مخاطر التعامل الالكتروني وآليات التعامل معها

قريقر فتيحة
أستاذ محاضر ب
جامعة زيان عاشور (الجلفة)

ملخص : أصبح الفضاء الالكتروني ساحة غير محددة الأبعاد ،يحكمها التطور التكنولوجي و السرعة في التعاملات ،و أكثر من ذلك أصبح هذا الفضاء مجالا لمختلف التبادلات ، وبالتبعية رافق هذا التطور مخاطر تفوق المزايا مثل الغش و الاحتيال و السرقة والتخريب باستعمال الانترنيت ، هذه الأفعال تمس الإفراد و المؤسسات كالبنوك و الشركات و المؤسسات الحكومية ، وتقف التشريعات عاجزة عن مواكبة هذا التطور ، وحتى قانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لم ينص إلا على الجرائم التقنية ،لذلك يجب ان تواكب التشريعات هذا التطور لتفادي المخاطر التي تنتج عنه سواء الوطنية أو الدولية ،كما يجب التنبيه الى مخاطر التعامل الالكتروني من طرف الأشخاص و رقابة المحتوى الذي تقدمها الانترنيت بمختلف صوره

Abstract :Electronic space has become a non-dimensional arena dominated by technological development and speed in dealing. Moreover, this space has become an area of various exchanges. This development has been accompanied by risks that exceed advantages such as fraud, fraud, theft and sabotage through the Internet. Such as banks, companies and government institutions, and legislation is unable to keep up with this development. Even Law 90-04 on the special rules for the prevention and control of crimes related to information and communication technologies provides only for technical crimes ; Therefore, the legislations must keep pace with this development in order to avoid the risks that result fromit, whether national or international, and the dangers of electronic dealing by persons and the control of the content provided by the Internet in various forms

الكلمات المفتاحية :تعاملات الكترونية -تصيد الكتروني -متتبعوا التفضيلات -أسماء النطاقات – انخفاض الجودة -مخاطر تكنولوجية – مخاطر معلومية -قراصنة انترنيت -خرق خصوصية التعامل – نسارع تكنولوجي

مقدمة

أحدثت التطورات في مجال تكنولوجيا المعلومات والاتصالات تغييرا في طبيعة ونمط الحياة الاقتصادية لكافة المستهلكين سواء في الدول المتقدمة أو النامية ، فقد أصبح بإمكان المستهلك اليوم أن يقوم بما يشاء من تعاملات مهما كان نوعها مدنية أو تجارية عن طريق الانترنيت، وأصبح بإمكانه أن يعمل ويتسوق ويدفع إلكترونيا عن طريق الحاسب،فإذ كان للتطور الإلكتروني

الكبير والسريع الأثر الواضح على عملية ربط العالم بشبكات إلكترونية جعلت منه -أي العالم -قرية كونية أو خلية مترابطة بشكل قوي فإن هذه الشبكة بمجرد ظهورها رافقتها موجات كبيرة من الخروقات والاعتداءات غير المتوقعة، الأمر الذي تسبب في تطور أشكال وصور الجرائم وأكثرها الغش والاحتيال والجوسسة

من صور التعامل الالكتروني شراء المنتجات عن طريق الإنترنت كالكتب والمجلات، والأفلام والبرامج ،ومعدات الكمبيوتر والأجهزة المختلفة والمقتنيات الشخصية والعائلية،بالتسوق من المواقع الرائدة كموقع أمازون واباي ، كما برزت حالات أكثر تطورا تمثلت في قيام العديد من المستهلكين بشراء السيارات وحتى المنازل من خلال الاتصال المباشر الكترونيا. وظهر إنشاء العديد من مراكز المزادات العلنية، التي تسعى لاستخدام خاصية الاتصال المباشر لتمكين العملاء من المشاركة في التجارة والمضاربة بشكل مباشر، لصفقات قد تعقد بالملايين أو المليارات من النقود. وهناك عمليات الكترونية أخرى حديثة تتمثل في استثمار العملة في إطار بنوك افتراضية عالمية تشهد إقبالا كبيرا من قبل المستهلك الذي لا توجد على الشبكة العنكبوتية معايير تضبط أهليته أمام كم هائل من وسائل الترويج التدليسية في أغلبها ما يجعل مخاطر التعامل الالكتروني فادحة مهما قورنت بمزاياه نتيجة وجود إمكانيات واسعة ومتطورة للغش أو الاحتيال في التعامل من خلال الإنترنت.إذ أن العديد من المستهلكين والمؤسسات التجارية والحكومية في العالم صارت مستهدفة وعرضة لهذه الممارسات اللامشروعة، وأيضا لأشكال جديدة من الغش التجاري الإلكتروني،الذي أصبح يطال حتى المصارف المؤسسات المالية، والصناعية، والجامعية والحكومية مع تزايد حاد في قيمة الخسائر المادية وحتى الأمنية،وبالتالي تتدرج هذه التعاملات الالكترونية أهمية وأثرا وخطورة باعتبار موضوعها وأفرادها ،حيث يتم نقل السوق الفعلية الى سوق افتراضية يجسد فيها المتعاقد عرضه سلعته أو خدمته من خلال موقع ترويجي آمن أو غير آمن ، في ظل تفاوت كبير بين قدرة العارض المحترف والمتلقي والمستهلك ، مما حرك الجهات الفاعلة دوليا ومحليا ،لتظهر محاولات نشطة تبحث عن الوسائل والأساليب الكفيلة بالحد من تلك الخروقات والاعتداءات، ومن ثم مكافحة الغش والاحتيال المرافق لها

لذلك ستعنى هذه الدراسة ببحث مخاطر التعامل الالكتروني وكيفيات التعامل معها وفق خطة عمل من مبحثين يخصص المبحث الأول لدراسة مخاطر التعاملات الالكترونية أنواعها ومظاهرها ،بينما المبحث الثاني يخصص لآليات مكافحتها سواء التقنية أو التثقيفية أو القانونية

المبحث الأول : مخاطر التعاملات الالكترونية

حتى يمكن لنا ان نحيط بهذه المخاطر سنتطرق لمظاهرها في مطلب أول ثم نعمد الى تحديد أنواعها في مطلب ثان

المطلب الأول : مظاهر مخاطر التعامل الالكتروني

يتعرض المستهلك عند قيامه بالتعامل الالكتروني لمخاطر تتفاوت نوعيتها بناء على مجموعة من العوامل، وأهمها طبيعة المنتج إذا كان سلعة أو خدمة، وطبيعة المستهلك، ومدى توافر المعلومات، ففي حالة الخدمة تكون المخاطر عالية مقارنه بالسلعة، وهذه المخاطر[1] تنبعث من تقنية التعامل عبر الانترنيت وتتخذ لها صورا كثيرة منها :

أولا-مخاطر أساسها متتبعو التفضيلات Track Préférences:

تحدث هذه المخاطر على مستوى الشخص الذي يقوم بتجميع البيانات لتكوين قاعدة بيانات عن مستخدمي الانترنت يستطيع من خلالها فهم سلوكيات واتجاهات هؤلاء الأشخاص والتي عادة ما تستخدمها المواقع التجارية فيتتبع سلوكيات واتجاهات المتسوقين في الموقع

ان عملية التتبع هذه ليست سيئة بحد ذاتها بقدر ما هي مفيدة للمتسوق المستهلك حيث يستفيد من تقديم العروض التي تتناسب مع ذوقه كمتسوق بناء على ما تم تجميعه من بيانات عن تفضيلات الزبائن، ولكن تظهر المشكلة عند الاستخدام السيء لهذه البيانات كبيعها لشركات التسويق أو شركات أخرى.ليتم توجيه رضا المستهلك لمنتوج معين وخدمة معينة ،دون علم المستهلك بأنه منقاد ومسلوب الإرادة وموجه .

ثانيا:التصيد الالكتروني Phishing والاختطاف[2]Hijacking

تتحقق هذه الحالة باستخدام تقنيات مختلفة لتوجيه الضحايا الى مواقع أخرى غير التي يريدونها مثل توجيه الشخص الى مواقع وهمية تكون مشابهة تماما لموقع الكتروني مشهور أو معروف لدى الضحية من خلال رسالة الكترونية لعروض وهمية ولكنها مغرية .

ثالثا: تسميم نظام أسماء النطاقات DNS Poisoning

ويحدث ذلك من خلال اختراق نظام أسماء النطاقات لخادم الشبكة المحلية وهذه الطريقة من أخطر طرق "الاختطاف" حيث يمكن ان تكتب العنوان الالكتروني المرغوب بشكل صحيح ومع ذلك يتم أخذك الى موقع الكتروني آخر كما حدث في الموقع التجاري المعروف ebay ألمانيا والذي قام من خلاله مراهق بتحويل عنوان الموقع الى موقع آخر ، وبالرغم من صعوبة تفادي هذا الأسلوب إلا أنه يمكن تقليل مخاطره من خلال التأكد من ان الموقع المرغوب يحتوي على شهادة رقمية صالحة .

رابعا: الاحتيال عبر الانترنت Online Fraud[3]

هذا النوع من المخاطر يتخذ له أساليب متنوعة يتم فيها الاحتيال بعدة أوجه في عملية التبادل التجاري ومنها:

-1 **السلعة غير موجودة** Goods Do not Exist :

حيث يتم التعاقد مع شخص أو شركة وهمية لشراء بضاعة تم الاتفاق عليها ودفع مبلغ معين دون إمكانية الحصول على هذه البضاعة أبدا حيث أنها لم تكن موجودة من الأساس.

-2 **إنخفاض الجودة** Low Quality:

هذا النوع شائع في التجارة الالكترونية أمام صعوبة تحديد جودة البضاعة بدقة وبالتالي هامش الاختلاف في تحديد جودة السلعة يكون كبيرا كذلك إمكانية الحصول على بضاعة مختلفة تماما عما تم الاتفاق عليه ، ولهذا في كثير من الأحيان يتم استخدام بعض الشركات الوسيطية لإجراء عملية البيع مثل PayPal الآمنة لضمان إتمام الصفقة بشكل مقبول.

-3 **رسائل الاحتيال النيجيرية** NigerianScam :

وهي من أشهر وأكثر طرق الاحتيال شيوعا على الانترنت حيث أن أي مستخدم للانترنت تعدى استخدامه لها 8-6 أشهر فإنه على الأرجح قد صادف رسالة احتيالية من هذا النوع. وهي كثيرة التنوع و المصادر ،وأحدث محاولات النصب من هذا النوع وهي

إرسال رسالة الكترونية من شخص يدعي انه إقطاعي كبير واسمه مايكل كومالو ويدعي انه من زيمبابوي وقد صادر الرئيس روبرت موغابي كل أمواله إلا أن لديه رصيد في البنك في جنوب أفريقيا وهو على استعداد ليعطيك 24 مليون دولار إذا أرسلت له مبلغ 200 ألف دولار، أو ما تمارسه مؤسسات دولية استثمارية ترويجية للسلع ،او البنوك الوهمية بمقرات إقامة مزورة بإقناع الأشخاص للانتماء إليها بمقابل مادي يتم استرداده مضاعفا ، لتتم الصفقة والتحويل المالي الكترونيا وبالتالي عملية النصب والاحتيال .

المطلب الثاني: أنواع المخاطر[4]

كل تكنولوجيا حديثه ورغم إيجابياتها الكثيرة إلا أن سلبياتها كثيرة كذلك، وفي حالتنا هذه سلبياتها تتجاوز الحد لتصنف بالخطيرة جدا، وفي حالة عدم التمكن من تحجيم تلك السلبيات والسيطرة عليها، ستكون النتائج كارثية ،للأسف إن مخاطر التجارة الإلكترونية كثيرة ومتعددة، وليس من السهل حصرها، خصوصا تكنولوجيا التجارة الإلكترونية التي تتسارع مع التغير والتطور، الذي تواكبه مخاطر جديدة أكيدة، ويكمن الخطر الرئيسي في التجارة الإلكترونية في إمكانية اختراق الغير للمعلومات الخاصة لكل من المستهلك والشركات. وهذه المخاطر تصنف ضمن نوعين رئيسيين

أولا : مخاطر تكنولوجية معلوماتية مألوفة ونسبية يمكن تداركها

هي تلك المخاطر التي يمكن اكتشافها والمقصود هنا بأن المتعامل المستهلك الشخص الطبيعي أو المعنوي بوصفه شركة وبوجود خبراء مختصين لديها قد تتمكن من اصطياد بعض الاختراقات في أنظمتها والتعامل معها في الوقت المناسب، ومن أشهر هذه الاختراقات

-1 **المخاطر التكنولوجية**:وهي المخاطر التي قد تنتج عن استعمال المستهلك للتكنولوجيا كتعرض الجهاز للتخريب بسبب الفيروسات، فالفيروسات الرقمية المعروفة وفي وجود نظام حماية مناسب، يستطيع نظام الشركة الحمائي تتبعها واصطياد هذه الفيروسات المعروفة له بشكل مسبق والقضاء عليها.

-2**المخاطر المعلوماتية**: هي تلك المخاطر المتعلقة بأمن المعلومات، ويقصد بها الخطر المصاحب للمعلومات الخاطئة التي تقدَّم عن طريق الإنترنت، وتشمل مخاطر استخدام معلومات مضللة وغير دقيقة وغير ملائمة في اتخاذ القرارات، وتشير إلى إمكانية أن يقوم شخص ما بالتلاعب في تنسيق بيئة معلومات موقع التسوق، من خلال معلومات غير متناسقة، وغير متماثلة، وخادعة للمتسوق عبر الإنترنت وذلك للحصول على معلومات المتسوِّق بشتَّى الطرق؛ لتستخدم ضده، كأن يعرف تاريخ ميلاده الذي لربما يكون كلمة السر المستخدمة، أو أن يقوم باستخدام مواقع مزيفة لاصطياد المتسوق، وهو ما يسمى ب (Phishing) ، أو أن يقوم المخترق بإرسال بريد إلكتروني إلى المتسوق يطلب منه تحديث بياناته عن طريق رابط يقود إلى موقع المخترق المزيف، وليس إلى موقع المتجر الحقيقي.

-3**قراصنة الإنترنت الهواة**[5]: يعتمد قراصنة الإنترنت في اختراقاتهم لنظام الشركة على معلومات ورموز دخول معينة، وفي حالة وجود أكثر من مستخدم لنظام الشركة قد يستطيع القرصان تتبع عملية الدخول والحصول من ذاكرة النظام على تلك المعلومات واستخدامها، ولهذا فإن كانت الشركة تستخدم آلية تغير تلك الرموز بشكل دوري ومسح الذاكرة المعنية بواسطة

خبرائها فستتمكن من تحجيم الاختراقات.ويمكن ذكر بعض صورها

-4**الهجمات المتعمدة** :Intentional Attacks والتي تتم إما بواسطة قراصنة الإنترنت، أو منافسي الشركة لغرض الوصول إلى المعلومات السرية للشركة، كأرقام بطاقات اعتماد الزبائن مثلا والمعلومات السرية بالزبائن، وحجم المبيعات، وأمور كثيرة قد يصعب حصرها

-5**خرق خصوصية التعامل**[6]: The Privacy Debate، تعتبر التعاملات الإلكترونية التي تتم بين الأفراد والشركة ذات طابع معلوماتي مهم جدا، من منطلق أنها تحفظ على ذاكرة النظام الرقمية، وهي معلومات قيمة جدا، وبالتالي إن تمكن أحد من معرفتها أو حتى تتبعها،كتتبع رقم بطاقة اعتماد العميل الذي سيشعر بأن خصوصيته قد تم اختراقها وبالتالي سيفقد الثقة بالشركة التي تعامل معها من منطلق أنها لم تتمكن من حماية خصوصيته

-6**فقدان الثقة**Loss of Trust: المقصود هنا فقدان ثقة الشركة بمعلومات عميلها، فمن المتعارف عليه بأن العميل يستخدم ما يسمى التوقيع الرقمي Digital Signature الخاص به لدخول نظام الشركة لإتمام عمليته المرغوب فيها، فكيف هو الحال إذا تمكن الشخص غير الصحيح من الدخول مستخدما توقيع العميل.

-7**فشل عملية التحويل** : Transmission Failures، رغم أن عملية الشراء الإلكترونية تتم بسرعة كبيرة جدا، إلا أنها عرضة لخطر فشل عملية التحويل، لأن عملية الشراء عبر التجارة الإلكترونية تتم بواسطة عدة خطوات، كأن يبدأ المستهلك بملء النموذج الابتدائي لعملية الشراء، ومن ثم الانتقال لنموذج ملء بيانات بطاقة الاعتماد، وخطوات أخرى قد تكون ضرورية وفقا لسياسات الشركة، وفي كل مرحلة تفتح صفحة جديدة عبر موقع الشركة ولأسباب تقنية أو أخرى قد تفشل إحدى الخطوات، وهنا ستظهر مشكلة جديدة وهي عدم التأكد من إتمام العملية

ثانيا : مخاطر تكنولوجية معلوماتية لا يمكن اكتشافها ويصعب تتبعها[7]

يقصد بها أن الاختراقات قد تتم دون سابق دراية بها في غياب التنبؤ المسبق بها والدراسات التقنية الحديثة في مجال التكنولوجيا الالكترونية ،وهذه الخروقات تحدث إما بسبب جدتها وحداثتها أو جهل الشركة بها، وتنتج عما يلي من الأسباب

-1**فيروسات غير معروفة** : رغم وجود أنظمة حماية من الفيروسات على أنظمة المؤسسة،إلا أن هنالك فيروسات غير معروفة بعد للنظام الحمائي للمؤسسة قد تتمكن من دخول نظام الشبكة وإحداث تلف كبير دون الشعور به إلا بعد فوات الأوان، كما حدث في عام 2000 عندما استطاع أحد الهواة اختراع فيروس I Love you، والذي تمكن من إيقاع خسائر عصية عن الحصر في ذلك الوقت

-2**قراصنة انترنيت ذوي خبرة عالية**: تعد هذه الحالة من أكبر المشاكل التي تواجهها المؤسسات،لأن قراصنة بعضهم يملك خبرة ومهارة تفوق كثيرا من المتخصصين، تمكنهم وفي كثير من الأحيان من اختراق أنظمة المؤسسة دون أن يشعر بهم ،وغالبا تتم جرائمهم دون اكتشاف.

-3**التسارع التكنولوجي**[8]: يصعب في كثير من الأحيان مواكبة التسارع التكنولوجي على المؤسسات في مجال الإنترنت بشكل عام والتجارة الإلكترونية بشكل خاص، مما يجعل التكنولوجيا التي تستخدمها المؤسسة قديمة جدا عاجزة عن التنبؤ والتعامل في

حينه وتصور الحلول المناسبة ومن صور هذه المخاطر

-غياب التوثيق :Lack of Authentication، إذا كانت التجارة التقليدية تعرف نظام توثيق الصفقة بأوراق ثبوتيه موقعة من قبل الأشخاص أصحاب السلطة والقرار فعليا حضوريا ،أو بواسطة اتصال شخصي ومباشر بين البائع والمشتري، غير أنه في التجارة تنعدم كليا هذه الآلية، مما يزيد من احتمالية التعامل مع الشخص غير الصحيح.

-صعوبة تعقب الاختراقات التي تتم عبر شبكة الإنترنت: يعد نظام التجارة الإلكترونية بيئة مثالية للسرقات والتلاعب وإخفاء آثار الجريمة بشكل متقن منقطع النظير

-إمكانية الدخول من عدة أماكن إن المتعامل عبر الإنترنت لا يحتاج إلى مكان محدد لدخول الشبكة، فأي شخص يمكنه الدخول إلى الشبكة من أي مكان يتوفر به جهاز كمبيوتر وخط اتصال، كمقاهي الإنترنت ومختبرات الجامعات والمدارس.

-سرعة العملية لا يحتاج المخترق المحترف إلى أكثر من بضع دقائق لاختراق موقع معين والتلاعب به ومغادرة الموقع دون أن يتم تعقبه

-تباعد المسافات :الشائع في عمليات الاختراق الالكتروني أنها تتم من أماكن تبعد آلاف الكيلومترات وفي بلد آخر، فشبكة الإنترنت صممت بشكل عالمي فلا يمكن معرفة ماهية المخترق أو مكانه إلا بعد قوات الأوان .

-إمكانية إتلاف بيانات جهاز الكمبيوتر:في حالة شعور أي مخترق بإمكانية تعقبه يستطيع إتلاف بيانات جهازه بضغطة زر بسيطة، مما يجعل عملية تعقبه عديمة الجدوى.

-عدم الإبلاغ عن الاختراقات :فهناك الكثير من المؤسسات لا تبلغ عن الاختراقات التي تعرضت لها أنظمتها، خوفا من فقدان عملائها وتفضل تحمل خسائر كبيرة عوضا عن فقدان الثقة بها، وخير دليل على ذلك عملية الاختراق التي تمت لبنك City Bank في مطلع عام 2001 من قبل شخص بروسيا كبدته خسائر قدرت بعشرة ملايين دولار والتي لغاية هذه اللحظة ترفض الإقرار بها

-حركية ونشاط الشركات الوهمية : تزداد أهمية الحذر من التسويق غير الصادق الذي لا يحمل مضموناً حقيقيا،لأنه من السهل نشر هذه المعلومة عن الشركة عبر الإنترنت فقد يتعرض الزبون لحالة خداع من هذه الشركة الوهمية أو غير الملتزمة، مثل التعامل ببطاقة ائتمان مسروقة أو تقديم ضمانات خدمات ما بعد التصنيع دون الالتزام بالتنفيذ الفعلي،أو عن طريق ادعاء صفة المصرف لتجميع الأموال وادعاء استثمارها في نشاطات تجارية وتقديم إغراءات بالحصول نسب من الأرباح التجارية، وغير ذلك من الأساليب.

المبحث الثاني: آليات حماية المستهلك الكترونيا

بدأ مفهوم الحماية الإلكترونية في التبلور خاصة بعد اتساع مستخدمي الإنترنت في العالم[9]، وهو ما يعني الحفاظ على حقوق المتلقي لمواضيع التقنية كمستهلك، وحمايته من الغش أو الاحتيال في صورة شراء بضائع مغشوشة باستخدام أدوات الويب التي تستطيع الوصول لكل مكان وتمارس تأثيرا يتجاوز بكثير الأدوات التقليدية،لذلك تتخذ الحماية صورا مختلفة هي الحماية التثقيفية والتقنية (مطلب اول) وتليها الحماية القانونية (مطلب ثان)

المطلب الأول :الحماية التثقيفية والتقنية

لعل الحماية التثقيفية تكون أكثر أهمية لأنها سابقة للوقوع في الخطر عموما أو متزامنة معه لذلك ستكون الأولى بالدراسة لتعقبه الحماية التقنية والتي تركز على تأمين استعمال الجهاز الالكتروني

أولا : الحماية التثقيفية[10]

تقوم هذه الحماية على رفع وعى المستهلك وتبصيره بحقوقه وواجباته، بما يضبط قراراته ويوجهه إلى ما يحقق له القدر الأكبر من الحماية،حيث تقوم مواقع حماية المستهلك بتقديم خدمات التوعية للمستهلك للوقاية من الوقوع في مخاطر التجارة الإلكترونية، وذلك من خلال منتديات لتبادل الخبرات أون لاين، والقيام بعرض قصص واقعية لتجارب المشترين مع السلع الرديئة، وتحديث مستمر لنشرات إخبارية تتضمن حوادث الغش التجاري مدعمة بآراء الخبراء والمتخصصين، كما توفر هذه المواقع أيضا خدمة استقبال الشكاوى عبر البريد الإلكتروني من خلال ما يسمى مركز الشكاوى، وتفرد بعض الصفحات التي تحتوي على المعلومات التي تساعد المستهلك على تجنب الوقوع في احتيال أو غش، وترتبط معظم الاحتيالات في التعاملات التجارية التي تتم عبر الإنترنت بممارسات التضليل والخداع التي تحاكي وتعكس الأنشطة المشابهة التي تحدث باستخدام التقنيات الورقية التقليدية، ويتمتع المحتالون على الإنترنت بالقدرة على الوصول المباشر للملايين من الضحايا في العالم، وبأقل تكلفة ممكنة، على سبيل المثال مكائد المكافآت العالية، مثل: مكائد الاحتيال الهرمي Pyramid scheme واحتيال Ponzi التي تستخدم سلسة خطابات ورسائل إلكترونية، ومكائد فرص التجارة، ومزادات الاحتيال والجوائز الخادعة والاستثمارات النقدية ببنوك وهمية .

أمام هذا الخطر الداهم يتعين نشر ثقافة الحماية الالكترونية على مختلف الفئات المستهلكة للنطاق الالكتروني من كل الجهات ذات الصلة وذلك مثلا ب:

-1عدم السماح للأطفال باستخدام الشبكة دون إشراف[11] ،إذ يتعين أن يكون استعمال الطفل للانترنيت موجها وتحت رقابة وإشراف، فلو كان الأطفال تحت الرعاية والرقابة الضرورية لما أقدم بعضهم على الانتحار جراء استخدامهم الكترونيا وسلب إرادتهم و دفعهم للانتحار دون التمكن من تعقب الفاعل او إيقاف رسائله ، هذا من ناحية ومن ناحية أخرى فإن الطفل قد يقدم على إعطاء جميع المعلومات الشخصية عن اهله وبحسن نية، والتي تكون تمكن الغير من اختراق الجهاز بسهولة ودون عناء .

-2استخدم المواقع المرخصة والمقصود بالمواقع المرخصة، تلك المواقع التي تم تقييمها وتأهيلها من قبل طرف ثالث مؤهل بأمور الحماية، وهذه المواقع تكون ممهورة بتوقيع إلكتروني خاص من طرف ثالث مهني متخصص معتمد دوليا، كمعهد المحاسبين القانونيين الأمريكي

-3 استخدام برنامج آمن للدخول إلى شبكة الإنترنت : من المعروف أن كل جهاز كمبيوتر يحتوي على برنامج خاص للدخول إلى شبكة الإنترنت، وفي الغالب، فإن هذه البرامج تحتوي على آليات معينة تحفظ في ذاكرة الجهاز جميع المعلومات التي تم تداولها في الشبكة من خلاله وفي كثير من الأحيان يستطيع المخترق وعبر الإنترنت الدخول لذاكرة هذا البرنامج والحصول على جميع المعلومات الخاصة بالمستخدم ودون أن يستشعر بذلك، ولهذا ينصح بشراء برنامج خاص يتمتع بحماية عالية لمنع أي مخترق

من الدخول إلى ذاكرته

ثانيا : الحماية التقنية

تكون هذه الحماية منصبة على المعاملات المالية من جهة وعلى جهاز الحاسب من جهة أخرى

-1حماية المعاملات المالية الإلكترونية[12]:و لها عدة نطاقات نذكر منها حافظة النقود الإلكترونية والافتراضية التي يقصد بها تجميع وحدات للقيمة وذلك في أداة مستقلة عن الحسابات البنكية تعرف بحافظة النقود الإلكترونية وحافظة النقود الافتراضية،فبالنسبة للأولى فإنها تشحن مسبقا برصيد مالي ويتم تسجيل هذا الرصيد المالي في بطاقة أما بالنسبة لحافظة النقود الافتراضية فإنها تشحن برصيد مالي على القرص الصلب لجهاز الكمبيوتر الخاص الذي يستعمل الشبكة وبالتالي فقطع النقود أو النقود الافتراضية تمثل من الناحية الفنية تلك المعاملات المختزلة على ذاكرة جهاز الكمبيوتر ويستطيع بذلك العميل الذي يرغب في التعامل بهذه النقود أن يحصل من أحد البنوك أو أحد المؤسسات الوسيطة على رخصة تسمح له باستعمال النقود الإلكترونية بالمقابل الذي يتفق عليه ويكون بدءا مفتاح عام وخاصمن أجل تأمين معاملاته وتحققها والهدف من هذه التقنية هو تفادي اختراق البيانات التي يتم تداولها عبر شبكة الإنترنت والتغلب على إمكان استخدامها غير المشروع من قبل الغير. لأنه بهذه التقنية يصبح لوحدات القيمة الإلكترونية ذاتية مستقلة حيث يمكن نقلها من محفظة إلكترونية إلى أخرى على نحو يؤدي إلى الوفاء من قبل المدين بمجرد نقل هذه الرموز الإلكترونية ويمكن لمتلقي هذا الوفاء على حافظة إلكترونية أن يقوم بتحويل هذه النقود الإلكترونية إلى نقود رقمية من خلال البنك المصدر لها .ومن سلبيات هذه التقنية فرض عمولات كبيرة على البنوك المتعاملة بهذا النظام مقابل تحويلات النقود الإلكترونية إلى نقود حقيقية ، كما أن تطور نظام النقد الإلكتروني ينطوي على تهديد احتكار مركزية عملية إصدار النقود .كما أن عدم إمكانية تتبع العمليات التي تتم من خلال النقود الإلكترونية يخشى منه ازدياد فرص التهرب الضريبي وربما يفتح بابا جديدا لعمليات غسل الأموال كما أن استخدام هذه التقنية لا يخلو من مخاطر فنية متمثلة في إمكانية تعطل القرص الصلب وضياع ما عليه من مبالغ نقدية إلكترونية

2: حماية المواقع الخاصة بالإنترنت[13]

تتجلى حماية المواقع الخاصة بالإنترنت ممن خلال نظام التشفير ونظام الجدران النارية

2-1 التشفير هو إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات ووسائل تحويل المعلومات تهدف الى إخفاء محتواها والحيلولة دون تعديلها أو استخدامها غير المشروع. ويعرف كذلك بأنه عملية تحويل المعلومات إلى رموز غير مفهومة تبدو غير ذات معنى بحيث يمنع الأشخاص غير المرخص لهم من الاضطلاع على المعلومة أو فهمها فعملية التشفير تنطوي على تحويل النصوص العادية أو نصوص مشفرة ومن المعلوم أن الإنترنت تشكل الوسيط الأضخم لنقل المعلومات ولابد من نقل المعلومات الحساسة للحركات المالية والتواقيع الإلكترونية بصيغة مشفرة للحفاظ على سلامتها من عبث القراصنة

يسمح نظام التشفير بتلافي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية حيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها ، فالتشفير يساعد على حفظ سرية المعلومات والتوقيع الإلكتروني الذي يتطلب الحفاظ على الأرقام والرموز لحمايته داخل التجارة الإلكترونية كما أن الغاية من

التشفير هي إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها حتى لا يستطيع أي شخص الاطلاع على هذه البيانات دون المتعاقدين أو من يصرح له قانونا بذلك ،ويهدف التشفير إلى منع الغير من التقاط الرسائل أو المعلومات ومن ثم منع وصولها مشوهة للطرف الآخر في المعاملات التجارية على نحو يعرقلها

2-2 : الجدران النارية تعتبر وسيلة لحماية المحتوى تستعمل لحماية الشبكات الخاصة من دخولها، وتمنع الوصول الغير مشروع للشبكة فتحمي وحدات التحكم والإرسال في الإنترنت وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة من هذه المشكلات ذلك أن الانترنيت تعمل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو لمجموعة من المضيفين ليرى ويسمع كل منهم الآخر ويوفر الهيكل الإذاعي المتكامل على الإنترنت عن طريق برنامج يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الإنترنت ولكن في ظل الجدران النارية يتم توفير الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها،وتسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها إلى الإنترنت أو قدومها منها وتسجيل كافة المعلومات عن حركة المرور والدخول والخروج

المطلب الثاني :الحماية القانونية للتعاملات الالكترونية

تتخذ هذه الحماية مظاهر مختلفة فهي حماية مدنية وحماية جنائية

أولا :الحماية المدنية [14]

تتمثل هذه الحماية في اعتماد وسائل محددة وتقدير مسؤولية للخروقات وفق القواعد العامة لذلك نركز على الحماية من خلال التزام شكلية معينة اقتضتها المنظومة التشريعية

1: الكتابة الإلكترونية

تلعب الكتابة الإلكترونية دورا مهما وتحتل الصدارة في الإثبات عن الوسائل الأخرى في الحفاظ على المعاملات وتوثيقها . والكتابة الإلكترونية شأنها شأن الكتابة العادية فهي كذلك تعد وسيلة للإثبات إذ جعلها المشرع مساوية للوثيقة المحررة على الورق سواء كانت مطلوبة للانعقاد أو الإثبات فقط .

نص المشرع في المادة 323 مكرر من القانون المدني الجزائري على الكتابة معرفا لها « ينتج الإثبات بالكتابة من تسلسل حروف وأوصاف وأرقام وأي علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها»

والملاحظ أن المشرع الجزائري لم يعرف الوثيقة الإلكترونية رغم تأكيده حجية هذه الورقة في الاثبات بخلاف القانون التونسي الذي عرفها في الفصل 453 من مجلة الالتزامات والعقود:»بأنها الوثيقة المتكونة من مجموعة أحرف وأرقام أو أي إشارات رقمية أخرى بما في ذلك تلك المتبادلة عبر وسائل الاتصال وتكون ذات محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة»

-2 : التوقيع الإلكتروني[15]

عرف المشرع التوقيع الالكتروني في قانون 04-15 المؤرخ في 1 نوفمبر 2015 والمحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين و ذلك في المادة 2»التوقيع الالكتروني بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى

تستعمل كوسيلة توثيق» وهذا يستوجب أن يتم استعمال وسيلة تعريف موثوق بها تضمن ارتباط ذلك التوقيع بالوثيقة المتصلة به

أما بالنسبة للجنة الأمم المتحدة للتجارة الدولية «الأونسترال» فقد أصدرت قانونا خاصا بالتوقيع الإلكتروني 2001 تناولت من خلاله تعريف هذا التوقيع وكيفية استخدامه والقواعد الخاصة به حيث عرفته في المادة 2 من هذا القانون بأنه «بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة عليها ومرتبطة بها منطقيا حيث يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في هذه الرسالة ويلاحظ من خلال هذا التعريف أنه لم يقم بتحديد أنواع التوقيع الإلكتروني تاركا المجال مفتوحا أمام التشريعات الوطنية للقيام بهذه المهمة

ثانيا : الحماية الجنائية للتجارة الإلكترونية والمستهلك[16]

تتركز هذه الحماية الخاصة ذات الطابع الجنائي في الحماية الجنائية لبرامج الحاسوب والمواقع الإلكترونية والحماية الجنائية للمستهلك الالكتروني

-1 الحماية الجنائية لبرامج الحاسوب :كرس المشرع القانون 04-09 المؤرخ في 5غشت 2009 للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأيضا في المواد 394 وما بعدها من قانون العقوبات حيث شملت هذه القوانين مجموعة من التدابير الوقائية وأخرى جزائية نظير ارتكاب جرائم متصلة بتكنولوجيات الإعلام والاتصال بصورة عامة فنصت المادة 2 من قانون 04-14 على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال / المنظومة المعلوماتية /المعطيات المعلوماتية / مقدمو الخدمات / المعطيات المتعلقة بحركة السير / الاتصالات الالكترونية / فالمساس بهذه المواضيع ينعكس على المستهلك وكذلك على الجهاز الحاسب والموقع الالكتروني

2 : الحماية الجنائية للمواقع الإلكترونية

وسنحاول تناول بعض صور جرائم الاعتداء على المواقع الإلكتروني والتي عالجها المشرع في القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها انطلاقا من المادة 2 من ذات القانون التي حددت هذه الجرائم وبينت آليات الرقابة القبلية التي تسمح بالتنبؤ بالخطر و حصر مخاطره والمحددة في المادة 4

2 1-تدمير المواقع : ويقصد به الدخول الغير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو النظام ،وهناك عدة وسائل تستخدم لتدمير المواقع من أهمها ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع المستهدف للتأثير على السلطة التخزينية للموقع فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغط يؤدي في النهائية إلى تفجير الموقع الحاصل على الشبكة وتشتت البيانات والمعلومات المخزنة في الموقع وتنتقل لجهاز المعتدي .

-2 2تشويه المواقع : يتم هذا التشويه عبر عدة أساليب يتبعها المخترقون من أهمها

- الدخول بهوية مخفية عبر منفذ برتوكول، وتتم هذه العملية بفك تشفير كلمة الدخول الخاصة بأحد المشرفين على الشبكة فيلجأ المخترق إلى استخدام برامج خاصة لتخمين كلمه السر.ولهذا ينصح باستخدام كلمة سر طويلة نسبيا مكونة من حروف

ورموز وأرقام معقدة حتى يتعسر فكها خلال فترات متقاربة للتقليل من احتمال توصل أحد المخترقين إليها

2-3استغلال الثغرات الأمنية في مزودات الويب وأنظمة التشغيل :إذا كان نظام تشغيل أو مزود الويب به ثغرات أمنية تعرض مستخدميه لخطر الاختراق فإنها تستغل في عمليات الاختراق وتبقى متاحة لفترة طويلة حتى يتم اكتشافها وذلك لأن أغلب الثغرات التي يكتشفها الهاكرز لا يعلنون عنها بسرعة .و هذا يستدعي على سبيل الإلحاح أن يكون مصممي نظام التشغيل على إطلاع الدائم محين يسمح لهم بالاطلاع على آخر ما توصل إليه من ثغرات أمنية واقتناء أحداث برامج الحماية من أجل حماية أنظمتهم من الاختراق

3:الحماية الجنائية للمستهلك[17]

نظرا للأضرار التي أصبحت تواجه المستهلكين والأخطار المحيطة بهم عند قيامهم بالتسوق عبر الشبكة العنكبوتية ذلك أن مبيعات البرامج المعلوماتية تتضمن العديد من المشاكل التي تتطلب تعزيز الحماية القانونية لمعاملات التجارة الإلكترونية وتحقيق حماية للمستهلك المتعامل إلكترونيا فإن التشريعات عمدت إلى وضع منظومة قانونية تضمن حماية المستهلك لهذه المنتجات ذات الطابع الالكتروني سواء بنصوص عامة كما في قانون حماية المستهلك 03-09 المتعلق بحماية المستهلك وقمع الغش اوقانون العقوبات او في قوانين خاصة كما في قانون04-09 السابق الذكر

خاتمة

في ظل التهافت على المنتجات الالكترونية بكل أنواعها وفي ظل العجز التشريعي و الرقابي على مواكبة تسارع تطورها ،الى حد أن صار المخترقون يوجهون ضحاياهم الى الانتحار وينفذون للحسابات الخاصة للأشخاص منتهكين الخصوصية بالعرض والتشهير ناهيك عن الخروقات التي تطال التعاملات التجارية وعمليات التسوق الالكتروني وما يرافقها من احتيال ونصب وفي ظل عمومية النص القانوني العقابي للخروقات من جهة وتباطؤ في مواكبة تطور الأفعال الموصوفة مخاطر تهدد المستهلك وأمنه الاجتماعي والاقتصادي والعلمي ،فأنه من الضرورة بمكان الشعور بهذه المخاطر و القيام بتثقيف المستهلك بها من جهة وتكوين جهازي رقابي عالي المستوى للحفاظ على الأمن الالكتروني الوطني وخاصة في جانبه الاقتصادي حيث يتصاعد النداء في مجتمعنا من كثير من المواقع الى اقتناء عمولات افتراضية ويجد له الصدى الواسع إضافة الى حركة الاحتيال المنتشرة بطريق توظيف الأموال عن طريق مؤسسات وهمية تنشط الكترونيا ،والدعوى لتفعيل عمل ودور جمعيات حماية المستهلك ومواكبتها للمتغيرات التكنولوجية خاصة

المراجع

1- أحمد السيد الكردي : المخاطر المدركة لدى المستهلك في التسوق عبر الانترنيت مقال منشور على الانترنيت .http://www /alukah.net/culture/0/78647

2- أحمد السيد الكردي : حماية المستهلك في التسوق عبر الانترنيت ، مقال منشور بتاريخ25/10/2014. http://www.alukah /net/culture/0/77589

3 -احمد السيد الكردي : حماية المستهلك الالكتروني ، مقال منشور في 8 جوان 2011 http://kenanaonline.com/users/

/ ahmedkordy/posts/275121

-4الدسوقي حامد أبوزيد:دور المستهلك المصري في تحقيق الحماية له ،دراسة ميدانية، مجلة العلوم الإدارية، العدد السادس، السنة الثالثة، مصر، يوليو 1993

-5أسامة أحمد بدر: حماية المستهلك في التعاقد الإلكتروني، الطبعة الأولى، الجامعة الجديدة للنشر، مصر، 2005

-6إسماعيل قطاف: العقود الالكترونية وحماية المستهلك ، رسالة ماجستير ،جامعة الجزائر ، 2005

https://www.syja.org/ar/sl/31041

-7خميخم محمد :الحماية الجنائية للمستهلك في عقود التجارة الالكترونية ،رسالة دكتوراه ، جامعة أي بكر بالقايد تلمسان ، سنة 2017

-8مريم قويدر : أثر الألعاب الالكترونية على السلوكيات لدى الأطفال ،رسالة ماجستير ،جامعة لجزائر 3 ، سنة 2012

-9محمد الفاتح محمود المغربي : التجارة الالكترونية ،دار الجنان للنشر والتوزيع ، ص98 https://books.google.dz/books?isbn=9957594206

-10 مروة زين العابدين صالح : الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي ...، طبعة 2016 ص 169 https://books.google.dz/books?id=C6kPDgAAQBAJ&dq

-11مسعودي يوسف/ أرجيلوسرحاب : مدى حجية التوقيع الالكتروني في الإثبات في التشريع الجزائري دراسة على ضوء أحكام القانون 04-15مجلة الاجتهاد للدراسات القانونية والاقتصادية / المركز الجامعي لتامنغست، سداسية محكمة/العدد11 جانفي 2017

-12 نوال عبد الكريم الأشهب :النجارة الالكترونية ،المنهل https://www.syja.org/ar/sl/31041

-13 صالح شنين : الحماية الجنائية للتجارة الالكترونية ،رسالة دكتوراه ،جامعة ابوبكر بلقايد تلمسان ، سنة 2013

-14عمر عبد الجواد إسماعيل :إدارة أخطار التجارة الالكترونية ،مقال ،كلية الاقتصاد والعلوم الإدارية ،جامعة الزيتونة الأردنية ،2004.

الهوامش:

1/ CYBER C3 Portal uaecyber.com>Articles» مخاطر التجارة الالكترونية/عمر عبد الجواد إسماعيل :إدارة اخطار التجارة الالكترونية،مقال،كلية الاقتصاد والعلوم الإدارية،جامعة الزيتونة الأردنية،2004 ،ص 3

2/https://www.sadeem.io/blog/dns-attacks-and-prevention/

3/http://www.ghorab.ws/2012/12/online-fraud-prevention-detection-recovery.html

4/أحمد السيد الكردي :المخاطر المدركة لدى المستهلك في التسوق عبر الانترنيت مقال منشور على الانترنيت http://www.alukah.net/culture/0/78647/

5/أحمد السيد الكردي :المخاطر المدركة لدى المستهلك في التسوق عبر الانترنيت، مقال منشور على الانترنيت/http://www.alukah.net

/culture/0/78647

6نوال عبد الكريم الأشهب :النجارة الالكترونية ،المنهل ، ص 69 https://www.syja.org/ar/sl/31041

7نوال عبد الكريم الأشهب :التجارة الالكترونية،المنهل،ص70https://www.syja.org/ar/sl/31041

8نوال عبد الكريم الأشهب :التجارة الالكترونية،المنهل،ص70 https://www.syja.org/ar/sl/31041

9 أحمد السيد الكردي : حماية المستهلك في التسوق عبر الانترنيت ، مقال منشور بتاريخ25/10/2014 http://www.alukah.net/culture/0/77589/

10احمد السيد الكردي : حماية المستهلك الالكتروني ، مقال منشور في 8 جوان 2011 http://kenanaonline.com/users/ahmedkordy/ posts/275121/

جمعية حماية المستهلك تطلق حملة توعية إلكترونية باستخدام وسائل الاتصال والتقنية الحديثةhttp://www.spa.gov.sa/944901

11مريم قويدر : أثر الألعاب الالكترونية على السلوكيات لدى الأطفال ،رسالة ماجستير ،جامعة لجزائر 3 ، سنة 2012 ،ص 123 و مابعدها

12 محمد الفاتح محمود المغربي : التجارة الالكترونية ،دار الجنان للنشر والتوزيع ، ص98 https://books.google.dz/books?isbn=9957594206

13مروة زين العابدين صالح :الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي ...، طبعة 2016 ص 169 https:// books.google.dz/books?id=C6kPDgAAQBAJ&dq

14إسماعيل قطاف: العقود الالكترونية وحماية المستهلك ، رسالة ماجستير ،جامعة الجزائر ، 2005 ،ص90

الدسوقي حامد أبوزيد:دور المستهلك المصريفي تحقيق الحماية له،دراسة ميدانية،مجلة العلوم الإدارية،العدد السادس،السنة الثالثة،مصر،يوليو 1993 ،ص 11 - 12

15أسامة أحمد بدر:حماية المستهلك في التعاقد الإلكتروني،الطبعة الأولى،الجامعة الجديدة للنشر،مصر، 2005 ،ص: 108

د.مسعودي يوسف/ أرجيلو سرحاب : مدى حجية التوقيع الالكتروني في الإثبات في التشريع الجزائري دراسة على ضوء أحكام القانون 04-15 مجلة الاجتهاد للدراسات القانونية والاقتصادية / المركز الجامعي لتامنغست، سداسية محكمة/العدد11جانفي2017ص84

-16صالح شنين : الحماية الجنائية للتجارة الالكترونية ،رسالة دكتوراه ،جامعة ابوبكر بلقايد تلمسان ، سنة 2013 ،ص 146 وما بعدها

17صالح شنين :الحماية الجنائية للتجارة الالكترونية،رسالة دكتوراه،جامعة ابوبكر بلقايد تلمسان،سنة 2013 ،ص 192ومابعدها

خميخم محمد :الحماية الجنائية للمستهلك في عقود التجارة الالكترونية ،رسالة دكتوراه ، جامعة أي بكر بلقايد تلمسان ، سنة 2017 ،ص 248 وما بعدها