وسائل حماية التجارة الالكترونية من مخاطر الهجمات السيبرانيه

Means of protecting electronic commerce from the dangers of cyber attacks

م.م. احمد عطا حسين
جامعة واسط – كلية الطب
ahussein@uowasit.edu.iq

الملخص:
يشهد العالم في الوقت الحاضر تطورا هائلا في وسائل الاتصالات الالكترونية الحديثة ، واضحى استخدام الانترنت في مجالات عديدة من مجالات الحياة ضرورة ملحة لا يمكن الاستغناء عنها ، ومن بين الجوانب الاقتصادية التي يُستخدم بواسطتها الانترنت ممارسة التجارة الالكترونية على نطاق واسع من العالم ، واصبحت التجارة الالكترونية تشكل احد الروافد الاقتصادية المهمة التي ترفد دول العالم بموارد مالية لا يمكن الاستغناء عنها ، وبالرغم من الجوانب الايجابية للتجارة الالكترونية على الاقتصاد العالمي الا ان هناك بعض الجوانب السلبية التي تعاني منها ، و تتمثل تلك الجوانب بالهجمات السيبرانيه التي يمكن ان تؤثر على تلك التجارة من نواح عدة ، وبالرغم من سن التشريعات القانونية اللازمة في معظم الدول التي تكفل تنظيم التجارة الالكترونية على الوجه المطلوب الا انها تعاني من نقص واضح في توفير الوسائل اللازمة لحمايتها من مخاطر الهجمات السيبرانية ، ولغرض بيان تلك الوسائل قسُم البحث على مبحثين تتبعهما خاتمة تتضمن اهم التوصيات والنتائج التي توصل اليها الباحث .

الكلمات الافتتاحية : [تجارة الكترونية ، هجمات سيبرانية ، حماية ، وسائل قانونية دولية ، سايبر ، الامن السيبراني]

Means of protecting electronic commerce from the dangers of cyber attacks

M.M Ahmed Atta Hussen
Wasit University / College of Medicine
ahussein@uowasit.edu.iq

Abstract

The world is witnessing at the present time a tremendous development in the means of modern electronic communications, and the use of the Internet in many areas of life that has become an urgent necessity that cannot be dispensed with. One of the important economic tributaries that provides countries with financial resources that cannot be dispensed with, is the electronic commerce and its positive aspect on the global economy, There are some negative aspects that it suffers from, and these aspects are represented by cyber attacks that can affect that trade in several ways ، Despite the positive aspects of electronic commerce on the global economy, there are some negative aspects that it suffers from, and these aspects are represented by cyber attacks that can affect that commerce in several ways, and despite the enactment of the necessary legal legislation in most countries that ensure the regulation of electronic commerce as required, however, it suffers from a clear lack of providing the necessary means to protect it from the dangers of cyber-attacks, and for the purpose of explaining those means, the research department has two sections followed by a conclusion that includes the most important recommendations and results reached by the researcher .

Key words: [Electronic commerce . Cyber attacks . Protection . International legal means . Cyber . Cyber security]

الكلمات الافتتاحية : [تجارة الكترونية ، هجمات سيبرانية ، حماية ، وسائل قانونية دولية ، سايبر ، الامن السيبراني]

المقدمة

يشهد العالم في الوقت الحاضر تطورا كبيرا في وسائل الاتصال الالكترونية ، واضحت الدول تتسابق فيما بينها للحصول على مستويات متقدمة من التطور التكنلوجي في المجال المذكور، وذلك بسبب دخول وسائل الاتصالات الحديثة في حياتنا اليومية واعتماد الكثير من الاعمال والخدمات التي نحتاجها على تلك الوسائل .وبالرغم من الجوانب الإيجابية العديدة التي احدثته وسائل الاتصالات في مجال التجارة الالكترونية ،

والتي تتمثل بجعل العالم المترامي الأطراف بين دفة اليدين ، وسهولة الوصول الى المعلومات الضرورية في شتى جوانب الحياة وسهولة استخدامها وكلفتها القليلة ، وكذلك الحصول على كافة الخدمات والمعلومات والبضائع في وقت يسير، الا انه لا يمكن اغفال الجانب السلبي لتلك الوسائل ، اذ ان قرصنة البرامج وظهور برامج فايروسيه يمكن من خلالها تهكير عمل تلك البرامج وتطورها أدى الى استخدامه من قبل افراد او شركات او حتى دول معادية ضد شركات او دول أخرى أدى الى ظهور ما يعرف بالهجمات السبرانية ، فبالرغم من اعتماد اغلب الشركات التجارية على أجهزة الكمبيوتر واتصالها بالشبكة العنكبوتية (الانترنت) مثل شركات النقل الجوي والبحري و المصارف العالمية وشركات مواقع التواصل الاجتماعي ، وظهور ما يعرف بالحكومة الالكترونية داخل دوله معينة ، الا انه يمكن لدوله منافسة أخرى السيطرة على عمل تلك الشركات من خلال برامج معينة يطلق عليه بالهجوم السبراني .

وتتمثل أهمية موضوع البحث في انه يعالج فكرة جديدة لم تظهر على ارض الواقع الا في الآونة الأخيرة ، فبالرغم من اعتماد التجارة الالكترونية على وسائل الكترونية حديثة وتنظيم أنشطتها عبر تلك الوسائل ، لا يوجد نظام قانوني يعالج مخاطر الهجمات السبرانية ، كذلك لا بد من تسليط الضوء على مفهوم تلك الهجمات ووضع الحلول القانونية اللازمة لمعالجة اضرارها بالتالي حماية التجارة الالكترونية من مخاطرها .

و تكمن مشكلة البحث في غياب التنظيم القانوني على مستوى التشريع الوطني في اغلب الدول ومنها العراق في معالجة هذه الهجمات بالرغم من ظهورها في الآونة الأخيرة بكثرة ، مما يطرح الموضوع عدة تسأولات نذكر منها : ماهو المفهوم القانوني للهجوم السيبراني ؟ وما هي خصائصها ؟ وما هي الوسائل القانونية اللازمة لحماية التجارة الالكترونية من مخاطرها ؟

وسوف نجيب على الاسئلة المذكورة من خلال هذا البحث ، و سوف نعتمد المنهج التحليلي المقارن في بحث الموضوع ، من خلال عرض المواد القانونية التي تناولت الهجمات السبرانية وتحليلها تحليلاً منطقياً شاملاً ، وكذلك بيان موقف القضاء الوطني والدولي من هذه الهجمات ، من خلال عرض احكام القضاء واحكام التحكيم والتعليق عليها ان امكن ، كذلك سوف نعتمد المنهج المقارن من خلال بيان موقف التشريعات المقارنة وبيان الاليات القانونية التي اعتمدتها تلك الدول لحماية تجارتها الالكترونية من خطورتها ، وسوف نبين ايضا الجهود الدولية التي بذلت في هذا الشأن قدر الامكان .

من اجل ذلك سوف نتناول موضوع وسائل حماية التجارة الالكترونية من مخاطر الهجمات السيبرانية على مبحثين ، نخصص المبحث الاول لبيان ماهية الهجمات السبرانية ومخاطرها على التجارة الالكترونية والذي يقسم ايضاً على مطلبين ، نبين في المطلب الاول مفهوم الهجمات السيبرانية ومخاطرها على التجارة الالكترونية ، بينما نخصص المطلب الثاني لبيان الطبيعة القانونية لمخاطر الهجمات السيبرانية على التجارة الالكترونية ، بينما نفرد المبحث الثاني لوسائل حماية التجارة الالكترونية من الهجمات السبرانية ، والذي سوف نقسمه ايضاً على مطلبين نتناول في المطلب الاول الوسائل الوطنية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية ونخصص المطلب الثاني لبيان الوسائل الدولية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية .

المبحث الأول

ماهية الهجمات السبرانية و مخاطرها على التجارة الالكترونية

أصبحت الحاجة الماسة للخدمات الالكترونية ضرورة فعلية على ارض الواقع ، واضحت اغلب العمليات التجارية تتم في وقتنا الحاضر بوسيلة الكترونية ، ومع تزايد العمل بالحواسيب الشخصية والمكتبية بصورة يومية وفي اغلب المجالات ومنها النشاط التجاري ، زادت في ذات الوقت اعمال التهكير الالكتروني والهجوم السبراني في مختلف الدول ، واصبح الهجوم المذكور يقع بين الحين والأخر ، مما يشكل خطرا حقيقياً على اقتصاديات دول العالم لا سيما وان اغلب العمليات ذات الجانب التجاري أصبحت تتم بموجب قوانين نافذة في العراق وبقية دول العالم بوسيلة الكترونية [١] ، ولغرض بيان ماهية الهجوم السبراني ومخاطره على التجارة الالكترونية لابد لنا من تقسيم هذا المبحث على مطلبين نتناول في المطلب الأول مفهوم الهجوم السبراني ومخاطره على التجارة الالكترونية ، بينما نخصص المطلب الثاني لبحث الطبيعة القانونية للهجوم السبراني و مخاطره على التجارة الالكترونية .

المطلب الأول

مفهوم الهجمات السيبرانية و مخاطرها على التجارة الالكترونية

لا يخفى علينا ان مصطلح الهجوم السيبراني ليس بالمصطلح الحديث نسبيًا ، فهذا المصطلح ظهر على ارض الواقع من مدة قريبة جداً وساعد على ظهوره الثورة التكنلوجيا والمعلوماتية التي يشهدها العالم في وسائل الاتصالات الالكترونية الحديثة ، ولغرض تحديد مفهوم الهجوم السيبراني لابد لنا ان نقسم هذا المطلب على فرعين ، نتناول في الفرع الأول تعريف الهجوم السيبراني ومخاطره على التجارة الالكترونية ،

بينما نفرد الفرع الثاني لخصائص الهجوم السيبراني .

الفرع الأول

تعريف الهجمات السبرانية ومخاطرها على التجارة الالكترونية

ان مصطلح الهجمات السيبرانية ومخاطرها على التجارة الالكترونية يتكون من قسمين هما : الهجمات السيبرانية والتجارة الالكترونية ، ولغرض بيان التعريف القانوني المنطقي لهذه العبارة لابد من تحديد مفهوم كلٍ واحد على انفراد ثم نحاول بيان تعريفا شامل لهما .

اما فيما يتعلق بتعريف التجارة الالكترونية فلم تتفق كلمة الفقه على وضع تعريفًا موحدًا لها ، فهناك جانب من الفقهاء يعرفها على انها " مفهوم عام يغطي كل شكل من اشكال الصفقات التجارية او تبادل للمعلومات يتم تنفيذه باستخدام تكنولوجيا المعلومات والاتصالات بين شركات او بين شركات وعملاء او بين شركات وادارات عامة وتشمل التجارة الالكترونية المتاجرة الكترونيا بالسلع والخدمات والمواد الالكترونية " [٢] ، ويلاحظ على التعريف المذكور انه قد بين مفهوم التجارة الالكترونية بصورة واضحة ودقيقة ويمكن ان يحظى بالتأييد والقبول من قبل الباحث .

كما ان هناك جانب اخر من الفقهاء يعرف التجارة الالكترونية بأنها " استخدام شبكات الحاسب الالكتروني لتسهيل المعاملات التجارية المتضمنة تداول المنتجات من السلع والخدمات وتوزيع البضائع ، وهذه السلع والخدمات تتضمن منتجات مادية (غير رقمية) او رقمية تتضمن نصوصا واصواتا ، صورا وافلاما يمكن ان تفسر كسلسلة من الأرقام المنفردة او الاصفار ، ولذا فهي تخلق فرصا مماثلة للمعاملات التجارية المتضمنة المنتجات الرقمية وغير الرقمية من خلال تداول الاعمال التجارية فيما بينها " . [٣]

يلاحظ على التعريف المتقدم انه يربط بشكل مباشر بين استخدام الحاسب الالكتروني وبين المعاملات التجارية التي تتم عن طريقها ، وكذلك بين الغرض من استخدام الوسائل الالكترونية هو لتسهيل تلك التجارة .

ويذهب اتجاها اخر لتعريف التجارة الالكترونية على انها " العمليات التجارية التي يتم تبادل الايجاب والقبول وتراضي الاطراف بسأنها واتفاقهم على كل بنود الصفقة التجارية عبر شاشات الحاسوب المتصلة بالشبكة العنكبوتية بحيث لا يبقى من انهاء الصفقة الا التسليم المادي للشيء محل التعامل " . [٤]

ويلاحظ على التعريف المذكور انه يركز على الصفة العقدية لعقود التجارة الالكترونية من جانب كما انه ومن جانب اخر جاء

مطولاً ولم يبين مفهوم التجارة الالكترونية بصورة دقيقة ، كما انه يضيق من نطاق التجارة الالكترونية ويخرج من نطاق الصفقة التسليم الالكتروني ، اذ ليس بالضرورة ان تكون الاشياء المباعة بواسطة التجارة الالكترونية اشياء مادية بحتة اذ من الممكن ان تكون سلع او خدمات الكترونية يمكن تسليمها بواسطة الانترنت مثل شراء برامج الكترونية او الحصول على اموال او ارصدة الكترونية .

هذا ما يتعلق بالتجارة الالكترونية اما فيما يتعلق بالهجمات السيبرانية ، فلقد ذكرنا سابقاً ان مصطلح السيبرانية [٥] ، مصطلح حديث نسبيا وقد بُذلت محاولات عديدة من قبل الفقهاء القانونيين لوضع تعريف محدد لها ، وبالرغم من تلك المحاولات فأن كلمة الفقه لم تتفق على وضع تعريفًا موحدًا لها ، فمنهم من يعرفهُا بأنها " هجوم عبر الانترنت يقوم على التسلل الى مواقع الكترونية غير مرخص بالدخول اليها ، بهدف تعطيل او اتلاف البيانات المتوفرة فيها او الاستحواذ عليها ، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى " . [٦]

يتبين من التعريف المذكور ان الهجوم السبراني هو هجوم يتم عن طريق شبكة الويب العالمية الانترنت وبالتالي يخرج من دائرة هذا الهجوم الهجمات الاخرى التي لا تتم بهذه الوسيلة ، كما ان الهجوم المذكور يتم عن طريق التسلل الى المواقع بدون علم مالكيها الحقيقين وبدون ترخيص مسبق من قبلهم ، كما ان الهدف منه تعطيل تلك المواقع او السيطرة عليها ، كما انه يتم من قبل دوله ضد دولة أخرى .

وبالرغم من ان التعريف المذكور قد اوجز في بيان ماهية الهجوم السبراني الا انه لا يخلو من بعض المثالب القانونية ، نذكر منها ان التعريف حسب اعتقادنا قد جاء مطولا يحمل اكثر من مفهوم لبيان الهجوم السبراني ، ومع تعدد المفاهيم للهجوم المذكور نجد انعدام التوافق بينها ، فهو من ناحية يستخدم مصطلح الهجوم ومن ناحية أخرى يصفه بالتسلل ، ولو فرضنا جدلاً ان السبرانية هجوم او تسلل فكيف تتم بأذن مالكيها ؟ هذا من جانب ومن جانب اخر تحدث التعريف على ان الهجوم السبراني يتم دائما من قبل دولة ضد دولة أخرى ، وبالرغم من ان الالية المذكورة غالبا ما نلاحظ وجودها في ارض الواقع الا انه ليس بالضرورة ان تقع دائما ، فالهجوم السبراني يمكن ان يوجه من قبل شخص ضد اخر او من قبل شخص ضد دولة .

ويذهب جانب اخر من الفقهاء الى تعريف السبرانية بأنها " مجموعه من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والاضرار بها ، وفي الوقت نفسة للدفاع عن نظم المعلومات

الخاصة بالدولة المهاجمة " [٧] ، ويلاحظ على التعريف المذكور انه جاء مختصراً لم يبين مفهوم الهجوم السبراني بصورة دقيقة ، كما لم يحدد الغرض المذكور منه كما انه لم يبين خطر الهجوم السبراني على اقتصاد الدولة والعمليات التجارية التي تتم بصورة الكترونية ، كما انه لا يخلو من التناقض فكيف يمكن للهجوم السبراني ان يكون وسيلة هجوم ودفاع في نفس الوقت .

وقد عرفت اللجنة الدولية للصليب الاحمر الهجوم السيبراني بأنه " استخدام انشطة متعمدة لتغيير او افساد او خداع او اضعاف او تدمير انظمة الحاسوب او شبكات الحاسوب للخصم او المعلومات او البرامج المدرجة في هذه الانظمة او الشبكات او التي ترسل من خلالها وقد تؤثر هذه الانشطة ايضا في الكيانات المرتبطة بهذه الانظمة والشبكات او التي ترسل من خلالها وقد تؤثر هذه الانشطة ايضا في الكيانات المرتبطة بهذه الانظمة والشبكات . وقد يستخدم الهجوم السيبراني في منع المرخص لهم من الولوج الى حاسوب او خدمة معلومات (هجوم الحرمان من الخدمة) او لتدمير الالات التي يتحكم فيها الحاسوب او لتدمير او تغيير بيانات حيوية ويمكن ملاحظة ان الاثار المباشرة للهجوم السيبراني قد تكون اقل اهمية من الاثار الغير مباشرة " [٨] .

من خلال ما تقدم يتبين لنا انه لا يوجد هناك تعريف محددا يبين لنا مفهوم مخاطر الهجمات السبرانية على التجارة الالكترونية وهذا يدل على ان موضوع البحث من المواضيع المستجدة على مستوى الدراسات القانونية من جانب ، و انه لم يحظى بالدراسات الفقهية ولم يحظى باهتمام الفقهاء ، ويمكننا ان نعرف مخاطر الهجمات السيبرانية على التجارة الالكترونية بحسب تقديرنا على انها :

(برامج الكترونية ، يتم استخدامها بواسطة الانترنت ، من قبل جهات معينه ، بهدف السيطرة والتحكم في مواقع التجارة الالكترونية التابع لجهات أخرى ، مسببة اضرارا جسيمة في تلك المواقع لتحقيق اغراض اقتصادية او سياسية او اجتماعية مختلفة) .

من خلال التعريف المتقدم يمكننا ان نبين خصائص مخاطر الهجوم السبراني على التجارة الالكترونية ، وهذا ما سيكون موضوع الفرع الثاني من هذا المطلب .

الفرع الثاني

خصائص الهجوم السيبراني على التجارة الالكترونية

هناك جملة من الخصائص التي يتميز بها الهجوم السيبراني على التجارة الالكترونية يمكن ان نبينها من خلال النقاط الاتية :

اولا – ان الهجمات السيبراني برامج الكترونية متطورة ظهرت نتيجة التطور

التكنلوجي في وسائل الاتصال الالكترونية تستهدف مواقع ذات نشاطات متعددة ومنها النشاط التجاري ، كما ان الهجوم السيبراني الذي يقع على مواقع التجارة الالكترونية يمتاز بصعوبة معرفة مصدره فهو يمكن ان يتم من داخل دولة معينة او من خارجها بسبب عدم إمكانية حصر الفضاء الالكتروني بحدود دولة معينة و بصوره دقيقة . (٩)

ثانيا – ان الهجوم السبراني يؤثر على التجارة الالكترونية بصورة مباشرة ، و يلحق اضرارًا بليغه في الاقتصاد العالمي ، ويؤثر في ثقة الافراد بتلك التجارة ، فبالرغم من ان الهجوم السيبراني يستهدف النشاط التجاري الالكتروني لدولة معينة الا انه يترك اثارا سلبية واضحة على دخل الافراد ، فالمتضرر الأخير هو المواطن البسيط الذي يدخر أموالا الكترونية او يقوم بإحدى العمليات التجارية بصورة الكترونيـــة . (١٠)

ثالثا – ان الهجوم السيبراني لا يحتاج الى تكاليف مادية عالية لكي يحقق اهدافة المضرة بالانشطة التجارية لدولة معينه ، فهو يعتمد بصورة أساسية على برامج الكترونية يتم تطويرها من قبل جهة معينة من ثم يستخدم عبر شبكة الويب العالمية ، وبالتالي لا يحتاج الى مبالغ مالية ضخمة لتحقيق الأهداف المرجوة منه ، كذلك صعوبة تفادي الهجوم السيبراني قبل وقوعه ، فبالرغم من المكنة التكنولوجيا المتطورة لأغلب دول العالم في المجال الالكتروني وكذلك استخدام الشركات التجارية برامج ذات إمكانيات عالية ، الا انه لا يمكن تفادي هذه الهجمات وما تسببه من اضرار ، فالهجوم السيبراني يستخدم المجال الالكتروني ليعطل مواقع حجز التذاكر لشركات الطيران المدني او يتسلل الفايروس الهجومي ليحصل على معلومات معينة من مصارف عالمية او يعطل مواقع التواصل الاجتماعي التابعة لشركات تجارية او افراد مهمين ، وبالتالي لا يمكن لأي جهة معينة او شخص ان يتخذ الاجراءات الكفيلة للتفادي هذا الهجوم مسبقًا وخصوصا مع وجود الفراغ التشريعي . (١١)

رابعا – عدم إمكانية تحديد زمان وقوع الهجوم السيبراني الذي يستهدف التجارة الالكترونية ، وكذلك لا يستطيع من يتعرض للهجوم السيبراني العلم بهذا الهجوم لحظة وقوعه ، فالشخص المتضرر من الهجوم يعلم حين استخدام موقعه الالكتروني المتضرر او حين استخدام الوسيلة الالكترونية التي من خلالها يمارس تجارته الالكترونية ، كما تمتاز هذه الهجمات بأنها وسيله للحصول على موارد مالية بصورة غير مشروعه ، فالهجوم السيبراني بالرغم من امتيازه بالطبيعه العدائية ويستهدف تعطيل المواقع التجارية الا انه يمكن ان يستخدم كوسيلة للحصول على مبالغ مالية

وخصوصا تلك الأموال التي تأخذ الصفة الرقمية كعملة البيتكوين الالكترونية . [١٢]

خامسا – أخيرًا يمتاز الهجوم السيبراني على مواقع التجارة الالكترونية بأنه هجوم غير ملموس ماديا ، بالرغم من انه يترك اثارا سلبية على الأنشطة التجارية على ارض الواقع ، فالهجوم السيبراني يتم باستخدام برامج فايروسية غير ملموسة ماديا تؤدي الى احداث اضرار بوسائل مادية مرتبطة ببرامج الكترونية ، فبطاقة الدفع الالكتروني هي وسيلة مادية مرتبطة الكترونيًا ببرامج معينه وتعطيل تلك البرامج يؤدي بطبيعة الحال الى عدم امكانية استخدام تلك البطاقة .

بعد ان بينا مفهوم الهجمات السيبرانية على مواقع التجارة الالكترونية من خلال تعريفها وبيان خصائصها لا بد لنا بيان الطبيعة القانونية لها ، وهذا ما سنتناوله في المطلب الثاني من هذا المبحث .

المطلب الثاني

الطبيعة القانونية للهجمات السيبرانية ومخاطرها على التجارة الالكترونية

ان تحديد الطبيعة القانونية للهجمات السبرانية على مواقع التجارة الالكترونية امر في غاية الأهمية ، وبالرغم من أهميتها من الناحية القانونية الا ان تحديدها بصورة دقيقة لم يكن مطروقاً من قبل الشراح وفقهاء القانون ، الامر الذي تكتنفه بعض الصعوبات ، ولغرض بيان دقيق لطبيعة الهجمات السيبرانية وتحديد مخاطرها على مواقع التجارة الالكترونية يمكننا ان نطرح تساؤلاً تكون الإجابة عليه بمثابة تحديدًا لطبيعة هذه الهجمات ومخاطرها على التجارة الالكترونية ، اذ يمكننا ان نتسأل هل هناك تشريع نافذ ينظم الهجمات السيبرانية ويبين المسؤولية الناشئة عنها ؟ وهل ان التشريع التجاري قد وفر الحماية القانونية لمستخدمي التجارة الالكترونية من مضار هذه الهجمات ؟ للأجابة على التساؤل المطروح ينبغي الرجوع الى التشريع التجاري العراقي وبالخصوص قانون التجارة رقم (30) لسنة ١٩٨٤ النافذ ، يلاحظ ان المشرع العراقي لم ينظم العمل التجاري الالكتروني ، وذلك بسبب حداثة التجارة الالكترونية من جهة وعدم حداثة تشريع التجارة العراقي النافذ من جهة أخرى ليواكب التطورات التي حصلت في الوقت الحاضر ، وبالتالي لم يبن لنا طبيعة الهجمات السيبرانية ومخاطرها على التجارة الالكترونية ، كما ان المشرع العراقي لم ينظم قانونًا للتجارة الالكترونية كما هو معمول به في معظم التشريعات العربية [١٣] ، وهذا نقص يجدر بالمشرع العراقي تفاديه ، ولكن يلاحظ ان المشرع العراقي قد تناول بصورة عامة حماية المستهلك من المنافسة التجارية غير مشروعه ، والتساؤل الذي يدور في الذهن هل يمكن تأطير الهجمات

السبرانية المضرة بالتجارة الالكترونية بأطار المنافسة غير المشروعه ؟

عند الاستعانة بنصوص قانون المنافسة ومنع الاحتكار العراقي رقم ١٤ لسنة ٢٠١٠ النافذ نجد ان المشرع العراقي ينص في المادة (٣) منه في اطار سريان القانون بأنه " أولاً : تسري أحكام هذا القانون على أنشطة الإنتاج والتجارة والخدمات التي يقوم بها الأشخاص الطبيعية والمعنوية داخل العراق كما تسري أحكامه على أية أنشطة اقتصادية تتم خارج العراق وتترتب عليها أثار داخله " ، كما ينص بموجب المادة (٧) على انه " ثامناً : التنسيق والتعاون مع الجهات المماثلة خارج العراق في مجال تبادل المعلومات والبيانات وما يتعلق بتنفيذ قواعد المنافسة ومنع الاحتكار في حدود ما تسمح به المعاهدات الدولية شرط المعاملة بالمثل " ، ويعرف الاحتكار بموجب المادة الأولى بأنه " ثانيا – كل اتفاق او فعل او تفاهم صدر من شخص او اكثر طبيعي او معنوي او ممن توسط بينهم للتحكم بالسعر او نوعية السلع او الخدمات بما يؤدي الى الحاق ضرر بالمجتمع " ، يتبين من خلال المواد المذكورة سابقا ان التعريف الذي أورده لنا المشرع العراقي يضع مفهوما واسعًا للاحتكار فلم يقصره على مجرد الأفعال الضارة التي يقوم بها التجار وانما يشمل بالإضافة الى ذلك الاتفاقات وكذلك التفاهم غير المشروع [١٤] ، كما انه يمكن ان يصدر من شخص او مجموعة اشخاص طبيعيين او معنويين الهدف منه الاضرار بالمجتمع ، وبالرغم من وجود نقاط تشابه بين الأخير والهجمات السيبرانية موضوع بحثنا ، فهل يمكن اعتبار الأخيرة نوع من أنواع الممارسات الاحتكارية الضارة ؟ اذا ما وجهت من اشخاص معينين عبر وسائل الكترونية لكي تكون مضرة بالمجتمع ؟

اجابة على التساؤل المطروح لو افترضنا جدلا ان الهجمات السيبرانية نوع من أنواع الاحتكار فهذا يعني اخراج تلك الهجمات من مفهومها الواسع وتقيدها بموضوع الاحتكار فقط ، بينما تكون الهجمات السيبرانية ذات مفهوم واسعًا شاملاً قد يؤدي الى اضرار اقتصادية لدولة معينة او عدة دول مجتمعه مما يعكس اثاره السلبية على المجتمع ، وبالتالي لا يمكن اعتبار الهجوم السيبراني ممارسة احتكارية غير مشروعه من قبل التجار بالرغم من وجود نقاط الشبه بينهما . [١٥]

من خلال ما تقدم وبسبب غياب تشريع قانوني يبين ماهية الهجمات السيبرانية بصورة عامة ومخاطرها على التجارة الالكترونية بصورة خاصة ، وبسبب حداثة موضوعها وتأثيرها الكبير على الأنشطة الاقتصادية التي تتم بصورة الكترونية ، يمكننا القول بأن الهجمات السيبرانية

ومخاطرها على التجارة الالكترونية ذات طبيعة قانونية خاصة ، قائمة بذاتها بالرغم من وجود تشابه ونقاط التقاء مع مفاهيم قانونية أخرى ، ويمكن ان تتمثل بحسب تقديرنا هذه الطبيعه على انها نوع من انواع التعدي على حقوق الغير توجب المسؤولية المدنية على مرتكبها .

وبعد ان بينا الطبيعة القانونية للهجمات السيبرانية ومخاطرها على التجارة الالكترونية يقتضي بنا بيان الوسائل القانونية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية ، وهذا ما سنتناوله في المبحث الثاني من هذا المبحث .

المبحث الثاني

الوسائل القانونية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية

تعد الهجمات السيبرانية وكما بينا في المبحث الأول من هذا البحث مصدر خطر على الاقتصاد العالمي بصورة عامة وكذلك تشكل تهديداً واضحًا للتجارة الالكترونية بصورة خاصة ، كما انها تترك اثارا سلبية على الافراد الذين يمارسون تلك التجارة بصورة يومية ، وتشير الدراسات القانونية والإحصاءات الاقتصادية ان هناك زيادة ملحوظة في نسبة العائدات المالية المتحصلة من التجارة الالكترونية في مختلف دول العالم [١٦] ، ويمكن القول ان اغلب دول العالم التي تشهد تطورا ملحوظا في مجال الاتصالات الالكترونية بدئت تطور تجارتها الالكترونية وتعتمد بنسبة معينة من اقتصادها على تلك التجارة ، وذلك بسبب سهولة الترويج لبضائعها والحصول على مستهلكين لتلك البضائع وكذلك قلة الكلفة المالية للترويج وتصريف تلك المنتجات ، وبالمقابل يمكننا ان نتسأل هل ان الدول التي يعتمد اقتصادها على التجارة الالكترونية بنسبة معينة قد اتخذت وسائل قانونية لحماية تجارتها من مخاطر الهجمات السيبرانية ؟ لبيان هذه المسألة لابد لنا ان نقسم هذا المبحث على مطلبين ، نبين في المطلب الأول الوسائل الوطنية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية ، بينما نخصص المطلب الثاني لبيان الوسائل الدولية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية .

المطلب الأول

الوسائل الوطنية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية

ادركت دول عديدة أهمية المخاطر المحدقة بتجارتها الالكترونية من خلال تعرضها للهجمات السيبرانية ، وقطعت تلك الدول شوطا كبيرا في سن التشريعات القانونية اللازمة لمواجهة تلك المخاطر والحد من اثارها بنسبة معينة ، ولذلك تتمثل الوسائل الوطنية بالتشريعات القانونية النافذة في دول

معينه لحماية تجارتها الالكترونية ، او قد تكون تلك الوسائل عبارة عن اتفاقات او عقود مدنية مبرمة من قبل اشخاص طبيعيين او معنويين مع شركات متخصصة في توفير الحماية من الهجمات السيبرانية ، ولغرض بيان تلك الوسائل لابد لنا ان نقسم هذا المطلب على فرعين ، نبين في الفرع الأول الوسائل التشريعية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية بينما نخصص الفرع الثاني لبيان الوسائل الاتفاقية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية .

الفرع الأول

الوسائل المقررة تشريعاً

تتمثل هذه الوسائل بتشريعات قانونية نافذة داخل حدود دولة معينه ، ولغرض بيان هذه الوسائل لابد من تسليط الضوء على التشريع العراقي ، كما سوف نستعرض بعض التشريعات المقارنه التي تناولت في قوانينها بعض الوسائل الناجعَ لحماية التجارة الالكترونية من مخاطر الهجمات المذكورة ، وبالرجوع الى التشريع العراقي نجد ان المشرع ينظم مؤخرا قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ النافذ ، اذ تناول فيه احكام المعاملات الالكترونية ومن ضمنها العقود التي تتم بصورة الكترونية وكذلك تضمن احكام للمعاملات الالكترونية ذات الجوانب التجارية [١٧] ، اذ ينص في المادة (٢) منه والمتعلقة باهداف القانون على انه " أولا – توفير الاطار القانوني لاستعمال الوسائل الالكترونية لأجراء المعاملات الالكترونية " ، كما ينص في المادة (٣) بأنه " تسري احكام هذا القانون على : جـ – الأوراق المالية والتجارية الالكترونية " ، كما نجد ان المشرع العراقي قد خصص فصلا كامل لاحكام الأوراق التجارية والمالية التي تتم بصورة الكترونية وهو الفصل السادس من القانون المذكور اذ تضمن احكاما خاصة بها وضمن المادتين (٢٢ و٢٣) منه ، كما خصص الفصل السابع لبيان احكام التحويل الالكتروني للأموال ، وذلك بموجب المادة (٢٤) والتي تنص على انه " يجوز تحويل الأموال بوسائل الكترونية " ، وفي ما يتعلق بحماية المعاملات التجارية المذكور والتي تتم بوسيلة الكترونية نجد ان المشرع العراقي قد اغفل النص عليها بما يؤمن تلك المعاملات من مخاطر الهجمات السيبرانية ، كما نجد ان حماية تلك المعاملات اقتصرت فقط في المادة (٢٥) منه والتي تنص بأنه " على كل مؤسسة مالية تمارس اعمال التحويل الالكتروني للأموال اتخاذ الإجراءات الكفيلة بتقديم خدمات مأمونة للزبائن والمحافظة على سرية المعاملات المصرفية".

من خلال النص المتقدم نجد ان المشرع العراقي لم يوفر حماية كافية للمعاملات التجارية الالكترونية بالرغم من انه قد نظم تلك المعاملات المتعلقة بالاوراق المالية والتجارية وعمليات التحويل المالي والمصرفي و بالرغم من خطورة التعامل بها في المجال الالكتروني وخصوصا مع زيادة الهجمات السيبرانية التي تستهدف هكذا معاملات ، نجد ان توفير الحماية لها قد أوكلت للمؤسسات المالية التي تتعامل بها وان تكون تلك الخدمات مأمونة بأجراءات معينة تتخذها تلك المؤسسات . [١٨]

من خلال ما تقدم يتبين لنا ان المشرع العراقي قد اغفل النص على وسائل قانونية كافية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية ، ومع الفراغ التشريعي المذكور ندعو المشرع العراقي الى تنظيم قانوني محكم يوفر الحماية اللازمة للتجارة الالكترونية من مخاطر الهجمات السيبرانية في العراق وخصوصا ان اهم الجوانب التجارية في العراق أصبحت تتم بصورة الكترونية بموجب قانون نافذ ، وهذا بخلاف ما موجود في التشريعات المقارنة التي قطعت شوطا كبيرا في سن التشريعات اللازمة لحماية تجارته الالكترونية من مخاطر الهجوم السيبراني .

وقد ادركت معظم الدول العربية مخاطر الهجمات السيبرانية ونظمت التشريعات اللازمة لكي تحافظ على امنها بصورة عامة وعلى تجارتها الالكترونية بصورة خاصة ، وهذا ما نجده في التشريع الاردني حيث نظم المشرع الاردني قانون الامن السيبراني رقم (١٦) لسنة ٢٠١٩ وتضمن القانون تسعة عشر مادة قانونية وضعت احكاما معينه لمعالجة خطورة الهجمات السيبرانية وتفادي مخاطرها . [١٩]

اذ نجد ان المشرع الاردني يعرف الامن السيبراني بموجب المادة الثانية من القانون المذكور على انه " الاجراءات المتخذ لحماية الانظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الامن السيبراني والقدرة على استعادة عملها واستمراريتها سواء كان الوصول اليها بدون تصريح او سوء استخدام او نتيجة الاخفاق في اتباع الاجراءات الامنية او التعرض للخداع الذي يؤدي الى ذلك " ، كما يعرف حادث الامن السيبراني في نفس المادة على انه " الفعل او الهجوم الذي يشكل خطرا على البيانات او المعلومات او نظم المعلومات او الشبكة المعلوماتية او البنى التحتية المرتبطة بها و يتطلب استجابة لأيقافهِ او للتخفيف من العواقب والاثار المترتبة عليه " ، كذلك نجد ان المشرع الاردني قد اسس مجلس وطني للامن السيبراني [٢٠] ، وحدد مهامه وذلك بموجب المادة الثالثة من القانون المذكور ، كما ينص المشرع الاردني بموجب المادة

التاسعه ومن ضمن صلاحيات المجلس المذكور على انه " أ- يحدد حادث الامن السيبراني الذي يشكل خطرا على امن المملكة وسلامتها بقرار من المجلس ... " ، كما انه ينص بموجب المادة (١٦ /أ) على انه " ٣- حجب او الغاء او مصادرة او تعطيل شبكة الاتصالات ونظام المعلومات والشبكة المعلوماتية واجهزة الاتصالات والرسائل الالكترونية الخاصة مع الجهات ذات العلاقة عن كل من يشتبه في ارتكابه او اشتراكه في اي عمل يشكل حادث امن سيبراني " .

وحسنا فعل المشرع الاردني حينما نظم قانونا خاصا يعالج حوادث الامن السيبرانية وذلك لخطورة الهجمات السيبرانية على جميع مفاصل الدولة بصورة عامة والتجارة الالكترونية بصورة خاصة ، ولكن مما يلاحظ على القانون المذكور انه لم يبين بصورة واضحة ودقيقة الاجراءات التي يجب اتخاذها لتفادي الهجوم السيبراني قبل وقوعه وهذا يعني ان القانون المذكور يكون دوره علاجي فقط وليس وقائيا ، كما انه لم يبين الجهة التي تتحمل المسؤولية من جراء الهجمات السيبرانية ، وكذلك لم يبين امكانية تعويض المتضررين من جراء الهجوم السيبراني ، ولم يتطرق الى سبل حماية التجارة الالكترونية في الاردن من الهجوم السيبراني وانما وضع قواعد عامة تعالج مسائل غير محددة بصورة دقيقة ، ومع ذلك فأنه لا يمكن انكار الدور الكبير الذي يمكن ان يؤديه هذا التشريع في معالجة خطورة الهجمات السيبرانية وكذلك ايجاد جهات مختصة متمثلة بالمجلس الوطني للامن السيبراني يمكن ان يمارس دوره الفعلي في التصدي للهجمات السيبرانية .[٢١]

ومن بين الدول المهتم في مجال الامن السيبراني والتي سنت تشريعا قانونيا نافذا ايضا نجد ذلك في المغرب ، حيث صدر قانون يعالج الامن السيبراني يتضمن ثلاث وخمسون مادة قانونية وهو قانون رقم (٠٥.٢٠) لسنة ٢٠٢٠ ، وعند مراجعة النصوص القانونية المتعلق بالتشريع المذكور نجد ان المشرع المغربي يعرف حادث الامن السيبراني وذلك بموجب المادة الثانية منه على انه " واقعة أو وقائع غير مرغوب فيها أو غير متوقعة ، مرتبطة بأمن نظم المعلومات، والتي يحتمل جدا أن تعرض للخطر أنشطة هيئة ما أو بنية تحتية ذات أهمية حيوية أو متعهد أو أن تهدد سلامة نظمهم المعلوماتية " كما يعرف ايضا ازمة الامن السيبراني بنفس المادة على انها " حالة ناتجة عن وقوع حدث أو عدة أحداث متعلقة بالأمن السيبراني، يمكن أن يكون لها وقع خطير على حياة الافراد أو على ممارسة الدولة لسلطاتها أو سير الاقتصاد أو على المحافظة على القدرات الأمنية

والدفاعية للبلاد " حيث يتبين من التعريف المذكور ان الحادث السيبراني يمكن ان يترك اثارا سلبية على اقتصاد الدولة بوجه عام . (٢٢)

كما اننا نعتقد ايضا بأنه يمكن ان يكون هذا التأثير من خلال المساس بالتجارة الالكترونية على وجه الخصوص ، ومن الملاحظ على التشريع المغربي انه اكثر دقه في معالجة حوادث الامن السيبراني من التشريع الاردني ، كما انه يتميز عن التشريع الاخير بتضمنه مواد قانونية لها دور وقائي في معالجة حوادث الامن السيبراني ، اذ نجد ان المادة (٢٩) من القانون الامن السيبراني المغربي تنص على انه " يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الانترنت ومقدمي خدمات الامن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الانترنت، في إطار توجيهات السلطة الوطنية ، اتخاذ التدابير الحمائية اللازمة لأجل الوقاية وإبطال مفعول التهديدات أو الانتهاكات التي تمس نظم معلومات زبائنهم".

اذ يتبين من النص المذكور ان المشرع المغربي يضع واجبا قانونيا على الجميع بما فيهم مزودي خدمة الانترنت ومقدمي خدمات الامن السيبراني باتخاذ اجراءات معينه الغرض منها تفادي الهجمات السيبرانية ، ونعتقد بأنه حسنا فعل المشرع المغربي بأيراد نص قانوني يكون له دور وقائي من الهجوم السيبراني ، الا انه ومن جانب اخر لم يبين ماهي هذه الاجراءات الوقائية وكيفية اتخاذها من قبل الملزمين بها تاركا هذا الامر لذوي الخبرة والشأن في هذا المجال . (٢٣)

كذلك نجد ان المشرع المغربي يلزم الجهات المذكورة بضرورة ابلاغ الجهات الحكومية بأي حوادث قد تؤثر على انظمة معلومات زبائنهم وذلك بموجب المادة (٣٠) من القانون المذكور والذي ينص على انه " عندما يقوم مستغلوا الشبكات العامة للمواصلات ومزودو خدمات الانترنت ومقدمو خدمات الامن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الانترنت برصد أحداث قد تؤثر على أمن نظم معلومات زبائنهم، وجب عليهم إخطار السلطة الوطنية فورا بذلك " ، كذلك نجد المشرع المغربي يعالج حالة التصدي للهجوم السيبراني ، اذ ينص بموجب المادة (٤١) بأنه " لأجل التصدي لأي هجوم إلكتروني يستهدف نظم المعلومات ويمس بالوظائف الحيوية للمجتمع أو الصحة أو السلامة أو الامن أو التقدم الاقتصادي أو الاجتماعي، يقوم أعوان السلطة الوطنية بالتحريات التقنية اللازمة لتحديد خصائص الهجوم ويسهرون على ضمان تنفيذ التدابير والتوصيات المتعلقة بها " .

من خلال العرض المتقدم يتبين لنا ان هناك بعض الدول ادركت مخاطر الهجوم السيبراني على اقتصاد الدولة بصورة عامة وعلى التجارة الالكترونية بصورة خاصة ، وبالرغم من وجود بعض الثغرات القانونية في التشريعات المذكورة الا ان هذه الثغرات لا تشكل امر سلبي امام وجود تشريع نافذ يعالج حالة ضرورية وملحة ويبين الوسائل اللازمة لتفادي وقوعها او معالجة سلبياتها باقل الخسائر في حالة وقوعها ، لذا ندعو المشرع العراقي ان يحذو حذو التشريعات العربية في سن قانون يعالج مخاطر الهجوم السيبراني ويخصص بعض المواد القانونية لتفادي خطرها على التجارة الالكترونية لاسيما نجد هناك تطورا ملحوظا وتوسعا في مجال التجارة الالكترونية في العراق .

الفرع الثاني

الوسائل المقررة اتفاقاً

وتتمثل هذه الوسائل بوجود عقد قانوني يبرم بين طرفان احدهما مزود خدمة الامن السيبراني والطرف الاخر المستفيد من خدمة الامن السيبراني ، ويحدد هذا العقد – وانطلاقا من قاعدة العقد شريعة المتعاقدين – حدود التزامات الطرفين وحقوقهما [٢٤] ، كما يبين الجهات المختصة بنظر المنزاعات التي تنشأ عنه والالية القانونية لانهائه ، ولغرض وجود العقد من الناحية القانونية لا بد من توفر اركان لهذا العقد وهي ذات الاركان التي يجب توفرها في سائر العقود من تراضي ومحل وسبب ، وكذلك يتكون من اطراف والتزمات تقع على عاتقهم تنفيذها وهذا هو الامر الجوهري في العقد ، ولغرض تسليط الضوء على العقد المذكور بصورة سريعة ومختصرة لابد لنا ان نبين اطراف العقد والتزاماتهما وعلى فقرتين تاركين البحث في اركانه للباحثين في القانون المدني .

اولا – اطرف عقد خدمة الامن السيبراني

يتكون عقد الامن السيبراني عادةً من طرفان ، الطرف الاول متعهد خدمة الامن السيبراني ، وهو طرف يكون عادةً شخص طبيعي او معنوي يتخذ شكل شركة معنوية يكون له خبرة ومعرفة كاملة في توفير الخدمة المذكورة من خلال امتلاكه برامج حاسوبية معينة لها دور فاعل وحقيقي في توقي الهجمات السيبرانية ، كما يمكن له ايضا حماية المعلومات الشخصية للطرف المتعاقد معه او حماية المعلومات التي يمتلكها ، كما يمُكّن الطرف الثاني من معرفة المواقع الوهمية او المزيفة والتي تكون مصدر ضرر مادي للزبائن ، كما يمكن ان يكون الطرف الاول في العقد مزود خدمة الانترنت ، وكما هو معمول به في العراق وفي معظم الدول العربية فأن تزويد خدمة الانترنت من قبل شركة متخصصة في هذا المجال توفر خدمة للمواطنين عن طريق اشتراك شهري يدفعه الزبون للشركة ، وعادةً هذه الشركة

تمتلك سيرفرات وبرامج تمكنها من معرفة البرامج الضارة او الهجمات التي يكون لها تأثير سلبي على المشتركين وتستطيع اتخاذ اجراءات معينة تحمي المواطنين من الهجمات السيبرانية والتي تكون مصدر ضرر بتجارتهم الالكترونية [٢٥] ، اما الطرف الثاني في العقد المذكور فهو الشخص المستفيد من خدمة الامن السيبراني ، وهذا الشخص يمكن ان يكون شخص طبيعي يأخذ صفة زبون يكون مرتبط بشبكة الانترنت ويمارس التجارة الالكترونية وذلك عن طريق الشراء من مواقع تجارية متوفرة على شبكة الانترنت او يمارس صفة البائع لبضائع سلع او خدمات عبر الشبكة المذكورة ويمكن ان تتضرر تجارته من الهجوم السيبراني ، او يمكن ان يكون الطرف الثاني شخص معنوي يأخذ صفة شركة تجارية تمارس اعمالها التجارية عن طريق الانترنت وتتضرر عادةً من الهجوم السيبراني في حالة وقوعه ، وترغب الشركة المذكورة من الحصول على خدمة توفير الامن السيبراني من الطرف الاول . [٢٦]

ثانيا – التزامات اطراف عقد الامن السيبراني

تقع على عاتق اطراف عقد الامن السيبراني التزامات متبادلة ، ويحدد اطراف العقد عادةً تلك الالتزامات بموجب بنود يضْمنوها في العقد المبرم بينهم ، وكما هو معلوم ان التزام كل طرف في العقد يمثل حق للطرف الاخر ، وتتمثل التزامات متعهد الامن السيبراني بتوفير الخدمة التي توفر الحماية اللازمة للطرف الاخر في العقد كما عليه ان يبذل العناية اللازمة لتحقيق التزامه ، ويكون ذلك من خلال توفير البرامج الالكترونية التي توفر حماية التجارة الالكترونية من الهجمات السيبرانية ويتخذ كل اجراء لازم لتوقي تلك الهجمات قبل وقوعها ، كما يلتزم الطرف الاول بأعلام الطرف الثاني بكل المعلومات الضرورية واللازمة قبل العقد وبعد ابرامه ، كما يقع على عاتق متعهد الامن السيبراني تنفيذ التزامه المذكور بحسن نية ، والالتزام بالاعلام يتمثل في اعلان متعهد الخدمة التعريف بنفسه للجمهور من خلال بيان المعلومات اللازمة التي تتضمن على الاقل اسمه وعنوان البريد الالكتروني وقيد اسمه التجاري ، وهذا ما يؤكده المشرع الفرنسي في قانون الثقة في الاقتصاد الرقمي المشار اليه سابقا ، حيث نجد ان المادة (6-3/1) من القانون المذكور تنص بأنه ": على متعهد الوصول الكشف لعملائه، على الاقل، عن اسمه وعنوانة البريدي والالكتروني ، ومكان ورقم قيده التجاري " [٢٧] ، كما يلتزم متعهد الامن السيبراني المحافظة على سرية المعلومات التي يحصل عليها من الزبون خلال تنفيذ التزامة . [٢٨]

اما فيما يتعلق بالتزامات الطرف الثاني وهو المستفيد من الخدمة فتتمثل بدفع الاجر المتفق عليه في العقد والذي يتمثل عادةً بمبلغ من المال يأخذ شكل مبلغ مقطوع او اقساط شهرية يلتزم بدفعها الزبون للمتعهد ، كما يلتزم الزبون ايضًا بالاستخدام الامثل للشبكة الانترنت من خلال تجنب المواقع المشبوهة واعلام المتعهد باي خرق يهدد امنه السيبراني كما يلتزم ايضا بالمحافظة على سرية المعلومات التي تكون بحوزته وعدم افشاء سريتها لأي جهة اخرى كالمحافظة على الرمز السري لبطاقة الائتمان او المحافظة على الارقام السرية للمواقع الالكترونية التي بحوزته كما ان أي اهمال من قبل الزبون يترتب عليه ضرر مادي لا يتحمله متعهد الخدمة ، وهذه هي مجمل التزامات اطراف عقد خدمة الامن السيبراني وهي تمثل حقوقا لأطراف العقد ، وان أي اخلال بهذه الالتزامات يعرض الطرف المخل بالتزامه للمسائلة القانونية والمسؤولية تكون عقدية يحكمها العقد المذكور والتعويض يكون بموجب احكام القانون المدنـــي . [٢٩]

من خلال ما تقدم تبين لنا ان هناك وسائل وطنية لحماية التجارة الالكترونية من الهجمات السيبرانية وايًا كانت هذه الوسائل سواء مشرعه بتشريع او مقرة بموجب اتفاق فهي توفر بعض الحماية للتجارة الالكترونية ، وبعد ان بينا الوسائل الوطنية لابد لنا من بيان الوسائل الدولية لحماية التجارة الالكترونية من الهجمات السيبرانية وهذا ما سوف نتناوله في المطلب الثاني من هذا المبحث .

المطلب الثاني

الوسائل الدولية لحماية التجارة الالكترونية من مخاطر الهجوم السيبراني

بينا فيما سبق ان اغلب الدول قد ادركت مخاطر الهجوم السيبراني على الاقتصاد العالمي وعلى التجارة الالكترونية بوجه خاص ، وقد بذلت الدول جهود كبيرة لوضع الاليات القانونية اللازمة لمكافحة الهجوم السيبراني وتوقي مخاطرة او تقليل الخسائر الناتجه عنه وكانت ثمرة هذه الجهود وضع اليات قانونية دولية تساعد الدول الاعضاء في سن القوانين اللازمة لمكافحة الهجوم السيبراني وتوفير قدر من الحماية للتجارة الالكترونية ، وكذلك تتمثل الجهود المذكورة بوضع قواعد قانونية ارشادية تستعين بها الدول لمكافحة الهجمات السيبرانية وتقليل مخاطرها على التجارة الالكترونية [٣٠] ، ولغرض بيان الجهود الدولية والقواعد الارشادية لابد لنا ان نقسم هذا المطلب على فرعين نبين فيهما ماورد سابقا ، مع ملاحظة ان الجهود المذكورة لم ترقى الى مستوى تنظيم اتفاقيات دولية لمكافحة مخاطر

الهجوم السيبراني وحماية التجارة الالكترونية من مخاطرها .

الفرع الاول

الجهود الدولية

من المعلوم ان هنالك محاولات دولية عديدة تكللت بالنجاح لوضع الاليات القانونية اللازمة لتنظيم التجارة الالكترونية على مستوى دولي ، فبعد ان برزت التجارة المذكورة على مستوى عالمي واصبحت تشكل جزء مهم من الاقتصاد المذكور ، و تمثل احد الموارد الرئيسة التي تعتمد عليها اغلب الدول لرفد ايرادتها المالية [٣١] ، سارعت اغلب الدول لوضع القوانين الازمة لتنيظم عمل التجارة الالكترونية ، ولكن بالرغم من ذلك نجد ان التشريعات المذكورة تعاني من نقص حاد في توفير الحماية اللازمة للتجارة الالكترونية من الهجوم السيبراني ، وبهذا الصدد نذكر الجهود التي اتخذت من قبل الامم المتحدة لسن قانون الاونستيرال النموذجي عام ١٩٩٦ وقد اعتمدت نصوص القانون المذكور اكثر من مائة دولة والذي وضع القواعد اللازمة التي تكفل المساواة بين المعلومات الالكترونية والورقية والاعتراف القانوني بالمعاملات الالكترونية ، وكذلك قانون الاونستيرال لسنة ٢٠٠١ الذي ينظم التوقيع الالكتروني ، وفي الاونة الاخيرة صدر قانون الاونستيرال النموذجي لسنة ٢٠١٧ والذي ينظم السندات الالكترونية القابلة للتحويل مثل الكمبيالات وسندات الشحن والشيكات والسندات الاذنية الالكترونية ، حيث ساعدت تلك القواعد القانونية اغلب الدول ومنها الدول العربية الاستعانة بها لتنظيم التشريعات القانونية الخاصة بالتجارة الالكترونية [٣٢] ، وكذلك يمكن ان نذكر ايضًا في هذا الصدد المذكرة الصادرة من لجنة الامم المتحدة للقانون التجاري الدولي في نيويورك لعام ٢٠٠٦ والتي بينت الاعمال التي يمكن اتخاذها مستقبلاً في مجال التجارة الالكترونية والتي جاء من ضمنها في (ثانيا / ز) والتي تتضمن العناصر الاخرى لاطار قانوني سليم للتجارة الالكترونية ، ويندرج تحتها اربع نقاط جوهرية تتمثل حماية الملكية الفكرية وحماية المستهلك في التجارة الالكترونية و الخطابات الالكترونية التطفلية والجريمة السيبرانية ، وقد بينت الفقرة المذكورة جانبا قانونيا مهما اذ اضفت طابع التجريم على الاعتداء السيبراني وبينت ان هذه الاعتداءات تؤثر بشكل مباشر وسلبي على التجارة الالكترونية ولا بد من اتخاذ التدابير اللازمة لمعالجتها . [٣٣]

كذلك نجد ايضا فيما يتعلق بحقوق الملكية الفكرية والتجارة الالكترونية فأن الجمعية العامة للويبو اصدرت مذكرة عن المدير العام للجمعية المذكورة في جنيف عام ١٩٩٩ في الدورة الرابعة والعشرون تضمنت

عدّة نقاط جوهرية تتعلق بالملكية الفكرية والتجارة الالكترونية ، حيث وافقت الجمعية العامة للويبو في اجتماعها المنعقد في سبتمبر/أيلول ١٩٩٨ على عدّة اقتراحات ترمي الى تعزيز التنسيق بين مختلف أنشطة المنظمة المتعلقة بأثر التجارة الالكترونية والاقتصاد الرقمي في الملكية الفكرية ، وقد تضمنت الوثيقة المذكور عدد من الاهداف الجوهرية نذكر منها ما جاء في النقطة التاسعه منها على انه " لا تزال التجارة الالكترونية في المراحل الأولى من نشأتها . وهي تتطور في محيط التكنولوجيا والأعمال الذي يتسم بسرعة التغيير وعمقه وفي ذلك السياق ، فلا مفر من أن يكون تقييم أثر التجارة الالكترونية في الملكية الفكرية عملية مستمرة تقتضي رصدا دقيقا للتطورات بغرض البت في أية تدابير ضرورية أو مناسبة من الممكن اتخاذها على الصعيد الدولي للحفاظ على فعالية حماية الملكية الفكرية وتعزيزها وعليه ، فان تحديد المسائل يعتبر جزءا أساسيا من برنامج عمل المنظمة فيما يتعلق بأثر التجارة الالكترونية في الملكية الفكرية. " [٣٤] ، وكذلك ايضا تطرح الوثيقة المذكورة مثالا حيا فيما يتعلق بأهمية الملكية الفكرية في التجارة الالكترونية وذلك ضمن النقطة الخامسة عشر والتي جاء فيها " ١- بناء على طلب أحد المتاحف الرئيسية في واحد من البلدان النامية ، تسهر المنظمة على تقديم المشورة والمساعدة بشأن السبل الكفيلة باتاحة مجموعة صوره (المرقمنة) على الشبكة دون أن يفقد المتحف سيطرته على المجموعة . ويأتي ذلك المشروع بمثابة مثال ملموس على الطريقة التي يمكن اعتمادها للانتفاع بالتجارة الالكترونية وحقوق الملكية الفكرية بغرض استغلال التراث الثقافي وبما يفيد أصحاب ذلك التراث و من يرغب في أن يتمتع به . وقد يفيد ذلك المشروع عددا كبيرا من البلدان النامية " ، وبالرغم من اهمية الوثيقة المذكورة للدول العربية ومنها العراق في الاستفادة منها لتوفير الحماية اللازمة للتجارة الالكترونية في اطار الملكية الفكرية نجد انها تعاني بعض النقص في ايجاد حماية قانونية خصبة للتجارة المذكورة من مخاطر الهجمات السيبرانية . [٣٥]

اما على المستوى العربي نجد هناك عدة محاولات من قبل جمعيات عربية لوضع الاليات القانونية في اطار توفير الحماية القانونية للتجارة الالكترونية من الهجوم السيبراني ، نذكر في هذا المجال ما صدر عن البرلمان العربي اول قانون شامل يوفر الحماية اللازمة للدول العربية من مخاطر الهجوم السيبراني بوجه عام وتمثلت الجهود المذكورة في وضع اطار قانوني شامل لمواجهة الهجمات السيبرانية، وتعزيز حماية الأنظمة التقنية ومكوناتها ، وتأمين ما تقدمه

من خدمات وما تحتويه من بيانات ، من جميع ألاعمال الغير مشروعة ، وهذا ما تم تأكيده في الجلسة الأولى للبرلمان العربي لدورة الانعقاد الثاني من الفصل التشريعي الثالث ، حيث أقر البرلمان المذكور في هذه الجلسة مشروع القانون الذي بدأ كمقترح مقدم من قبل رئيس البرلمان من ثم تمت إحالته إلى لجنة الشؤون الخارجية والسياسية والأمن القومي لإعداد المسودة الأولى لمشروع القانون ، و يتكون القانون من ستة فصول ، يتناول الفصل الأول تعريف المصطلحات الواردة في القانون وأهدافه وبعض الأحكام العامة ، ويضم الفصل الثاني عدداً من المواد بشأن بناء القدرات التشريعية للدول العربية في حماية وتعزيز الأمن السيبراني و إنشاء مؤسسات وطنية مستقلة للأمن السيبراني وبناء الكوادر البشرية المؤهلة في هذا المجال ، وقد تناول الفصل الثالث التعاون العربي في مجال الأمن السيبراني من حيث تبادل الخبرات والمعلومات بين الدول العربية والمساعدة القانونية المتبادلة ، وكذلك إنشاء مركز عربي لتعزيز مواجهة الجرائم السيبرانية ، ويتناول الفصل الرابع التعاون الدولي في مجال الأمن السيبراني من حيث تبادل الخبرات وتنسيق المواقف مع الدول الأخرى في إطار الاتفاقيات الدولية والإقليمية والثنائية المُصادق عليها ، فضلاً عن دعم الجهود المبذولة للتوصل إلى اتفاقية دولية شاملة للأمن السيبراني ، ويتناول الفصل الخامس تحديد وتشخيص الجرائم التي يعاقب عليها وفقاً لأحكام هذا القانون ، وصولاً إلى الفصل السادس والأخير، الذي يتناول بعض الأحكام الختامية . [٣٦]

مما تقدم يتبين لنا ان الجهود الدولية المذكورة اصبحت تشكل دعامة اساسية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية ، اذا لابد من تكثيف جميع الجهود وعلى المستوى الدولي والعربي لحث المنظمات الدولية والدول الاعضاء فيها لسن اتفاقية شاملة تتبنى حماية التجارة الالكترونية من الهجمات السيبرانية .

الفرع الثاني

القواعد والاجراءات الارشادية

بينا سابقا بأنه بالرغم من خطورة الهجمات السيبرانية على الاقتصاد العالمي و على التجارة الالكترونية على وجه التحديد ، الا انه لا توجد لحد الان اتفاقيات منظمة بين دول معينة تلزم اعضاءها على التصدي لهذه الهجمات او تقليل الاثار الناجمة عنها ، وان الجهود الدولية المبذولة في الوقت الحاضر لا تعد ان تتمثل بمجموعه من القواعد الارشادية التي يمكن ان تستعين بها الدول للاسترشاد بها لوضع التشريعات اللازمة ، وبالرغم من اهمية القواعد المذكورة

في تقديم العون والمساعدة للوصول الى قواعد قانونية وطنية ملزمة الا انها بطبيعة الحال يكون لها دور ارشادي فقط ، بمعنى انها لا تكون ملزمة لاي دولة من الدول للأخذ بها ، ومن هذا القبيل ما وضعته اللجنة الاقتصادية والاجتماعية لغربي اسيا (الأسكوا) مجموعة من القواعد القانونية الارشادية تهدف الى ايجاد مكنة قانونية لزيادة الوعي القانوني في الدول العربية حول الهجمات السيبرانية و مخاطرها [٣٧] ، وقد زاد اهتمام اللجنة المذكورة ومنذ عام ٢٠٠٧ بموضوع الهجمات المذكورة ، وقد قامت بالعديد من الانشطة القانونية وكان من ابرزها واهمها مشروع (تنسيق التشريعات السيبرانية لتحفيز المعرفة في المنطقة العربية) والذي كان تمويله من الامم المتحدة والذي بداء بتنفيذها في عام ٢٠٠٩ ، وقد تضمن مشروع ارشادات الأسكوا للتشريعات السيبرانية ستة محاور اساسية ، وهذه المحاور هي : محور التجارة الالكترونية وحماية المستهلك ، ومحور الاتصالات الالكترونية وحرية التعبير ، ومحور المعاملات الالكترونية والتوقيع الالكتروني ، ومحور معالجة البيانات ذات الطابع الشخصي ، ومحور الملكية الفكرية في المجال المعلوماتي والسيبراني ، واخيرا محور الجرائم السيبرانية ، وقد اعتمدت اللجنة المذكورة على العديد من التجارب القانونية الدولية السابقة وخصوصا تجربة المفوضية الاوربية في هذا المجال ، وبالرغم من اهمية الارشادات المذكورة وجوهرية المواضيع التي تنظمها وخصوصا فيما يتعلق بالتجارة الالكترونية وحماية المستهلك وكذلك فيما يتعلق بالجرائم السيبرانية وتحديدها [٣٨] ، الا انه ومن جانب اخر تفتقد الارشادات المذكورة الى وضع معالجة شاملة فيما يتعلق بحماية التجارة الالكترونية من مخاطر الهجوم السيبراني و هذا نقص لا بد من تلافيه ، وكذلك تعاني الارشادات المذكورة بعدم التناسق والربط في المواضيع المتناولة ونعتقد ان سبب ذلك هو ايجاد نوع من الشمولية والعموم لتحقيق اكبر قدر من الاستفاده من النصوص القانونية للدول التي تستعين بها ، ولكن العيوب المذكورة لا تشكل معوقا جوهريا في عدم اعتماد الارشادات المذكورة ومن جانبنا نقترح على المشرع العراقي ضرورة الافادة من الارشادات المذكورة في سن التشريعات اللازمة وعلى وجه الخصوص فيما يتعلق بالتجارة الالكترونية وحمايتها من الهجمات السيبرانية .

ومن الاجراءات والقواعد الاجرائية نذكر في هذا الصدد ايضا ما سنته اللجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات التابعة للاتحاد الافريقي في دورتها الثالثة جملة من

الاجراءات و التوصيات المتعلقة بالامن السيبراني ، ومن هذه الاجراءات التوصية بضرورة انتداب ثلاث خبراء عن كل دولة عضو في الاتحاد والبالغة (٤٢ دولة) لتدريبهم على استراتيجية الأمن السيبراني والتشريعات والقدرات السيبرانية [٣٩] ، وقد جاء في المحور التاسع والمتعلق بالبرامج والمشاريع الجارية في الاتحاد الافريقي وكان من ضمنها مجموعة اجراءات تتعلق بالامن السيبراني في الاتحاد وخصوصا في (الفقرة د) ، والتي تضمنت ضرورة اعتماد (اتفاقية مالابو ٢٠١٤) لبناء القدرات في مجال الأمن السيبراني ، بالتعاون مع الشركاء الرئيسيين والمجتمعات الاقتصادية الإقليمية والدول الأعضاء ، لتعزيز ثقافة الأمن السيبراني وبناء الأمان والثقة في استخدام تكنولوجيا المعلومات والاتصالات من قبل المواطنين الأفريقيين ولصالحهم ، وتوفير التوجيه بشأن سياسة الأمن السيبراني وتعزيز القدرات السيبرانية للدول الأعضاء بشأن منع الجريمة السيبرانية ، و الخصوصية في استخدام الإنترنت وحماية البيانات الشخصية ، وكذلك إعداد استراتيجية السيبرانية والتشريع السيبراني ، و إعداد آليات الاستجابة للحوادث مثل فرق التصدي للحوادث الحاسوبية ، و فرق الاستجابة للطوارئ الحاسوبية ، كما وضعت مفوضية الاتحاد الافريقي بالتعاون مع جمعية الانترنت مبادئ ارشادية يأمن البنية التحتية للانترنت وحماية البيانات الشخصية لمواطني افريقيا ، كما نشرت المفوضية المذكورة وبالتعاون مع وزارة الخارجية الامريكية في عام ٢٠١٦ تقريرا عن اتجاهات الامن السيبراني والجرائم السيبرانية في افريقيا [٤٠] ، وبالرغم من اهمية الاجراءات المذكورة والالتفات الى اهمية الامن السيبراني وتعزيز لحماية الاقتصاد الافريقي من مخاطرة الا انها لم تضع قواعد ومعالجات تشريعية لحماية الاقتصاد و التجارة الالكترونية من مخاطرة وهذا نقص لا بد من معالجته وخصوصا في الوقت الحاضر .

الخاتمة

ختاما وفي نهاية هذا البحث توصلنا الى النتائج والتوصيات والتي يمكن ان نوردها على النحو الاتي :

النتائج :

١- تبين لنا من خلال البحث انه لا يوجد مفهوما قانونيا على المستوى التشريعي والفقهي لوسائل حماية التجارة الالكترونية من مخاطر الهجمات السيبرانية وقد اوردنا مفهوما لها يتلخص بأنها

(برامج الكترونية ، يتم استخدامها بواسطة الانترنت ، من قبل جهات معينه ، بهدف السيطرة والتحكم في مواقع التجارة الالكترونية التابع لجهات أخرى ، مسببة

اضرارا جسيمة في تلك المواقع لتحقيق اغراض اقتصادية او سياسية او اجتماعية مختلفة) .

٢- تبين ان من خصائص الهجمات السيبرانية على التجارة الالكترونية تتمثل ببرامج الكترونية تستخدم عن طريق شبكة الانترنت ويمكن ان تستهدف الاقتصاد العالمي والتجارة الالكترونية على وجه الخصوص ، كما انها ظهرت في وقت متأخر نتيجة ازدياد التطور التكنلوجي وزيادة استخدام وسائل الاتصال الحديثة على مستوى عالمي كما انها لا تحتاج تكاليف مالية عالية مقارنة بالاضرار الجسيمة التي تحدثها .

٣- تبين لنا ايضا ان هناك انواع كثيرة من البرامج الالكترونية التي يمكن استخدامها في الهجمات السيبرانية كما ان لها طبيعة قانونية خاصة بها .

٤- تبين لنا ان هناك وسائل وطنية لحماية التجارة الالكترونية من الهجوم السيبراني وتتمثل هذه الوسائل بالتشريعات الوطنية النافذة والوسائل الاتفاقية التي يمكن ان تكون وسيله لحماية التجارة الالكترونية من مخاطر الهجمات المذكورة ، مع ملاحظة قصور التشريع العراقي في تنظيم الوسائل المذكورة .

٥- تبين لنا ان هنالك وسائل دولية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية وتتمثل بالجهود الدولية والقواعد والاجراءات الارشادية لحماية التجارة الالكترونية من مخاطر الهجمات السيبرانية مع ملاحظة عدم وجود اتفاقية دولية تقرر حماية التجارة الالكترونية من مخاطر الهجمات السيبرانية .

التوصيات :

١- نوصي المشرع العراقي بضرورة اجراء تعديل على قانون التجارة رقم (٣٠) لسنة ١٩٨٤ النافذ يتضمن احكام تتعلق بالتجارة الالكترونية وكذلك الوسائل القانونية اللازمة لحمايتها من مخاطر الهجمات السيبرانية .

٢- كذلك نوصي المشرع العراقي بضرورة سن التشريعات اللازمة التي تضمن انضمام العراق الى المنظمات الدولية والاتفاقيات المتعلقة بتوفير حماية لازمة للتجارة الالكترونية من مخاطر الهجمات السيبرانية .

٣- حث الفقه القانوني والباحثين في مجال التشريع التجاري بتسليط الضوء على وسائل حماية التجارة الالكترونية من مخاطر الهجمات السيبرانية كذلك نشر الثقافة الوطنية في المجتمع العراقي فيما يتعلق بالامن السيبراني من خلال اقامة الندوات التثقيفية والورش التوعوية في اطار الموضوع مدار البحث .

الهوامش والتعليقات:

(١) سمير عبد السميع الاودن – العقد الالكتروني – منشأة المعارف – مصر – ٢٠٠٥ – ص٢٥ .

(6) Perreault,William D. and Garthy, E. Jerome Mc (2003) . "Essentials of Marketing: Globalmanagerial Approach " McGraw– Hill , Inc., P 21 .

(٣) د. عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعه الجديدة، مصر، الإسكندرية ، ٢٠٠٨ ، ص١٨ .

(٤) د. حمودي محمد ناصر ، العقد الدولي الالكتروني المبرم عبر الانترنت ، دار الثقافة للنشر والتوزيع ، الطبعة الاولى ، الاردن ، عمان ، ٢٠١٢ ، ص ٨ .

(٥) ان المعنى اللغوي لكلمة السيبرانية غير موجود في معاجم اللغة العربية وهذه الكلمة مشتقة من كلمة اخرى هي سايبر وقد استخدم هذا المصطلح في وقت حديث نسبيا تحديدا في عام ١٩٤٨ من قبل عالم الرياضيات الامريكي (نوربرت وينر) في احدى مؤلفاته الشهيرة المعروف بأسم (علم التحكم الالي) ويرى البعض ان المعنى اللغوي للكلمة المذكورة هو (علم التحكم الاوتوماتيكي) او (علم الضبط) ، نقلا عن نور امين الموصلي – الهجمات السيبرانية في ضوء القانون الدولي الانساني – رسالة ماجستير – الجامعة الافتراضية السورية – ٢٠٢١ – ص٩ وما يليها .

(٦) احمد عبيس نعمة الفتلاوي – الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر) – الطبعة الاولى – منشورات زين الحقوقية – بيروت – لبنان – ٢٠١٨ – ص ١٦ .

(٧) احمد عبيس نعمة الفتلاوي – المصدر السابق – ص ١٧ .

(٨) لين هربت – النزاع السيبراني والقانون الدولي الانساني – مجلة اللجنة الدولية للصليب الاحمر – مجلد ٩٤ / ٨٨٦ – ٢٠١٢ – ص ٥١٥ والصفحات التي تليها .

(٩) د . عادل عبد الصادق – الاقتصاد الرقمي وتحديات السيادة السيبرانية – المركز العربي لابحاث الفضاء الالكتروني – مصر – القاهرة – ٢٠٢٠ – ص١٥ .

(١٠) احمد عبيس نعمة الفتلاوي – مصدر سابق – ص٢٥ .

(١١) مقال منشور على شبكة الويب العالمية من الموقع (www.it-pillars.com) ، تاريخ الزيارة ١٠-١١-٢٠٢١ .

(١٢) د. عادل عبد الصادق ، الاقتصاد الرقمي وتحديات السيادة السيبرانية ، المركز العربي لابحاث الفضاء الالكتروني ، جمهورية مصر العربية ، القاهرة ، ٢٠٢٠ ، ص٥٥ .

(١٣) د. ابو العلا علي ابو العلا النمر – المشكلات العملية والقانونية في التجارة الالكترونية – الطبعة ١ – دار ابو المجد – ٢٠٠٤ – ص ٧١ .

(١٤) د. مهند ابراهيم علي فندي – التنظيم القانوني لمناهضة الاحتكار – بحث منشور – مجلة الرافدين للحقوق – العدد ٣٣ – ٢٠٠٧ – ص ٧٥ .

(١٥) د. حسين محمد فتحي – الممارسات الاحتكارية واتحالفات التجارية لتقويض حرية التجارة والمنافسة (دراسة لنظام الانتيترست في النموذج الامريكي) – دار النهظة العربية – مصر – بدونن سنة نشر – ص ٢٥ ، ٣٠ .

(١٦) تشير الدراسات الاقتصادية الى زيادة اعتماد الدول على التجارة الالكترونية وسبب ذلك هو ازدياد الايرادات المالية العائدة من التجارة الالكترونية ، وتشير الدراسات في هذا الشأن ان التجارة الالكترونية بلغت في عام ١٩٩٧ نحو (٢٦ مليار دولار) اصبحت تشكل عائداتها ما يقارب (٥٠٠٠ مليار دولار) في عام ٢٠٠٩ وهي بزيادة مستمرة حتى وقتنا الحاضر . د. جواد كاظم البكري – دورات الاعمال في الاقتصاد الامريكي – اطروحة دكتوراه – غير منشورة – كلية الادارة والاقتصاد – جامعة الكوفة – ٢٠٠٥ – ص١٣٦ .

(١٧) د. عبد الله عبد الامير طه و اشواق عبد الرسول عبد الامير – اثر التوقيع الالكتروني في تحديد مشروعية التصرفات القانونية – بحث منشور – مجلة رسالة الحقوق – كلية القانون جامعة كربلاء – العدد الثالث – ٢٠١٦ – ص ١٨٠ .

١٨ – د. خضير مخيف فارس – النظام القانوني للتحويل الالكتروني للنقود – المركز القومي للاصدارات القانونية – الطبعة الاولى – ٢٠١٦ – ص ٥٥ وما بعدها .

(١٩) محمد احمد عبابنة – جرائم الحاسوب وابعادها الدولية – دار الثقافة – عمان – الطبعة الثالثة – ٢٠٢٠ – ص٢٣٠ وما يليها .

(٢٠) محمد امين الشوبكة – جرائم الحاسوب والانترنت (الجريمة المعلوماتية) – دار الثقافة للنشر والتوزيع – عمان – الاردن – ٢٠١٩ – ص٢٣٠ .

(٢١) اسامة المناعسة و جلال الزعبي و صايل الهواوشة – جرائم الحاسب الالي الانترنت (دراسة تحليلية مقارنة) – دار وائل للنشر – الاردن – عمان – ٢٠٢٠ – ص ٢٢٦ .

(٢٢) طلال ياسين العسي وعدي أحمد عناب – المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر– بحث منشور – مجلة الزرقاء للبحوث والدراسات الانسانية– المجلد١٩، العدد الاول– جامعة الزرقاء – الاردن، ٢٠١٩ .

(٢٣) د. رامي عبود – المحتور الرقمي العربي على الانترنت (نظرة على التخطيط الاستراتيجي العربي والعالمي) – العربي للنشر والتوزيع – مصر – ٢٠١٣ – ص ١١٦ .

(٢٤) د. عصمت عبد المجيد بكر – مصادر الالتزام في القانون المدني (دراسة مقارنة) – المكتبة القانونية – بغداد – ٢٠٠٧ – ص ١٥ .

(٢٥) محمد حسين منصور – مصدر سابق – ص١٢٧ .

(٢٦) عبد الفتاح بيومي حجازي – النظام القانوني لحماية الحكومة الالكترونية – دار الفكر الجامعي – الطبعة الاولى – الاسكندرية – ٢٠٠٣ – ص ١٥٥ .

(٢٧) نص المادة (١ / ٣ – ٦) باللغة الفرنسية :

(Le livreur communique à ses clients, au moins, ses nom, adresse postale et électronique, ainsi que le lieu et le numéro de son immatriculation commercial .)

(٢٨) محمد حسين منصور – مصدر سابق – ص١٠٩ .

(٢٩) احمد قاسم فرح – النظام القانوني لمقدمي خدمة الانترنت (دراسة تحليلية مقارنة) – رسالة ماجستير – جامعة ال البيت – كلية الدراسات الفقهية والقانونية – قسم الدراسات القانونية – ص١٤٠ .

(٣٠) لا يمكن انكار التوجه الدولي في محاولة التوصل الى اتفاقيات دولية تضع حدا للهجمات السيبرانية وتقلل الاثار الناتجة عنها قدر الامكان ، انظر في هذا الصدد د. لمى عبد الباقي محمود – مدى فاعلية الجهود الدولية والاقليمية في مواجهة جرائم الكمبيوتر والحد منها – بحث منشور – مجلة العلوم القانونية – المجلد ٢٨ – العدد ١ – ٢٠١٣ – ص٢٩٥ .

(٣١) د. عبد العزيز خنفوسي – قانون الدفع الالكتروني – مركز الكتاب الاكاديمي – الاردن – عمان – ٢٠١٨ – ص١٨ .

(٣٢) اشار الى ذلك كتاب قانون الاونستيرال النموذجي بشأن السجلات الالكترونية القابلة للتحويل الصادر عن لجنة الامم المتحدة للقانون التجاري الدولي – ٢٠١٧ – ص ١٠ وما يليها – متاح على الرابط: (https://books.google.iq/books?id=AfP-DwAAQBAJ&hl=ar&source=gbs_navlinks_s)

(٣٣) لجنة الامم المتحدة للقانون التجاري الدولي – الدورة التاسعة والثلاثون – نيويورك – ١٩حزيران ، ٧ تموز ٢٠٠٦ – ص٢٢ . متاح على الموقع الالكتروني (https://undocs.org/pdf?symbol=ar/A/CN.9/604)

(٣٤) المنظمة العالمية للملكية الفكرية – الجمعية العامة للويبو – الدورة الرابعة والعشرين – جنيف – ١٩٩٩ – ص ٣ . متاح على الرابط (https://www.wipo.int/edocs/mdocs/govbody/ar/wo_ga_24/wo_ga_24_2.pdf)

(٣٥) د. حسيب الياس حديد – الملكية الفكرية والتجارة الالكترونية – مقال منشور على شبكة الانترنت – متاح في الموقع : (http://www.alnoor.se/article.asp?id=207864) تاريخ الزيارة ٢٠٢٢/١/٩ .

(٣٦) د. عادل عبد الصادق – مصدر سابق – ص ٣٩ ، كذلك اشار الى المضمون اعلاه مقال منشور على الانترنت ومتاح على الموقع (https://www.almasryalyoum.com/news/details/2453786) .

(٣٧) اللجنة الاقتصادية والاجتماعية لغربي اسيا (الاسكوا) – ارشادات الاسكوا للتشريعات السيبرانية (مشروع تنسيق التشريعات السيبرانية في الدول العربية) – ٢٠١٢ – ص ٥ – متاحة على الرابط : (https://archive.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf) .

(٣٨) المصدر نفسه – ص١٢٢ .

(٣٩) الاتحاد الافريقي – اللجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات – الدورة الثالثة – مصر – شرم الشيخ – ٢٠١٩ – متاح على الرابط (https://au.int/sites/default/files/ne

wsevents/reports/37470-rp-draft_experts_report_a.doc) .

(٤٠) المصدر نفسه – ص ٢٢ .

القوانين

١- قانون التجارة العراقي رقم (٣٠) لسنة ١٩٨٤

٢- قانون المنافسة ومنع الاحتكار العراقي رقم ١٤ لسنة ٢٠١٠

٣- قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢

٤- قانون الامن السيبراني الاردني رقم (١٦) لسنة ٢٠١٩

٥- قانون الامن السيبراني المغربي رقم (٠٥.٢٠) لسنة ٢٠٢٠

٦- قانون الاونستيرال النموذجي لسنة ١٩٩٦

المذكرات والارشادات القانونية

١- المذكرة الصادرة من لجنة الامم المتحدة للقانون التجاري الدولي في نيويورك لعام ٢٠٠٦

٢- المذكرة الصادرة عن المدير العام للجمعية العامة للويبو ١٩٩٩

٣- ارشادات الالسكوا للتشريعات السيبرانية لسنة ٢٠٠٩

٤- ارشادات اللجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات التابعة للاتحاد الافريقي لسنة ٢٠١٩