



جامعة دمشق

كلية الحقوق

مسؤولية المصارف في السرقات

عن طريق القرصنة الالكترونية

بحث علمي لنيل درجة الماجستير في القانون التجاري

إعداد الطالب عارم ظهير الطويل

الأستاذ المشرف الدكتور هيثم الطاس

أستاذ مساعد في قسم القانون التجاري

١٤٣٧ هـ - ٢٠١٦ م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ * خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ * اقْرَأْ وَرَبُّكَ

الْأَكْرَمُ * الَّذِي عَلَّمَ بِالْقَلَمِ * عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ

صَدَقَ اللَّهُ الْعَظِيمُ

سورة العلق

الإهداء

إلى من أثار لي حياتي بأصابع يديه ... وجعل من أحلامه درباً أسير عليه حتى رأى في
نجاحي نوراً لعينه وكان لي خير ظهيرا
أي الحنون المحامي ظهير الطويل

* * *

إلى من يعجز عن شكرها الكلام وتشهد على تضحياتها الأيام
يا أعظم من عرفت نفسي وأطهر ما لمست كفي
أمي الحبيبة المحامية حسناء ضبيان الكيلاني

* * *

إلى من كان لي معلماً بارعاً ، وأخاً ناصحاً فاتخذته قدوة وإماماً
المحامي محمد الطير

* * *

كما وأتقدم بجزيل الشكر للمهندسة هدى سمير الشالح لدورها الحثيث بالإشراف الفني على
هذا البحث

وأتقدم بجزيل الشكر للأستاذ المشرف تقديراً لجهوده التي أثمرت هذا البحث لما
منحه لي من وقته الثمين في مهمة الإشراف .

الدكتور هيثم الطاس

* * *

وأقدم بتحياتي و شكري العميق لأعضاء الهيئة التدريسية في قسم القانون التجاري ،
ولأعضاء الهيئة التدريسية في كلية الحقوق جامعة دمشق .

وخير ما يقال في فضلهم علينا

قم للمعلم وفه التبجيلا كاد المعلم أن يكون رسولا

بسم الله الرحمن الرحيم

المقدمة

لكم فكرت ملياً وترددت كثيراً في اختيار موضوع هذه الأطروحة وذلك لعلمي المسبق أن موضوعها واسع وكثير الشباب يتخلله العديد من التعقيدات ، وكيف لا وموضع هذه الأطروحة يشكل تاج نتاج التطور العلمي المذهل الذي بلغه الإنسان على صعيد التكنولوجيا ، التي مابرحت في كل يوم بل في كل ساعة تغير وتطور كل مناحي حياتنا وعلى الأخص (الحياة الاقتصادية) الأمر الذي انعكس على سرعه نقل وتداول وتجارة الأموال والذي بدوره أدى إلى انتشار واسع لكبرى البنوك والشركات مع زيادة منقطعة النظير في الفعاليات الاقتصادية المختلفة .

وإنني لأشاطر الكاتب الصيني (تاي تنج) الذي نشر في القرن الثالث عشر كتاباً بعنوان (تاريخ الكتابة الصينية) عندما قال " لو كنت لأنتظر الكمال مفرغت من كتابي إلى الأبد " .

لعل أهم ما يميز المجتمعات البشرية عن سائر مجتمعات الكائنات الحية في الكون ، هو القدرة على التطور المستمر في كافة مجالات الحياة ، فلو قمنا بمقارنة بسيطة بين نمط و سلوكيات حياة الإنسان البدائي مع نمط وسلوك حياة الإنسان في القرن الواحد والعشرين ، نجد بأن نتاج ماتوصل إليه العقل البشري في زمننا هذا ربما كان من المستحيلات في أزمان أسلافه ، وأن مايفكر به

أحدنا أو يقوم به في هذا اليوم ، من المستحيل أن يدور في تفكير الإنسان البدائي ، بينما لو قمنا بذات المقارنة على مجتمعات الكائنات الحية الأخرى على الأرض ، فلا نجد بأن هناك أي تطور يذكر قد طرأ على نمط معيشتها وسلوك حياتها ، وإن هذه السمة تعد من أبرز سمات العقل البشري ، وبالتالي فإن اتساع انتشار استخدام شبكة الانترنت في كافة مجالات الحياة هو أحد صور تطور المجتمعات البشرية ، وهو ما دفع بممتهني التجارة إلى إقحام نشاطاتهم التجارية ضمن شبكة الانترنت ، مستفيدين من الانتشار الكبير الذي حققته ، ناهيك عن سرعه تداول المعلومات بواسطة الانترنت ، وهو ما يشكل أهم العوامل لدى التجار لاثمار تجارتهم .

وكنتيجة طبيعية ، فإن دخول العمل التجاري إلى العالم الافتراضي ، خلق الحاجة إلى وجود مؤسسات مالية تسهل عمليات التجارة عبر الانترنت ، ودفع بالمؤسسات المصرفية إلى تطوير خدماتها كي تلبي حاجات تطور الأعمال التجارية المستمر في تلك المجالات .

وكأية نشاطات، كذلك للتجارة الالكترونية مخاطر وصعوبات تعيق انتشارها، وتلح معها الحاجة لإيجاد الحلول المسعفة لتلك المخاطر من الجانب القانوني ، حيث إن غياب وجود التكييفات القانونية للتصرفات التي تجرى عبر الانترنت، يثير مشكلة في تحديد التزامات مستخدمي الانترنت، ما يشكل عدم وضوح المراكز القانونية و غموضها، ما قد يكون سبباً في إحجام الكثيرين عن الخوض في هذا المجال، وينشأ عنه حالة من الفوضى القانونية ضمن أروقة العالم الافتراضي.

مشكلة البحث :

لما كانت التجارة الالكترونية في العالم الافتراضي تنفرد بخاصيتها المغايرة للتجارة التقليدية في كثيرٍ من النواحي ، وبات ذلك واقعاً مفروضاً مستوجباً الأخذ بعين الاعتبار الجوانب القانونية ، وهذا ما ألقى بعبئه على كاهل الفقهاء والباحثين في مجال القانون ، للتصدي لهذه المسائل القانونية من خلال الدراسات والأبحاث الفقهية لإيجاد التكييفات القانونية الملائمة ، أي أن خصوصية التجارة الالكترونية وكذلك الانترنت تجعل من الصعوبة بمكان إمكانية إدراج التصرفات أو تكييفها وفقاً لما هو متبع في العالم المحسوس وتعذر تطبيق النظريات القانونية التقليدية في خضم تصرفات الأفراد عبر الانترنت ، هذا ما فتح الباب أمام مناقشة قانونية قد لا تنتهي تبعاً لاستمرار تطور وسائل التكنولوجيا والمليديا .

وبالتالي فإن الخصوصية التي تتسم بها نشاطات التجارة الالكترونية عبر الانترنت ، وطبيعته العالم الافتراضي ، والانتشار الواسع والمستمر الذي حققه ، إضافةً إلى التطور المستمر في هذا المجال ، والذي تزداد مخاطره تبعاً لازدياد تطوره ، ناهيك عن الأثر المزدوج لتطور التكنولوجيا فكل جديد في مجالات البرمجة وحماية الشبكات يقابله نظيره في تطوير أساليب اختراق الشبكات وبالعكس ، ما أدى لظهور نظريات قانونية حديثة تختلف عن النظريات التقليدية في التكييفات القانونية لبعض التصرفات ، وتنتهج نهجاً مغايراً إلى حدٍ ما لما هو مستقر عليه في النظريات التقليدية ، ولكون تلك النظريات حديثة النشوء فإن الأساس القانوني الذي تستند إليه مازال مبهماً بعض الشيء الأمر

الذي فرض واقعاً تتزاحم فيه التساؤلات القانونية عن الأساس القانوني للنظريات الحديثة المطبقة على العمليات الالكترونية لتثمر بنتائجها العلمي في هذا المجال ، فقياساً بالتشريعات التجارية التقليدية التي يعتمد المشرعون فيها إلى رد العديد من أحكامها إلى الأعراف التجارية لا النصوص القانونية التي تتسم بالجمود ولا تلبي المرونة المطلوبة للأعمال التجارية ، وبالتالي تقييد النشاطات التجارية التي تتغير باستمرار وتنشئ أحكامها الخاصة وفق أعراف وليدة الواقع العملي ، ومن هنا تفنقر التجارة الالكترونية من الناحية القانونية إلى أحكام ومؤيدات وضوابط واضحة تحدد مراكز مستخدميها من الوجهة القانونية ، ما بات يلقي على قاضي الموضوع من جهة عبء إيجاد التكيف الملائم لكل واقعة على حده ، ومن جهة أخرى يلقي هذا التطور بكاهله على فقهاء القانون عبء الاستمرار في البحوث القانونية المتعلقة بهذا المجال بالسرعة المطلوبة للحفاظ على إخضاع النشاطات المتجددة ضمن مجالات التجارة الالكترونية إلى أحكام وقواعد قانونية تحفظ مراكز الأفراد ضمن هذه النشاطات .

صعوبات البحث :

لا شك بأنه في أي بحث علمي ، تعترض الباحث بعض الصعوبات أثناء بحثه ، يشكل تذليلها بالنهاية مصدر إغناء للبحث أكثر من كونها صعوبات تعثر الباحث ، وبالنسبة لموضوع هذا البحث فنتجلى صعوباته في النقاط التالية:

أولاً : ندرة وجود مراجع باللغة العربية لجهة حداثة المعلومات في كل ما يتعلق بالتجارة الالكترونية ، وبالتالي وبالرغم من كثرة الأبحاث في هذا المجال إلا أنها مكررة في معلوماتها.

ثانياً : قلة المراجع القانونية عموماً فيما يتعلق بالمسؤوليات القانونية عن الهجمات الالكترونية ، وذلك لحداثة انتشار جرائم القرصنة لاستهداف المصارف والمؤسسات المالية ، وبالتالي قلة الأبحاث المتعلقة بالمسؤوليات القانونية في هذا المجال بالإضافة لقلة الحوادث والوقائع في هذا الجانب مقارنة بغيرها من الوقائع في العالم المحسوس .

ثالثاً : خصوصية هذا البحث كونه يبحث في مسألة تقنية فنية بحتة إلى جانب المعالجة القانونية ، وهي مسألة القرصنة ومفهومها وأنواعها وطريقتها وخطواتها ، والتي كان لابد من الخوض فيها ودراستها بشيء من التعمق وذلك للتمكن من شرح عملية القرصنة بشكل مفصل ما يسهم في تحديد المسؤوليات القانونية ، ويؤثر في أنواع التكييفات القانونية لأنواع القرصنة .

رابعاً : التطور المستمر لمجالات التكنولوجيا ، فحيث أن التطور المستمر الذي يكاد أن يكون آنياً ، وبالتالي فمن المحتمل وجود ما هو جديد في كل لحظة ، مما يتطلب من الباحث المتابعه الدقيقة لكافة التطورات التي تطرأ في هذا المجال .

خامساً : عدم وجود آراء قانونية فقهية واضحة وتضاربها في هذا المجال ، مما يولي بالمسؤولية على الباحث لبذل جهد استثنائي في التحليل والدراسة ، للوصول للنتائج القانونية السليمة .

منهج البحث :

تبعاً لطبيعة موضوع البحث والذي يغلب عليه الطابع الفني في مجال التكنولوجيا ، مما فرض اتباع المنهج القانوني التحليلي ، لحداث المشاكل التي يناقشها البحث ، والتي تتطلب دراسة الموضوع من خلال دراسة القضايا المعروضة في هذا المجال للوقوف عند كل قضية وتحليل حيثياتها وظروفها ودراسة آراء قضاة الحكم فيها وتحليل تكييفاتهم القانونية لنخلص إلى النتيجة المرجوة ، وحيث أن المنهجية المتبعة في دراسة الأبحاث الانجلوسكسونية قد تخدم موضوع البحث وتتيح لنا دراسة هذا الموضوع بشكل أوسع من أنماط المنهجية الأخرى ، كونه ستم دراسة العديد من النواحي الفنية المتعلقة بالتكنولوجيا ، قبل الدخول في المسائل القانونية ، لذا كان لابد من اتباع المنهج الانجلوسكسوني لعلاج هذا الموضوع .

حيث تم تقسيم البحث إلى أربعة فصول ، فبحث الفصل الأول في انطلاق ثورة المعلوماتية وتطور الشبكة العنكبوتية والمليديا والتي ساهمت بالنيجة في ظهور التجارة الالكترونية ، وتناول الفصل الثاني التعريف بالقرصنة والقرصنة وأنواعها وتحليل خطواتها وذلك ليتم فهم عملية القرصنة بشكل تام للوصول بشكل دقيق إلى التكييف القانوني السليم لعملية القرصنة في الفصل

الثالث ، وفي النهاية خلصنا إلى دراسة حالات تفعيل مسؤولية المصارف عن الهجمات الالكترونية في الفصل الرابع وفق مخطط البحث المبين :

مخطط البحث

الفصل الأول : نشأة التكنولوجيا وتطور وسائل الاتصال .

أولاً : ثورة المعلوماتية .

ثانياً : تطوير برمجة الشبكة العنكبوتية .

ثالثاً : ظهور التجارة الالكترونية .

* * *

الفصل الثاني : التعريف بالقرصنة الالكترونية .

أولاً : افتقار شبكة الانترنت للخصوصية .

ثانياً : تعريف القرصنة الالكترونية وأنواعها .

ثالثاً : تحليل خطوات عملية القرصنة الالكترونية .

* * *

الفصل الثالث : التكيف القانوني لعملية القرصنة الالكترونية .

أولاً : التكيف القانوني لعملية القرصنة الالكترونية .

ثانياً : المسؤولية الجزائية عن القرصنة الالكترونية .

ثالثاً : موثوقية التوقيع الالكتروني .

* * *

الفصل الرابع : تفعيل مسؤولية المصارف تجاه عملائها جراء الاحتيال عن طريق القرصنة .

أولاً : مسؤولية البنوك في النظرية التقليدية .

ثانياً : مسؤولية البنوك في النظرية الحديثة .

ثالثاً : تحديد مسؤولية البنوك جراء عمليات القرصنة والإعفاء منها .

* * *

الفصل الأول

نشأة التكنولوجيا وتطور وسائل الاتصال

أولاً : ثورة المعلوماتية

– Information technology revolution –

(I.T)

لاشك بأن من أعظم منجزات الثورة الصناعية الأولى والثانية كان تطوير تقنيه وسائل الاتصال عن بعد ، والتي كانت تثير لعاب القاده العسكريين وتشكل محطة الاهتمام لما تقدمه هذه التقنية من مزايا غاية في الأهمية في تكتيكات العمليات العسكرية ما بات يشكل عامل تنافس لدعم التطوير في مجال وسائل الاتصال عن بعد بين الدول الكبرى انذاك بغية تحقيق التقدم العسكري ومن هنا كانت الريادة في مجال تطوير الاتصالات هي القوة العسكرية الألمانية ، حيث يعود الفضل للعديد من العلماء الألمان لما قدموه من نظريات عملية تطبيقية في مجال الحواسب القابلة للبرمجة أُخرجت للواقع واستخدمت فعلا في الجيش الألماني ، حين تم اختراع أول حاسب قابل للبرمجة وهو عبارة عن آلة تشفير كهرو ميكانيكية "ENIGMA" استخدمت من قبل

الجيش النازي لتشفير وفك تشفير الرسائل النصية منذ عام ١٩٣٦ قبل وأثناء الحرب العالمية الثانية على يد العالم "Arthur Scherbius"

مما دفع ذلك بالمقابل القوى المتنافسة عسكرياً لبذل المزيد من الجهود لدعم تطوير أبحاث العلوم التطبيقية لخرق نظام الاتصال هذا وفك تشفير رسائل الجيش الألماني ، ومن هنا شكلت هذه التنافسات في مجال الآلات الحاسوبية الشرارة الأولى لانطلاق ثورة المعلوماتية في النصف الثاني من القرن العشرين عندما قام العالم البريطاني ALAN TURING المتخصص في مجال الرياضيات ، في تأسيس مفاهيم النظريات الخوارزمية بالإضافة لكونه يعتبر أول من وضع مبادئ الحواسيب الحديثة في ورقته المقدمة عام ١٩٣٦^٢

يعود ظهور الانترنت إلى أواخر الخمسينات في أروقة وزارة الدفاع الأمريكية (DoD) U.S Department of Defense في وقت ازدادت

^١ ١٢٧. Singh ,Simon. ١٩٩٩. *The Code Book*. London: Fourth Estate.pg. ٢٠١٦. Wikipedia. "Enigma Machine".
راجع الموقع الإلكتروني
http://en.wikipedia.org/wiki/Enigma_machine.

^٢ With An ، Alonzo. ١٩٣٧. "Turing A. M.. On Computable Numbers,Church Application To The Entscheidungs Problem. Proceedings Of The London Pp. ٢٣٠-٢٦٥.". *The* ، ٢ S. Vol. ٤٢ (١٩٣٦-١٩٣٧)،Mathematical Society *Journal Of Symbolic Logic* ٢ (٠١): ٤٢-٤٣.
doi:١٠,١٠١٧/s.٠٠٢٢٤٨١٢٠٠٣٩٥٨٨x.

حيث قاد ALAN TUNING الفريق الحكومي البريطاني في مركز الإشارة لفك شيفرة جهاز ENEGMA وخرق رسائل الجيش الألماني حيث بدأ مشروعه في سبتمبر ١٩٣٨ وحتى ديسمبر من العام ١٩٣٩

الحاجة فيه بشكل ملح لوجود وسيلة اتصال آمنة تربط مراكز الأبحاث القائمة على تطوير برامج تطوير السلاح النووي وقد تم إنشاء وكالة مشروع أبحاث متقدمة (ARPA) Advanced Research Projects Agency هدفها تطوير تكنولوجيا المعلومات لحاجتها لنقل البيانات عبر الحواسيب بخصوص مشروع السلاح النووي وفي عام ١٩٦٩ قامت الـ ARPA net بتفعيل أول شبكة اتصال بين الحواسيب ربطت أربعة مواقع في الولايات المتحدة هي جامعة كاليفورنيا في لوس أنجلوس، وجامعة كاليفورنيا في سانتا باربرا، ومعهد ستانفورد للأبحاث، وجامعة ولاية يوتا^٣

وفي بداية الثمانينيات أنشأت العديد من الشبكات المحلية إلى أن ظهرت في عام ١٩٨٦ NSFnet المدعومة من قبل مؤسسة العلم الوطنية national science foundation لتربط مختلف الجامعات في الولايات المتحدة وبحلول عام ١٩٩٢ أصبحت هذه الشبكة تربط أكثر من مليون حاسوب حول العالم، ويبدو أن هذا الانتشار الواسع الذي تحققه شبكة الانترنت في كل لحظة حتي يومنا هذا منح شبكة الانترنت الاهمية التي تحظى بها اليوم والتي لا بد من التطرق لدراسة تطوير برمجة شبكة الانترنت بكافة مراحلها وذلك لاهميتها في مجالات التجارة الالكترونية ، منذ البدء في تطوير شبكة الانترنت إلى حين ظهور الشبكة العنكبوتية مروراً بتطوير أسماء النطاق .

^٣ <http://education.illinois.edu/wp/commercialism/history-of-the->

internet.htm ٢٠١٦ راجع الموقع الالكتروني

ثانياً : تطور برمجة الشبكة العنكبوتية

تتألف شبكة الانترنت من مجموعة ضخمة من الحواسيب المرتبطة مع بعضها عبر شبكة اتصالات تستخدم نموذج مخصص لنظام اتصال أجهزة الحواسيب بين بعضها البعض ، حيث قامت منظمة الإيزو العالمية بعمل نظام موحد TCP/IP model يسمح بتواصل هذه الأجهزة المختلفة وهذا النظام يعمل على بروتوكول **Transmission Control Protocol/Internet Protocol (TCP/IP)** : حيث أصبح هذا البروتوكول هو معيار الاتصال بين الحواسيب في عام ١٩٨٢ بالإضافة لإمكانية استخدامه بشكل مباشر ليسمح لبرنامج ما على الحاسب من التواصل مع برامج أخرى ضمن أجهزة معينة عبر الانترنت ^٤.

وقد عرف قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم ١٧ لعام ٢٠١٢ الشبكة في المادة ١ بما يلي :

ترابط من الأجهزة الحاسوبية والمنظومات المعلوماتية يسمح بتبادل المعلومات أو التشارك فيها بين مرسل ومستقبل أو مجموعة من المستقلين وفق إجراءات محددة

عناوين بروتوكول الانترنت IP Addresses:

^٤ باسل مصطفى الخطيب - تاريخ الانترنت - الجامعة الافتراضية السورية قسم الهندسة المعلوماتية

تُحدد العقد على الانترنت بالنسبة للمستخدمين بأسماء محددة ، أما بالنسبة للحواسب فهي تُعرف بعناوين رقمية .



حيث يتكون العنوان الفريد Internet Protocol (IP) addresses لكل جهاز متصل بالانترنت من رقم فريد يتألف من ٣٢ - bit يكتب هذا العنوان عادة باستخدام أربعه أرقام بين الـ ٠ - ٢٥٥ يتألف كل منها من ٨ بت يفصل بينها نقاط (١٩١,٥٧.١٦٢,١٢١)

١٩١,٥٧,١٦٢,١٢١ → ١٠١١١١١١,٠٠١١١٠٠١,٠١١١١١١٠,٠١١١١٠٠١

يقوم هذا البروتوكول بفسح المجال بشكل متسلسل من هذه الأرقام لكل منظمة ، والتي تقوم بدورها بتوزيع الأرقام ضمن هذا المجال على حواسيبها المتصلة مع الانترنت ، فعلى سبيل المثال لوزارة الدفاع الامريكية المجال من ١٢,٠٠,٠٠٠ إلى ١٢,٢٥٥,٢٥٥,٢٥٥ أي ١٦ مليون عنوان ، ومع تزايد

الطلب على هذه المجالات ظهر في عام ١٩٨٨ معيار IP اجدید (IPv٦)
يوسع العنوان إلى ١٢٨ بت إلا أنه لم ينشر على نطاق واسع حتى الآن ° .

١ - أسماء النطاق Dmoain name :

لما كان التعريف بالحواسب عبر الانترنت عن طريق الأرقام يشكل عائق
يعترض مستخدمي الانترنت فقد تم التوصل لاستخدام الأسماء عوضاً عن
العناوين الرقمية ، حيث يتألف الاسم عادة من اسم المضيف host متبوعاً
بأسماء نطاقات domains مجموعات من الحواسب محتواة ضمن بعضها
البعض يميز النطاق الأخير نوع المنظمة التي ينتمي الحاسب المضيف لها
فمثلاً يميز النطاق edu المؤسسات التعليمية والنطاق com المؤسسات
التجارية^٦ ففي العنوان movies.comedy.marxbros.com

يكون movies هو اسم المضيف و هي النطاق المحلي comedy لـ
movies والتي هي جزء من النطاق marxbros والذي هو بدوره جزء من
النطاق com

° باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص٣

٦ باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص٤

ويدعى هذا الاسم الكامل باسم النطاق المحدد تماماً fully qualified domain name^٧



وبالتالي ستقوم برمجيات أو أجهزة خاصة تدعى name server بتحويل أسماء النطاقات التي يكتبها المستخدم في متصفح الويب إلى العناوين الرقمية الموافقة .

فعندما يقوم المستخدم بطلب وثيقة باستخدام اسم النطاق يتم توجيهه هذا الطلب إلى أقرب مخدم للحصول على العنوان IP

وقد ورد تعريف النطاق على الانترنت في القانون السوري ضمن المادة ١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم ١٧ لعام ٢٠١٢ بما يلي : (نطاق على الانترنت زمرة من أسماء المواقع الالكترونية

^٧ باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص ٤

على الانترنت تخضع لسلطة إدارية واحدة وتندرج تحت اسم واحد هو اسم النطاق

أما اسم النطاق العلوي فقد ورد تعريفه في ذات القانون بأنه : أوسع نطاق ينتمي إليه موقع الكتروني ما على الانترنت ويكون الحقل الأخير من اسم هذا الموقع .

وكذلك عرف قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري مقدم خدمات التواصل على الشبكة في المادة ١ : مقدم الخدمات الذي يتيح التواصل على الشبكة وذلك عن طريق موقع الكتروني أو أكثر أو أي منظومة معلوماتية مشابهة .

وكذلك عرفت المادة ١ من ذات القانون مقدم خدمات الاستضافة على الشبكة : مقدم الخدمات الذي يوفر مباشرة أو عن طريق وسيط البيئة والموارد المعلوماتية اللازمة لتخزين المحتوى بغية وضع موقع الكتروني على الشبكة ويسمى اختصاراً المضيف ^٨ host



^٨ باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص ٤

وفي منتصف الثمانينات ظهر العديد من البروتوكولات التي تعمل وفق البروتوكول tcp/ip لنظام مستخدمي الانترنت ومن أشهر هذه البروتوكولات :

١-١- البروتوكول telnet والذي يستخدم للولوج لحاسب آخر متصل عبر الانترنت

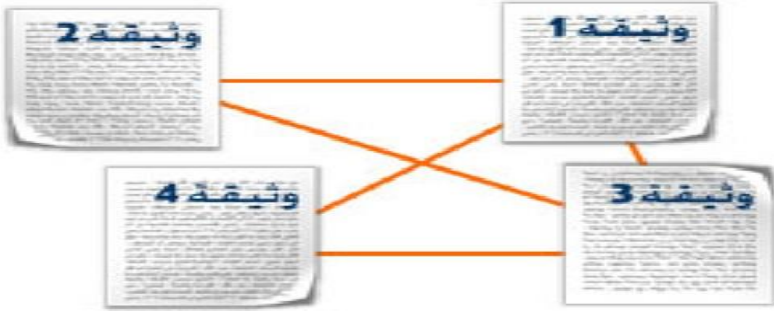
١-٢- البروتوكول ftp والذي يستخدم لنقل الملفات عبر الانترنت^٩

٢ - شبكة الويب “www” World Wide Web :

قامت مجموعة من المهندسين في المخبر الأوروبي للأبحاث النووية CERN عام ١٩٥٩ باقتراح بروتوكول جديد يهدف إلى السماح للعلماء حول العالم باستخدام الانترنت لتبادل الوثائق الموصوفة لأعمالهم ، وأطلق على هذه المنظومة “World Wide Web” والتي صممت بهدف السماح لأي مستخدم للانترنت بالبحث والحصول على الوثائق من قواعد البيانات لأي حاسب آخر مخدم للوثائق ، وبحلول العام ١٩٩١ أصبحت هذه المنظومة متوفرة للجميع استخدمت هذه المنظمة شكلاً معيناً للوثائق يدعى النصوص الفائقة Hypertext والذي هو عبارة عن نص يحوي ارتباطات مضمنة إلى نصوص أخرى في وثائق أخرى ، مما يسمح باستعراض غير تسلسلي بالضرورة للنصوص ، فيمكن للوثائق أن تحوي صور أو مقاطع صوتية أو أي نوع آخر من الوسائط فتدعى فائقة الوسائط Hypermedia وبهذا يمكن أن نرى الويب

^٩ - باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص٤

بأنها مجموعة ضخمة من الوثائق والتي يمكن لبعضها ان يكون مرتبط مع وثائق أخرى^{١٠}

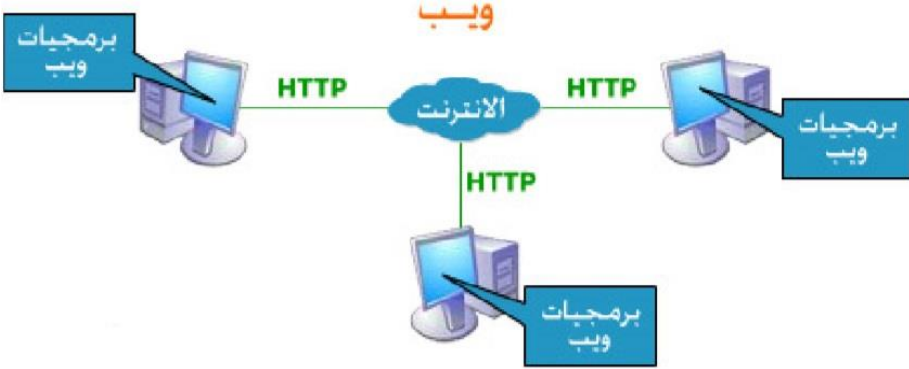


ولا بد من التمييز بين الانترنت والتي هي مجموعة من الحواسيب والتجهيزات مرتبطة مع بعضها بحيث يمكن لكل منها التخابط مع الآخر



^{١٠} باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص ٥

والويب والذي هو مجموعة من البرمجيات والبروتوكولات التي تم وضعها بشكل مسبق على حواسيب الانترنت ، باستخدام الويب بروتوكول " http" Hyper text transfare protocol وبهذا فإن شبكات الانترنت كانت



وماتزال ذات فائدة كبيرة حتى قبل ظهور الويب . مع الملاحظة بأن مستخدمي الانترنت هم في الواقع يستخدمون الانترنت عن طريق الويب.^{١١}

^{١١} باسل مصطفى الخطيب - تاريخ الانترنت - مرجع سابق ص٦

ثالثاً : ظهور التجارة الالكترونية

- Electronic commerce -

لما كان لتطوير وسائل الاتصال دورها في التوصل بالنهاية لإيجاد مايسمى اليوم بالوسائط المتعددة حيث ألحق هذا الانفتاح التقني تغيراً بالغاً في الحياة البشرية عما كانت عليه من ذي قبل ، وأضحت الوسائط المتعددة وسيلة يكاد لا يخلو منها أي مكان في بقاع العالم ، وفي مختلف المجالات ولعل النشاطات التجارية هي من أكثر النشاطات حاجة للتكنولوجيا لما تقدمه من خدمات توفر الجهد والوقت والمال في التعامل والتواصل بغية تحقيق القدر الأكبر من الربح ، ومن هنا نشأت التجارة الالكترونية التي توسعت وتطورت تبعاً للتطورات التكنولوجية وخاصة ما يتم منها من خلال شبكة الانترنت العالمية التي باتت تشكل بالنسبة لمستخدميها نافذة صغيرة تطل على كافة بقاع العالم ، و لما كانت النشاطات التجارية تقوم على عاملين أساسيين هما السرعة والثقة في التعامل ، وبالتالي فإن خصوصية شبكة الانترنت توفر عامل السرعة بما يلبي الحاجة إليه بالنسبة للأعمال التجارية ، حيث شكلت هذه الخصوصية لدى الأفراد دافع قوي جعلهم يقحمون شبكة الانترنت ضمن نشاطاتهم التجارية ، و من هنا كانت نشأة التجارة الالكترونية والتي استمرت بالانتشار سواء بين المؤسسات التجارية وزبائنها أو بين المؤسسات التجارية ذاتها ، واستمر التطور في هذا المجال إلى أن باتت التجارة الالكترونية أحد أهم مصادر تمويل وتطوير الملتيميديا ، وكانت إحدى صوره إيجاد نظام دفع آلي عبر الانترنت .

ومع تطور الأساليب التكنولوجية الحديثة والتوسع في استخدامها ، في شتى مجالات الحياة حيث نجد أن التجارة تطورت بشكل كبير بفضل تزايد عقد الصفقات التجارية ، حيث حقق الانترنت حلم رجال الأعمال والمال، وأشغل الاهتمام بالتجارة الإلكترونية ومختلف البيانات المتعلقة بها باستخدام وسائل تبادل البيانات الاستثمار إلكترونياً Electronic Data Inter (EDI)، وقد بدأ هذا النظام في السبعينيات من القرن الماضي ومازال حتى الآن يعتبر حجر الأساس للتجارة الإلكترونية .

يعتمد EDI بصورته التقليدية على شبكة تسمى القيمة المضافة Value Added Network (VAN)

حيث تقوم EDI بتجميع المعلومات والبيانات مثل بيانات المبيعات من عدة فروع حيث ينتج عنها طلبات شراء الموردين وترسل EDI هذه المعلومات إلى VAN حيث يوجد صندوق بريد إلكتروني يسمح بالاتصال المباشر بأجهزة حواسيب الشركاء ، مما أدى إلى سرعة إرسال البيانات وزيادة كفاءة العمليات .

واليوم وفي مجال التجارة الإلكترونية ، يحول عدد كبير من شركات الأعمال التي تتبع نظام EDI إلى VAN لكن عن طريق أنظمة حديثة تتمثل في X400 والبريد الإلكتروني e-mail وشبكة الانترنت. Internet. والعمليات التي تتم على الشبكة العنكبوتية Web لكن عدداً من الشركات الصغيرة وجدت أن استخدامها لتكنولوجيا الاتصالات أصبح مكلفاً ، فالتجته إلى استخدام ما يسمى بتجارة الشبكات Net Commerce التي تسهل

تبادل المعلومات داخل الشركات من خلال شبكة الانترنت Intranet أو من خلال شبكة الاكسترانت Extranet التي تستخدم معايير شبكة الإنترنت لتبادل المعلومات التجارية والمالية^{١٢} .

١- مفاهيم التجارة الالكترونية :

أعطى الخبير الاقتصادي الأمريكي نيكولاس بيرتلي مفهوماً للتجارة الإلكترونية " إن مفهوم التجارة الإلكترونية يشير إلى تسويق المنتجات عبر شبكة الإنترنت الدولية وتفرغ البرامج الإلكترونية دون الذهاب إلى متجر أو إلى شركة " وعلاوةً على ذلك فإن التجارة الإلكترونية تشمل على الاتصالات بين مختلف الشركات على المستوى المحلي أو الدولي بما يسهل عملية التبادل التجاري ويزيد من أحجامها^{١٣}

أما منظمة التجارة العالمية فقد عرفت التجارة الإلكترونية على أنها مجموعة متكاملة من عمليات الصفقات وتأسيس الروابط وتوزيع وتسويق وبيع المنتجات والخدمات بوسائل إلكترونية^{١٤} ، كما تعرف المؤسسة العربية لضمان الاستثمار ، التجارة الإلكترونية على أنها " التجارة التي تتم باستخدام

^{١٢} محمد سعيد أحمد اسماعيل - أساليب الحماية القانونية لمعاملات التجارة الالكترونية - جامعة دمشق - الحلبي الحقوقية ٢٠٠٩ - ص ٥٩

^{١٣} التجارة الإلكترونية وواقع العالم العربي ، شؤون خليجية أكاديمية السادات للعلوم الإدارية ، قسم البحوث القاهرة ، ١٩٩٩ ديسمبر ، ص ٢٥.

^{١٤} التجارة الإلكترونية النشرة الاقتصادية البنك الاهلي المصري العدد الثالث ، المجلد الثاني والخمسون ، ١٩٩٩ ، القاهرة، ص ١٠.

التقنيات التي وفرتها ثورة المعلومات والاتصالات وشبكة الانترنت عبر التبادل الالكتروني لبيانات متجاوزة الزمان والمكان وتغطي وتضع قطاعات عديدة وتنظم قواعد جديدة لعمليات البيع والتسجيل"^{١٥}

كما يعرف البعض التجارة الإلكترونية بأنها تنفيذ بعض أو كل العمليات التجارية فيما يخص السلع والخدمات عبر شبكة الإنترنت والشبكات التجارية العالمية ، أي باستخدام تكنولوجيا المعلومات والاتصالات ، وهي وسيلة سهلة وسريعة لإبرام الصفقات التجارية الكترونياً، سواء كانت التجارة في السلع والخدمات أو المعلومات وبرامج الكمبيوتر .

أما المشرع السوري فقد أورد في المادة ١ من القانون ٢٠١٤/٣ المتعلق بالمعاملات الالكترونية تعريفاً للمعاملات الالكترونية : إجراء معاملة أو جملة من الإجراءات التي تجري بين طرفين أو أكثر ولها طابع مدني أو تجاري أو إداري

استفاد الكثيرون من فوائد التجارة الالكترونية في خفض التكاليف وتحسين الكفاءة، عن طريق التقليل من استعمال الأوراق مع تفصيل وملاءمة السلع والخدمات طبقاً لاحتياجات ومتطلبات العملاء بالإضافة تحسين وضع المنتجين التنافسي .

شهدت التجارة الإلكترونية نمواً متزايداً في السنوات الأخيرة سواء من حيث حجمها أو عدد مستخدميها، ففي الولايات المتحدة الامريكية هناك أكثر

^{١٥} بهاء شاهين ، العولمة والتجارة الالكترونية ، الطبعة الأولى ، دار الفاروق الحديثة للطباعة والنشر القاهرة ٢٠٠٠ ، ص ٦٢

من ٥٠٠٠٠ شركة خاصة تستخدم التجارة الإلكترونية أو الانترنت في تسهيل تعاملاتها التجارية ، حيث تشير بعض المصادر الأمريكية إلى أن حجم التجارة الإلكترونية بين الشركات الأمريكية يفوق ٣٠٠ مليار دولار في بداية هذا القرن، كما بلغ عدد الأمريكيين المشتركين في شبكة الانترنت ٤٠ مليون مشترك في سنة ٢٠٠٠ ، أما في دول شرق آسيا فقد بلغ حجم التجارة الإلكترونية ٨٠٠ مليون دولار و ٥٠٠ مليون دولار في كل من إندونيسيا والفلبين وتايلاند ، وقد بدأت هذه الدول في تنفيذ خطط لتوسيع نطاق التجارة الإلكترونية بحيث تكون الوسيلة الأولى لترويج صادراتها ، أما في الدول العربية فقد بلغ حجم التجارة الإلكترونية ١٥ مليون دولار فقط وبلغ عدد مستخدمي الانترنت ٥٠٠٠٠٠ مشترك منهم ٥% فقط يستخدمون الانترنت في تسهيل وإتمام تعاملاتهم التجارية^{١٦} ، ويجب التنويه إلى أن انتشار استخدام الانترنت في بلد ما لا يشكل ضماناً أكيداً لقيام ورواج التجارة الإلكترونية، فقد تناولت دراسة أعدتها شركة IBM واقع التجارة الإلكترونية في كندا حيث وجدت أنه بالرغم من أن كندا تبنت الانترنت منذ مدة طويلة ونسبة مستخدمي الشبكة فيها يفوق نسبة مستخدمي الشبكة في الولايات المتحدة الأمريكية حيث بلغ ١٦% عام ١٩٩٧ بالمقارنة مع الولايات المتحدة ١٠% عام ١٩٩٧ ٢٣% ل ١٧% عام ١٩٩٨ ، بالرغم من ذلك فإن عدد

^{١٦} التجارة الإلكترونية وواقع العالم العربي - ص ٢٦ مرجع سابق

المتسوقين خلال الشبكة وصل إلى ١٠% في كندا مقابل ٣٤% في الولايات المتحدة الأمريكية^{١٧}

٢-أنواع التجارة الالكترونية :

يمكن أن تصنف التجارة الإلكترونية إلى نوعين أساسيين من نشاط الأعمال :

الأول : تجارة الأعمال مع الأعمال Business to Business :
ويقتصر التعامل فيها على الشركات ومورديها وزبائنها الكبار وذلك من خلال كلمات سرية وعناوين خاصة بتلك الشركات وحدها غير معلنة أو منشورة ، مثل نظام السويفت SWIFT المصرفي أو نظام IBAN

والثاني : تجارة الأعمال للمستهلكين Business to Consumer B٢C :
يسمى البعض بالتسويق الإلكتروني Electronic Shopping.
أو تجارة التجزئة الإلكترونية^{١٨} Electronic Retailing

٣-أهمية التجارة الالكترونية :

ستتصدر التجارة الإلكترونية في المستقبل القريب قائمة التعاملات التجارية في جميع أنحاء العالم لكونها :

^{١٧} التجارة الإلكترونية وواقع العالم العربي ، مرجع سابق ص ٢٦

^{١٨} التجارة الإلكترونية وواقع العالم العربي ، مرجع سابق ص ٢٨

- وسيلة سهلة وبسيطة يمكن استخدامها من خلال جميع الطبقات والأنواع من الأفراد والشركات في وقت قصير وبأقل تكلفة ممكنة.
- تجتاز حاجز الزمان وتتخطى المكان ، حيث يمكن التعامل معها في أية ساعة من اليوم ، ومن أي مكان في العالم ، فهي بذلك تعتبر من أهم وأكبر تطبيقات العولمة.
- تعمل على تدفق المعلومات في الوقت المناسب الذي يحتاج فيه المتعامل إلى اتخاذ القرار المناسب.

٤- نظام الدفع الآلي عبر الانترنت :

تم الاتفاق بين أكبر مؤسسة مصرفية في هونج كونج وهي مؤسسة هونج كونج وشنغهاي البنكية hsbc وشركة كومباك لأجهزة الحاسب على تطوير أول نظام آلي أمن للتجارة الالكترونية^{١٩} واعتباراً من شهر أكتوبر ١٩٩٩ فإن هذه الخدمة تمنح التجار نظام دفع آمن لقبول المدفوعات عبر شبكة الانترنت بواسطة البطاقات الائتمانية وقد وفّت شركة كومباك البنية التحتية اللازمة لإتمام عمليات الدفع من العملاء إلى شركات وبين الشركات بعضها البعض ويتضمن هذا النظام الآليات الأمنية الكفيلة بتأمين العمليات الالكترونية وقد دفع إلى هذه الخطوة التي سبقتها خطوات مماثلة في أوروبا والولايات المتحدة واليابان الرغبة الهائلة

^{١٩} زيدان محمد - دور البنوك الالكترونية في تطوير التجارة الالكترونية - جامعة حسنية بن علي بالشلف - الجزائر - ص ٨

المتولدة لدى الجمهور المتعاملين مع الشركات لإنهاء معاملاتهم بالكامل من خلال شبكة الانترنت وكانت العقبة الوحيدة التي تحول دون القفزة الكبيرة للتجارة الالكترونية هو أمن المعاملات على الشبكة ولكن آليات التشفيرة المستخدمة في هذا النظام وغيره من النظم التي تستخدم أجهزة الخدمة الآمنة كسرت إلى حد ما حاجز الخوف الذي كان يجعل الكثيرين يحجمون عن ذكر بيانات بطاقتهم الائتمانية على الشبكة وساهم في ذلك دخول البنوك كطرف ثالث بين الشركة البائعة والعملاء مما يطمئن العميل أن البنك يضمن له حقوقه فيما لو أُسيء استخدامها .

وعرف المشرع السوري الدفع الالكتروني في قانون المعاملات الالكترونية بأنه : أي تحويل للأموال يتم بوسائل الكترونية تخول المؤسسة المالية إجراء عمليات القيد على حسابات المتعاملين وذلك وفق الأنظمة والتعليمات النافذة الصادرة عن مصرف سورية المركزي .

٥- دور البنوك الالكترونية في زيادة تداول حجم التجارة الالكترونية:

بدأت البنوك الإلكترونية أو بنوك الإنترنت في منتصف التسعينات من القرن الماضي ، حيث ظهر على الشبكة في الولايات المتحدة الأمريكية ، وقد بلغ عدد البنوك التي تعمل عبر شبكة الإنترنت وفقاً لتقرير مؤسسة Online Banking الصادر في عام ١٩٩٨ أكثر من ٢٠٠ بنك^{٢٠}

^{٢٠} التجارة الإلكترونية وواقع العالم - مرجع سابق ص ٢٧

لم يتطرق المشرع السوري في قوانينه المتعلقة بتنظيم التجارة الالكترونية أو تنظيم التواصل على الشبكة أو أية قوانين متصلة بهذا الصدد أي تعريف للبنوك الالكترونية ، وإنما أورد تعريفاً للمؤسسة المالية التي تقدم خدمات عبر الانترنت بصرف النظر عن نشاطها أو شكلا القانوني وذلك في المادة ١ من قانون المعاملات الالكترونية بما يلي : الجهة المرخص لها بالمعاملات المالية وفق هذا القانون ووفق الأنظمة والقوانين النافذة .

٦- مفاهيم عن البنوك الالكترونية :

يستخدم تعبير أو مصطلح البنوك الإلكترونية كتعبير متطور وشامل للعديد من المفاهيم التي ظهرت في مطلع التسعينات كمفهوم الخدمات المصرفية والمالية عن بعد، أو البنك المنزلي أو الخدمات المالية الذاتية أو البنك على الخط^{٢١} وكلها تعابير تعني قيام العملاء بإدارة حساباتهم وإنجاز معاملاتهم المتصلة بالبنك في الوقت والمكان الذي يرغب به العميل ، من خلال الدخول عبر خط خاص إلى حساباته لدى البنك .

كما تعرف البنوك الإلكترونية بأنها منافذ إلكترونية تقدم خدمات مصرفية متنوعة دون توقف وبدون عمالة ، بينما يشير إليها آخرون بأنها منافذ لتسليم الخدمة المصرفية قائمة على الحاسبات الآلية ذات مدى حر المكان والزمان^{٢٢} ومن أهم تلك المنافذ الإلكترونية آلات الصرف الآلي.

^{٢١} حسام لطفي ، أبعاد التجارة الالكترونية ، الندوة الوطنية للتجارة الالكترونية ، ٥-٦ ١٩٩٨

^{٢٢} طارق عبد العال حماد ، تطبيقات التكنولوجيا في المصارف ، أكاديمية السادات للعلوم الإدارية ،

تقدم البنوك الإلكترونية حلولاً متكاملة وشاملة للعملاء تتطوي على أكثر من خدمة وبتكلفة أقل من البنوك التقليدية وقد ساهم التطور في نظام الدفع النقدي الإلكتروني المصاحب لتطور وانتشار مواقع التجارة الإلكترونية في قدرة البنوك الإلكترونية على المنافسة والتميز

وقد بدأ أول بنك افتراضي على شبكة الانترنت Net Bank عام ١٩٩٥ ثم تلتها بنوك أخرى مثل SOFT BANK عام ١٩٩٦ وفي نفس العام أقامت America Online بنكاً افتراضياً انضم إليه America Bank Of ، Citi Bank ، Union Bank Of California و America حيث أصدرت هذه المجموعة ١٣٥ مليون عرض سعر في يوم وأحد خلال شهر يناير ٢٣١٩٩٩

وقد ساهمت البنوك الإلكترونية في رواج التجارة الإلكترونية بفضل وسائل الدفع التي توفرها للمتعاملين إذ يمكن لرجال الأعمال عقد الصفقات ودفع مستحقات تلك الصفقات عن طريق هذه البنوك دون السفر وتحمل المشاق العادية وفي سرعة قياسية مقارنة مع الصفقات العادية .

٧- أهم الخدمات المقدمة من قبل البنوك الإلكترونية :

تقدم البنوك الإلكترونية العديد من الخدمات تتمثل أهمها فيما يلي :

٧-١- Phone Bank الهاتف المصرفي :

^{٢٣} طارق عبد العال حماد ، ٢٠٠٠ - مرجع سابق ص ٣

مع تطور الخدمات المصرفية على المستوى العالمي ، أنشأت البنوك خدمة " الهاتف المصرفي " لتفادي طوابير العملاء في الاستفسار عن حساباتهم أو بعض الخدمات الأخرى ، حيث تستمر هذه الخدمة ٢٤ ساعة طوال أيام الأسبوع ، ولقد تعددت صور الخدمات التي يقدمها الهاتف المصرفي و نعرض منها :^{٢٤}

- يتم من خلاله ومن خلال الاتصالات الهاتفية بالبنك عن طريق رقم سري خاص يمكن العميل من سحب أو تحويل الأموال أو الأمر بالدفع لصالح دائنيه مثل سداد فاتورة الهاتف أو الكهرباء وغيرها من الخدمات، كما يمكن الاستفسار عن جميع ، المعلومات التي يطلبها العميل .

وتم تقديم هذه الخدمة في بريطانيا عام ١٩٨٥ حيث تعمل بواسطة شاشة متوفرة لدى العميل في منزله تمكنه من الاتصال المباشر بالبنك تمكنه من معرفة كل المعلومات المتعلقة بحساباته والقيام بتحويلات الأموال أو سحب الأوراق التجارية أو مختلف العمليات الأخرى^{٢٥}.

^{٢٤} طارق طه ، إدارة البنوك والنظم المصرفية ، دار الكتب للطباعة والنشر ، القاهرة ٢٠٠٠ ، ص

^{٢٥} زيدان محمد - دور البنوك الالكترونية في تطوير التجارة الالكترونية - مرجع سابق ص ١٠

وباعتبار **المشرع السوري** لم يتطرق حتى اليوم لسن تشريع خاص بالمعاملات المصرفية الالكترونية فلا بد من التعويل على القوانين الأخرى المتصلة بهذا السياق حيث ورد في قانون تنظيم التواصل عبر الشبكة تعريفاً للجهاز الحاسوبي في المادة ١ :أي جهاز يستخدم التقانات الالكترونية أو الكهرطيسية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها ، وقد جاء في التعليمات التنفيذية لهذا القانون ت ١ يدل الجهاز الحاسوبي على أي جهاز لاسلكي أو سلكي مهما كان نوعه أو شكله يملك معالجا للمعلومات مثل المخدم والحاسوب الشخصي والمساعد الرقمي والهاتف الذكي والمسير الشبكي وبالتالي يمكن إدراج الهاتف الذكي في زمرة الأجهزة الحاسوبية الوارد تعريفها في قانون تنظيم التواصل على الشبكة السوري

٧-٢- التحويل الإلكتروني للأموال :

تقوم العديد من البنوك في المشاركة في شبكة حاسبات تتولى التداول الإلكتروني لملايين القيود المحاسبية بين مختلف المصارف ، وبذلك تؤدي هذه الخدمة نظيراً للدور التقليدي لغرف المقاصة المصرفية ولكن بشكل

أكثر سرعة وبدرجة عالية من الكفاءة ومن المتوقع مد نطاق التسويات المصرفية باستخدام الأقمار الصناعية لتشمل مختلف ، البنوك العالمية .

ويهدف نظام التحويل الإلكتروني للأموال إلى تسهيل وتعجيل المدفوعات والتسويات بين المصارف بما يكفل تقديم خدمات أفضل للعملاء . كما سوف يعطي البنوك ميزة تنافسية في الأسواق العالمية إذ سوف يتيح لهذه ، البنوك إمكانية التسوية الفورية من دفع وتلقي للأموال عبر حساباتها الجارية لدى البنوك المركزية وتوفير نظام دفع فوري لعملائها كما يشمل هذا النظام تسوية المدفوعات التي تتم عن طريق شبكة المدفوعات^{٢٦} .

٧-٣- النظم المصرفية المباشرة مع العميل (On Line) :

بدأت مجموعة من البنوك العالمية الكبرى في تطبيق النظم المصرفية المباشرة مع عملائها من خلال الحاسب الآلي (جهاز الكمبيوتر التقليدي) ومن خلال هذا النظام يتمكن العميل من إجراء معظم العمليات المصرفية الروتينية مثل تحويلات الأموال من حسابه إلى حسابات أخرى، الاستفسارات عن كشف الحساب ، كما تمكن هذه النظم العميل من سرعة حصوله على الخدمات المطلوبة^{٢٧}

^{٢٦} زيدان محمد - دور البنوك الالكترونية في تطوير التجارة الالكترونية- مرجع سابق ص ١١

^{٢٧} Berman.B ، Marketing channels ، john wiley & Sons Inc، London ، ١٩٩٦

٧-٤- الانترنت المصرفي internet banking :

إن نظام الانترنت القائم على البنك المنزلي نظام له أهمية كبيرة سواء على مستوى البنوك أو على مستوى العملاء الذين يتوفرون على خطوط للانترنت كما وتعتبر الخدمات المصرفية عبر الانترنت أقل تكلفة أو معدومة التكلفة مقارنة مع الخدمات المصرفية التقليدية .

ويتطلع العالم اليوم إلى مرحلة ما بعد الانترنت وهو ما يسمى بطريق المعلومات السريع ومن أهم ملامحها :^{٢٨}

إن الكمبيوترات الدفترية هي أصغر الحاسبات المعروفة اليوم وأكثرها قابلية للنقل والحمل وباتت منتشرة بشكل مطلق نسبة لوجودها فهي بحجم الجيب و بشاشات ملونة في حجم الصورة الفوتوغرافية العادية يطلق عليها The wallet PC الكمبيوتر الشخصي أو المحفظة الالكترونية الشخصية يمكن أن تعرض جميع الرسائل والخطابات وجداول المواعيد والوصول إلى شبكة الانترنت المباشرة^{٢٩}

ظهور ما يسمى Spatial Navigation يتيح للعميل أن يتجه إلى حيث توجد المعلومات من خلال تمكينه من التعامل مع نموذج مرئي لعالم واقعي أو كأنه الواقع تماماً

^{٢٨} دور تكنولوجيا المعلومات في تطوير الخدمات المصرفية ، أوراق بنك مصر البحثية ، العدد الرابع ، القاهرة ١٩٩٨ . ص ٤٥

^{٢٩} دور تكنولوجيا المعلومات في تطوير الخدمات المصرفية ، مرجع سابق - ص ٤٥

ظهور ما يسمى الوكيل على شبكة المعلومات السريعة وهو عبارة عن مصفاة اتخذت شكل شخصية قادرة على المبادرة حيث تكون مهمتها مساعدة العميل في البحث عن أي معلومات يطلبها العميل

ISDN Integrated Services Digital Net work ظهور تكنولوجيا تسمى الشبكة الرقمية للخدمات المتكاملة حيث تقوم هذه التقنية بنقل الصورة والبيانات بمعدل يبدأ من ٦٤٠٠٠ بت حتى ١٢٨٠٠٠ في الثانية الواحدة وهو ما يعني بإمكانها إنجاز أي عملية أو إيصال أية رسالة بصورة تكاد تكون متزامنة مع الواقع ^{٣٠}

وبهذا أضحت التجارة الالكترونية وتطورها مرتبط وبشكل وثيق مع تطوير عالم الملتيميديا ، فكل جديد في مجال الملتيميديا لابد وأن يكون له صده وتأثيره على عالم التجارة الالكترونية .

ومما لا شك فيه بأن لكل نشاط أخطار محدقه به ومعوقات تعرقل تطوره ، وصعوبات يجب تذليلها لحسن واستمرارية سيره ، وخصوصية توجب مراعاتها ، كي تتم ممارسة النشاط بالشكل الأمثل دون الوقوع في دائرة مخاطره ، وبالتالي فإن نشاطات التجارة الالكترونية لا تخلو من تلك المخاطر والمعوقات ، والتي أهمها عمليات الهجمات الالكترونية (القرصنة) والتي سيتناولها الفصل الثاني من هذا البحث .

^{٣٠} D. Geiben ، La banque à distance ، Revue d'économie financière ، N° ،

* * *

الفصل الثاني

التعريف بالقرصنة الالكترونية

- Definition of Hacking-

أولاً : افتقار شبكة الانترنت للخصوصية

ثانياً : التعريف بالقرصنة الالكترونية وأنواعها

١- تعريف القرصنة الالكترونية

٢- تعريف القراصنة

٣- أنواع القراصنة

٣-١- من حيث سلوك القراصنة :

٣-١-١- القبعات السوداء

٣-١-٢- القبعات البيض

٣-٢- من حيث درجة خبرة المقرصن :

٣-٢-١- القراصنة الهواة

٣-٢-٢- القراصنة متوسطي الخبرة

٣-٢-٣- القراصنة المحترفين

٣-٣- من حيث هدف القرصنة :

٣-٣-١- القرصنة الذين يعملون لحساب

الحكومات أو المؤسسات العسكرية

٣-٣-٢- القرصنة المستأجرون

٣-٣-٣- القرصنة المحتالون

٣-٣-٤- القرصنة الإرهابيون

ثالثاً : تحليل خطوات عملية القرصنة الالكترونية .

الفصل الثاني : التعريف بالقرصنة الالكترونية وخطواتها

لا يمكن تصور ممارسة أي نشاط في مجال التطبيق العملي دون مواجهة مخاطر خاصة وفقاً لطبيعته تعرقل سيره وتشكل عقبة أمام انتشاره و شعبيته، وكغيرها من المعاملات ، فإن للتجارة الالكترونية مخاطر عديدة تعرقل تطورها وتدفع العديد من المستخدمين للإحجام عن الإنخراط ضمن نطاقها ، حيث يرى البعض بأن مجرد إخراج بياناتهم من الخزن المكتبية أو الملفات الورقية وجمعها في مكان واحد هو الكمبيوتر يزيد من خطر تعرضها للانتهاك حيث تشكل خصوصية المعلومات عاملاً إضافياً يثير قلق مستخدمي الانترنت من أفراد أو منشآت تجارية أو حكومية ، خاصة وأن قوانين احترام الخصوصية في دول العالم الثالث على وجه الخصوص تفتقر للانضباط والصرامة بشكل يؤمن للمستخدم الدرجة المطلوبة للحفاظ على خصوصية معلوماته التقنية ، حيث أن مستخدم الانترنت في مجال التجارة قد يفصح عن العديد من المعلومات الشخصية السرية كرقم حسابه المصرفي أو توقيعه الالكتروني باستخدام بطاقته الائتمانية وكذلك بالنسبة للمنشآت التجارية التي قد تخاطر بجزء مهم من معلوماتها السرية في خضم تعاملها بالتجارة الالكترونية ، كمعلومات تتعلق بالزبائن أو معلومات تتعلق ببراءات الاختراع وغيرها من المعلومات التجارية السرية ، وبالتالي فإن افتقار شبكة الانترنت للخصوصية يجعل مستخدميها تحت خطر محقق من جراء إمكانية اطلاع الغير على معلوماته الشخصية واستغلالها بسوء نية لغرض غير مشروع .

وقد شكل هذا الهاجس دافعاً يضع ذوي الخبرة المعنيين بهذا المجال أمام واقع مفروض يحتم عليهم التدخل لإيجاد حلول لتقادي تلك المخاطر التي باتت تتزايد طردياً مع التقدم التكنولوجي ولعل أهم تلك المخاطر " جرائم نظم المعلومات " والتي يكون الهدف منها التسلل إلى حواسيب المستخدمين أو اختراق لنظام محلي أو إقحام فيروس من خلال الشبكة وذلك للحصول على معلومات حيوية ليصار إلى استخدامها أثناء عملية القرصنة أو للحصول على معلومات تجارية لمنشأة ما ليصار إلى بيعها لشركة منافسة أخرى (التي قد تكون معلومات متعلقة بالزبائن أو ملكية فكرية أو نماذج صناعية أو أرقام حسابات مصرفية) وبالتالي يشكل ذلك خرقاً لخصوصية مستخدم الانترنت ويجعل من استخدامه خطراً محدقاً قد يؤدي إلى إحجام العديد من أصحاب المنشآت التجارية إلى ممارسة نشاطاتهم التجارية أو تقديم خدماتهم عبر الانترنت ومن هنا باتت مسألة أمن المعلومات " Information Security " من أبرز المشاكل التي تواجه تقدم التجارة الالكترونية وتحد من انتشارها وذلك لما ينعكس عنها من افتقار شبكة الانترنت للخصوصية ، بالإضافة لما قد تلحقه هذه المخاطر من أضرار أو خسائر تلحق بالمؤسسات المالية والشركات التجارية أو حتى الحكومات ، حين تكون كافة بياناتها عرضةً للسرقة ، ومن هنا يتضح بأن شبكة الانترنت تفتقر للخصوصية المطلوبة في أي عمل تجاري أو مالي أو أي عمل يتعلق بأية حقوق مالية للمستخدمين .

أولاً : افتقار شبكة الانترنت للخصوصية

- Lack of internet privacy -

قد لا يختلف رأيان بتنوع و اتساع عالم الانترنت بالعديد من المعلومات التي تشكل جاذباً براقاً لمختلف الشرائح العقلية والعمرية ، إلا أن افتقار شبكة الانترنت للخصوصية يشكل بالمقابل هاجساً مقلقاً أمام الكثير من مستخدميها فخلافاً للمعتاد ، قد تصبح البيانات الشخصية البسيطة لأي مستخدم ، معلومات ذات قيمة كبيرة لمتطفي الانترنت تشكل لهم نقطة البداية لانطلاق عملية قرصنة ما .

فأي عمل يقوم به المستخدم عبر الانترنت يترك خلفه أثر عن معلوماته الشخصية المسجلة على حاسبه الشخصي (COOKIES) ، ومع كل ضغطة زر يقوم بها مستخدم الانترنت قد يأتى فيها العديد من الصور أو المحادثات أو الرسائل الالكترونية أو أرقام حسابات مصرفية أو أرقام لبطاقات ائتمان والمزيد من المعلومات الشخصية الأخرى إلى مواقع مختلفة عندما يقوم بزيارتها (twitter....etc,yahoo، facebook، e-bay,google) لكن تلك المعلومات لن تكون في ملاذ آمن باعتبارها في متناول شركات المواقع ذاتها وأيضاً الحكومات التي تحاول جمع تلك المعلومات وتخزينها ، وبالتالي ستشكل هذه المعلومات جاذباً قوياً يستهوي القراصنة الذين يسعون لسرقتها لتعريضهم في عمليات الاختراق وعادة قد يكون الإنسان في هذه الحالة أقل حرصاً على معلوماته الشخصية كونه يفشيها إلى جهاز حاسوبي وليس لإنسان آخر ، وهذا

مايشكل خرقاً لخصوصية مستخدم الانترنت حينما يقوم بعض متطفلي الانترنت بمحاولة اختراق خصوصية شبكة ما بغية الحصول على بعض المعلومات التي قد تكون غاية في البساطة ولكنها من الممكن أن تشكل نقطة البدء لعملية قرصنة قد تستهدف مؤسسة مالية ضخمة وتلحق الضرر بعشرات الملايين من الأشخاص وينتج عنها خسارة تقدر بمليارات الدولارات بغية تحقيق كسب شخصي غير مشروع عن طريق الاحتيال .

وفي هذا الصدد فقد عرف المشرع السوري في المادة ١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الخصوصية ((حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية ومراسلاته وسمعته وحرمة منزله وملكيته الخاصة وفي عدم اختراقها أو كشفها دون موافقته)) ، بل وعاقب على اعتراض المعلومات الخصوصية في المادة ١٨ فقرة ب من قانون تنظيم التواصل على الشبكة حيث نصل على أنه : يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مائة ألف إلى خمسمائة ألف ليرة سورية كل من استخدم الخداع للحصول على معلومات شخصية سرية من المستخدمين على منظومة المعلوماتية أو الشبكة يمكن استغلالها إلى أغراض جرمية .

وبالتالي فقد نص المشرع السوري على أحكام صارمة لحماية خصوصية التواصل عبر شبكة الانترنت مما يسهم بشكل فعال في مكافحة القرصنة الالكترونية .

وكذلك اندلعت في الولايات المتحدة الامريكية معركة سياسية كبرى خلال حقبة الثمانينات من القرن العشرين عندما قُدم للكونجرس اقتراح بتحويل صكوك ملكية الأسهم والسندات إلى الصورة الالكترونية ، أي أن تصبح مجرد سجل الكتروني في ملف مخزن على الحاسب ، وثار المستثمرون الذين كانوا يريدون الاحتفاظ بصكوكهم في أيديهم غير مؤمنين بفكرة أن تتحول صكوكهم إلى مجرد بيان مخزن في إحدى حاسبات شركة السمسرة، فكيف للمستثمر أن يتأكد من أن خطأ ما لن يتسبب في محو بيانات صكوكه من الحاسب ومن أين له أن يثق في أن صلاحية وسائط التخزين يمكن أن تمتد عشرات السنين ؟

ويبدو بأن المعارضين لتلك الخطوة آنذاك كانوا قد التمسوا شيئاً من الصواب ، فالبيانات المخزنة مغناطيسياً على الأقراص أو الأشرطة الممغنطة تزول بعد فترة من الزمن ولذلك فهي تتطلب باستمرار تحديثها وإعادة كتابتها على وسيط آخر ، ونظراً لكثرة المستجدات في مجال التقنية فكيف للمستثمر أن يتأكد من أن أجهزة قراءة الأشرطة أو الأقراص التي خزنت بياناته عليها ستظل موجودة بعد عشرات السنين ؟ فربما تبقى الأشرطة والأقراص ولكن تختفي الأجهزة القادرة على قرائتها وتظهر أجهزة جديدة ، وهذا التفكير ليس بغريب فمن الصعب الآن أن تجد أجهزة تقرأ الأشرطة القديمة المستديرة reel tapes بعد أن تحولت معظم مراكز الحاسب الآلي إلى floppy disk و CDs^{٣١} .

^{٣١} حسن طاهر داود - جرائم نظم المعلومات - أكاديمية نايف العربية للعلوم الامنية- الرياض

وبنهاية هذا النزاع حسمت المعركة السياسية لصالح أصحاب الصكوك الورقيه عام ١٩٩٠ بقرار من الكونجرس الأمريكي ، بينما في فرنسا والعديد من دول الاتحاد الأوروبي فالصورة مختلفة إذ تحولت الصكوك فيها إلى سجلات الكترونية بالفعل^{٣٢}.

لكن ماهو تعريف عملية القرصنة ؟ وكيف تتم عملية القرصنة ؟ وماهي أنواعها ؟ جميع هذه التساؤلات وإن كانت خارجة عن موضوع عنوان البحث القانوني لكن من الأهمية بمكان دراستها ولو بشكل عابر ليتتبي لنا لاحقاً تكييف عملية القرصنة قانوناً لتمكين تحديد المسؤولية فيها .

^{٣٢} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٥٦

ثانياً : تعريف القرصنة الالكترونية وأنواعها

نحاول في هذا الفصل إيجاد تعريفٍ مناسبٍ لعملية القرصنة ولبعض مصطلحاتها المتداولة في مجال جرائم نظم المعلومات وكذلك لتعريف القرصنة ليصار فيما بعد إلى تحديد بعض أنواعها وفق الواقع العملي .

١ - تعريف القرصنة الالكترونية :

إن تعريف مصطلح Hacking يثير الكثير من الجدل ، ويمكن أن يُقصد به إما شخص يقوم بمحاولة اختراق نظام البرمجة لحاسب ما ، أو أنه مطور المهارة في البرمجيات الحرة open source أو ما يعرف بتطوير البرامج "مفتوحة المصدر"

قد تعرف قرصنة الحواسيب على نطاق واسع بأنها (الوصول بقصد إلى قاعدة بيانات خاصة بحاسب ما دون وجود قبول للوصول أو في حال تجاوز صلاحيات الوصول للمستخدم)،^{٣٣}

لا شك أن مختلف القوانين في الدول المتقدمة تعاقب على عمليات القرصنة ، و لا مثار للجدل بأن عملية القرصنة تتدرج تحت جرائم نظم

^{٣٣} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٢٣

المعلومات وبالتالي فهي تعتبر جريمة معاقب عليها في القانون الجزائي بالنسبة للتشريعات الحديثة المتلازمة في تطويرها مع مقتضيات الواقع العملي .

تعريف ستيفي ليفي ((مدمن الكمبيوتر الذي يجد لذته في الوصول إلى البيانات الممنوعة))^{٣٤}

وفي التشريع السوري ، لم يتطرق المشرع السوري ضمن قوانينه النازمة لجرائم المعلوماتية تعريفاً للقرصنة ، مما يكشف عن نية المشرع لتجنب إيجاد تعريف ضيق لمفهوم القرصنة والاكتفاء بتعريف جريمة المعلوماتية في المادة ١ من قانون تنظيم التواصل عبر الشبكة حيث عرف الجريمة المعلوماتية بأنها جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكية أو تقع على المنظومات المعلوماتية أو الشبكة .

وفي رأينا فطالما كنا أمام حالة دخول غير مصرح به أو تسلل بصورة غير مشروعة لنظام حاسوبي مؤمن أو شبكة معينة مؤمنة فتكون هناك عملية قرصنة بصرف النظر عن غاية الفاعل أو دافعه أو هدفه من وراء تلك العملية ، وفي معرض محاولة إيجادنا لتعريف لعملية القرصنة فيمكن أن نضع التعريف التالي : ((عملية القرصنة هي الدخول الغير مصرح به لأي نظام حاسوبي أو شبكة أو موقع أو حساب الكتروني أو أي تسلل بصورة غير مشروعة لأي نطاق أو مخدم أو حاسوب على شبكة ما))

^{٣٤} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٢٣

مستقبل جرائم المعلومات في مجال الأعمال :

من الواضح بصفة عامة أن حجم الخسارة في العملية الواحدة من جرائم المعلومات في مجال الأعمال في ازدياد مستمر بينما عدد الجرائم من هذا النوع بالنسبة للحجم الضخم من العمليات المالية التي تتم كل يوم هو في تناقص مستمر ومن المتوقع أن يتناقص عدد الجرائم المعلومات خلال العقد الأول من القرن الحادي والعشرين بسبب الاتجاه السائد حالياً نحو استخدام المزيد من الضوابط وزيادة فاعلية هذه الضوابط في حماية الحواسيب وشبكات الاتصال وكذلك انتباه المؤسسات لأهمية تسجيل كافة الوقائع مثل دخول الأفراد إلى النظام واستخدامهم للمعلومات المخزنة في الحاسب بالإضافة إلى ازدياد الاهتمام بالتحليل الآلي لهذه الوقائع لتسليط الضوء على الوقائع المشبوهة مما يسهل على مسؤولي أمن المعلومات اكتشاف الجريمة فور وقوعها أو ربما قبل وقوعها (من خلال الأعمال التنفيذية التي تسبق ارتكاب الجريمة) فيمكن مثلاً اكتشاف تكرار تنفيذ عملية إضافة أو خصم من الرصيد مرتين ، بل يتم هذا الاكتشاف قبل أن يتم صرف المبلغ من الحساب المستفيد أو تحويل المبلغ إلى البنك الآخر .

وهناك سبب آخر وراء الاعتقاد بتناقص القرصنة وهو انتشار نظام التشفير وهي وسيلة يمكن أن تؤثر بشكل ملحوظ في تقليص أو ربما في منع هذا النوع من الجرائم خاصة عمليات التنصت أو الاختراق أو تزوير العمليات المالية ولكن من المهم أن نعلم أن استخدام التشفير وحده لن يقضي على هذه الجريمة تماماً فالبرامج عليها في النهاية أن تفك شفرة المعلومات قبل عرضها

على المستفيد وهنا مربط الفرس فالبشر ربما كانوا أضعف الحلقات في منظومة أمن المعلومات فالتشفير في الواقع ليس له وظيفة سوى أنه ينقل مكن الخسر من الشبكات والحاسبات إلى شبكات وحاسبات أكثر تأميناً أي أنه لا يقتصر دوره في النهاية إلا على تأخير فك تشفير المعلومات لحين وصولها لمكان يفترض تأمينه بشكل تام وبذلك يجب أن تكون هناك ضوابط مصاحبة للتشفير لاكتمال الفائدة . ولكن علينا أن ننتبه إلى أن التقدم التقني الذي يساعد على مكافحة الجرائم له تأثير مزدوج فهو من جانب يهدف لاستئصال تلك الجرائم ولكن بالوقت ذاته إنما يقوم بمساعدة المجرمين الذين يزدادون خبرة واستخداماً للتقنية يوماً بعد يوم مما يجعلنا نتوقع ازدياد حجم الخسارة الذي يتحقق في الجريمة الواحدة تناسباً مع ازدياد حجم التعامل في مجال التجارة الالكترونية الذي يأخذ منحاً تصاعدياً ، فعلياً أن نضع في الاعتبار أن مجرم الغد لن يخاطر باحتمال انكشاف أمره بعد تخطي الحواجز الأمنية العديدة من أجل مبالغ ضئيلة ولكنه سوف يجري وراء الصيد الثمين ، وليس بعيداً عن الذاكرة واقعة التزوير التي تعرض لها بنك ((بارينج)) وكان حجم الخسارة فيها ٨٦٩ مليون جنيه استرليني أي حوالي مليار ونصف المليار من الدولارات الأمريكية والتي مازالت أصدائها تدوي في عالم المال والأعمال^{٣٥} .

وليس بعيداً عما حدث في عام ١٩٩٦ من محاولة الاحتيال التي وقعت في روسيا لتحويل عشرة ملايين دولار إلى مصارف مختلفة موزعه على أنحاء

^{٣٥} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٣٢ و ١٢٥

العالم ، وكذلك قضية شركة التأمين ضد الاستثمارات التي سوف نتعرض لها في هذا الفصل والتي بلغ حجم الخسارة فيها بليون دولار . وربما لولا استخدام الحاسب في هذه الجرائم لانخفض حجم الخسائر عن ذلك بشكل كبير ولعلنا نعلم جميعاً كيف أن نقل الفاصلة العشرية من مكانها رقماً وأحداً يمكن أن يؤدي إلى خسارة ضخمة .

مايميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية هو مرتكبيها ، الذين ليسوا أشخاصاً ذو سلوك غير سوي ، أو يفتقرون للوعي والعلم بل على العكس، فإن مرتكب جريمة القراصنة هو من الأشخاص المتميزين من الناحية العملية والفنية ، وسيتضح ذلك بدراسة المطلب الثاني من هذا المبحث .

٢ - تعريف القرصنة

القرصنة Hackers : مصطلح يطلق على أولئك المرتبطون ارتباطاً وثيقاً لايقبل التجزئة بتطوير الحواسيب وأنظمتها خارج نطاق الهيكل التقليدي للتطوير ، وحركات البرمجيات الحرة (البرامج مفتوحة المصدر الغير تابعة لمصلحة منشأة أو شركة محددة) open source حيث تسمح مثل هذه البرامج لأي مختص أن يقوم بتطويرها أو تعديلها ، وهؤلاء الذين يساعدون في تطوير أو إنشاء برامج جديدة ومشاركة تلك البرامج مع قرصنة آخرين وبناءً على ذلك ، فإن القرصنة هم من يُدخلون ابتكارات جديدة خارج إطار البرمجيات التقليدية ، فهم من يملكون مهارة استثنائية في مجال برمجة الحواسيب ، وبالمقابل هناك قسم من القرصنة cracker من هواة البرمجة ممن يقومون بعمليات اختراق بنية حسنة لا لسرقة معلومات ما ولا للقيام بعملية احتيال عبر الانترنت وليس لهم دور في ابتكار برامج جديدة ، وإنما يقتصر نشاطهم على كسر شيفرات البرامج المحكرة لمصلحة جهة ما ، قد تكون الشركة المنتجة للبرنامج ، أو إنشاء الفيروسات وتعطيل دور المخدم الوظيفي لتلك الشركة لابقصد الأضرار بالشركة ولا للكسب الشخصي الغير مشروع إنما لنفع الصالح العام ونشر المعرفة ، والجدير بالملاحظة أن وسائل الاعلام غالباً ما تخطئ بين هذين المصطلحين عندما يتم ذكرها في وسائط الأنباء .

وبالتالي فإن فلسفة القرصنة تمثل بشكل أو بآخر إلى حد ما إحدى صور المشاركة والانفتاح واللامركزية والتي تساعد على عملية الابتكار وتزويد القاعدة العملية للثقافة ، ومن هنا فإن ثقافة فكرة القرصنة لا تتوافق مع مفهوم سلوك

الشركات المسيطرة على صناعة التكنولوجيا (مثل شركة مايكروسوفت أو شركة أبل) التي تعتمد على تحويل هذه المعرفة إلى مكاسب شخصية (أرباح مالية) أكثر من مفهوم مشاركة المعرفة والإيمان بحرية العلم أو المعرفة .

ومن الواضح أن هذه الثقافة تتعرض لتأثير الشبكات فكلما ازداد عدد الأفراد المساهمين في مشروع معين كلما زاد النفع العائد على كل فرد من هؤلاء الأفراد من ابتكارات يقدموها للآخرين ، ويعتبر هذا من جوهر الأسباب التي جعلت من نظام التشغيل linux (open source) أكثر أمناً من نظام تشغيل ويندوز خلال فترة زمنية قصيرة ، ومرد ذلك إلى أن نظام التشغيل linux غير منتشر على الصعيد الفردي لاستخدام الأفراد وبالتالي فلا يشكل هدفاً للقراصنة لمحاولة اختراقه وذلك يرجع لقصور انتشاره مقارنة مع نظام الويندوز .

بعض المصطلحات الخاصة بعمليات القرصنة :

وبعد دراسة مفهوم عملية القرصنة ، لابد من التطرق إلى بعض أنواعها الأكثر شيوعاً أو بعض الأنواع التي تمت معرفتها حتى الآن .

قرصنة البرامج : حيازة أو استخدام برامج الحاسب بدون ترخيص من المالك .

حصان طروادة : زرع بعض الأوامر خلسة في برامج أو إضافة دارات إلكترونية خلسة في بعض قطع الحاسب وأجهزته .

الفيروس : برنامج يعد خصيصاً ليتم إقحامه خفية في أحد البرامج في الكمبيوتر ومن خصائصه أن تكون لديه القدرة على مضاعفة نفسه وعلى أن ينسخ نفسه في برامج أخرى عند تشغيله في الحواسيب

المتسلل : الهكرز أحد المغرمين بالحواسب والبارعين في علومه والذي لديه الفضول لاكتشاف ماتحتويه حواسيب الآخرين ولكنه يقوم بذلك عن طريق استخدام وسائل غير مشروعة^{٣٦}

أما **المشرع السوري** فقد أورد في المادة ١ من قانون تنظيم التواصل على الشبكة تعريفاً للبرمجيات الخبيثة بأنها : برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الالكترونية أو الشبكة أو تعطيل عملها أو تبطئته أو تخريب محتوياتها أو مواردها أو جمع المعلومات عنها أو عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة ، وقد ورد في التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة من أكثر البرمجيات الخبيثة شيوعاً الفيروسات virus والديدان worm و أحصنة طروادة Trojan hours والبرمجيات التي تتجسس التحكم في جهاز حاسوبي أو منظومة معلوماتية دون علم صاحبها سواء كان

Grok.lsu.edu. "Definition: Hackers And Crackers – GROK Knowledge"^{٣٦}

Base". <http://grok.lsu.edu/Article.aspx?articleId=٧٢٠٣> . راجع المقالة

في الموقع الالكتروني

بغرض السرقة للمعلومات الموجودة عليها أو لاستخدامها في مهاجمة أجهزة حاسوبية أخرى أو منظومات معلوماتية أخرى ... إلخ

٣- أنواع القرصنة

مصطلح القرصنة ليس سيئاً بمعناه الحرفي فكلمة قرصنة لا تعني جريمة أو شخص سيء و جميع الكتّاب في هذا المجال عادة مايستخدمون مصطلح القبة السوداء أو القبة البيضاء أو القبة الرمادية وذلك من أجل تحديد المقصود من معنى كلمة قرصنة وفقاً لسلوك القرصنة ، ولذلك يمكن إدراج القرصنة ضمن عدة تصنيفات وفقاً لما يلي :

٣-١- من حيث سلوك القرصنة

٣-١-١- القبعات السوداء : وهو النوع النمطي المعروف من قبل مستخدمي الانترنت بالمتسلل (HACKERS) وهذا النوع من القرصنة يقومون بانتهاك خصوصية أنظمة الحواسيب واختراق أمنها بغرض تحقيق الكسب الغير مشروع لجلب المنفعة الشخصية للهكر (كسرقة أرقام بطاقات الائتمان - أو الوصول إلى قواعد البيانات للحصول على المعلومات المطلوبة أو الهويات الشخصية ليتم بيعها لدى لصوص الهوية) .

أي أنهم الصورة النمطية الفعلية لمصطلح القرصنة فهم من يجسدون جرائم المعلومات بمعناها الحقيقي ومن يخرج تلك الجريمة إلى حيز الوجود .

٣-١-٢ - القبعات البيض : Crackers هم خبراء في البرمجيات الحاسوبية ولديهم الخبرة الكافية لاختراق أنظمتها، إنما يقومون باستغلال مهاراتهم لأهداف عكس أهداف أصحاب القبعة السوداء (الهاكرز) ويستغلونها لأغراض جيدة بعيدة عن الكسب الشخصي الغير المشروع ومفهوم جريمة نظم المعلومات، على سبيل المثال غالباً مايكون أصحاب القبعات البيضاء هم خبراء برمجة لدى شركات تطوير البرامج أو شركات تأمين الشبكات وبالرغم من مهاراتهم وخبراتهم البرمجية والتي لاتقل شأنًا عن نظرائهم أصحاب القبعات السوداء إلا أن أصحاب القبعات البيضاء يوظفون مهاراتهم في تطوير أنظمة الحماية الالكترونية من قرصنة القبعات السوداء^{٣٧}

٣-٢ - من حيث درجة خبرة المقرصن

٣-٢-١ - الهواة script kiddies : هم من مبتدئي القرصنة المفتقرين للخبرة ، وهم هواة يسعون لاكتساب الخبرة التي تمكنهم من رفع مهاراتهم في القرصنة ، وعادة ما يستخدمون البرامج المطورة من قبل القرصنة المحترفين دون معرفة التفاصيل التقنية وعادة ما يقتصر دور هؤلاء القرصنة على محاولة تخريب بعض المواقع أو لمجرد المشاكسة بدوافع دينية أو سياسية لا أكثر.

^{٣٧}. <http://www.howtogeek.com/١٥٧٤٦٠/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/>
<http://blogs.mcafee.com/consumer/family-safety/٧-types-of-hacker-motivations>.
٢٠١٦ - راجع المقالة في الموقع الالكتروني

٣-٢-٢- القراصنة متوسطي الخبرة intermediate hackers :

يتمتع عادة هذا النوع بقدر من المعرفة بأجهزة الحواسيب وأنظمة الشبكات ولديهم المعرفة الكافية في مجال البرمجة التي تمكنهم من الفهم بشكل نسبي لعملية القرصنة من الناحية التقنية ولكنهم في الوقت ذاته كمبتدئي القرصنة لا يملكون الوسائل ولا البرامج اللازمة للقرصنة وإنما يقومون باستخدام البرامج المطورة من قبل القراصنة المحترفين أو أنهم يستغلون خلل ما أو ضعف ما في برنامج معين ليتمكنوا من اختراق نظامه والسيطرة عليه .

٣-٢-٣- القراصنة المحترفين elite hackers : وهم من يملكون

الوسائل والأدوات والبرمجيات اللازمة للسيطرة على أي جهاز حاسب للتمكن من اختراق نظامه والسيطرة عليه وطمس أثرهم بشكل احترافي^{٣٨}

٣-٣- من حيث غاية القرصنة

٣-٣-١- القراصنة الذين يعملون لحساب الحكومات أو المؤسسات

العسكرية State Sponsored Hackers : حيث يعمل هؤلاء القراصنة من خلال تمويل بعض الحكومات أو المؤسسات العسكرية فكما ذكرنا آنفاً بأن جميع الاختراعات في عالمنا ترجع لأروقة المختبرات العسكرية فحيث كانت القاعدة القديمة تقول من يسيطر على البحار يسيطر على العالم ، فقد تبدلت هذه القاعدة مع التطور الصناعي لتعطي أفضلية التفوق العسكري لمن يملك

^{٣٨} ، David. ٢٠١٠. *Hacker's Underground Handbook*. Lexington، Melnichuk

الجو والآن ومع اندلاع ثورة التكنولوجيا أضحى ذلك المثل يعول التفوق العسكري لمن يملك الفضاء يملك العالم (ويقصد بالفضاء الأقمار الصناعية ومجالات الاتصالات والوسائط المتعددة) وبالتالي فإن هؤلاء القراصنة لا يبتغون المصلحة الشخصية الغير مشروعة من نشاطاتهم وإنما يعملون لحساب الحكومات والمؤسسات العسكرية بهدف تمويلها بالمعلومات المطلوبة .

٣-٣-٢ - **القراصنة المستأجرون Spy Hackers** : تلجأ عادة المنشآت التجارية إلى استئجار بعض القراصنة يعملون لحسابها بغية تحقيق القدر الأكبر من المنافسة عن طريق سرقة الأسرار التجارية لمنشآت تجارية منافسة ، كسرقة خططها التسويقية أو مصادر تمويلها أو أية معلومات تجارية أو نماذج صناعية أو دراسات اقتصادية قد تفيد تلك الشركة في المنافسة التجارية .

٣-٣-٣ - **القراصنة الإرهابيون Cyber Terrorists** : يعمل هؤلاء القراصنة وراء دوافع دينية أو سياسية وغالباً لا يكون لهم أي هدف أو غاية من أعمالهم سوى بث الرعب والخوف بين المجتمعات لخلق الفوضى والذعر بين الأفراد من خلال تعطيل الأنظمة الحاسوبية للبنى التحتية الحساسة أو اختراق مواقعها عبر الانترنت لإيصال رسالة معينة لا مبعثي منها سوى إشاعة الفوضى والرعب بين الناس .

٣-٣-٤ - **القراصنة المحتالون** : هذا النوع غالباً ما يكون العديد من القراصنة يشكلون شبكة احتيالية واسعة هدفها اختراق الحسابات المصرفية أو المؤسسات المالية لتحقيق الكسب الغير مشروع ، وهذا النوع هو موضوع بحثنا هذا ، ومن الجدير بالذكر بأنه لا يمكن حصر أنواع القرصنة بالشكل الكامل

حيث أن طبيعته الانترنت والوسائط المتعددة تجعل من الصعوبة بمكان الحد من تطورها ونشاطها فلم يشهد القرن الماضي عمليات قرصنة لسرقة معلومات شخصية عن أفراد محددة ليتم بيعها لجهات معينة بينما شهد القرن الحالي العديد من تلك الحالات ، بالرغم من مرور أكثر من أربعين عاماً على استخدام الانترنت إلا أن مجال تكنولوجيا المعلومات لايزال يعتبر حديث النشأة ويتميز بالتطور الذاتي الذي يجعل من الصعوبة البالغة الحد من استخدامه أو انتشاره.^{٣٩}

ومن العودة إلى أنواع القرصنة بمختلف أشكالها نجد بأنها قاطبة لاتخرج عن مفهوم الجريمة الالكترونية فبصرف النظر عن سلوك المقرصن أو هدفه أو غايته أو دافعه أو مرجعيته لحساب من ، فإن صلب عمله يقوم على اختراق الخصوصية لمؤسسة أو شخص أو منشأة ما وهو ما يشكل الخطر الأكبر أمام انتشار شبكة الانترنت في العالم أجمع .

وتبعاً لما سبق دراسته يتبين لنا تعدد أنواع جريمة القرصنة ولكن وفي مجال بحثنا هذا سنعترض لنوع واحد من تلك الجرائم وهو قرصنة الحسابات المصرفية .

فحيث أن القراصنة غالباً ماتستهويهم المعلومات المتعلقة بالحسابات المالية لدى البنوك التي تقوم بعملياتها البنكية بواسطة نظام الشبكات سواء

^{٣٩} Siciliano, Robert. ٢٠١١. "٧ Types Of Hacker Motivations – McAfee".

McAfee. [http://blogs.mcafee.com/consumer/family-safety/٧-types-of-](http://blogs.mcafee.com/consumer/family-safety/٧-types-of-hacker-motivations)

[hacker-motivations](http://blogs.mcafee.com/consumer/family-safety/٧-types-of-hacker-motivations). راجع الموقع الالكتروني

كانت شبكة مغلقة أو مفتوحة ، وبالتالي قد تشكل أبسط المعلومات المتعلقة ببيانات أصحاب الحسابات المصرفية كأرقام حساباتهم المصرفية أو معلومات بطاقاتهم الائتمانية أو أرقام هواتفهم النقالة حين يتم استخدامها لإتمام عملية المصادقة أثناء القيام بعملية مصرفية عبر شبكة الانترنت ، وبالتالي تشكل جميع هذه المعلومات هدفاً ذو أهمية بالغة بالنسبة للمتطفلين ، الذين يقومون باختراق أنظمة الحواسيب بهدف الحصول على أية معلومات تفيدهم في عملية القرصنة عبر استخدام برامج خاصة بهم - من تصميمهم - تحقق لهم القدر المطلوب من الحماية وطمس أثرهم لتفادي إمكانية تتبع نقاط اتصالهم وبالتالي كشف عملياتهم وإخفاء هويتهم بشكل مطلق باستخدام أسماء وحسابات وهمية تعينهم على إتمام عملية السرقة دون معرفة هويتهم وغالباً ماتت هذه العمليات عن طريق مجموعة أشخاص وفي مواقع مختلفة من العالم وقد تقوم العملية الواحدة بعدة خطوات وتستهدف عدة حسابات في وقت واحد ، و يكون هدفها النهائي الاختلاس من حسابات العديد من العملاء وتحويلها لعدة حسابات خاضعة لمصلحتهم الشخصية .

وفي معرض هذه الدراسة وللوصول للتكييف القانوني المناسب و السليم لعملية القرصنة لابد من تحليل عملية القرصنة من خلال دراسة خطواتها.

ثالثاً : تحليل خطوات عملية القرصنة

كغيرها من الجرائم ، كذلك جريمة الاحتيال الالكتروني تتطلب وسائل معينة يحتاجها المقرصن لتمكنه من القيام بعملية الاحتيال ، فهو يحتاج بداية لمعلومات شخصية متعلقة بصاحب الحساب و تقنية خاصة بالبرامج المعتمدة من قبل البنك الذي ينوي اختراقه ومن ثم يؤمن وسيلة اتصال تمكنه من الاتصال بشبكة الانترنت ومن ثم يحتاج لعتاد ذو مواصفات أداء عالية وكذلك لبرمجيات خاصة إضافة إلى أنه يجب أن يتمتع بخبرة احترافية في مجالات البرمجة ، وحاجته إلى وسيلة اتصال بشبكة الانترنت لتمكنه من الاتصال بشبكة انترنت واسعة الحزمة تلبي حاجته للسرعة أثناء القيام بتنفيذ عملية القرصنة ، لذلك كان لابد من دراسة كل خطوة على حده بشكل دقيق لمعرفة تفاصيلها وتحديد ماهيتها من الوجهة القانونية .

١ - إصابة البنية التقنية التحتية للهدف بغية جمع المعلومات المطلوبة لعملية القرصنة وتحديد المعلومات الحساسة :

Infect the target's IT infrastructure Locate

sensitive information:

إن عملية القرصنة وإن كانت تعد من الجرائم التي يعاقب عليها القانون إلا أن مرتكبيها يختلفون في صورتهم عن النظرة العامة للمجرم التقليدي فلما كانت عملية القرصنة تعتبر من أكثر عمليات الاحتيال تعقيداً حيث أنه لا يكفي

للمقرصن أن يعتد بالأجهزة والبرمجيات اللازمة لعملية القرصنة ، وإنما عليه أن يتمتع بالمهارة العالية و الخبرة الواسعة في البرمجيات الحاسوبية بالإضافة لأهمية تحليله بالصبر ، فقد يستمر المقرصن في مراقبة شخص ما على الانترنت لعدة أشهر من أجل الحصول على المعلومات اللازمة لبدء عملية القرصنة التي قد تكون رقم بطاقته الائتمانية أو رقم حسابه المصرفي ، وبالتالي فإن المقرصن - مجرم العصر - يختلف تماماً في مفهومه وشخصيته وتحصيله العلمي عن المجرم التقليدي في أذهاننا ، فهو شخص ذو معرفة واسعة ويتمتع بدرجة كبيرة من العلم والخبرة في مجال التكنولوجيا على النقيض تماماً من النظرة العامة للمجرم التقليدي الذي غالباً ما يكون شخص غير متعلم جاهل يفتقر للوعي ، وبالتالي فإن مجرم العصر هذا يستحق الاحترام من الناحية الاحترافية في مجال البرمجيات .

وفي هذا الصدد فهناك العديد من الطرق التي تمكن المقرصن من الوصول إلى المعلومات الأساسية التي تشكل نقطة البدء بالنسبة له لعملية اختراق معينة ،

إن أولى خطوات المقرصن في عملية القرصنة هي التريص لرصد أية معلومات شخصية متعلقة بحسابات مصرفية ، يحصل عليها المقرصن بالعديد من الطرق ، وتعد الطريقة الأكثر شيوعاً هي إرسال رسائل بواسطة البريد الالكتروني للضحية تبدو مشروعة في شكلها ولكنها تحتوي على رابط - خبيث - قد يكون إعلان دعائي أو إعلان يخبر المستخدم بأنه قد تم اختياره ليكون رابحاً لجائزة مالية ما ، أو إعلان لمواقع إباحية ، أو أي موضوع يثير الاهتمام

قد يجبر المستخدم للضغط عليها وبمجرد قيام المستقبل بالضغط على هذا الرابط يكون المقرصن قد حصل على نسخة كاملة من مخزن البريد الالكتروني لهذا الشخص ، ويضيف الباحث في هذا السياق Michael Jordon وهو مستشار الأمن الالكتروني في كبرى شركات الحماية الالكترونية " إن القرصنة عندما يقومون عادة باتباع هذا الأسلوب فإنهم يتوخون الحذر في إرسال رسالة مماثلة إلى جميع العاملين في مؤسسة ما - في حال كان الاستهداف لعاملي المؤسسة بغية الحصول على معلومات معينة - وذلك بغية تجنب أن تُثار الشكوك حول إعلان أو رسالة محددة تصل لجميع العاملين في مؤسسة ما ، وإنما يقوم القرصنة إما باستهداف موظف محدد ولفترة معينة ، أو باستهداف جميع الموظفين ولكن برسائل مختلفة^{٤٠}

من إحدى الطرق التي يلجأ إليها القرصنة في سياق عملهم للوصول إلى قواعد البيانات لمؤسسة ما (وخير مثال على ذلك قضية TARGET) كاستخدام مواقع التواصل الاجتماعية بغية التسلل للحاسب الشخصي لأحد الموظفين ، ومن أمثلة ذلك قيام القرصنة بعملية بحث في مواقع التواصل facebook- عن موظف ما ليس لديه حساب على الفيسبوك فيقومون بإنشاء حساب وهمي له على ذلك الموقع ويقومون بإرسال طلبات صداقة إلى زملائه في العمل تحوي على رسالة الكترونية تحتوي على رابط خبيث بمجرد

^{٤٠} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٨٣

النقر عليه من قبل أحدهم يكون المقرصن قد نجح في تحقيق غايته وقام باختراق الحاسب الشخصي لهؤلاء^{٤١}

فبمجرد إصابة جهاز الحاسب المحمول للهدف فإن البرامج الضارة تمكن المقرصن من السيطرة ولو جزئياً على ملفات هذا الحاسب (العائد لأحد الموظفين) ، ومن الجدير بالذكر إن مجرد إصابة جهاز موظف ما بفيروسات وتمكين المقرصن من السيطرة عليه لا يعني بالضرورة وصول المقرصن إلى معلومات حساسة ولكنه بالوقت ذاته فإنه يساعد المقرصن على الحصول على معلومات تتعلق بالزبائن أو العملاء وأرقام حساباتهم أو أية معلومات أخرى عن أرصدتهم ، أو أنها قد تمكن المقرصن من معرفة الأسماء المستعارة (رقم المعرف الشخصي ID) التي يستخدمها الموظفون لدخولهم لمخدم المؤسسة كأن يكون الاسم المستعار لهذا الموظف هو jane١ فمن البديهي أن يكون هناك jane٢، jane٣..... إلخ

ومن الوسائل الأخرى التي يستخدمها القراصنة في عملية القرصنة هي اختراق مخدمات شبكة شركات الاتصالات الخلوية التي وإن كانت معقدة ومستحيلة نوعاً ما إلا أن ليس هناك ما يحول دون اختراقها ، حيث أن معظم

^{٤١} قد حدث ذلك في كبرى الشركات الأمريكية عندما قام أحد المقرصنين بإرسال رسالة وهمية من المفترض أن تصل لمديره في العمل تحتوي على ملف مرفق عنوانه (سري جداً) حيث قام المقرصن بإرسال تلك الرسالة إلى أحد العاملين وأوهمه فيها أن المحتوى هو ملف سري يقوم بإرساله لمديره في العمل وأنه وصل إلى زميله عن طريق الخطأ وعندما استلم زميله الرسالة قام بالفور بالنقر على محتواها من باب الفضول ليرى ماذا يحوي الملف ، وماكان هذا الملف إلا برنامج خبيث قام المقرصن بزرعه في هذا الملف لتضليل الهدف ليقوم بالضغط عليه ويقع ضحية لعملية القرصنة .

البنوك التي تسمح لعملائها باستخدام الانترنت تتطلب إدخال رقم سري يقوم نظام حماية البنك عادة بإرساله إلى الهاتف النقال للعميل ليقوم الآخر بإدخاله في الخانة المخصصة، وبالتالي فإن المقرصن قد يقوم باختراق مخدمات الشبكة لشركة الاتصالات أو قد يتسلل إلى الهاتف الذكي لهذا العميل للحصول على نسخة كاملة عن رسائله النصية وبالتالي الحصول على الرقم السري للعميل ، والعديد من الطرق الخداعية الأخرى ، كأن يقوم المقرصن بالتواطؤ مع بعض موظفي العميل - لا البنك - الذين قد يكونوا جزء من عملية القرصنة فيما لو كان الحساب خاص بشركة تجارية للحصول على معلومات حساب الشركة المصرفي وقد يحصل ذلك بالتعاون مع بعض موظفي البنوك الذين قد يكونوا جزءاً من شبكة القرصنة ذاتها .

وبالتالي يكون المقرصن قد حصل على المعلومات التي يحتاجها للقيام بعملية القرصنة.

حيث تتطلب عملية هجوم المقرصن على حسابات المصارف معرفة رقم الحساب المستهدف أو الاسم المستعار للعميل على مخدم البنك ، ليتمكن من الدخول إلى شبكة المصرف ومن ثم الوصول إلى قاعدة البيانات الخاصة بالمصرف - وهذا ما سيتم التعرض له مفصلاً في مجال دراسة حالات تفعيل مسؤولية المصارف في القرصنة - وعند الحصول على المعلومات المطلوبة يكون المقرصن قد خطى الخطوة الأهم في التحضير لعملية القرصنة ومن ثم يقوم بالبداية بعملية القرصنة و محاولة اختراق بيانات المصرف والتسلل إليها بشكل غير شرعي لإتمام عملياته

قد لا تكفي مهارة المقرصن وخبرته الواسعة في مجال البرمجيات للقيام بعمليات القرصنة وإنما لابد من اقتنائه لبرمجيات وعتاد ذو مواصفات تقنية خاصة تعينه على إتمام عملياته الاحتمالية فهو يقوم بالتسلل إلى حسابات المصرف حيث تتطلب منه هذه العملية درجة عالية من الدقة والمهارة والتمرس للقيام بها كي يتقضى أثر تتبعه ، وبعد نجاحه في التسلل إلى بيانات المصرف من خلال مخدم المصرف ، يقوم باستخدام رقم الحساب الذي حصل عليه مسبقاً ويقوم باختراق كلمة المرور ليدخل إلى الحساب ليكون بمقدوره التحكم بالحساب بشكل كامل .

٢ - الخطوة الثانية انتظار ساعة الصفر وفق حساسية البرامج

المراد اختراقها - Find a zero day vulnerability:

إن من أهم العوامل التي تؤثر في نجاح عملية القرصنة هو نوعية نظام البرمجيات المستخدم في نظام الشبكة المراد اختراقها .

فعلى سبيل المثال جميع البرامج التي تعتمد على لغة الجافا java معرضة للاختراق - نسبة لغيرها من البرامج - في ساعة محددة وفقاً منظومة عملها التي تضعف فيها جدران الحماية بحالات معينة .

وقد أضاف James Forshaw الباحث في هذا السياق "بأن ٣ مليارات من الأجهزة والتي تستخدمها العديد من الشركات منها (مايكروسوفت ، apple ، ابل ، mirosoft ، فيسبوك facebook) مصممة بلغة الجافا وبذلك يجعل ذلك منها هدفاً سهلاً بالنسبة للقراصنة ، وهو ما يضعف آلية التأمين في

ملفات الجافا الوسائط المساعدة والروابط الإعلانية التي تظهر في متصفحات الانترنت التي تستخدمها ملفات الجافا مايجعل من ملفات الجافا لقمة سائغة بالنسبة للمقرصنين " .

ويوضح الباحث ذاته قائلاً " أن العديد من نقاط الضعف الناشئة عن استخدام ملفات الجافا تعمل بطريق التداخل مع المعالجة (stack walking) والذي يبرر استخدامه من قبل أصحاب الشركات على الرغم من افتقاره للحماية المطلوبة بأنه الملف الأكثر سهولة في استخدامه من قبل العملاء أثناء الاتصال بشبكة الانترنت ، الأمر الغير موجود في أنظمة التشغيل لينوكس linux التي يؤخذ عليها صعوبة استخدامها بالنسبة للمستخدمين الغير مختصين ولكنها تتمتع بدرجة عالية من الحماية "٤٢

وبالتالي يستغل المقرصنين الثغرات الموجودة في أنظمة عمل ملفات الجافا ليتمكنوا من اختراق الحواسيب من خلالها للوصول إلى المعلومات المطلوبة .

٣- الخطوة الثالثة : تبديل نقاط الاتصال - تفادي أثر التتبع) (connection bouncing) - (avoid the impact of :(traceability

٤٢- <http://www.information-age.com/technology/security/١٢٣٤٥٦٩٥٩/how-> .

[to-hack-a-bank--theoretically.](#) -٢٠١٦ راجع المقالة في الموقع الالكتروني

يتمتع أي مخدم من مخدمات الشبكات بنظام حماية ذاتي تكون وظيفته تتبع أي مصدر يحاول الدخول عبر هذا المخدم ، فيقوم نظام الحماية هذا بجمع معلومات عن مصدر الاتصال وعنوان البوابة التي تم الاتصال منها والعديد من المعلومات الأخرى بما فيها البرمجيات والعتاد المستخدم ، ففي حال كان الجهاز المتصل مرخص له بالدخول عبر هذا المخدم فيتم السماح له بإتمام العملية ، أما في حال لم يكن مرخص لهذا المستخدم أو الجهاز أو البرنامج بالدخول عبر هذا المخدم أو في حال حدوث خطأ ما أثناء الدخول فيقوم المخدم بحفظ جميع تلك البيانات ومن ثم يقوم بقطع محاولة الاتصال أو الدخول عند أية محاولة اختراق يتعرض لها المخدم بشكل غير شرعي^{٤٣}

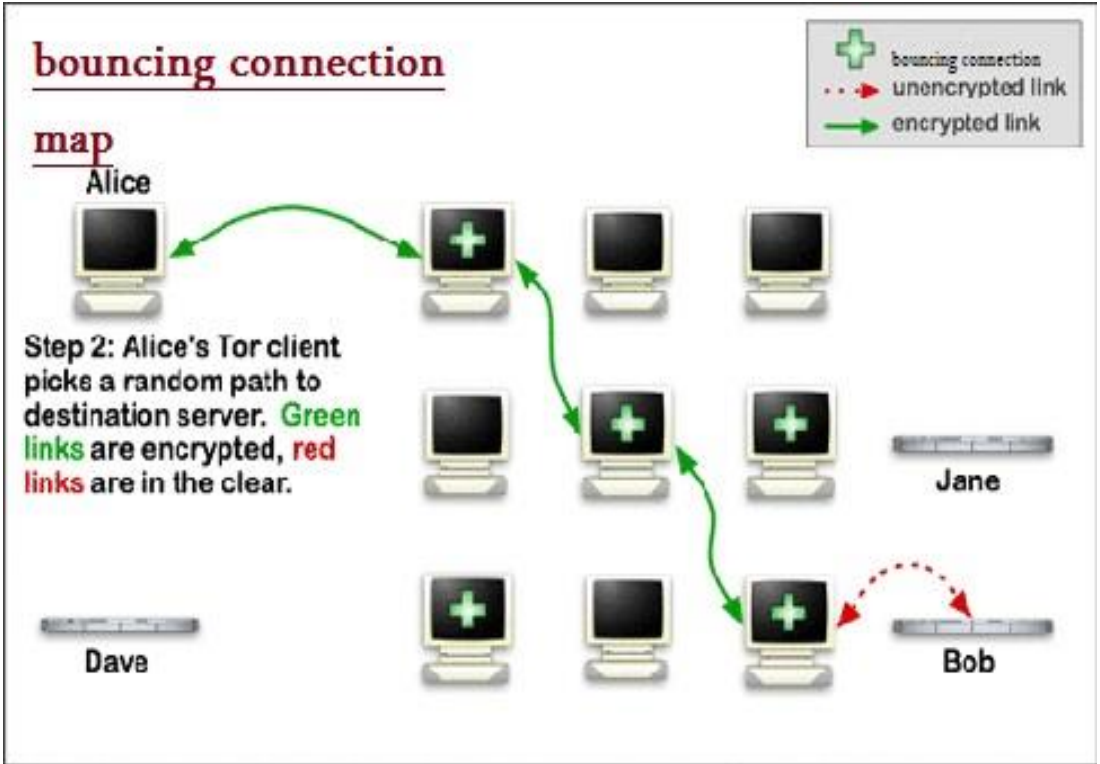
لذلك فإن المخترق بحاجة لاستخدام برامج تقوم بتغيير نقاط الاتصال بشكل متتابع لمحاولة منع المخدم من تتبع مصدر الاتصال وهذه ماتسمى بمرحلة تقادي تتبع الأثر حيث أن المخدم يقوم بتتبع مصدر الاتصال الغير مسموح به مهما تعقدت شبكة نقاط الاتصال المتتابعه وكل مازاد التعقيد يزداد الوقت اللازم لتتبع المصدر الفعلي للاتصال الغير مسموح به^{٤٤}

وهنا يكون المقرصن قد تقادى أثر التتبع وحصل على نافذة زمنية ويكون بالتالي في حالة الرسم التوضيحي الآتي :

^{٤٣} section 1 the basics ،2016. the ultimate uplink guide

^{٤٤} <http://guide.modlink.net/section1.php> ٢٠١٦ راجع الموقع الالكتروني

^{٤٤} Explain for man in the middle (layer).Ibid



٤ - الخطوة الرابعة إنهاء عملية القرصنة بالحصول على المال

Getting the money out

عند نجاح المقرصن باختراق مخدم شبكة المصرف والتسلل إلى بياناته لاستهداف حساب أحد العملاء الذي يكون قد حدده مسبقاً ، يمكنه بعدها التمتع بصلاحيّة التحكم بالحساب بشكل تام ، أو أن يستهدف المقرصن صلاحيّة أحد موظفي البنك للوصول إلى قاعدة البيانات وفي هذه الحالة يستطيع التحكم فيها وكأنه أحد الموظفين المصرح لهم بالوصول إليها والتحكم في حسابات العملاء .

من البديهي ألا يقوم المقرصن بتحويل المبلغ إلى حسابه الخاص فوراً لأن ذلك ببساطة سيؤدي إلى تتبع أثره ومعرفة هويته ومن ثم إحالته للمحاسبة القانونية لذا يقوم بتحويل المال إلى حساب آخر لا يمكن كشف هويته من خلاله . وقد يقوم المقرصنون باستخدام مجموعة حسابات وهمية - لأشخاص وحسابات وهمية - أو أنه يقوم باختراق عدة حسابات في آن واحد لاستخدامها في عملية التحويل تفادياً لأثر التتبع فيقوم باستخدامها لتحويل المبالغ بشكل عشوائي حتى ينتهي الأمر لتحويلها إلى حسابه الخاص بعد تضليل تتبعها ، وقد لا يلجأ المقرصنون إلى حساباتهم الشخصية لإتمام العملية فيمكنه استخدام حساب يسمى (account cashing up) ، حيث يقوم المقرصن بذلك بالاستعانة بحسابات لأشخاص من محيطه الاجتماعي ويقوم بإقناعهم باستقبال بعض الحوالات في حساباتهم الشخصية لأسباب من نسج خياله كأن يستعين بشخص ما ويقنعه بأنه لا يملك حساب مصرفي وبأن عليه تلقي حوالة من أحد ما قد يكون صاحب عمل أو صديق له في مكان آخر ويقوم بعدها باستخدام تلك الحسابات لتحويل المبالغ التي قام بسرقتها إلى هذا الحساب ومن ثم سحبها - دون علم صاحب الحساب الحقيقي بأن الأموال التي تم تحويلها لحسابه هي أموال مسروقة - ومن الواضح بأن هذه الطريقة لا يمكن تطبيقها إلا في عمليات القرصنة التي تستهدف مبالغ متواضعة .

إن تعقيد عملية القرصنة وصعوبة إمكانية تتبعها ومعرفة مرتكبيها تكاد تخلق نوعاً من الفوضى لجهة عدم إمكانية تعيين المسؤولية من جانب أي طرف ، فالبנק الذي تتعرض حساباته للقرصنة قد يكون في منأى عن خطر

المسؤولية لعدم وجود إهمال أو إخلال بالواجبات من خلاله ، وبذات الوقت قد يجعل عملاء ذلك البنك يتحملون وحدهم الخسائر التي قد تنشأ من جراء الهجمات الالكترونية ، مما قد يشكل هاجساً لدى البعض من اللجوء للبنوك ، وبالتالي تنعدم الثقة بالبنوك وقد ينتج عن ذلك كارثة اقتصادية كبيرة ، ومن هنا أصبحت الحاجة ملحة لإيجاد تكييف قانوني واضح لعملية القرصنة من أجل تحديد المسؤوليات وما يترتب عن ذلك من مراكز قانونية لمستخدمي الانترنت ، وبعد دراسة ماهية الانترنت والقرصنة الالكترونية في الفصلين السابقين ، أصبح من الملائم الانتقال في الفصل الثالث من هذا البحث إلى المناقشات القانونية لدراسة مسألة القرصنة وفق النظريات القانونية الفقهية والتطبيقية والتشريعية .

* * *

الفصل الثالث

التكييف القانوني لعملية القرصنة الالكترونية

أولاً : التكييف القانوني لعملية القرصنة الالكترونية

ثانياً : المسؤولية الجزائية عن محاولة القرصنة

ثالثاً : موثوقية التوقيع الالكتروني

١ - ماهية التوقيع الالكتروني

٢ - حجية التوقيع الالكتروني

٢ - ١ - البطاقة المغناطيسية

٢ - ١ - البطاقة الذكية

٢ - ٣ - التوقيع الرقمي لتوثيق معاملات التجارة

الالكترونية

٢ - ٤ - أنظمة التشفير في استخدام التوقيع الالكتروني

الفصل الثالث

التكييف القانوني لعملية القرصنة الالكترونية

نظراً لحدثة نشأة التجارة الالكترونية عموماً وحدثاً جرائم نظم المعلومات عبر الانترنت يكاد لا يوجد تكييف قانوني دقيق لعملية القرصنة الالكترونية وقد يغيب عن تشريعات معظم الدول وجود تشريع خاص ينظم أحكام الجرائم الالكترونية و حتى تشريعات تنظيم التجارة الالكترونية ، مما يلقي بكامله على الفقهاء القانونيين وكذلك السلطة القضائية لإيجاد تعريفاً مناسباً لعملية القرصنة في معرض تصديها لمثل هذه الوقائع ، وبالتالي لاجال في البحث بالمعنى المراد لتكييف عملية القرصنة سوى من خلال القضايا التي نظرت في مواضيع مشابهة عن طريق تحليل حيثيات القضية والتكييف الذي طبقه القاضي لإدراج الوقائع المعروضة أمامه لحكم النصوص القانونية ، فلا تتلاشى المسؤولية ولا تُهدر الحقوق .

أولاً : التكييف القانوني لعملية القرصنة .

لعل الحالة الأكثر انتشاراً والتي تعم على عملية القرصنة هي انتحالهم لشخصية موثقة أو مصرح لها بالدخول إلى أنظمة الاتصال المستهدفة لتحقيق غايتهم الشائنة .

والمقصود بانتحال الشخصية مايعمد إليه المقرصن من استخدام اسم أو عنوان أو مفتاح دخول مصرح له بالدخول ليتمكن من التسلل إلى وحدة تخزين البيانات المستهدفة وقد يحصل ذلك بغاية البساطة فقد نجد الكثير من الإعلانات المشبوهة على شبكة الانترنت على سبيل المثال (تبرع بنصف دولار لمرضى السرطان - أنت الزائر رقم المليون إلى هذا الموقع وقد حصلت على جائزة ... الخ) وماعليك سوى القيام بإدخال بريدك الالكتروني أو رقم بطاقة الائتمان الخاصة بك وبهذا يكون المقرصن هو من صنع هذا الإعلان الزائف لإيقاع الضحايا والحصول على بياناتهم الخاصة والجدير بالذكر أن جريمة انتحال الشخصية من أقدم الجرائم ولا تقتصر على الانترنت ، وإنما تغلغل الانترنت في حياة الأفراد اليومية - وبالأصح تغلغل الأفراد داخل شبكة الانترنت - بات يشكل مجالاً واسعاً للقراصنة للإيقاع بالعديد من الضحايا دون عناء يذكر ، ومن الممكن أن يؤدي ذلك إلى استنزاف رصيد الضحية المصرفي

ورد في قضية عرضت على المحكمة العليا في كاليفورنيا عام ١٩٩٦ أن فتاة ادعت على شركة كبرى مختصة بالبرمجيات بالفصل التعسفي مستندة في ادعائها على رسالة من بريد الكتروني وارد ادعت هذه الفتاة أن رئيسها في الشركة قام بإرسال رسالة إلى المدير التنفيذي تنص " لقد قمت بفصل الموظفة -أدلين - بناء على طلبك " ولكن المدير التنفيذي أنكر بأنه فصل الموظفة لرفضها إقامة علاقة معه مؤكداً أن الرسالة غير صحيحة ، وبعد انتهاء محكمة الدرجة الأولى بحكمها بالتعويض للفتاة وقدره مائة ألف دولار أمريكي ، قام محامي الشركة باستئناف الحكم مؤسماً استئنافه على اعتبار أن الرسالة المزعومة قد أُقحمت داخل الأنظمة الحاسوبية للشركة ، وقد أبرز محامي الشركة للمحكمة سجلات مراقبة الحاسب التي تثبت بأن شخصاً ما قام بالدخول إلى الحاسب الخاص بالشركة من موقع بعيد وليس من داخل النطاق المرخص له بالدخول ضمن الشركة باستخدام رقم المعرف الخاص بنائب الرئيس ، ثم انتقل إلى معرف شخص آخر وظل ينتقل بين رقم المعرف الخاص بنائب الرئيس ورقم المعرف الخاص لهذا الشخص الآخر عدة مرات في نفس اليوم والساعة التي أرسلت فيها الرسالة موضوع التحقيق ، وأثبت نائب الرئيس أنه كان يقود سيارته في ذلك الوقت ويجري بعض المكالمات من هاتفه النقال في اللحظة التي أرسلت فيها الرسالة المزعومة ، وبالرغم من أن المحققين لم يتمكنوا من التأكد من أن البيانات الواردة في سجلات الحاسب الخاص بالشركة تعود للفتاة المدعية إذ أنها قامت بمسح كافة البيانات من حاسبها الشخصي إلا أن المحكمة أدانت الفتاة وحكمت عليها بقضاء عام في السجن وغرامة وقدرها مائة ألف دولار أمريكي بتهمة اقتحام شبكة حاسب وصنع وثيقة مزيفة

والحُث باليمين أمام المحكمة العليا^{٤٥}، ومن مناقشة هذه القضية يتضح بأن المحكمة وبالرغم من عدم وجود تشريع خاص يجرم الاختراق أو القرصنة عبر الانترنت وبالرغم من عدم وجود تعريف دقيق لعملية القرصنة إلا أنها تمكنت من إيجاد التكييف الملائم للقضية المعروضة عليها آنذاك ، والذي سنعرضه لاحقاً في هذا الفصل .

في هذا الصدد لا يقتصر انتحال الشخصية في جرائم نظم المعلومات على انتحال شخصية الأفراد فقط بل يتعدى ذلك إلى انتحال شخصية المواقع أيضاً.

حيث يعتبر أسلوب انتحال شخصية المواقع على شبكة الانترنت من الأساليب الحديثة نسبياً في عالم جرائم نظم المعلومات ولكنه أشد خطورة وأكثر صعوبة في اكتشافه من أسلوب انتحال الشخصية ، ومرد ذلك إلى أن انتحال الشخصية يقوم به المقرصن بمواجهة مخدم الشركة المعنية والتي يفترض بأنها أحاطت بمخاطر الانترنت وحصنت شبكتها قدر الإمكان بالشكل الذي يمكنها من الاكتشاف والتصدي لأية محاولة اختراق ، أما انتحال شخصية المواقع فيقوم على استغلال جهل المستخدم الذي لن يتمكن من اكتشاف الفخ الذي وقع به^{٤٦}.

^{٤٥} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٨٧

^{٤٦} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٨٥

النقطة الرئيسية التي يقوم المقرصن باستغلالها في هذا الأسلوب هو أن أي حاسب على الانترنت يمكنه أن يقحم نفسه في مواقع بينية بين المستعرض الالكتروني الذي يستخدمه الضحية أثناء تصفحة عبر الانترنت ، والجدير بالذكر أن عملية انتحال شخصية الموقع يمكن تنفيذها حتى ولو تم الاتصال من قبل الضحية عبر برامج حماية يظن أنها آمنة فبالرغم من أن كثير من المواقع تشير للمستخدم أنه يتصل عبر النطاق الآمن إلا أن أسلوب انتحال شخصية الموقع يمكنه وبكل بساطة اختراق هذا الحاجز ، حيث أن المستخدم عندما يقوم بالتصفح عبر الانترنت فإنه يقوم بالتنقل من موقع إلى آخر عن طريق سلسلة من العناوين يقود كل منها إلى عنوان آخر حتى يصل إلى الوجهة المطلوبة فإذا قام المستخدم بالضغط على أيقونة معينة للدخول إلى إحدى مواقع الشركات الكبرى مثلاً www.company.com وكان العنوان URL المتربط بهذه الأيقونة على النحو التالي :

www.evil.com/http/www.company.com فإن خادم الموقع سوف يقوم بوصل هذا المستخدم إلى العنوان الذي يريده وهو www.company.com ولكن الاتصالات جميعها سوف تتم من خلال العنوان www.evil.com ويستطيع القرصنة منتهجو هذا الأسلوب إخفاء ظهور الموقع المتوسط وذلك من خلال استخدام برامج بلغة الجافا سكريبت لعرض صفحات الموقع عبر مستعرض الانترنت^{٤٧}

^{٤٧} حسن طاهر داود - جرائم نظم المعلومات - مرجع سابق ص ٩١

وقد عاقب المشرع السوري على انتحال شخصية المواقع أو شغل اسمها بشكل غير مشروع في المادة ١٦ من قانون تنظيم الجرائم المعلوماتية :

شغل اسم موقع الكتروني ..

يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من شغل اسم موقع الكتروني من دون علم صاحبه أو حد من قدرة مالك نطاق على الانترنت على التحكم في هذا النطاق .

وكذلك في التشريع السوري نرى أن المشرع السوري كغيره من المشرعين تجنب إيجاد تعريف أو تكييف واضح لعملية القرصنة واقتصرت نصوص التشريعات المتعلقة بهذا الصدد على وضع تعاريف عدة متصلة بهذا السياق ففي المادة ١ من قانون تنظيم التواصل على الشبكة ورد تعريف الجريمة المعلوماتية جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكية أو تقع على المنظومات المعلوماتية أو الشبكة . وقد ورد في التعليمات التنفيذية لهذا القانون ت ١٥ : تنقسم الجرائم المعلوماتية (جرائم الفضاء السبراني) عموماً إلى نوعين أساسيين الأول : هو الذي يكون فيه الحاسوب مجرد وسيلة تسمح بارتكاب الجريمة وهي غالباً جريمة اعتيادية (مثل جريمة التهديد عن طريق الانترنت) لكن الضرر منها عادة مايكون أعظم ، والثاني : هو النوع الذي تكون فيه المنظومة المعلوماتية أو الشبكة موضوعاً للجريمة (مثل اختراق المنظومات المعلوماتية وتخريبها) وهي غالباً جرائم مستحدثة لا بد من النص على ارتكابها ومعاقتها ، وكذلك أورد تعريف العصابة المنظمة في المادة ١ منه بأنها : جماعة أشخاص أو فعاليات عادة ماتكون ذات تنظيم مركزي تهدف إلى

ممارسة الأنشطة الإجرامية سواء على الصعيد الوطني أو الإقليمي أو الدولي

. وغيرها من الأفعال التي عاقب المشرع على القيام بها دون التطرق إلى تعريفها بشكل دقيق كالاختيال واعتراض المعلومات و إرسال البريد الواعل وغيرها من الأفعال التي سنتطرق إليها في مجال مناقشة المسؤولية الجرائية ، وقد أصاب المشرع بسلوكه هذا النهج كسائر التشريعات المماثلة له وذلك لتجنب تقييد قضاة المحاكم والتضييق عليهم في إدراج الأفعال المرتكبة ضمن المواد النافذة .

والنقطة المنتجة في بحثنا هذا لناحية التكييف القانوني لعملية القرصنة ، نص المادة ٢١ من قانون تنظيم التواصل على الشبكة والتي جاءت بعنوان الاحتيال عن طريق الشبكة حيث نصت على أنه :

الاحتيال عن طريق الشبكة..

/أ/ يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمائة ألف إلى مليونين ونصف المليون ليرة سورية كل من استولى باستخدام الأجهزة الحاسوبية أو الشبكة على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية أو سند يتضمن تعهداً أو إبراء أو أي امتياز مالي آخر وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه بأي وسيلة كانت .

/ب/ وتكون العقوبة الاعتقال المؤقت والغرامة من خمسمائة ألف إلى مليونين ونصف المليون ليرة سورية في الحالات التالية:

١- إذا وقعت الجريمة على ثلاثة أشخاص فأكثر .

٢- إذا تجاوز مبلغ الضرر مليون ليرة سورية .

٣- إذا وقع الاحتيال على مصرف أو مؤسسة مالية .

ج- ولا تطبق الأسباب المخففة التقديرية إلا إذا أسقط المضرور حقه الشخصي .

ونجد بأن المشرع قد جعل جريمة الاحتيال عن طريق الشبكة جريمة جنائية الوصف خلافاً لأحكام قانون العقوبات العام التي تصنف جرم الاحتيال ضمن الجرائم جنحوية الوصف في المادة ٦٤١ ، وبالتالي فإن المشرع السوري وفي تعليماته التنفيذية لقانون تنظيم الجرائم المعلوماتية ، قد أوجد تكييفاً لعملية القرصنة كجريمة احتيال جنائية الوصف ولا تختلف عن جريمة الاحتيال العادية إلا كونها تتم عبر أنظمة معلوماتية وأجهزة حاسوبية ، وقد جاءت التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة مؤيدة لذلك حيث نصت في المادة ٢١ ت ١ مايلي :

تنطبق هذه الفقرة على جرم الاحتيال أو الغش عن طريق الشبكة بقصد إلحاق ضرر مالي بالغير ، ولا تخرج هذه الجريمة عن نطاق جريمة الاحتيال العادية إلا في كونها تستخدم الأجهزة الحاسوبية أو الشبكة في خداع المجني عليه ، أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه.

حيث نصت المادة ٦٤١ من قانون العقوبات العام السوري في أحكام الاحتيال :

١ . كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقولاً أو أسناداً تتضمن تعهداً أو ابراء فاستولى عليها احتيلاً:

إما باستعمال الدسائس .

أو بتلفيق أكذوبة أيدها شخص ثالث ولو عن حسن نية .

أو بطروف مهد له المجرم أو ظرف استفاد منه .

أو بتصرفه بأموال منقولة أو غير منقولة وهو يعلم أن ليس له صفة للتصرف بها .

أو باستعماله اسماً مستعاراً أو صفة كاذبة .

عوقب بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من مائة إلى خمسمائة ليرة .

وبالتالي فإن تكييف عملية القرصنة كجريمة احتيال يتوافق مع أغلب وجهات النظر الفقهية السائدة والمناقشة لموضوع القرصنة حيث أن كافة وسائل الاحتيال المنصوص عليها في القواعد العامة لجرم الاحتيال تصلح لأن ترتكب في العالم الافتراضي وأن يتم إسقاطها على جريمة القرصنة الالكترونية .

ومن دراسة النقاط السابقة وبالرجوع إلى خطوات عملية القرصنة والتي يتضح فيها بأن المقرصن يستخدم وسائل خاصة أثناء عملية القرصنة ليتمكن من التسلل إلى الأجهزة الغير مرخص له بالدخول إليها وذلك لتحقيق مكاسب

شخصية غير مشروعه منتحلاً صفحة شخص ما أو موقع ما أو شركة ما وبالتالي فإن معظم أحكام المحاكم التي تفصل في النزاعات المشابهة تقوم بتكييف عملية القرصنة كعملية احتيال وهذا ما سنعرض لدراسته أثناء البحث في القضايا المتعلقة بمسؤولية المصارف دون وجود تشريع يلزمها بتكييف أو تعريف محدد للقرصنة ومرد ذلك ترك مجال واسع لقاضي الموضوع يمكنه من تكييف الواقع المعروضة أمامه بكل مرونة ، مما دفع بالعديد من الحكومات لاستصدار تشريعات جزائية تعاقب على الاحتيال عبر الانترنت وتجرم مجرد محاولة الاختراق لشبكة ما دون أن تلتفت لإيجاد تعريف أو تكييف لعملية القرصنة ، بيد أن المشرع السوري متميزاً على التشريعات النظيره له قد أوجد ضمن تعليماته التنفيذية تكييفاً قانونياً لعملية القرصنة الالكترونية عندما أدرج جريمة القرصنة تحت جرائم الاحتيال ومشدداً عقوبتها مقابلة مع جريمة الاحتيال العادية ومعاقباً على الشروع فيها استثناءً من القواعد العامة مراعى لخصوصية العالم الافتراضي ، وهذا ما سنتطرق لبحثه في المسؤولية الجزائية في جرائم المعلوماتية .

ثانياً : المسؤولية الجزائية عن عمليات القرصنة

لما كان موضوع هذه الأطروحة يبحث في نطاق مسؤولية البنوك تجاه عملائها الذين تعرضت حساباتهم للقرصنة ، فلا بد من التوسع في مجال المسؤولية المدنية فضلاً عن النواحي الجزائية التي نترك لأصحاب الاختصاص مهمة البحث في هذا المجال آمليين أن نجد مواضيع متصلة بهذا الشأن ، لكن هذا لا يغني عن التعرض للموضوع الجزائي لمعرفة المبدأ القانوني السائد بالنسبة لجرائم نظم المعلومات .

لاشك أن التطور الذي تشهده الوسائط المتعددة الملتيميديا شاقولياً من حيث تنوع البرمجيات والاستمرار في إيجاد وسائل جديدة للتواصل عبر الانترنت ، و أفقياً من حيث اتساع شريحة مستخدمي الانترنت بشكل واسع عالمياً ، يكاد عالم الانترنت يحيط بكافة مجالات الحياة الاجتماعية والعملية والاكاديمية والتجارية والإعلامية والحكومية والعسكرية وغيرها الكثير من المجالات المختلفة ، مما يضع حكومات الدول أمام مسؤولياتها بالتصدي لهذا الاتساع من الناحية القانونية والتنظيمية لما قد ينتج من مخاطر عدة جراء استخدام الانترنت وخاصة مع سهولة ارتكاب الجريمة الالكترونية التي قد يقوم بها أي شخص بصرف النظر عن سنه أو جنسه أو بنيته البدنية .

إن المبدأ القانوني السائد في هذا السياق هو اتجاه التشريعات المعنية في هذا الموضوع إلى إيجاد ضوابط وأحكام صارمة نوعاً ما مقارنة بالجرائم العادية ومرد ذلك إلى خطورة الجرائم الالكترونية على المجتمع نسبة للجرائم العادية لما

فيها من خصوصية تجعل من اليسير ارتكاب هذا النوع من الجرائم ، فعلى سبيل المثال في جرائم السلب بالعنف تتطلب استخدام بعض الأسلحة البسيطة أو تتطلب تمتع المجرم ببنية جسدية تعينه على ارتكاب هذا النوع من الجرائم أو جريمة السرقة الموصوفة عبر تسلق جدران أو أسوار أو كسر وخلع فهي تتطلب بنية جسدية معينة للفاعل تمكنه من القيام بها ، ناهيك عن الحالة النفسية والظروف الخارجية وتأثيرها على الفاعل كتسلله ليلاً وهو مرتبك وحذر خوفاً من إصدار أية أصوات قد تؤدي إلى افتضاح أمره وكشفه كل تلك النقاط التي تشكل بعض الصعوبات على الفاعل قد تدفع من حيث النتيجة إلى فشل الجريمة أو عدول الفاعل عنها ، فجميع هذه النواحي لأوجود لها في الجريمة المعلوماتية التي قد يرتكبها الفاعل في منزله أو مكتبه أو في مقهى عام وهو يحتسي كوباً من الشاي دون أن يشعر بأي تهديد بالخطر ودون أن يتمتع بأي بنية جسدية معينة أو حاجته لأي نوع من أنواع الأسلحة ، مما دفع بالمشرعين إلى تشديد أحكام الجريمة المعلوماتية مقارنة بمثيلاتها العادية ، والتي وصلت إلى حد تجريم مجرد محاولة اختراق الشبكة (الشروع) بصرف النظر عن تحقق النتيجة أو الحصول على المعلومات ، فبمجرد محاولة أحدٍ ما اختراق شبكة مؤمنة فإن ذلك يعد جرماً معاقباً عليه بصرف النظر عن نجاح عملية القرصنة ، فيقول المحامي روبرت وهو من المحامين المتمرسين في قضايا إساءة استعمال الحاسوب " مصطلح القرصنة لا وجود له في التشريعات البريطانية لكن المادة ١ من قانون إساءة استعمال الحاسوب البريطاني عام ١٩٩٠ عاقبت على عملية الوصول الغير مصرح به إلى الحواسيب **unauthorised access to computer material** وبالتالي فقد

وضع التشريع آنذاك مصطلح القرصنة في معرض التفسير القانوني وبالوقت نفسه أراد المشرع محاولة تغطية كافة أعمال القرصنة لتمكين القاضي من تطبيق النصوص القانونية دون قيود وبالتالي لم يسعَ لإيجاد تعريف منضبط لمصطلح القرصنة ، فسعت معظم التشريعات إلى تجريم محاولة الاختراق بصرف النظر عن تحقيق النتيجة فقد نص قانون إساءة استخدام الحاسب البريطاني في القسم الجزائي منه على تجريم الوصول الغير مصرح به إلى الحواسيب وفقاً لمايلي :

١: الوصول غير المصرح به إلى الحاسب ويعاقب عليها بالسجن لمدة ٦ أشهر أو غرامة لا تتجاوز (£ ٥٠٠٠) بعد التعديل الأخير على الغرامة في عام ٢٠١٤).

٢: الوصول غير المصرح به بقصد ارتكاب أو تسهيل ارتكاب المزيّد من الجرائم يعاقب عليها ٦ أشهر أو الغرامة القصوى على ملخص الإدانة، أو ٥ سنوات أو غرامة على لائحة الاتهام.

٣: التعديل غير المصرح به داخل الحواسيب ، يخضع لنفس أحكام المادة ٢ من هذا القانون".

وفي ذات السياق تبنت هذا المبدأ معظم التشريعات في الولايات المتحدة وأوروبا عموماً .

وفي التشريع السوري نظم المشرع السوري أحكام الجريمة المعلوماتية في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الصادر

بالمرسوم ٢٠١٢/١٧ والذي نص في الفصل الثالث على موضوع مكافحة الجريمة الالكترونية حيث نصت المادة ١٥ (يعاقب بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية كل من دخل قصداً بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع الكتروني على الانترنت ، دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك)

وقد جاء في التعليمات التنفيذية لهذا القانون ت ١ : تنطبق هذه الفقرة بوجه خاص على كل من يخترق جهازاً حاسوبياً أو منظومة معلوماتية أو موقع الكتروني سواء أكان ذلك عن بعد أي عن طريق الشبكة بأي وسيلة كانت مباشرة أم غير مباشرة أي بالدخول كمستخدم لا يملك الحق أو الصلاحية أو التصريح اللازم للقيام بذلك ، ومن ذلك سرقة بيانات الدخول ، ولا ينطبق الحكم المذكور في هذه الفقرة على الدخول غير المقصود الذي لا ينطوي على إجراءات يقوم بها الفاعل بهدف تجاوز الحمايات الموضوعية أو الالتفاف عليها.

وبالتالي يكون المشرع السوري قد نحى منحى التشريعات المقابلة له في هذا السياق وذلك بتجريمه الشروع في الجريمة المعلوماتية حيث نصت المادة ٣١ من قانون تنظيم التواصل على الشبكة على مايلي (يعاقب على الشروع في الجنب المنصوص عليها في هذا القانون وفق الأحكام الواردة في قانون العقوبات النافذ) ، حيث تنص المادة ٢٠١ من قانون العقوبات العام السوري على أنه (لا يعاقب على الشروع في الجنحة وعلى الجنحة الناقصة إلا في الحالات التي ينص عليها القانون صراحة) وبالتالي فإن المادة ٣١ من قانون

تنظيم التواصل على الشبكة عاقبت على الشروع في الجرح المنصوص عليها في هذا القانون .

وقد أصاب المشرع السوري بالمعاقبة على الشروع في القرصنة أي مجرد محاولة القرصنة و إن لم تتجس تلك العملية وأضافت كذلك الفقرة ب من المادة ١٥ من قانون تنظيم التواصل على الشبكة بتشديد العقوبة لتصبح (الحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة ألف ليرة سورية إلى خمسمائة ألف ليرة سورية إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها ، أو إلغائها أو تغييرها أو تشويهها أو تزيفها أو استخدامها أو إفشائها) وهذه الحالة فيما لو نجحت عملية القرصنة وتمكن المقرصن من التسلل إلى الهدف .

وفيما يتعلق بجريمة القرصنة ذهب التشريع السوري إلى أبعد من ذلك ، فعلى سبيل المثال وكما ذكرنا سابقاً إن عملية القرصنة تبدأ نواتها بالحصول على معلومة واحدة (كرقم البطاقة الائتمانية أو رقم الحساب المصرفي أو اسم المستخدم لأحد مستخدمي الشبكة) وقد يعتمد المقرصن للحصول على تلك المعلومات دون أن يقوم بالتسلل إلى أية منظومة على الشبكة ، فقد يحاول القرصنة الحصول على تلك المعلومات بالخداع أو التحايل كأن يحاول استغلال جهل أحدهم بسرية معلوماته المصرفية أو معلوماته المطبوعة على بطاقته المصرفية أو رقم حسابه المصرفي عن طريق إرسال رسالة احتالية قد يكون محتواها (أرسل رقم حسابك المصرفي أو رقم بطاقتك الائتمانية لتتبرع لرعاية مرضى السرطان بمبلغ مائة ليرة سورية ، وغيرها الكثير من الوسائل) ،

فهنا يكون المقرصن قد حصل على تلك المعلومات دون الحاجة لأيّة عملية قرصنة ، ومعالجة لهذه الحالة فقد نص المشرع السوري على نص خاص في المادة ١٨ من قانون تنظيم التواصل على الشبكة بعنوان (اعتراض المعلومات) ونصت الفقرة أ من هذه المادة على أنه (يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة ألف ليرة سورية ، كل من اعترض أو التقط قصداً بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها)

وجاء في التعليمات التنفيذية لهذه الفقرة ت ١ : تنطبق هذه الفقرة على كل من أقدم قصداً بوجه غير مشروع على اعتراض أو التقاط المعلومات المتداولة على منظومة معلوماتية أو على الشبكة ، أو تنصت عليها بوسائل المعلوماتية وذلك عند نقلها من أو إلى أو في منظومة المعلوماتية سواء أجرى استغلال هذه المعلومات لاحقاً أم لا ويفترض في هذا الفعل أيضاً أن تكون المعلومات المعنية غير متاحة أصلاً لاطلاع عامة الجمهور عليها أي لايمكن الوصول إليها إلا من قبل المخولين بذلك .

وقد أصاب المشرع في النص بهذا التفصيل على هذه الفقرة حيث أنه قد تتعدد حالات تطبيقها في الواقع العملي فعلى سبيل المثال قد يقوم أحد موظفي مصرف ما أو أحد الموظفين الفنيين الذي يقومون بصيانة أجهزة حواسيب المصرف بتحميل برنامج^{٤٨} يسجل ضربات لوحة المفاتيح على الحاسب

^{٤٨} يعرف هذا البرنامج باسم keylogger وهو برنامج احترافي يقوم بتسجيل كافة الضربات لوحة المفاتيح للحاسب ويضعها ضمن ملف ويتم أرشفتها لتسجل تقريراً كاملاً عن كل ضغطة رز على لوحة المفاتيح من =

وبالتالي قد يقوم هذا الموظف بتحميل هذا البرنامج على حواسيب المصرف لتسجل كل ضربة على لوحة المفاتيح وبالتالي يكون قد حصل على تقرير كامل عن أية معلومة حول أي حساب ، وبالتالي فإن استخدام برنامج كهذا يخرج عن زمرة البرامج الخبيثة المنصوص عليها ضمن التعاريف الواردة في المادة ١ من قانون تنظيم التواصل على الشبكة وبالتالي يبقى خارج تطبيق أحكام نص المادة ١٩ التي تعاقب على تصميم أو ترويج أو استخدام البرمجيات الخبيثة ، ولذلك خص المشرع اعتراض المعلومات بأحكام خاصة في حالة اعتراض المعلومات عن طريق الشبكة ، بل وأضاف في الفقرة ب من المادة ١٨ من قانون تنظيم التواصل على الشبكة (يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مائة ألف إلى خمسمائة ألف ليرة سورية كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة المعلوماتية أو الشبكة يمكن استغلالها لأغراض جرمية) وجاء في التعليمات التنفيذية لهذه المادة أنه تنطبق هذه الفقرة على كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة سواء أكان ذلك باستخدام البريد الإلكتروني أو بانتحال أسماء أو محتوى المواقع الإلكترونية أم بأية وسيلة أخرى .

= قبل مستخدم الكمبيوتر ، ومن الممكن استخدام هذا البرنامج على شبكة تربط بين عدة حواسيب وبالتالي سيقوم هذا البرنامج بتسجيل كل ضربة زر لكل حاسب وسيحفظها ضمن ملف كسجل تقرير والجدير بالذكر أن هذا البرنامج لا يصنف ضمن البرامج الخبيثة malwar فعادة ما تستخدمه بعض الشركات لضبط عمل موظفيها - <https://techterms.com/definition/keylogger> , راجع الموقع الإلكتروني .

ويبدو أن المشرع السوري قد انتهج نهجاً صارماً في مواجهة عمليات القرصنة كجريمة معلوماتية مفاده تجريم كل فعل يتصل بموضوع القرصنة بأي شكل أو وسيلة سواء ما يشكل أفعال تحضيرية أو تنفيذية أو تمهيدية أو أي فعل قد يسهل أو يسهم في اتمام عملية القرصنة ، فجاء نص المادة ١٩ فقرة أ من قانون تنظيم التواصل على الشبكة بتجريم تصميم البرمجيات الخبيثة والترويج لها بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمائة ألف إلى مليونين ونصف المليون ليرة سورية ، أي أن المشرع قد أسبغ الصفة الجنائية على جريمة تصميم وترويج البرامج الخبيثة لأغراض إجرامية ، وهذا عين الصواب إذ أن الحلقة الفعالة في جريمة القرصنة هو توافر البرامج الخبيثة التي لا غنى عنها في عملية القرصنة .

وكذلك نصت الفقرة ب من المادة ١٩

(يُعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية، كل من استخدم البرمجيات الخبيثة، أيّاً كان نوعها، وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة) وقد نصت التعليمات التنفيذية ت ١ تنطبق هذه الفقرة على كل من استخدم البرمجيات الخبيثة، أيّاً كان نوعها، وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة ، أي أن استخدام البرمجيات الخبيثة أو دراستها و الاطلاع عليها لأغراض البحث والتطوير، أو بهدف التصدي لها، لا يدخل في نطاق تطبيق هذه الفقرة ، وهنا نجد بأن المشرع قد اشترط في هذه المادة توافر القصد الخاص لتفعيل نصها وتطبيق حكمها ، حينما نص في نهاية الفقرة أ بعبارة أغراض جرمية أي أنه لتفعيل نص

هذه المادة لابد من توافر القصد الجرمي الخاص للفاعل فمجرد تصميم بعض البرامج وترويجها لا يشكل جرمًا ما لم يتوافر القصد الخاص لدى الفاعل لاستخدامها لأغراض جرمية ، وكذلك في الفقرة ب حينما جاء في نصها عبارة بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة ، فكثيراً ما قد يقوم البعض باستخدام بعض البرامج الخبيثة دون أن يتوافر لديه القصد بالإضرار بأي جهاز حاسوبي (ومثال ذلك قيام المستخدم بزيارة بعض المواقع المحجوبة عن سورية كموسوعة ويكيبيديا العملية باستخدام برامج تأمين قناة مفتوحة tunnels والشائعة باسم كاسر البروكسي) وفي هذه الحالة يبقى المستخدم بمنأى عن أثر تطبيق نص هذه المادة .

ومن هنا نجد أن المشرع السوري قد أحاط بشكل وافي بكافة الأفعال التي قد يترتب عليها ضرر مادي أو معنوي أو قد تكون جزء من الجريمة المعلوماتية أو تسهل ارتكابها ، وقد ختم المشرع أحكام تطبيق القانون الجزائي على الجرائم المعلوماتية في المادتين ٢٨ و ٣٠ حيث نصت المادة ٢٨ من قانون تنظيم التواصل على الشبكة على مايلي :

((تطبيق القوانين الجزائية ..

/أ/ اذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون تطبق العقوبة التي هي أشد .

/ب/ يضاعف الحد الأدنى للعقوبة المقررة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين ..

١- إذا ارتكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة .

٢- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها)).

ويتضح من نص هذه المادة بأن المشرع بالرغم من سنه لنصوص تشريعية خاصة بجرائم المعلوماتية إلا أنه لم يرغب بحصرها ضمن أحكام هذا القانون وبالتالي يكون نص المادة ٢٨ قد أحال لأحكام قانون العقوبات العام أي فعل جرمي يرتكب ولايجد له قاضي الموضوع تكييفاً ضمن أحكام القوانين الخاصة ولايبقى الفاعل بمنأى عن العقاب .

أما المادة ٣٠ من قانون تنظيم التواصل على الشبكة احتوت على ظروف تشديد للجريمة المعلوماتية حيث جاء في نصها :

تشديد العقوبة..

تشدد العقوبات وفق القواعد العامة للتشديد المنصوص عليها في قانون العقوبات النافذ في الحالات التالية ..

١- إذا كان موضوع الجريمة يمس الدولة أو السلامة العامة .

٢- إذا جرى ارتكاب الجريمة بواسطة عصابة منظمة .

٣- إذا وقعت الجريمة على قاصر أو من في حكمه .

٤- إذا استغل مرتكب الجريمة عمله الوظيفي لارتكاب الجريمة .

ونظراً لخطورة هذا النوع من الجرائم والتي غالباً مايكون الضرر الناجم عنها أكبر بكثير من أن يعوض قانوناً من خلال المؤيدات الجزائية كون الأضرار

الناجمة عن هذه الأفعال قد تبلغ مئات ملايين الدولارات ، ومن غير المقبول منطقياً أن يجبر ضرر أصاب شخصاً ما ويقدر بمليوني دولار على سبيل المثال أن يقبل هذا الشخص بحبس الفاعل لعدة سنوات في حال تمت معرفته - وهذا في الحالات النادرة عملياً - ولا يقبل العقل البشري ولا المنطق القانوني أن تبقى حوادث كهذه دون تعويض فعلي ، ، لهذا فإن التشريعات الجزائية في هذا الصدد لن تلبى الغاية المطلوبة في هذا المجال ولن تشكل الرادع الحقيقي أمام المقرصن الذي قد يجني من عملية واحدة مبالغ طائلة وهو مدرك بأن نسبة اكتشافه وتعرضه للمسؤولية الجزائية والتي قد لا تتجاوز الحبس لمدة خمس سنوات هي نسبة ضئيلة جداً لدرجة أنها غالباً ما تتعدم هذه النسبة أمام مهارته العالية في مجال البرمجيات .

لهذا فالاتجاه السائد حالياً في خضم الدراسات القانونية المعنية بمجال مكافحة القرصنة والجريمة المعلوماتية هو إيجاد تشريعات تلزم البنوك والشركات والمؤسسات المالية التي تقدم خدماتها عبر الانترنت أن تخضع لأحكام صارمة في حماية حساباتها وحسابات عملائها وأنظمتها المعلوماتية بالإضافة إلى إلزام تلك الشركات أو المؤسسات المالية أو المصارف بإخبار عملائها عن أي محاولة لاختراق حساباتهم و في هذا الصدد دعت العديد من مراكز الأبحاث الأمريكية لإيجاد تشريع اتحادي يهدف إلى إجبار الشركات الأمريكية لتكون أكثر استعداداً عندما يتم فقدان بيانات بطاقات الائتمان والمعلومات الاستهلاكية الأخرى في عمليات الخرق الذي تتعرض له عبر

الانترنت مثل العملية التي استهدفت شركة سوني، وكذلك شرك تارغيت ،
وشركة هوم ديبوت في العام ٢٠١٤.

حيث إن هذه الأخطار المحدقة بالبيانات الشخصية تتطلب من الحكومة
الأمريكية إيجاد وسائل حماية تصون حقوق الأفراد عن طريق قانون حماية
موحد يلزم الشركات المعنية إبلاغ عملائها في غضون ٣٠ يوماً من اكتشاف
أن البيانات الخاصة بهم قد تعرضت لمحاولة اختراق وقال الرئيس الأمريكي
في كلمة ألقاها أمام لجنة التجارة الاتحادية " أن التشريعات الحالية من قوانين
الدولة لا تحمي المواطنين الأمريكيين بالشكل الأمثل ويتوجب علينا تحميل
الشركات في جميع أنحاء البلاد عبء المشاركة في حماية حقوق الأفراد تبعاً
لقاعدة تحمل المخاطر"^{٤٩}

^{٤٩} Michael. ٢٠١٥. "Obama To Call For Laws Covering Data ،Singer
Hacking And Student Privacy". *Nytimes.Com*.
[http://www.nytimes.com/٢٠١٥/٠١/١٢/us/politics/obama-to-call-for-laws-
covering-data-hacking-and-student-privacy.html?_r=٠](http://www.nytimes.com/٢٠١٥/٠١/١٢/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=٠). راجع الموقع

ثالثاً : موثوقية التوقيع الالكتروني

لما كان التوقيع يتمتع بأهمية كبيرة في التصرفات القانونية لما يترتب عليه من أثر في ثبوت الحق وإقرار الموقع بمحتوى المستند الموقع من قبله ، وقبوله بما يتضمنه من التزامات ، إضافة إضفاء القطعية على التصرف بأنه قد صدر من قبل صاحب التوقيع دون أدنى شك ، لكن هذه الأهمية للتوقيع تأخذ الحيز الواسع لها في الأهمية ضمن بيئة المستندات الورقية التقليدية وذلك لاستحالة إمكانية تزوير بصمة شخص ما أو تقليد توقيعه الذي يمكن دحضه من خلال الخبرة التي تجريها المحاكم فيما يتصل بهذه المواضيع ، بينما يختلف المبدأ في المعاملات الالكترونية سواء بالنسبة لآلية التوقيع وكيفيته أو لجهة إثبات موثوقية هذا التوقيع - إثبات بأن التوقيع قد صدر بالفعل من صاحب التصرف المنسوب إليه - فعلى سبيل المثال صدور مستند عن بنك ما ممهور بخاتم البنك وموقع من المدير المختص بشكل أصولي هو دليل قطعي وحجة قاطعة على صاحب التوقيع (البنك) ، وكذلك قيام العميل بالتوقيع على أمر التحويل أو طلب السحب أمام الموظف المختص هو كذلك حجة قاطعة على صاحب الحساب ودليل قاطع على اتجاه إرادة العميل لإتمام تلك العملية ، لكن النقاش يثور في مدى تطبيق هذه القواعد في العالم الافتراضي ، فعند قيام أحدنا بدفع فاتورته عبر شبكة الانترنت من خلال حسابه المصرفي الذي يتضمن خدمات تسديد فواتير عبر شبكة الانترنت ، فهو بذلك يقوم بإدخال توقيع الكتروني لإتمام عملية التحويل من حسابة إلى الحساب المراد التحويل إليه ، وكذلك قيام أحدنا بسحب مبلغ من المال من حسابه بواسطة الصراف الآلي فهو كذلك

يستخدم توقيع الكتروني ، أو قيام أحدنا بعملية شراء عبر شبكة الانترنت مستخدماً بطاقته المصرفية في تسديد الثمن ، و السؤال المطروح في هذه المسائل، مامدى حجية إدخال الرمز الشخصي PIN كتوقيع الكتروني على صاحب الحساب ؟

فقد يكون المقرصن هو من قام باختراق الأنظمة المعلوماتية لمؤسسة ما وقام بتشويه محتوى حزمة البيانات وأقحم داخلها مايوهم الحاسب بأنه تم بالفعل إدخال التوقيع الالكتروني .

في هذا الصدد لابد من البحث في ماهية التوقيع الالكتروني وموثوقيته ومدى ثبوته وحجيته على صاحب التصرف من خلال دراسة التوقيع الالكتروني وماهيته وصوره وأشكاله ووظائفه .

١- ماهية التوقيع الالكتروني

إن صفة الإلزام لعقد أو مستند ما ، تتطلب وبالضرورة في مختلف الحالات قيام جميع الأطراف بالتوقيع على ذلك المستند ، ففي وقت سابق وعندما كان معظم الناس أميين ، وبالرغم من عدم معرفتهم للكتابة لم تتجرد الوثائق المنظمة بينهم من التواقيع سواء بالرسوم أو الأختام أو بصمة الإصبع ، وفي مرحلة متقدمة جاء التوقيع بخط اليد والمكتوب من قبل الموقعين بديلاً عن بصمة الإصبع والأختام.

ويعرف التوقيع التقليدي بأنه : ((علامة أو إشارة تميز شخصية الموقع وتعتبر عن إقراره و التزامه بمضمون السند الموقع من قبله))، والجدير بالذكر أن التشريعات لم تتطرق لتعريف قانوني محدد للتوقيع ، لذلك فإن معظم التشريعات تتبنى المبدأ الواقعي لتعريف التوقيع بأنه أي علامة أو إشارة تكون كافية في حال ثبوتها لتمييز شخص الموقع ولاتجاه نيته إلى الالتزام بمضمون الوثيقة الموقعه وقرينة قاطعة على علمه بفحواها وقبولها بشكل تام ، وبالتالي يتيح ذلك المجال لإمكانية إلزامه بتصرفاته الصحيحة والتزاماته الصادرة عنه في حال نكوله عنها ، أو تحديد مسؤوليته أو اكتسابه للحقوق في أحوال لامجال لحصرها في واقع الحياة^{٥٥}

^{٥٥} محمد سعيد أحمد اسماعيل - أساليب الحماية القانونية لمعاملات التجارة الالكترونية - مرجع

وبعد الانتشار الواسع الذي حققته التجارة الالكترونية ، كان لابد من إيجاد طريقة لضبط المعاملات التي تتم عبر شبكة الانترنت تحل محل التوقيع التقليدي بحيث تتلائم مع ماهية التجارة الالكترونية و تضمن أن من قام بالتصرف في الواقع هو الشخص المعني أو صاحب الحق أو الصلاحية في ذلك .

هناك العديد من الوسائل التقنية في الوقت الحاضر تتيح للوثائق الالكترونية بأن تتمتع بالحجية القانونية و تكون موقعة من قبل الشخص المعني ، وتختلف هذه الوسائل و تتنوع بشكل كبير تبعاً لطبيعة أنظمة البرمجة في فلك تطورها .

من هذه التقنيات التوقيعات الرقمية والتوقيعات البديلة (البيوغرافية) وتعتبر التوقيعات الرقمية هي الأكثر استخداماً حيث تعتمد على التشفير اللامتناظر ، وباستخدام تلك التقنيات أصبح من الممكن إخضاع المعاملات التي تتم على شبكة الانترنت لآلية التوقيع ضمن السجلات و الملفات التي تتضمن بيانات مخزنة إلكترونياً على الحواسيب وأياً كانت الوسائل التقنية المومي إليها والمستخدمة في آليات التوقيع وتخزينها في سجلات خاصة لإمكانية التحقق منها فالهدف الأساسي من ذلك هو إيجاد نظائر لوظيفة مايلي:

. التوقيعات الخطية .

. طرق التوثيق الأخرى المستخدمة في البيئة الورقية (كالأختام والشعارات) .

ومن الممكن ان تؤدي هذه التقنيات وظائف إضافية في مجال التجارة الإلكترونية مستمدة من وظائف التوقيع لا وجود لها في بيئة المعاملات الورقية ، فقد يستطيع شخص ما إثبات اسمه أو أن يشير بعلامة أو إشارة الي مستند معين لأسباب عديدة فعلى سبيل المثال عندما يرسل أحد الأشخاص رسالة إلكترونية من خلال بريده الإلكتروني ويضع اسمه في أسفل الرسالة فإن تصرفه هذا يمكن أن يشير إلى عدة أمور مثل :

أ- التعريف الشخصي بهويته كمحرر أو منشئ لمضمون الرسالة .

ب-الموافقة على عقد أو التزام ما .

ت-قد تختتم الرسالة بقوله وهذه هي الرسالة التي قد استلمت فإذا قام زيد بإرسال رسالة إلى عمر وقام عمر بإعادة إرسالها مع موافقته على العرض الوارد في الرسالة وتطابقت النسختان عندئذ يفيد ذلك بأن الرسالة الموجهة من عمر هي رسالة صحيحة ولم تتعرض لأي تحريف .

ويعرف قانون التوقيع الإلكتروني للتجارة الداخلية والعالمية الأمريكي التوقيع الإلكتروني في المادة ١٠٦ بأنه :

((يعني صوت الكتروني أو رمز أو عملية مضافة إليها أو مرتبطة منطقياً بعقد أو سجل آخر وتبني من قبل شخص يقصد توقيع السجل الإلكتروني)) ويلاحظ بأن المشرع الأمريكي قد تبني التعريف الوارد في قانون الأونسيترال UETA النموذجي بشأن التوقيعات الإلكترونية لعام ٢٠٠١ ،

بالوسائل التقنية التي ينتج عنها التوقيع الالكتروني باعتباره نظيراً وظيفياً للتوقيع الخطي وتتضمن الفقرة أ من المادة ٢ من هذا القانون تعريفاً للتوقيع الالكتروني بأنه ((بيانات في شكل الكتروني مدرجة في رسالة بيانات مضافة أو مضافاً إليها أو مرتبطة بها منطقياً يجوز أن تستخدم لتعيين هوية الموقع بالنسبة رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات)) .

ويبدو بأن فريق العمل الذي قام بإعداد مشروع هذا القانون كان يقصد من هذا التعريف بأن يشمل التوقيع الالكتروني جميع الاستعمالات التقليدية للتوقيع الخطي لأحداث الأثر القانوني المطلوب ، سواء لناحية تعيين هوية الموقع أو بيان نيته للتوقيع ، ولكن يؤخذ على هذا التعريف بأن التقنيات المستخدمة لإنشاء التوقيع الالكتروني يمكن أن تستخدم لأغراض أخرى ذات دلالة قانونية.

ويعتبر مبدأ النظر القانوني أحد المعالم الرئيسية لقانون الأونستيرال النموذجي بشأن التجارة الالكترونية

يهدف مبدأ النظر الوظيفي إلى الاعتراف بالتوقيع الالكتروني باعتباره نظيراً وظيفياً للتوقيع الخطي

وقد عرّف التوجيه الأوروبي رقم ٩٣ لعام ١٩٩٩ الخاص بالتوقيعات الالكترونية التوقيع الالكتروني ((بيانات في شكل الكتروني مضافاً إلى أو مرتبط منطقياً مع بيانات أخرى والتي تعمل كطريقة للتصديق))

بيد أن التوجيه الأوروبي أضاف شكلاً آخر يدعى بالتوقيع الالكتروني المعزز ويقصد به التوقيع الالكتروني الذي يحقق الشروط التالية :

أ- يرتبط بصفة منفردة بالموقعين

ب- إمكانية تمييز الموقعين وتحديد هويتهم

ت- ينشأ بوسائل أو تقنيات يستطيع الموقعين من خلالها أن يظلوا

تحت سيطرته الوحيدة

ث- يرتبط بالبيانات التي تتعلق بها (المضافة إليها) وبهذه الطريقة

يمكن كشف أي تغيير لاحق يطرأ على هذه البيانات^{٥١}

و في التشريع السوري عرف المشرع السوري في المادة ١ من القانون رقم ٤ لعام ٢٠٠٩ والخاص بالتوقيع الالكتروني وخدمات الشبكة بأنه : التوقيع الإلكتروني Electronic signature: جملة بيانات تُدرج بوسيلة إلكترونية على وثيقة إلكترونية وترتبط بها، وتتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أي شكل آخر مشابه، ويكون لها طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره وينسب إليه وثيقة إلكترونية بعينها.

والجدير بالملاحظة أن غالبية الصيغ المستخدمة في تعريف التوقيع الالكتروني تتضمن عبارات (المضافة إليها أو المرتبطة بوثيقة ما أو بعملية أو بتصرف آخر منطقي) وذلك لإحاطة مختلف حالات و عمليات استخدام التوقيع الالكتروني ، فحيث أن التوقيع التقليدي جرت العادة أن يكون بديل

^{٥١} محمد سعيد أحمد اسماعيل - أساليب الحماية القانونية لمعاملات التجارة الالكترونية - مرجع

السند ليكون دليلاً على قبول وإدراك الموقع لما قام بالتوقيع عليه أعلاه وبالتالي يفترض قراءته وإدراكه واستيعابه لجميع العبارات والدلائل والكلمات التي تسبق التوقيع والواردة في متن الوثيقة واتجاه إرادته لقبولها وقبول ما ينشأ عنها من التزامات ، الأمر الذي لأوجود له في أغلب حالات استخدام التوقيع الالكتروني ، وكذلك في عملية الدفع الالكتروني عبر الصراف الآلي يتوجب على الدافع إدخال رمز التعريف الشخصي personal identification number=pin الخاص ببطاقته الانتمانية والذي يقوم بوظيفته التوقيع الالكتروني دون أن يكون في هذه الحالة أي قبول أو اتجاه نية للالتزام بأمر ما قانوناً وإنما تكون الغاية منه ثبوت إجراء عملية الدفع من قبل الشخص الصحيح دون غيره و موافقته المفترضة على عملية الدفع .

وهنا موضع الدراسة في هذا البحث ، إذ من الضروري معرفة مدى موثوقية التوقيعات الالكترونية في المعاملات التي تجري عبر الانترنت و مدى حجيتها تجاه أصحابها الحقيقيين ، فعندما يقوم شخص ما بتحويل مبلغ معين من حسابه المصرفي إلى حساب آخر عبر شبكة الانترنت فإنه يقوم بذلك باستخدام التوقيع الرقمي ، فما هي مدى حجيه إدخال هذا الرمز تجاه صاحب الحساب فيما لو تم اختراق حسابه وقام المقرصن بتحويل مبالغ مالية من هذا الحساب إلى حساب آخر بشكل أصولي مجتازاً كافة إجراءات الحماية ومتخظياً أسئلة الأمان ؟

هل يعتبر استخدام التوقيع الرقمي pin personal identification number حجة قاصرة وقاطعة على صاحب التوقيع بأن عملية التحويل قد صدرت من قبله بشكل مطلق ؟ هذا ما ستتم دراسته مقدماً .

٢- حجية التوقيع الالكتروني

يتيح مجتمع المعلومات الحديث بالتقنيات المتاحة أن يرفق أو يلحق توقيعاً الكتروني بأي مستند مسجل الكترونياً (مثل رسائل البريد والصور وصفحات الويب) ولا يتطلب ذلك سوى نقرة على الفأرة الخاصة بالحاسب أو عدة ضربات على لوحة المفاتيح من خلال بعض البرامج الداعمة .

ومنذ فترة قصيرة كانت الطريقة الوحيدة الفعّالة للتحقق من هوية المتصل على شبكة الانترنت هي استعمال تقنيات تعتمد على زوج من المفاتيح اللامتناظرة وقد اصطلح على تسميتها (توقيع رقمي) digital signature وفي مرحلة متقدمة بدأت تلك التقنيات بالتطور حتى أصبح التعبير الشائع لأي توقيعات الكترونية للإشارة إلى كل الطرق الالكترونية المحتملة للتحقق من الهوية لذلك فإن التوقيعات الالكترونية تتضمن الأنظمة البيومترية وأي طريقة الكترونية أخرى وأصبح التوقيع الرقمي مجرد أحد أنواع التوقيعات الالكترونية والنقطة الرئيسية التي يتم من خلالها التمييز بين هذين النوعين من التوقيعات هي الحضور والغياب لتقنية التشفير المفتاح العام PKC حيث تتضمن هذه التقنية المتطورة العديد من التقنيات الأخرى لتحقيق الغاية المطلوبة من وظيفة التوقيع الالكتروني^{٥٢} ،

^{٥٢} محمد سعيد أحمد اسماعيل - أساليب الحمائية القانونية لمعاملات التجارة الالكترونية - مرجع

في غياب أي معنى متفق عليه عالمياً لمصطلح (التوقيع الرقمي) فإن أي توقيع رقمي ينشأ بعلاقة رياضية ذات صفة فردية من الناحية الاحتمالية ، ويرتبط بالبيانات المخزنة على شكل الكتروني للقيام بالوظائف المختلفة للتوقيع وأهمها استخدامه كأداة لتسيير المعاملات المصرفية هو توقيع الكتروني.

وتعد الصور التالية هي الصور الأكثر شيوعاً والأكثر أمناً لتأدية وظيفة التوقيع الالكتروني .

٢-١- البطاقة المغناطيسية magnetic cards :

بالرغم من أن هذه البطاقة ليست من الأدوات المتطورة في مجال التوقيع الالكتروني إلا أنها لا تزال تحتل مركزاً بارزاً في الكثير من الصفقات التجارية اليومية ، وأن معظم الاستعمالات المألوفة لهذه البطاقة نجدها في بطاقات الائتمان حيث أن المعلومات المخزنة باستخدام المعايير الدولية لتشفير البيانات الرقمية على شريط مغناطيسي تكون مقروءة من قبل جهاز الصراف الآلي بطريقة تتيح فك الشيفرة الموجودة على ذلك الشريط المثبت على البطاقة.

٢-٢- البطاقة الذكية smart card :

وهي تشبه بطاقات الشريط المغناطيسي لكنها تحتوي على كمية ضخمة من المعلومات التي تتضمنها كل بطاقة ويتم معالجتها بشكل دقيق وتكاملي ، وإن أمن البطاقات الذكية يكون نموذجياً باتباع مجموعة من إجراءات السلامة كمعلومات المفتاح العام والمفتاح الخاص الذي سنتحدث عنهما لاحقاً .

وهناك نوعان للبطاقة الذكية :

الأول : البطاقات الذكية ذات الرقائق الالكترونية حيث يتمتع هذا النوع بقوة حسابية لتزويد أكثر أمناً وتسمح بالتحقق من حامل هذه البطاقة بإدخال الرقم السري وتعمل هذه البطاقات الذكية بنظام offline أي غير متصل أو عن طريق الاتصال غير المباشر حيث تتم إضافة المعلومات الجديدة بعد الانتهاء من المعاملات البنكية الالكترونية ، أي أنه عندما يقوم شخص ما بسحب مبلغ من المال من حسابه عبر هذه البطاقة فإن المعلومات الجديدة المتغيرة بعد عملية السحب سوف يتم تحديثها في حسابات المصرف بعد إتمام عملية السحب أي بعد الانتهاء من العملية وقبض المال و إخراج البطاقة من الصراف فيقوم نظام آلة الصرافة بإرسال التحديثات المخزنة إلى نظام البنك دون الحاجة للاتصال المباشر بين جهاز الصراف والبنك أثناء تنفيذ العملية ، **الثاني :** البطاقات الذكية التي تحتوي على وحدة معالجة مركزية

وتتمتع هذه البطاقات بقابليتها لإضافة ومعالجة المعلومات الجديدة حيث تتم معالجة البيانات وتخزينها لتأخذ مكانا في البطاقة نفسها حيث أنها تعمل بنظام online الذي يمثل الاتصال المباشر عبر الشبكة^{٥٣}

٢-٣- التوقيعات الرقمية لتوثيق معاملات التجارة الالكترونية:

يعتمد التوقيع الالكتروني على تقنية التشفير بالمفتاح العام PKC باستخدام العلاقات الرياضية التطبيقية التي تقوم بتشفير الرسائل الالكترونية ، وترسل إلى الوجهة المقصودة حيث يتم فك تشفيرها ، وفيما بعد تطور هذا النوع من انظمة التشفير ليعطي تأمينا أقوى في نقل البيانات حيث أصبح يتم تشفيره بواسطة مفتاحين مفتاح عام ومفتاح خاص

المفتاح الخاص : هو تشفير متناظر يحقق سرية وخصوصية ويكون خاص بشخص معين ويُعرف فقط من قبله ويقوم باستخدامه لتشفير الرسالة التي ترسل من قبله ويتم فك تشفيرها بالمفتاح العام للشخص ذاته .

المفتاح العام : تشفير لامتناظر يحقق جميع استخدامات التشفير عدا سلامة المعلومات ، ويعطى للمستخدمين المصرح لهم بالوصول للشبكة ، لفك ماتم تشفيره بالمفتاح الخاص والحفاظ على سرية المحتوى^{٥٤}.

^{٥٣} محمد سعيد أحمد اسماعيل - أساليب الحماية القانونية لمعاملات التجارة الالكترونية - مرجع

Hash functions ويحقق سلامة المعلومات.

من الملاحظ أن الأساس الذي تقوم عليه فكرة التوقيع الالكتروني هو تشفير البيانات المرسله عبر شبكة الانترنت وهذا بديهي إذ أنه لا فائدة من فكرة التوقيع مالم تكن البيانات المرسله محصنة من أي تشويه (تحريف) قد يدخل عليها من قبل الغير ، وسنتأول أهم التقنيات المستخدمة في تشفير البيانات.

٣- أنظمة التشفير

معنى التشفير هو الكتابة بلغة غير مفهومة من أجل حجبها عن الغير حيث تستخدم من أجل : الخصوصية - سرية المعلومات - التحقق من الهوية - عدم إنكار حدث ما تم القيام به من خلال التوقيع الرقمي - سلامة الرسالة أو المعلومة بشكل عام من أجل منع تشويهها .

إن الاختلاف الجوهري بين نظام التشفير المتناظر واللامتناظر يكون في التقنية المستخدمة لفك التشفير .

فمن حيث الأسلوب كلا النظامين يعمل على تشفير الرسالة بطرف المرسل وفك تشفيرها بطرف المستقبل ، ومن **حيث التقنية** فإن نظام التشفير المتناظر

^{٥٥} محمد سعيد أحمد اسماعيل - أساليب الحمائية القانونية لمعاملات التجارة الالكترونية - مرجع

يستخدم نفس المفتاح لتشفير الرسالة وفك تشفيرها، في حين أن النظام الآخر يستخدم مفتاح لتشفير الرسالة ومفتاح آخر لفك تشفير الرسالة^{٥٥}.

فإن التشفير اللامتناظر يستخدم نوعين من المفاتيح (عام - خاص) فيما يعتمد التشفير المتناظر على مفتاح واحد .

علماً أن هذان المفتاحان العام والخاص يعملان كزوج ويقترن كل منهما بالآخر وإن اية رسالة أو مستند يتم تشفيره بأحد المفتاحين ، يتم فك تشفيره بالمفتاح الآخر ، فإذا كانت الوثيقة مشفرة بالمفتاح الخاص فلا يفك تشفيرها إلا بالمفتاح العام للمرسل .

إن عمليات التوقيع الرقمي وعمليات التحقق من البيانات المرسلة وسلامتها من التشويه تتم باستخدام تقنيات متطورة جداً وليس فقط بالاعتماد على زوج من المفاتيح (عام وخاص) وتعتمد هذه التقنيات على القيام بعمليات رياضية كالخوارزميات أو اللوغاريتميات وخاصية البعثرة ولوغاريتم التوقيع ، وهذه الخوارزميات هي عبارة عن معادلات رياضية سهلة بالبداية من أجل عملية التشفير لكنها تعتمد على عكس العمليات الحسابية من أجل فك التشفير والتي تعتبر من حيث النتيجة مستحيلة الحل ، وإن تطبيق خوارزمية البعثرة على الرسالة الالكترونية الأصلية تؤدي إلى تشفيرها بشكل ثنائي وهذا ما يدعي بملخص الرسالة الذي يكون عبارة عن مجموعة من الأرقام الفردية

^{٥٥} محمد سعيد أحمد اسماعيل - أساليب الحمائية القانونية لمعاملات التجارة الالكترونية - مرجع

بالنسبة للرسالة الأصلية وإن خوارزمية التوقيع بعد ذلك تؤدي إلى هذا الملخص للرسالة وتشكل هذه المجموعة من الأرقام فيما يدعى بالتوقيع الرقمي .

عندما ينهي المرسل رسالته الالكترونية فإنه يرفق معها أو يلحق بها حسب الحال توقيعها الالكتروني ، وقد تكون هذه الرسالة مشفرة أو غير مشفرة ويقوم المرسل بإرسال الرسالة الالكترونية مرفقةً بتوقيعه الالكتروني إلى المستلم المقصود ويستخدم المتلقي المفتاح العام للموقع لفك تشفير الرسالة و التوقيع الرقمي للمرسل ، ومن ثم تقوم برمجيات خاصة بحساب قيمة Hash Value للتحقق من التوقيع الرقمي، حيث يقوم بحساب Hash Value باستخدام نفس الخوارزمية ، وحينها يمكن للمستلم المقارنة بين قيمتي Hash Value المحسوبة والمستقبلة فإن كانتا متطابقتين فهذا يعني بأن الرسالة لم تتعرض لأي تشويه وذلك دلالة على عدم وجود أي تحريف على البيانات المرسله والتحقق من هوية المرسل .

ومن أكثر الخوارزميات شيوعاً من أجل التشفير باستخدام المفتاح العام والخاص تستخدم خاصية هامة من خصائص الأعداد الأولية : حيث تنتج هذه الأرقام من عملية ناتج ضرب تلك الأعداد ببعضها لإنتاج عدد جديد يكون من الصعب التعرف على أي عددين أوليين أنشأ ذلك الرقم الجديد والكبير ، ويبدو ذلك بوضوح في حالة الأشخاص الذين يستخدمون المفتاح العام لموقع معين ويستخدمونه في التحقق من صحة توقيعاته فإنهم لن يتمكنوا من اكتشاف المفتاح الخاص للموقع ليستخدموه في تزوير التوقيعات الرقمية .

ولكن ما هو مدى فاعلية أنظمة التشفير في قطعية ثبوت صحة التوقيع والرسالة المتضمنة أو المعنية بالتوقيع ؟؟

يعتمد هذا النوع من التوقيعات على تطبيق خوارزمية hash function والتي تقوم على طريق إجراء العديد من العمليات المنطقية المتفق عليها مع المستقبل لتوليد شيفرة معينة تضمن سلامة البيانات من التشويه ، وبعدها يتم تشفير هذه النتيجة باستخدام المفتاح الخاص للمرسل وعند وصول هذه البيانات للمستلم فإنه يقوم بفك تشفير هذه الشيفرة باستخدام المفتاح العام للمرسل نفسه ومن ثم يعيد تطبيق خوارزمية hash function ويقوم بمقارنة المحتوى وناتج العملية المنطقية الأولى فإذا كانت النتائج متطابقة فهذا يدل على هوية الشخص المرسل وعلى أن البيانات لم تتعرض لأي تشويه بعد إرسالها ، حيث أن أي تغيير سيطرأ على هذه الرسالة سيؤدي إلى رفض المرسل إليه لهذه الرسالة ، ففي حال حدوث أي تشويه على البيانات وإن كان صحيحاً ولا يشوبه أي خطأ (كأن يكون أحد ما قد قام باستبدال التوقيع بتوقيع آخر يحتفظ به مسبقاً أو يقوم بتغيير أرقام الحسابات أو مبالغها أو أي عنصر آخر) فسيحدث ذلك اختلاف في حزمة التزامن للرسالة ، الأمر الذي يحدث تغيير في نتيجة العملية المنطقية وبالتالي عدم تطابق النتيجتين الأولى و الأخيرة مما يعني رفض المستلم للرسالة المشوهة .

لاشك أن التقدم والتطور المستمر في مجال أمن المعلومات ، استتبع ذلك بالضرورة تطوير أساليب المخترقين في عملياتهم وتنوعها ، والعكس صحيح فهناك رابط قوي بين مجال أمن المعلومات ومجال اختراقها ، إذ أنه كلما

ما تطورت وسائل الحماية والأمن في تبادل المعلومات كلما ازادت مهارات المخترقين ليتمكنوا من اختراق تلك الشبكات مثل Man-IN-The-Middle(Sniffing)Relaying والكثير غيرها ، وكذلك كلما ازادت عمليات القرصنة والاختراق كلما ازاد البحث والتطوير في مجال أمن المعلومات ، و كان لا بد من إيجاد طريقة آمنة لتخطي هذه الأمور وخصوصاً في التعاملات المالية كالتجارة الالكترونية وعمليات كشف الحسابات عن طريق الانترنت وغيرها ، حيث تم تطوير تقنية الـ SSL : Secure Socket Layer حيث هيأت هذه الطريقة لوجود اتصال آمن مشفر Encrypted ضمن تعقيدات متقأوة فمنها الـ ٤٠ Bit ومنها ١٢٨ bit فتم استخدام الـ SSL لتشفير وحماية قنوات الاتصال التي تنتقل عبرها البيانات مثل SMTP أو الـ Database Communications^{٥٦}.

وتم استخدام ما يعرف بالـ SSL over HTTP في المواقع التجارية ومواقع البريد الالكتروني فأصبحت تسمى :

HTTPS – Secure Hyper Text Transfer Protocol

واستخدم بورت ٤٤٣ بدلاً من ٨٠ الخاص بالـ HTTP ، وانتشر واشتهر هذا البروتوكول بشكل كبير .

ثم ظهرت تقنية مشابهة له ولاستخدامه وهي

^{٥٦} <http://www.startimes.com/?t=١٤١٤٠٢٩١> ٢٠١٦ راجع الموقع الالكتروني

SSL TLS : Transport Layer Security وهي تقنية محسنة من ال ولكنهما يختلفان في طريقة أداء العملية ، والطريقتان تحتاجان للشهادات الالكترونية Certificates أو بالأحرى Web-based Certificates وظهرت تقنية أخرى داخل الشبكة نفسها وليس على شبكة عالمية كالانترنت ، وهي SMB Signing .

فإن ال SMB : Server Message Block وهي ال packets التي يتم إرسالها بين السيرفر والأجهزة في عملية مشاركة الملفات وغيره Sharing ، وللحماية من طريقة سرقة المعلومات أثناء مرورها في الأسلاك Man In The Middle MITM وهذه الطريقة تدعى SMB Signing، يتم بواسطتها إضافة ال Hash وهي طريقة يتم من خلالها استخلاص رمز معين تم حسابه باستخدام عمليات رياضية من الرسالة ، ومن الأمثلة عليه MD٤، MD٥ ، (SHA-١) ويتم تشفير هذا ال Hash واضافته للرسالة وبذلك نحافظ على صحة الرسالة Message Packet Integrity^{٥٧}.

لكن ظهرت المشكلة الكبرى بكون جميع هذه التقنيات تعمل على طبقة التطبيقات المسماة بـ Application Layer في النموذج المعياري لربط النظم المفتوحة المسمى بـ (OSI Model) أي أن وظائف هذه التقنيات السابقة محدودة جداً، فهي لا تستطيع تشفير إلا ما بنيت لأجله، ولذلك كان لا بد من ابتكار طريقة تمكننا من تشفير كل حزمة (Packet) تصدر من أي جهاز ،

^{٥٧} <http://www.startimes.com/?t=١٤١٤٠٢٩١> راجع الموقع الالكتروني - مرجع سابق

فتم ابتكار تقنية ال IPsec وهي تقنية تعمل على طبقة الشبكة المسماة بـ (Network Layer) في نظام ال OSI Model بمعنى أنه يقوم بتشفير كل شيء يصدر عن الجهاز ويرسله على الشبكة Network وبما ان ال (Network Layer) هي الجهة التي من خلالها يمر كل شيء للشبكة فإن تقنية IPsec توفر الموثوقية والصحة والتشفير لكل ما قد يمر من خلالها على مستوى ال IP Packet. وفي هذه الدراسة سنتناول كل ما يتعلق بال IPsec من أنواعه وأقسامه وفوائده وكيفية عمله :

Application	S/MIME	PGP	
Presentation	أمن المواقع والمنتجات والشبكات		
Session	Kerberos	HTTP	SSL
Transport		UDP	
Network		TCP	IPsec
Data Link			
Physical			

مخطط يوضح موقع ال IPsec في ال OSI Model^{٥٨}

ولكن ما هي ال IPsec ، وماهي وظائفها وآلية عملها ومزاياها ؟

^{٥٨} <http://www.startimes.com/?t=١٤١٤٠٢٩١> ٢٠١٦ راجع الموقع الالكتروني - مرجع سابق

IPSec :هي مجموعة من البروتوكولات التي طورت بواسطة اللجنة الخاصة لنظام الانترنت (IETF) Internet Engineering Task Force وتم اعتمادها كمعايير للإنترنت لإمكانية التحقق من سلامة وسرية المعلومات التي أرسلت عبر شبكات الـ IP ، وذلك بجعلها تعمل في طبقة الـ IP بحيث تتمكن من حماية أي نوع من نقل البيانات من خلال الـ IP .

عادةً يعبر عن الـ IPSec بأنها Transparent Security Protocol لأن المستخدم و التطبيقات لا يشعرون بوجودها لأنها تعمل على طبقة الشبكة (Network Layer)، ويعمل الـ IPSec في البيئات التي تكون سرعة الاتصال بها سريعة .

بروتوكولات الـ IPSec

ينقسم الـ IPSec إلى ثلاث بروتوكولات :

٣-١ - AH : Authentication Header

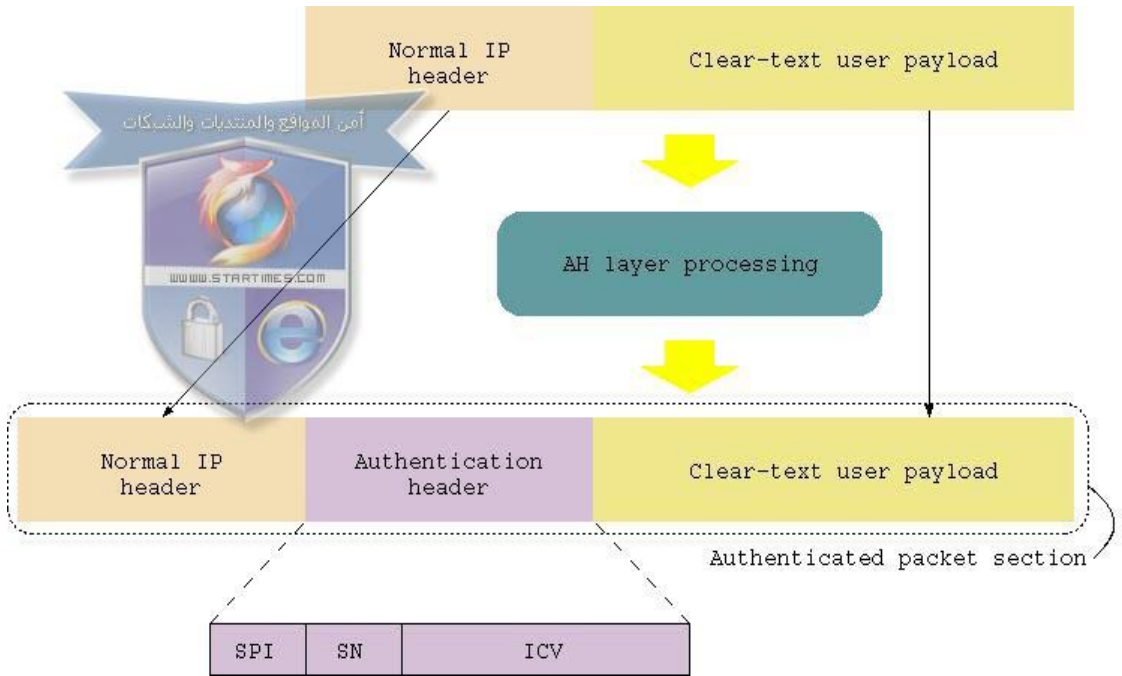
يستخدم الـ AH في توقيع (Sign) الرسائل والبيانات ولا يعمل على تشفيرها ، حيث يحافظ على :

٤-١-١-١ موثوقية البيانات Data authenticity : أي أن البيانات المرسله من هذا المستخدم قد أرسلت منه وليست مزورة أو مدسوسة .

٤-١-٢-٢ صحة البيانات Data Integrity : أي أن البيانات المرسله لم يتم تعديلها على الطريق (أثناء مرورها عبر الأسلاك)

٤-١-٣-عدم إعادة الإرسال Anti-Replay : وهذه الطريقة التي يستخدمها المخترقون حيث يقومون بسرقة كلمة المرور وهي مشفرة ويقومون بإعادة إرسالها في وقت آخر للسيرفر وهي مشفرة وبالطبع يفك السيرفر التشفير ويدخل اسم المستخدم على أنه شخص آخر، فال IPsec يقدم حلاً لمنع هذه العملية من الحدوث.

٣-٢--الحماية ضد الخداع Anti-Spoofing protection : ويوفر أيضاً ال IPsec حماية ضد الخداع من قبل المستخدمين ، مثلاً يمكن أن يحدد مدير الشبكة أنه لا يسمح لغير المستخدمين على ال subnet ١٩٢,١٦٨,٠.X بينما لا يسمح لحاملي الهوية ١٩٢,١٦٨,١.X من دخول السيرفر ، فيمكن للمستخدم أن يغير ال IP Address الخاص به ، لكن ال IPsec يمنع ذلك ،(وأيضاً يمكن القياس على ذلك من خارج الشبكة إلى داخلها) فيكون لكل حزمة Packet توقيعها Digitally signed .



الشكل العام لحزمة البيانات Packet التي تمر في بروتوكول AH

٣-٣ - Encapsulating Security Payload :ESP

يوفر هذا البروتوكول التشفير والتوقيع للبيانات في آنٍ واحد معاً Encryption and Signing ، و يستخدم هذا البروتوكول لضمان سرية المعلومات Confidential أو Secret ، أو عند إرسال المعلومات عن طريق شبكة عامة Public Network مثل الانترنت يوفر الـ ESP المزايا التالية :

١-٢-٤ Source authentication مصداقية المرسل :

حيث كما وضعنا في مثال ال Spoofing أنه لا يمكن لأي شخص يستخدم الIPSec لتزوير هويته (هوية المرسل) .

٤-٢-٢ - Data Encryption التشفير للبيانات : حيث يوفر التشفير حماية البيانات من أي تعديل أو تغيير أو قراءة .

٣-٤ - Internet Key Exchange :IKE

الوظيفة الأساسية لهذا البروتوكول هي ضمان الكيفية وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي الIPSec، فهو بروتوكول ال negotiation أي التفاوض في نظام الIPSec كما أنه يعمل على تأكيد طريقة الموثوقية Authentication والمفاتيح الواجب استخدامها ونوعها (حيث ان الIPSec يستخدم التشفير ٣ DES وهو عبارة عن زوج من المفاتيح ذاتها يتولد عشوائياً بطرق حسابية معقدة ويتم إعطائه فقط للجهة الثانية ويمنع توزيعه وهو من نوع Symmetric Encryption أي التشفير المتوازي ويستخدم تقنية ال Private Key .

أقسام الIPSec أو انواع الIPSec التي يستخدمها في الشبكة:

وينقسم الIPSec إلى نظامين أو نوعين وهما :

١. نظام النقل Transport Mode

٢. نظام النفق Tunnel Mode

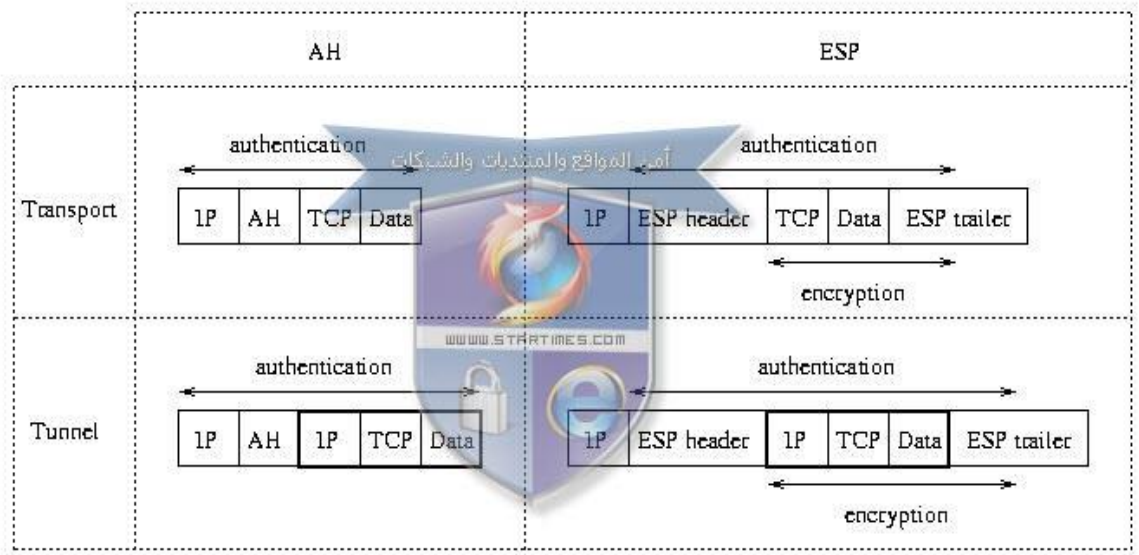
نظام النقل transport mode : يستخدم هذا النظام عادة داخل الشبكة المحلية LAN: Local Area Network حيث يقدم خدمات التشفير للبيانات التي تتطابق والسياسة المتبعة في الـ IPSec بين أي جهازين في الشبكة أي يوفر Endpoint-to-Endpoint Encryption فمثلاً إذا قمت بضبط سياسة الـ IPSec على تشفير جميع الحركات التي تتم على بورت ٢٣ وهو بورت الـ Telnet حيث أن الـ Telnet ترسل كل شيء مثلما هو دون تشفير PlainText فإذا تمت محادثة بين السيرفر والمستخدم على هذا البورت فإن الـ IPSec يقوم بتشفير كل البيانات المرسلة منذ لحظة خروجها من جهاز المستخدم إلى لحظة وصولها إلى السيرفر، ويتم تطبيق هذا النظام في الحالات التالية :

أ- المحادثة تتم بين الأجهزة في داخل أو نفس الشبكة الداخلية الخاصة . Private LAN

ب- المحادثة التي تتم بين جهازين لا يقطع بينهما Firewall حائط ناري يعمل عمل Translation NAT : Network Address وهو نظام يمكن الـ Firewall من استبدال جميع عناوين الـ IPs في الشبكة الداخلية من حزمة البيانات Packet واستبدالها في عنوان Public IP اخر ، ونستفيد من ذلك هو أننا لن نحتاج سوى إلى عنوان IP واحد One Public IP ، وأيضاً يقوم بإخفاء عناوين الأجهزة عن شبكة الانترنت للحماية من الاختراق الخارجي .

نظام النفق Tunnel mode : يتم استخدام هذا النظام لتطبيق الـ IPsec بين نقطتين تكون عادةً بين ٢ Routers، إذاً يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافياً أي سيتم قطع الانترنت في طريقها إلى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعدة جغرافياً WAN : Network Wide Area ، يستخدم هذا النظام فقط عند الحاجة لتأمين البيانات فقط أثناء مرورها من مناطق غير آمنة كشبكة الانترنت ، فمثلاً إذا أراد فرعين لشركة أن يقوموا بتشفير جميع البيانات التي يتم إرسالها فيما بين هذين الفرعين على بروتوكول FTP :

File Transfer Protocol فيتم إعداد الـ IPsec على أساس الـ . Tunnelling Mode



مخطط توضيحي لكل من الـ Packets في الـ AH ، ESP في كلتا النظامين Tunnel and Transport Modes

فوائد بروتوكول الـ IPSec :

لقد ظهر ضعف كبير في عملية التشفير Encryption العادية التي تتم بين الأجهزة في الشبكات ، وهذا الضعف تمثل في صعوبة تطبيق هذا الموضوع ، وأيضاً استهلاكه للوقت أي بطئه الشديد في القيام بعملية التشفير وفك التشفير Encryption and decryption ، فالفائدة الكبرى من وراء الـ IPSec هي أنه يوفر حماية كاملة وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالثة Layer 3 of the OSI Model وما بعدها.

ومن مميزات الـ IPSec أيضاً هو أنه موجود أصلاً Built-in في داخل حزمة الـ IP Packet ، فلذلك هو لا يحتاج لأية إعدادات لانتقاله عبر الشبكة ولا يحتاج لأية أجهزة إضافية لذلك.

الأخطار المحيطة بالرسائل المتضمنة لتوقيع الكتروني ، كيف يحمي الـ IPSec من الهجوم على الشبكة؟

إن الشبكة والبيانات التي تمر فيها يمكن أن تتعرض للعديد من أنواع الهجمات المختلفة ، بعض الهجمات تكون غير فعالة Passive مثل مراقبة الشبكة Network Monitoring ، ومنها ما هو الفعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر أسلاك الشبكة. و سوف نستعرض بعض أنواع الهجمات على الشبكات.

أولاً: التقاط حزم البيانات Eavesdropping، sniffing or snooping :

حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكة بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ، ويعالجها الـ IPsec عن طريق تشفير حزمة البيانات ، عندها حتى لو التقطت الحزمة فإن الفاعل لن يستطيع قراءتها أو العبث بها، لأن الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل .

ثانياً: تعديل البيانات Data modification : حيث يتم بذلك سرقة حزم البيانات من الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل ، ويقوم الـ IPsec بمنع ذلك عن طريق استخدام الهاش Hash ووضعه مع البيانات ثم تشفيرها معاً ، وعندما تصل الحزمة إلى الطرف المستقبل فإن الجهاز يفحص Checksum التابع للحزمة إذا تمت مطابقته أم لا، فإذا تمت المطابقة مع الهاش الأصلي المشفر تبين أن الحزمة لم تعدل، لكن إذا تغير الهاش فإن حزمة البيانات قد تم تغييرها على الطريق وبالتالي سيرفضها المستقبل .

ثالثاً: انتحال الشخصية Identityspoofing : بحيث يتم استخدام حزم البيانات على الشبكة والتقاطها وتعديلها ليتم استخدامها كهوية مزورة للمرسل، أي خداع المستقبل بهوية المرسل، ويمنع ذلك بواسطة الطرق الثلاثة التي يستخدمها الـ IPsec وهي: بروتوكول الكيربوس Kerberos Protocol والشهادات الالكترونية Digital Certificates ، ومشاركة مفتاح معين.(Preshared Key)

حيث لا تتم عملية بدء المحادثة وإرسال البيانات قبل التأكد من صحة الطرف الثاني من خلال إحدى الطرق المذكورة.

رابعاً DoS – Denial of Service: رفض الخدمة أو حجبتها : حيث تعمل هذه الهجمة على تعطيل خدمة من خدمات الشبكة للمستخدمين والمستفيدين منها ، مثلاً كإشغال السيرفر في الشبكة بعمل عليه Flood (فيض من بيانات ليست ذات أهمية) مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين ويعمل الـ IPSec على منع ذلك عن طريق إمكانية غلقه أو وضع قواعد للمنافذ المفتوحة Ports .

خامساً MITM – Man In The Middle: من أشهر الهجمات في الشبكات ، وهي أن يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسلة من طرف لآخر وإمكانية العمل على تعديلها أو العمل على عدم إيصالها للجانب الآخر، ويعمل الـ IPSec على منعه بواسطة طرق التحقق من الموثوقية . Authentication methods

سادساً: الهجمات على طبقة التطبيقات Application Layer Attacks : حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في أجهزة الشبكة وأيضاً تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الأمثلة عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى أخطاء المستخدمين. يعمل الـ IPSec على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أية حزمة بيانات لا تتطابق مع الشروط الموضوعه لذلك ، فتعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج.

وكنتيجة لما سبقت دراسته فال IPsec يحمي من معظم الهجمات عن طريق استخدامه ميكانيكية التشفير المعقدة ، حيث يوفر التشفير الحماية للبيانات والمعلومات أياً كانت أثناء انتقالها على الوسط مهما كان عن طريق عمليتي التشفير Encryption والهاش Hashing^{٥٩}.

ومن الخطوات المتبعة في توثيق التوقيعات الالكترونية والتأكد من موثوقيتها هي التأكد من أن من يقوم بإدخال هذا التوقيع أو عملية الدفع هو شخص حقيقي بالفعل وليس مجرد برنامج خبيث أو جهاز ما أو عملية تقنية احتيالية تحوي تفاصيل محتوى بيانات التوقيع بشكل رقمي ، فلما كان كل ملف حاسوبي هو بالنهاية عبارة عن محتوى من أعداد النظام الست عشري ، سواء كان هذا المحتوى هو ملف صوتي أو ملف نصي أو صورة ضوئية محفوظة فهو بالنهاية مجموع من أرقام نظام العد الثنائي أو الست عشري ، فمن حيث المبدأ النظري أن مجموع الأرقام المكونة لمفتاح pin ستترجم للحاسب من حيث النتيجة لمجموعة أرقام ، فلو قام أحد القراصنة بمعرفة مجموع أعداد معينة تكون من حيث النتيجة الرمز pin وليكن ٢٢٤٤ فان هذا الرمز ٢٢٤٤ سيتترجم للكمبيوتر بالحقيقة (٠٠١٠-٠٠١٠-٠٠٠١-٠٠٠١) على سبيل المثال ، فلو تمكن شخص من الوصول إلى هذا المحتوى وقام بإقحامه في حزمة هذا التوقيع فسيتمكن بالنهاية من تعديل أي حزمة تحوي توقيع مغاير ليقحم فيها هذا التوقيع ، وتقديماً لهذا الخطر ، فأحدى الوسائل للتأكد من

^{٥٩} <http://www.startimes.com/?t=١٤١٤٠٢٩١> - ٢٠١٦ - راجع الموقع الالكتروني - مرجع سابق

موثوقية هوية الموقع تطلب منه قبل إتمام عملية الدفع أن يقوم بإدخال رموز ظاهرة على الشاشة ضمن إطار محدد يتم إرسال هذه الحزمة مع حزمة البيانات الأخرى ليتمكن المستقبل من التأكد من أن من قام بالتوقيع ليس جهاز أو برنامج ، وأن التوقيع الذي استلمه والذي هو عبارة عن (٠٠١٠-٠٠١٠-٠٠١٠) قد تم إدخاله من شخص حقيقي وليس من خلال برنامج خبيث قام بإقحام هذا التوقيع ضمن الملف المرفق .



٦٠

أو أن يتم إرسال كود معين إلى الجهاز المحمول للمستخدم ليتم ربطه بذات الحزمة المرسله للتأكد بأن المستخدم هو شخص حقيقي وليس مجرد برنامج خبيث أو عملية احتيالية من جراء هجمة الكترونية ، وفي هذا الرسم

^{٦٠} <https://www.rt.com/news/٢١١١٧٥-google-ditches-captcha-system> - ٢٠١٦ - راجع

التوضيحي نبين آلية عامل التوثيق بالرموز ، كثيراً ماتظهر لنا هذه الأنماط من الصور أثناء تصفحنا عبر شبكة الانترنت ، وتظهر هذه الصورة بالتحديد عندما يقوم المستخدم بإنشاء حساب ما أو لدى قيامه بعملية ما تتطلب التوثيق من هويته (كما في حالة الدفع الالكتروني) ، أغلب المستخدمين لايعون فكرة هذه الصورة أو وظيفتها ، عندما يقوم أحد القراصنة بعملية اختراق ما فهو يستخدم برامج خبيثة في كل خطوة يقوم بها تفادياً لتتبع أثره وبالتالي إخفاء هويته ، كأن يكون بحاجة إلى إنشاء حساب وهمي ضمن شبكة ما ليتمكن من تصفح محتواها وبالتالي الوصول إلى مخدماتها ، ولطمس أثره يقوم المقرصن باستخدام برامج خبيثة تتولى مهمة إنشاء الحسابات الوهمية ، فعلى سبيل لمثال لو أراد أحد ما الاشتراك بالموقع الشهير ebyه للتسوق عبر الانترنت فذلك يتطلب منه إنشاء حساباً على هذا الموقع وإن إنشاء الحساب دون استخدام البرامج الخبيثة سيسجل كافة المعلومات المتعلقة بالاتصال (منفذ الشبكة - بوابة الاتصال - نوع ومواصفات الجهاز المتصل هل هو حاسب محمول أم مكتبي أم هاتف ذكي) وبالتالي ستسجل كافة المعلومات لدى أنظمة الموقع مما لايخدم غرض القراصنة في طمس أثرهم ، لذلك يعتمد القراصنة لاستخدام برامج خبيثة يدخل إليها الأوامر (commands) مسبقاً وتقوم البرامج بإنشاء الحسابات تلقائياً وبشكل آلي (فعلى سبيل المثال قد تتمكن من إنشاء مايقارب ٢٠٠٠ حساب على موقع التواصل facebook خلال بضع ساعات بأسماء متسلسلة ١xyz، ٢xyz، ٣xyz.....) وبالتالي ابتدع مطورو البرمجيات وفنيو أمن الشبكات طرق تأمين عديدة للتوثق أن المستخدم هو شخص حقيقي وليس مجرد برنامج ، وبالتالي فإن هذه الصورة تحتوي على رموز مدركة من قبل

الأشخاص ولكنها غير قابلة لإدراك من قبل البرامج الخبيثة ، مما يعني أنه لا يمكن اجتيازها إلا من قبل شخص حقيقي .

التوقيع الالكتروني في التشريع السوري :

نظم المشرع السوري التوقيعات الالكترونية ضمن أحكام القانون ٤ لعام ٢٠٠٩ ، حيث جعل المشرع للتوقيع الالكتروني ذات الحجية المقررة في الأدلة الكتابية وفق أحكام قانون البيانات السوري شريطة مراعاة أحكام قانون التوقيع الالكتروني في إنشاء التوقيع وذلك في المادة ٢ فقرة أ من قانون التوقيع الالكتروني والتي تنص على أنه : أ- للتوقيع الإلكتروني المصدق، المدرج على وثيقة إلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للأدلة الكتابية في أحكام قانون البيانات، إذا روعي في إنشائه وإتمامه الأحكام المنصوص عليها في هذا القانون، والنواظم والضوابط التي يصدرها الوزير، بناء على قرار من مجلس إدارة الهيئة، المنصوص على أحداثها في الفصل الثالث من هذا القانون.

وبالرجوع لنص المادة آنف الذكر نبين أنه لكي يكون للتوقيع الالكتروني الحجية ذاتها المقررة للأدلة الكتابية يجب أن يكون هذا التوقيع مصدقاً والتوقيع الالكتروني المصدق وفقاً لقانون التوقيع الالكتروني هو التوقيع الالكتروني

المصدق بشهادة تصديق الكترونية تبعاً لنص المادة ١ من القانون المذكور والتي نصت على أحداث جهة مختصة مرخص لها بإصدار شهادات التصديق الالكتروني ، وقد عرف القانون عينه شهادة التصديق الالكتروني Electronic certificate : شهادة اعتماد تصدر عن جهة مختصة مرخص لها الهدف منها إثبات عائدة توقيع الكتروني إلى شخص طبيعي أو اعتباري معين سنداً للارتباط بين الموقع وبيانات إنشاء التوقيع الالكتروني المعتمدة الخاصة به ، أي أن المشرع قد عمد إلى إنشاء آلية أو منظومة مُحكمة ومنضبطة القواعد يناط إليها مسؤولية توثيق التوقيعات الالكترونية ضمن أطر محددة ، حيث نصت كذلك المادة ١٤ في الفصل الثالث من قانون التوقيع الالكتروني على أحداث هيئة وطنية لخدمات الشبكة وأولى المشرع لهذه الهيئة عدة مهام ذكرت في المادة ١٥ نذكر منها :

تتولى الهيئة القيام بالمهام التالية:

١. تنظيم نشاطات تقديم خدمات التوقيع الإلكتروني، وغيرها من النشاطات في مجال المعاملات الالكترونية.
٢. تحديد وضبط مواصفات المنظومات الخاصة بالتوقيع الإلكتروني، واعتماد تلك المنظومات.

٣. تحديد نواظم وضوابط إصدار شهادات التصديق الإلكتروني.
٤. منح وتجديد وتعليق وإلغاء التراخيص اللازمة لمزاولة أعمال خدمات التوقيع الإلكتروني، وفقاً لأحكام هذا القانون وسائر القوانين والأنظمة النافذة، ومراقبة الالتزام بشروط تلك التراخيص.
٥. إدارة النطاق العلوي السوري على شبكة الانترنت والسجل الخاص به، وتحديد السياسات والقواعد النافذة لتسجيل الأسماء تحت هذا النطاق.
٦. منح وتجديد وتعليق وإلغاء التراخيص للمسجلين المخولين بتسجيل الأسماء تحت النطاق العلوي السوري، والتحقق من التزامهم بالقواعد النافذة لذلك، وفقاً لأحكام هذا القانون وسائر القوانين والأنظمة النافذة.
٧. إدارة عمليات تخصيص عناوين الانترنت في الجمهورية العربية السورية، والتنسيق مع السلطات الإقليمية والعالمية المختصة من أجل ذلك.
٨. وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ومواقع الانترنت والإشراف على حسن الالتزام بها.
٩. وضع المعايير الخاصة بمواجهة حالات الطوارئ على الانترنت أو غيرها من الشبكات المعلوماتية والحاسوبية، والإشراف على حسن الالتزام بها، وتأليف فرق عمل للتصدي لهذه الحالات.

وبالتالي ستكون الهيئة المحدثة وفقاً لأحكام قانون التوقيع الالكتروني هي الجهة المعنية بإنشاء نظام معلوماتي متكامل تعمل على تأمينه من الناحية الفنية بشكل مُحكم لتأدية الغرض منه وهو إعطاء موثوقية للتوقيعات الالكترونية ليؤدي التوقيع الالكتروني وظائف التوقيع التقليدي ويقوم مقامه وبالتالي يكون للوثيقة الالكترونية حجية الأدلة الكتابية وفقاً لأحكام قانون البيانات وبالتالي تنظيم المعاملات الالكترونية وضبطها وإخضاعها لقوانين مناسبة تراعي طبيعة العالم الافتراضي وتحدد المسؤوليات وتنظم الالتزامات ضمن أنظمة الشبكات .

وقد أضع القانون في المادة ١٢ منه كافة التصرفات في المعاملات المدنية والتجارية المحررة والموقعة الكترونياً لأحكام هذا القانون ليكون لها ذات القوة الثبوتية المقررة في القواعد العامة شريطة مراعاة آلية إصدار التوقيعات الالكترونية وتصديقها ، بيد أن المشرع استثنى زمرة من التصرفات والمعاملات من نطاق تطبيق أحكام هذا القانون في المادة ١٣ التي نصت على مايلي :

باستثناء ما يُنصّ عليه بتعليمات خاصة تصدر عن مجلس الوزراء، لا تسري أحكام هذا القانون على:

٢- المعاملات والعقود والمستندات والوثائق التي تنظم بصورة معينة وفقاً

لتشريعات خاصة، أو تُجرى بإجراءات محددة، ومنها:

- المعاملات المتعلقة بالأحوال الشخصية.
 - معاملات التصرف بالأموال غير المنقولة، ومن ذلك الوكالات المتعلقة بها وسندات ملكيتها وإنشاء الحقوق العينية عليها، باستثناء عقود الإيجار الخاصة بهذه الأموال.
 - لوائح الدعاوى والمرافعات وإشعارات التبليغ القضائية وقرارات المحاكم.
- ومن الرجوع لنص المادة سالفة الذكر أن المشرع أورد بعض التصرفات التي استثنائها على سبيل المثال لا الحصر في الفقرة الثانية من المادة ١٣ ويبدو بأن المشرع قد أصاب في ذلك لما تختص به بعض التصرفات من ضرورة مراعاة إجراءات معينة قد يتعارض تطبيق هذا القانون مع أحكامها كقانون السجل العقاري النافذ الذي لامجال للتوفيق بين أحكامه الحالية وأحكام قانون التوقيع الالكتروني ، أو كالمرافعات أمام المحاكم التي تتطلب إنشاء محكمة الكترونية ابتداءً ليصار إلى إخضاعها لأحكام قانون قانون التوقيع الالكتروني .

وكذلك الأمر فيما يتعلق بالأوراق المالية (القيم المنقولة) حيث أن طبيعة إنشاؤها وتسجيلها تتعارض مع تطبيق أحكام هذا القانون ، حيث يستوجب أن تصدر أسهم الشركات على سبيل المثال بوسيلة الكترونية وتحفظ في سجلات الكترونية لإمكانية إخضاعها لأحكام التوقيع الالكتروني أو المعاملات الالكترونية .

ومن هنا فإن المشرع منح التوقيع الالكتروني الحجية المطلقة وفق شروط معينة فيما لايتعارض مع الأحكام الخاصة ، وفي ذلك شيئاً من التقدير رغب المشرع السوري بمراعاته في سن أحكام التوقيع الالكتروني .

وقد حرص المشرع السوري على تحصين التوقيع الالكتروني ليكتسب ثقة الأطراف في التعامل حيث أوجب على مزود خدمات التصديق الالكتروني تعليق العمل بشهادة التصديق الالكتروني أو إلغائها في حالات معينة في المادتين ٨و٩ واللذان نصتا على أنه :

يجب على مزود خدمات التصديق الإلكتروني تعليق العمل بشهادة التصديق الإلكتروني في الحالات التالية:

المادة ٨:

١. بطلب من صاحب الشهادة.
٢. إذا قامت قرائن، بناء على معطيات موثقة يمكن التحقق منها، تدل على إحدى الحالات التالية:

- استعمال الشهادة بغرض التدليس أو الغش.
- انتهاك منظومة إنشاء التوقيع الإلكتروني.

المادة ٩ :

يجب على مزود خدمات التصديق الإلكتروني إلغاء شهادة التصديق الإلكتروني في الحالات التالية:

١. بطلب من صاحب الشهادة.
٢. عند إعلام مزود خدمات التصديق الإلكتروني بوفاة الشخص الطبيعي أو حل الشخص الاعتباري صاحب الشهادة.
٣. عند ثبوت إحدى الحالات التالية:

- عدم صحة المعلومات المتضمنة في الشهادة المعلقة.
- تغيير المعلومات المتضمنة في الشهادة
- استعمال الشهادة بغرض التدليس أو الغش.
- انتهاك منظومة إنشاء التوقيع الإلكتروني.

وهنا قد راعى المشرع السوري احتمال تعرض منظومة التوقيع الالكتروني للهجمات الالكترونية فعمد على تعليق أو إلغاء اعتماد شهادة التصديق وفقاً لكل واقعة على حدة .

وبعد هذه الدراسة التحليلية والمتعمقة ، وكنتيجة للاستفاضة في موضوع التوقيع الالكتروني والخوض في تفاصيله و آلية تطبيقه و تقنيه استخدامه ، وشرح أساليب حمايته ، وفوائده ، فإن موثوقية التوقيع الالكتروني تكاد تكون مطلقة ، مما يكسبه الحجية القانونية المطلوبة في مجالات استخدامه والكافية لقيامه بوظائف التوقيع التقليدي التامة .

ومن جهة أخرى فمن المتوقع مستقبلاً أن يحتل التوقيع الالكتروني مكاناً بارزاً في الواقع العملي وكذلك في أوساط النظريات القانونية وذلك لاستحالة تزويره من حيث المبدأ ، فقد يعتقد الكثير للحظات بأن التواقيع التقليدية في معاملات البيئة الورقية هي أكثر أماناً منها لنظيراتها عبر الانترنت ولكن إذا تمعنا جيداً في ماهية التوقيع الالكتروني ، وما قد يقدمه من خدمات في الواقع العلمي فلربما في المستقبل سيكون له استخداماً في نطاق أوسع من معاملات الانترنت ، وقد نجد له استخداماً في مجالات أخرى ضمن دوائر التسجيل العقاري على سبيل المثال ، أو الكتاب بالعدل أو غيرها من الجهات الأخرى التي تقتقر أصلاً لأية وسيلة لتقادي أو كشف أية عملية تزوير ، وإنما يقتصر عملها في سبيل ذلك باعتمادها على جهد الموظف المختص في التمعن بالشخص الحاضر أمامه لسماع إقراره ومن ثم التدقيق في الصورة الشمسية الموجودة

على زاوية وثيقة إثبات شخصيته ، بينما يختلف الأمر فيما لو أتيح المجال للتوقيع الالكتروني للقيام بوظيفة التحقق من الشخصية في بعض المعاملات الحساسة كعمليات الفراغ لدى الدوائر العقارية أو عمليات التوكيل لدى كتاب العدل ، كأن يستعاض عن التواقيع التقليدية بالتواقيع البيومترية التي ستعطي نتيجة مطلقة للموظف للتوثق من أن المتصرف هو زيد من الناس دون غيره .

* * *

الفصل الرابع

تفعيل مسؤولية المصارف تجاه عملائها جراء الاحتيال عن طريق القرصنة الالكترونية و الإغفاء منها

أولاً : مسؤولية البنوك في النظرية التقليدية

ثانياً : مسؤولية البنوك في النظرية الحديثة

ثالثاً : حالات دفع المسؤولية جراء عمليات القرصنة

الالكترونية

١ - تحديد مسؤولية المصارف الاتفاقي

٢ - دفع المسؤولية عن طريق توكيل شركات حماية أمن

المعلومات

الفصل الرابع

تفعيل مسؤولية المصارف تجاه عملائها جراء الاحتيال عن طريق القرصنة الالكترونية و الإغفاء منها

إن افتقار معاملات التجارة الالكترونية من الناحية القانونية للتكيفات المناسبة فرض آلية دراسة محددة على هذا البحث ، فلا مجال لدراسة مسؤولية المصارف في الاحتيال عن طريق القرصنة سوى من خلال قضاء المحاكم من الواقع العملي في قضايا تُظر فيها من قبل محاكم متنوعة وفصلت فيها بحالات عديدة وأحكام مختلفة وفقاً لحيثيات كل قضية فمنها ما فُصل وفقاً لأحكام النظرية التقليدية في مسؤولية البنوك ومنها ما ظهر ضمن مناقشاتها اتجاه جديد خرج فيه عن مسار النظرية التقليدية في ترتيب المسؤولية من جانب البنوك .

أولاً : مسؤولية البنوك في النظرية التقليدية

لما كان نشاط المصارف يقوم ابتداءً على قبول الودائع من العملاء ، لذلك فالعلاقة بين البنوك و العملاء يحدد إطارها العام بعقد الوديعة ، حيث يشكل عقد الوديعة حجر الأساس الذي نشأت منه الدراسات القانونية لتكييف العلاقة بين البنوك وعملائها^{٦١} ، فحين أن الوديعة المصرفية تقترب من الوديعة العادية بالتزام الوديع برد مثل الوديعة إلا أن الوديعة المصرفية تختلف عن الوديعة العادية في التزام الوديع الرئيس الذي يتمثل بحفظ الوديعة العادية بينما في الوديعة المصرفية يكون المصرف مأذوناً له باستخدام المال المودع لديه وله حرية التصرف به تلازماً مع التزامه برد مثله للمودع ، وكذلك لايجوز الدفع بالمقاصة في الوديعة العادية الأمر الجائز في الوديعة المصرفية ، وبالتالي فإن المصرف يمتلك المال المودع لديه ويستخدمه بحرية مطلقة مالم تكن الوديعة مخصصة لغرض معين ، ما أدى لظهور دراسات فقهية أسست لظهور فكرة الوديعة الشاذة أو الوديعة الناقصة لتطبيقها على الوديعة المصرفية التي يمتلك فيها الوديع (البنك) المال المودع لديه ويلتزم برد مثله فقط وبالتالي يكون مأذوناً له باستخدامه ويجوز له الدفع بالمقاصة ، بينما لا يمتلك الوديع المال المودع لديه في الوديعة العادية ولايحق له استخدامه ويلتزم برده عنه ولا يجوز فيها الدفع بالمقاصة، وهذا مايجعل فكرة الوديعة المصرفية أقرب إلى عقد القرض الذي ورد تعريفه في القانون المدني السوري المادة ٥٠٦ : **(القرض**

^{٦١} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية - ص ٣٥

عقد يلتزم به المقرض أن ينقل إلى المقترض ملكية مبلغ من النقود أو أي شيء مثلي آخر. على أن يرد إليه المقترض عند نهاية القرض شيئاً مثله في مقداره ونوعه وصفته ، ويرد على ذلك أصحاب فكرة الوديعة الناقصة أنه بالرغم من امتلاك البنك للوديعة والإذن له باستعمالها إلا أن ذلك لا يلغي التزامه بحفظها بل عليه أن يحتفظ بمبلغ مسأو لقيمة الوديعة في خرائنه باستمرار^{٦٢} ، وبالعودة لأحكام الوديعة الواردة في القانون المدني السوري في المادة ٦٨٤ نجد بأنه لا يمكن تطبيقها على الوديعة المصرفية حيث نصت المادة آنفة الذكر على أنه :

(الوديعة عقد يلتزم به شخص أن يتسلم شيئاً من آخر، على أن يتولى حفظ هذا الشيء، وعلى أن يرده عيناً.)

أي أن المشرع السوري حدد التزامات الوديع في عقد الوديعة بحفظ الشيء المودع ورده عيناً وهو ما لا ينطبق في حالة الوديعة المصرفية .

ومن هنا يتلشى تطبيق مبدأ فكرة الوديعة على الوديعة المصرفية ، ولو فرضنا جديلاً أن الوديعة المصرفية هي عبارة عن وديعة عادية فبالرجوع إلى أحكام القانون سنجد بأن الوديعة العادية يعتبرها القانون قرضاً إذا كان محلها مبلغاً من النقود ، وأذن للوديع باستعمالها وفقاً لما نصت عليه المادة ٦٩٢ من القانون المدني السوري :

^{٦٢} علي جمال الدين عوض – عمليات البنوك من الوجهة القانونية - مرجع سابق ص ٤٠

(إذا كانت الوديعة مبلغاً من النقود، أو أي شيء آخر مما يهلك بالاستعمال، وكان الوديع مأذوناً له في استعماله، اعتبر العقد قرضاً.)

ويقابل ذلك في التقنين المصري ويطابقه في النص ، أحكام المادة ٧٢٦ من القانون المدني المصري ،

وبالتالي تكون أحكام عقد القرض أقرب إلى الوديعة المصرفية منها للوديعة العادية ، وتنص المادة ٥٠٦ من القانون المدني السوري في تعريف عقد القرض بما يلي:

(القرض عقد يلتزم به المقرض أن ينقل إلى المقترض ملكية مبلغ من النقود أو أي شيء مثلي آخر. على أن يرد إليه المقترض عند نهاية القرض شيئاً مثله في مقداره ونوعه وصفته.)

وتؤسس هنا فكرة التكييف القانوني للوديعة المصرفية بعقد القرض ، على أساس امتلاك المال المودع للوديع والإذن له باستعماله والالتزام برد مثله لا رده عينه حتى في حالات القوة القاهرة ، إضافة إلى إن هذا التكييف يمكّن البنك من التمسك بالمقاصة بصفته مقترض الأمر الذي لايجوز تبعاً لأحكام الوديعة.

ويتجه زمرة من الفقهاء إلى أنه بالرغم من اقتراب أحكام الوديعة المصرفية لعقد القرض إلا أنهم لايستبعدون بشكل مطلق تطبيق فكرة عقد الوديعة ، حيث أنهم يرون أن الوديعة المصرفية في حالات محددة تأتلف مع أحكام الوديعة العادية ومثال ذلك الوديعة تحت الطلب ، حيث يلتزم البنك فيها تجاه العميل

برد النقود عند طلب العميل مباشرة وبالتالي لن يتمكن البنك من استخدام النقود ولن يكون مقترضاً من حيث النتيجة^{٦٣} .

ويتبين لنا بالتدقيق في أحكام الوديعة أن مجرد التزام البنك برد النقود عند الطلب غير كافٍ لاستبعاد فكرة القرض عن الوديعة المصرفية وتكييفها على أنها وديعة عادية ، فقد يكون هناك اتفاق بين المودع و الوديع في عقد الوديعة على تعيين أجل معين لمصلحة الوديع لايجوز فيها للمودع طلب رد الوديعة قبل حلول الأجل وفقاً لنص المادة ٦٨٨ مدني سوري والتي نصت على أنه :

(يجب على الوديع أن يسلم الشيء إلى المودع بمجرد طلبه، إلا إذا ظهر من العقد أن الأجل عين لمصلحة الوديع. وللوديع أن يلزم المودع بتسليم الشيء في أي وقت، إلا إذا ظهر من العقد أن الأجل عين لمصلحة المودع.)

وبالتالي فتعيين الأجل في عقد الوديعة لاينفي عنها هذه الصفة ، وكذلك كون الوديعة المصرفية تحت الطلب لا يستبعداها من دائرة أحكام القرض .

ويبدو لنا في الوديعة المصرفية أن طرفا الالتزام - البنك من جهة والعميل من جهة أخرى - كلاهما لا تتصرف نيته لحفظ المال المودع ، فبالنسبة للبنك فهو يقبل الودائع من العملاء ليقوم باستعمالها في نشاطاته المصرفية لا لحفظها وحمايتها ، وبالنسبة للعميل فهو عادة ما يقوم بإيداع المبالغ المالية إما للحصول على الفوائد أو لتسهيل نشاطاته الحياتية كالحصول على دفتر شيكات

^{٦٣} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ٤٦

أو الحصول على بطاقة ائتمان أو توظيف رواتب الموظفين وغيرها من الخدمات المصرفية أي أن العميل عندما يودع مبلغاً من المال لدى أحد البنوك فإنه يقوم بذلك للحصول على مقابل ما بشكلٍ أو بآخر ، وفي حال انصراف نيته إلى إيداع أمواله من أجل حفظها فقط ابتكرت الأنظمة المصرفية صناديق حديدية يودع فيها العميل أمواله لمجرد حفظها فقط ، إضافة إلى أن العملاء في حالات الحروب والاضطرابات يسارعون إلى سحب ودائعهم المصرفية لاعتقادهم بأن البنوك لن تكون آمنة كمنازلهم ولن تكون حريصة على مال أحد كحرص صاحب المال على أمواله ، علاوة على ذلك يوجد اختلاف جوهري في التزامات الوديع في الوديعة العادية من جهة والوديعة المصرفية لجهة أخرى ، حيث نصت أحكام القانون السوري في المادة ٦٨٦

١ . إذا كانت الوديعة بغير أجر، وجب على الوديع أن يبذل من العناية في حفظ الشيء ما يبذله في حفظ ماله، دون أن يكلف في ذلك أزيد من عناية الرجل المعتاد.

٢ . أما إذا كانت الوديعة بأجر، فيجب أن يبذل في حفظ الوديعة عناية الرجل المعتاد.

ومن نص المادة سالف الذكر نجد بأن التزامات الوديع بحفظ الوديعة لا تتجاوز عناية الرجل المعتاد كحدٍ أقصى وبالتالي فلن يتحمل الوديع تبعه هلاك الشيء المودع لديه إذا اتبع في عانيته وحفظه للوديعة عناية الرجل المعتاد ، الأمر الغير مقبول بالنسبة للمصارف التي تلتزم بشكل دائم برد مثل

المال المودع لديها ، إضافة إلى ذلك ففي أحكام الإفلاس فإذا شهر إفلاس البنك سيدخل عملائه التقليسه حتماً شأنهم شأن سائر الدائنين بينما لو اعتمدنا تطبيق أحكام الوديعة على الوديعة المصرفية فلن يدخل العملاء بالتقليسة وسيكون لهم الحق باسترداد ودائعهم عيناً دون الدخول في كتلة الدائنين كون الوديع لايمتلك الشيء المودع ولو أُذن له باستعماله .

ومن دراسة النظريات السابقة يتضح بأن التكييف الذي يأتلف والمنطق القانوني بالنسبة للوديعة المصرفية هو إدراجها ضمن أحكام عقد القرض فالمصرف يمتلك النقود المودعة لديه ويُأذن له باستعمالها ويكون ملزماً برد مثلها من نفس النوع وهو ما يتوافق مع أحكام التشريعات العربية عموماً^{٦٤}.

- انطلاقاً من النظرية التقليدية في مسؤولية البنوك ، تنهض مسؤولية البنوك تجاه عملائها إما تأسيساً على فكرة المسؤولية العقدية أو وفقاً لنظرية تحمّل المخاطر المهنية (المسؤولية المفترضة) ، وقد تترتب بجانب البنوك مسؤولية تقصيرية تجاه الأغيار (غير العملاء بالنسبة للبنك) .

ففي كل واقعة لايمكن فيها القاضي من تحميل المسؤولية على الغير وإن لم يوجد أي خطأ بجانب أحد أطراف النزاع ، سيقوم مع ذلك بتحميل البنك المسؤولية وفقاً لنظرية المسؤولية المفترضة التي تقوم على مبدأ تحمل المخاطر المهنية (الغرم بالغرم) تبعاً لقبول البنوك ودائع عملاءها ، وهذا من انتهجته

^{٦٤} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ٤٧

المحاكم أثناء نظرها في قضايا مسؤولية البنوك تجاه عملائها حيث ورد في قرار محكمة النقض المصرية (نقض ١١ يناير ١٩٦٦ مج ١٧ ص ٩٤) بمسؤولية البنك تجاه العميل بصدد وفاء شيك يحمل توقيع مزور منسوب إلى الساحب دون أن يثبت خطأً على العميل صاحب الحساب تسبب في وقوع التزوير، ولا خطأً على البنك في عدم كشف التزوير وذلك تفعيلاً لنظرية تحمل مخاطر المهنة ^{٦٥} ، وإن امتلاك البنوك للنقد المودعة لديها والتزامها برد مثلها هو من أهم آثار تطبيق فكرة عقد القرض مما يترتب عليه اعتبار العميل المودع ^{٦٦} دائماً للبنك وبالتالي فإن البنك سيبقى ملتزماً برد مثل ما اقترض وفق أحكام القانون ويتحمل تبعة هلاكه ويبقى العميل في منأى عن تمسك البنك بأحكام القوة القاهرة ^{٦٧} .

وما يبدو لنا بعد التمهيص بالعبرة الواردة سابقاً في حكم محكمة النقض المصرية بصدد وفاء شيك يحمل توقيع مزور منسوب إلى الساحب ((دون أن يثبت خطأً على العميل صاحب الحساب تسبب في وقوع التزوير)) واستناداً لمفهوم المخالفة يتبين لنا إمكانية ترتيب المسؤولية من جانب العميل فيما لو صدر منه خطأً ما تسبب في وقوع التزوير ، ويبدو بأن هذه النقطة هي

^{٦٥} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ١٢١٣

^{٦٦} ونعتقد بأن الأدق إطلاق لفظ المقرض على العميل عوضاً عن المودع سنداً لتكليف الوديعة المصرفية كعقد قرض، لكن يبدو بأن المصارف تنتهج نهجاً تسويقياً بإطلاق لفظ المودعين على عملائها ، فشيوخ فكرة عقد القرض بين الأفراد قد تلجم بعضهم من التعامل مع البنوك ، بينما استخدام مصطلح المودع قد يشعر العميل بشيء من الأمان ويبعث في نفسه الاطمئنان بأن نقوده في مأمن .

^{٦٧} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ٦١

الأساس التي ارتكزت عليه فكرة النظرية الحديثة لمسؤولية البنوك ، التي ترفض قيام مسؤولية البنوك في تعويض عملائها جراء الهجمات الالكترونية دون حدود أو ضوابط وتحاول استبعاد فكرة بقاء البنوك ملزمة بتحمل المسؤولية والأضرار الناجمة عن عمليات القرصنة الالكترونية دون الالتفات إلى الوقائع التفصيلية المكونة لكل حالة على حده ، ودون البحث في وقوع الخطأ بالفعل من قبل البنوك من عدمه .

فوفقاً للنظرية التقليدية في مسؤولية البنوك تجاه عملائها في حال تعرض حساباتهم المصرفية للقرصنة الالكترونية ستتحقق مسؤولية البنوك عن التعويض لعملائهم تحت أي ظرف كان ، وذلك باعتبار أن عملية القرصنة تكيف على أنها جريمة احتيال وبالتالي فالبنك هو من عليه تحمل تبعاتها وهو من يتوجب عليه حماية مخدماته على الشبكة وتأمين حسابات عملائه ، ولا مجال للدفع بأن البنك لم يتوقع وقوع الاحتيال (القرصنة) وهو من أولى مخاطره في الوقت الراهن أو أنه قد بذل العناية الكافية لمنع حدوث أو استمرار عملية القرصنة ، كون ذلك لا يخرج عن دائرة مخاطر مهنته كمصرف يستقبل ودائع المودعين ويقدم لهم خدمات عبر الشبكة .

بعد الخوض في هذا البحث يلاحظ اتجاهاً حديثاً ينادي بتبديل محدود للمبدأ السائد منذ القدم والذي يعتبر مسؤولية البنوك متحققة بشكل مستمر ، ويبدو بأن الغاية من ذلك هو التخفيف عن المصارف في تحمل المسؤولية من جراء عمليات القرصنة وما قد تلحقه من أضرار تقدر بعشرات لا بل مئات وقد تبلغ مليارات الدولارات وهذا قد يؤدي بلا شك إلى انهدام النظام المصرفي العالمي ،

وسيتضح من خلال دراسة القضايا المختلفة غياب لنظرية المسؤولية المفترضة في قضايا مسؤولية المصارف في معرض الهجمات الالكترونية التي تستهدف الحسابات المصرفية وإنما عندما تعرض قضية ما في هذا الصدد على القاضي سيقوم كل من المتداعين بمحاولة إلقاء عبء المسؤولية على خصمه ويسعى جاهداً في البحث لإثبات خطأ ما وقع من خصمه ، وفي إثبات العلاقة السببية بين هذا الخطأ والضرر ، وفي النهاية يصدر القاضي حكمه وفقاً للحثيات والدفع المعروضه أمامه ويتجنب تفعيل نظرية المسؤولية المفترضة في حال عجز العميل عن إثبات الخطأ الفعلي للبنك بصد الهجمات الالكترونية .

ثانياً : مسؤولية البنوك في النظريات الحديثة

عندما يقوم القراصنة باختراق حسابك المصرفي لسرقة بعض المبالغ المالية ، فإن البنك سيكون مسؤولاً بتعويضك عن الخسارة جراء الهجمات الالكترونية في معظم الحالات وسيعيد الأموال المسروقة إلى أصحابها تبعاً لوجهة النظر السائدة في الدراسات القانونية والفقهية والمستقرة في أروقة قضاء المحاكم .

لكن هذه القاعدة لن تطبق على إطلاقها ، حيث أن الاتجاهات الحديثة في نظرية مسؤولية البنوك جراء الهجمات الالكترونية على الشبكة تسعى لتخفيف المسؤولية التي تترتب من جانب البنوك وذلك تبعاً لاتساع نشاطات القرصنة بشكل ملحوظ في العقد الأخير ناهيك عن إيقاعها لخسائر ضخمة تقدر بمئات ملايين الدولارات ، وإن الاستمرار بتطبيق مبدأ النظرية التقليدية بمواجهة البنوك في خضم هذه النزاعات سيرهقها حتماً وسيؤدي من حيث النتيجة إلى انهيار النظام المصرفي العالمي شيئاً فشيئاً .

إضافة إلى الاتجاه الراغب بتخفيف المسؤولية بجانب البنوك جراء الهجمات الالكترونية فثمة فكرة تطرح نقاشاً هاماً ومفصلياً قد يشكل نقطة الفصل بين النظرية التقليدية والنظرية الحديثة ، وهي مدى مساهمة العميل صاحب الحساب في الخطأ أو الإهمال من جانبه والذي هيأ أو سهل أو أتم عملية القرصنة الالكترونية (سلوك الضحية) ، وتضح لنا هذه الفكرة من العودة لحكم القضاء المصري بصدد شيك يحمل توقيع مزور - المذكورة آنفاً في البحث - فكيف ستكون نظرة المحكمة فيما لو كان قد صدر خطأ من جانب العميل

الساحب ساهم في وقوع التزوير ؟ وهل كانت المحكمة ستتجه لتحميل المسؤولية لجانب العميل والبنك معاً ؟ أم أنها ستبحث في خطأ العميل وفقاً لنظرية الخطأ المُستغرق والخطأ المُستغرق ، ومامدى مسؤولية العميل عن عملية القرصنة فيما لو أنها بدأت ضمن أنظمتها الشبكية ، أي أن المقرصن قد اخترق أنظمة العميل المعلوماتية وقام بعملية القرصنة من خلال شبكة العميل ، مع الأخذ بعين الاعتبار أن العميل قد يكون شخص اعتباري ومهني وبالتالي عليه أيضاً التصدي لمسؤولياته المهنية والتصدي لبعض المخاطر المحتملة كتأمين شبكته المعلوماتية التي يقدم من خلالها خدمات عبر الانترنت ، وبالتالي ترتيب المسؤولية إلى جانبه في حال ثبوت خطئه أو إهماله في ذلك الواجب .

- ثمة تمييز بالنسبة لمسؤوليات البنوك ، بين أنواع الحسابات الشخصية و الحسابات التجارية التي تعود لشركات أو منظمات تتمتع بالشخصية الاعتبارية وتتخذ حداً أدنى من التنظيم في إدارتها ، وتنتهج أسلوب واضح في كيفية إدارتها وتحديد مسؤولية القائمين على هذا الشخص الاعتباري ، والقوانين عموماً تعالج مسألة الحسابات الشخصية أو حسابات الأفراد والشركات بشكل مختلف يتوافق والمبدأ المذكور آنفاً ، ومرد ذلك أن الشركات أو الأشخاص الاعتبارية عموماً ، يجب أن تكون أكثر حرفية ومهنية من الأفراد في تأمين حساباتها ومعلوماتها السرية الهامة ، خاصة في معرض تقديمها لخدمات عبر الانترنت ، فعندما يتعرض حساب مصرفي لشركة ما للقرصنة عبر مخدمات الشركة أو انطلاقاً من أنظمتها المعلوماتية الخاصة التابعة لسلطتها وتوجيهها

وسياستها في الإدارة ، فلن تترتب المسؤولية كاملةً إلى جانب البنك بل سيتحمل صاحب العمل (الشخص الاعتباري) المسؤولية نسبياً أو جزئياً مع البنك .

يعود السبب في ذلك إلى أن البنوك تعتقد أن الشركات التجارية يتوجب عليها أن تتخذ التدابير الأمنية المناسبة لحماية أصولها وموجوداتها وأموالها وأجهزتها وأنظمتها المعلوماتية التابعة لرقابتها وأن تتوخى الحذر الكافي لتلافي وصول معلوماتها المصرفية السرية للغير ، وأن تتحمل تبعة عدم ثقة موظفيها الذين قد يكون في متناولهم بعض المعلومات السرية ، ففي حال تمكن أحد القراصنة من استدراج موظف تابع لشركة ما وتمكن من خلاله من الحصول على بعض المعلومات السرية للشركة ومن ثم قام بعملية قرصنة استهدفت حساب هذه الشركة المودع لدى أحد البنوك ، فإن هذا الأمر هو من مسؤولية الشركة أو صاحب العمل ولا يمكن ترتيب أي مسؤولية على البنك جراء هذا العمل وفقاً للقناعة السائدة لدى المصارف ، والتي تؤيد قناعاتها في تفعيل مبدأ المسؤولية عن عمليات القرصنة والهجمات الالكترونية على مبدأ نظرية المسؤولية التقصيرية ، والتي تقوم على الخطأ والضرر والعلاقة السببية ، حيث تركز أحكام هذه النظرية على مبدأ الخطأ المستغرق والخطأ المستغرق^{٦٨} .

^{٦٨} عبد الرزاق السنهوري - الوسيط في شرح القانوني المدني - المجلد الأول - نظرية الالتزام - دار

النهضة العربية - القاهرة - ١٩٦٤ - فقرة ٥٩٣-٥٩٤-٥٩٥ ص ١٠٠٠ .

فانطلاقاً من تكيف عملية القرصنة كجريمة احتيال وعلى اعتبار أن كل جريمة هي خطأ ، وأن الخطأ المسبب للضرر يوجب التعويض وفقاً لأحكام المسؤولية التقصيرية فالبنوك تعتبر بأنها تضررت من الخطأ المتمثل بجريمة الاحتيال وبالتالي فإن هذا الخطأ قد ألحق بها خسائر تتمثل في سرقة حسابات بعض العملاء المصرفية والذين سيطالبون بتعويض حساباتهم المسروقة وبالتالي فلو كان الخطأ المتمثل بجريمة الاحتيال كان نتيجة لخطأ آخر غيره صدر من العميل أو أن خطأ العميل قد استغرق خطأ البنك في إيقاف أو كشف عملية القرصنة (كإهمال العميل كشخص اعتباري تأمين أنظمتة المعلوماتية أو تأمينها بنظام هش يسهل اختراقه أو عدم حفظه للبيانات السرية بشكل أمن مما سهل على القراصنة الحصول عليها والقيام بعملية القرصنة) فهنا لن تترتب المسؤولية بالتعويض إلى جانب البنوك .

ويبدو لنا أن هذا المبدأ مقارب للصواب إلى حدٍ معقول ، فلما كان أفراد المجتمع متقاعون في الوعي والحرص والإدراك والمقدرات العقلية ، فمنهم من هو شديد الحرص والوعي وبالتالي يبقى هذا الصنف من الأفراد في منأى عن الخضوع لأحكام المسؤولية التقصيرية ، ومن هنا نجد بأن قواعد نظرية المسؤولية التقصيرية لاتطال في أحكامها سوى الفئة الأخرى من أفراد المجتمع وهم من يكونون بدرجة أقل من تلك الفئة الأولى في الحرص والوعي والذكاء ، وبالتالي يكون ماقد يصدر من أخطاء وأفعال ضارة من جانب الفئة الأخيرة يشكل الواقع الأمثل لتفعيل أحكام المسؤولية التقصيرية .

ففي حال أن الضرر الواقع كان بخطأ المتضرر أو بخطأ تابعيه واستغرق هذا الخطأ خطأ البنك في فشله في كشف عملية القرصنة وإخماد نشاطهم ، فإن على المتبوع أن يتحمل تبعه أخطاء متبوعيه وبالتالي لن تترتب هناك أية مسؤولية على البنوك بالنسبة لحسابات الشركات التي قد تتعرض للقرصنة ،

ومن المثير للاهتمام في مثل هذه النزاعات بأن البنوك لا تعتقد بأنها هي من تعرض للسرقة ، بل تعتبر أن حسابات عملائها هي التي تمت سرقتها بسبب قلة احترازهم بالعناية المطلوبة وعدم حمايتهم لبياناتهم السرية وأن هذه المسألة هي مشكلة يتحملها العملاء لا البنوك .

بينما يسعى العملاء أصحاب الحسابات المسروقة إلى تفعيل مبدأ المسؤولية العقدية بمواجهة البنوك وفقاً للأحكام العامة لطبيعة العلاقة بين البنك والعميل في الوديعة المصرفية والتي تكيف كعقد قرض في صفتها الغالبة ، وبالتالي سيكون البنك ملزماً برد مثل النقود المسروقة التي استلمها في الوديعة المصرفية مما دفع بالبنوك للسعي جاهدة في تضمين عقودها الموقعة مع الشركات الكبرى بنداً خاصاً يتعلق بتحديد مسؤولية البنوك ضد الهجمات الالكترونية ، وإخضاع أحكامها إلى المسؤولية التقصيرية باعتبارها من الجرائم ولا مجال إلا لتفعيل مبدأ المسؤولية التقصيرية في هذا الصدد، بالإضافة إلى تحديد مسؤولية البنوك في مجال أمن المعلومات والوقاية من الهجمات الالكترونية بعناية الرجل العقلاني being rational كما سيتضح ذلك لاحقاً .

وبالرغم من المناقشة الدقيقة التي تجريها المحاكم في دراستها للقضايا إلا أنه لا يبدو أن هناك أساس واضح تستند إليه المحاكم في ترتيب المسؤولية لجانب

أحد الأطراف ، الأمر الذي أثقل كاهله علينا في هذا البحث بدراسة مبادئ النظرية الحديثة لمسؤولية البنوك من ضمن الأحكام القضائية ومناقشتها للوقائع وتكييفها للعلاقات ، واستخلاص قواعد ومبادئ تلك الاتجاهات القانونية.

فقد صدر حكم عن محكمة مقاطعة ميتشغن في الولايات المتحدة في قضية في العام ٢٠٠٩ .

^{٦٩}: Ocean Bank vs Patco Construction Company Inc

حينما أقامت شركة باتكو دعوى قضائية بمواجهة بنك المحيط في عام ٢٠٠٩ تطالبه فيها بتعويضها عن عملية القرصنة التي استهدفت حسابات الشركة لدى البنك بمبلغ حوالي \$٦٠٠٠٠٠٠ دولار امريكي .

حيث دفع محامو البنك بأن القراصنة قد تمكنوا من الحصول على القبول والموثوقية للتسلل لحسابات الشركة لدى البنك في شهر مايو ٢٠٠٩ من خلال برامج تسجل ضربات لوحة المفاتيح تم دسها ضمن أجهزة موظفي الشركة ، وبالتالي سمحت لهم بالوصول إلى إجابات أسئلة الأمان الموضوعة من قبل نظام البنك من أجل استخدام التحويل عبر الانترنت ، وبالتالي فإن ذلك يلقي

^{٦٩}. "Three Recent Cases Against Banks And The Aegis Journal ٢٠١٦ Liability For Losses Suffered By Their Client From Hacking And Phishing." <http://www.aegisjournal.com/book-and-product-reviews-%E2%80%93three-recent-cases-against-banks-and-the-liability-for-losses-suffered-by-their-client-from-hacking-and-phishing/>. راجع الموقع الالكتروني

بتحمل المسؤولية على شركة المقاولات التي لم تقم بتوفير الحماية اللازمة لأجهزتها التي تحوي معلومات مصرفية سرية ولم يلحظ موظفوها وجود برامج تطفل مدسوسة داخل أنظمتهم أثناء عملهم مما سمح للقراصنة بالحصول على المعلومات السرية المطلوبة التي تمكنهم من الوصول إلى حسابات الشركة لدى البنك .

ومن وجهة نظر صاحب الشركة ، أن شركته هي شركة عمل صغيرة ليس لديها موظفين محترفين في مجال أمن المعلومات ضمن فريق العمل ويتابع قوله " نحن لسنا صيارفة محترفين وليست لدينا الدراية الكافية حول كافة تهديدات أمن المعلومات وليس لدينا الخبرة اللازمة في كيفية التعامل معها أو في كيفية تهيئة وسائل الحماية من أخطارها "

حيث قضت المحكمة من حيث النتيجة لصالح بنك المحيط ضد شركة المقاولات وقضت في حكمها بعدم تحمل البنك أية مسؤولية عن سرقة \$٣٤٥٠٠٠ . خاصة وأن البنك تمكّن من كشف عملية القرصنة في وقت لاحق واستطاع من استرجاع جزء من المبالغ المسروقة .

ويبدو بأن المحكمة في مناقشتها لقرارها هذا وفي اتجاهها لترتيب المسؤولية إلى جانب متحملها استندت على مبدأ خطأ المضرور - الذي وقع من قبل موظفي شركة باتكو التابعين لها - حيث استغرق خطأهم خطأ البنك المفترض في عدم كشفه لعملية القرصنة منذ البداية .

- وفي قضية أخرى تعد من أكبر و أهم القضايا التي ناقشت المحاكم فيها عملية قرصنة غير مسبوقة في تاريخ الهجمات الالكترونية على البنوك ، في العام ٢٠١٣ وهي قضية Target Corporation VS Umpqua Bank – Mutual Bank – Village Bank – CSE Federal Credit Union – and First Federal Savings of Lorain^{٧٠}

سنناقش في هذه القضية جانب من استدعاء الدعوى المقدم من المدعين - والذي بلغ أكثر من ٤٠ صفحة - وكيفية معالجته لمبدأ المسؤولية والأساس القانوني الذي يستند إليه المدعون في إثبات دعواهم وإلقاء المسؤولية على الشركة التي تمت قرصنتها لا على البنوك الحافظة لأموال المودعين أو العملاء .

تتلخص وقائع هذه القضية وفقاً لاستدعاء الدعوى ، بأن المؤسسات المالية التي أصدرت بطاقات الائتمان المرتبطة باتفاقات دفع الكتروني مع شركة تارغيت تعرضت لعملية احتيال عن طريق قرصنة حواسيب وأنظمة شركة تارغيت وألحقت الخسائر الكبيرة بعملاء هذه المصارف بعد أن تعرضت شركة تارغيت لعملية قرصنة غير مسبوقة .

في ١٥ نوفمبر ٢٠١٣ تعرضت شركة تارغيت لعملية الاختراق -هجمات الكترونية غير مسبوقة- ، عندما قام قراصنة باختراق شبكة شركة تارغيت

^{٧٠} Target Corporation VS Umpqua Bank – Mutual Bank – Village Bank –

CSE Federal Credit Union – and First Federal Savings of Lorain. ٢٠١٦.

بسهولة عن طريق قيامهم بإنشاء حساب وهمي - غير حقيقي - باسم فايزو ، وقاموا من خلال هذا الحساب - فايزو - الذي أوهم حواسب الشركة بأن فايزو هو زبوناً لشركة تارغيت ، وبمجرد قيام القراصنة بتسجيل الدخول على نظام الشركة بالاسم الوهمي وهو "فايزو" تمكّن القراصنة من الحصول على تصريح من قبل حاسب الشركة سمح لهم بالوصول إلى قسم الفواتير وقسم العقود وقسم إدارة المشاريع ، وذلك بسبب عدم قيام الشركة باعتماد نظام يقوم بتجزئة وتنظيم أقسامها بشكل أكثر أمناً ، وفقاً لوثائق مبرزة ، واستغل القراصنة هذه الثغرة في نظام الشركة وتمكنوا من زرع برامجهم الخبيثة على أكثر الأنظمة حساسية وهي أنظمة دفع العملاء وقسم تخزين المعلومات الشخصية للعملاء والتي تتضمن أرقام بطاقات اعتمادهم وأرقام حساباتهم وغيرها من المعلومات المصرفية السرية.

والثغرة التي استغلها القراصنة متعلقة بآلية حفظ البيانات على مخدم الشركة ، وفي هذه الحالة حينما تكون الحواسب متصلة بشبكة الانترنت فإنه ينبغي أن تكون بعض البيانات السرية مؤمنة بشكل لايسمح للوصول إليها إلا من الموظفين المصرح لهم بالوصول إليها ، ولكنها في الواقع كانت متاحة دون قيود ، ووفقاً لخبراء المحكمة " لاينبغي ان تكون هذه الشبكة متاحة لعميل خارجي متصل من خارج شبكة الشركة (كما في حال قيام أحد الزبائن عن بعد باستخدام الخدمات المتاحة عن طريق شبكة الانترنت) حيث كان ينبغي أن يكون هناك فصل بحفظ البيانات ، لإبقاء المعلومات الأمنية خارجة عن متناول الغير ، وهذا هو الخلل الذي استغله القراصنة"

وفي داخل قسم المدفوعات وقسم العملاء لتارغت قام القراصنة بزرع برامجهم الخبيثة و استهدفوا من خلالها في البداية المبالغ الصغيرة لصغار العملاء المسجلين لدى تارغيت ، وخلال هذه الفترة قام القراصنة باختبار برامجهم الخبيثة ليتأكدوا من فاعليتها .

ولمنع ذلك كان ينبغي على تارغيت أن تخصص نظام الاقتران الخاص بها من خلال عاملين للتوثيق : العامل الأول التوثيق من هوية المستخدم و إيجاد تأمين خاص بطريقة الدفع عن طريق بطاقة الائتمان ، ولو كان ذلك لتعذر على القراصنة الوصول إلى الشبكة من خلال حساب "فايزو" . والعامل الثاني هو التوثيق من أن المستخدم هو شخص حقيقي وليس مجرد جهاز أو برنامج خبيث وهمي ، وذلك عن طريق إرسال رسائل تأكيد على الهاتف المحمول للعميل المستخدم ، أو من خلال أسئلة أمنية احتياطية (قد لايمكن للقراصنة تخطيها) ، أو من خلال استخدام وسائل التأكيد بالرموز التي لايمكن إدراكها إلا من قبل شخص حقيقي مما يتعذر على البرامج الخبيثة تخطيها .

وفي ٣٠ نوفمبر قام القراصنة بتثبيت برنامج سرقة أرقام البطاقات الخبيث على شبكة تارغيت عن بعد .

وكذلك بدأ القراصنة نشاطهم بجمع البيانات الحية للعملاء وكان ذلك غاية في السهولة دون أي تعقيد ، فعند قيام أحد العملاء بالذهاب لأي متجر لتارغيت فإنه يقوم بتمرير بطاقته على الجهاز الخاص المرتبط بشبكة تارغيت وبكل بساطة فإن كافة البيانات المحفوظة على البطاقة - الشريط

المغناطيسي- ستصل إلى القراصنة عندما تحفظ على النظام المعلوماتي لشبكة تارغيت .

وتابع القراصنة نشاطهم أيضاً في ١ ديسمبر ٢٠١٣ حيث قام القراصنة بزرع برامج خبيثة أخرى ، وتمكنوا من تأمين اتصال مستمر مع قاعدة بيانات الشبكة التي تحوي على ملفات التخزين الاحتياطية ، وتمكنوا من خلال ذلك أن يحصلوا على نسخة كاملة عن محتوى الملفات الاحتياطية التي يتم إرسالها بشكل تلقائي إلى مخدم شبكة يقع في روسيا تقادياً لخطر التتبع الذي تقوم به مخدمات الشبكة بشكل آلي ومن ثم أخذوا يقومون ببيع معلومات البطاقات المسروقة وتوابعها الالكترونية ورموز التعريف الشخصية لكل بطاقة PIN في السوق السوداء على المواقع الغير شرعية^{٧١}.

والمثير للاهتمام وفقاً لما جاء باستدعاء الدعوى " أن نظام الأمن eye fire كان قد سجل تنبيهات لعدة عمليات مشبوهة ، كان بإمكان الشركة من خلالها إحباط عملية القرصنة بأكملها ، وفريق أمن المعلومات في تارغيت لم يقوم بدوره بأي تدبير من شأنه إحباط عملية القرصنة "

^{٧١} حيث تعتمد هذه الطريقة في سرقة الحسابات على استهداف أصحاب الحسابات الصغيرة ، وتقوم بسرقة كافة معلومات البطاقات الائتمانية وتقوم ببيع معلومات البطاقة بنصف قيمة الرصيد فعلى سبيل المثال يتم بيع بطاقة تحتوي على رصيد يبلغ \$٣٠٠ بمبلغ ١٠٠ أو \$١٥٠ فقط ، ومن يقوم أحدهم بشراء البطاقة مع الملاحظة أن المشتري لم يشتري البطاقة عيها وإنما حصل على بياناتها المصرفية كاملة وأصبح بإمكانه التسوق عبر الانترنت وشراء كل مايرغب ويقوم بتسديد الثمن عن طريق معلومات البطاقة فيدخل رقم الحساب ويدخل رقم البطاقة ويدخل التوقيع الالكتروني الخاص بالبطاقة وبالتالي يكون القراصنة قد سرقوا معلومات الحسابات وباعوها دون أن يقوموا بسرقة أي مبلغ من داخل الحساب ذاته ودون وقوعهم في دائرة أي خطر كون طريقة البيع هذه ستكون على مواقع غير شرعية أو مواقع تواصل اجتماعية أو مواقع غرف دردشة خاصة الأمر الذي يجعل من المحال إمكانية ضبط منافذ البيع هذه .

- من الواضح من خلال ما تقدم به المدعون في هذه الدعوى أن البنوك كطرف مدعي في هذه القضية تسعى لنفي المسؤولية من جانبها بالنسبة لعملية القرصنة التي وضعت حسابات العملاء في البنوك الهدف الرئيس لها ، لا حسابات العملاء لدى تارغيت ، ولم تكن مخدمات أنظمة تارغيت المعلوماتية سوى المنفذ الذي تم من خلاله الحصول على المعلومات المطلوبة ، ولكن البنوك تسعى من خلال هذه الادعاءات إلى إثبات استغراق خطأ شركة تارغيت المتمثل في إهمالها لحماية البيانات السرية لعملائها وعدم اتخاذها التدابير الوقائية اللازمة وتجاهلها للتنبيهات التي رُصدت على برامج الجدران النارية ، حيث تحاول البنوك هنا إثبات أن هذا الخطأ والإهمال من جانب تارغيت كان السبب الرئيس لنجاح عملية القرصنة و استغرق خطأ البنوك في حماية حساباتها التي كانت هي الهدف الحقيقي لعملية القرصنة .

واعتبرت البنوك المدعية أن شركة تارغيت وهي شركة عالمية تعد ثاني أكبر شركة في أمريكا وتضم حوالي ١٧٩٧ متجر في الولايات المتحدة وكندا والمكسيك ، وفي الفترة الواقعة من ١١/١٢ إلى ١٢/١٥ من العام ٢٠١٣ ، وفي واحدة من أكبر عمليات القرصنة في تاريخ الهجمات الالكترونية ، تعرضت حواسيب وأنظمة هذه الشركة لهجمات الكترونية تمكن القراصنة من خلالها من الوصول إلى معلومات مالية وشخصية استهدفت حوالي ١١٠ مليون زبون من زبائن هذه الشركة ، وأن هذه الشركة وهي بهذه الأهمية التجارية لا يمكن أن تكون في منأى عن أخطار الهجمات الالكترونية وأن واجبها بحماية المعلومات السرية لا يقل أهمية عن واجب البنوك في حماية

حساباتها ، وأنه كان يتوجب عليها القيام بكل ما هو ممكن من تدابير سواء من الناحية التقنية أو من ناحية احتوائها لبرامج الحماية المطلوبة أو سواء للحرفية المطلوبة في التعامل مع الهجمات الالكترونية ، وأنه لا مجال للبحث في مسؤولية البنوك في هذه الحالة.

ومن خلال مناقشة قرار الحكم في هذه القضية الذي قرر من حيث النتيجة بعدم تحميل البنوك أية مسؤولية عن عملية الاحتيال التي قام بها القراصنة أو عن أية تحويلات مالية تمت بواسطة الحسابات التي تمكن القراصنة من الوصول إلى معلوماتها ، حيث ثار جدال قانوني شديد في إلقاء كل طرف في القضية بالمسؤولية على خصمه ، فحيث أن البنوك تعتبر أن حساباتها لم تكن لتتعرض لأي عملية قرصنة لولا الإهمال من جانب تارغيت في التعامل مع هذه الهجمات الالكترونية التي لم تكن لتتجح لو لم تتمكن من الحصول على المعلومات السرية من قاعدة بيانات تارغيت ، في حين أن تارغيت دفعت بعدم تحملها المسؤولية كلياً أو على الأقل جزئياً مؤسسة دفعوها على اعتبار أنها ليست مؤسسة مالية لإصدار بطاقات الائتمان ولايجوز للبنوك التوصل من المسؤولية التي تقع عليها بشكل رئيسي في حماية حسابات عملائها ، فبالرغم من أن القراصنة قاموا بسرقة المعلومات من قاعدة بيانات تارغيت إلا أنه كان يتوجب على البنوك اتخاذ تدابير الأمن المطلوبة لمنع أي عملية احتيال الكترونية من استهداف حسابات العملاء ، بصرف النظر عن مصدر سرقة المعلومات المصرفية ، وهذا واجب ومسؤولية البنوك من حيث النتيجة .

ويبدو من خلال ماورد في حيثيات الحكم كيفية تأسيس المحكمة للمسؤولية بعيداً عن نظرية المسؤولية المفترضة ، وإنما اتبعت قواعد الإثبات بشكل منفصل دون أي أعمال لنظرية المسؤولية المفترضة من جانب البنوك التي كانت حساباتها هي الهدف الحقيقي لعملية القرصنة بشكل مباشر تمكن القراصنة من خلالها من سرقة أكثر من ٤٠ مليون بطاقة ائتمان .

ووفقاً لتقرير مجلس الشيوخ الذي أصدر رأيه في هذه القضية قبل عرضها على المحكمة ، فإنه كان بإمكان تارغيت إحباط عملية القرصنة فيما لو تعاملت بجدية مع التحذيرات المسجلة على نظام fireeye ، وكذلك كان بإمكان تارغيت تجنب الاختراق فيما لو كانت تولي الاهتمام للتقارير الفنية والحكومية المتعلقة بتهديدات الهجمات الالكترونية ، التي قد تقلل من أخطار تلك التهديدات بعد أن تبين لاحقاً وجود ضعف في أنظمة الحماية لتارغيت .

حيث تضمنت هذه التقارير توصيات لاتخاذ خطوات أمنية تمكن من تجنب إنشاء حسابات افتراضية غير حقيقية كما فعل القراصنة في حساب "فايزو" ، وكذلك ما تضمنته تلك التوصيات من ضرورة توفير أنظمة أمان أكثر حساسية تُعنى بحماية البيانات السرية الهامة للعملاء وأن إهمال هذه المتطلبات سمح للقراصنة بإنشاء حساب وهمي وتمكنوا من خلاله من الوصول إلى قسم المدفوعات والبيانات الشخصية العائدة لتارغيت .

وكذلك في ٣٠ نوفمبر وفي ذات الوقت الذي قام به برنامج fireeye بإرسال تنبيهات خطر عن نشاطات مشبوهة فإن نظام التأمين antivirus

spy system كذلك قد أعطى تنبيهات بذات الصدد ولكن تقاعس تارغيت عن التعامل بجدية مع تلك التنبيهات سمح بإتمام عملية القرصنة.

وكذلك في ٢ ديسمبر أرسل نظام fireeye تحذيرات جديدة عن عمليات مشبوهة وللمرة الثالثة تجاهلت تارغيت تلك التنبيهات دون القيام بأدنى جهد لمحاولة إحباط عملية القرصنة وبالتالي فإن شركة تارغيت قد تجاهلت ثلاثة فرص كان بإمكانها من خلالها إحباط عملية القرصنة ، وبعدها تمكن القراصنة بكل سهولة من الحصول على بيانات كل بطاقة تمرر على جهاز الدفع الالكتروني لدى أي متجر تابع لتارغيت ، من خلال تمكن القراصنة من الوصول إلى وحدة التخزين المؤقت على شبكة تارغيت وإمكانية الوصول إليها وحفظها عبر مخدم يقع في روسيا تابع للقراصنة ، وقد كرر القراصنة هذه العملية لمدة أسبوعين تقريباً دون أية مضايقة تذكر .

ووفقاً لتقرير مجلس الشيوخ فإنه كان من الممكن تعطيل عملية لقرصنة في هذه المرحلة من خلال إقامة جدران حماية نارية بين شبكات تارغيت وشبكات الانترنت وكان ذلك يمنع القراصنة من السيطرة على بيانات تارغيت بسهولة .

وأن البيانات المسروقة من شركة تارغت سرعان ما ملأت السوق السوداء وسارع القراصنة لبيع المعلومات التي استولوا عليها خلال عمليات الاختراق .

وفي ١٢ ديسمبر كان أحد البنوك قد نبّه أن هناك بعض البطاقات الائتمانية تمت سرقتها وأن جميع البطاقات المسروقة كانت تستخدم في متاجر عائدة لشركة تارغيت.

وفي ١٣ ديسمبر اتصلت وزارة العدل الأمريكية بشركة تارغيت لتنبيهها حول الهجمات التي تتعرض لها لكن تارغيت لم تباشر بتطهير أجهزتها قبل ١٥ ديسمبر مما سمح باستمرار عمليات القرصنة لمدة ثلاثة أيام أخرى ، وفي النهاية أوقفت تارغيت عملية القرصنة بعد أسبوعين من الاتصال المستمر بحواسيب وشبكات تارغيت دون انقطاع .

ووفقاً لجلسة استماع مجلس الشيوخ ووفقاً للتحقيقات التي أجراها الصحفيين الاستقصائيين وخبراء القانون وخبراء أمن المعلومات فقد تبين بأن البيانات التي تم الحصول عليها بسهولة كان من الممكن إفشالها وأن الشركة لم تتخذ الخطوات المناسبة لحماية بياناتها كما وأنها تجاهلت التحذيرات الواضحة التي كان من الممكن معها إحباط عملية القرصنة التي استهدفت أنظمتها .

وإن المدّعين طالبوا بتحميل تارغيت المسؤولية بسبب إهمالها في حفظ معلوماتها السرية ومعلومات عملائها وفشلها في التصدي لخطر الهجمات الالكترونية .

وباتجاه آخر ثمة أسباب أخرى توجب ترتيب المسؤولية إلى جانب تارغيت ومنها خرق قانون مينسوتا للبطاقات المصرفية ، والذي يوجب على المؤسسات المالية التي تستخدم بطاقات الائتمان في أنظمة الدفع الالكترونية بحذف كافة

المعلومات المتعلقة ببطاقات الدفع خلال ٤٨ ساعة منذ ساعه الدفع ، كذلك ،
مؤسسين إدعاءهم انطلاقاً من ذلك على نظرية القرينة الظاهرة القابلة لإثبات
العكس ، أي أن مسؤولية تاريخت ثابتة ظاهرياً بسبب إهمالها وخرقها لقانون
مينسوتا مما ينهض بمسؤوليتها عن عملية القرصنة ويلقي عليها عبئ الإثبات
لنفي الأخطاء المزعومة .

وكانت قد دفعت تاريخت بالمقابل بعدم جواز اعتماد المدعين على مبدأ
القرينة الظاهرية دون إثبات الإهمال بالفعل ، معتبرين أنه لا يجوز تفعيل هذا
المبدأ في هذه القضية ، وسبب ذلك أن الضرر الذي أصاب المدعين كان
خطر مستقبلي أي محتمل الوقوع ، على اعتبار أن مجرد وصول القرصنة
للمعلومات لم يترتب أي ضرر وإنما هو مجرد خطر مستقبلي محتمل أن يلحق
ضرر بالغير فيما لو استخدم القرصنة بالفعل هذه المعلومات ، وأن المسؤولية
الحقيقية تترتب على البنوك المودع لديها هذه الحسابات ، ووفقاً لوجهة نظر
تاريخت فإن الضرر لم ينشأ من الحصول على المعلومات إنما من إمكانية
استخدام تلك المعلومات في استهداف حسابات العملاء لدى البنوك التي لم تقم
بواجبها في حفظ حسابات عملائها .

وقد ناقشت المحكمة هذه المسألة بقولها " ان المدعين لايمكنهم الاعتماد
على القرينة الظاهرة قبل إثباتهم لواجب العناية وإهمال تاريخت لهذا الواجب ،
وإثبات خرقهم لقواعد أمن المعلومات وأن هذا الخرق والإهمال أدى إلى
حدوث الاختراق "

وهذا ما يشكل جوهر مبدأ النظرية الحديثة في المسؤولية عن عمليات القرصنة حيث أن المحكمة لم تقبل من المدعين تمسكهم بالقرينة الظاهرة بل أوجبت عليهم السعي لإثبات واجب العناية المفروض على تاريخيت ابتداءً ومن ثم إثبات إهمال أو خطأ تاريخيت لهذا الواجب وأن هذا الخطأ أو الإهمال هو السبب في وقوع الضرر ، وهنا يتجلى لنا المبدأ الذي تقوم عليه النظرية الحديثة والتي يرفض مؤيدوها ترتيب أي نوع من أنواع المسؤولية دون خطأ فعلي ودون علاقة سببية بين الخطأ والضرر الواقع ، ويبدو أن المحكمة في هذا الصدد كانت تمارس مبدأ العلاقة السببية بين الخطأ والضرر ، وأن العديد من دفوع تاريخيت اتجهت إلى أن " الخطر الذي يمكن أن يقع في المستقبل " لا يمكن إثباته عن طريق قاعدة القرينة الظاهرة و إنما لابد من إثباته بالفعل من خلال حيثيات القضية .

وكان المدعون قد طالبوا بترتيب المسؤولية على تاريخيت بسبب إهمالها لحفظ البيانات ، وخرقها لقانون مينسوتا الخاص بالبطاقات البلاستيكية التابعة للمؤسسات المالية ، وعدم اعتمادها لنظام تجزئة أقسامها بشكل ينسجم وطبيعة البيانات الخطيرة التي يتوجب إبلاؤها الحماية المطلوبة .

لكن المحكمة قالت في مناقشتها لجهة الإهمال :

" هناك فرق جوهري بين الضرر المحتمل وقوعه مستقبلاً في حالة هذه القضية والذي تعتمد تاريخيت في الخطر المحتمل الوقوع مستقبلاً ، أنه مجرد احتمالية تولد خطر عن الوصول للبيانات المالية ، وبين الأضرار التي أصابت المدعين بالفعل في هذه الدعوى والتي تدفع تاريخيت بأنه لم يحدث

أي ضرر من جراء الوصول إلى هذه المعلومات كون البنوك التي أصدرت تلك البطاقات قد أوقفتها جميعها فور علمها بالحادثة " ولكن ناقشت المحكمة في أن " هذه الحالة ليست أخطار مستقبلية وإنما هذه مسؤولية نتجت وقت عملية الاختراق الأولى ونتيجة للاختراق الذي استهدف شبكة تارغيت "

وفيما يتعلق بخرق قانون مينسوتا جاء في قرار المحكمة أنه وفقا لقانون مينسوتا لحماية البطاقات الالكترونية :

لايجوز لأي شخص أو كيان - شخص اعتباري - يقدم خدمات بواسطة التسديد الالكتروني أن يحتفظ بأيّة معلومات سرية مثل PIN أو أية معلومات أخرى بعد ٤٨ ساعة على الأكثر من إتمام العملية وكذلك نص هذا القانون عينه:

في حالات الهجمات الالكترونية على أنظمة الشبكة لشخص ما أو كيان ما خرق هذه الأحكام فإن هذا الشخص أو الكيان لن يكون في منأى عن المسؤولية و عن التعويض للمؤسسات المالية التي أصدرت هذه البطاقات و التي تأثرت من جراء هذا الاختراق ،

ومن حيث النتيجة فإن المحكمة قبلت الدعوى المرفوعة من قبل المدعين ضد تارغيت وقررت بأن شركة تارغيت هي المسؤولة عن التعويض من جراء عملية اختراق نظامها .

- هذا هو المبدأ السائد في أروقة الدراسات القانونية المتعلقة بمسؤولية البنوك ضد الهجمات الالكترونية ، ولكن هذا المبدأ أخذ يتمايل ببطئ في صالح

شركات الاعمال الصغيرة ، لاستثنائها من زمرة الشركات الضخمة أو الشركات ذات التركيبة المعقدة .

ويعود ذلك بسبب تزايد نسبة الهجمات على شركات الأعمال الصغيرة ، ففي النصف الأول من عام ٢٠١٢ ، ارتفع العدد الإجمالي للهجمات التي تستهدف الشركات الصغيرة أو المتوسطة إلى ما يقارب ١٥١ هجمة في اليوم خلال شهر مايو ويونيو ٢٠١٢ ، وفقاً للبيانات الصادرة عن شركة أمن تكنولوجيا المعلومات Symantec Corp.released.

حيث ارتفعت نسبة تلك الهجمات التي تركزت بشكل واضح على شركات الأعمال الصغيرة أو المتوسطة لأكثر من ٣٠٪، مقارنةً مع ١٨٪ في نهاية ديسمبر ٢٠١١ ، وفقاً لنتائج الدراسة الواردة ضمن تقرير أمن المعلومات ضد الهجمات الالكترونية ، والذي عرف - التقرير - بدوره الشركات الصغيرة أو المتوسطة بأنها الشركات التي لايزيد عدد موظفيها عن ٢٥٠ موظف ، وذلك بحكم أن هذا النوع من الشركات ليس لديها من الإمكانيات الكافية لحماية الأنظمة المعلوماتية وتأمينها مما يجعل هذه الشركات هدف سهل للقراصنة .

عدد قليل من تلك الشركات الذي قد يلجأ لإقامة دعاوى قضائية ضد بنوكهم لاستعادة الأموال المسروقة من جراء الهجمات الالكترونية .

ويقول خبراء قانونيون أن العديد من هذه الشركات تفضل تسوية الأوضاع مع بنوكهم مقابل تعويض اتفاقي جزئي أو حتى مع قبولهم لتحملهم بعض الخسائر عوضاً عن لفت الانتباه إلى تعرضهم للاختراق في مسألة تتعلق بأمن

المعلومات الأمر الذي قد يضر بسمعتها التجارية ، وهناك ما هو أكثر من ذلك ، حيث أن تكاليف التقاضي قد تكون مكلفة وباهظة خاصة بالنسبة للشركات الصغيرة ، لأنها عادةً لا تملك العلاقات الكافية للحصول على خصومات لأجور المحامين المختصين في هذا النوع من الدعاوى .

وأن العديد من المحامين كانوا يقدمون النصائح لأصحاب تلك الشركات بعدم محاولة ملاحقة البنوك للمطالبة باسترجاع أموالهم المسروقة بسبب عمليات القرصنة ، ويقول خبراء أمن المعلومات في هذا المجال أن البنوك التي تتخذ خطوات "معقولة تجارياً" لحمايتها من الهجمات الالكترونية في المعاملات التجارية لا يمكن أن تكون مسؤولة شرط حسن النية -good faith- عن الأموال المسروقة من قبل قراصنة ، وعادةً ما يتم وضع تلك الشروط في العقود المبرمة بين البنوك وعملائها .

- وقد كتب السيد بيكر في هذا المجال وهو باحث قانوني في مجال أمن المعلومات في تحليله لأحد أحكام المحاكم في هذا الشأن " الشركات الصغيرة لا يمكن لها أن تجعل حساباتها في منأى عن خطر الهجمات الالكترونية ، لذلك فهم بحاجة للمساعدة من البنوك ، التي لديها وضوح أكبر في أنماط الاحتيال " و يتابع قوله "الحقيقة هي أن هناك الملايين من الشركات الصغيرة التي ليس لديها أدنى فكرة عن تطور التهديد الالكتروني الذي قد يصيبها يوماً ما " .

ويبدو أن هذه العوامل والدراسات آتت ثمراتها في مجال مسؤولية البنوك ضد الهجمات الالكترونية ، حيث باتت المحاكم تتجه اتجاه آخر ينسجم

والمنطق القانوني في تفسيراته ، ويحاكي مبادئ العدالة بشكل أكبر مما كان عليه في أي وقت مضى .

حيث باتت المحاكم تعتمد في قضائها على نظرية سلوك الرجل العقلاني وفي تفعيل مبدأ حسن النية ، وبالتالي فإن دراسة القضايا ستكون في الوقوف على كيفية تفسير هذا المبدأ في كل قضية على حده وفي مقارنته مع مبدأ حسن النية وفي تفسير مدى التزامات البنوك بالضمانات التي تتعهد بتقديمها للعملاء أثناء التعاقد .

حيث قضت محكمة استئناف بوسطن الدائرة الأولى ذات القضية التي استعرضناها بداية وهي قضية شركة المقاولات باتكو وبك المحيط

Ocean Bank vs Patco Construction Company Inc^{٧٢}

بأن bank ocean لم يحم بالحماية اللازمة لحسابات عملائه ولم يكن لديه أساليب الحماية الملائمة والكافية للسرقة التي استهدفت شركة المقاولات باتكو ، وقال رئيس المحكمة القاضي Sandra Lynch ، الذي ناقش حكم الدائرة الأولى ، في هذه القضية ، بأن محكمة الدائرة الأولى "لم تفسر مبدأ الرجل

^{٧٢} "Three Recent Cases Against Banks And The ، Aegis Journal . ٢٠١٦ .

Liability For Losses Suffered By Their Client From Hacking And Phishing. .

<http://www.aegisjournal.com/book-and-product-reviews-%E2%80%93-three-recent-cases-against-banks-and-the-liability-for-losses-suffered-by-their-client-from-hacking-and-phishing/>

٢٠١٦ راجع الموقع الالكتروني

العقلاني ومبدأ حسن النية بشكل سليم وأن هذه المحكمة اعتمدت - مقاس
وأحد يناسب الجميع- " وهو أن النهج الذي كان يتبعه نظام البنك لأمن
العملاء فشل في حماية حساب شركة المقاولات ودليل ذلك أن البنك كان قد
قبل عمليات الحوالات على مدى خمسة أيام في شهر مايو ٢٠٠٩ وبمجرد
اكتشافه الاحتيال ، استطاع البنك أن يتراجع عن تحويل ٢٤٠٠٠٠ \$ أي
أنه عندما قام بالتدقيق في عمليات التحويل استطاع أن يكشف عملية
القرصنة " ، وبالتالي فإن عملية القرصنة لم يكن من الصعب كشفها لو قام
موظفي البنك بواجبهم على أتم وجه في وقت أقرب ولكانت الخسائر أقل أو
لربما انعدمت ، وكان بوسعهم كبح عملية القرصنة والتصدي بشكل تام منذ
البداية"

وأن شركة Patco أقامت دعواها القضائية ضد بنك المحيط لاسترداد بقية
رصيد الحساب "

رفض محامي بنك المحيط التعليق حيث أن العديد من البنوك الصغيرة
والإقليمية حريصون على بناء قاعدة عملاء صغيرة من أجل المنافسة بشكل
أفضل مع البنوك الكبرى ، التي اكتسبت حصة في السوق على مدى العقد
الماضي.

بعد أن كان قد جادل بنك المحيط سابقاً في وثائق المحكمة بأن أمنها في ذلك
الوقت كان أعلى من المتوسط وأنه كان يمكن للشركة أن تُفشل عملية القرصنة
منذ بدايتها فيما لو كانت تقوم بتدقيق حساباتها يوميا

وكان ما يقدر ب ١٣٠٠ إلى ١٥٠٠ من البنوك الأخرى تستخدم برامج أمان مشابهة لتلك التي يستخدمها بنك المحيط في ذلك الوقت، وفقاً لمذكرات قضائية ، مما يجعل بالتالي عناية البنك لمواجهة عمليات القرصنة متبعاً بذلك عناية معقولة تجارياً .

مما شجع العديد من الشركات الصغيرة أو المتوسطة إلى اللجوء إلى القضاء لمواجهة بنوكهم في حوادث الهجمات الالكترونية ،

وقد جاء في حكم المحكمة الاتحادية في قضية

Experi-Metal Inc. vs Comerica Bank^{٧٣}

حيث تقدمت شركة EMI بدعوى قضائية لمواجهة البنك كوميرك في شهر نوفمبر ٢٠٠٩ بعد تحويل احتيالي استهدف حساب الشركة لدى بنك كوميرك والذي يبلغ رصيده ٢ مليون دولار أمريكي عن طريق عملية احتيال عبر هجمات الانترنت في بداية عام ٢٠٠٩

^{٧٣} Robert. ٢٠١٦. "Court Says Comerica Bank Must Pay After 'McMillan

Customer Is Hacked". *Pcworld*.

٢٠١٦ راجع المقالة في <http://www.pcworld.com/article/٢٣٠٣٩٢/article.html>

الموقع الالكتروني

في هذه القضية كانت الشركة لم تقم بأية عملية تحويل من خلال حسابها لمدة تزيد عن عام كامل ، وفجأة في يوم واحد تم تحويل مبلغ \$٩٠٠٠٠ عن طريق عملية قرصنة .

استطاع بنك كوميرك استرجاع معظم التحويلات التي تمت عبر نظامه ولكنه اعتبر بأن الشركة هي المسؤولة عن رصيد الحساب الذي لم يتم استرجاعه ، بعد أن أقامت دعواها ساعية لاستعادة مبلغ \$٥٦٠٠٠ ، وقضت المحكمة الاتحادية في ولاية ميتشغن بأن بنك كوميرك يجب أن يغطي الخسارة للشركة ، ويقول القاضي Patrick J. Duggan " هناك العديد من الاعتبارات المتعلقة في أن البنك تصرف بحسن نية مع هذه الحادثة" وأضاف بأن " البنك تعامل باعتدال مع عميله تحت هذه الظروف وقام بإيقاف وعدم السماح أو التحقق من عملية الاحتيال التي بدأت نشاطها مبكراً " .

وفي هذه القضية ثمة دليل يشير إلى أن البنك كان على معرفة بوجود هجمات الكترونية تستهدف عملاءه ولكن " ما الذي كان بوسع البنك القيام به ولم يقم به " ، وفقاً لما جاء في دفاع محامي البنك الذي سعى لإثبات أن البنك راعى قواعد الحماية بحرفية ودون تقصير وكذلك كان متقيداً بقواعد الحيطة والحذر وفق مبدأ الرجل العقلاني .

وقد قضت المحكمة من حيث النتيجة بأن البنك التجاري كان ينبغي عليه أن يتحقق ويمنع عملية الاحتيال من خلال مراجعة سجل نشاطات حساب الشركة الذي لم تجر ضمنه أية عملية لأكثر من عام ، لا أن يقبل بشكل سلبي عمليات التحويل التي استهدفت الحساب ، وبالتالي خلصت المحكمة إلى أن

بنك كوميرك لا يتعامل بحسن نية مع عملائه عندما يقدم لهم الوعود حول أمن المعلومات ، وجدوى متابعة وتدقيق سجلات الحسابات بشكل مستمر وبالتالي فهو لم يتقيد بالتزاماته العقدية تجاه الشركة صاحبة الحساب والمتعلقة بواجب البنك متابعة الحسابات بشكل دوري.

وفي هذا السياق يضيف Richard B. Tomlinson، وهو المحامي الوكيل عن شركة Experi-Meta في هذه القضية ، بأن هناك اعتراف ضمني من قبل المحكمة بأن أصحاب الأعمال الصغيرة بحاجة إلى المزيد من الحماية كالتي تمنح للأفراد ، في معاملاتهم مع البنوك وخاصة فيما يتعلق بالهجمات الالكترونية .

وقضت محكمة مقاطعة ميتشغن أن البنك كوميرك بنك يتحمل مسؤولية الهجمة الالكترونية التي بلغت \$٥٦٠.٠٠٠ ، وأنه كان يتوجب على البنك أن يبذل عناية أكبر ليحصن ويحمي ملايين الدولارات من عمليات التحويل الاحتمالية بعد أن تعرضت أحد حسابات عملاء هذا البنك للقرصنة قبل عامين ، في ١٣ كانون الأول عندما قررت المحكمة لصالح شركة المعادن اكسبرت في ولاية ميتشغن بموجب الدعوى القضائية المرفوعة بمواجهة بنك كوميرك بعد حادثة يناير ٢٠٠٩ حينما حاول القراصنة القيام بتحويل ملايين الدولارات إلى أوروبا الشرقية قبل قيام أنظمة المصرف بإخفاق عملية القرصنة و أن معظم المبالغ قد تم استرجاعها القاضي دوغان قاضي المحكمة الاتحادية في ولاية ميتشغن قرر في حكمه بأن البنك كان يتوجب عليه بذل جهد أكبر لحماية العملاء وكبح الهجمات الالكترونية المحتملة والمتوقعة ، " البنك تعامل بشكل

معتدل مع عملائه في هذه الظروف وكان يتوجب عليه كشف عملية القرصنة

وإيقافها بشكل مبكر أكثر مما حصل " كما كتب القاضي دوغان في قراره .

كان قد بدأ قلق شركه المعادن اكسبرت في وقت سابق بتاريخ ٢٢ كانون الثاني ٢٠٠٩ عندما تلقى موظف إداري في الشركة رسالة الكترونية من البنك لملى استمارة بيانات خاصة بالبنك للتحويل عبر الانترنت - حيث أن البنك قد تواصل مع العميل من خلال - إعادة توجيه - رسالة الكترونية سبق وأن استلمها من الشركة - لقسم التحكم الذي بدوره قام بتسجيل الدخول من خلال موقع يعود للقراصنة - وهنا نكون أمام حالة man in the middle - والمجرمين كانوا قد بأشروا عملياتهم على مدى ست ساعات ونصف وسارعوا لسرقة معظم رصيد الحساب قبل أن يتم إيقاف منافذ الفرص المفترضة لإتمام العملية .

علم بنك كوميرك بالمشكلة في غضون أربع ساعات من بدء عملية القرصنة عندما تلقى بنك تشيس تقارير حول بعض التحويلات الغير شرعية تدخل حسابه من حساب شركة المعادن وهو بنك أضخم من بنك كوميرك وكان يقوم بعمليات تحويل ضخمة باستمرار لذلك كان يستخدمه القراصنة لضخ الحوالات في حساباته ومن ثم نقلها إلى روسيا و استونيا .

قسم متابعة العمليات الاحتيالية العائد لبنك كوميرك قام على الفور بإيقاف حساب الشركة المعدنية لكنهم ارتكبوا خطأً . بأنهم لم يقوموا بإيقاف عملية الاحتيال من خلال إيقاف session وبالتالي بقي القراصنة في حالة تسجيل دخول وتمكنوا من إتمام ١٥ عملية تحويل قبل أن تتمكن منظومة المخاطر

أخيراً من إفشال الجلسة المفتوحة session حيث بلغت الدفعة الأخيرة التي قام بها القراصنة حوالي \$٥٠٠٠٠

بعد أن رفض بنك كوميرك تغطية خسارة بلغت \$٥٦٠٠٠٠ قامت شركة المعادن بإقامة دعوى قضائية على بنك كوميرك ادعت فيها بأنه كان ينبغي على البنك عدم السماح بإتمام عملية التحويل ودفع البنك بأنه لما كان الحساب المستهدف هو لشركة أعمال فكان يتوجب عليها التدقيق في حساباتها بشكل أكثر دقة وبأنه يتوجب عليها تحمل المسؤولية عن عملية القرصنة

القاضي دوغان أعطى رأياً في بداية القضية لصالح بنك كوميرك عندما قال " البنك تعامل باعتدال مع عميله تحت هذه الظروف وقام بإيقاف وعدم السماح أو التحقق من عملية الاحتيال التي بدأت نشاطها مبكراً " ولكنه لم يحدد بعد مقدار المسؤولية التي يتوجب على البنك التعويض بموجبها ، وسرعان ما بادر إلى توضيح وجه نظره القانونية ووضح بأن البنك قد فشل في محاولته لإخفاق عملية القرصنة وارتكب خطأ عندما أوقف عمليات التحويل دون إيقاف الجلسة المفتوحة وأن خطأه هذا مكّن القراصنة من اتمام ١٥ عملية تحويل نتيجة سهو القائمين في قسم أمن المعلومات التابع للبنك عن إيقاف الجلسة المفتوحة على المخدم .

ومن هنا نجد التفسير العميق الذي انتهجه القاضي دوغان في تفسيره لمسألة حسن النية وتطبيق مبدأ الرجل العقلاني ، وبالتالي ومن دراسة هذا الحكم ، يبدو أن القاضي دوغان كان يتبع ذات المبدأ الذي تقوم عليه النظرية الحديثة من خلال دراسة أدق التفاصيل ضمن الوقائع المسرودة والاستدلال على

الأخطاء من تلك الوقائع وترتيب المسؤولية من حيث النتيجة إلى جانب الطرف المقصر أو المخل في واجباته أو التزاماته .

ومن هنا بدأت اتجاهات المحاكم تتضح بشأن تفعيل مسؤولية البنوك في الهجمات الالكترونية ، وتتسجم ومبادئ القانون وفق أسس واضحة ، وسليمة قانوناً ، وأضحت البنوك لا تشعر بالاطمئنان بالاعتماد على عقودها لحمايتهم من المسؤولية من خلال تضمينها بنود ترفع عنها المسؤولية فيما يتعلق بأخطار الهجمات الالكترونية ، بل يتوجب عليها بالفعل السعي بشكل حثيث لحماية حسابات عملائها حفاظاً من الهجمات الالكترونية ، كونها لن تكون بمنأى عن تحمل المسؤولية ولو ضمننت عقودها بنوداً تحميها من المسؤولية مالم تقترن هذه البنود مع حسن النية و عناية الرجل العقلاني ، حيث أنه يتضح من القضية السابقة بأن القاضي ذهب إلى تفسير معيار الرجل العقلاني بالنسبة للبنوك آخذاً بعين الاعتبار مهنية وحرفية الصيرافة في ممارسة نشاطاتهم المصرفية .

وبانت المحاكم تتجه اتجاه واحد بهذا الصدد وتعتمد النهج الذي يشدد مسؤولية البنوك عندما يكون المضرور أصحاب حسابات فردية أو شركات أعمال صغيرة وبين الشركات أو المؤسسات المالية الضخمة التي تعتمد نظام فني وإداري واحترافي لا يقل في أهميته عن أنظمة البنوك الإدارية ، حيث جاء في مناقشة قضية في عام ٢٠١٠

Village View Escrow Inc. vs. Professional Business Bank^{٧٤}

في هذه القضية تقدمت شركة VVEI بادعاء بمواجهة Professional Business Bank في شهر يوليو ٢٠١٠ تطالب فيه بتعويضها عن سرقة حسابها الذي بلغت خسارت \$٤٦٥٠٠٠ بعد الوصول إلى حساباتها إثر عملية قرصنة استهدفت حساباتها لدى البنك المدعى عليه و سعت الشركة في ادعائها لإلقاء المسؤولية على البنك عن كامل الخسارة التي استهدفت حساباتها .

وتبدو أهمية هذه القضية في مناقشتها لمسألة عناية الرجل العقلاني لتطبيق معايير التوجيه العامة .

حيث أسست الشركة ادعاءها من خلال إثباتها بأن البنك فشل في اتخاذ التدابير اللازمة وكذلك في اتخاذ الإجراءات الكافية لحماية الحسابات من الهجمات الالكترونية وأنها تجاهلت التحذيرات والانذارات بشأن تهديدات خطر الهجمات الالكترونية .

والنتيجة التي خلصت إليها المحكمة في حكمها أن عناية الرجل العقلاني قد لا تكون كافية بالنسبة للبنوك إذا كانت تقدم خدماتها عبر الانترنت ، مالم تتلائم مع الأنفاق الكافي - لا القليل - للمال والجهد لمواجهة الهجمات الالكترونية ، وأن البنوك التي لاتتخذ الخطوات اللازمة والجهد الكافي لحماية حساباتها فإنها في هذه الحالة تكون " تغازل الكارثة - courting

^{٧٤} <http://www.aegisjournal.com> ٢٠١٦ راجع الموقع الالكتروني

disaster – إذا ما أنفقت القليل من الجهد والمال لمواجهة أخطار الهجمات

الإلكترونية " وفقاً لما جاء بقرار المحكمة

ويبدو بأن حكم قضية شركة المعادن ضد بنك كوميرك يوضح الأساس القانوني الذي تنتهجه المحاكم في هذه القضايا فقد ناقش وقائع القضية كاملة وألم بكافة ملامحها حيث راعى في حكمه أدق التفاصيل مع التزامه بقواعد الإثبات في المسؤولية ، وبالتالي فإن البنوك بشكل طبيعي ستكون مسؤولة عن التعويض ضد القرصنة للحسابات الشخصية ، لكن ذلك يلقي بعبء الإثبات على المدعي لإثبات أن البنك لم يحمي الكافية لأموال المودعين ، أي أنه لا مجال للمطالبة بالتعويض تبعاً لنظرية تحمل المخاطر ، وإنما على المدعي أن يثبت أولاً واجب العناية من قبل البنوك ومن ثم يثبت إخلال البنوك بتلك الواجبات .

ثمة اعتراف ضمني ساد أروقة المحاكم بأن أصحاب الأعمال الصغيرة أو الشركات الصغيرة غالباً ما تفتقر للفهم الكافي أو الدراية في مسائل الاختراق خاصةً عندما يقومون بفتح الحسابات لدى البنوك ويقبلون شروط العقد المكتوب من قبل البنك دون مناقشتها أو الاطلاع عليها وخاصةً البنود المتعلقة بموضوع إجراءات أمن المعلومات وفقاً لما يقوله محامو هذه الشركات في نزاعاتهم القضائية المنظورة .

إن قرار محكمة ميتشغن كان غاية في الأهمية لأن المحاكم الاتحادية في تلك الأونة كانت في صدد الإجماع على مبدأ قانوني سليم في هذه القضايا ، ويعتقد خبراء أمنيون في مجال أمن المعلومات بأن القرصنة المحتالون

استطاعوا جمع مبالغ تقدر بمئات آلاف الدولارات خلال السنين القليلة الماضية ، وعادة يستهدفون حسابات الشركات الصغيرة أو المنظمات الاجتماعية التي تتعامل مع بنوك محلية غير ضخمة ، والقراصنة يسرقون الأموال عبر الانترنت المتاح لإجراء بعض العمليات المصرفية معتمدين في ذلك على بعض الموظفين العاملين لدى أصحاب الحسابات .

ثالثاً : تحديد مسؤولية البنوك جراء عمليات القرصنة والإعفاء منها

لما كانت مسألة الهجمات الالكترونية تشكل مصدر قلق لا يستهان به من جانب البنوك والمؤسسات المالية المعنية بإصدار بطاقات الائتمان أو بطاقات الدفع الالكتروني ، مما يجعل المصارف تبحث بجهد حثيث عن السبل التي تعفيها من المسؤولية إما بإثبات التزامها بقاعدة حسن النية وعناية الرجل العقلاني وبذل الجهد الكافي ومن حيث النتيجة إثبات التزامها بالعادات المصرفية الصحيحة أو عن طريق تضمين عقودها شروط خاصة للإعفاء من المسؤولية قبل تعرضها لحادثة قرصنة^{٧٥} .

١ - تحديد المسؤولية الإعفاء الإتفاقي :

إن كافة البنوك التي تقدم خدمات عبر شبكة الانترنت تقوم بتضمين عقودها المبرمة بنوداً تعفيها من المسؤولية في حال تم الوصول إلى المعلومات السرية بخطأ من العميل ، مع مراعاة القواعد العامة على شروط الإعفاء من مسؤولية البنوك وفقاً لما يلي :

١ - لا يرتب الشرط أثره مالم يثبت البنك قبول العميل لهذا الشرط .

٢ - لا يجوز أن يتضمن الشرط إعفاء البنوك من التزام جوهرى .

^{٧٥} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ١٢١٩

٣- تحديد نطاق شرط الإعفاء ، فعلى سبيل المثال إن الشرط الذي يعفي البنوك من مسؤوليتها عن أخطاء تابعيها لن يشمل الأخطاء الشخصية للبنوك أي الأخطاء الواقعة من ممثليه المعبرين عن إرادة البنك .

٤- لا يصح الإعفاء المطلق من المسؤولية التقصيرية .^{٧٦}

وبالتالي لا يجوز للبنوك التصل من مسؤوليتها الشخصية والتي تصدر عن ممثليهم القانونيين حيث يعتبر المديرون على سبيل المثال في عملهم معبرين عن إرادة البنك تبعاً لتصرفاتهم ضمن الأطر المحددة الظاهرة حيث تبقى هذه الأخطاء مشمولة بأحكام مسؤولية البنوك ولا مجال لتضمينها في شروط الإعفاء ، حتى وإن تجاوز المدراء حدود وظيفتهم شريطة مراعاة الوضع الظاهر بالنسبة للعميل ففي حال كان تجاوز المدير لصلاحياته ظاهر للعميل فلا مجال لترتيب المسؤولية من جانب البنك بينما ستترتب مسؤوليته في حال لم تتضح للعميل الحقيقة بأن المدير تجاوز صلاحياته بالفعل وبقي الوضع الظاهر للعميل أن المدير كان يقوم بعمله ضمن اختصاصه كمدير معبر عن إرادة البنك ، وبذات السياق تعاملت المحاكم في النظر لمسؤولية البنوك عن أخطاء التابعين حيث تترتب المسؤولية بجانب البنوك في كل واقعة يتعامل فيها العميل مع الموظف كموظف تابع للبنك وفقاً لنظرية الحالة الظاهرة ، وسيعفى البنك

^{٧٦} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ١٢١٩ ص

من المسؤولية في كل مرة يتعامل فيها العملاء مع أحد التابعين وفقاً للعلاقة الشخصية التي قد تربط بينهما^{٧٧}.

ومن حيث النتيجة يسأل البنك عن أفعال تابعيه في الحالات التالية :

- ١- متى وقع الفعل الضار من موظف أثناء تأدية وظيفته أو بمناسبتها.
- ٢- متى وقع الفعل الضار خارج حدود الوظيفة ولكن لم يكن العميل عالم بخروج الموظف عن حدود وظيفته
- ٣- حالات إساءة الموظف لاستعمال سلطته دون علم من العميل بذلك
- ٤- متى كان الموظف يتعامل لحسابه الشخصي ولكن لم يكن العميل يقصد التعامل معه على هذا الأساس بل كان ينظر إلى البنك وكان لنظره ما يبرره من الظروف .
- ٥- لايجدي البنك أن تكون اختصاصات موظفيه معلنة على الجمهور مادام الجمهور لم يعلم بالفعل بتوزيع الاختصاص .
- ٦- لاترفع المسؤولية عن البنوك كون سلطات المدراء محددة بنظام البنك طالما أن المدير يتصرف داخل السلطات المعتادة لأمثاله في بنوك مماثلة وفقاً للمألوف^{٧٨}.

^{٧٧} علي جمال الدين عوض - عمليات البنوك من الوجهة القانونية مرجع سابق ص ١٢٢٤

أي أن معيار تفعيل مسؤولية البنك عن أفعال تابعيه تدور في فلك نظرية الحالة الظاهرة فكل فعل ضار يصدر من التابعين وإن كان هذا الفعل مرتبط بعلاقة شخصية بين العمل والتابع فلا مجال لإعفاء البنوك من مسؤوليتها طالما أن ظاهر الحال بالنسبة للعميل أو الجمهور كان يظهر فيه التابع وكأنه يتصرف ضمن حدود إختصاصاته الفعلية أو إختصاصته المألوفة في مجال البنوك وإن كان الموظف قد تجاوز بالفعل حدود إختصاصاته المحددة وفق الأنظمة الداخلية للبنك ، طالما أنه لم يتحقق علم العميل بذلك وكان ظاهر الحال يشير إلى قيام التابع بأفعاله ضمن حدود الاختصاص المألوفة ضمن نشاط البنوك .

إلا أن النظرية الحديثة في مسؤولية البنوك باتت تنظر لشروط إعفاء المسؤولية من زاوية أخرى ، ولم تعد المحاكم تطبق هذا البند بشكل مطلق وإن ثبت قبول العميل لهذا الشرط ، ففي العديد من القضايا اتجهت المحاكم إلى ترتيب المسؤولية على البنوك بالرغم من تضمينها هذه البنود في العقود الموقعة مع العملاء ، مؤسسة حكمها في ذلك على مدى تطبيق مبدأ حسن النية لدى البنك و جدية قيامه بواجبه بحماية حسابات عملائه من الهجمات الالكترونية ، وتتجه المحاكم إلى تعطيل هذا البند في عقود البنوك حتى وإن كانت المعلومات السرية قد سربت بالفعل من قبل موظفي الشركة صاحبة الحساب أو بخطأ من المضرور ذاته ، إذا ثبَّت للمحكمة عدم قيام البنك بواجب العناية

^{٧٨} علي جمال الدين عوض – عمليات البنوك من الوجهة القانونية مرجع سابق ص ١٢٢٧

العقلانية المترافقة ومبدأ حسن النية ، والذي بالنهاية يعود لمحكمة الموضوع
تفسير هذين المبدأين كما جرى في قضية that Ocean Bank vs Patco
Construction Company Inc وكذلك في قضية شركة المعادن ضد بنك
كوميرك .

مع الأخذ بعين الاعتبار مجال البحث في فكرة الإذعان التي تجد مجالاً
لتطبيق أحكامها على بنود الإعفاء بشكل واسع ، ومرد ذلك إلى أن الإذعان
وإن كان لا يمكن تصنيفه كعيب من عيوب الإرادة إلا أنه بالرغم من ذلك يشكل
إكراه متصل بعوامل اقتصادية تجعل الطرف المُذعن في مركز أقوى من
الطرف المُذعن يفرض على من خلاله على المُذعن إما القبول بالتعاقد بجملة
شروطه الموضوعية أو رفض التعاقد ، دون أن يفسح المجال لمناقشة بنود العقد.

ومما تقدم يمكن تحديد النقاط التي تسبغ صفة الإذعان على العقود ، حيث
لابد من خصائص معينة يجب توافرها في العقد لإدراجه تحت زمرة عقود
الإذعان وهي :

١- تعلق العقد بسلعه أو مرافق تعتبر من الضروريات بالنسبة للمستهلكين
أو المنتفعين .

٢- احتكار الموجب لهذه السلعة احتكاراً قانونياً وفعلياً^{٧٩} .

^{٧٩} الاحتكار القانوني هو ما يكون بنص القانون كأن يحصر المشرع شركات توليد الطاقة الكهربائية بالقطاع العام ، أما
الاحتكار الفعلي هو احتكار التجار للسلع أو الخدمات المختلفة - عبد الرزاق السنهوري - الوسيط في شرح القانون المدني

٣- صدور الإيجاب إلى كافة بشروط واحدة وعلى نحو مستمر غير محدد المدة^{٨٠}

ويبدو بأن الخصائص المذكورة قد تجعل من الصعب نوعاً ما تكييف بنود الإعفاء من مسؤولية البنوك تحت أحكام الإذعان ، حيث أنه وإن كان التعاقد مع البنوك بالنسبة للعملاء يشكل ضرورة قسوة كما لو كان العميل أحد الشركات الكبرى التي ألزمها القانون بإيداع حساباتها ضمن البنوك ، إلا أنه لا يمكن اعتبار البنوك محتكرة لنشاطات الصيرفة ، وبالتالي استبعاد فكرة الإذعان عن العقود التي تبرمها المصارف .

إلا أن المشرع السوري انتهج نهجاً أكثر مرونة في تطبيق فكرة الإذعان حيث نصت المادة ١٠١ من القانون المدني :

(القبول في عقود الإذعان يقتصر على مجرد التسليم بشروط مقررة يضعها الموجب ولا يقبل مناقشة فيها.)

أي أن المشرع السوري اشترط لتطبيق فكرة الإذعان فقط وجود شروط مقررة مسبقاً يضعها الموجب ولا يقبل المناقشة فيها ، ويكون على القابل التسليم بالشروط كاملة دون مناقشة أو يرفض العقد ككل ، وإن المشرع السوري قد أصاب بحكمه هذا في اعتبار مجرد عدم قابلية المناقشة لشروط موضوعة مسبقاً هو من قبيل الإذعان ، دون اشتراطه احتكار الموجب للسلعة أو الخدمة

^{٨٠} عبد الرزاق السنهوري - الوسيط في شرح القانون المدني - مرجع سابق ص ٢٤٥

المقدمة فحيث أن نشاطات ومجالات الحياة أضحت تتعدد بشكل كبير ، وما هو غير ضروري لشخص ما قد يكون مهماً جداً بالنسبة لغيره ، أي أن ضرورة حاجات الحياة أصبحت أمراً نسبياً يختلف من شخص لآخر.

وكذلك نصت المادة ١٥٠ من القانون المدني السوري :

(إذا تم العقد بطريق الإذعان، وكان قد تضمن شروطاً تعسفية، جاز للقاضي أن يعدل هذه الشروط أو أن يعفي الطرف المذعن منها، وذلك وفقاً لما تقتضي به العدالة. ويقع باطلاً كل اتفاق على خلاف ذلك.)

ونجد في هذه المادة تطبيقاً لما تتبعه المحاكم في تفسير بنود الإعفاء من مسؤولية البنوك في النظرية الحديثة ، فحيث أن قضاء المحاكم المنتهج النظرية الحديثة لا يطبق بنود الإعفاء من المسؤولية بشكل أصم ، وإنما ينظر إليها ضمن جملة من الالتزامات والواجبات والوقائع وإما أن يقوم بتفعيل أحكام هذه البنود أو يقوم بتعطيلها ، وهو ما ينتهجه المشرع السوري في أحكام الإذعان وفقاً للمادة آنفة الذكر حيث اعتبر مسألة الإذعان من المسائل الموضوعية الخاضعة لقناعة قاضي الموضوع الذي يقدر مدى توافقها مع قواعد العدالة ويقدر نطاقها المفترض على الوقائع فإما أن يعدل تلك الشروط أو أن يعفي منها ، وكذلك سعى المشرع لتحديد سلطة القاضي في تفسير شروط الإذعان مراعيّاً فيها مصلحة الطرف المذعن ، فحيث أنه وفقاً لقواعد العامة التي تجيز للمحاكم تفسير البنود الغير واضحة أو التي بحاجة إلى تفسير بما يتوافق مع

مصلحة المدين ، إلا أن المشرع السوري خرج عن هذه القاعدة ليستثني منها عقود الإذعان في المادة ١٥٢ التي نصت على مايلي :

١. يفسر الشك في مصلحة المدين.

٢. ومع ذلك، لا يجوز أن يكون تفسير العبارات الغامضة في عقود الإذعان ضاراً بمصلحة الطرف المذعن.

وبالتالي أضحي شرط الإعفاء من المسؤولية مجرد واقعة مادية يعود تقديرها لقاضي الموضوع الذي يدقق في الوقائع ويمحص في أدلتها ويقرر تفعيل أحكام بنود الإعفاء من عدمها وفقاً لظروف كل قضية على حده .

مما دفع بالبنوك لاتباع آلية جديدة لتتأى بنفسها عن أحكام المسؤولية بشكل أكثر فاعلية من اعتمادها على بنود الإعفاء التي يتم تضمينها في عقودها المبرمة لعدم جدواها فعلياً في النزاعات القضائية .

٢ - إعفاء مسؤولية البنوك عن طريق توكيل شركات متخصصة في أمن المعلومات :

لما كان الأساس القانوني الذي تستند إليه المحاكم في دفع المسؤولية من جانب البنوك هو مدى مراعاة البنوك لمبدأ حسن النية في التعامل مع العملاء وكذلك بذل عناية الرجل العقلاني being rational المقترنان ببذل الجهد الكافي لحماية حسابات عملائهم ، كما جاء في قضية شركة المعادن ضد بنك كوميرك " عناية الرجل العقلاني قد لا تكون كافية بالنسبة للبنوك اذا كانت تقدم خدماتها عبر الانترنت ، مالم تتلائم مع الأنفاق الكافي - لا القليل - للمال والجهد لمواجهة الهجمات الالكترونية ، وإن البنوك التي لاتتخذ الخطوات اللازمة والجهد الكافي لحماية حساباتها فإنها في هذه الحالة تكون " تغازل الكارثة - courting disaster - إذا ما أنفقت القليل من الجهد والمال لمواجهة أخطار الهجمات الالكترونية " مما يجعل البنوك في قلق مستمر جراء احتمال تعرضها للمسؤولية عن عملية قرصنة ما ، وأن تنتظر باضطراب قناعة المحكمة في مدى تفسيرها لمبدأ عناية الرجل العقلاني ومبدأ حسن النية ومدى تقييم المحكمة لمعيار " الجهد الكافي " ، مما دفعها بها إلى اللجوء إلى وسائل مجدية تجعلها بمنأى عن خطر المسؤولية جراء الهجمات الالكترونية ، فبالتلازم مع التطور المستمر الذي تشهده تكنولوجيا المعلومات والذي يشهد بالمقابل تطور عمليات القرصنة وزيادة مهاراتها تبعاً للنفع المزدوج الذي يقدمه العلم في دراسات التكنولوجيا ، الأمر الذي أصبح معه من الصعوبة بمكان بالنسبة للبنوك التصدي لهذه الجبهات أو حتى اتخاذ التدابير

الوقائية اللازمة لحماية بياناتها المصرفية بشكل ذاتي اعتماداً على موظفيها وفنييها ، كون هذا المجال أضحى من المجالات المعقدة والتي لا يمكن للبنوك الإلمام بها حتى ببذل الكثير من الجهد والمال ، فباتت المؤسسات المالية تلجأ إلى توكيل شركات متخصصة ومرخص لها في مجال أمن المعلومات تتوافر لديها الخبرة المطلوبة والحرفية المناسبة التي تبقّيها على اطلاع بكل ما هو جديد في العالم الافتراضي للتعامل مع هذه التكنولوجيا المعقدة وأخطارها ، وبالتالي فإن البنوك عندما تعقد اتفاقات كهذه مع شركات متخصصة في أمن المعلومات فأصبح بإمكانها أن تثبت للمحكمة قيامها بواجباتها المتعلقة بحماية حسابات عملائها مراعية في ذلك عناية الرجل عقلائي being rational و كذلك إثبات حسن نيتها المطلق بقيامها بتوكيل شركات متخصصة في أمن المعلومات وبالتالي فإن أي عملية اختراق محتملة الوقوع سيكون البنك بمنأى عن المسؤولية فيها بسبب قيامه بتوكيل شركات متخصصة تتمتع بالحرفية العالية بالنسبة لأمن المعلومات .

الخاتمة

مما سبقت دراسته ومن خلال اتجاهات المحاكم وكيفية معالجتها للقضايا المتعلقة في المسؤوليات المترتبة جراء عمليات القرصنة الالكترونية يتضح لنا الأساس القانوني الذي تقوم عليه النظرية الحديثة في مسؤوليات البنوك تجاه عملائها جراء الهجمات الالكترونية ، والتي ترفض مبدأ المسؤولية المفترضة أو مبدأ مسؤولية تحمل المخاطر في تطبيقاتها على الواقع العملي ، وتفسح المجال أمام مبدأ ترتيب المسؤولية بجانب الخطأ الفعلي ، وبالتالي لن يكون البنك مسؤولاً مالم يتم إثبات واجباته ابتداءً ومن ثم إثبات الإخلال بها أو النكول في تطبيقها ومن هنا تنتهض المسؤولية من جانب البنك من خلال إخلاله بأحد الواجبات التالية وهي :

١- واجب التعامل بحسن نية مع العملاء وفي الهجمات الالكترونية :
وأساس هذا الواجب هو الوعد الذي يطلقه البنك للعملاء عند استلام ودائعهم ويتمثل بتعهده بمتابعه حساباتهم بشكل مستمر والقيام بكافة واجباته كمصرفي بكل حرفية ومهنية ، وبالتالي فإن إخلال البنوك بوعودها هذه تنفي عنها حسن النية مما يستوجب ترتيب المسؤولية من جانبها .

٢- التزام البنوك بالتعامل مع الهجمات الالكترونية ببذل عناية الرجل العقلاني ، ويبدو أن معيار الرجل العقلاني هو معيار موضوعي يرجع

لتقدير قاضي الموضوع الذي يقوم بتطبيقه تبعاً للوقائع المسرودة أمامه في القضية فتارة يتشدد في تطبيق أحكامه وتارة يتراخى في تحديد مدى الالتزام بقواعده وفقاً لمعطيات القضايا وما يناسبها ، ونستشف من مفهوم الرجل العقلاني (هو الرجل الذي يملك أرضية جيدة تخوله اكتشاف المخاطر التي قد تنتج عن الأنظمة التي يتعامل بها وكيفية معالجتها).

٣- تلازم حسن النية لدى البنوك والتزامها قواعد عناية الرجل العقلاني مع الجهد الكافي في حال تعرض البنوك للقرصنة أو قبل تعرضها ، فثمه واجب مهني على البنوك يفرض عليها في الواقع الحالي ومراعاة للتطور الذي تشهده التكنولوجيا أن تقوم بكل ما هو ممكن من أجل حماية حسابات عملائها بعيداً عن أخطار الهجمات الالكترونية وأن تتفق المال والجهد الكافي سواء لجهة تدريب الموظفين وإخضاعهم لدورات تدريبية باستمرار لتطوير مهاراتهم في التعامل مع أخطار الهجمات الالكترونية أو لجهة التطوير المستمر لكافة التجهيزات والبرمجيات والأنظمة المعلوماتية لتواكب التطور الآني الذي يشهده العالم الافتراضي بشكلٍ منقطع النظير .

وفي ختام هذا البحث وبعد الدراسة التفصيلية لمسألة الهجمات عن طريق القرصنة الالكترونية التي تستهدف المؤسسات المالية خلال ممارستها لنشاطها التجاري عبر شبكة الانترنت وتوضيح مبدأ المسؤولية المدنية للمصارف تجاه عملائها في عمليات القرصنة ، فمن الأهمية بمكان وبعد التعرض للمشكلات العديدة التي نوقشت في هذا البحث فكان لابد من تحديد

النتائج التي خلصنا إليها في من حيث النتيجة ، ومن ثم عرض التوصيات المناسبة التي من شأنها تذليل تلك العقبات التي تعترض أمن الشبكات والمعلومات ، والمقترح مراعاتها في مجال القرصنة الالكترونية في سبيل الوصول للقيمة المبتغاة من هذا البحث :

أولاً النتائج :

تتجلى نتائج البحث في عرض المشكلات الأساسية ذات التأثير الأكبر في نظرية المسؤولية جراء القرصنة الالكترونية سواء من الناحية القانونية أو الفنية أو الاجتماعية في القضايا المعروضة في هذا السياق :

١- **فمن الناحية القانونية :** عدم وضوح التشريعات القانونية وعدم إحكام النصوص القانونية الموضوعية وتعطش الدراسات القانونية من الناحية الفقهية لنظريات واضحة تحدد التكييفات القانونية المطلوبة لتمكين الوصول إلى مبدأ المسؤولية في مجالات الهجمات الالكترونية ، إضافةً إلى عدم وجود طاقم قضائي ملم بالأمور الفنية المتعلقة بطبيعة عمليات القرصنة ، والتي تستوجب من القاضي الناظر في هذه النزاعات الدراية الكافية التي تمكنه من التعامل مع حيثيات هذه القضايا.

٢- **من الناحية التقنية .** إن اتسام بيئة تكنولوجيا المعلومات بخصائص معينة سواء لجهة افتقارها للخصوصية وبالتالي تعتبر البيانات

الشخصية (كأرقام الحسابات المصرفية أو أرقام بطاقات الائتمان وغيرها العديد من البيانات الشخصية) متاحة للكافة بغاية البساطة ، أو لجهة سهولة الوصول للبيانات الحساسة المخزنة ضمن أنظمة المؤسسات المالية التي تستخدم شبكة الانترنت ، كل ذلك يجعل من السهل على العديد من الأفراد القيام بهذا النوع من الهجمات ، ما يوسع مخاطر التجارة الالكترونية .

٣- أما من الناحية الاجتماعية (مستخدمي شبكة الانترنت) وأهم صورها عدم إدراك الأفراد للمخاطر المحيطة بهم من جراء استخدامهم لشبكة الانترنت ، فقيام الأفراد أو الشركات ذات الأعمال المتوسطة أو الصغيرة ، وكذلك الأشخاص الاعتبارية الغير تجارية التي تستخدم شبكة الانترنت في نشاطها دون تمتعها بالوعي الكافي لإدراك مدى مخاطر شبكة الانترنت يسهم بشكل كبير في تعرض أصحاب هذه الحسابات لخطر الهجمات الالكترونية ويجعل منهم لقمة سائغة للقراصنة المحتالين عبر الانترنت ، من خلال إهمالهم أو قلة احترازهم أثناء استخدام شبكة الانترنت ، كعدم استخدامهم لبرامج حماية فعالة ، وكذلك تصفحهم للعديد من المواقع دون الحرص من جانبهم لتجنب تسلل بعض البرامج الخبيثة إلى حواسيبهم الشخصية ، أو عدم تأمين حساباتهم الشخصية على مواقع الانترنت بشكل فعال .

ثانياً التوصيات :

١- رفع مستوى الوعي الفردي لمستخدمي شبكة الانترنت :

عندما يتمتع مستخدم شبكة الانترنت بدرجة عالية من الوعي ويدرك تماماً مخاطر استخدامه لشبكة الانترنت و يعلم كيفية الحفاظ على معلوماته الشخصية والسرية ، فإن ذلك يسهم وبشكل كبير في الحد من مخاطر جرائم نظم المعلومات لابل يقطع دابر تلك الجرائم من جذوره ، وبالتالي فإن توشي الحذر من جانب مستخدم الانترنت سيقص بالضرورة نتائج محاولة الهجوم على الأقل إن لم يمنعها على الإطلاق ، لذلك فمن الضرورة إيجاد أسلوب فعال يسهم في رفع درجة الوعي لدى الأفراد في مجالات الاستخدام الآمن لشبكة الانترنت ، عن طريق إدخال أمن الشبكات والتصفح الآمن عبر الانترنت في المناهج التعليمية الأكاديمية و المهنية ، وإخضاع موظفي الأشخاص الاعتبارية الذين يستخدمون شبكة الانترنت في عملهم لدورات رفع مهارات الاستخدام الآمن لشبكة الانترنت ، وكذلك إيجاد أسلوب يلزم الأفراد أو الزبائن الذين يودون الحصول على خدمات الدفع عبر شبكة الانترنت بتوشي الحذر واتباع تعليمات أمان عامة تقيهم من مصيدة القرصنة .

٢- اتخاذ التدابير المناسبة من جانب المؤسسات المالية التي تستخدم شبكة الانترنت :

من خلال إلزام تلك المؤسسات التي تمارس نشاطها التجاري وتقدم خدماتها لزبائنهم عبر شبكة الانترنت برفع مستوى الأمان لدى برامجها

ومخدماتها إما عن طريق تخصيص قسم يُعنى بأمن المعلومات ، أو عن طريق توكيل إحدى الشركات المختصة بأمن المعلومات ، ما يشكل الكفاءة والحرفية المطلوبة للحفاظ على البيانات المعرضة للاختراق والتشويه ، وبالتالي يسهم ذلك من حيث النتيجة في الحفاظ على مصالح الشركات وحماية زبائنها من خطر هجمات القرصنة الالكترونية .

٣- ترسيخ المبادئ والنظريات والتشريعات القانونية التي تتناسب مع طبيعة التجارة الالكترونية وتراعي خصوصيتها :

لعل من أهم المسائل التي توضحت لنا من هذه الدراسة هي ضعف التشريعات القانونية واضمحلال الدراسات الفقهية في هذا المجال ، ولاشك بأن مرد ذلك كما يبدو للوهلة الأولى - حادثة التجارة الالكترونية - لكن في الواقع أن العائق الرئيس في ضعف التشريعات القانونية المتعلقة بهذا الشأن يرجع إلى سرعة التطور الذي يعد من أهم ماتتسم به ثورة التكنولوجيا ، فحيث أنه في كل يوم تشهد بيئة التكنولوجيا تطوراً جديداً بشكل فعلي ، فمن الصعوبة بمكان على الفقهاء القانونيين كما على المشرعين ، مواكبة تلك التطورات بالتزامن مع سن التشريعات المناسبة لها ، وخروجاً عن الفكرة التي تقول بأن "القانون كالمسافر يجب أن يكون مستعداً للغد ويجب أن يحمل بذرة التطور في ذاته" فإن هذا المبدأ غير قابل للتطبيق على جرائم نظم المعلومات التي تحمل في كل يوم جديد وذلك بسبب التناسب الطردي

بين تطوير نظم المعلومات و تطور طرق اختراقها ، ما يعني بأن التشريعات المتعلقة بهذا المجال يجب أن تتسم بالمرونة المطلقة دون أي تقييد لأحكامها ، أي يجب أن تقتصر تلك القوانين على أطر عامة وعناوين رئيسة مطلقة وواضحة تترك للسلطة القضائية المختصة سلطة تقديرية واسعة تمكنها من مناقشة الوقائع وتكييفها وفقاً لكل واقعة على حده ، وتكون بيئة خصبة للدراسات القانونية الفقهية باستمرار ، وبالتالي فإن ذلك يتطلب جهات قضائية مختصة ومتمرسه وخيرة في الجانب الفني لبيئة التكنولوجيا ومخاطرها ، فبالرغم من أنه لايجوز للقاضي الحكم بعلمه الشخصي في المسائل الفنية إلا أنه لكي يتمكن من الوصول إلى الرأي السديد فلا بد له في هذا النوع من القضايا أن يكون على دراية واطلاع تام في كل ما يتعلق بهذا المجال ، ليتمكن من ملاحظة الوقائع المؤثرة في هذه القضايا ومعرفة الاتجاه نحو الوقائع المنتجة في القضية ومناقشتها حيث أن كون القاضي أو المحامي الذي يرافع في مثل هذه القضايا يجب أن يتحلى بالخبرة الواسعة في هذا المجال لكي يتمكن على الأقل من إبراز النقاط الحيوية ولفت نظر المحكمة للتفاصيل الدقيقة حيث يجب تحليلها وإجراء الخبرة عليها وبالتالي إظهار الحقيقة وتحديد المراكز القانونية الصحيحة ومن حيث النتيجة ترتيب المسؤولية إلى الجانب المسؤول الفعلي وإمكانية تعويض الفريق المتضرر ، وعلى سبيل المثال فدائرة الشؤون القانونية لمؤسسة مالية ما ، لن تستطيع أن تحقق الهدف الأمثل لوظيفتها فيما يخص الهجمات الالكترونية ما لم يكن طاقهما ملم إماماً واسعاً

بتفاصيل عالم الأرقام والمعلومات لتتمكن من تقديم المشورات وتجنب
الهدفات وتصويب سير المؤسسة من الناحية القانونية .

* * *

تم بعون الله تعالى

قائمة المراجع باللغة العربية

الكتب :

- بهاء شاهين :
العولمة والتجارة الالكترونية - الطبعة الأولى - دار الفاروق الحديثة
للطباعة والنشر - القاهرة ٢٠٠٠
- حسن ظاهر داود :
جرائم نظم المعلومات - أكاديمية نايف العربية للعلوم الأمنية - الرياض
٢٠٠٠
- دينيس لويد :
فكرة القانون - سلسلة عام المعرفة - مطابع الأنباء - الكويت - ١٩٨١
- طارق طه :
إدارة البنوك والنظم المصرفية ، دار الكتب للطباعة والنشر ، القاهرة
٢٠٠٠
- عبد الرزاق أحمد السنهوري :
الوسيط في شرح القانون المدني - دار النهضة العربية - القاهرة
- علي جمال الدين عوض :
عمليات البنوك من الوجهة القانونية - دراسة للقضاء المصري والمقارن
- محمد سعيد أحمد اسماعيل :
أساليب الحماية القانونية لمعاملات التجارة الالكترونية - دراسة مقارنة -
٢٠٠٩ منشورات الحلبي الحقوقية - دمشق

الأبحاث العملية :

- باسل مصطفى الخطيب :

تاريخ الانترنت - الجامعة الافتراضية السورية قسم الهندسة المعلوماتية

- حسام لطفي :

أبعاد التجارة الالكترونية ، الندوة الوطنية للتجارة الالكترونية ،

٥-٦ - نيسان - القاهرة - ١٩٩٨

- زيدان محمد :

دور البنوك الالكترونية في تطوير التجارة الالكترونية - جامعة حسبية بن

علي بالشلف - الجزائر

- طارق عبد العال حماد :

تطبيقات التكنولوجيا في المصارف ، أكاديمية السادات للعلوم الإدارية ،

القاهرة ٢٠٠٠

- مصطفى محمد نجم :

أمن الشبكات - network security - كلية الهندسة المعلوماتية جامعة

دمشق - ٢٠٠٩

- التجارة الإلكترونية وواقع العالم العربي ، شؤون خليجية أكاديمية

السادات للعلوم الإدارية ، قسم البحوث - القاهرة ، ١٩٩٩ ديسمبر

المجلات العملية :

- التجارة الإلكترونية النشرة الاقتصادية البنك الأهلي المصري العدد الثالث ، المجلد الثاني والخمسون ، ص ١٩٩٩ ، القاهرة
- دور تكنولوجيا المعلومات في تطوير الخدمات المصرفية - أوراق مصر البحثية - بنك مصر - العدد الرابع - ١٩٩٨
- صالح نصولي و أنديرا شاختر : تحديثات المعاملات المصرفية الالكترونية - مجلة التمويل والتنمية - واشنطن - ٢٠٠٢

* * *

قائمة المراجع باللغة الإنكليزية

الكتب :

- Berman.B ، Marketing channels ، john wiley & Sons Inc، London ، ١٩٩٦ .
- Eric Hobsbawm، *The Age of Revolution: Europe ١٧٨٩–١٨٤٨*، Weidenfeld & Nicolson A Division of Random House، Inc. New York
- The Electromagnetic Telegraph، J. B. Calvert، April ٢٠٠٠.
- Melnichuk، David. ٢٠١٠. *Hacker's Underground Handbook*. Lexington، KY: Createspace.
-
-

الأحكام القضائية :

المقالات :

- Dr. Ljubo Vujovic “Tesla’s Biographt” – New York، ١٠july – الموقع الإلكتروني راجع <http://www.teslasociety.com/biography.htm>

- Siciliano, Robert. ٢٠١١. "٧ Types Of Hacker Motivations – McAfee". *McAfee*. ٢٠١٦ راجع الموقع الالكتروني :<http://blogs.mcafee.com/consumer/family-safety/٧-types-of-hacker-motivations>

-

المواقع الالكترونية :

- <http://www.bbc.com/news/technology-٢٩١٢٥٢٠٤>.
- <http://education.illinois.edu/wp/commercialism/history-of-the-internet>
- <https://en.wikipedia.org>
- <http://www.howtogeek.com/>
- <http://inventors.about.com/library/weekly>
- <http://www.startimes.com/?t=١٤١٤٠٢٩١>
- <https://techterms.com/definition/keylogger>
- Melnichuk, David. ٢٠١٠. *Hacker's Underground Handbook*. Lexington, KY: Createspace.
- *David R. Singh, Teresa Brady and Jane Lee– Data Breach Class Action Defendants Find an Ally in Warrantless Wiretaps – Class Action Monitor – ٢٠١٤*
- ٢٠١٦. the ultimate uplink guide , section ١ the basics <http://guide.modlink.net/section١.php>.
-
- Klooster, John W. ٢٠٠٩. *Icons Of Invention*. Santa Barbara, Calif.: Greenwood Press.

- Church, Alonzo. 1937. "Turing A. M.. On Computable Numbers, With An Application To The Entscheidungs Problem. Proceedings Of The London Mathematical Society, 2 S. Vol. 42 (1936-1937)". *The Journal Of Symbolic Logic* 2 (1): 42-43. doi:10.1017/s.02248112.0.3908X.
- Loring, A. E. 1878. *A Hand-Book Of The Electromagnetic Telegraph*. New York: D. Van Nostrand.
- Singer, Michael. 2010. "Obama To Call For Laws Covering Data Hacking And Student Privacy". *Nytimes.Com*.
http://www.nytimes.com/2010/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0.
- De Bellis, Jack. 1991. "Updike: A Selected Checklist 1974-1990". *MFS Modern Fiction Studies* 37 (1): 129-156. doi:10.1303/mfs.0.9.0.
- <<http://inventors.about.com/library/weekly/aa00298.htm>
- 2016. <http://www.information-age.com/technology/security/123456789/how-to-hack-a-bank--theoretically>.

- Rit, S, M Vila Oliva, S Brousmiche, R Labarbe, D Sarrut, and G C Sharp. 2014. "The Reconstruction Toolkit (RTK), An Open-Source Cone-Beam CT Reconstruction Toolkit Based On The Insight Toolkit (ITK)". *J. Phys.: Conf. Ser.* 489: 012079. doi:10.1088/1742-6596/489/1/012079.
- McMillan, Robert. 2016. "Court Says Comerica Bank Must Pay After Customer Is Hacked". *Pcworld*. <http://www.pcworld.com/article/230392/article.html>.
- 2016. <http://www.howtogeek.com/107460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/> <http://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations>.
- Webcitation.org,. 2016. "Webcite Query Result". <http://www.webcitation.org/1EKr7FUKw>.
- Target Corporation VS Umpqua Bank – Mutual Bank – Village Bank – CSE Federal Credit Union – and First Federal Savings of Lorain. 2016.
- Grok.Isu.edu,. 2016. "Definition: Hackers And Crackers GROK Knowledge Base". <http://grok.isu.edu/Article.aspx?articleId=7203>.
- Aegis Journal,. 2016. "Three Recent Cases Against Banks And The Liability For Losses Suffered By Their Client From Hacking And Phishing".

<http://www.aegisjournal.com/book-and-product-reviews-%E2%80%93three-recent-cases-against-banks-and-the-liability-for-losses-suffered-by-their-client-from-hacking-and-phishing/>.

- PDF generated using the open source mwlib toolkit.

See <http://code.pediapress.com/>

* * *

المفهرس

المقدمة.....	١
مخطط البحث.....	٩
الفصل الأول : نشأة التكنولوجيا وتطور وسائل الاتصال.....	١١
أولاً : ثورة المعلوماتية	١١
ثانياً : تطور برمجة الشبكة العنكبوتية	١٤
ثالثاً : ظهور التجارة الالكترونية	٢٢
الفصل الثاني : التعريف بالقرصنة الالكترونية.....	٣٩
أولاً : افتقار شبكة الانترنت للخصوصية	٤٣
ثانياً : تعريف القرصنة الالكترونية وأنواعها	٤٧
١- تعريف القرصنة الالكترونية	٤٧
٢- تعريف القراصنة	٥٢
٣- أنواع القراصنة	٥٥
٣-١- من حيث سلوك القراصنة	٥٥
٣-٢- من حيث درجة خبرة المقرصن	٥٦
٣-٣- من حيث غاية القرصنة	٥٧
ثالثاً : تحليل خطوات عملية القرصنة	٦١
١- إصابة البنية التقنية التحتية للهدف:	٦١

٢- الخطوة الثانية انتظار ساعة الصفر وفق حساسية البرامج المراد اختراقها	٦٦
٣- الخطوة الثالثة : تبديل نقاط الاتصال - تفادي أثر التتبع	٦٧
٤- الخطوة الرابعة إنهاء عملية القرصنة بالحصول على المال	٦٩
الفصل الثالث : التكيف القانوني لعملية القرصنة الالكترونية.	٧٣
أولاً : التكيف القانوني لعملية القرصنة	٧٦
ثانياً : المسؤولية الجزائية عن عمليات القرصنة	٨٥
ثالثاً : موثوقية التوقيع الالكتروني	٩٧
١- ماهية التوقيع الالكتروني	٩٩
٢- حجية التوقيع الالكتروني	١٠٦
٣- أنظمة التشفير	١١٠
الفصل الرابع : تفعيل مسؤولية المصارف تجاه عملائها جراء الاحتيال عن طريق القرصنة الالكترونية و الإغفاء منها.	١٣٩
أولاً : مسؤولية البنوك في النظرية التقليدية	١٤٢
ثانياً : مسؤولية البنوك في النظريات الحديثة	١٥١
ثالثاً : تحديد مسؤولية البنوك جراء عمليات القرصنة والإغفاء منها	١٨٣
١- تحديد المسؤولية الإغفاء الإتفاقي	١٨٣
٢- إغفاء مسؤولية البنوك عن طريق توكيل شركات متخصصة في أمن المعلومات	١٩١

الخاتمة.....	١٩٣
قائمة المراجع باللغة العربية.....	٢٠١
قائمة المراجع باللغة الانكليزية.....	٢٠٤
المفردات.....	٢٠٩