# ٧

# المتطلبات والمشكلات

يلزم لقيام التجارة الإلكترونية وانتشارها توافر عدد من المتطلبات على مستوى كل دولة على حده، وكذلك على الصعيد الدولى. **فعلى الصعيد الوطنى**، يتطلب الأمر:

١ - بنية متطورة للاتصالات ونظم جيدة لإدارتها، وبخاصة زيادة إمكانات الاتصالات عن بعد ذات النطاق وذات السرعات العالية.

٢ - توافر التسهيلات اللازمة للوصول إلى الإنترنت بتكلفة فى حدود إمكانات النسبة الكبرى من المواطنين، بما فى ذلك اقتناء الحاسبات.

٣ - إقامة بنية وبيئة قانونية أو تشريعية توفر الحماية والثقة والأمان للمتعاملين فى التجارة الإلكترونية، بما فى ذلك حماية المستهلك من الغش ومن التطفل على المعلومات الخاصة به، وحماية حقوق الملكية الفكرية وتنظيم المسائل الخاصة بالضرائب وما إلى ذلك، وتشجيع الشركات العامة والخاصة والأفراد على الدخول فى ثورة المعلومات.

٤ - توافر خدمات مصرفية ملائمة للتعامل عبر الإنترنت، مع كفالة الصفة القانونية للتوقيعات والمستندات الإلكترونية، ومع توفير إجراءات الأمان وتقليل المخاطر للبنوك والعملاء على السواء، وكذلك تأمين الرقابة الفعالة.

٥ - قوة بشرية مؤهلة ومدربة تدريباً جيداً على استعمال تكنولوجيا المعلومات، وعلى صيانة الأجهزة والمواقع، بما فى ذلك تطوير مناهج التعليم لتزويد الطلاب بجرعات أكبر من المعلومات والتدريب فى مجال المعلوماتية وتكنولوجيتها على العموم، وفى مجالات مخصوصة كالتجارة الإلكترونية والحكومة الإلكترونية وما إلى ذلك.

٦ - وعى عام لدى الشركات ولدى الحكومة ولدى الجمهور بأهمية تكنولوجيا المعلومات وما يمكن أن تحققه من منافع.

**وعلى الصعيد الدولي:**

لما كانت التجارة الإلكترونية بطبيعتها لا تتقيد بالحدود الوطنية بين الدول، فإنها ذات طابع عالمى بالضرورة (على ما سبق بيانه فى القسم ٣)، فإن على الدول أن تتعاون فى وضع التشريعات والنظم التى تسمح بنمو التجارة الإلكترونية، مع توفير الحماية والأمان والثقة للمتعاملين عبر الحدود. والتعاون بين الدول فى هذا الشأن سيؤمن درجة معقولة من التنسيق أو منع التضارب، خاصة فيما يتعلق بالمعاملة الضريبية والجمركية والاختصاص القضائى بفض المنازعات وما إلى ذلك.

أما على **مستوى الشركة**، فإن دخول شركة ما فى مجال التجارة الإلكترونية يقتضى توجيه الاهتمام لعدد من القضايا، ومن أهمها (Abolhassani; Al Chen et al):

أ - **اقتناء الأجهزة والبرمجيات اللازمة**، سواء لإنشاء موقع الشركة على خادم خاص بالشركة، أو على خادم مضيف إنترنت. ويتوقف الاختيار هنا على درجة تعقد الموقع الذى تنشئه الشركة. وهذه بدورها ينبغى أن تتحدد فى ضوء الاحتياجات المستقبلية للشركة وخطط توسعها، وألا تتقيد فقط بالاحتياجات الحالية. ويقال فى هذا الشأن أن الاستثمار فى طاقة فائضة ستحتاجها الشركة مستقبلاً أقل تكلفة وعناءً من البدء بطاقة محدودة أولاً ثم محاولة تحديثها وتوسيعها مستقبلاً، خاصة فى المستقبل القريب.

**ب - تصميم وصيانة موقع الشركة على الإنترنت.** وتنبغي ملاحظة أن الموقع يجب أن يكون أكثر من مجرد واجهة إعلانية إلكترونية لنشاط الشركة. بل ينبغي أن يقدم الموقع الخدمات التي يتلقاها العملاء في أي متجر. وعلى ذلك فعلى الموقع أن يكون في آن واحد الكتالوج وموظف المبيعات، ومركز خدمة المستهلك، والخزينة ...الخ. وعلاوة على ذلك يجب أن يكون الموقع متاحاً للدخول فيه على مدار الساعة، وجذاباً، وصديقاً للمستهلك بمعنى أن يسهل التعرف عليه والتجول فيه، وأن يوحي بالثقة لدى المستهلك، وأن يشعره بالأمان بشأن معلوماته الخاصة.

ويجب أن يراعى في تصميم الموقع تقديم مستويات مختلفة للاستخدام، وإتاحة إمكانية الحصول على استجابات فورية (أو سريعة على الأقل) لأسئلة المستخدم، وتوفير إمكانية الحصول على مساعدات فورية، خاصة فيما يتعلق بالاستعلام عن معنى مصطلح معين (مع تجنب استعمال مصطلحات معقدة أو غامضة)، مع تقديم اقتراحات أو نصائح للمستهلك عندما يتردد في الشراء، واستخدام وسائط اتصال متعددة، وحبذا لو توافرت إمكانية التعامل بلغات مختلفة وعملات مختلفة أو وسائط دفع مختلفة، وذلك للاستفادة من خاصية العالمية في التجارة الإلكترونية، وكذلك ينبغي أن يوفر تصميم الموقع للشركة إمكانية تحليل المعلومات المتاحة عن سلوك المستهلكين واتجاهاتهم، حتى تتمكن الشركة من التكيف مع التغيرات في هذا الشأن. وعموما يمكن للشركة الراغبة في إقامة موقع اختيار تصميم للموقع من بين التصميمات المتعددة التي تقدمها شركات الكمبيوتر والإنترنت. كما يمكنها تكليف شخص أو مجموعة أشخاص من ذوي الاختصاص في تصميم المواقع للقيام بهذه المهمة.

ومن المهم بعد إنشاء الموقع أن يخضع لعمليات صيانة مستمرة، أي عمليات مراجعة وتحديث لمحتويات الموقع وطريقة تنظيمه، مع التحسين المستمر في إجراءات الأمان على الموقع. ويجب الانتباه إلى أن صيانة الموقع ليست بالمهمة السهلة، ولا هي بالمهمة قليلة التكلفة. فطبقاً لبعض التقديرات، فإن حوالي ٨٠% من تكاليف مواقع الشركات تذهب إلى عمليات الصيانة، بينما لا تزيد تكلفة الإنشاء على ٢٠%.

**جـ - اختيار اسم للموقع (اسم الدومين) وتسجيله لدى الهيئة المختصة.** ويجب أن يراعى فى اختيار اسم الموقع أن يكون جذاباً، ومثيراً للخيال، ويسهل تذكره، وذلك فضلاً عن أن يكون من السهل ربطه فى ذهن المستخدم بالشركة ومنتجاتها.

وبعد اختيار اسم الموقع، يتعين على الشركة تسجيله لدى شركة الإنترنت المختصة بتسجيل الأسماء والأرقام ICANN (راجع القسم ٢). ويمكن أن تنوب عن الشركة صاحبة الموقع فى القيام بهذه المهمة أى شركة إنترنت، وذلك مقابل أتعاب زهيدة.

د - **تسويق الموقع.** بعد إنشاء الموقع واعتماد الاسم الخاص به، يجب إشهاره والإعلام عن وجوده لدى الناس، وذلك بالإعلان عنه لدى إحدى أدوات البحث مثل Yahoo أو Infoseek وغيرها، وكذلك الإعلان فى الصحف والراديو والتليفزيون، وذلك إضافة إلى إثبات عنوان الموقع على مراسلات الشركة ووسائل النقل الخاصة بها وما إلى ذلك.

أيضاً يجب أن توضح الشركة لزوار الموقع أنه يحظى بإجراءات أمان جادة، وأن أية معلومات خاصة بهم لن يتاح للآخرين الوصول إليها أو تداولها. وفى هذا الشأن أيضاً، يجب أن تتاح لزائر الموقع الفرصة للاستيثاق من أن الموقع الذى يزورونه هو موقع الشركة المعنية فعلاً، وليس موقعا مدسوساً عليها. وتقدم بعض شركات الإنترنت **خدمات الاستيثاق من الموقع**[٦]. حيث تسجل الشركة المعنية موقعها مع شركة من هذا النوع، وتتسلم منها **بطاقة تعريفية رقمية**[٧] تشهد بأن هذا الموقع خاص بالشركة فعلاً. وعلاوة على ذلك، ومن أجل بناء الثقة فى الشركة وموقعها لدى المستهلك، يمكن الحصول على **خاتم الثقة**[٨] من جهة معتمدة وموثوق فيها مثل جمعية المحاسبين العموميين الأمريكية أو معهد المحاسبين حيث أنه إقرار من الجهة المختصة بأن الشركة تتبع إجراءات ونظم رقابة فعالة فيما يتعلق بحماية وتأمين موقعها على الإنترنت.

---

٦ Web site authentication services مثل شركة Verisign

٧ Digital ID

٨ Web trust seal

## المشكلات

من أبرز المشكلات التى تعترض التجارة الإلكترونية، علاوة على المشكلات المعتادة فى التجارة التقليدية، ما يلى:

(١) **المخاطر التى تتعرض لها الشركات صاحبة المواقع على الإنترنت.** تواجه شركات الممارسة للتجارة الإلكترونية مشكلات كتلك التى يواجهها معظم أصحاب المواقع الأخرى على الإنترنت مثل تعرض البيانات للتخريب، والتدخل أو "التشويش" على الموقع، وتحوير أو استبدال البيانات، وإساءة تقديم البيانات والاستخدام الزائف لها، واختراق الحظر على بعض المعلومات أو إنزالها من الموقع بطريقة غير مرخص بها، وهذا فضلاً عن إساءة الاستخدام غير المتعمد نتيجة لأخطاء البشر (Mc Guire & Roser).

(٢) **المخاطر التى يتعرض لها الأفراد عند التعامل مع الشركات "على الخط"**، وأهمها إفشاء المعلومات الخاصة بالعميل مثل ما الذى اشتراه ولمن طلب إرساله ومن سدد الثمن ...الخ، ومثل التعرض للنصب والاحتيال، خاصة بالسطو على المعلومات الخاصة ببطاقات الائتمان، وذلك فضلاً عن الخطأ غير المقصود من جانب العميل عند إدخال بياناته أو تقديم طلبه الشراء إلكترونيا.

وأمثلة النصب والاحتيال كثيرة نذكر بعضها فيما يلى:

**مثال أول:** يستطيع أى محتال بتكاليف قليلة جداً، ومن أى مكان، أن يعرض على الإنترنت صفحة معلومات عن شركته الوهمية تضاهى ما تستطيع عرضه أكبر الشركات. ويستطيع اللصوص أن يوفروا وصلة[٩] بعنوان سوق الأوراق المالية تجعلهم يبدون وكأنهم حاصلون على موافقة السوق على تعاملاتهم ، مما يوقع المتعامل معهم فى الخديعة.

**مثال ثان:** عرضت شركة أصحابها أمريكيون وألمان على المستثمرين عن طريق الإنترنت ما بدا أنه صفقة جيدة. وهى أن يشتروا أسهم فى شركة جديدة سريعة النمو يقدر عائدها ما نسبته ٤٢٠% فى السنة. وجمعت هذه

---

٩ Link

الشركة أكثر من مليون دولار بعد أن ذكرت للمستثمرين أن بنكاً كبيراً يساند عملياتهم، وأن عمليات شركتهم مؤمنة ضد الخسارة. وثبت بعد ذلك أنه لم يكن هناك وجود لمثل هذا البنك الكبير. ولحسن الحظ أمكن ضبط أصحاب هذه الشركة وجرت محاكمتهم، وصدر بحقهم حكم برد الأموال إلى أصحابها.

**مثال ثالث:** قد يعترض محتال سبيل رسالة إلكترونية مرسلة إلى مسئول فى شركة ما، ويغير محتوياتها بإضافة بعض المعلومات الزائفة، ثم يرسل الرسالة المحرفة فوراً إلى ملايين الناس فى محاولة للتلاعب بسعر سهم أو سند مثلاً (وكالة الاعلام الأمريكية).

وبالإضافة إلى ما تقدم، قد يقع المستهلك دون قصد فى خطأ يمكن أن يترتب عليه ضرر كبير. فقد يحدث الخطأ فى طباعة طلب الشراء بكتابة ١٢ وحدة بدلاً من وحدة واحدة تكون هى المطلوبة فعلاً. وقد يضغط المستهلك على خانة "نفذ الطلب" بدلا من الخانة المقصودة وهى "إلغ الطلب".

(٣) **مخاطر عامة لمستخدمى الإنترنت.** ومن أشهرها أن يتدخل طرف ثالث عند اتصالك بأحد مواقع الإنترنت لإرسال معلومات أو لتلقيها، فيخترق الاتصال ويبدأ فى الحصول على بياناتك بطريقة آمنة أو غير آمنة، أى بتعريضها للتلف أو التعديل. ومن الأمثلة الشهيرة أيضاً أن تصلك رسالة بالبريد الإلكترونى متضمنة بعض الصور والوصلات. وعندما تنقر أحد هذه الوصلات ينتقل فوراً إلى حاسبك فيروس ما، ويبدأ هذا الفيروس على الفور فى تدمير ما فى ذاكرة حاسبك من بيانات أو ملفات تشغيل. ومن المعروف كذلك أن الإنترنت حافلة بالمواقع التى تتضمن برمجيات مجانية، ولكنها محملة بالكثير من الفيروسات، أو على الأقل يؤدى تشغيلها إلى مشاكل تعوق تشغيل جهازك. (أبو العطا).

ومن حسن الحظ أن عدداً من أدوات الحماية قد أصبح متوافراً لمستخدمى الإنترنت. وعلى سبيل المثال يتضمن برنامج Windows 98 ومستعرض الإنترنت Internet Explorer (IE5) عدة إجراءات وقواعد لتوفير الحماية والأمان. فعلى سبيل المثال يقدم برنامج IE5 عدداً من برامج الأمان التى يمكن تطبيقها على صفحات

ومواقع الإنترنت. ويقسم البرنامج المواقع إلى مجموعة الدخول عليها محدود كالمواقع داخل الشبكة المحلية[١٠]، ومجموعة الدخول عليها غير محدود كالمواقع الخاصة بالإنترنت عموماً. كما يقسم البرنامج المواقع إلى مواقع موثوقة[١١] وأخرى مقيدة أو محظورة[١٢]، مع إتاحة أربعة مستويات للأمان يختار المستخدم الأنسب منها لكل موقع. كما أن داخل برنامج IE5 عدداً من الأدوات التي يمكن أن تستخدم لحجب صفحات معينة (كالصفحات غير المناسب إطلاع الأطفال عليها)، أى لجعلها غير متاحة إلا لمن يعرف كلمة السر[١٣] أو لحماية المعلومات الشخصية. (أبو العطا).

ويعتبر استعمال البرامج الحمائية ضد المتسللين إلى مواقع الشركات، والبرامج المضادة للفيروسات من أكثر الطرق شيوعاً لتوفير الأمان على الإنترنت. ومن أمثلة الأولى برامج من نوعية Firewalls ومن أمثلة الثانية برامج Norton وMcafee. وتقوم هذه البرامج بوظيفة ضابط الجوازات الذى يفحص مستندات القادمين إلى الدولة، ولا يأذن بالدخول للمشتبه فيهم أو للمحظور دخولهم. كما تقوم هذه البرامج بالتخلص من الفيروسات وإصلاح بعض أنواع الضرر الذى تلحقه بالحاسبات.

ويمكن الإشارة إلى ثلاث وسائل مهمة لتأمين التعامل على الإنترنت وتفادى مخاطر انتهاك الخصوصية والغش والاحتيال والنصب وما إليها (McGuire & Roser):

(١) **أدوات التحقق من شخصية المستخدم**[١٤]. وهى تتمثل أساساً فى استخدام كلمات سر، غالباً باستعمال بطاقات ذكية، أو شهادات رقمية[١٥]. وتحتوى

---

١٠ LAN

١١ Trusted sites

١٢ Restricted sites

١٣ Password

١٤ User ID/ Authentication Control

١٥ Smart Cards/ Digital Certificates

البطاقة الذكية على معالج صغير[١٦] يخزن عليه ما بين ١٠ و ٢٠ مفتاحاً للدلالة على صاحب البطاقة أو أحقيته فى الدخول إلى مواقع معينة. وتستخدم هذه البطاقات حالياً فى توقيع وتشفير[١٧] الوثائق الإلكترونية. فعندما يدخل المستخدم معلومات البطاقة الذكية الخاصة به فى الإنترنت، فإنه يدخل رقماً كودياً، متبوعاً برقم يدل على الهوية الشخصية[١٨]، أو بعبارة تشكل كود المرور[١٩]. ويستخدم خادم الشركة التى يريد المستخدم الاتصال بها هذه المعلومات فى التحقق من شخصية المستخدم والتثبت من أحقيته فى الدخول إلى الموقع. وتؤدى الشهادات الرقمية وظيفة مشابهة لما تؤديه البطاقات الذكية. والشهادة عبارة عن ملف معلومات يتم فيه تعريف شخص أو مؤسسة. ويقوم المستخدم بمراجعة الشهادة للتحقق من شخصية صاحبها قبل الموافقة على استقبال معلومات يقوم بإرسالها. كما يستخدمها فى تشفير المعلومات قبل إرسالها لشخص آخر عبر الإنترنت. وبطبيعة الحال فإن الثقة فى الشهادة لا أساس لها سوى الثقة فى الجهة التى تصدرها (أبو العطا).

(٢) **أدوات الترخيص**[٢٠]. ومن أشهر هذه الأدوات البرامج من نوعية Firewall التى تشبه جهاز الإنذار المنزلى. وهذه الأدوات تشمل على عتاد[٢١] وبرمجيات[٢٢]. وهى توضع بين الشبكة الداخلية للشركة والإنترنت. ومن هذه الأدوات أيضاً ما يعرف بفلاتر دفعات المعلومات[٢٣] التى تحول دون دخول دفعات المعلومات غير المتوافقة مع إجراءات الأمان إلى شبكة الشركة أو موقعها على الإنترنت. وأخيراً، هناك أداة يطلق عليها Socks 5 وهى عبارة عن بروتوكول أى برنامج شبكات يمكن وضعه على خادم الشركة المعنية أو

---

١٦ Micro Processor

١٧ Encryption

١٨ PIN = Personal Identify Number

١٩ Pass Code

٢٠ Authorization Controls

٢١ Hardware

٢٢ Software

٢٣ Packet Filtering

خادم مضيف الإنترنت لمراقبة وتقييد الدخول من جانب الخوادم الأخرى. كما يمكن استخدامه فى تشفير الرسائل المتبادلة بين الخوادم.

(٣) **أدوات ضمان السلامة والسرية.** ويعتبر التشفير الوسيلة الأكثر أهمية فى هذا الشأن، حيث تستخدم رموز أو صيغ رياضية لتحويل الرسائل بحيث لا يستطيع الإطلاع عليها إلا لمن يمكنه فك الشفرة برموز أو مفاتيح معينة. وتعتبر هذه الأدوات ذات أهمية خاصة عند استعمال أرقام بطاقات الائتمان أو المعلومات المصرفية الأخرى على الإنترنت[٢٤]. ويلاحظ أن عنصر الأمان الذى توفره أدوات وبرامج التشفير له تكلفة، ألا وهى زيادة الوقت الذى يستغرقه إرسال البيانات واستقبالها بين موقعين على الإنترنت. ذلك أن كل حرف أو رقم من المعلومات التى يتم إرسالها يجرى تشفيره قبل إرساله، ثم يتم تحريره من الشفرة وتحويله إلى حروف وأرقام مرة أخرى عند استقباله.

وتجدر الإشارة إلى أن تكنولوجيا المعلومات فى تطور مستمر لتحقيق درجات متزايدة من الأمان على الإنترنت. ومع التسليم بأن هذه التكنولوجيات قد لا تكون مضمونة المفعول ١٠٠%، وأنه يمكن لذوى الدهاء الحاسوبى التحايل عليها، إلا أنه لا يمكن التهوين من شأنها. فهى على الأقل تزيد من مصاعب اختراق الشبكات والوصول غير المشروع إلى المعلومات أو تخريب المعلومات والعبث بالأجهزة.

---

[٢٤] استحدث برنامج IE5 محفظة wallet أو حقيبة خاصة لتأمين بيانات بطاقة الائتمان أو البيانات الشخصية الأخرى والحفاظ عليها عند التسوق. حيث يتم تخزين هذه البيانات على القرص الصلب بشفرة خاصة لا يمكن قراءتها، فى مكان يطلق عليه Microsoft Wallet. وعندما تتسوق عبر الإنترنت، يمكن أن تخبر الشركة ببياناتك الشخصية باستخدام المعلومات المسجلة فى المحفظة. وبدلاً من كتابة هذه البيانات، يمكنك أن تختار رمزاً من مربع حوار العناوين (address options) بحيث يتم تمرير هذه البيانات مشفرةً إلى الموقع المطلوب. ويمكن بنفس الأسلوب إرسال بيانات بطاقة الائتمان إذ يمكنك فتح مربع حوارى اسمه (Wallet Payment option) وهذا المربع يعطيك قائمة منسدلة بأنواع بطاقات الائتمان المختلفة، كى تختار نوع البطاقة التى تملكها. ثم تقوم بإضافة بيانات البطاقة. ولا يستطيع أحد أن يطلع على هذه المعلومات إلا إذا كان يعرف كلمة السر التى حددتها أنت. (أبو العطا).

وترمى هذه التكنولوجيات فى مجموعها إلى تقييد التدخلات غير المشروعة عبر الإنترنت، ووقف التدفق غير المقيد أو غير المسيطر عليه للمعلومات عبر الإنترنت.

وفى مسح حديث لهذه التكنولوجيات (The Economist,13 Jan, 2001)، أشير إلى انتشار استخدام الفلاتر أو المرشحات. حيث أمكن تصميم برمجيات يجرى تشغيلها على الحاسبات الشخصية أو على البوابات[٢٥] التى تربط بلداً بآخر على الإنترنت، بحيث يمتنع الوصول إلى مواقع معينة. وكما أشير إلى أن بعض المواقع تستطيع منع بعض المستخدمين من الوصول إليها والدخول فيها، وذلك من خلال التعرف على عنوان مقدم الخدمة على الإنترنت[٢٦] أى الأرقام التى تعرف بها الكمبيوترات الخادمة والتى يمكن عن طريقها الاستدلال على مكان وجود المستخدم. وقد كان الإدراك بوجود مثل هذه التكنولوجيا هو الأساس فى أحد أحكام القضاء الفرنسى ضد شركة yahoo[٢٧]. ومن المعروف أيضاً أن الصين قد غطت نفسها بشبكة (Intranet) معزولة عن باقى عالم الاتصالات المباشرة، وذلك باستخدام برمجيات تمنع الوصول إلى المواقع ذات المحتوى غير المرغوب فيه.

ومن الأمثلة الأخرى على تكنولوجيات التحكم فى تدفق المعلومات عبر الإنترنت، ما بدأت مؤخراً شركة Akamai تقديمه من خدمات يطلق عليها Edge Scape . وهذه الخدمة تمكن مواقع الإنترنت من تحديد أين يوجد الزائر للموقع فى الوقت الذى يقوم فيه بالزيارة، وذلك بفرض التحكم فيما يقدم للزائرين من محتوى معلوماتى حسب مناطق تواجدهم أو حسب البلدان التى يجرون منها اتصالهم.

---

[٢٥] Gateways

[٢٦] ISP's IP address

[٢٧] حكمت إحدى المحاكم الفرنسية فى ٢٠ نوفمبر ٢٠٠٠ ضد شركة yahoo بأن تبحث عن طريقة تمنع إطلاع المستخدمين الفرنسيين على المواد الإعلامية على بعض المواد الإعلامية المتاحة على بعض المواقع الأمريكية والتى تتضمن احتفاءً بالنازية ومحاولة لإحيائها. وفى حالة عدم التزام الشركة بذلك ستتعرض لدفع غرامة قدرها ١٣٠٠٠ دولار يومياً اعتباراً من آخر فبراير ٢٠٠١ (The Economist, 26 May 2001).

بقى أن نشير فى ختام هذا القسم إلى أمرين. **أولهما** أن الحلول التكنولوجية الرامية إلى تأمين المعاملات التجارية الإلكترونية تتضمن حلاً لم نتطرق إليه بعد، وهو النقود الإلكترونية. ونظراً لأهمية هذا الموضوع فسوف نخصص له القسم التالى (الثامن) من هذه الدراسة. **وثانيهما** أن تأمين المعاملات التجارية الإلكترونية بالوسائل التكنولوجية هو جزء من موضوع أشمل، وهو توفير بيئة آمنة لهذه المعاملات. ولا شك أن أحد العوامل الأساسية فى توفير مثل هذه البيئة هو إيجاد إطار قانونى ملائم لطبيعة هذا النوع الجديد من المعاملات التجارية. وهذا هو الموضوع الذى سنتناوله فى القسم التاسع من دراستنا.