العقود الإلكترونية وحمايتها في القوانين الوطنية والدولية (دراسة مقارنة)

د.أحمد إسحق شنب محمد

أستاذ مشارك- القانون الدولي العام- كلية القانون والشرعية - جامعة نيالا

المستخلص:

تناولت الورقة العلمية العقود الإلكترونية وحمايتها في القوانين الوطنية والدولية (دراسة مقارنة) وكان هدف الورقة يتركز حول التعرف على الموضوعات المتعلقة بالحماية القانونية للعقود الإلكترونية في ظل القوانين الوطنية والدولية، وذلك باستخدام المنهج العلمي الوصفي التحليلي، وقد إعتمد الباحث على طرق ووسائل لجمع المعلومات والتي لها علاقة بالورقة من ذلك الكتب والمراجع والمجلات المختصة والانترنت، وتتكون الورقة من الإطار العام للورقة: المقدمة المنهجية ومحورين، تناول المحور الأول: مفهوم الحماية الجنائية وفق القوانين السودانية، بينما تناول المحور الثاني: الحماية القانونية للعقود الإلكترونية في القوانين المقارنة وأخيراً الخاتمة وأهم النتائج والتوصيات وأهم المصادر والمراجع.

Absttract

The scientific paper dealt with electronic contracts and their protection in national and international laws (a comparative study). The aim of the paper was to identify issues related to the legal protection of electronic contracts in light of national and international laws, using the descriptive and analytical scientific approach, and the researcher relied on methods and means to collect information that is relevant to The paper includes books, references, specialized magazines and the Internet, and the paper consists of the general framework of the paper: the methodological introduction and two axes, the first axis deals with the concept of criminal protection according to Sudanese laws, while the second axis deals with the legal protection of electronic contracts in comparative laws and finally the conclusion and the most important findings and recommendations The most important sources and references.

المقدمة:

عـززت ثـورة المعلوماتيـة والاتصـالات جهـود الكثيريـن مـن فقهـاء القانـون بـضرورة إدراج القوانين التـي صـدرت في مجـال تنظيـم التجـارة الإلكترونيـة والعقـود التـي تـبرم في بيئتهـا، إن أمـر التجـارة الإلكترونيـة والعقـود الإلكترونيـة رغـم التحفظـات التـي تحيـط بهـا في الـدول الأوربيـة والولايـات المتحـدة الأمريكيـة إلا أنهـا أخـذت مكانتهـا تمامـاً في حيـاة الأشـخاص الطبيعيـين والشـخصيات الاعتباريـة لاسـيما وأنهـا قـد نظمـت تنظيـماً تشريعيـاً وقانونيـاً فيـه كثـير مـن الطمأنينـة والعفـة في نفـوس المتعاملـين، فضـلاً عـن السرعـة والأمـان والزمـن الـذي يمكـن أن يتكبـده الأطـراف. بطبيعـة الحـال لم يكـن محيطنـا العـربي منفـرداً وبعيـداً عـن هـذا الحـراك والتحـدي المعلومـاتي في أوجهـه المختلفـة حيـث صـدرت حزمـة مـن القوانـين التـي تعنـى بالتجـارة الإلكترونيـة في عديـد مـن الـدول العربيـة، منهـا قانـون المبـادلات التجاريـة الإلكترونيـة التونـسي لسـنة 2000م كأول قانـون يصـدر في هـذا الشـأن ثـم توالـت بعـد ذلـك مشروعـات القوانـين في مـصر والإمـارات وفي بلادنـا صـدر قانـون المعامـلات الإلكترونيـة وقانـون جرائـم المعلوماتيـة لسـنة 2007م بـل ذهـب المـشرع السـوداني أبعـد مـن ذلـك حيـث أنشـأ نيابـة للتجـارة الإلكترونيـة.

أ مفهوم الحماية الجنائية وفق القوانين السودانية

يعتـبر هـذا القانـون مـن أهـم القوانـين التـي أصدرهـا المـشرع السـوداني 2007م وذلـك في إطـار مواكبتـه لمعطيـات وتحديـات التجـارة الإلكترونيـة. نتطـرق في هـذا الجـزء لقانـون جرائـم المعلوماتيـة السـوداني لسـنة 2007م

الجريمة المعلوماتية:

الجريمـة لغـة مـن جَـرم جرمـاً أي أذنـب ذنبـاً، ويقـال جَـرَم نفسـه وقومـه وجَـرَم عليهـم وإليهـم وفي القـرآن الكريـم (يَـا أَيُّهَـا الَّذِيـنَ آمنـوا آوفـوا بِالْعُقُـودِ)[1]، أي لا يحملنكـم بغـض قـوم عـلى تـرك العـدل والاعتـداء عليهـم ويقـال أجـرم عليهـم وإليهـم أي جَنـىَ جنايـة[2].

تعريـف كلمـة جريمـة حيـث جـاءت كالآتي: «تشـمل كل فعـل معاقـب عليـه بموجـب أحـكام هـذا القانـون أي قانـون آخـر، والفعـل كـما هـو معـروف في هـذه المـادة يشـمل الامتناع»[3].أمـا كلمـة المعلوماتيـة فقـد أورد قانـون جرائـم المعلوماتيـة لسـنة2007م تعريفهـا في المـادة 3 تفسـير بأنهـا[4]: يقصـد بهـا نظـم وشـبكات ووسـائل المعلومـات، البرمجيـات والحواسـيب والإنترنـت والأنشـطة المتعلقـة بهـا. ومـن جملـة مـا ذكـر يمكننـا القـول إن الجريمـة المعلوماتيـة وفقـاً لهـذا القانـون هـي الفعـل أو الامتنـاع المعاقـب عليـه بموجـب هـذا القانـون والمتعلـق باسـتخدام نظـم وشـبكات ووسـائل المعلومـات والبرمجيـات والحواسـيب والإنترنـت والأنشـطة المتعلقـة بهـا اسـتخداماً مجرمـاً... سـنأتي بالنتائـج لـشرح تلـك المصطلحـات حتـى نقـف عـلى القيمـة العلميـة والعمليـة لهـا.

أولاً: المعلوماتيـة:أول مـن اسـتخدم لفـظ المعلوماتيـة هـو مديـر المعهـد الاتحـادي للمعلومـات والتقنيـة بالاتحـاد السـوفيتي سـابقاً كصفـة لعلـم المعلومـات العلميـة، ثـم ذاع اسـتخدامه بعـد ذلـك عـلى مسـتوى جغـرافي واسـع بمفاهيـم متباينـة حتـى أحـصى لـه البعـض أكـثر مـن ثلاثـين تعريفـاً مختلفـاً في الكتابات المتخصصة في علم المعلومات[5]. قـد عرفتهـا الأكاديميـة الفرنسـية في إبريـل 1967م

بأنه علم التعامل العقلاني وعلى الأخص بواسطة الآلات الأتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للاتصالات في ميادين التقنية والاقتصاد والاجتماع[6].

فيما نرى فإن تعريف القانون للمعلوماتية اقتصر على تعريف وسائلها وكان الأسلم أن تعرف بأنها(استخدام نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والإنترنت في الأنشطة المتعلقة بها) لأن المعلوماتية هى استخدام هذه الأجهزة والنظم في التعامل مع المعلومة، وبالتالي يتفق هذا التعريف مع تعريف الجريمة المعلوماتية في استخدام الأجهزة للتعامل مع أو الوصول للمعلومة على نحو مجّرم.

ثانياً: النظم والشبكات:تعرف الشبكة بأنها مجموعة حواسيب مرتبطة مع بعضها عن طريق وسيط نقل مناسب ومتطلبات الشبكة جهازان من أجهزة الحاسوب على الأقل وكرت شبكة، ووسيلة نقل وبروتوكولات وذلك للشبكة المحلية، أما الشبكة الواسعة فتحتاج لأجهزة حاسوب ومودم (MODEM) وخط هاتف وبروتوكولات أما فوائد الشبكة فهي المشاركة في المعلومات وتسهيل الوصول إليها وتقليل التكلفة ووجود مركزية (إدارية للشبكة) مع وجود الأمنية على المعلومات.

قد عرف القانون شبكة المعلومات في المادة 3 تفسير بأنها أي ارتباط بين أكثر من نظم معلومات للحصول على المعلومات أو تبادلها، وهذا التعريف يتسق مع تعريف الشبكات التي أوردناها من أنها مجموعة حواسيب مرتبطة مع بعضها عن طريق وسيط مناسب.

ثالثاً: وسائل المعلومات:تعريف المعلومات يسبقه تعريف البيانات والتي تعرف بأنها مجموعة من الحقائق يتم التعبير عنها بالكلمات أو الأرقام أو الأشكال أو الرموز أما المعلومات فيمكن تعريفها بأنها (بيانات خضعت للتشغيل والتحليل والتفسير لتحقيق زيادة المعرفة لمتخذي القرارات ومساعدتهم لتحقيق أغراض معينة وتمكينهم من الحكم السديد على الظواهر والشواهد والبيانات بهذا المعنى تشكل المادة الخام التي يتم تشغيلها للحصول على شكل أكثر فائدة واستخدامها بحسبان أن البيانات هي المادة الخام التي تشتق منها المعلومات.

رابعاً البرمجيات: تعد برمجيات الحاسوب(Soft Ware) من أهم البرمجيات التي لا يمكن للحاسب الآلي الاستغناء عنها وتعد هي لغة الحاسب ومنها ما قد يتم الاستغناء عنه ويستخدم عند الرغبة في البرمجة مثل كتابة الرسائل أو عمل جداول حسابية أو قواعد بيانات وقد حدث تطور هائل في برمجيات الحاسوب كي تواكب عصرنا حيث لم تعد قاصرة على استخدامها في الحواسيب الشخصية فقط ولكن أصبحت تستخدم حالاً بصورة أوسع على الشبكات المختلفة[7].

خامساً: الحواسيب والإنترنت: الحواسيب جمع حاسب آلي وهى ترجمة لكلمةComputer)) الإنجليزية ويقصد بها المعالجة الآلية للمعلومات بالحاسب الآلي أو المعلوماتية والتكنولوجيا من حيث تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر.

هذه إذاً تفاصيل تعريفات لما ورد في نص المادة (1) من القانون التي عرفت المعلوماتية، وكان لا بد من الإشارة إليها لارتباطها بما سيرد من مواد القانون لاحقاً وندلف إلى شرح المادة 2

مـن القانـون وهـي التـي تنـص عـلى تطبيـق القانـون.

المـادة (2) تطبيـق: تطبـق أحـكام هـذا القانـون عـلى أي مـن الجرائـم المنصـوص عليهـا فيـه إذا ارتكبـت كليـاً أو جزئيـاً داخـل أو خـارج السـودان أو امتـد أثرهـا داخـل السـودان وسـواء كان الفاعـل أصليـاً أو شريـكاً أو محرضـاً عـلى أن تكـون تلـك الجرائـم معاقبـاً عليهـا خـارج السـودان مـع مراعـاة المبـادئ العامـة الـواردة في القانـون الجنـائي لعام1991م.هـذه المـادة تنـص عـلى مبـدأ إقليميـة القانـون الجنـائي وكذلـك مبـدأ شـخصية القانـون الجنـائي ويندرج المبـدآن تحـت مبـدأ تطبيـق القانـون الجنـائي مـن حيـث المـكان ومـن الواضـح أن قانـون جرائـم المعلوماتيـة مـن القوانـين المسـاعدة للقانـون الجنـائي لـذا كان لا بـد مـن الإشـارة لهـذه المبـادئ لارتباطهـا الوثيـق بالجانـب الإجـرائي عنـد المحاكمـة.. وبتحليـل هـذه المـادة نجـد أنهـا تشـتمل عـلى الـشروط الآتيـة ليتـم تطبيـق أحـكام نصـوص مـواد القانـون:

1. أن ترتكـب الجريمـة المنصـوص عليهـا فيـه كليـاً أو جزئيـاً داخـل السـودان أو خارجـه أو يمتـد أثرهـا داخـل السـودان.
2. يستوي أن يكون الفاعل أصلياً أو شريكاً أو محرضاً.
3. يجب ان تكون الجرائم محل التطبيق معاقباً عليها خارج السودان.
4. تراعى المبادئ العامة الواردة في القانون الجنائي السوداني 1991م.

ونتعرض بالتفصيل لهذه الشروط:

الـشرط الأول: ارتـكاب الجريمـة كليـاً أو جزئيـاً داخـل السـودان أو خارجـه أو امتـداد أثرهـا لداخـل السـودان:النظر لهـذه الفقـرة يوضـح أنهـا تشـتمل عـلى ثلاثـة بنـود أولهـا ارتـكاب الجريمـة كليـاً أو جزئيـاً داخـل السـودان، والـذي يعنـى بـه إقليـم السـودان بحـدوده المعروفـة جـواً وبـراً وبحـراً. ويفهـم مـن ارتـكاب الجريمـة كليـاً أن ترتكـب الجريمـة نفسـها وتظـل آثارهـا داخـل السـودان، أمـا ارتكابهـا جزئيـاً فيعنـي أن يرتكـب جـزء مـن الفعـل المجـرم داخـل البـلاد ويكـون أثرهـا قـد تحقـق في الخـارج أو يمكـن أن يكـون مرتكـب الفعـل شريـكاً بالتحريـض أو المعاونـة مـن داخـل السـودان ويكـون الفاعـل الأصـلى خارجـه[8].

الـشرط الثـاني: وهـو امتـداد الأثـر إلى داخـل السـودان عـلى ذات التفصيـل المذكـور آنفـاً ويختلـف عنـه فقـط في أن الجريمـة ترتكـب كليـاً أو جزئيـاً خـارج السـودان. والملاحـظ أن هـذا القانـون يبـدو وكأنـه اسـتند عـلى مبـدأ عالميـة النـص الجنـائي إذ لم يشـتمل النـص عـلى عبـارة أن يكـون الجـاني سـودانيا وإنمـا جـاء معمـماً وهـذا وضـع اقتضتـه طبيعـة الجرائـم التـي تحكمهـا نصوصـه ومبـدأ عالميـة النـص الجنـائي يعنـى وجـوب تطبيـق القانـون عـلى كل جريمـة يقبـض عـلى مرتكبهـا في إقليـم الدولـة أيـاً كان جنسـية مرتكبهـا ويمتـاز هـذا المبـدأ بأنـه يقـرر للنـص الجنـائي نطاقـاً متسـعاً يـكاد يمتـد للعـالم بـأسره، إذ لا يجعـل لمـكان ارتـكاب الجريمـة أو لجنسـية مرتكبهـا اعتبـاراً ولا يشـترط سـوى أن يقبـض عـلى الجـاني في إقليـم الدولـة التـي تطبـق عليـه تشريعهـا، وأهميـة هـذا المبـدأ مسـتمد مـن خطـورة الإجـرام الـدولي[9].

لا شـك لدينـا في أن جرائـم المعلوماتيـة تمثـل أعتـي أنـواع الإجـرام الـدولي الخطـير والمنظـم وتتمثـل خطورتهـا في سـهولة ارتكابهـا، وصعوبـة الوصـول لمرتكبهـا، وآثارهـا المدمـرة عـلى النواحـي الاجتماعيـة

والاقتصادية فإطلاق فيروس واحد يمكن ان يسبب آثاراً لا يسهل تداركها.

نماذج لبعض الجرائم الواردة في قانون جرائم المعلوماتية:

أولاً: المادة (4) دخول المواقع وأنظمة المعلومات المملوكة للغير: كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً له ويقوم: (أ)بالإطلاع عليه أو نسخه يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو العقوبتين معاً.(ب)بإلغاء بيانات أو معلومات ملكاً للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً.

جاءت هذه المادة تحت عنوان دخول المواقع وأنظمة المعلومات المملوكة للغير. ويتضح من خلال النص أن أركان هذه الجريمة كما يلي:

1. أن يقوم الجاني بدخول موقع أو نظام معلومات.
2. أن لا يكون مصرحاً للجاني بدخول الموقع أو نظام المعلومات.
3. أن يقوم الجاني بالاطلاع على الموقع أو نسخه أو إلغاء بيانات أو معلومات مملوكة للغير أو حذف هذه المعلومات أو تدميرها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه. وشرح هذه المادة يتطلب التعرض لتعريف معنى المواقع وأنظمة المعلومات.

عرف القانون الموقع في المادة(3) بأنه: يقصد به مكان إتاحة المعلومات على شبكة المعلومات من خلال عنوان محدد. كما عرف في ذات المادة نظام المعلومات بأنه يقصد به مجموعة البرامج والأدوات المعدة لإنتاج وتخزين ومعالجة البيانات والمعلومات أو إدارة البيانات والمعلومات، ويبين من هذا التعريف أن الموقع يقصد به المواقع الإلكترونية الموجودة على شبكة الإنترنت وغيرها والتي لها عناوين محددة ويتضح ذلك من تعريف القانون لشبكة المعلومات في المادة (3) بأنها أي ارتباط بين أكثر من نظام معلومات للحصول على المعلومات أو تبادلها إذ من الواضح أن المشرع لم يقصر تعريف شبكة المعلومات على شبكة الإنترنت وإنما مدها لأي ارتباط بين أكثر من نظام معلومات أياً كان.

ونعود لتفصيل أركان هذه المادة على النحو الذي ذكرناه آنفاً:

الركن الأول: قيام الجاني بدخول موقع أو نظام معلومات: دخول المواقع الإلكترونية قد يكون بالطريقة المعتادة في الدخول وهي كتابة إسم الموقع بالطريقة المعروفة، غير أن الدخول بقصد تحقيق ما نصت عليه المادة قد يتم عن طريق اختراق هذه المواقع، ويصنف الاختراق إلى ثلاثة أقسام هي[10]: أولًا: اختراق الأجهزة، ثانياً: اختراق الموقع، ثالثاً: اختراق البريد الإلكتروني.

لكي تتم عملية الاختراق لا بد من برنامج يتم تصميمه ليتيح للمخترق الذي يريد إختراق الحاسب الآلي لشخص آخر أو اختراق موقع إلكتروني على شبكة الإنترنت أو اختراق البريد الخاص بشخص ما. وقد صممت العديد من البرامج التى تتيح عملية الاختراق وتجعلها سهلة عندما يتم استخدامها بواسطة محترفين.

الركن الثاني: ألا يكون الجاني مصرحاً له بدخول النظام والتصريح بدخول النظام محل

الإختراق.هـذا يعنـي أن الجـاني لـه هـذا الحـق بصفـة أو بأخـرى سـواء كان مسـتخدماً لـدى الجهـة مالكـة النظـام، أو تـم التصريـح لـه مؤقتـاً بدخـول النظـام للحصـول عـلى معلومـات معينـة لصالحـه هـو أو لصالـح جهـة أخـرى ويقـوم بالأفعـال المجرمـة المنصـوص عليهـا في المـادة.

إذ نـرى أن هـذا الجـزء مـن المـادة أي أن يكـون الشـخص غـير مـصرح لـه بدخـول النظـام لا معنـى للنـص عليـه أصـلاً.لأن الأمـر لا يخـرج عـن حالتـين هـما:(أ) أن يكـون الشـخص قـد أخـترق الموقـع أو نظـام المعلومـات بـلا تصريـح أصـلاً بقصـد الإضرار أو لواحـد مـن الأسـباب الـواردة في المـادة.(ب) أن يكـون لـه هـذا التصريـح ويقـوم بإرتـكاب ذات الفعـل. وفي الحالتـين فـإن الجريمـة تكـون قـد وقعـت بغـض النظـر عـن وجـود التصريـح مـن عدمـه خاصـة وأن المـشرع نـص في المـادة (5) مـن القانـون عـلى ارتـكاب فعـل مشـابه مـن الموظـف العـام والـذي قـد يفهـم أن لـه الصفـة في دخـول النظـام.

الركـن الثالـث: أن يكـون الغـرض مـن الدخـول للموقـع الاطـلاع عـلى الموقـع أو نسـخه أو إلغـاء بياناتـه أو معلومـات موجـودة بـه مملوكـة للغـير أو حذفهـا أو تغييرهـا أو إعـادة نشرهـا أو تغيـير تصاميم الموقـع أو إلغائـه أو شـغل عنوانه.وهـذا الركـن يعنـي أن تكـون المعلومـات الـواردة بالموقـع أو نظـام المعلومـات سريـة وغـير متاحـة للكافـة ويتحقـق ضرر مـن واحـد أو أكـثر مـن الأفعـال المنصـوص عليهـا في المـادة كـما أن تغيـير تصاميـم الموقـع أو إلغائـه تمامـاً أو شـغل عنوانـه بعنـوان آخـر يشـكل جريمـة بموجـب هـذه المادة.مثـل هـذا الفعـل يرتكبـه عـادة قراصنـة الكمبيوتـر وهـم المعروفـون بالهاكـرز (Hakers))والكراكـرز ((Cracker)أماالمـادة العقابيـة لهـذه الجريمـة فهـي السـجن مـدة لا تتجـاوز أربـع سـنوات أو بالغرامـة أو بالعقوبتـين معـاً[11].

المادة(5):دخول المواقع وأنظمة المعلومات من موظف عام:

كل موظـف عـام يدخـل بـدون تفويـض موقـع أو نظـام معلومـات خـاص بالجهـة التـى يعمـل بهـا أو يسـهل ذلـك للغـير يعاقـب بالسـجن مـدة لا تتجـاوز خمـس سـنوات أو بالغرامـة أو بالعقوبتـين معـاً.

أركان المادة:

1. أن يكون الجاني موظفاً عاماً.
2. أن يدخل موقعا أو نظام معلومات أو يسهل هذا الدخول للغير.
3. أن يكون الموقع أو نظام المعلومات الذي تم دخوله خاصا بالجهة التي يعمل بها الجاني.
4. أن يكون الدخول بدون تفويض.

هـذه المـادة تحكـم سـلوك الموظـف العـام، ولم يتطـرق القانـون لتعريفـه غـير أن القانـون الجنـائي السـودانى لعـام 1991م عـرف الموظـف العـام في المـادة (3) بأنـه يعنـى(كل شـخص تعينـه سـلطة عامـة للقيـام بوظيفـة عامـة سـواء كان التعيـين بمقابـل أو بـدون مقابـل وبصفـة دائمـة أم مؤقتـة) وبما أنـه لم يـرد تعريـف في القانـون للموظـف العـام كـما سـلف فـإن التعريـف الـذي يؤخـذ بـه هـو تعريـف القانـون الجنـائي 1991م، والملاحـظ أن هـذه المـادة جعلـت مجـرد الدخـول بـدون تصريـح أوتسـهيل هـذا الدخـول للغـير لموقـع أو نظـام معلومـات خـاص بالجهـة التـى يعمـل بهـا الموظـف العـام جعلتـه فعـلاً

مجرماً وإن لم يترتب عليه إتلاف أو تمليك للمعلومات الموجودة بالموقع أو غير ذلك من الأفعال التي وردت في المادة (4) من القانون، وفي هذا تشدد سببه أن الموظف العام يمكنه الدخول للموقع أو نظام المعلومات على ما في ذلك من خطورة تنبع من أهمية المعلومات التي يمكن أن تتوفر في الموقع ويكون هو مؤتمناً عليها[12].من جانبٍ آخر جاءت العقوبة في هذه المادة أشد من سابقتها فأصبحت خمس سنوات سجناً أو الغرامة أو العقوبتين معاً والسبب في ذلك ذات الأسباب آنفة الذكر.

ثانياً: المادة(6): التنصت أو التقاط أو اعتراض الرسائل:كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو العقوبتين معاً.

أركان المادة:

1. ان يقوم الجاني بالتنصت على أي رسائل أو يلتقطها أو يعترضها.
2. أن يكون هذا التنصت أو الالتقاط أو الاعتراض عن طريق شبكة المعلومات أو أجهزة الحاسوب أو ما في حكمها.
3. أن يكون هذا التنصت أو الاعتراض أو الالتقاط بدون تصريح من النيابة العامة أو الجهة المالكة للمعلومة.

حددت المادة عقوبة لهذا الفعل بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً[13].عرف القانون الالتقاط في المادة 3 بأنه يقصد به (مشاهدة البيانات أو المعلومات الواردة في أي رسالة الإلكترونية أو سماعها أو الحصول عليها). كما عرف البيانات والمعلومات وهي ما يكون محلاً للالتقاط كفعل مجرم بموجب هذه المادة بأنها (يقصد بها الأرقام والحروف والرموز وكل ما يمكن تخزينه ومعالجته وتوليده وإنتاجه ونقله بالحاسوب أو أي وسائط إلكترونية أخرى)، هذا من جانب ومن جانب آخر لم يتعرض القانون لتعريف الحاسوب الذي نص على ارتكاب الجريمة عن طريقه على عكس القانون السعودي (نظام مكافحة جرائم المعلوماتية السعودي لسنة 2006) والذي عرف الحاسب الآلي في المادة الأولى الفقرة 6 بأنه يقصد به (أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على معالجة البيانات أو تخزينها أو ارسالها أو استقبالها أو تصفحها يؤدي وظائف محددة بحسب البرنامج والأوامر المعطاة له). أما قانون مكافحة جرائم المعلوماتية الإماراتي فلم يتعرض لتعريف الحاسوب على قرار القانون السوداني.

الملاحظ أن القوانين الثلاثة المذكورة لم تقصر ارتكاب الجريمة على وسيط واحد وإنما تركت الباب مفتوحاً بالنص على إمكانية ارتكابها بأي من وسائل تقنية المعلومات وهذا اتجاه محمود فيما نرى لأن هذه الوسائط في تزايد مستمر وما أتى بالحاسب الآلي يمكن أن يأتي بغيره، ففي المادة محل الشرح يمكن تصور إلتقاط هذه الرسائل أو اعتراضها سواء وردت عن طريق البريد الإلكتروني[14] أو الهاتف السيار Mobile أو أجهزة الفاكس أو التلكس أو غيرها من الوسائط[15].

ثالثاً: المادة(7): جريمة دخول المواقع عمداً بقصد الحصول على بيانات أو معلومة أمنية:

كل من يدخل موقعاً أو نظاماً مباشرة أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها بغرض:(أ)الحصول على بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معا. (ب) إلغاء بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني أو حذفها أو تدميرها أو تغييرها يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً[16].

أركان المادة:

1. أن يدخل الجانى موقعاً أو نظاماً.
2. أن يكون هذا الدخول مباشرة أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها.
3. أن يكون هذا الدخول بغرض الحصول على بيانات تمس الأمن القومي للبلاد أو الاقتصاد الوطني أوحذفها أو تغييرها[17].

المادة(8):إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات:

كل من يدخل بأى وسيلة نظاماً أو وسائط أو شبكات المعلومات وما في حكمها ويقوم عمداً بإيقافها أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات أو مسحها أو حذفها أو إتلافها، يعاقب بالسجن مدة لا تتجاوز ست سنوات أو بالغرامة أو بالعقوبتين معاً[18].

أركان المادة:

1. أن يقوم الجاني بالدخول لنظام أو وسائط أو شبكات المعلومات أو ما في حكمها.
2. أن يقوم عمداً بإيقاف أو تعطيل أو تدمير البرامج أو البيانات أو المعلومات أو مسحها أو حذفها أو إتلافها.هذه المادة تجرم تعطيل أو تدمير البرامج أو البيانات أو المعلومات أو حذفها أو إتلافها. وتختلف عن المادة السابقة في أن هذه الأخيرة لا تشترط أن تكون المعلومات أو البيانات تمس الأمن القومي أو الاقتصاد الوطني. كما تختلف عن المادة 4 في أنها تقترب منها في وصف أركانها غير أنهما تختلفان في أن المادة 4 نصت صراحةً على أن تكون البيانات أو المعلومات ملكاً للغير ونرى دمج المادتين معاً لعدم وجود إختلاف يذكر.هذا وتقع جريمة الإتلاف في نطاق المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي وذلك بالتعدي على البرامج Loqical والبيانات data والمخزنة والمتبادلة بين الحواسيب وشبكاته الداخلية(المحلية) أو العالمية (الإنترنت). وتأخذ جريمة الإتلاف في نطاق المعلوماتية إما صورة الإتلاف المادي وذلك بالاعتداء على المكونات المادية للحاسب الآليHardware)) من أجهزة ودعامات وشرائط وأقراص ممغنطة وما تحتوى من معلومات أو الشاشات والكوابل....إلخ. أو الاعتداء على البرامج أو البيانات المخزنة في قواعد الحاسب الآلي والمتبادلة بين الحواسيب عبر قنوات الاتصال في شبكة الإنترنت سواء بمحوها أو تعديلها أو تغيير نتائجها[19].

المادة (9): إعاقة أو تشويش أو تعطيل الوصول للخدمة:

كل من يعوق أو يشوش أو يعطل عمداً وبأي وسيلة الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً.

أركان المادة:

1. أن يقوم الجاني بإعاقة أو تشويش أو تعطيل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات عمداً وبأي وسيلة.
2. أن يكون الدخول عن طريق شبكة المعلومات أو أحد أجهزة المعلومات أو ما في حكمها.

لم توضح المادة المقصود بالخدمة التى تقع بشأنها الجريمة ولكن يفهم من النص أنها الخدمة المتعلقة بمصادر البيانات والمعلومات، مثل الدخول إلى شبكة الإنترنت ويمكن أن تشمل خدمة الهاتف الجوال أو الوصول لخدمة القنوات الفضائية التلفزيونية.

رابعاً: المادة (12): الحصول على أرقام أو بيانات بطاقات الائتمان:

كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول إلى أرقام أو بيانات للبطاقات الائتمانية أو ما في حكمها بقصد ستخدامها في الحصول على بيانات الغير أو أموالها وما تتيحه تلك البيانات والأرقام من خدمات يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً.

أركان المادة:

1. أن يستخدم الجاني شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول إلى أرقام أو بيانات البطاقات الائتمانية أو ما في حكمها.
2. أن يكون ذلك بغرض الحصول على بيانات الغير أو أمواله، أو ما تتيحه تلك البيانات أو الأرقام من خدمات[20].

ووفقاً لهذه المادة فإن الجريمة المرتكبة بموجبها يمكن أن ترتكب بصورتين الصورة الأولى من قبل الشخص حامل البطاقة نفسه، وذلك بأن يتحصل عليها عن طريق تقديم بيانات مزورة عن شخصه للحصول على بطاقة الإئتمان إبتداءً شريطة أن يتم ذلك عن طريق استخدام شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها وفقاً لنص المادة، ويمكن تصور ذلك بأن يتقدم الشخص بالبيانات المزورة، عن طريق موقع البنك الإلكتروني على الشبكة العنكبوتية للحصول على البطاقة. والصورة الثانية هي استخدام شبكة المعلومات أو أحد أجهزة الحاسوب في الحصول على بيانات الغير حامل البطاقة ومن ثم استغلالها في الحصول على السلع أو الخدمات ويتم ذلك في الغالب عن طريق الولوج غير المشروع إلى حواسيب البنك والحصول على بيانات الأشخاص حاملي البطاقات ومن ثم استغلالها، والملاحظ أن الجاني يمكن أن يكون من داخل البنك نفسه كأن يكون هو الموظف المسؤول عن حفظ البيانات أو أي موظف آخر، كما يمكن أن يكونِ شخصاً جاء عرضاً

للبنك واستغل فرصة إهمال الموظف المعني بترك جهاز الحاسوب مفتوحاً أو تحصل على كلمة السر للولوج للنظام، أو قصد الحضور لذلك.

المادة:(13):الانتفاع دون وجه حق بخدمات الاتصال: كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً[21].هذه المادة تجرم الانتفاع غير المشروع بخدمات الاتصال عن طريق شبكة المعلومات أو ما في حكمها، وهذا الفعل فيما نرى يشمل الانتفاع غير المشروع بخدمات الهاتف السيار ويشمل ذلك الحصول على أرقام بطاقات شحن الهاتف السيار سواء عن طريق سرقة البطاقات نفسها وإدخال أرقامها للهاتف، أو تخمين هذه الأرقام وتدوينها وإرسالها للشركة فإذا كان التخمين صحيحاً تم إدخال القيمة تلقائياً وهو أمر صعب ولكنه ممكن الحدوث كما يمكن تصور ان يتم الحصول على الأرقام من عامل بالشركة المعنية فإذا قام ببيعها لآخرين وكانوا على علم بذلك يكونوا قد إرتكبوا هذه الجريمة ويكون هو قد ارتكب مخالفة للمادة 23 من القانون والتي جاءت تحت عنوان التحريض أو الاتفاق أو الاشتراك، كما تشمل هذه المادة الانتفاع غير المشروع بخدمات القنوات الفضائية المشفرة، فضلاً عن خدمات الإنترنت[22].

الحماية القانونية للعقود الإلكترونية في القوانين المقارنة

طرق حماية العقد الإلكتروني:

الحماية الجنائية للتوقيع الإلكتروني:

للتوقيع الإلكتروني أهمية رئيسة في التجارة الإلكترونية، فعن طريقه يتم تأكيد العقود والاتفاقيات التجارية، وتحديد هوية المرسل والمستقبل، والتأكد من صحة وصدق البيانات..إلخ ونظراً لهذه الأهمية فإن من الضروري وجود حماية جنائية للتوقيع الإلكتروني إذ إن الاعتداء عليه يعتبر اعتداءً على مضمون التجارة الإلكترونية وليس فقط على البيانات المتعلقة بها[23].

وقد قامت بعض الدول العربية بالنص على تجريم بعض الأعمال المتعلقة بالاعتداء على التوقيع الإلكتروني ووضع العقوبات المناسبة لهذه الجرائم.

ومن هذه الجرائم ما يلي:

1. الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني.
2. جريمة صنع أو حيازة برنامج لإعداد توقيع إلكتروني.
3. جريمة تزوير وتقليد المحررات الإلكترونية والتوقيع الإلكتروني[24].

الحماية الجنائية للتوقيع الإلكتروني في الفقه الإسلامي:

اهتمت الشريعة الإسلامية بحفظ الأموال، وأمرت باتخاذ الوسائل الكفيلة بحفظها، وشرَّعت العقوبات الرادعة لمن يتجرأ أو يحاول الاعتداء عليها بالتزييف أو التزوير أو غير ذلك من طرق

الاعتداء.وقد حرَّم الله عز وجل أكل الأموال بالحيل الماكرة والطرق الملتوية، قال تعالى: ﴿ وَلا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ﴾[25] وأباحت الشريعة الإسلامية للإنسان المدافعة عن ماله إذا اعتدى عليه ولو باستعمال القوة وأنَّ «من قتل دون ماله فهو شهيد»[26].وجعلت كل من تسبب في اتلاف مال متقوم بغير حق فإنه يضمنه حتى لو كان ذلك بطريق الخطأ[27]. وهذه الأحكام وغيرها تبين مدى حرص الشريعة الإسلامية على إيجاد الحماية الجنائية للأموال ذاتها وعلى وسائل حفظها أيضاً.وبما أن الاعتداء على التوقيع الإلكتروني أو محاولة القيام بذلك يترتب عليه مخاطر كبيرة على المجني عليه خاصة، وعلى التجارة الإلكترونية عامة، حيث يؤدي إلى استخدام هذا التوقيع في المعاملات والحقوق المالية مما يسبب سرقة الأموال وضياعها فإن وضع الحماية الجنائية للتوقيع الإلكتروني يتفق مع مقاصد الشريعة الإسلامية في حفظ الأموال والحقوق الخاصة وحرمة الاعتداء عليها بأي وجه كان.

والعقوبات في الشريعة الإسلامية ثلاثة أقسام:

1. الحدود: وهي العقوبات المقدرة شرعاً لحق الله تعالى، وهي حد الزنا والقذف والشرب والسرقة والحرابة والردة.
2. القصاص: وهي عقوبة مقدرة شرعاً لحق الأفراد، فمن حق المجني عليه أو ورثته أن يستوفيه أو يعفو عنه، وهو قسمان: في النفس، وفي الأطراف.
3. التعزيرات: وهي عقوبات غير مقدرة شرعاً، وإنما ترك شأنها وتقديرها إلى ولي أمر المسلمين، [29]فمن حِكَم الشارع أن جعل لولي الأمر مجالاً لينظر الجرائم التي تقع في عصره والتي تكون مخالفة لأحكام الشريعة ومقاصدها، فيضع لها العقوبات الرادعة الزاجرة مراعياً في ذلك نوع الجريمة والآثار المترتبة عليها[28].

والاعتداء على التوقيع الإلكتروني أو محاولة القيام بذلك يعتبر جريمة بحد ذاته، سواءً كان بصنع برنامج لإعداد توقيع إلكتروني بدون إذن الجهة صاحبة الصلاحية، أو تزوير وتقليد التوقيع الإلكتروني، أو الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني، أو غير ذلك من الجرائم التي تقع على التوقيع الإلكتروني.وضع عقوبة محدَّدة على هذه الجرائم هو من باب التعزير الموكول إلى ولي أمر المسلمين سواءً بنفسه أو عن طريق السلطة التنظيمية في الدولة الإسلامية التي تتولى تحديد الجرائم ووضع العقوبات المناسبة لها.إن العقد المبرم بالطريقة التقليدية يعتمد على الكتابة والتوقيع التقليديين كعامل اسناد في الاثبات، في حين ان العقد الذي يبرم عن طريق شبكة المعلوماتية يقوم على تبادل البيانات الكترونيا" على دعامات غير ورقية داخل اجهزة الاتصال أو خارجها والتوقيع عليها ممن يرسل الرسالة الإلكترونية بواسطة التوقيع الالكتروني.

الحماية القانونية في القوانين العربية:

في التجارة والمعاملات الإلكترونية تنساب البيانات والمعلومات والأموال عبر وسائط إلكترونية ومن ثم فإن أي اعتداء على هذه البيانات أو المعلومات سواء عن طريق الاستيلاء عليها أو إتلافها

أو تدميرها يمثل جريمة جنائية يتعين العقاب عليها، كذلك قد يتم السطو على أموال هذه التجارة حال انتقالها بطريقة الدفع الإلكتروني من وسيط إلى آخر ومن ثم فهي في حاجة إلى حماية جنائية وفضلاً عن ذلك فإن نصوص القانون يتعين لاحترامها أن يكون لها طابع الإلزام والإجبار ولن يتأتى ذلك إلا بتقرير عقوبات تقع على المخالف بما فيها العقوبات الجنائية متى كانت المخالفة تشكل جريمة جنائية.

أوضح في هذه الورقة العلمية: كيفية الحماية الجنائية للتجارة الإلكترونية من خلال بعض الأنظمة العربية التي تقدمت في هذا المجال كدولة تونس التي أصدرت قانونا اسمته قانون المبادلات والتجارة الإلكترونية، والإمارات العربية المتحدة التي أصدرت قانونا أسمته قانون المعاملات والتجارة الإلكترونية، والمملكة العربية السعودية تمثل نظامها في التعاملات الإلكترونية ويكون ذلك على النحو الآتي:

أولاً: الحماية الجنائية للتجارة الإلكترونية في النظام السعودي:

تعد المملكة العربية السعودية ذات ثقل دولي من الناحية السياسية بموجب موقعها من العالم ككل وبموجب موقعها الإسلامي والعربي ومن ناحية أخرى تعتبر المملكة العربية السعودية ذات ثقل اقتصادي متميز على مستوى المنطقة العربية[30]، وبعد انضمام المملكة العربية السعودية لمنظمة التجارة العالمية ولانتشار استخدام الإنترنت كان من الطبيعي تزايد التجارة الإلكترونية في البلاد هذا النوع من التجارة الذي وفر فرص الاستثمار بعيداً عن معوقات التجارة التقليدية والمتمثلة في الرسوم الجمركية ومشاكل المنافذ الجمركية والنقل وغيرها من الإجراءات التقليدية الأخرى.وقد بدأت المملكة العربية السعودية منذ عام 1996م في تحديث البنية التحتية الخاصة بقطاع الاتصالات تمهيداً للدخول بقوة إلى سوق التجارة الإلكترونية ونظراً إلى شبكة الاتصالات الحديثة والقوة الاقتصادية الهائلة التي تملكها وانخفاض نسبة الأمية وتحديث تشريعاتها التي جعلتها في مصاف الدولة المنفتحة اقتصادياً على العالم وكل ذلك ساهم في جعلها مركزاً متقدماً للمال والأعمال ومن ثم دخولها إلى التجارة الإلكترونية بقوة، ثم أصدرت المملكة العربية السعودية نظام التعاملات الإلكترونية بتاريخ 8 من شهر ربيع الأول سنة 1428هـ ويعد هذا النظام إطاراً قانونياً مهماً جداً في تعريف التعاملات الإلكترونية وإيضاح الجرائم والعقوبات الواقعة عليها وبذلك يكون هذا النظام هو الأمثل لحماية التجارة الإلكترونية في المملكة العربية السعودية من الجرائم التي تقع على هذا النوع من التجارة، ويتضمن هذا النظام واحداً وثلاثين (31) مادة تناولت المادة الأولى منها واحداً وعشرين (21) فقرة أوضحت تعريفات المصطلحات والمسميات الواردة في النظام مثل (الحاسب الآلي، الشخص، إلكتروني، التعاملات الإلكترونية، البيانات الإلكترونية، السجل الإلكتروني، التوقيع الإلكتروني، شهادة التصديق الرقمي).

كما حددت المواد (4/2) أهداف النظام في الحد من الجرائم الواقعة عن طريق التعاملات الإلكترونية ونطاق تطبيقها[31].ومن ثم أوردت المواد (5- 9) من النظام الآثار النظامية للتعاملات والسجلات والتوقيعات الإلكترونية في الفصل الثاني من النظام. وكما أوردت المواد (10- 13) من النظام عن كيفية انعقاد التعامل الإلكتروني في الفصل الثالث من النظام.

ثانياً: الحماية الجنائية للتجارة الإلكترونية في القانون التونسي:

يعد قانون المبادلات والتجارة الإلكترونية التونسي والصادر في التاسع من شهر أغسطس من عام 2000م[32]، من التشريعات العربية المبكرة والمتكاملة في شأن التجارة الإلكترونية التي لا نعلم أن تشريعاً آخر قد صدر في دولة عربية أخرى في شأن هذه التجارة غير ذلك القانون، ولقد خصص هذا القانون باباً كاملاً يتعلق بهذه الحماية الجنائية هو الباب السابع بعنوان: في المخالفات والعقوبات، والذي تضمن المواد من (43) وحتى (53) وهي كالآتي:

نص المادة (43) من القانون: وقد نصت هذه المادة على أنه " تتم معاينة المخالفات لأحكام هذا القانون من قبل أعوان الضابطة العدلية والأعوان المحلفين للوزارة المكلفة بالاتصالات والوكالة الوطنية للمصادقة الإلكترونية وأعوان المراقبة الاقتصادية وفق الشروط المنصوص عليها بالقانون رقم 64 لسنة 1991م المؤرخ في 29 يوليو المتعلق بالمنافسة والأسعار والنصوص المنقحة والمتممة له." فنجد لهذا النص أن ضبط الجرائم المشار إليها حسب أحكام هذا القانون يتم بمعرفة مأموري الضبط القضائي وأعوانهم التابعين للوزارة المشرفة على الوكالة الوطنية للمصادقة الإلكترونية وهي الوكالة المشرفة على أحكام هذا القانون وتتولى المنح أو التراخيص بمنح شهادات المصادقة الإلكترونية على التوقيع الإلكتروني وغيرها مما يستلزم إتمام عقد التجارة الإلكترونية، وحسب هذا النص فإنه تطبق أحكام القانون كذلك بمساعدة مأموري الضبط المكلفين بالمراقبة الاقتصادية حسب قانون المنافسة والأسعار الصادر برقم 1991/64 في29 يوليو 1991م، والتشريعات المكملة له[33].

ثالثاً: الحماية الجنائية للتجارة الإلكترونية في القانون الإماراتي:

تعتبر الإمارات العربية المتحدة أول دولة من دول مجلس التعاون الخليجي قامت بإصدار قانون للتجارة الإلكترونية وكان ذلك بتاريخ 12 من شهر فبراير2002م، الموافق 30 من شهر ذي القعدة 1422هـ وذلك لحماية التجارة الإلكترونية جنائياً من أي اعتداء يتم عليها، ونقلاً عن ذلك فإن نصوص القانون يتعين لاحترامها أن يكون لها طابع الإلزام والإجبار ولن يتأتى ذلك إلا بتقرير عقوبات تقع على المخالف بما فيها العقوبات الجنائية متى كانت المخالفة تشكل جريمة جنائية ولقد وردت الجرائم والعقوبات الجنائية في هذا القانون ضمن أحكام الفصل السابع في المواد (28 -35) منه، ولم تتعلق المواد كلها بتقرير ما يعد جريمة والعقوبة الجنائية المقررة لها وإنما أشير إلى بعض الأحكام العامة ذات العلاقة بالجريمة الجنائية من ذلك خطر نشر شهادة التصديق الخاصة بالتوقيع الإلكتروني أو بيانات التجارة الإلكترونية ونسبتها إلى مزود خدمة أو موقع بالمخالفة للحقيقة، وفضلاً عن ذلك فقد نصت المادة (34) من القانون على المصادرة كعقوبة ثانوية يقضي بها في حالة الإدانة وذلك بالنسبة للأدوات التي استعملت في ارتكاب الجريمة.

أوضح فيما يلي مضمون هذه النصوص:

أولا: نص المادة (28) من القانون[34]: «لا يجوز لأي شخص أن ينشر شهادة تشير إلى مزود خدمات تصديق مدرج اسمه في الشهادة إذا كان الشخص يعرف أن:

1. مزود خدمات التصديق المدرج اسمه في الشهادة لم يصدر الشهادة.
2. الموقع المدرج اسمه في الشهادة لم يقبل الشهادة.
3. الشهادة قد ألغيت أو أوقفت إلا إذا كان ذلك النشر بغرض التحقق من توقيع إلكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء، فنجد في هذه المادة إذا ما توافرت الجريمة بركنيها المادي والمعنوي تعين معاقبة الجاني وهو الأمر الذي لم ينص عليه في المادة (28) من هذا القانون لكنه يبدو أن المشرع قد احتكم في العقاب على هذه الجريمة إلى نصي المادتين (29، 32) من هذا القانون وترك تقدير ذلك لمحكمة الموضوع.

رابعا: نص المادة (31) من القانون: نصت الفقرة (1) من هذه المادة

"يعاقب كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الإطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية أو أنشئ متعمداً أياً من هذه المعلومات بالحبس وبغرامة لا تجاوز (100000) درهم أو بإحدى هاتين العقوبتين وتكون العقوبة الغرامة التي تجاوز (100000) درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات. "فوفق هذا النص فإنه يجرم الحالة التي يقوم فيها أي شخص استطاع لسبب منصوص عليه في هذا القانون أن يطلع على معلومات مدونة في السجلات أو المراسلات أو المستندات الإلكترونية على التفصيل السابق ثم يقوم بإفشائها متعمداً أو يتسبب بإهماله في إفشاء هذه المعلومات[35].

خامساً: نص المادة (32) من القانون:

مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون يعاقب كل من ارتكب فعلاً يشكل جريمة بموجب التشريعات النافذة باستخدام وسيلة إلكترونية بالحبس لمدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز(100000) درهم أو بإحدى هاتين العقوبتين ويعاقب الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذه المادة. فوفق هذا النص فالجاني يرتكب أية جريمة سواء كانت مخالفة لهذا القانون أو أي قانون آخر بوسيلة إلكترونية ولذلك فالمشرع حدد وسيلة ارتكاب الجريمة وهي وسيلة إلكترونية دون أن يحدد مضمون الفعل أو السلوك الإجرامي الذي ورد عاماً وهو أمر غير مرغوب عند التشريع في النطاق الجنائي وذلك احتراماً لمبدأ شرعية الجريمة والعقوبة والذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص وهو ما يقتضي تحديد طبيعة ذلك السلوك الإجرامي.

رابعاً: الحماية الجنائية للتجارة الإلكترونية في التشريع المصري:

(أ): أهم ملامح الحماية الجنائية في المشروع:

1. عاقب المشروع كل من يقوم بكشف مفاتيح التشفير المودع بمكتب التشفير ، أو بفض معلومات مشفرة في غير الأحوال المصرح بها قانوناً وذلك بالحبس الذي لا تقل مدته عن سنة والغرامة التي لا تقل عن ثلاثة آلاف جنيه ولا تزيد عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين وفي حالة العود من قبل الجاني لهذه الجريمة تكون عقوبة الحبس في حدها الأدنى عامين والغرامة ما بين عشرة آلاف وخمسين ألف جنيه دون تخيير بين العقوبتين لحكمة الموضوع.
2. عاقب المشروع كذلك كل من استخدم توقيعاً إلكترونياً أو محاه أو عدل فيه أو في مادة المحرر الإلكتروني دون موافقة كتابية مسبقة من صاحب الحق وذلك بالحبس الذي لا تقل مدته عن ثلاثة أشهر والغرامة التي لا تقل عن ألف جنيه ولا تزيد عن ألفين جنيه أو بإحدى هاتين العقوبتين[36]. وفي حالة العود تكون العقوبة المقدرة الحبس الذي لا تقل مدته عن ثلاثة أشهر والغرامة ما بين ألفي جنيه وخمسة آلاف جنيه وذلك دون تخيير لحكمه الموضوع ما بين الحبس والغرامة.
3. وفي جميع الأحوال تتم مصادرة الأجهزة والأنظمة والبرامج المستخدمة في ارتكاب الجرائم المشار إليها، والتي تحصلت عنها، كما يحكم على الجاني بغرامة تساوى ضعف ما عاد عليه من ربح أو فائدة بسبب هذه الجريمة.

(ب) استعراض نصوص الحماية الجنائية في المشروع:

المادة (26) من المشروع:

قد نصت على أنه: «مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر يعاقب بالحبس وبغرامة لا تقل عن ثلاثة آلاف جنيه أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة بيانات أو قاعدة تتعلق بالتوقيعات الإلكترونية، ويعاقب بنفس العقوبة من اتصل وأبقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة، وهذا النص يعاقب بالحبس والغرامة، أو بأي من هاتين العقوبتين كل من استعمل الغش المعلوماتي أو الاحتيال في الدخول على نظام معلوماتي، يتعلق بالتجارة الإلكترونية. أو قاعدة بيانات تتعلق بهذه التجارة، وكذلك قواعد البيانات والمعلومات والتى تتعلق بالتجارة الإلكترونية، وذلك لأن التوقيع الإلكتروني هو أمر لازم في التجارة الإلكترونية ويساهم في حمايتها.

المادة: (27) من المشروع:

وقد نصت هذه المادة على أنه: «يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز أو حصل على نظام معلومات أو برنامج لإعداد توقيع إلكتروني دون موافقة صاحب الشأن. وهذا النص يواجه حالة قيام أحد الأشخاص بصنع أو حيازة نظام معلوماتي أو برنامج لإعداد توقيع إلكتروني أو الحصول عليه دون موافقة صاحب الشأن.والفرض في هذه الحالة أن الجاني غير مأذون له من قبل صاحب الشأن في الصنع والحيازة والحصول على ذلك البرنامج.

من ناحية أخرى يفترض أن الشخص الذي قام بالصناعة أو الحيازة **أو** الحصول ليس مأذوناً من الناحية القانونية في القيام بهذا العمل، كما لو صدر له إذن من السلطات القضائية المختصة في القيام بالفعل الذي يعد جريمة، وفي هذه الحالة لا يعاقب بوصف أنه قد توافر في حقه سبب من أسباب الإباحة، كذلك تتعين الإشارة إلى أن تجريم مثل هذه الأفعال يساعد على الحماية الجنائية لهذه التجارة لأنها كما أسلفنا، نظام معلوماتي يعتمد أولاً وأخيراً على تدفق المعلومات عبر وسائط إلكترونية بالنسبة للعقد في مراحله المختلفة حتى القيام بالخدمة أو تسليم السلعة محل العقد، كما أن التجارة الإلكترونية تعتمد التوقيع الإلكتروني " بديلاً للتوقيع التقليدي في إبرام عقود هذه التجارة أو في عمل التحويلات النقدية الخاصة بمقابل الوفاء في هذه التجارة، ومن هنا تأتي أهمية النص المذكور في حالة إقراره، كوسيلة لحماية أموال التجارة الإلكترونية ونظامها.

المادة (28) من المشروع:

قد نصت على أنه « مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس مع الشغل كل من زّور أو قلد محرراً أو توقيعاً إلكترونياً أو شهادة اعتماد توقيع إلكتروني. ويعاقب بذات العقوبة المقررة كل من استعمل محرراً أو توقيعاً إلكترونيا مزوراً أو شهادة مزورة باعتماد توقيع إلكتروني مع علمه بذلك»[37].

هذا النص يواجه حالة تقليد أو تزوير المحرر الإلكتروني أو التوقيع الإلكتروني. وكذلك استعمالها مع العلم بالتزوير بالإضافة إلى استعمال شهادة مزورة في شان توقيع إلكتروني.

" وقد عرف الشروع التوقيع الإلكتروني بأنه: حروف أرقام أو رموز أو أشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره».

كما عرف المشروع المحرر الإلكتروني أنه: «كل بيان يتم تدوينه أو تخزينه أو نقله من خلال وسيط إلكتروني، وبذلك يكون المشرع قد أورد حماية جنائية لواجهة جريمة تقليدية هي تقليد أو تزوير المحرر أو التوقيع، ولأن المحرر هنا ليس تقليداً، وكذلك التوقيع فكليهما يتم بطريقة إلكترونية فقد ثارت مشكلات عديدة بخصوص مدى الاعتراف بتزوير أي منهما أو حمايتهما حسب نصوص التزوير في قانون العقوبات التقليدي[38].

نص المادتين (29، 30) من المشروع:

تنص المادة «29» على أنه: (مع عدم الإخلال بأية عقوبة أخرى أشد يعاقب بالحبس مع الشغل كل من استخدم نظام أو برنامج للحيلولة دون إتمام المعاملات التجارية بالوسائل الإلكترونية، وذلك بالتعديل فيها أو محتوياتها أو إفسادها أو تدميرها» وذلك بتعطيل أنظمتها).

تنص المادة (30)، من ذات القانون على أنه: « مع عدم الإخلال بأية عقوبة أشد، يعاقب بالحبس كل من أذاع أو سهل أو استعمل ولو في غير علانية محرراً أو توقيعاً إلكترونياً أو فض شفرته دون مسوغ قانوني أو دون موافقة صاحب الشأن، وتكون العقوبة، الحبس مدة لا تقل عن سنتين إذا كان مرتكب الأفعال المشار إليها بالفقرة الأولى من كان أميناً على المحرر أو التوقيع الإلكتروني بمقتضى صناعته أو وظيفته أو كان من العاملين لديه. وهاتان المادتان في المشروع المصري، تواجهان

مسألتين مهمتين في شأن التجارة الإلكترونية على الخصوص وفي شأن نظم المعلومات عموماً، ألا وهما تأمين المعلومات أولاً ثم تأمين نقل المعلومات والبيانات فيما يسمى بأمن الاتصالات[39].

فالمادة (29) من المشروع، تعاقب كل من استعمل نظاما أو برنامجاً معلوماتياً لإفساد إتمام الصفقات التجارية إليكترونية بالطبع وذلك بوسيلة إليكترونية، وذلك بتعديل هذه المعاملة أو محو بياناتها أو إفساد هذه البيانات أو تدميرها أو تعطيل نظمها، ولعل هذا النص يثير مسألة تأمين معلومات هذه التجارة ضد الاختراق، وذلك لأن الجريمة المعلوماتية في تقدم يكاد يسبق التنظيم التشريعي لتكنولوجيا المعلومات وتجريم الاعتداء عليها، لذلك حاول المشرع حصر صور الاعتداء على نظام اتمام صفقات التجارة الإلكترونية، والذي يكون بتعديل بيانات هذه المعاملات أو محو بياناتها أو إفسادها أو تدميرها أو تعطيل نظمها عن العمل.

نص المادة (31) من المشروع:

وقد نصت هذه المادة على أنه «مع عدم الإخلال بأية عقوبة أخرى أشد يعاقب بالحبس مع الشغل كل من أدخل بعمد أو إهمال فيروس إلى نظام معلوماتي بدون مرافقة مالك النظام أو حائزه الشرعي، وهذا النص يواجه حالة تدمير نظام التجارة الإلكترونية أو أي نظام معلوماتى عن طريق الفيروس ، سواء كان ذلك عمداً أو بطريق إهمال، ذلك أن الفيروس المعلوماتي قد يؤدى إلى تحريف المعلومات الموجودة بالنظام أو تحريفها وتعييبها أو حذفها أو محوها تماماً. ولذلك يرى الفقه الجنائي أن إتلاف البرامج أو المعلومات معلوماتياً قد يكون عن طريق محو المعلومات وتدميرها كلياً بطريقة إلكترونية وتشويه المعلومات والبرنامج على نحو يؤدى لإتلافه ومن تم يجعله غير صالح للاستعمال، والحقيقة أن تجريم تدمير النظم المعلوماتية عن طريق الفيروس هو أمر يؤدى إلى حماية التجارة الإلكترونية، لأنه كما سبق القول أن هذه التجارة عبارة عن نظام معلوماتي سواء في مرحلة المفاوضات أو إبرام العقد أو تنفيذه وكذلك الوفاء بقيمة عقد التجارة الإلكترونية، ولذلك فتجريم إدخال الفيروس عمدا أو بطريق إهمال إلى هذا النظام يؤدى إلى حماية هذه التجارة.

نص المادة (32) من المشروع:على أنه: «يحكم في جميع الأحوال بمصادرة الأجهزة والأنظمة والبرامج المستخدمة في ارتكاب الجرائم المشار إليها سالفاً والتي تحصلت عنها.كما يحكم عليه بغرامة ضعف ما عاد عليه من ربح أو فائدة من جرائم ما ارتكبه. ووفقاً لهذا النص فإن الأجهزة والأنظمة والبرامج التي استخدمت في ارتكاب الجرائم السابقة يقضى بمصادرتها وفي كل ألأحوال فهي أجهزة وأدوات مادية لها علاقة بالمعلوماتية منها أجهزة الحاسب الآلي وملحقاتها من شاشات عرض وماسحات ضوئية، وغيرها من البرامج التي تتعلق بتشغيل أجهزة الحاسب الآلي وتطبيقاتها، سواء كانت تتعلق مثلا بالتوقيع الإلكتروني أو تشفير أو ترميز البيانات التي تتعلق بالتجارة الإلكترونية، من ناحية أخرى وبالإضافة للمصادرة يحكم ضد الجاني بغرامه مضاعفة لما حصل عليه الجاني من ربح أو فائدة من الجريمة المعلوماتية[40].

موقف الأنظمة القانونية المعاصرة من الجرائم المعلوماتية

بعدالتقدم العلمي والتكنولوجي في مجال المعلوماتية، وانتشار المعالجة الآلية للمعلومات واتساع نطاق التجريم المعلوماتي، وتدخله في كافة نواحي الحياة الادارية والاقتصادية والسياسية والاجتماعية والحياة الشخصية والحريات الفردية وأمن المواطنين وأسرارهم ونظر اًلحداثة الجرائم المعلوماتية وتطورها السريع وسهولة ارتكابها وادراكاً لخطورتها وآثارها السلبية على الأشخاص والأموال، دفع ذلك الحكومات والمنظمات الدولية للتدخل لحماية المجتمع من هذه الظاهرة الإجرامية المستحدثة وذلك بوضع قواعد قانونية جديدة لمكافحة الاجرام المعلوماتي، لذا سنحاول ان نبين موقف الأنظم القانونية المعاصرة من ظاهرة الإجرام المعلوماتي من خلال الآتي:

أولاً: موقف النظام اللاتيني من الجرائم المعلوماتية:

يقتضي البحث في هذا المطلب بيان موقف بعض التشريعات اللاتينية التي تصدت للجريمة المعلوماتية على النحو الآتي:

في فرنسا تتعدد القواعد التشريعية التي تخضع لها الجريمة المعلوماتية في القانون الفرنسي، فهذا النمط من الجرائم تحكمه قواعد قانونية اعلى قيمة من القواعد القانونية في القانون الفرنسي تتمثل بقواعد القانون الأوربي[41] بالوقت الذي عالج فيه قانون العقوبات الفرنسي الجديد رقم 33692 الصادرفي 16 / ديسمبر1992م الجرائم المعلوماتية بنصوص مستقلة في الفصل الثاني، وفي ثلاثة محاور الأول يهدف إلى حماية نظم المعلوماتية ذاتها[42]، اما المحور الثاني فيتضمن حماية الوثائق من التزوير[43]، في حين تضمن المحور الثالث الردع وتغليظ العقاب بهدف الحيلولة دون الإقدام على هذه الجرائم.

في اليونان أضاف المشرع إلى قانون العقوبات الصادر عام 1950، المادة (370) والتي تجرم الدخول غير المشروع للمعلومات والبيانات.

في المكسيك أضيف إلى قانون العقوبات البند رقم (2) قسم 211 ويتعلق بالدخول المحظور إلى الكمبيوتر الخاص. كما أضيفت البنود (3،4،5) قسم211 والتي تتعلق بالدخول المحظور للحاسبات في حكومة المكسيك أو أنظمة الأموال المكسيكية، أما البند رقم (7) قسم 211 فقد خصص للعقوبات.، في النمسا صدر تنظيم خاص للمعلومات في عام 2000 تضمنه القسم العاشر من قانون العقوبات في المادة (52) من هذا القانون.

في جمهورية التشيك طبقت قواعد القانون الجنائي القائم على الجرائم المعلوماتية في المواد (182،249، 257 أ)، في فنلندا أضاف المشرع إلى قانون العقوبات الفصل (38) الذي يجرم افعال الاعتداء على البيانات والمعلومات.في استونيا اضاف المشرع إلى قانون العقوبات بعض النصوص منها (م269)التي تعاقب على تدمير برامج وبيانات الكمبيوتر، والمادة (270) التي تجرم افعال تخريب الكمبيوتر، والمادة (271) التي تعاقب على اساءة استعمال أجهزة الحاسوب، والمادة (273) التي تحظر نشر فيروسات الكمبيوتر.في اليابان صدر قانون حظر الدخول للكمبيوتر رقم (128) والذي بدأ تنفيذه في 3 فبراير2000م حيث جرم في المادة (3) أي فعل للدخول المحظور في الكمبيوتراما

المادة (4) فقد جرمت أي فعل من شأنه تسهيل الدخول المحظور للكمبيوتر . اما المادة (8،9) فقد تضمنت العقوبات.في قانون العقوبات المجري اضيف القسم رقم (300ج) وسمي بالغش أو الاحتيال المتعلق ببرامج الكمبيوتر.

ثانياً: موقف النظام الأنجلوأمريكي من الجرائم المعلوماتية:

سوف نشير إلى موقف النظام الانجلوأمريكي[44] من الجرائم المعلوماتية من خلال بعض النظم القانونية والتشريعات التي صدرت في بعض الدول التي تطبق هذا النظام والمتمثلة في :

المملكة المتحدة حيث لا توجد تشريعات مكتوبة تعالج ظاهرة الجرائم المعلوماتية، وذلك بسبب كون النظام القانوني الإنجليزي يعتمد على السوابق القضائية، غير أنه في عام 1990صدر في المملكة المتحدة قانون تحت مسمى قانون إساءة استخدام الكمبيوتر تناول المسؤولية الجنائية الناشئة عن الجرائم المعلوماتية في القسم الثامن عشر من خلال ثلاثة بنود، تضمن البند الأول الدخول المحظور على مواد الكمبيوتر، وتناول الثاني الدخول المحظور بقصد التسهيل والتحريض على الجرائم، واحتوى الثالث على جرائم حظر تبديل أو تحويل مواد الكمبيوتر[45].

في الولايات المتحدة الأمريكية صدرت عدة قوانين وتشريعات خاصة للتصدي لبعض الجرائم، المعلوماتية ومن أهمها قانون تقرير الأشخاص الصادرعام1970، وقانون الخصوصية الصادر عام1974م وقانون الخصوصية والحقوق الأسرية والتعليمية الصادرعام 1974م، وقانون حرية المعلومات الصادرعام 1976، وقانون حماية السرقة لعام1980م، وقانون سياسة الاتصالات السلكية واللاسلكية لعام1984م والذي يستهدف حماية خصوصية المشتركين في الخدمة التليفونية عبرالإنترنت. أماقانون العقوبات الأمريكي فقد كان من أسبق التشريعات التي تعرضت للجرائم المعلوماتية. ويمكن القول أن الولايات المتحدة الأمريكية قد استكملت بنيتها التشريعية مع نهايةالقرن العشرين في شأن التشريعات التي تحكم المعاملات الإلكترونية وتواجه الجريمة المعلوماتية سواء في تشريعاتها المحلية على مستوى الولايات أم الاتحادية على مستوى الدولة الفيدرالية، ولعل أحدث هذه التشريعات هو قانون التوقيع الإلكتروني الصادر عام2000م[46].في الهند وضع تشريع لتكنولوجيا المعلومات برقم (21) لسنة 2000م وتموضعه في الباب الأول من قانون العقوبات تضمنته المادة (66) وسمى القرصنة على نظام الكمبيوتر.في النرويج تضمن قانون العقوبات مواد جديدة هي المادة (145) وتعاقب على الدخول المحظور للوثائق، والمادة (151) وتعاقب على تدمير البيانات والمعلومات، والتي تتعرض لعدة نواح منها تخزين أو تدمير أو تحطيم النظام المعلوماتي، في البرتغال صدر قانون المعلومات الجنائي في 17 آب عام1991م وتضمن في القسم الأول المادة السابعة المتعلقة بالجرائم المعلوماتية، وفي بولندا أضيفت إلى قانون العقوبات المواد (267، 268، 269) وجميعها تتعلق بحظر الدخول للأنظمة وإساءة استخدام البيانات والمعلومات.في ايرلندا صدرتشريع الإتلاف الجنائي عام1991م وقد تموضع في القسم الخامس حيث عاقب الشخص المسموح له بالدخول للحاسب من التلاعب في البيانات والمعلومات.في أستراليا صد تشريع الجرائم الاتحادي عام 2001م والذي تضمن تعديل قانون العقوبات الصادر عام1995 م وذلك باستبدال الجزء المتعلق بجرائم الكمبيوتر من

خلال المادة (478/أ) حيث حظرت الدخول وتبديل المعلومات في أيسلندا أضاف المشرع إلى قانون العقوبات في القسم الأول المادة (228) وقد نصت فيها على أن العقاب المناسب سيحكم به على أي شخص يتناول أي طريقة للدخول إلى البيانات أو البرامج المعدة للبيانات. في سنغافورة وضع الباب رقم (50/أ) المتعلق بإساءة استخدام الكمبيوتر تحت مسمى الدخول المحظور لمواد الكمبيوتر. في تركيا عدل قانون العقوبات في القسم رقم (525/أ) المتعلق بالدخول المحظور إلى برامج وقواعد البيانات.أما في جنوب إفريقيا فلم يصدر تشريع خاص بالجرائم المعلوماتية وإنما اكتفى بتطبيق الباب الثاني الخاص بالجرائم على الجرائم المعلوماتية. كذلك الحال في أسبانيا لم يصدر تشريع خاص بالجرائم المعلوماتية وإنما طبق الباب الأول من قانون العقوبات على الجرائم المعلوماتية.

خاتمة: تم بحمد الله وتوفيقه إنجاز هذه الورقة العلمية أتمنى أن تكون مفيدة لجميع المتعاملين مع تقنية المعلومات الإلكترونية وقد بذلت جهدي في دراسة القوانين المتعلقة بالتعاملات الإلكترونية مع المقارنة ببعض الأنظمة العربية والأجنبية فقد توصلت إلى نتائج وتوصيات وهي:

أولاً: النتائج:

1. إن مسألة تحديد مكان انعقاد العقد الإلكتروني فيما يرى الباحث مسألة في غاية التعقيد وذلك لمساهمة جهات عديدة في تكوينه لتفرق أماكن وجودها بين دول مختلفة.
2. إن التجارة الإلكترونية تشمل جميع الأنشطة التجارية مثل الخدمات، التراخيص، والخدمات المصرفية والخدمات الاستشارية.
3. للتجارة الإلكترونية عدة تحديات تواجهها على نحو يتسبب في إعاقة تطورها كالتحديات القانونية واتجاهات النظم والقضاء لمواجهة منازعاتها.
4. أي اعتداء على البيانات أو المعلومات سواء عن طريق الاستيلاء عليها أو إتلافها أو تدميرها يمثل جريمة جنائية يتعين العقاب عليها.
5. حماية المستهلك هي الأساس في أي عملية تعاقدية بوصفه الطرف الضعيف أمام شركات الإنتاج والخدمات.
6. إن عقود التجارة الإلكترونية تتم في الغالب بين أطراف في أماكن مختلفة أما في دولة واحدة أو دول متعددة لذا تختلف الأنظمة الدولية في الاختصاص القضائي لقضايا التجارة والعقد الإلكتروني.
7. الجريمة المعلوماتية هي الفعل أو الامتناع المعاقب عليه وفقاً للقانون والمتعلق باستخدام نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والأنشطة المتعلقة بإستخدامها.
8. إن تجريم تدمير النظم المعلوماتية يعتبر حماية للتجارة الإلكترونية سواء في مرحلة المفاوضات أو إبرام العقد الإلكتروني أو تنفيذه.
9. التوقيع الإلكتروني هو بيانات إلكترونية مدرجة في رسالة بيانات أو مضاف إليها ويستخدم لتعيين هوية الموّقع لرسالة البيانات ويكون دليل للإثبات في حالة قيام نزاع مستقبلي بين الأطراف.

10. إن التشفير من وسائل حفظ وسرية المعلومات وتطبيقاتها للتجارة الإلكترونية وهو يعتبر مضمون الرسالة باستخدام برنامج معين يسمى مفتاح التشفير.
11. للتعاملات الإلكترونية أهمية قصوى في التأكد من مضمونها ومدى سلامتها وخلوها من الاحتيال والغش.
12. إن جرائم الحاسب الآلي جرائم ماسة بالكيانات الاعتبارية والأفراد مما يسبب خسائر مادية ومعنوية فادحة.

ثانياً: التوصيات:

1. ضرورة تعزيز طرق الحماية للعقود الإلكترونية لتوفير أكبر قدر من ثقة المتعاملين في البيئة الإلكترونية، ما يخفف من نظرة الخوف والتوجس التي تدمغ بها المعاملات الإلكترونية.
2. إدخال تعديل على قانون المعاملات الإلكترونية السوداني لسنة 2007م يحدد مكان إبرام العقد وفقاً لما أخذ به قانون الأونسترال النموذجي باعتبار مكان إنعقاد العقد الإلكتروني هو مكان مقر أعمال المرسل أو المرسل إليه رسالة البيانات أو المكان الأوثق صلة بالرابطة العقدية أو مقر العمل الرئيسي في حالة عدم وجود هذه الرابطة.
3. إستيعاب قوانين التجارة الإلكترونية لمسائل الوفاء والإثبات والتنفيذ لمواجهة التحديات التي تعيق تطور التجارة الإلكترونية.
4. ضرورة تنقية القوانين القائمة أو إصدار قوانين جديدة لمعالجة ظاهرة الإجرام المعلوماتي مثل السرقة المعلوماتية للبرامج والاستخدام غيرالمشروع للحاسب الآلي وذلك للحماية المادية والمعنوية.
5. ضرورة تضافر الجهود المحلية والدولية لرفع الوعي لدى جمهور المستهلكين بصور وطرق الاحتيال الإلكتروني لتفشي هذه الظاهرة في الآونة الأخيرة.
6. ضرورة تدريب القائمين على أمر المعلوماتية مع تبادل الخبرات داخلياً وخارجياً لضمان أكبر قدر من تطبيق قواعد الحماية الإلكترونية.
7. سن تشريعات تعمل على وجوب اتباع تقنية التشفير الإلكتروني لحماية العقود الإلكترونية ومعاقبة من يقوم بفض مفاتيح التشفير الإلكترونية دون سبب مشروع.
8. تكملة مظلة التشريعات العقابية الخاصة بالجريمة المعلوماتية فإن ذلك سيؤدي حتماً لحماية العقود الإلكترونية وزيادة الثقة فيها والإقبال عليها ومن ثم نموها وتطورها كما هو الحال في البلدان المتقدمة معلوماتياً.

المصادر والمراجع

(1) سورة المائدة، الآية (8)

(2) المعجم الوجيز، باب جيم، إصدار مجمع اللغة العربية، جمهورية مصر العربية، 2004م، ص 101

(3) القانون الجنائي السوداني لسنة1991م في م (3) ف (7)

(4) د. إبراهيم قسم السيد، شرح قانون جرائم المعلوماتية السوداني لسنة 2007 مقارناً بالقانون السعودي والاماراتي، ص 1

(5) د. إبراهيم قسم السيد، شرح قانون جرائم المعلوماتية السوداني لسنة 2007 المرجع السابق، ص 1

(6) سامي على حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، 2007م، ص 35

(7) سامي على حامد، الجريمة المعلوماتية، مرجع سابق، ص 24

(8) د. يس عمر يوسف، النظرية العامة للقانون الجنائي السوداني 1991م، الدار الجامعية، الطبعة الثانية، 1996م، ص 76

(9) د. يس عمر يوسف، المرجع السابق، ص 77

(10) منير الجنبيهي وممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، 2005م، ص16

(11) منير الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص17

(12) منير الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص18

(13) تقابل المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودى والذي نص في المادة الثالثة على الاتى:- يعاقب بالسجن مدة لاتزيد على سنة وبغرامة لاتزيد على خمسمائة الف دينار أو باحدى العقوبتين ، كل شخص يرتكب ايا من جرائم المعلوماتية الاتية: -1 التصنت على ماهو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الالى دون مسوغ نظامى صحيح – أو إلتقاطة أو إعتراضه وتقابل كذلك المادة 8 من القانون الاتحادى رقم 2 لسنة 2006م في شأن مكافحةجرائم تقنية المعلومات لدولة الامارات العربية المتحدة والذي نص على الاتى:- كل من تصنت أو إلتقط أو إعترض عمداً بدون وجه حق ماهو مرسل عن طريق الشبكة

المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

(14) البريد الالكترونى هو نظام لتبادل الرسائل بين مستخدمى الانترنت ويرمز له ب e. mail ويمتاز بكلفته المخفضة وسرعته الكبيرة إذ تصل الرسالة لوجهتها خلال ثوانى ومن ميزاته الهامة إمكانية إرفاق ملفات الرسائل ويمكن ان تحتوى الرسائل على صور أوثائق أو برامج ويتسلم المرسل إليه رسائله الالكترونية عندما يتصل بالانترنت ويفحص محتويات صندوق بريده.

(15) مقال المستشار معاوية عيسى جرائم الانترنت في السودان مجلة العدل ،وزارة العدل جمهورية السودان العدد التاسع ،2003 ، ص 165

(16) تعادل المادة السابعة (2) من نظام مكافحة جرائم المعلوماتية السعودى 2006م والتى تنص على (يعاقب بالسجن مدة لاتزيد على عشر سنوات وبغرامة لاتزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب اياً من الجرائم العلوماتية الاتية: الدخول غير المشروع إلى موقع إلكترونى أو نظام معلومات مباشرة أو عن طريق الشبكة المعلوماتية أو احد أجهزة الحاسب الالى للحصول على بيانات تمس الامن الداخلى أو الخارجي أو الإقتصاد الوطنى كما. تقابل المادة (2) من قانون مكافحة جرائم المعلوماتية الإمارات والتى تنص على: يعاقب بالسجن كل من دخل وبغير وجه حق موقعا أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك. فاذا ترتب على الدخول إلغاء كل البيانات والمعلومات أو إتلاف أو تدميرها أو نشرها تكون العقوبة السجن مدة لاتقل على خمس سنوات.

(17) ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية الاخرى والتجارية والاقتصادية. والملاحظ ان القانون السعودى على غرار القانون السودانى تحدث عن مساس الفعل بالامن الوطنى والاقتصاد الوطنى في حين خلا القانون الاماراتى من ذلك . كما ان القانون الاماراتى جعل عقوبة السجن إلزامية في حالة أن يترتب على الدخول غير المشروع إلغاء أو تدمير البيانات أو نشرها أو إتلافها.

(18) تقابل المادة الخامسة نظام مكافحة جرائم المعلوماتية السعودي والتى تنص على:-

يعاقب بالسجن مدة لا تزيد عن اربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من جرائم المعلوماتية الاتية:-

1- الدخول غير المشروع لالغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها

2- إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها.

3- إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت. كما تقابل المادة 4،5 من القانون الإماراتي هذا ونشير إلى أن جريمة التشويش أو إعاقة الوصول للخدمة أفرد لها المشروع السوداني مادة منفصلة هى المادة 9 من القانون.

(19) المحامى محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الاولى ،2007م ،ص 216 ،217

(20) تقابل المادة المادة الرابعة 11من القانون الإماراتي والتي جرمت الوصول دون مسوغ قانوني الي بيانات البنوك أو الائتمان أو ملكية الاوراق المالية بغرض الوصول الي بيانات أو معلومات أو أموال أو خدمات تترتب علي هذه المعلومات، في حين ان القانون السعودي لم يفرد مادة خاصة بتجريم إساءة استخدام البطاقات الممغنطة وجرم الوصول غير المشروع للبيانات البنكية.

(21) هذه المادة لا يوجد لها مقابل في القانونين السعودي والإماراتي

(22) ظهرت في الأسواق مايعرف بأجهزة (الديجتال كاسر الشفرة) وهو مصطلح يعني إمكانية الدخول الي ومشاهدة القنوات الفضائية المشفرة بدون دفع الرسوم المقررة من قبل القنوات مقدمة الخدمة، وهي غالباً قنوات رياضية أو قنوات أفلام.

(23) د. عبد الفتاح حجازي، التجارة الإلكترونية وحمايتها القانونية، ج 2، ص 294.

(24) مشروع التجارة الالكترونية في المصر، المواد 26و27و28

(25) سورة البقرة، الآية 188

(26) صحيح الترغيب والترهيب رقم الحديث «1411" ، أنظر د. عبد الفتاح حجازي النظام القانوني لحماية التجارة الالكترونية 2/296-304.

(27) محمد عقله، الإسلام مقاصده وخصائصه في حفظ المال وأهميته، –ص 209-224.

(28) علاء الدين، أبو بكر بن مسعود بن أحمد الكاساني الحنفي، بدائع الصنائع في ترتيب الشرائع، دار الكتب العلمية 1986م، ج7، ص 63.

(29) عبد القادر عودة ، التشريع الجنائي الإسلامي –129/10.

(30) خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، رسالة ماجستير منشورة، جامعة نايف للعلوم الأمنية، 2009م، ص 134

(31) خالد بن عبد الله بن معيض العبيدي، المرجع السابق، ص 135

(32) د هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، القاهرة، دار النهضة العربية، ص 120

(33) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، الإسكندرية، دار الفكر الجامعي، 2006م، ص 689.

(34) وائل أنور بندق، موسوعة القانون الإلكتروني وتكنولوجيا الاتصالات، الإسكندرية، دار المطبوعات الجامعية، 2007م، ص 493

(35) د.عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، مرجع ص272

(36) د. هدى حامد قشقوش، الرجع السابق ، ص 98

(37) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص373

(38) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص373

(39) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص374

(40) عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، مرجع سابق، ص380

(41) صادقت فرنسا على الاتفاقية التي اعدها مجلس اوربا والخاصة بالجرائم المعلوماتية بعد اقرار البرلمان الفرنسي لها بالقانون رقم (89) الصادر في اكتوبر1982م وقد طبق هذا القانون بعد نشره في الجريدة الرسمية بتاريخ 2نوفمبر 1985.كما تعتبر فرنسا عضو في منظمة التجارة العالمية منذ عام1995و بذلك تكون احكام هذه الاتفاقية ملزمة للقانون الفرنسي بل وأعلى قيمة منها ستنادا للمادة (55) من الدستورالفرنسي

(42) يتضمن هذا المحور ثلاثة انواع من الجرائم هي الدخول أو البقاء غير المشروع داخل نظام المعلوماتية والاعتداء على سير نظام المعلوماتية وادخال معلومات بصورة غير شروعة في نظام المعلوماتية، وإتلاف المعلومات الموجودة وقد عالجتها المادة (463،ف 4،3،2).

(43) يتضمن هذا المحور جريمتين هما: تزوير الوثائق المعالجة معلوماتياً واستخدام الوثائق المعالجة معلوماتياً المزورة وقدعالجتها(م462 / ف5).

(44) يرجع أساس هذا النظام إلى القانون الانجليزي القديم الذي انتقل إلى امريكا الشمالية نتيجة غزو انجلترا لها في القرن السابع عشر. وهذا النظام يجعل للسوابق القضائية دوراً مهماً في مجال التجريم والعقاب ولا يقتصر تطبيق هذاالنظام على انجلترا والولايات المتحدة الأمريكية وإنما يمتد لتشمل استراليا والهند والبرتغال وسويسرا وجنوب إفريقيا وايرلندا وغيرها.

(45) د. احمد خليفة الملطال جرائم المعلوماتية، دار الفكر العربي، الإسكندرية، ص168.

(46) د. عبدالفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي دارالفكر الجامعي الإسكندرية.6020ص78.