنسي الجديد حيث نص على أن الركن المادي للتزوير هو التغيير التدليسي للحقيقة، وبذلك أصبح النص يتعامل مع حالات التزوير التقليدي للمحررات، وكذا تزوير المحررات التقليدية والإلكترونية التي تكون مطبوعة على سند أو دعامة أو بأية وسيلة[٦٦]. ولا يكفي لاكتمال الركن المادي لجريمة التزوير أن يقع تغيير الحقيقة في محرر وأن يحصل هذا التغيير بإحدى الطرق التي بينها القانون، وإنما ينبغي أن يكون من شأنه أن يسبب ضرراً للغير، وإذا انعدم الضرر تكون الجريمة غير قائمة. ويكفي أن يكون الضرر محتمل الوقوع.

ومن أكثر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني استخدام برامج حاسوبية، وأنظمة معلوماتية (Information Systems) خاصة بذلك، يتم تصميمها على غرار البرامج والنظم المشروعة، أو محاولة بعض الأشخاص كسر الشفرة (Breaking of the Code)، والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها وإعادة استخدامها بعد ذلك[٦٧].

(٦٦) المادة ٤٤١/ ١، قانون العقوبات الفرنسي الجديد .

(٦٧) خالد ممدوح إبراهيم ، الجرائم المتصلة بالتوقيع الإلكتروني ، الدار الجامعية ، الإسكندرية، ٢٠١٠م. ص٢٧٩ وما بعدها . انظر أيضاً عبدالمحسن عبدالعزيز الخنين ، الجرائم المتصلة بالتوقيع الإلكتروني ، معهد الإدارة العامة ، الرياض ، ١٤٣٢هـ . ص ٧٣ وما بعدها.

ومع صعوبة تزوير التوقيع الإلكتروني الرقمي المعتمد على تقنية المفتاحين العام والخاص إلا أنه متصور الحدوث، كما لو تحصل شخص على منظومة توقيع إلكتروني لشخص آخر بسرقة أو اختلاس أو ما شابه ذلك، ثم حصل منه توقيع عن طريق هذه المنظومة، فلا فرق بين حصول التزوير من منظومة اصطنعت خصيصاً للتزوير ومنظومة حقيقية حصل منها توقيع عن طريق الغش والتزوير(٦٨).

الركن المعنوي لهذه الجريمة:

جريمة التزوير من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، ويتحقق بإرادة الجاني تغيير الحقيقة، مع العلم بكافة عناصر ومكونات الجريمة.

وعلى ذلك لا بد أن يعلم الجاني حال ارتكابه لجريمة التزوير أن هذا الفعل محظور ومعاقب عليه، ومع ذلك يقبل القيام به وتتجه إرادته للفعل ويقبل النتائج المترتبة عليه.

ويلزم كذلك توافر القصد الخاص، أي اتجاه إرادة الجاني إلى تحقيق غاية معينة من إرتكاب الركن المادي (٦٩).

وقد ثار خلاف حول تحديد مفهومه، فقيل بأنه اتجاه نية المزور لحظة ارتكاب فعل تغيير الحقيقة إلى استعمال الشيء المزور فيما زور من أجله، وقيل بأنه

(٦٨) وقد جاء في أحد قرارات ديوان المظالم ما يدل على هذا، حيث نص على أنه " يستوي أن يكون التوقيع بختم اصطنع خصيصاً للتزوير ، أو أن يحدث خلسة بالختم الحقيقي ، ووضع توقيعات أو أختام مزورة عن طريق التزوير المادي . انظر قرار ديوان المظالم رقم هـ/ ١/ ٧٦ لعام١٤٠١هـ في القضية رقم ٢٦٢/ ١/ ق لعام ١٤٠١هـ الصادر بجلسة ١٦/ ٧/ ١٤٠١هـ والمنعقدة بمقر ديوان المظالم بالرياض ، مجموعة القرارات الجزائية الصادرة عن دوائر هيئة الحكم في قضايا الرشوة والتزوير لعام ١٤٠١هـ .

(٦٩) خالد ممدوح إبراهيم ، المرجع السابق . ص ٢٨٠ وما بعدها .

اتجاه نية الجاني إلى إحداث ضرر للغير، سواء كان الضرر حقيقياً أو احتمالياً، وهذا أوسع مفهوماً [٧٠].

رابعاً : جريمة استعمال توقيع إلكتروني مزور مع العلم بالتزوير:

جرم المنظم السعودي فعل استعمال توقيع إلكتروني مع العلم بتزويره.إذ نص في نظام التعاملات الإلكترونية على تجريم فعل " تزوير سجل إلكتروني، أو توقيع إلكتروني، أو شهادة تصديق رقمي، أو استعمال أي من ذلك مع العلم بتزويره".

الركن المادي لهذه الجريمة:

يتمثل الركن المادي لهذه الجريمة في السلوك الإجرامي، وهو فعل استخدام توقيع إلكتروني مزور، واستعمال التوقيع المزور قد يتم بإبرازه والاحتجاج به فيما زور من أجله، وذلك على اعتبار أنه صحيح. والأمر متروك للقاضي لتحديد ما إذا كان الفعل يعد استعمالاً من عدمه [٧١].

الركن المعنوي لهذه الجريمة:

هذه الجريمة عمدية، يتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، والذي يتحقق باتجاه إرادة الجاني إلى استعمال توقيع إلكتروني مزور مع العلم بتزوير ذلك التوقيع [٧٢].

خامساً: جريمة إتلاف التوقيع الإلكتروني:

جرم المنظم السعودي إتلاف التوقيع الإلكتروني وقد نص على ذلك في

(٧٠) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥. ص٥٨٢ وما بعدها.
(٧١) عبدالفتاح بيومي حجازي ، النظام القانوني للتوقيع الإلكتروني ، دار الكتب القانونية ، القاهرة، ٢٠٠٧م. ص ٥٦٨ وما عبدها .
(٧٢) عبدالفتاح حجازي ، المرجع السابق . ص ٥٦٩ .

نظام مكافحة الجرائم المعلوماتية السعودي حيث جرم فعل الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه أو تعديله، أو شغل عنوانه [٧٣].

الركن المادي لهذه الجريمة:

ويتحقق الركن المادي لهذه الجريمة إما بإتلاف أو تعييب أو تعطيل التوقيع الإلكتروني. ويقصد بالإتلاف التأثير في المال مع بقائه قابلاً للإصلاح أي إنقاص صلاحيته للاستعمال بينما مؤدى التخريب أو التوقيع أن التوقيع أو الوسيط أو المحرر الإلكتروني قد فقد صلاحيته للاستخدام[٧٤].

وقد يقع الإتلاف على المعلومات المنسوخة على شرائط أو دعامات، وقد يقع أيضاً على المكونات المادية والأجهزة المستخدمة في عمل التوقيع الإلكتروني مثل شاشات العرض (Monitors) والأشرطة والأسطوانات والكابلات والمفاتيح والأقراص الممغنطة، وغيرها من المكونات المادية سواء كانت تحوي بيانات أو برامج أو مجرد أوعية فارغة، بشرط أن يؤدي الإتلاف أو التخريب إلى التقليل من قيمتها الاقتصادية أو يؤدي إلى تعطيلها أو عدم صلاحيتها للاستخدام[٧٥].

وفعل الإتلاف يتحقق بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني قدرته على العمل، وقد يحدث ذلك عن طريق نشر فيروس معلوماتي أو حتى بسكب سائل على الوسيط الإلكتروني (Medium) المخزن عليه، ويحدث تعييب

(٧٣) المادة (٣) الفقرة (٣) ، نظام مكافحة الجرائم المعلوماتية السعودي.

(٧٤) عبدالفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية، القاهرة ، ٢٠٠٢م . ص ٢٠٣ وما بعدها .

(٧٥) عبدالفتاح حجازي ، المرجع السابق ، ص ٢٠٤ . انظر أيضاً عبدالفتاح حجازي ، النظام القانوني للتوقيع الإلكتروني ، دار الكتب القانونية ، القاهرة، ٢٠٠٧م. ص ٥٤٢ وما بعدها .

التوقيع الإلكتروني كذلك بنفس الوسيلة على نحو يفقده القدرة على العمل أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوهاً أو غير واضح كما يتحقق إتلاف المحرر الإلكتروني أو التوقيع الإلكتروني بأي وسيلة تؤدي إلى عدم الانتفاع به مثل تمزيقه أو حرقه أو نشر فيروس (Virus) على الوسيط المدون عليه يعدم الفائدة منه. أما التعييب فإنه يتحقق بأي سلوك إجرامي يؤدي إلى إفقاد المحرر الإلكتروني وظيفة من وظائفه مثل طمس التوقيع الإلكتروني المدون عليه أو طمس بعض الأسطر المكتوبة بطريقة إلكترونية فيه [٧٦].

ولا يتصور إتلاف أو تعييب المحرر الإلكتروني دون أن يمتد ذلك إلى الوسيط الإلكتروني، لأن الوسيط الإلكتروني عبارة عن دعامة تدون عليها المحررات الإلكترونية. وقد تكون قرصاً مدمجاً (CD) أو شريطاً ممغنطاً كما قد تكون جهاز الحاسب الآلي ذاته [٧٧].

ويتطلب قيام الجريمة ضرورة توافر الضرر حيث إن الضرر هو النتيجة الطبيعية لفعل الإتلاف الذي يقع على المال المعلوماتي، سواء المادي أو غير المادي، ويتسبب عنه أضرار بمالك هذا المال سواء بالإتلاف الكلي أو الجزئي للشيء أو بإنقاص قيمته، فالضرر هو النتيجة الإجرامية التي تترتب على الاعتداء وترتبط بالفعل برابطة سببية قانونية بمجرد توافر أركان الجريمة. ويستوي أن يتحقق الضرر في صورة الضرر المادي أو الضرر المعنوي [٧٨].

(٧٦) جميل عبدالباقي الصغير ، جرائم الإنترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠١م، ص٦٧ وما بعدها .
(٧٧) عبدالمحسن الخنين ، المرجع السابق . ص ٧٧ وما بعدها .
(٧٨) عبدالمحسن الخنين ، المرجع السابق . ص ٧٨ وما بعدها .

الركن المعنوي لهذه الجريمة:

هذه الجريمة من الجرائم العمدية، وصورة الركن المعنوي فيها هو القصد الجنائي العام في صورتي التعييب والإتلاف، بالإضافة إلى القصد الخاص المتمثل في نية التزوير في صورة التزوير المعلوماتي.

وعلى ذلك لا بد أن يعلم الجاني حال ارتكابه لجريمة الإتلاف أو التعييب أو التزوير أن هذا الفعل محظور ومعاقب عليه، ومع ذلك يقبل القيام به وتتجه إرادته لاقتراف الفعل وقبول النتائج المترتبة عليه. هذا فضلاً عن توافر القصد الخاص في جريمة تزوير المحرر الإلكتروني أو التوقيع الإلكتروني[٧٩].

سادساً: جريمة إنشاء توقيع إلكتروني أو نشره أو استعماله لغرض احتيالي أو لأي غرض غير مشروع:

جرم نظام التعاملات الإلكترونية السعودي إنشاء شهادة رقمية أو توقيع إلكتروني أو نشرهما، أو استعمالها لغرض احتيالي، أو لأي غرض غير مشروع"[٨٠].

الركن المادي لهذه الجريمة:

ويتمثل الركن المادي لهذه الجريمة بارتكاب السلوك الإجرامي ويتمثل في إنشاء توقيع إلكتروني أو نشره أو استعماله لغرض احتيالي أو لأي غرض غير مشروع.

والغرض الاحتيالي يقصد به خداع المجني عليه، كمن ينشئ شهادة رقمية أو توقيعاً إلكترونياً ليدعم صفقة وهمية عن طريق البيع الإلكتروني (Electronic

(٧٩) أشرف شمس الدين، المرجع السابق. ص ١٢١ وما بعدها.
(٨٠) المادة (٢٣)، الفقرة (٥)، نظام التعاملات الإلكترونية السعودي.

(Sale أو لخداع الناس لأي غرض كان [٨١].

الركن المعنوي لهذه الجريمة:

أما الركن المعنوي لهذه الجريمة فهذه الجريمة جريمة عمدية، يتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، ويتحقق ذلك بإنصراف إرادة الجاني إلى إنشاء توقيع إلكتروني أو نشره أو استعماله لغرض احتيالي، أو لأي غرض غير مشروع، مع علمه بتجريم هذا السلوك.

ويتطلب الركن المعنوي أيضاً توافر قصد خاص يتمثل في الغاية أو الباعث الذي من أجله ارتكب الجاني هذا السلوك المجرم، وهو في هذه الجريمة تحقيق غرض احتيالي أو غرض غير مشروع [٨٢].

المطلب الثاني:
العقوبات المقررة في النظام السعودي
للجرائم المتعلقة بالتوقيع الإلكتروني:

نص نظام التعاملات الإلكترونية السعودي على أنه " مع عدم الإخلال بأي عقوبة أشد ينص عليها في نظام آخر، يعاقب كل من يرتكب أياً من الأعمال المنصوص عليها في المادة (الثالثة والعشرين) من هذا النظام بغرامة لا تزيد على خمسة ملايين ريال. أو بالسجن مدة لا تزيد على خمس سنوات، أو بهما معاً. ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة[٨٣].

ويتضح لنا من المادة السابقة أن هناك عقوبتين للجرائم المتصلة بالتوقيع

(٨١) عبدالفتاح حجازي ، النظام القانوني للتوقيع الإلكتروني ، المرجع السابق . ص ٥٦٣ وما بعدها.
(٨٢) عبدالفتاح حجازي ، المرجع السابق . ص ٥٦٤ وما بعدها.
(٨٣) المادة (٢٤) ، نظام التعاملات الإلكترونية السعودي .

الإلكتروني.

أولاً: العقوبة الأصلية: وهي العقوبة الأساسية المقررة للجريمة، والتي توقع منفردة دون أن يكون النطق بها متوقفاً على النطق بعقوبة أخرى.

وتتمثل العقوبة الأصلية للجرائم المتصلة بالتوقيع الإلكتروني بغرامة لا تزيد على خمسة ملايين ريال، أو بالسجن مدة لا تزيد على خمس سنوات، أو بهما معاً. والملاحظ أن المنظم السعودي قد شدد في قيمة الغرامة إذا ما ارتكبت إحدى المخالفات المنصوص عليها في هذا النظام وهو أمر سيساعد في مكافحة هذه الجرائم.

ثانياً: العقوبة التكميلية: وهي العقوبة التي لا توقع بالمحكوم عليه إلا إذا نص عليها الحكم بشكل صريح، وهي قد تكون وجوبية يلتزم القاضي بالحكم بها، وقد تكون جوازية يترك الأمر فيها لتقدير القاضي. وتتمثل العقوبة التكميلية للجرائم المتصلة بالتوقيع الإلكتروني بالحكم جوازاً بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة [٨٤].

(٨٤) فوزية عبدالستار ، مبادئ علم الإجرام والعقاب ، دار النهضة العربية ، القاهرة ، ١٩٨٢م . ص ٢٢٠ وما بعدها.

الخاتمـــــة:

تناولنا في هذا البحث موضوع جرائم الاعتداء على التوقيع الإلكتروني في النظام السعودي. إذ مع التطور الكبير في استخدام الحاسب الآلي وشبكة الإنترنت ظهرت الحاجة إلى استخدام المحررات والتوقيعات الإلكترونية خاصة مع ظهور التجارة الإلكترونية وانتشارها كأحد أبرز وأهم تطبيقات استخدام التقنية الحديثة وكذلك استخدامات الحكومة الإلكترونية. وقد أدى انتشار استخدام التوقيع الإلكتروني إلى زيادة مضطردة في الجرائم الواقعة عليه. وقد توصلنا في نهاية البحث إلى النتائج والتوصيات الآتية:

أولاً: النتائج:

١- لا يمكن للتعاملات والتجارة الإلكترونية أن تتطور وتنمو وتزدهر في غياب إطار تشريعي وقانوني متكامل يقر صحة ونفاذية العقود والتعاملات الإلكترونية ويمنح المحررات والسجلات الإلكترونية الحجية في الإثبات تماماً كالمحررات والسجلات التقليدية. وتأكيداً لحرص مشرعي الدول المختلفة على وضع الضمانات الكفيلة بحرية التجارة الإلكترونية وإسباغ الحماية الجنائية على المستند الإلكتروني، تم تجريم أفعال الاعتداء على التوقيع الإلكتروني.

٢- أن من أبرز العقبات والمشاكل التي تواجه التعاملات الإلكترونية والتوقيعات الإلكترونية هي مشكلة تأمين سلامة وأمن هذه التعاملات والتوقيعات الإلكترونية.

٣- إن ما قد يتعرض له التوقيع من جرائم مستحدثة يستعصي تطبيق النصوص النظامية التقليدية عليها، مما يستدعي تقنين الجرائم ذات

الصلة بالتوقيع الإلكتروني في نظام خاص.

٤- لم يكن نظام التعاملات الإلكترونية السعودي موفقاً عندما وردت نصوصه خالية من تجريم صنع أو حيازة أو الحصول على برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني. ذلك أن العبث بالتوقيع الإلكتروني لا بد أن يتم من خلال تقنية فنية وبالتالي فإن تجريم سلوك صنع البرنامج أو النظام المعلوماتي أو حيازته أو الحصول عليه هو في حقيقته تجريم للأعمال التحضيرية التي يكون من شأنها الاعتداء على التوقيع الإلكتروني أياً كانت صورة الاعتداء وهو ما يعكس صورة من الحماية الجنائية الوقائية التي تستهدف منع الجريمة قبل وقوعها، تبررها خطورة هذه الأفعال، ومن جانب آخر، فإنه كان بمقدور المنظم السعودي أن يعاقب على الشروع في ارتكاب تلك الجريمة.

٥- تتعدد الصعوبات التي تعترض إثبات جرائم الاعتداء على التوقيع الإلكتروني ويتعلق بعضها بالعنصر البشري حيث تتم أفعال الاعتداء على التوقيع الإلكتروني عادة عن بُعد وقد تمتد إلى الاختصاص الإقليمي لدولة أخرى مما يضاعف صعوبة كشفها أو ملاحقتها، فضلاً عن نقص خبرة القائمين على التحقيق في تلك الجرائم. ويتعلق البعض الآخر بطبيعة أدلة إثبات جرائم التوقيع الإلكتروني مثل سهولة محو الدليل أو تدميره، وتعذر الوصول إلى الدليل الإلكتروني في تلك الجرائم، فضلاً عن ضخامة كم البيانات المتداولة، وصعوبة التعاون الدولي في ملاحقة مرتكبي جرائم الاعتداء على التوقيع الإلكتروني.

ثانياً – التوصيات:

١. ضرورة تطوير النصوص الإجرائية، بحيث تتسع للبحث عن الجرائم ذات الصلة بالتوقيع الإلكتروني، وضبطها بما يتفق مع طبيعتها.

٢. نرى أهمية قيام المنظم السعودي بإضافة فقرة للمادة (٢٣) من نظام التعاملات الإلكترونية السعودي تتعلق بتشديد العقوبة والتوسع في نطاق التجريم فيما يتعلق بالجرائم التي تمس حاسبات ونظم معلومات التوقيع الإلكتروني وشبكاته الخاصة بالدوائر والمصالح والمؤسسات الحكومية وما يتعلق بالأمن الوطني والمصلحة العامة.

٣. ضرورة وضع قواعد وآليات خاصة ومعايير لحفظ المحررات الإلكترونية، وذلك بإنشاء مرافق تعمل على القيام بهذه المهمة، على أن تنظم هذه القواعد والآليات مسؤولية هذه المرافق عن الإخلال بسرية هذه المحررات.

٤. ضرورة تطوير الوسائل التي يتم بها تلقي البلاغات في جرائم التوقيع الإلكتروني أو المنازعات الناشئة بشأنه مع ضرورة إيجاد آلية للتعاون الشرطي والقضائي الدولي في مجال التحقيق في جرائم الاعتداء على التوقيع الإلكتروني والانضمام للاتفاقيات الخاصة بالتعاون الشرطي والقضائي في مجال مكافحة تلك الجرائم حتى يتسنى ملاحقة مرتكبي مثل هذه الجرائم وتقديمهم للعدالة من خلال إجراءات التسليم والمساعدة والإنابة القضائية.

٥. ضرورة تأهيل الشرطة والمحققين وأعضاء النيابة العامة والقضاة في جرائم الحاسب الآلي على الأساليب التقنية المستخدمة في ارتكاب

جرائم الاعتداء على التوقيع الإلكتروني والعمل على تدعيم قدراتهم في الموضوعات المرتبطة بتلك الجرائم، وآليات مكافحتها، وكيفية البحث والتحقيق فيها، خصوصاً في الجانب المتعلق بجمع وسائل الإثبات وتقديم الأدلة. والتأكيد على أهمية عقد دورات تدريبية لهم حول التقنيات المستخدمة في ارتكاب مثل هذا النوع من الجرائم.

٦. ضرورة تصدي المشرعين لمسألة تحديد الاختصاص القضائي والقانون الواجب التطبيق في حالة حدوث نزاع بين الأطراف.

٧. ضرورة إجراء تعديل تشريعي لإزالة الغموض السائد بشأن الانتقال والمعاينة في جرائم الاعتداء على التوقيع الإلكتروني، وجواز إجراء ذلك عن طريق شبكة الإنترنت لتتواءم مع الطبيعة الافتراضية (Virtual Nature) لجرائم التوقيع الإلكتروني.

٨. ضرورة التأكيد على مقدمي خدمات التصديق بالحفاظ على المعلومات الشخصية للمشتركين وحمايتها من الإفشاء وترتيب المسئولية المدنية والجنائية على مقدمي خدمات التصديق في حالة حصول مثل هذا الإفشاء غير المشروع.

٩. ضرورة عقد دورات تدريبية وندوات ومؤتمرات وحلقات نقاش تتعلق بنظام التعاملات الإلكترونية وتعريف القضاة والمحامين والتجار والموظفين والمحققين والمدعين العامين ورجال الشرطة بهذا النظام وتطبيقاته المختلفة. كما يجب على كليات الحقوق وأقسام القانون والمعاهد المتخصصة تدريس مواد دراسية تتعلق وتشرح نظام التعاملات الإلكترونية وتطبيقاته المختلفة.

المراجـــع :

أولاً – الكتب والأبحاث العربية :

١- إبراهيم، خالد ممدوح، حجية البريد الإلكتروني في الإثبات : دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م .

٢- إبراهيم خالد ممدوح، الجرائم المتصلة بالتوقيع الإلكتروني، الدار الجامعية، الإسكندرية، ٢٠١٠م .

٣- أبوالليل، إبراهيم الدسوقي، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، الكويت، ٢٠٠٣م .

٤- أبوهيبة، نجوى، التوقيع الإلكتروني، تعريفه ومدى حجيته في الإثبات، بدون ناشر، بدون تاريخ .

٥- الأبيوكي، عادل رمضان، التوقيع الإلكتروني في التشريعات الخليجية، دارسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٩م .

٦- الجنبيهي، منير وممدوح، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤م .

٧- حجازي عبدالفتاح بيومي، النظام القانوني للتوقيع الإلكتروني (دراسة تأصيلية مقارنة)، دار الكتب القانونية، القاهرة، ٢٠٠٧م .

٨- حجازي، عبدالفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٢م .

٩- الخنين، عبدالمحسن عبدالعزيز، الجرائم المتعلقة بالتوقيع الإلكتروني، معهد الإدارة العامة، الرياض، ١٤٣٢هـ .

١٠- ربضي، عيسى غسان، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م .

١١- رمضان، مدحت عبدالحليم، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م .

١٢- الرومي، محمد أمين، المستند الإلكتروني، دار الكتب القانونية، القاهرة، ٢٠٠٨م .

١٣- رستم،هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م .

١٤- سليم، أيمن سعد، التوقيع الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٤م .

١٥- السند، عبدالله، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات " الإنترنت ")، دار الوراق للطباعة والنشر، ط٣، ٢٠٠٦م .

١٦- شرف الدين، أحمد، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة إلى مؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية، ٢٠٠٠م .

١٧- شمس الدين، أشرف توفيق، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، دار النهضة العربية، ط١، القاهرة، ٢٠٠٦م .

١٨- الصغير، جميل عبدالباقي، الإنترنت، القانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠١م .

١٩- عبدالحميد، ثروت، التوقيع الإلكتروني، ماهيته، مخاطره، دار الجامعة الجديدة، القاهرة، ٢٠٠٧م .

٢٠- عبدالحميد، خالد عبدالتواب، تطور مفهوم الدين الكتابي في ضوء التقنيات الحديثة، دراسة مقارنة، مجلة البحوث الأمنية، العدد ٤٤، ٢٠٠٩م .

٢١- عبيدات، لورنس محمد، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م .

٢٢- الغريب، فيصل سعيد، التوقيع الإلكتروني، وحجيته في الإثبات، بحوث ودراسات المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٠٥م .

٢٣- فهمي، خالد مصطفى، النظام القانوني للتوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م .

٢٤- قنديل، سعيد السيد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٦م .

٢٥- الكعبي، محمد عبيد، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، بدون تاريخ .

٢٦- مبروك، ممدوح محمد علي، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، ٢٠٠٩م .

٢٧- منصور، محمد حسين، مبادئ الإثبات وطرقه، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٤م .

٢٨- الملط، أحمد خليفه، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية،

٢٠٠٥م .

٢٩- المومني، عمر حسن، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دراسة قانونية وتحليلية مقارنة، دار وائل للنشر، الطبعة الأولى، عمان، ٢٠٠٣م .

ثانياً - القوانين والأنظمة :

١- القانون المدني الفرنسي .

٢- قانون التوقيع الإلكتروني الفرنسي رقم (٢٣٠) لعام ٢٠٠٠م .

٣- القانون رقم (١٥) المصري لعام ٢٠٠٤م والخاص بتنظيم التوقيع الإلكتروني .

٤- قانون الإثبات المصري .

٥- نظام التعاملات الإلكترونية السعودي، الصادر بقرار مجلس الوزراء رقم (٨٠) وتاريخ ٧/ ٣/ ١٤٢٨هـ .

٦- قانون المعاملات الإلكترونية الأردني لعام ٢٠٠١م .

٧- قانون رقم (٢) لعام ٢٠٠٢م بشأن المعاملات والتجارة الإلكترونية الخاص بإمارة دبي .

٨- القانون الاتحادي الإماراتي رقم (١) لعام ٢٠٠٦م في شأن المعاملات والتجارة الإلكترونية .

ثالثاً - المراجع الأجنبيـــة :

1. Burke, Anthony, EU and Irish Internet Law an Overview, 13 Int'l L. Practicum, at 107, 113 15 (autumn 2000).

2. Dunn, Amy J, Survey of Legislation: Uniform Electronic Transactions

Act, 24 U, ARK. Little Rock L. Rev. 603, 612, (2002).
3. Klosek, Jacqueline, EU Telecom Ministers Approve Electronic Signatures Directive, 4 Cyberspace Law 12 (2000)
4. Pappas, Christapher William, Comparative U.S. and EU Approaches to E-Commerce Regulations: Jurisdiction, Electronic contracts, Electronic Signatures and Taxation 31 DENV. J. Int'l and Poly 325, 341, (2002.(
5. Rambarran, I Accept But Do They? : The Need for Electronic Signature Legislation on Mainland China, 15 TRANSNAT'l Law 405, 417-18 .
6. Suksomnil, Beijamin, an Analysis of the Electronic Signatures in Global and National Commerce Act and its Effects on E-Commerce and the Online Consumer, 2002 Syracuse L and Tech J. 2, and 5 (2002).

رابعاً – القوانين الأجنبيـــة :

1. U.S. Unified Electronic Transactions Act: 7A U.L. A 252 (2002.(

خامساً – الاتفاقيات والقرارات الإقليمية والدولية :

1. European Council Directive 2000/31/EC, 2000 O.J. (L .178) 1-12.
2. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), United Nations Commission on International Trade Law.
3. European Union Electronic Commerce Directive, 1999/93/EC.

سادساً: الإنترنت:

1. BBC News, Business, Digital Signature Becomes Law, at : http://news.bbc.co.uk/2/hi/business/1446426
2. BBC News, Clinton Oks, e-signatures at: http://news.bbc.co.uk/2hi/science/nature/813437.stn.

سابعاً : الأحكام الأجنبية:

1. PNC Telecom V. Thomas (2002) EWHC 284 (Ch)

ثامنا: الصحف:

١) جريدة الشرق الأوسط، ١٤/ ٥/ ٢٠١٠م، العدد ١١٤٩٠. ص٣١.