اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)

بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا

Distr.
GENERAl

E/ESCWA/ICTD/2009/4
10 March 2009
ORIGINAL: ARABIC

اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)

بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا

10-0272

المحتويات

الصفحة

المحتويات (تابع)

الصفحة

قائمة الأطر

المحتويات (تابع)

الصفحة

قائمة الأشكال

قائمة المصطلحات

أحصنة طروادة	Trojans
إخفاق	Failure
إرتياب	Uncertainty
استجابة	Reaction
استيقان	Authentication
إغفال الهوية	Anonymity
امتدادات بريد الإنترنت الآمنة والمتعددة الأهداف	Secure/Multipurpose Internet Mail Extensions (S/MIME)
الأمن السيبراني	Cyber-security
أمن بروتوكول الإنترنت	Internet Protocol Security (IPSec)
أمن طبقة النقل	Transport Layer Security (TLS)
انتحال	Spoofing
تعادل الخصوصية السلكي	Wired Equivalency Privacy (WEP)
برمجيات التجسس	Spyware
برمجيات الدعاية	Adware
برمجيات خبيثة	Malware
برنامج تحميل أو برنامج تنزيل	Downloader
بروتوكول التحكم بالإرسال/بروتوكول برقية معطيات المستخدم	Transmission Control Protocol/User Datagram Protocol (TCP/UDP)
بروتوكول النقل الآمن للنصوص المترابطة	Secure-HyperText Transfer Protocol (S-HTTP)
بروتوكول بسيط لنقل البريد	Simple Mail Transfer Protocol (SMTP)
بروتوكول نقل النصوص المترابطة	HyperText Transfer Protocol (HTTP)
بروتوكول نقل ملفات	File Transfer Protocol (FTP)
بريد دعائي	Spam
بريد معزز الخصوصية	Privacy-Enhanced Mail (PEM)
بطاقة ائتمان	Credit card
بطاقة لسحب المال	Debit card
بنية أساسية للمفاتيح العمومية	Public Key Infrastructure (PKI)
بوابة أو عبارة	Gateway
تدقيق المجموع	Checksum
تخويل	Authorization
تسجيل الدخول	Keylogger
تسيير	Routing
تشفير	Encryption
تصيد	Phishing
تغذية مستمرة بالتيار الكهربائي	Uninterruptible power supply (UPS)

قائمة المصطلحات (تابع)

تغيير الأثر	Defacement
تفويض	Delegation
تكامل	Integrity
تلبيد	Hashing
توعية	Awareness
ثقة	Trust
جريمة سيبرانية	Cyber-crime
جهة ثالثة موثوقة	Trusted Third Party (TTP)
الحفظ الاحتياطي أو التخزين الاحتياطي أو النسخ الاحتياطي	Backup
حماية البنى الأساسية للمعلومات الحرجة	Critical Information Infrastructure Protection (CIIP)
حوكمة	Governance
خدمات مقدمة من قطاع الأعمال إلى المواطنين	Business to Citizen (B2C) services
خدمة بالصوت التفاعلي	Interactive Voice Response
خصوصية	Privacy
خصوصية حسنة	Pretty Good Privacy (PGP)
خوارزمية التلبيد الآمن	Secure Hash Algorithm (SHA)
الخوارزمية الدولية لتشفير البيانات	International Data Encryption Algorithm (IDEA)
خوارزمية مستخلص الرسالة – النسخة الخامسة	Message Digest Algorithm 5 (MD5)
الدفع عبر الإنترنت	Online payment
دودة	Worm
رخصة إلكترونية	E-permit
رفض الخدمة	Denial of Service (DoS)
رفض الخدمة الموزع أو هجوم موزع	Distributed Denial of Service (DDoS)
رقعة	Patch
رماز	Bits
روبوتات	Bots
روبوتات شبكية	Botnets
سرية	Confidentiality
سلامة البيانات	Data integrity
سلطة مصادقة	Certification Authority (CA)
شبكات افتراضية خصوصية	Virtual Private Networks (VPN)
شبكات عريضة الحزمة	Broadband networks
شفرة ريفيست	Rivest Cipher5 (RC5)

قائمة المصطلحات (تابع)

شهادة رقمية	Digital Certificate
صراف إلكتروني	E-sarraf
صغار المبرمجين	Script kiddies
ضبط النفاذ	Access Control
طابع إلكتروني	E-stamp
طبقة مقبس آمنة	Secure Socket Layer (SSL)
الجيل الثالث من طبقة المقبس الآمنة	SSL 3
عدم الإنكار	Non repudiation
عدم حصانة	Vulnerability
عرض إلكتروني	E-bid
علام	Token
عنوان بروتوكول الإنترنت	Internet Protocol address
فريق الاستجابة لطوارئ الحاسوب	Computer Emergency Response Team (CERT)
فريق الاهتمام الخاص المعني بالاتصالات الرقمية	Special Interest Group on Data Communication (SIGCOMM)
قنبلة منطقية	Logic bomb
مانح الثقة	Trustor
مبحرون فضيون	Silver Surfers
متاحية	Availability
متعدد الأشكال	Polymorphouse
المجلس المعني بأنشطة الإنترنت	Internet Activities Board (IAB)
مجموعة المعايير المعنية بنظم إدارة أمن المعلومات	ISMS Family Of Standards
محطم	Cracker
محطمون طيبون	Sneakers
مخترق للشبكة	Hacker
مخترق ناشط للشبكة	Hacktivisit
مداولة	Transaction
مداولة إلكترونية آمنة	Secure Electronic Transaction (SET)
مربع تحكم	Checkbox
مرشح	Filter
مزود خدمة شهادات المصادقة	Certificate Service Provider (CSP)
مستخلص الرسالة	Message digest
مستعرِض الشبكة	Web browser
مصفوفة متكررة من الأقراص المستقلة	Redundant Array of Independent Disks (RAID)
معايير البروتوكولات الرسمية	Official Protocol standards

قائمة المصطلحات (تابع)

معمم	Pervasive
معيار التشفير المتقدم	Advanced Encryption Standard (AES)
معيار الممارسات السليمة	Standard of Good Practice (SoGP)
معيار تشفير البيانات	Data Encryption Standard
مغلف	Envelop
مفتاح خصوصي	Private key
مفتاح عمومي	Public key
الملاءمة مع الحاجة	Profiling
من الحكومة إلى الحكومة	Government-to-Government (G2G)
من الحكومة إلى المواطن	Government-to-Citizen (G2C)
من الحكومة إلى الموظف	Government-to-Employee (G2E)
من الحكومة إلى قطاعات الأعمال التجارية	Government-to-Business (G2B)
منتدى الفرق المعنية بالأمن والاستجابة للحوادث	Forum Incident Response and Security Teams (FIRST)
مواراة	Steganography
موثوقية	Reliability
موقع إلكتروني	E-site
نظام إسم النطاق	Domain Name System (DNS)
نظام كشف الاختراق	Intrusion Detection System (IDS)
نظام وسيط	Mediating system
نظم إدارة أمن المعلومات	Information Security Management Systems (ISMS)
نظم الدارة التليفزيونية المغلقة	Closed-Circuit Television Camera (CCTV)
نفاذ محمي من إنتاج مجموعة واي-فاي	Wi-Fi Protected Access (WPA)
نقاط بيع إلكترونية	Electronic Point Of Sale (e-pos)
نقود إلكترونية	E-money
هجوم	Attack
وكيل	Agent
وكيل إنترنت	Proxy

مقدمـة

شهد القرن الحادي والعشرون نمواً سريعاً في تكنولوجيا المعلومات والاتصالات وازدياداً ملحوظاً في استخدامها في القطاعات الاقتصادية والاجتماعية والثقافية والترفيهية. وازدهرت معها الخدمات الإلكترونية المتاحة عبر الإنترنت، والتي يستعملها الأفراد وأصحاب الأعمال وسائر فئات المجتمع من دون الحاجة إلى بذل جهود مادية تُذكر. ولكن هذه الخدمات، شأنها شأن التطبيقات الإلكترونية، ليست محصنة ضد المخربين المعلوماتيين، وهي اليوم عرضة لمخاطر جديدة تهدد استمرارها في المستقبل. وقد برزت هذه المخاطر بعد أن استغل المخربون المعلوماتيون الثغرات الفنية في النظم الحاسوبية والتطبيقات الإلكترونية، واستفادوا من الثغرات القانونية في النظم التشريعية التي لم تعد ملائمة لرعاية العمل الرقمي، واعتمدوا على مهاراتهم الفنية المتقدمة لإلحاق الضرر بالبيئة الرقمية وبمستخدميها. وقد أثرت المخاطر المعلوماتية على ثقة الأفراد بالبيئة الرقمية واستخدامهم لها في أعمالهم الحيوية، وأثرت على هذه الثقة عوامل أخرى اجتماعية وتربوية.

وتتفاوت مستويات انتشار تكنولوجيا المعلومات والاتصالات، وتطور الخدمات الإلكترونية والاستثمار فيها بين بلدان الإسكوا. وتشير الدراسات إلى أن استعمال الخدمات الإلكترونية بأشكالها المختلفة، ومنها الحكومة الإلكترونية والمداولات الإلكترونية والخدمات المصرفية الإلكترونية، لا يزال في بداياته في معظم بلدان الإسكوا. ويعود ذلك إلى تأخر الحكومات والقطاع الخاص في تقديم هذه الخدمات، بالإضافة إلى هشاشة الثقة بالبيئة الرقمية والخدمات الإلكترونية، وضعف التشريعات السيبرانية التي تنظم المداولات الإلكترونية.

وقد باشرت بلدان متقدمة ونامية، ومنها عدد من بلدان الإسكوا، بوضع تشريعات خاصة بتنظيم المداولات الإلكترونية وتبادل المعلومات حول الفضاء السيبراني، وبتجريم إساءة استخدام تكنولوجيا المعلومات والاتصالات. ولكن التشريعات السيبرانية التي وضعها معظم البلدان لا تزال غير كافية، وتسمح للمخربين المعلوماتيين باستغلال الفجوات القانونية لارتكاب أعمال تخريبية.

وتتناول هذه الدراسة السياسات والإجراءات اللازمة لبناء الثقة بالفضاء السيبراني والخدمات الإلكترونية وتعزيز أمنها، وبناء مجتمع آمن للمعلومات يتمكن فيه الأفراد من تبادل المعلومات واستعمال الخدمات الإلكترونية بحرية وأمان ومن دون خوف على أمن نظمهم الحاسوبية ومعلوماتهم (الموجودة في البيئة الرقمية). وتركز الدراسة على الأبعاد الأساسية الأربعة التي تؤثر على بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها، وهي الأبعاد القانونية والفنية وتلك المتصلة بالتوعية والتدريب وبكيفية توفير خدمات إلكترونية موثوقة. فتشير إلى أوجه القصور في كل من هذه الأبعاد، وتقترح آليات لتحسين الثقة بالبيئة الرقمية.

وتكمن أهمية هذه الدراسة في مناقشتها مختلف الأبعاد التي تؤثر على ثقة المستخدمين بالفضاء السيبراني وبخدماته. فهي لا تعالج النواحي الفنية المرتبطة بالتكنولوجيا والنظم والبرمجيات وحسب، بل تعرض أيضاً الجوانب القانونية والإنسانية التي تؤثر بشكل ملموس على عامل الثقة. وتعتمد الدراسة على النتائج التي توصل إليها عدد من المنظمات الدولية والإقليمية في مجال أمن الشبكات والنظم الحاسوبية وحمايتها، لا سيما منها الاتحاد الدولي للاتصالات.

ويشير الفصل الأول من الدراسة إلى إشكاليات البيئة الرقمية والخدمات الإلكترونية، وهي ثقة المستخدم بالخدمات المقدمة، وأمن البنى الحاسوبية ونظمها المعلوماتية، والنقص في الأطر القانونية التي ترعى الفضاء السيبراني، وضعف البنى المؤسسية اللازمة لمواجهة التهديدات الخارجية، وبناء ثقة المستخدم بالفضاء السيبراني. ويتناول الفصل عدداً من المساعي الدولية والإقليمية التي قام بها الاتحاد الدولي

للاتصالات، والاتحاد الأوروبي، ومنظمة التعاون والتنمية في الميدان الاقتصادي بهدف زيادة الثقة بالفضاء السيبراني وتعزيز أمنه.

ويتناول الفصل الثاني الإطار الوطني لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها، وضرورة وضع سياسة وطنية لحماية الفضاء السيبراني وتطبيقاته وخدماته وتعزيز أمنها. ويشير الفصل إلى أبرز البنود التي يمكن أن تتضمنها هذه الاستراتيجية، وإلى أدوار أصحاب المصلحة فيها. ويتطرق كذلك إلى مراكز الاستجابة لطوارئ الحاسوب، فيشرح مهامها وأهمية وجودها. كما يعرض الفصل عدداً من المبادرات التي اتخذها كل من اليابان (كدولة أجنبية) وتونس (كدولة من المنطقة العربية) لتعزيز الثقة بالعمليات الإلكترونية وضمان أمنها.

ويتناول الفصل الثالث المسائل القانونية المرتبطة ببناء الثقة بالخدمات الإلكترونية وتعزيز أمنها في بلدان الإسكوا، وضرورة وضع تشريعات سيبرانية من أجل بناء مجتمع معلوماتي آمن. ويعرض الفصل باختصار حالة التشريعات السيبرانية في المنطقة، ويبين أهم ركائز الاستراتيجية التشريعية العربية الملائمة للخدمات الإلكترونية. ويشير هذا الفصل إلى بنية التشريعات السيبرانية اللازمة ومحتواها في المجالات التالية: الحق في الوصول إلى المعلومات، والحق في الخصوصية وحماية البيانات الشخصية، والجرائم السيبرانية، والملكية الفكرية المتصلة بتكنولوجيا المعلومات والاتصالات، والمداولات الإلكترونية بمختلف أشكالها.

ويركز الفصل الرابع على المسائل الفنية المرتبطة بتقديم خدمات إلكترونية آمنة، ويوضح الصعوبات الفنية التي تواجهها حماية البنى الأساسية والنظم الخاصة بتكنولوجيا المعلومات والاتصالات، والأخطار التي تهدد الاستثمار في هذه التكنولوجيا. ويتطرق الفصل إلى آليات وطرق حماية الفضاء السيبراني من الأخطار والتهديدات، ويعرض حلولاً متكاملة للتخفيف منها. كما يستعرض أبرز المعايير الدولية المعتمدة في إدارة نظم أمن المعلومات، وعدداً من الممارسات الناجحة في المنطقة العربية.

ويتناول الفصل الخامس موضوع التوعية بأهمية حماية استخدام تكنولوجيا المعلومات والاتصالات وتحقيق أمنها. ويعرض عدداً من التوجيهات الدولية والإقليمية المتصلة بنشر ثقافة حماية الفضاء السيبراني وضمان أمنه. كما يستعرض الخطة العامة للتوعية الوطنية التي نص عليها دليل أعده الاتحاد الأوروبي، والتي تهدف إلى ضمان الحماية والأمن في استخدام تكنولوجيا المعلومات والاتصالات. ويعرض الفصل كذلك عدداً من المبادرات الناجحة في مجال التوعية في بلدان عربية وأجنبية.

وأما الفصل السادس فيتناول عدداً من المنهجيات التي تعتمد في استحداث خدمات إلكترونية، والتي تساعد على تعزيز الثقة بالتكنولوجيا المستخدمة. فيشير إلى أن موضوع تقديم الخدمات الإلكترونية لا يتطلب معالجة المسائل الفنية والقانونية فحسب، بل يستدعي كذلك معالجة المسائل الاجتماعية والنفسية لدى المستخدمين، ومراعاة عاملي الثقة والطمأنينة في استعمال الخدمات الإلكترونية.

وأخيراً، يعرض الفصل السابع ملخصاً للتوصيات التي وردت في الفصول الستة الأولى، كما يبين الإطار العام الوطني الذي يجب إعداده وتنفيذه على المستوى الوطني من أجل بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها.

وتجدر الإشارة إلى أن فصول التقرير مترابطة ومتكاملة من حيث مواضيعها، إنما يمكن قراءتها بشكل منفصل من أجل معالجة قضايا منفصلة حول بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات.

أولاً- إشكاليات استعمال الخدمات الإلكترونية والتدابير الدولية المتخذة لمواجهتها

يحتاج بناء الثقة بالخدمات الإلكترونية إلى توفير بنى أساسية محمية وآمنة على مختلف مستويات تكنولوجيا المعلومات والاتصالات (من شبكات اتصالات، وشبكات حاسوبية، ونظم معلوماتية، وتطبيقات) بمنأى عن الأخطار والتهديدات الخارجية التي قد تؤثر على تشغيلها وطريقة عملها، والتي قد تسبب عطلاً جزئياً أو كلياً في أحد مكوناتها.

ويستدعي بناء الثقة بالخدمات الإلكترونية توفير تطبيقات إلكترونية موثوقة تلائم احتياجات المستخدمين ويسهل الاستثمار فيها. وينبغي أن تكون هذه التطبيقات محمية وآمنة وقادرة على حماية المعلومات التي تخزنها وتحفظها لفترات زمنية طويلة أو قصيرة. كما يتطلب بناء الثقة تزويد المستخدم بخدمات إلكترونية قائمة على الشفافية في التعامل والتفاعل، بحيث يكون على بينة من السياسات والإجراءات التي تطبقها المؤسسة أو الشركة التي تؤمن الخدمات في مجال حماية المعلومات وضمان أمنها وسريتها.

ويستلزم بناء الثقة على المستوى الوطني وجود إطار قانوني صلب يحمي المستخدمين العاديين من سوء استعمال التكنولوجيا وتطبيقاتها، ومن الأخطاء العرضية أو المقصودة، ومن التلاعب والاستغلال. ويجب أن يتلاءم هذا الإطار القانوني لتكنولوجيا المعلومات والاتصالات واستثماراتها في كافة المجالات الاقتصادية والاجتماعية والثقافية مع النصوص القانونية الوطنية والإلتزامات الدولية للدولة.

ولكن جذب اهتمام الأفراد وتشجيعهم على التحول من أسلوب العمل التقليدي إلى الأسلوب الإلكتروني يحتاج إلى اقتناعهم بأن الخدمات الإلكترونية تقدم لهم قيمة مضافة جديدة لا يوفرها أسلوب العمل التقليدي، وبأن أسلوب العمل الإلكتروني لا يشكل خطراً على معلوماتهم وممتلكاتهم، وأنه يتلاءم واحتياجاتهم في مختلف الميادين الإدارية والاقتصادية والثقافية.

ومع اتساع انتشار البرمجيات الخبيثة كالفيروسات والديدان المتطفلة والبرمجيات التجسسية، أصبح المستخدمون بحاجة إلى التدرب على آليات الحماية الشخصية من التهديدات الخارجية، والتوعية بضرورة التعامل بحذر مع الخدمات المقدمة عبر الفضاء السيبراني لحماية معلوماتهم وممتلكاتهم الشخصية الحاسوبية.

يتبيّن مما تقدّم أن موضوع الثقة بالخدمات الإلكترونية موضوع متشعب وذو أبعاد مختلفة، وهو يتطلب تضافر جهود جهات وطنية مختلفة في القطاعين العام والخاص لبناء الثقة بالعالم الرقمي وتعزيز أمنه. ويعتبر عامل الثقة بتكنولوجيا المعلومات والاتصالات موضوعاً شائكاً في مجتمع المعلومات. فالثقة تحتاج إلى الحماية والأمن على المستوى التكنولوجي، ووضع التشريعات السيبرانية وتطبيقها إلى جهود كبيرة وإلى توفر كوادر بشرية تملك الكفاءة اللازمة لتشغيل النظم المعلوماتية واستثمارها.

ومن أجل الإحاطة بمختلف الاحتياجات، لا بد لكل بلد أن يضع إطاراً وطنياً عاماً لتوضيح احتياجاته من حيث تطوير الخدمات الإلكترونية واستخدامها وطنياً، لما لتلك الخدمات من أثر إيجابي على تطوير مجتمع المعلومات ونمو الهياكل الاقتصادية والاجتماعية.

لقد باشرت بلدان كثيرة بتطبيق العديد من المنهجيات والآليات الفنية والتعليمية للدخول في مجتمع معلومات آمن، ولكنّ هذه البلدان ما زالت بحاجة إلى تحديث منهجيات وآليات عملها أو تعديلها واستكمالها لكي تتوافق مع النهج اللازم لتعزيز ثقة المواطن بها.

ويبين هذا الفصل الإشكاليات الفنية والقانونية التي يعاني منها مجتمع المعلومات، والتي تعيق انتشار استخدام تكنولوجيا المعلومات والاتصالات عموماً، والخدمات الإلكترونية خصوصاً. كما يشير إلى الأنشطة التي اضطلعت بها منظمات دولية وإقليمية لحماية الفضاء السيبراني وتحقيق أمنه. ومن المؤكد أن بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها لا يقتصر على حماية أمن النظم المعلوماتية والشبكية فحسب، بل يتطلب كذلك تحديد مواصفات خاصة للخدمات الإلكترونية تحظى بثقة المستخدم وتشعره بالأمان، وتوفير بيئة قانونية ملائمة للفضاء السيبراني تحمي مستعملي هذه الخدمات ومستثمريها من الاعتداءات والاستخدامات غير اللائقة.

ألف- إشكاليات البيئة الرقمية والخدمات الإلكترونية

1- ثقة المستخدم بالبيئة الرقمية

خلال العقدين الماضيين، غيّر نظام شبكة الإنترنت الكثير من أوجه الحياة العصرية مع ارتفاع معدلات استخدامه وتزايد عدد المواقع الإلكترونية واتساع أحجامها. ولكن بلداناً كثيرة لا تستثمر عدداً كبيراً من الاستخدامات الممكنة للإنترنت والشبكات والنظم الحاسوبية، أو أنها تستثمرها بشكل جزئي، بينما لا تزال بلدان أخرى في مرحلة التفكير في هذا الاستثمار. ويشكل انعدام ثقة المستخدمين بالإنترنت وبالعالم الرقمي أحد الأسباب الرئيسة التي تحول دون استثمار الإمكانات الكامنة لشبكة الإنترنت وتطوير تطبيقات وخدمات إلكترونية جديدة.

ويُعد عنصرا الثقة والأمن بين أبرز العناصر اللازمة لتوفير بيئة مؤاتية لبناء مجتمع المعلومات حيث يرتبط استعمال الأفراد الخدمات الحكومية بشعورهم بالراحة والطمأنينة والأمان عند استخدامها. وينطبق هذا الأمر على جهات أخرى، كالمستهلكين والشركات المتوسطة والصغيرة، لأنها تحتاج إلى التأكد من أمن خدمات التجارة الإلكترونية والمداولات الإلكترونية قبل استخدامها.

ومع تعدد الأدوات المستعملة للدخول إلى شبكة الإنترنت، ومنها الحاسوب والهاتف المحمول والتلفاز الرقمي والأجهزة المحمولة الأخرى، أصبح الأفراد أكثر اهتماماً بحماية ممتلكاتهم وبياناتهم الشخصية ضمن العالم الرقمي المترابط شبكياً. ويتوقع أن يكتسب عامل الثقة بالعالم الرقمي أهمية كبيرة في المستقبل نظراً إلى استعمال الرقاقات الحاسوبية في العديد من الأجهزة ذات الاستخدام اليومي والشخصي، ومع ازدياد الترابط بين الأجهزة. وقد يتطلب بناء الثقة حلولاً أكثر شمولاً من الناحية الفنية من تلك الموجودة اليوم. كما أن قبول المجتمع بالتجهيزات الشخصية المحوسبة سيتطلب اعتماد منهجية أكثر حداثة وتطوراً من أجل إدارة المعلومات الشخصية عبر واجهات تحكم سهلة الاستخدام وجديرة بالثقة، مع أخذ ضرورات توفير الحماية الشخصية ونظام حماية البيانات في الاعتبار. وينبغي ألا يقتصر الاهتمام على واجهات الاستخدام وحسب، بل أن يمتد إلى حماية المعلومات والبنى الحاسوبية الأساسية والشبكات غير المرئية بالنسبة إلى المستخدم العادي.

2- إشكاليات البنى الأساسية والنظم المعلوماتية[1]

في ظل توسع نطاق الإنترنت، أصبح المجرمون المعلوماتيون المحترفون قادرين على إيجاد فرص جديدة في البيئة الرقمية القابلة للخرق، وذلك للقيام بأعمال إجرامية ضدها أو ضد البنى الأساسية الوطنية

(1) *Challenges to Building a Safe and Secure Information Society*. World Information Society Report 2007, chapter 5.

الحرجة، كشبكات الاتصالات وشبكات النقل والشبكات الخاصة بالمعلومات الصحية. وأصبحت البرمجيات الخبيثة والاعتداءات على الشبكات والنظم عن بعد معروفة بالنسبة إلى مستخدمي شبكة الإنترنت، ولا ينجو منها إلا المستخدمون المحصنون. ويضاف إلى هذه المخاطر الانتشار الواسع للبريد الدعائي، وكذلك الإعلانات الخادعة التي تجتاح البريد الإلكتروني.

ولا تقتصر الأخطار على الخدمات الإلكترونية الموجهة إلى الأفراد والمواطنين، بل تطال البنى الأساسية، والنظم والخدمات الإلكترونية المرتبطة بالمصارف والشؤون المالية، والرعاية الصحية، والطاقة والنقل، خاصة وأن القطاعات الخدماتية الأساسية بشتى أنواعها تعتمد إلى حد بعيد اليوم على تكنولوجيا المعلومات والاتصالات من أجل تبادل المعلومات وتخزينها والتحكم بها.

3- إشكاليات الأطر القانونية المنظمة للفضاء السيبراني

يستغل المجرمون المعلوماتيون غياب نظم المساءلة، والثغرات في بنى تكنولوجيا المعلومات والاتصالات وأنظمتها وفي التشريعات الوطنية والإقليمية لارتكاب الجرائم المعلوماتية أو استخدام الفضاء السيبراني بشكل غير شرعي. وتبين الحقائق أن هذه الجرائم تستهدف خصوصاً البلدان التي لم تسن قوانين تجرم الاعتداءات المعلوماتية أو التي لا تطبق هذه القوانين.

وفي ضوء توسع شبكات الحواسيب، أصبحت مهاجمة الشبكات والنظم في أي مؤسسة أو دولة ممكنة. ولم يعد للبعد الجغرافي أي أهمية، إلا في حالات السرقة المادية التي تتعرض لها الأجهزة والحواسيب. فبإمكان المجرمين شن هجمات سيبرانية باستخدام طرق غير مركزية وتقنيات تفاعلية وتعاونية وتشاركية. كما أصبح الكشف عن المجرمين الحقيقيين والفعليين معقداً جداً، شأنه شأن محاسبة العمليات الإجرامية التي يتعرض لها الفضاء السيبراني. فلا حدود جغرافية تقف عندها هذه العمليات ولا قوانين دولية موحدة تطبق في البلدان كافة، ولا وجود لمحاكم دولية تجرم الاعتداءات السيبرانية.

وقد وضع بعض البلدان قوانين لمكافحة الجرائم المعلوماتية وسوء استخدام تكنولوجيا المعلومات والاتصالات. ولكن تطبيقها ما زال يواجه عدداً من الصعوبات، لا سيما في المنطقة العربية، في غياب آليات للتطبيق ومحامين وقضاة مدربين على تطبيقها. وأما إثبات الجريمة وتحديد الجهة المرتكبة للعمل الإجرامي فمن المسائل الهامة في المجال السيبراني، وهما رهن بدقة الخبراء المعلوماتيين الفنيين القادرين على المساهمة في الكشف عن الجريمة المعلوماتية وبدرجة احترافهم. وتجدر الإشارة إلى أن التعاون الدولي في موضوع جرائم المعلوماتية مهم نظراً إلى الطبيعة الكونية التي تميز الفضاء السيبراني.

وتجدر الإشارة إلى أن وجود أطر قانونية متناسقة ومتجانسة في البلدان يسهل عمل القضاة والمحامين على المستويين الإقليمي والدولي. وتسعى مناطق عديدة، كالاتحاد الأوروبي مثلاً، إلى استحداث إطار إقليمي للتشريعات السيبرانية لتسهيل كشف الجرائم وحماية أمن الفضاء السيبراني في بلدان الاتحاد الأوروبي. وتُبذل كذلك جهود دولية لإبرام اتفاقيات ومعاهدات دولية خاصة بالفضاء السيبراني، ولكنها تبقى غير كافية ومثلها التجانس بين الأطر القانونية. وينبغي بذل مزيد من الجهود على المستويين القطري والإقليمي من أجل معالجة النقص في الأطر القانونية الخاصة بالجرائم المعلوماتية والفضاء السيبراني في منطقة الإسكوا.

4- ضعف البنى المؤسسية

يشكل غياب بنى تنظيمية ومؤسسية تتعامل مع الأخطار المعلوماتية إحدى الإشكاليات التي تعيق حماية الفضاء السيبراني. فالمؤسسات والشركات التي تستخدم تكنولوجيا المعلومات والاتصالات لا تعتبر عنصري الحماية والأمن أساسيين في حالات عديدة، ولا تستحدث في هيكلها المؤسسي أي إدارة أو وحدة تختص بمراقبة أمن تكنولوجيا المعلومات والاتصالات وتطبيقاتها وبحمايته وضمانه. كما أنها لا تضع أي سياسات أو خطط عمل لمواجهة التهديدات المعلوماتية الخارجية.

وتقوم البلدان المتقدمة وبعض البلدان النامية، ومنها بلدان عربية، بإنشاء وكالات خاصة لرصد الحوادث الطارئة في الشبكات المعلوماتية والإنذار بوقوعها ومعالجتها، وبنى تنظيمية لإدارة عملية مواجهة الهجمات عبر الشبكات وتنسيقها. ولكن الحاجة إلى بذل مزيد من الجهود في عدد كبير من البلدان العربية لا تزال شديدة.

ومن ناحية أخرى، لا تزال بلدان كثيرة تفتقر إلى بنى مؤسسية خاصة بالتوقيع الرقمي والشهادة الرقمية، وهما عنصران ضروريان للتعرف على هوية الأشخاص وحماية العمليات الإلكترونية ومحاربة الأخطار السيبرانية. وبهدف تسهيل الاعتراف بهذه الشهادات على المستويات الوطنية والإقليمية والدولية، ينبغي إعداد إطار شامل يساعد البلدان على وضع إطار وطني للشهادات الرقمية الشخصية، ويتلاءم وسائر الأطر الوطنية.

وقد سعت المؤسسات الوطنية والإقليمية المعنية بحماية أمن الفضاء السيبراني إلى تنسيق جهودها الرامية إلى تسهيل التعاون وتبادل المعلومات بينها، والاعتراف بالاعتمادية الرقمية، غير أن هذه المساعي تظل غير كافية. ولذلك ينبغي اتخاذ مزيد من الإجراءات لتمكين البنى المؤسسية من مواجهة المخاطر المعلوماتية، والتوصل إلى حلول شاملة للتحديات العديدة.

ويبين الإطار 1 أدناه حالة بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها في منطقة الإسكوا.

الإطار 1- حالة بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها في منطقة الإسكوا

أشارت الدراسة التي أعدتها الإسكوا حول الملامح الإقليمية لمجتمع المعلومات في غربي آسيا لعام 2007 إلى أوجه التشابه بين الإجراءات المتبعة في بلدان الإسكوا لبناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها، وإلى فوارق بسيطة بينها. فجميع البلدان تعاني من قلة الاهتمام الفعلي بأمن المعلومات والشبكات وحماية الخصوصية، لا سيما في مواقع الحكومة الإلكترونية، بينما يزداد هذا الاهتمام في شركات القطاع الخاص، لا سيما المصارف.

وقد أشارت الدراسة إلى تحسن في مستوى أمن المعلومات في بلدان مجلس التعاون لدول الخليج العربية خلال السنوات القليلة الماضية، وفي مستوى وعي كوادر الإدارات العليا وخبراء تكنولوجيا المعلومات والمستخدمين بأمن تلك المعلومات خلال السنوات الخمس الأخيرة. ولكن بلدان مجلس التعاون الخليجي وسائر البلدان الأعضاء في منطقة الإسكوا لا تزال بحاجة إلى بذل مزيد من الجهود.

وأشارت الدراسة كذلك إلى أن عدد القراصنة المحترفين يزداد سنوياً في منطقة الشرق الأوسط حيث تكثر شبكات الحواسيب غير المحمية والمعرضة بالتالي للقرصنة. وقد صنفت هذه الدراسة بلدان الإسكوا في فئتين استناداً إلى قدرتها على بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتحقيق أمنها، وإلى استعدادها لمواجهة القرصنة وغيرها من

المخاطر السيبرانية. وهاتان الفئتان هما كما يلي:

الإطار 1 (تابع)

1- الفئة الأولى: وتضم الأردن والبحرين والجمهورية العربية السورية وعمان وفلسطين ولبنان واليمن. وهي تفتقر بشكل شبه تام إلى السياسات المتعلقة بأمن المعلومات والخصوصية والتشريعات القانونية المتعلقة بسوء الاستخدام.

2- الفئة الثانية: وتضم الإمارات العربية المتحدة والعراق وقطر والكويت ومصر والمملكة العربية السعودية. وهي تشهد ظهور بوادر اهتمام بالسياسات المتعلقة بأمن المعلومات والخصوصية والتشريعات القانونية المتعلقة بسوء الاستخدام.

المصدر: الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، الملامح الإقليمية لمجتمع المعلومات في غربي آسيا 2007، E/ESCWA/ICTD/2007/15.

باء- الجهود الدولية والإقليمية الرامية إلى بناء الثقة بالبيئة الرقمية وتعزيز أمنها

يشكل الفضاء السيبراني، بشبكاته الحاسوبية المنتشرة في جميع بلدان العالم وبطبيعته الكونية التي لا تقف معها البلدان عند أي حدود في الفضاء، حافزاً للتعاون الدولي والإقليمي في بناء مجتمع المعلومات وتطويره. ويستدعي ذلك عملاً مشتركاً بين البلدان والشعوب، ليس من أجل تبادل التجارب الناجحة والخبرات وحسب، بل كذلك لمواجهة الأخطار والتهديدات التي تخترق البيئة الرقمية ولا تعرف حدوداً بين البلدان. ولا شك في أن المستوى الأهم لأمن المعلومات والبنى الأساسية لتكنولوجيا المعلومات والاتصالات وحمايتها هو المستوى الوطني، لا سيما لجهة ارتباطه بالأمن القومي.

وقد ركز مؤتمر القمة العالمي لمجتمع المعلومات في إعلان المبادئ وخطة العمل على أهمية أمن المعلومات والشبكات، وضرورة حماية المعلومات والخصوصية من أجل بناء مجتمع المعلومات[2]. وقد أشارت الوثيقتان إلى ضرورة بناء ثقة الأفراد وأصحاب الأعمال بالبيئة الرقمية حرصاً على نمو هذه البيئة وتعزيز الاعتماد عليها في المجالات الحيوية المختلفة. وشددت الوثيقتان أيضاً على ضرورة التعاون بين أصحاب المصلحة كافة في مجتمع المعلومات، كونهم يؤثرون على بناء الثقة بتكنولوجيا المعلومات والاتصالات ويستفيدون منها. كما بينت الوثيقتان أهمية التعاون الدولي وتضافر الجهود من أجل مكافحة التهديدات والأخطار والممارسات الخاطئة التي تؤثر على الثقة بالبيئة الرقمية، وعلى إمكانية مواجهة الجرائم الإلكترونية.

وشكل موضوع بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات في البلدان العربية وضمان أمنها محوراً أساسياً من محاور الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات - بناء مجتمع

(2) الأمم المتحدة، مؤتمر القمة العالمي لمجتمع المعلومات، جنيف، 10-12 كانون الأول/ديسمبر2003: إعلان المبادئ، بناء مجتمع المعلومات: تحد عالمي في الألفية الجديدة، WSIS-03/GENEVA/DOC/4-A، 12 كانون الأول/ديسمبر 2003 (http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/SO3-WSIS-DOC-(0004!!PDF-E.pdf)؛ خطة العمل، WSIS-03/GENEVA/DOC/5-A، 12 كانون الأول/ديسمبر 2003، (http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-A.doc).

المعلومات (2007-2012) التي أقرها مجلس وزراء الاتصالات العرب في عام 2007[3]. وتعتبر الاستراتيجية أن هذا المحور أساسي لتحقيق الهدف الأول من الاستراتيجية العربية المتمثل في توفير سوق تنافسية للمجتمع العربي للمعلومات. وفي إطار السعي إلى بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتحقيق أمنها، تحدد الاستراتيجية ضرورة توفير أمن المعلومات والشبكات للمحافظة على خصوصية المواطن العربي وتفعيلها، ووضع تشريعات لحماية البيانات، وتعزيز التعاون الدولي في مكافحة جرائم الفضاء الإلكتروني، وسوء استخدام تكنولوجيا المعلومات والاتصالات.

ويعتبر موضوع بناء الثقة والأمن كذلك أساساً في خطة العمل الإقليمية لبناء مجتمع المعلومات التي أعدتها الإسكوا في عام 2005[4]. وبينت هذه الخطة عدداً من الأهداف والإجراءات الاستراتيجية اللازمة من أجل تحسين ثقة المستخدمين بالبيئة الرقمية وزيادة الأمن فيها.

1- أمثلة على أنشطة الاتحاد الأوروبي في مجال بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها

أشار مجلس الاتحاد الأوروبي إلى ضرورة وضع استراتيجية لبناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها، وذلك لرفع مستوى الأنشطة المضطلع بها على المستويين الوطني والإقليمي بهدف تطوير مجتمع المعلومات، وتحفيز مختلف أصحاب المصلحة على اتخاذ إجراءات تشجع الأفراد على استخدام تطبيقات تكنولوجيا المعلومات والاتصالات عموماً، والخدمات الإلكترونية خصوصاً. فقد صدر عن مجلس أوروبا القرار 2007/C 68/01[5] المؤرخ 22 آذار/مارس 2007، والمتعلق بوضع استراتيجية من أجل مجتمع معلومات آمن في أوروبا. ويشير هذا القرار إلى سرعة تغير التكنولوجيا وتقدمها في مجتمع المعلومات، ويشدد على أهمية الثقة كعنصر أساسي من العناصر التي تكفل النجاح في بناء مجتمع جديد للمعلومات. وينص القرار أيضاً على ارتباط هذه الثقة بتجارب المستعملين النهائيين، وعلى الحاجة إلى احترام الخصوصية.

ولخص القرار المذكور العناصر الرئيسة في الاستراتيجية الأوروبية لبناء الثقة بمجتمع المعلومات وتعزيز أمنه. ومن هذه العناصر دعوة البلدان الأعضاء إلى دعم برامج التدريب والتوعية العامة المتصلة بأمن الشبكات والمعلومات، والموجهة نحو جميع فئات المواطنين والمستخدمين والقطاعات الاقتصادية، وخصوصاً الشركات المتوسطة والصغيرة، فضلاً عن المستخدمين النهائيين ذوي الاحتياجات الخاصة. كما دعا إلى إطلاق يوم أمن الشبكات والمعلومات[6] نظراً إلى أهمية هذا الموضوع، وأشار إلى ضرورة تعزيز البحث والتطوير في المواضيع المتعلقة بأمن الفضاء السيبراني وحمايته. وأوضح القرار أيضاً ضرورة تشجيع الشراكات الابتكارية التي تسعى إلى تعزيز أمن تكنولوجيا المعلومات والاتصالات على المستوى

(3) الأمانة الفنية لجامعة الدول العربية، الاستراتيجية العربية العامة لتكنولوجيا المعلومات والاتصالات، بناء مجتمع المعلومات (2007-2012)، 2007. http://www.aticm.org.eg.

(4) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، خطة العمل الإقليمية لبناء مجتمع المعلومات، 18 أيار/مايو 2005، E/ESCWA/ICTD/2004/4.

(5) Official Journal of the European Union. Council Resolution of 22 March 2007 on a *Strategy for a Secure Information Society in Europe*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:068:0001:0004:EN:PDF.

(6) Information and Security Network Day، مرجع سبق ذكره.

الأوروبي، وتحسين استخدام التكنولوجيا الحديثة للشبكات والمعلومات وخدماتها، وبالتالي زيادة مردودها التجاري.

ودعا القرار إلى أهمية إجراء نقاش استراتيجي بين أصحاب القرار لوضع منهجيات متجانسة حول الأبعاد الخاصة بتنظيم مجتمع المعلومات، والبحث والتطوير، والحكومة الإلكترونية والتعليم، مع أخذ التطور المستمر الذي يشهده مجتمع المعلومات في الاعتبار.

وتجدر الإشارة إلى أن البلدان الأعضاء في الاتحاد الأوروبي أنشأت الوكالة الأوروبية لأمن الشبكات والمعلومات[7]، وهدفها تعزيز قدرات البلدان الأعضاء في الاتحاد الأوروبي وقطاع الأعمال في مواجهة مشاكل أمن المعلومات. وتزود الوكالة البلدان الأعضاء في الاتحاد الأوروبي بإرشادات وخبرات في مجال أمن المعلومات، كما تساعدها على التواصل والحوار مع القطاع التجاري لمعالجة المسائل الخاصة بأمن البنى الحاسوبية والشبكية والنظم المعلوماتية. وتعمل الوكالة على جمع البيانات المتصلة بحوادث الأمن والأخطار الناشئة في أوروبا وتحليلها، وتقدم الدعم لتقييم المخاطر وإدارتها من أجل تحسين قدرة البلدان على مجابهتها. وتنظم الوكالة برنامجاً للتوعية يهدف إلى تشجيع التعاون بين مختلف أصحاب المصلحة، لا سيما بين القطاعين العام والخاص.

وأصدر الاتحاد الأوروبي عدداً من التوجيهات المتعلقة بالإطار التشريعي للأمن السيبراني، ونورد أهمها في ما يلي:

(أ) التوجيه الأوروبي 1995/281/EC. ويوصي هذا التوجيه بإصدار قوانين لحماية المعلومات الشخصية واستخدام السجلات العامة التي تتضمن معلومات رسمية، تجنبا لتخزين معلومات لا فائدة منها أو استخدام طرق غير مناسبة لتخزينها؛

(ب) التوجيه الأوروبي 1997/7/EC. وهو يتعلق بقضايا البيع عن بُعد والتعاقد عبر التجارة الإلكترونية؛

(ج) التوجيه الأوروبي 1999/93/EC. وهو يُعنى بالتوقيع الإلكتروني، ويميز بين ثلاثة مستويات من التواقيع الإلكترونية؛

(د) التوجيه الأوروبي 1997/7/EC. وهو يتعلق بحقوق إلغاء البيع؛

(•) التوجيه الأوروبي 1995/46/EC. وهو يتصل بحماية الملكية الفكرية لمواقع الإنترنت وأسماء النطاقات والمحتويات؛

(و) التوجيه الأوروبي 1995/46/EC. وهو يتعلق بمكافحة البريد الدعائي وحماية معالجة البيانات الشخصية وحرية حركتها.

2- أنشطة الاتحاد الدولي للاتصالات في مجال الأمن السيبراني

(7) European Network and Information Security Agency (enisa). http://www.enisa.europa.eu/pages/01_01.htm. http:www.itu.int/aboutitu/annual.

قام المجتمع الدولي بتعيين الاتحاد الدولي للاتصالات الجهة المسؤولة عن التنسيق والاتصال بشأن تنفيذ الخط جيم 5 للعمل من خطة عمل جنيف، والمتعلق ببناء الثقة باستعمال تكنولوجيا المعلومات والاتصالات والسعي إلى ضمان أمنها.

وأصدر مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات لعام 2006، الذي عقد في أنطاليا بتركيا خلال الفترة من 6 إلى 24 تشرين الثاني/نوفمبر 2006، القرار 130[8]. وقد هدف هذا الأخير إلى تعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات، وتحديد مهامه في هذا المجال. وتجدر الإشارة إلى أن الاتحاد الدولي للاتصالات يضطلع بعدد من الأنشطة وفقا لما ينص عليه قرار الجمعية العامة للأمم المتحدة 239/57 المؤرخ 31 كانون الثاني/يناير 2003، والذي دعت فيه إلى إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي.

ويبذل الاتحاد الدولي للاتصالات منذ عام 2005 جهوداً ملحوظة لبناء الثقة بالفضاء السيبراني وتعزيز أمنه، حيث يعِد الكثير من الدراسات حول الممارسات الفضلى في البلدان في مجال حماية البنى الحاسوبية والشبكات. كما ينظم اجتماعات دورية للخبراء، وورشات عمل تدريبية على المستويين الإقليمي والدولي. وقد أنشأ الاتحاد بوابة خاصة بأمن الفضاء السيبراني[9]، وهي تُعتبر مصدراً هاماً للمعلومات المرتبطة بالسياسات أو المعلومات الفنية أو التجارب الناجحة في مجال الأمن السيبراني.

وأطلق الاتحاد الدولي للاتصالات في عام 2007[10] برنامج عمل الاتحاد للأمن السيبراني العالمي[11] الذي يشكل إطاراً للتعاون الدولي، ويهدف إلى تعزيز الثقة بمجتمع المعلومات. ويسعى برنامج العمل إلى تشجيع العمل المشترك بين جميع الشركاء في مجتمع المعلومات من أجل بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

وعلى المستوى الوطني، قامت إدارة التنمية في الاتحاد الدولي للاتصالات بوضع إطار عمل لحماية الفضاء السيبراني، ونشرت تقريراً حول الممارسات الفضلى المعتمدة، واستحدثت أداة لتقييم درجة حماية الفضاء السيبراني على المستوى الوطني. وفي ما يلي عرض موجز للإطار المقترح وأداة التقييم اللذين يساعدان على تحديد الإطار الوطني لحماية الفضاء السيبراني.

(أ) إطار للتعاون الدولي في مجال الأمن السيبراني[12]

يشير الإطار إلى أن أمن الفضاء السيبراني مسؤولية مشتركة تقع على عاتق الجهات المعنية به كافةً. ومن أهم هذه الجهات القطاع الحكومي، وخصوصا الهيئات المسؤولة عن أمن المعلومات، وتشغيل البنى الأساسية في الفضاء السيبراني وبرمجياته وتطبيقاته، والقطاع الخاص بشركاته المعنية بتطوير تكنولوجيا

(8) Final Acts of the Plenipotentiary Conference 2006, Resolution 130, *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf.

(9) http://www.itu.int/cybersecurity/gateway/index.html.

(10) http://www.itu.int/ITU-D/cyb/cybersecurity/.

(11) أنشطة الاتحاد الدولي المتصلة بالأمن السيبراني، http://www.itu.int/council/C2008/hls/cyb/cybersecurity-ar.html .

(12) *Management Framework for Organizing National Cyber security/CIIP Efforts*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/richardson-cybersecurity-framework-and-readiness-assessment-CITEL-Mar-08.pdf.

المعلومات والاتصالات وتشغيلها وتقديم خدماتها. وتمتد المسؤولية إلى جميع مستخدمي الفضاء السيبراني، من جامعات وشركات وطلاب وأفراد، سواء كانوا ينتجون معلومات للفضاء السيبراني، أو يستخدمون نظم المعلومات والشبكات فيه، أو يدربون على استخدام هذه النظم.

وقد حدد الإطار العملي لحماية الفضاء السيبراني خمسة إجراءات أساسية ينبغي اتخاذها في هذا الصدد. وهي تتمثل في وضع استراتيجية وطنية لحماية الفضاء السيبراني وضمان أمنه، والتعاون بين القطاعين العام والخاص، ومنع الجرائم السيبرانية، وإدارة الأخطار والتهديدات، ونشر ثقافة حماية الفضاء السيبراني. ويعرض الإطار السياسة التي يجب أن توجه الجهود الوطنية، والأهداف الرئيسة من تنفيذ السياسة الوطنية بالإضافة إلى الخطوات العملية اللازمة لبلوغ هذه الأهداف. وفيما يلي تلخيص لمكونات الإطار العملي الذي وضعه الاتحاد الدولي للاتصالات.

(1) الإجراء الأول: وضع استراتيجية وطنية لحماية الفضاء السيبراني وضمان أمنه

وفقاً لتوصيف الاتحاد الدولي للاتصالات، ينبغي أن تنص الاستراتيجية الوطنية على إطلاق حملة لتوعية أصحاب القرار بضرورة وضع خطة عمل وطنية ترعى حماية الفضاء السيبراني، والتعاون الدولي في هذا المجال، والمشاركة في الجهود الدولية الرامية إلى تعزيز أمنه. ويتطلب وضع استراتيجية وطنية لحماية الفضاء السيبراني تعيين مسؤول عن تحفيز حماية الفضاء السيبراني وتحقيق أمنه، وإطلاق الجهود الوطنية اللازمة لذلك، وتحديد الجهة التي ستقع على عاتقها مسؤولية تطوير الاستراتيجية.

ويجب أن تتضمن الاستراتيجية عدداً من محاور العمل، وأن تحدد الجهات المسؤولة عن الإجراءات الخمسة الأخرى من إطار العمل. ويمكن أن تحدد الاستراتيجية كذلك المؤسسات أو الجهات الحكومية المعنية بحماية الفضاء السيبراني، والجهات غير الحكومية التي تؤدي دوراً في توفير الأمن والحماية لتكون شريكاً في تنفيذ الاستراتيجية.

(2) الإجراء الثاني: التعاون بين القطاعين العام والخاص

تتطلب حماية الفضاء السيبراني، كونها مسؤولية مشتركة، تعاوناً بين مختلف أصحاب المصلحة، لا سيما بين القطاعين العام والخاص. ويهدف هذا المحور إلى تطوير التعاون بين هذين القطاعين من جهة، وإلى استثمار خصائص القطاع الخاص بهدف تحسين أمن الفضاء السيبراني الوطني من جهة أخرى. ويجب أن يتضمن هذا المحور تشجيع التفاعل والتعاون بين مؤسسات القطاع الخاص لحماية المصادر ذات الطبيعة المتشابهة، ومعالجة عدد من المواضيع ذات الاهتمام المشترك بين القطاعين العام والخاص في مجال أمن الفضاء السيبراني.

(3) الإجراء الثالث: خفض معدلات الجرائم السيبرانية

تتطلب حماية الفضاء السيبراني تعديل قانون العقوبات واعتماد إجراءات وسياسات جديدة تهدف إلى التصدي للجرائم السيبرانية. وبالتالي، يجب أن يهدف هذا المحور إلى وضع عدد من القوانين المتجانسة

والمتكاملة، والمرتبطة بأمن الفضاء السيبراني والجرائم السيبرانية، والمتلائمة مع الاتفاقية بشأن الجريمة السيبرانية لعام 2001[13].

ويحتاج تطوير التشريعات السيبرانية إلى تحديد الجهات الوطنية المعنية بأمن الفضاء السيبراني، والتعاون معها ومع القطاع الخاص المعني بتقديم الخدمات الإلكترونية وذلك لمناقشة القوانين الخاصة بالفضاء السيبراني من الناحيتين القانونية والفنية، ومن ناحية استخدامه. كذلك يتطلب إصدار تشريعات خاصة بالجرائم السيبرانية تفاهماً واتفاقاً بين السلطات التشريعية والقضائية والفنيين والمشرعين في البلد الواحد.

(4) الإجراء الرابع: إدارة الأخطار والتهديدات المعلوماتية ومواجهتها

تتطلب حماية الفضاء السيبراني تحديد جهة تنسيق وطنية (أي شخص أو مؤسسة)، تكون مسؤولة عن مراقبة الأخطار والإشعار بحدوثها، وبالتالي مواجهتها. ويجب أن تتعاون جهة التنسيق هذه مع الجهات الحكومية والقطاع الخاص، وكذلك مع مؤسسات المجتمع الدولي المعنية بشؤون حماية الفضاء السيبراني وضمان أمنه.

(5) الإجراء الخامس: ثقافة حماية الفضاء السيبراني وضمان أمنه

يستلزم تشجيع ثقافة حماية الفضاء السيبراني وضع وتنفيذ برامج توعية وتدريب موجهة إلى المسؤولين المعنيين بالنظم المعلوماتية في الأجهزة الحكومية، وأخرى إلى مستخدمي التطبيقات الحكومية بشأن أمن المعلومات. وينبغي تشجيع القطاع الخاص، وكذلك المنظمات غير الحكومية والطلاب والأفراد، على تطوير ثقافة أمن الفضاء السيبراني.

(ب) أداة الاتحاد الدولي للاتصالات لتقييم الأمن السيبراني على الصعيد الوطني[14]

استحدث الاتحاد الدولي للاتصالات أداة تساعد على تقييم الجهود الوطنية بهدف حماية الفضاء السيبراني وضمان أمنه. وتهدف هذه الأداة إلى مساعدة الشعوب على تنظيم الجهود الوطنية لدرء الأخطار وإدارتها، وعلى استرجاع المعلومات والنظم عند وقوع تلك الأخطار.

وقد أخذ الاتحاد الدولي للاتصالات عند استحداثه هذه الأداة في الاعتبار التباين في الإجراءات التي تضعها البلدان بهدف حماية الفضاء السيبراني من حيث قدراتها ومزاياها وخصائصها وافتقارها إلى التكامل وعدم تطبيقها في جميع الحالات.

وقد استمد الاتحاد الدولي للاتصالات فكرة هذه الأداة من التقرير المعني بالممارسات الفضلى في وضع منهجيات وطنية لحماية الفضاء السيبراني[15] الذي نشر في عام 2008. وصُمّمت الأداة بحيث تساعد

(13) مجلس أوروبا، اتفاقية بشأن الجريمة السيبرانية، بودابست، 21 تشرين الثاني/نوفمبر 2001. http://www.unicri.it/wwd/trafficking/legal_framework/docs/convention_on_cyber_crime.pdf.

(14) ITU National Cyber Security/CIIP Self-Assessment Tool, September 2008 Draft, ITU.

الحكومات الوطنية على فهم النهج الوطني المعتمد في حماية الفضاء السيبراني، وتحديد المجالات التي تستدعي بذل مزيد من الجهود الوطنية، وتحديد أولويات هذه الجهود. وتجدر الإشارة إلى أن هذه الأداة تسمح برصد التقدم المحرز في تطبيق الإجراءات المتخذة ضمن الإطار الإداري لحماية الفضاء السيبراني وتعزيز أمنه على مستوى السياسات العامة الوطنية. كما يمكن بواسطة هذه الأداة النظر في البنى التنظيمية للإطار على مستوى الأفراد والمؤسسات، والتعاون على مختلف المستويات والتنسيق وبشأن السياسات والإجراءات المتخذة. كما تحدد هذه الأداة مدى ملاءمة موارد الميزانية لمستوى الأمن والحماية المرجوين.

3- التدابير المتخذة في منظمة التعاون والتنمية في الميدان الاقتصادي

وضعت اللجنة المعنية بسياسات المعلومات والحواسيب والاتصالات[16] في منظمة التعاون والتنمية في الميدان الاقتصادي توصيات تهدف إلى تعزيز أمن البيانات وحماية الخصوصية في مجتمع المعلومات. ونشرت اللجنة عدداً من التقارير، أهمها التقرير المتعلق بالبرمجيات المغرضة وتهديدها أمن اقتصاد الإنترنت[17]، والتقارير حول السياسات العامة لحماية البنى الأساسية المعلوماتية الحرجة[18]. وأصدرت اللجنة عدداً كبيراً من التوصيات حول أمن نظم المعلومات والشبكات[19]. كما صدر عن المؤتمر الوزاري الذي عقدته المنظمة في سيول، في كوريا الجنوبية، في حزيران/يونيو 2008 توصيات بشأن مستقبل اقتصاد الإنترنت[20]. وقد تضمنت توصيات بشأن حماية البنى الأساسية للمعلومات، وحماية المستخدمين، ودعم التجارة الإلكترونية بواسطة الهاتف النقال، ومكافحة البرمجيات المغرضة، ومكافحة سرقة الهوية الرقمية.

واعتمدت منظمة التعاون والتنمية في الميدان الاقتصادي في عام 2007 توصية وتوجيهاً[21] بشأن التحقق الإلكتروني من الأشخاص الطبيعيين والاعتباريين، وتأثير التحقق الإلكتروني على تعزيز الثقة بالعمليات الإلكترونية وفي تنمية الاقتصاد الرقمي. وأشارت التوصية إلى ضرورة أن يكون التحقق حيادياً من الناحية الفنية، وذلك في سياق نظام الهوية الرقمية الذي يعتبر أهم العناصر المؤثرة على الاقتصاد الرقمي ومجتمع العلومات. وتؤكد التوصية على دعم البلدان الأعضاء استخدام توقيعات إلكترونية محايدة ومكافئة للتوقيعات اليدوية على الورق. ونصت التوصية على عدد من مبادئ التحقق في المعاملات الإلكترونية والاتصالات بين الحكومات والمؤسسات، وكذلك بين هذه الجهات والأفراد، وفي ما بين الأفراد. وتقسم المبادئ الى الفئتين التاليتين:

---

(15) ITU Study Group Q.22/1 *Report on Best Practices for a National Approach to Cybersecurity: A management Framework for Organizing National Cybersecurity Efforts*. http://www.itu.int/ITU-D/cyb/cybersecutiry/docs/itu-draft-cybersecurity-framework.pdf.

(16) Information, Computer and Communications Policy Committee (ICCP-OECD). http://www.oecd.org/dataoecd/18/39/37328586.pdf.

(17) Malicious Software (Malware): A Security Threat to the Internet Economy. http://www.oecd.org/dataoecd/53/34/40724457.pdf.

(18) The Development of Policies for the protection of Critical Information Infrastructures (CII). http://www.olis.oecd.org/olis/2006doc.nsf/linkto/dsti-iccp-reg(2006)15-final.

(19) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_37441,00.html.

(20) Recommendations and reports for the Seoul Ministerial on the Future of the Internet Economy. http://www.oecd.org/document/54/0,3343,en_2649_34255_40898870_1_1_1_1,00.html.

(21) *OECD Recommendation on Electronic Authentification and Guidance for Electronic Authentification*.

(أ) المبادئ الأساسية: وتضم مختلف أساليب التنظيم المعتمدة لضمان التأمين الشامل، وتقدير المخاطر، وتوزيع المسؤوليات والمخاطر بين الأطراف بالتناسب ووفقاً للمعرفة المفترضة، والقدرة على التحكم والتوجيه، وتحديد الأدوار والمسؤوليات وتوزيعها، ومعرفة كل طرف لدوره، وتوزيع مسؤوليات بناء الأمن والثقة وإدارة المخاطر، وضرورة احترام الخصوصية وحماية البيانات الشخصية؛

(ب) المبادئ العملية: وتشمل الجوانب العملية للاستخدام أي الحرص على فعالية التحقق الإلكتروني وسهولة استعماله وموثوقيته، وملاءمته للغرض المستخدِم له، وعلى استمرار الأعمال ومعالجة الأعطال. وتنص هذه المبادئ على ضرورة وضع خطط للتوعية والتدريب، وآليات للإفصاح عن المعلومات وتبادلها، وآليات للتعامل مع الشكاوى، وأخرى للتقييم والمراجعة المستقلة بهدف التحقق من سلامة النظم، وذلك طبقاً للمعايير الدولية ذات الصلة. كما تنص هذه المبادئ على وضع منهجيات للتعامل مع التحقق الإلكتروني عبر الحدود السياسية وفقاً لمعايير التشغيل المتبادل، وتفعيل المواصفات والمعايير القياسية لضمان حد أدنى من التبادل بين مزودي الحلول ومزودي الخدمات.

4- الجمعية العامة للأمم المتحدة

صدر عن الجمعية العامة للأمم المتحدة عدد من القرارات حول أمن المعلومات، وكان أبرزها القرار 63/55 المتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[22]. ويدعو هذا القرار الدول إلى اتخاذ عدة تدابير، ومنها ما يلي: تنسيق التعاون في ما بينها في مجال إنفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية؛ وتبادل المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية؛ وتدريب العاملين في مجال إنفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية. ووفقاً للقرار أيضاً، ينبغي للنظم القانونية أن تحمي سرية البيانات ونظم الحواسيب وسلامتها وتوفرها، من أي عرقلة غير مأذون بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية؛ وأن تسمح بحفظ البيانات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة. كما ينبغي لنظم المساعدة المتبادلة أن تضمن التحقيق في الوقت المناسب في إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وجمع الأدلة في مثل هذه الحالات وتبادلها في الوقت المناسب.

(22) الأمم المتحدة، قرار الجمعية العامة 63/55 المؤرخ 22 كانون الثاني/يناير 2001 بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، (A/RES/55/63).

ثانياً- الإطار الوطني لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها

مع اتساع نطاق انتشار التهديدات المعلوماتية، مثل الفيروسات والبرمجيات الخبيثة، والهجوم على الشبكات، وتخريب المعلومات، ونشر المحتوى غير اللائق، وتعدد أنواع هذه التهديدات وتفاقم خطورتها، ينبغي أن تتخذ البلدان التدابير اللازمة لحماية البنى الأساسية والنظم المعلوماتية على مستويات ثلاثة، أولها البنى والشبكات والنظم المعلوماتية الوطنية الحرجة، وتليها الشبكات والنظم المعلوماتية في القطاعين العام والخاص، ومن ثم الشبكات والنظم المعلوماتية المخصصة للاستخدام الفردي أو العائلي.

ونستعرض فيما يلي هذه المستويات الثلاثة حسب أهمية الحماية والأمن فيها:

1- المستوى الأول: **وهو يضم البنى والشبكات والنظم الأساسية الحرجة في الدولة،** أي شبكات الاتصالات الأساسية، والشبكات والنظم المعلوماتية المستخدمة من أجل إدارة بعض القطاعات الأساسية كالكهرباء والنقل، والشبكات الخاصة بالمعلومات الصحية حول المواطنين. ويُعتبر المساس بهذه النظم خطراً على الأمن القومي، وعلى تأمين الخدمات الأساسية للمواطن.

2- المستوى الثاني: **وهو يضم الشبكات والنظم والمعلومات التابعة لمؤسسات القطاع الحكومي أو شركات القطاع الخاص.** وبما أن هذه الفئة تقدم في حالات معينة بعض الخدمات إلى المواطن باستخدام شبكاتها الخاصة، فقد تتعرض بالتالي إلى تهديدات معلوماتية خارجية تؤثر على سير عمل النظام المعلوماتي داخل المؤسسة أو الشركة، وعلى خدماته الإلكترونية.

3- المستوى الثالث: **وهو يضم الشبكات والنظم المعلوماتية المخصصة للاستخدام الفردي أو العائلي، أو للاستخدام في الشركات الصغيرة.** وتؤثر التهديدات المعلوماتية في هذه الحالة على حاسوب الفرد أو العائلة أو الشركة الصغيرة، وعلى شبكتها ومعلوماتها الخاصة.

ويساعد التقسيم أعلاه في تحديد درجة خطورة التهديدات المعلوماتية على البنى والنظم المعلوماتية وبالتالي في تبيان أهمية حماية البنى الأساسية والنظم والمعلومات، كما أنه يساعد على تحديد المسؤوليات. فحماية النظم الحرجة في الدولة وضمان أمنها مسألة وطنية تقع بشكل رئيس على عاتق الدولة ومؤسساتها المعنية بهذه النظم، ويجب أن تتضافر الجهود الوطنية لحماية هذه البنى والنظم المعلوماتية من التهديدات الخارجية مهما كان نوعها. وأما حماية النظم والمعلومات التابعة لمؤسسات القطاع الحكومي أو شركات القطاع الخاص وتعزيز أمنها فتقع بشكل رئيس على عاتق المؤسسات والشركات المعنية بهذه النظم والمعلومات، علماً أن التعاون ضروري لتبادل الخبرات واعتماد المعايير نفسها في الحماية والأمن، واعتماد استراتيجيات متجانسة من أجل بناء ثقة المواطن باستعمال الخدمات الإلكترونية التي تقدمها هذه الشركات. وأما حماية النظم المعلوماتية المخصصة للاستخدام الفردي أو العائلي، أو للاستخدام في الشركات الصغيرة فتقع على عاتق مستخدميها، إنما يبقى على الدولة والمؤسسات التعليمية أن تُعنى بتوعية الأفراد وتدريبهم ومساعدتهم على حماية نظمهم الشخصية.

يتناول هذا الفصل الإطار الوطني لبناء الثقة باستخدامات تكنولوجيا المعلومات والاتصالات والخدمات الإلكترونية. وهو يبين ضرورة وضع استراتيجية وطنية لتحفيز الاستثمار الآمن في تكنولوجيا المعلومات والاتصالات ودعمه، ويحدد المكونات الأساسية لهذه الاستراتيجية، ودور أصحاب المصلحة فيها.

ثم يقترح اتخاذ إجراءات استراتيجية وطنية على الصعيد الوطني أو على صعيد المؤسسات للتشجيع على استخدام تكنولوجيا المعلومات والاتصالات في المجالات الاقتصادية والاجتماعية والثقافية، وعلى تطويرها. وبهدف توضيح التوجهات والإجراءات الوطنية اللازمة، يشير هذا الفصل إلى تجارب بعض البلدان في مجال بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها.

ويقترح هذا الفصل اتخاذ مبادرات وإجراءات على المستوى الوطني لحماية الفضاء السيبراني، وبناء ثقة المواطن به وتعزيز أمنه. أما الفصول التالية فتشير إلى المكونات الأساسية الأربعة لبناء الثقة بتكنولوجيا المعلومات والاتصالات واستخداماتها وتعزيز أمنها. وتجدر الإشارة إلى أن هذا الفصل يعتمد جزئياً على الإطار الذي وضعه الاتحاد الدولي للاتصالات بشأن الأمن السيبراني[23] (انظر الفصل الأول من هذه الدراسة)، وعلى دليل الإسكوا التوجيهي لصياغة وتنفيذ سياسات واستراتيجيات تكنولوجيا المعلومات والاتصالات[24]. وتشير الفقرة الرابعة من هذا الفصل إلى عدد من المبادرات الوطنية الناجحة في تونس واليابان.

ألف- صياغة استراتيجية وطنية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها

لا شك في أن صياغة استراتيجية وطنية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها أمر ضروري على المستويين الوطني والمؤسسي من أجل تحديد الخطوط العامة للدولة وتوجهاتها في هذا المجال، وتشجيع مختلف أصحاب المصلحة في مجتمع المعلومات على اتخاذ الإجراءات الكفيلة بكسب ثقة المواطنين بالخدمات الإلكترونية. كما يساعد وضع استراتيجية وطنية على تحديد الجهات المعنية بتنفيذ هذه الإجراءات وإيضاح دورها ومسؤولياتها، بحيث لا تتحمل الدولة وحدها هذه المسؤولية، خصوصاً مع تنامي دور القطاع الخاص في بناء مجتمع المعلومات في المنطقة العربية.

1- الرؤية والأهداف

ينبغي أن توضح الاستراتيجية الرؤية والأهداف الوطنية المتصلة ببناء الثقة بالخدمات الإلكترونية وتعزيز أمنها، بحيث تبين الأهداف والنتائج التي تسعى الإدارة السياسية والقيادة العليا إلى بلوغها. ولذلك، يجب أن تكون تلك الاستراتيجية خاصة ببناء الثقة بالخدمات الإلكترونية وتعزيز أمنها. ويتعين أن تشير الرؤية والأهداف إلى أن الاستراتيجية تشمل فعلاً المستويات الثلاثة المبينة في المقدمة، وهي المستوى الوطني والمستوى المؤسسي ومستوى الأفراد، وأن تعنى بجميع القطاعات وخاصة القطاعات الاقتصادية والاجتماعية والثقافية والعلمية. كذلك يجب أن تتضمن الاستراتيجية أهدافاً وتوجهات ومحاور عمل تهدف إلى حماية البنى الأساسية الحرجة في الدولة وإلى ضمان أمنها، لأن حماية الفضاء السيبراني ضرورية لحماية الأمن القومي والازدهار الاقتصادي في البلد.

ويجب أن تأخذ الاستراتيجية الوطنية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها الاستراتيجيات الوطنية الأخرى في الاعتبار، وخصوصاً استراتيجية تكنولوجيا المعلومات والاتصالات، والاستراتيجية

(23) *Management Framework for Organizing National Cybersecurity/CIIP Efforts*، مرجع سبق ذكره.

(24) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، دليل توجيهي لصياغة وتنفيذ سياسات واستراتيجيات تكنولوجيا المعلومات والاتصالات، 12 شباط/فبراير 2007، E/ESCWA/ICTD/2007/2.

الأمنية، والاستراتيجيات التنموية. ونظراً إلى الطبيعة الكونية والشاملة التي يتميز بها مجتمع المعلومات، يستحسن أن تكون الاستراتيجية الوطنية ملائمة للتوجهات العالمية في مجال بناء أمن الخدمات الإلكترونية ولنتائج المؤتمرات العالمية في هذا الخصوص.

ومن المجدي أن تتضمن هذه الاستراتيجية توصيفاً للوضع الراهن على صعيد استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها في الأنشطة الاقتصادية والاجتماعية والثقافية. وقد يتضمن هذا التوصيف حالة حماية البنى والنظم المعلوماتية الوطنية وأمنها، وحماية شبكات الاتصالات المعتمدة التي تُعتبر العمود الفقري للبنى والنظم القائمة على الصعيد الوطني. ويمكن أن يتضمن التوصيف كذلك بيانات ومعلومات إحصائية حول التهديدات المعلوماتية الخارجية والآليات والمنهجيات المعتمدة وطنياً للوقاية منها. من جهة أخرى، يجب أن يتضمن التوصيف التشريعات السيبرانية المعتمدة التي تؤمن الحماية القانونية للمواطن من التهديدات المعلوماتية، ومن سوء استخدام تكنولوجيا المعلومات والاتصالات بالشكل الذي يمس أمنه ومعلوماته. ويمكن الاستفادة من الأداة التي استحدثها الاتحاد الدولي للاتصالات[25] من أجل تقييم الوضع الراهن على المستوى الوطني.

2- محاور الاستراتيجية الوطنية

بهدف تخطي الإشكاليات التي تواجه الاستخدام الآمن لتطبيقات تكنولوجيا المعلومات والاتصالات، وفي ضوء تجارب البلدان والإرشادات والتوجيهات الصادرة عن منظمات دولية وإقليمية، يمكن تلخيص المسائل التي ينبغي معالجتها في الإطار الوطني لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها ضمن خمسة محاور أساسية للاستراتيجية الوطنية المقترحة، وهي كما يلي:

(أ) حماية البنى الأساسية الحرجة في الدولة

يحدد هذا المحور البنى الأساسية الحرجة في الدولة والمستوى المطلوب من الحماية، والمنهجيات والآليات التي ستُتبع لتأمين هذه الحماية. ويجب أن يحدد كذلك الجهة أو الجهات المسؤولة عن حماية البنى الأساسية الحرجة ودعمها وطنياً. وغالباً ما تشارك في هذه المسؤولية وزارة تكنولوجيا المعلومات والاتصالات ووزارة الداخلية والجهات الأمنية في الدولة، بالإضافة إلى جهات تمثل القطاعات المهمة في الدولة، مثل المصارف وقطاع الصحة وقطاع الكهرباء. ومن المجدي إنشاء لجنة عليا من أصحاب القرار والخبراء المحليين للإشراف على تنفيذ الخطط الهادفة إلى حماية البنى الأساسية الحرجة في الدولة.

ويمكن أن تنشئ الدولة مراكز خاصة بطوارئ الحاسوب، على غرار ما قام به عدد من البلدان المتقدمة والعربية . وتُعتبر مراكز طوارئ الحاسوب بشكلها المتكامل من أشهر الآليات المعتمدة في حماية تلك البنى الأساسية الحرجة، وتنسيق التعاون على الصعيدين الوطني والدولي في مجال حماية الفضاء السيبراني وتعزيز أمنه.

(25) International Telecommunications Union, National Cyber Security/CIIP Self-Assessment Tool، مرجع سبق ذكره.

وتهدف المراكز الوطنية للاستجابة لطوارئ الحاسوب عموماً إلى الوقاية من أخطار الفضاء السيبراني والتصدي لها والحماية منها[26]. كما تهدف إلى إعلام الأفراد والمؤسسات والشركات العاملة في الدولة بآخر المستجدات حول التهديدات الخارجية، والأخطار المعلوماتية، وكيفية الحماية منها أو معالجتها. وتعتبر هذه المراكز الجهة المركزية لتجميع المعلومات عن الأخطار المحتملة وتحليلها، وإصدار تقارير دورية بشأنها. وتسعى هذه المراكز إلى رفع مستوى الوعي والمعرفة على الصعيد الوطني بأخطار أمن المعلومات والشبكات، كما تقوم بتدريب الأخصائيين على حماية بنى تكنولوجيا المعلومات والاتصالات ونظمها ومعلوماتها، وعلى مواجهة الأخطار الحاسوبية والشبكية.

ويَعد النموذج الذي وضعته الولايات المتحدة الأمريكية من النماذج الناجحة عالمياً في هذا الصدد. فقد أنشأت فريقاً وطنياً مركزياً تابعاً لوزارة الأمن الداخلي، يَعرف بفريق الجهوزية لطوارئ الحاسوب [27]. ويعمل هذا الفريق مع العديد من الفرق المنتشرة في المرافق الحكومية الحيوية والجامعات ومراكز البحث والشركات المتخصصة، وينسق معها. وفي أستونيا، كان لفريق الاستجابة لطوارئ الحاسوب فضل كبير في التعامل مع الحرب الإلكترونية التي تعرض لها هذا البلد، بدءاً بمرحلة المراقبة والتحليل، ووصولاً إلى قيادة الجهود والتعبئة العامة والتنسيق على المستويين الوطني والدولي للتغلب على الهجمات.

(ب) حماية الشبكات وتطبيقات المؤسسات

ينبغي أن تضع الاستراتيجية توجيهات لمؤسسات القطاع العام وشركات القطاع الخاص حول حماية الشبكات والتطبيقات الحاسوبية من الأخطار الداخلية والخارجية، وأن تشدد على ضرورة حماية الخدمات الإلكترونية الموجهة إلى المواطنين أو الشركاء الخارجيين.

وينبغي أن تقوم إحدى الجهات المعنية بالإشراف على قطاع تكنولوجيا المعلومات والاتصالات، مثل وزارة تكنولوجيا المعلومات والاتصالات أو مركز طوارئ الحاسوب، بتوجيه المؤسسات والشركات حول كيفية حماية النظم والشبكات المعلوماتية وضمان أمنها. ويمكن أن تقوم بذلك عن طريق نشر أدلة حول البرمجيات المتوفرة للحماية، والحماية المطلوبة على المستوى الوطني، والمعايير الدولية والوطنية المعتمدة لحماية الشبكات والنظم المعلوماتية والحفاظ على أمنها.

وبإمكان القطاع الخاص أن يضطلع بعدة أدوار في هذا الصدد. فيمكنه مثلاً أن يساهم في وضع حلول برمجية مرنة تتجاوب مع المستجدات التكنولوجية من أجل حماية النظم المعلوماتية، أو أن يؤدي دوراً في استخدام برمجيات الحماية والأمن التي تنتجها الشركات العالمية للمؤسسات، وتطبيقها وتحديثها. ويمكن أن يؤدي مركز طوارئ الحاسوب دوراً أساسياً في التنسيق والتعاون على المستوى الوطني، وفي توجيه مؤسسات القطاعين العام والخاص في ما يتصل بحماية شبكاتها ونظمها ومعلوماتها وأمنها. ويتناول الفصل الرابع بالتفصيل الأخطار المحيقة بالشبكات والنظم الحاسوبية، وكيفية التصدي لها من الناحية الفنية، كما يشير إلى عدد من المعايير الدولية المعتمدة.

(26) ITU, Case Study on National Cybersecurity Strategy: Qatar, February 2008. http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/huth-incident-management-qcert-doha-feb-08.pdf, http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf.

(27) US CERT. National Cyber Alert System. http://www.uscert.gov/.

(ج) التشريعات السيبرانية

لا تكفي الحماية الفنية من الأخطار والتهديدات الخارجية في مجتمع يعتمد بشكل متزايد على تكنولوجيا المعلومات والاتصالات في جميع أنشطته الحيوية من اقتصادية واجتماعية وثقافية وسياسية. فلا بد من وجود إطار قانوني يجرم الاختراقات المعلوماتية، ويحارب الاستخدام غير المشروع لهذه التكنولوجيا، سواء كان اختراقاً لسرية تبادل المعلومات وحريتها بواسطة الاتصالات الإلكترونية، أم استخداماً غير مشروع للبيانات الشخصية، أم تحريضاً على اقتراف عمل إرهابي باستخدام تكنولوجيا المعلومات والاتصالات.

وقد حددت دراسة الإسكوا حول التشريعات السيبرانية[28] المحاور الأساسية التي يجب إدراجها في قانون موحد للتشريعات السيبرانية أو في قوانين منفصلة ومتجانسة. وهذه المحاور هي كما يلي: (1) حماية البيانات الشخصية وحماية معالجتها؛ (2) حرية المعلومات وسريتها وحق الوصول إلى المعلومات؛ (3) حماية الملكية الفكرية والصناعية؛ (4) المعاملات الإلكترونية والتوقيع الإلكتروني؛ (5) التجارة الإلكترونية والتعاقد الإلكتروني؛ (6) الجرائم السيبرانية. ويجب أن تشدد الاستراتيجية الوطنية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها على ضرورة سن قوانين تغطي هذه المحاور الستة.

ومن المجدي أن تحدد الاستراتيجية الجهات المعنية بوضع التشريعات السيبرانية، وأن تحث على الإسراع بإصدار هذه التشريعات وتطبيقها نظراً إلى تأثيرها الإيجابي على حماية مستخدمي الفضاء السيبراني. ولهذا الغرض، لا بد من التعاون والتفاعل بين عدد من الوزارات في الدولة، وعلى رأسها وزارتا العدل والوزارة المسؤولة عن تكنولوجيا المعلومات والاتصالات، وغيرها من الوزارات مثل وزارة الاقتصاد المعنية بقانون التجارة الإلكترونية. ويتناول الفصل الثالث بالتفصيل أهمية وضع التشريعات السيبرانية ومحتواها.

(د) التوعية والتدريب لبناء الثقة باستخدام تكنولوجيا المعلومات والاتصالات وتعزيز أمنها

تعتبر التوعية بالأخطار المعلوماتية من أهم محاور الاستراتيجية الوطنية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها. وقد خصتها حكومات البلدان المتقدمة والنامية باهتمام خاص من أجل تثقيف المستخدمين وتوعيتهم بالمخاطر التي قد تواجههم عند استخدام تطبيقات الفضاء السيبراني، خصوصاً مع تزايد التطبيقات التي تجذب اهتمام المستخدمين العاديين وفضولهم، ومنها الشبكات الاجتماعية مثل Facebook وMyspace.

ولا تقتصر برامج التوعية على توعية الأفراد فقط، بل تستهدف أيضاً العاملين في الشركات المتوسطة والصغيرة وفي القطاع الحكومي. فينبغي لبرامج التوعية أن تتوافق واحتياجات كل مستخدم، ودرجة استثماره النظم المعلوماتية والمعلومات المتوفرة على هذه الشبكات.

وينبغي تخصيص أحد برامج التوعية لتعزيز إدراك أصحاب القرار بأهمية حماية النظم الحاسوبية وضمان أمنها، وضرورة حماية المعلومات المتوفرة في هذه النظم، ووضع إجراءات ترعى تداولها داخلياً

(28) الإسكوا، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، 27 حزيران/يونيو 2007، E/ESCWA/ICTD/2007/8.

وتبادلها مع العالم الخارجي. ويتعين أن تشمل برامج التوعية هذه طرق التفاعل مع الفضاء السيبراني، مثل عدم تزويد الآخرين بمعلومات شخصية حساسة، والتعامل الأخلاقي مع الفضاء السيبراني، وإبلاغ المؤسسات المزودة للخدمات الإلكترونية بالمشاكل التي تعترض استخدام هذه التطبيقات.

وبالإضافة إلى برامج التوعية، يجب أن تشير الاستراتيجية إلى ضرورة تأهيل اختصاصيين في مجال حماية النظم المعلوماتية وضمان أمنها، ووضع برامج تدريبية مهنية عالية المستوى تواكب التطورات التكنولوجية والاحتياجات الأمنية في مختلف النظم المستخدمة وطنياً. ويمكن أن تقوم الجامعات ومراكز التدريب المهني وشركات القطاع الخاص المتخصصة في الحلول الأمنية بدور هام في هذا الصدد. ويتناول الفصل الخامس بالتفصيل التوعية والتدريب اللازمين لحماية مجتمع المعلومات وتعزيز أمنه.

(•) بناء ثقة المستخدمين بالخدمات الإلكترونية

يحتاج الأفراد وأصحاب الأعمال الراغبون في استعمال الخدمات الإلكترونية إلى الشعور بالطمأنينة حيال استخدامها، خصوصاً عندما يُطلب منهم إدخال معلومات شخصية. فالعوامل النفسية هي التي تشجع الإنسان أو تكبحه عند إدخاله بيانات شخصية. وتشير الدراسات إلى أن هذه العوامل مرتبطة بثقة المستخدم بالتطبيق المستعمَل، وبالموقع الإلكتروني، وبالمؤسسة التي تقدم الخدمة. كما أنها ترتبط بثقته باستخدام التكنولوجيا كأداة لتخزين معلوماته ومعالجتها ونقلها والتصرف بها، بعلمه أو بغير علمه، وبثقته بالأشخاص الذين يديرون النظم الحاسوبية ويطلعون على المعلومات الشخصية. ويتناول الفصل السادس بالتفصيل هذه العوامل الإنسانية وكيفية معالجتها.

ولبناء ثقة المستخدمين بالخدمات الإلكترونية، ينبغي أن تشير الاستراتيجية إلى أهمية هذه الثقة، وأن توجه انتباه مزودي الخدمات في القطاعين العام والخاص إلى ضرورة مراعاة القواعد والشروط الخاصة بحماية المواطنين وأمنهم، وبشفافية التعامل، وبضرورة استثمار الخدمات الإلكترونية وفق منهجيات مهنية لا تؤثر سلباً على حماية بيانات المواطن وكسب ثقته.

3- أدوار مختلف أصحاب المصلحة في بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها

يتطلب بناء الثقة بتكنولوجيا المعلومات والاتصالات واستخداماتها المتعددة وتعزيز أمنها تعاوناً بين جميع أصحاب المصلحة في مجتمع المعلومات، وتضافر الجهود من أجل حماية البنى الأساسية والنظم والمعلومات، وتشجيع الأفراد على استخدام التطبيقات الإلكترونية بطمأنينة. فذلك كله يعزز تطوير التطبيقات، ويساهم في تطوير مجتمع المعلومات.

وينبغي أن تحدد الاستراتيجية الوطنية أصحاب المصلحة الأساسيين المعنيين بتنفيذها. وتختلف هذه الجهات بين دولة وأخرى وفقاً لبنيتها التنظيمية الإدارية والمسؤوليات الموكلة إلى مختلف هيئاتها. ويصعب بالتالي تحديد تلك الجهات ضمن هذه الدراسة، ولكن من الطبيعي أن تكون الوزارة المسؤولة عن تكنولوجيا المعلومات والاتصالات معنيةً بحماية البنى الأساسية للاتصالات وأمنها، وأن تكون وزارة العدل مسؤولة، بالتعاون مع جهات أخرى، عن وضع القوانين والتشريعات السيبرانية. وتكون وزارة الداخلية عادة مسؤولة عن ضمان أمن المعلومات الشخصية المتعلقة بالمواطنين وحمايتها. كما تكون كل وزارة مسؤولة عن

ضمان أمن الشبكات والنظم والمعلومات الخاصة بها وعن حمايتها في غياب جهاز مركزي وطني للمعلومات.

(أ) دور الدولة

تؤدي الدولة دوراً أساسياً في حماية مواطنيها من التهديدات الإلكترونية الخارجية، وتساهم بذلك في بناء فضاء سيبراني كوني آمن. والدولة هي المسؤولة الأساسية عن تحديد الاستراتيجية الوطنية المتعلقة بأمن الفضاء السيبراني وحمايته وعن الإشراف على تنفيذها. وعندما تضع الدولة السياسة الوطنية لحماية الشبكات والنظم المعلوماتية الوطنية وتعزيز أمنها، عليها أن تحدد مستوى الأخطار الإلكترونية الذي تقبل أن يتعرض له المواطنون وأصحاب الأعمال فيها. ويجب أن تحدد الدولة إطاراً للتعاون الدولي من أجل حماية الفضاء السيبراني على المستويات الوطنية والإقليمية والدولية.

وفي المجال التشريعي، تُعتبر وزارات الدولة وأجهزتها المسؤولة الرئيسة عن وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية. ويشارك الدولة في وضع هذه التشريعات ذوو الخبرة في القطاع الخاص وفي مؤسسات المجتمع المدني، كما يجري الاسترشاد بالخبرات والتجارب والمبادرات الدولية ذات الصلة.

والدولة مسؤولة عن وضع الإطار التنظيمي لحماية أمن الفضاء السيبراني على المستوى الوطني، وعن إنشاء البنى التنظيمية والفنية الملائمة لتعزيز الثقة بالمداولات الإلكترونية، مثل هيئات اعتماد التوقيع الإلكتروني، ومراكز الجدارة الائتمانية. وهي مسؤولة، بالمشاركة مع مراكز البحوث والقطاع الخاص، عن وضع حلول وطنية لحماية الهوية الرقمية، مثل البنية الأساسية للمفتاح المعلن.

والدولة هي المسؤولة عن تأمين حماية البنى الأساسية الحرجة في الفضاء السيبراني والنظم المشغلة لنظام تكنولوجيا المعلومات والاتصالات على الصعيد الوطني، وتقع على عاتقها مسؤولية تأمين حماية هذه البنى الوطنية وضمان أمنها وموثوقيتها. كما أن الدولة مسؤولة عن توجيه الجامعات والمراكز التدريبية لوضع برامج إعداد الكوادر البشرية وتنفيذها، وإتاحة الخبرات اللازمة لتوفير الحماية والأمن في استخدام تكنولوجيا المعلومات والاتصالات. والدولة مسؤولة أيضاً عن وضع خطط وحملات تهدف إلى توعية المجتمع حول الفرص والمزايا التي توفرها الخدمات الإلكترونية للأفراد والمؤسسات، وحول أهمية الأمن السيبراني في حماية تلك الخدمات، وعن تنفيذ تلك الخطط والحملات.

(ب) دور القطاع الخاص

يضطلع القطاع الخاص أيضاً بدور رئيس في بناء الثقة بالخدمات الإلكترونية التي يقدمها مباشرة إلى المواطنين أو عبر إعداده تطبيقات الخدمات الإلكترونية لصالح القطاع العام، وفي ضمان أمن هذه الخدمات. ويَعتبر القطاع الخاص، بشركاته ومؤسساته وخدماته، عنصراً أساسياً في بناء مجتمع المعلومات وتطويره في البلدان المتقدمة والنامية على السواء. وتجدر الإشارة إلى الدور الهام الذي يؤديه مزودو خدمات الإنترنت ومقدمو المعلومات في مراكز البيانات، في القطاعين العام أو الخاص، في حماية النظم المعلوماتية، والمعلومات المخزنة فيها أو العابرة بها.

ونظراً إلى الخبرات التي يملكها القطاع الخاص وإلى مرونته في التعامل مع التكنولوجيا المتطورة باستمرار، يمكنه القيام بدور هام في تقييم التكنولوجيا الجديدة واعتمادها على المستوى الوطني، وفي تقييم الأخطار المعلوماتية المتجددة وإيجاد الحلول الفنية والتنظيمية لمواجهتها.

ونظراً إلى التعقيد الذي تتميز به البرمجيات الخاصة بحماية البنى والنظم المعلوماتية، تسند المؤسسات في معظم البلدان المتقدمة أو النامية مسؤولية حماية نظمها المعلوماتية إلى القطاع الخاص الذي يتمتع بالكفاءة والمرونة اللازمتين لمواكبة التطورات التكنولوجية وحمايتها. وتتعاون المؤسسات التي لا تضم أخصائيين في تكنولوجيا المعلومات والاتصالات مع القطاع الخاص من أجل حماية نظمها ومعلوماتها.

أما المؤسسات الكبيرة، ولا سيما تلك المسؤولة عن البنى الأساسية الحرجة في الدولة، فيفضل أن تضم في هيكلها الملاك الخاص بها والمسؤول عن حمايتها.

(ج) دور المؤسسات غير الحكومية

تؤدي المؤسسات غير الحكومية دوراً هاماً في بناء ثقة المواطن بالخدمات الإلكترونية، نظراً إلى أهمية دورها كوسيط بين القطاع العام والمواطنين في إطار برامج التوعية ونشر المعلومات، وفي صون حقوق المستخدمين والمستهلكين.

(د) دور المدارس والجامعات

لا شك في أن المدارس والجامعات والمراكز التدريبية قادرة على أداء دور هام في توعية الطلاب والأجهزة التعليمية والمواطنين في ما يتصل بالاستثمار الآمن لتكنولوجيا المعلومات والاتصالات وخدماتها، وفي تدريب المتخصصين في حماية البنى والنظم المعلوماتية وتعزيز أمنها. ولذلك، ينبغي أن تؤدي الجامعات دوراً أساسياً في تأهيل الكوادر المختصة بحماية الشبكات والنظم المعلوماتية وأمنها، وفي تهيئة كوادر تساهم في وضع حلول وتطبيقات وخدمات إلكترونية آمنة، ومحمية ضد الهجمات الخارجية، ومطابقة للمعايير الدولية المتعلقة بمستلزمات الثقة والأمن.

وتقع على الجامعات المسؤولية الأساسية في إجراء البحوث حول المواضيع المرتبطة بتعزيز الثقة بالخدمات الإلكترونية، ومتابعة التطورات التكنولوجية والتهديدات المترتبة عليها وكيفية الحماية منها. كما يتعين عليها أن تشارك في استثمار البرمجيات المفتوحة المصدر بغية وضع حلول محلية لحماية البنى والتطبيقات المعلوماتية الحرجة في الدولة.

4- التعاون الدولي

يكتسب التعاون على الصعيدين الدولي والإقليمي أهمية كبيرة في بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها، وذلك لأن الفضاء السيبراني بطبيعته الكونية لا يعرف حدوداً، ولأن المشاكل والتهديدات الخارجية المحيقة بالبنى الأساسية والنظم المعلوماتية هي نفسها في مختلف المؤسسات والبلدان، وبالتالي تنطبق عليها الحلول الفنية والتنظيمية ذاتها.

كذلك يكتسب التعاون على الصعيدين الدولي والإقليمي الأهمية ذاتها في مجال التشريعات السيبرانية. فتعزيز هذا التعاون، بشقيه، يحتاج إلى التزام بالاتفاقيات والمعاهدات الدولية ذات الصلة، مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية الصادرة عن مجلس أوروبا في عام 2001[29]، والتشريعين الأوروبيين لحماية البيانات والخصوصية الصادرين في عامي 1995[30] و2002[31]، والقانون النموذجي بشأن التجارة الإلكترونية الصادر عن لجنة الأمم المتحدة للقانون التجاري (الأونسيترال) في عام 1996[32]، وقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع الصادر في عام 2001[33]، واتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية الصادرة عن الأونسيترال في عام 2005[34].

وللتعاون على الصعيدين الدولي والإقليمي الأهمية الكبيرة نفسها في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية. فقد برزت أهمية التعاون والتنسيق الدولي على المستويين السياسي والفني خلال الحرب الإلكترونية التي تعرضت لها أستونيا في عام 2007، وكان لدول الجوار والدول الصديقة كالسويد والولايات المتحدة الأمريكية دوراً فاعلاً في وقف تلك الهجمات والتغلب عليها. وقد دعت ماليزيا مؤخراً إلى تضافر الجهود الدولية لمحاربة الإرهاب السيبراني، وأطلقت الشراكة الدولية المتعددة الأطراف لمكافحة أخطار الفضاء السيبراني[35] بغية تحقيق مزيد من التنسيق والتواصل والتكامل بين الخبراء في العالم في مكافحة أخطار الفضاء السيبراني.

باء- مراكز الاستجابة لطوارئ الحاسوب

تعتبر مراكز حماية الفضاء السيبراني، والمعروفة أيضاً بمراكز الاستجابة لطوارئ الحاسوب، إحدى الآليات التي تساعد على مواجهة الأخطار الرقمية للشبكات الحاسوبية. وقد تنشأ هذه المراكز للعناية بمسائل الأمن والحماية على المستوى الوطني، أو للتركيز على قطاع حساس محدد، مثل القطاع المصرفي أو قطاع الصحة أو الاتصالات. ويختلف مدى تعقد المهام التي يضطلع بها المركز باختلاف المجال الذي يُعنى به.

وتختلف تسميات هذه المراكز بين البلدان والمناطق ولكنها تتشابه من حيث المهام، ودواعي إنشائها وأنشطتها. وقد نشأت فكرة هذه المراكز في الولايات المتحدة الأمريكية[36]، وبالتحديد في جامعة كرنجي

---

(29) Council Of Europe, Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

(30) Directive 1995/46/EC of the European Parliament and the Council of 24 October 1995 on the *Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

(31) Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the *Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* (Directive on Privacy and Electronic Communications). http://www.dataprotection.ie/documents/legal/directive2002_58.pdf.

(32) http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/1996Model.html.

(33) http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/2001Model_sign.

(34) http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/2005Convention.

(35) International Multilateral Partnership Against Cyber-Terrorism or IMPACT. http://english.peopledaily.com.cn/200605/07/eng20060507_263614.html.

(36) http://en.wikipedia.org/wiki/Computer_Emergency_Response_Team.

ميلون يونيفرستي (Carnegie Mellon University) في عام 1988، إثر ظهور الديدان للمرة الأولى في إحدى شبكات شركة آي. بي. أم (IBM)، ومن ثم انتشارها عبر الإنترنت. وقد تنبهت البلدان المتقدمة عندئذ إلى ضرورة حماية شبكات الحواسيب بمختلف أشكالها من الاستخدام الخاطئ والمسيء لتكنولوجيا المعلومات والاتصالات. ودعمت الحكومة الأمريكية إنشاء أول مركز للاستجابة لطوارئ الحاسوب في الولايات المتحدة الأمريكية في جامعة كرنجي ميلون يونيفرستي، ودعت إلى نشر مراكز مشابهة في جميع أنحاء الولايات المتحدة الأمريكية.

ومع زيادة التهديدات على الشبكات الحاسوبية وتعدد أشكالها، أنشأت بلدان عديدة مراكز للاستجابة لطوارئ الحاسوب، وأصبحت هذه التسمية تقليداً وإن تفاوتت المراكز من حيث حجمها وخدماتها ومكوناتها. وتنتشر هذه المراكز اليوم في أوروبا على مستوى المؤسسات والشركات المتوسطة والكبيرة. أما في المنطقة العربية، فقد أنشأ عدد من البلدان مراكز وطنية للاستجابة لطوارئ الحاسوب، ومنها الإمارات العربية المتحدة وتونس وعمان وقطر والمملكة العربية السعودية.

وتهدف المراكز الوطنية للاستجابة لطوارئ الحاسوب عموما إلى الوقاية من أخطار الفضاء السيبراني والتصدي لها[37]. كما تسعى إلى تزويد الأفراد والمؤسسات والشركات العاملة في البلد بأحدث المعلومات حول التهديدات الخارجية والأخطار المعلوماتية، وكيفية الحماية منها أو معالجتها. وتُعتبر هذه المراكز أيضاً الجهة المركزية في الدولة، والمعنية بتجميع معلومات عن الأخطار التي تواجهها البنى الأساسية والنظم المعلوماتية الحرجة في الدولة، وبتحليل هذه الأخطار وإصدار تقارير دورية عنها. وتعمل هذه المراكز على رفع مستوى الوعي الوطني بأخطار أمن المعلومات والشبكات، وتقوم بتدريب الأخصائيين على حماية بنى تكنولوجيا المعلومات والاتصالات ونظمها ومعلوماتها، وعلى مواجهة الأخطار الحاسوبية والشبكية.

وتُسند إلى هذه المراكز الوطنية مهمة تنسيق الجهود الوطنية لحماية مصادر المعلومات الحرجة في الدولة، وتنسيق الجهود والتعاون مع القطاعين العام والخاص من أجل تحسين سبل حماية البنى الأساسية والخدمات. وتتعاون هذه المراكز عادة مع مراكز مشابهة على المستويين الإقليمي والدولي من أجل تبادل معلومات حول المخاطر ومعالجتها، كما تتبادل التجارب الناجحة والخبرات في كل ما يتعلق بأمن الفضاء السيبراني وحمايته.

وتضطلع هذه المراكز، مثل مركز قطر لأمن المعلومات[38] والمركز الوطني الإرشادي لأمن المعلومات في المملكة العربية السعودية[39]، بعدد من الأنشطة، أهمها حماية البنى الوطنية الأساسية الحرجة. ولذلك، تقوم هذه المراكز بوضع خطط العمل وتنفيذها بالتعاون مع جهات وطنية أخرى، وتدعم تطبيق القوانين والإجراءات الخاصة بالفضاء السيبراني، كما ترسم السياسة الوطنية لإدارة حماية المعلومات، وتحدد منهجية من أجل تقييم الأخطار والتخفيف من آثارها.

---

(37) *Case Study on National Cybersecurity Strategy: Qatar*. http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/huth-incident-management-qcert-doha-feb-08.pdf, http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf.

(38) http://www.qcert.org/.

(39) http://www.cert.gov.sa/.

وتنظم هذه المراكز برامج لتوعية أصحاب القرار ومؤسسات القطاعين الحكومي والخاص، وكذلك الأفراد، حول أخطار الفضاء السيبراني وكيفية حماية الحواسيب والشبكات في المؤسسات المتوسطة والصغيرة، وفي المنازل. كما تزود الفئات المجتمعية المختلفة، حسب احتياجاتها، بأدلة حول أمن الشبكات الحاسوبية والنظم المعلوماتية والمعلومات الشخصية وحمايتها، وبتوجيهات حول التفاعل مع العالم الخارجي عبر الإنترنت والبريد الإلكتروني.

وتنشئ هذه المراكز عادة موقعاً إلكترونياً يساهم في نشر المعلومات الخاصة بالتوعية حول أمن الفضاء السيبراني وحمايته. ويمكن أن يشكل الموقع الإلكتروني للمركز مخزناً ومرجعاً لحماية المعلومات وتعزيز أمنها على المستوى الوطني. ويعتبر موقع الوكالة الوطنية للسلامة المعلوماتية في تونس[40] أحد المواقع الهامة، ومرجعاً أساسياً لسلامة الفضاء السيبراني في تونس. فهو يتضمن معلومات عن الوكالة وخدماتها، والإطار القانوني المتعلق بحماية الفضاء السيبراني على المستوى الوطني في تونس، بالإضافة إلى أدوات لحماية الشبكات والمعلومات وضمان أمنها، والعديد من المنشورات الخاصة ذات الصلة. ويوفر الموقع الإلكتروني كذلك أدلة وتوجيهات للأطفال والعائلات حول حماية الحواسيب والشبكات المنزلية.

وتتعاون هذه المراكز الوطنية مع الجهات الوطنية المعنية بحماية الشبكات الحاسوبية الوطنية الحرجة وضمان أمنها. كما تتعاون مع القطاع الخاص، لا سيما مع مزودي خدمات الإنترنت ومراكز البيانات إذا وُجدت، ومع شركات المعلوماتية التي تملك حلولا لحماية البنى والنظم المعلوماتية.

كذلك تتعاون هذه المراكز مع مراكز مشابهة على المستويين الإقليمي والدولي من أجل تبادل المعلومات والحلول الفنية والإدارية والتجارب الناجحة وكذلك الخبرات والخبراء. وتسعى بعض المناطق إلى إنشاء مركز إقليمي لتنسيق الجهود على مستوى كل منطقة. وفي المنطقة العربية مثلاً، تتعاون المراكز الوطنية المعنية بأمن الفضاء السيبراني في بلدان مجلس التعاون لدول الخليج العربية، ومن المهم توسيع هذا التعاون ليشمل البلدان العربية كافة.

جيم- تجارب وطنية في مجال حماية تكنولوجيا المعلومات والاتصالات وتعزيز أمنها

1- الاستراتيجية اليابانية[41]

أدركت الحكومة اليابانية أهمية حماية مجتمع المعلومات وتعزيز أمنه، ووضعت في عام 2006 الاستراتيجية الوطنية الأولى حول أمن المعلومات تحت شعار "نحو تحقيق مجتمع جدير بالثقة"، وذلك بعد إصدارها القانون الأساسي لتكنولوجيا المعلومات والاتصالات في عام 2000. وقد نصت المادة 22 من هذا القانون على ضرورة تحقيق أمن شبكات الاتصالات والمعلومات المتقدمة.

وكانت اليابان قد أنشأت في عام 2005 المركز الوطني لأمن المعلومات الذي يعنى بتنسيق الجهود الوطنية لحماية أمن الشبكات والمعلومات الحكومية الحرجة، وبوضع الآليات، وبالإجراءات التي ينبغي أن

(40) www.ansi.tn.

(41) *The First National Strategy on Information Security. Toward the Creation of a Trustworthy Society. National Information Security Center*. http://www.nisc.go.jp/eng/index.html.

تتخذها جميع أجهزة الحكومة من أجل حماية شبكات معلوماتها وضمان أمنها، وبالتوعية والتدريب في هذا الصدد. ولكن مع تزايد ظهور الأخطار في بداية هذا القرن، وبروز العديد من المسائل المرتبطة بالسلوك الاجتماعي، وتزايد استخدام التطبيقات عبر شبكات الخدمة العريضة، أصبحت الحاجة ماسة إلى تعزيز الجهود الرامية إلى حماية الشبكات والمعلومات. وقد دفع هذا الأمر بالحكومة اليابانية إلى وضع الاستراتيجية الوطنية الأولى حول أمن المعلومات التي تمتد فترة تنفيذها على ثلاث سنوات (2006-2009).

وحددت الاستراتيجية أهدافها الأساسية، وهي خلق بيئة لتكنولوجيا المعلومات تتسم بالأمان وتتلاءم مع القانون الأساسي لتكنولوجيا المعلومات في اليابان، وإيجاد توازن بين ملاءمة التطبيقات للاستخدام من جهة، وأمنها وحمايتها من جهة ثانية. كما حددت الاستراتيجية أربعة توجهات أساسية، وهي: (أ) تعزيز القناعة المشتركة لدى المؤسسات العامة والخاصة بأهمية حماية المعلومات وضمان أمنها واتخاذ الإجراءات الكفيلة بذلك؛ (ب) متابعة التقدم التكنولوجي، والبحث والتطوير من أجل تحديد التهديدات والمخاطر الجديدة؛ (ج) تعزيز قدرة القطاع العام على مواجهة التهديدات، وخصوصا المؤسسات العامة التي تقدم خدمات إلكترونية للمواطن؛ (د) تحفيز الشراكات والتعاون على المستويات الوطنية والإقليمية والدولية في مجال حماية تكنولوجيا المعلومات والاتصالات وضمان أمنها.

وبينت الاستراتيجية أيضاً المهام الموكلة إلى مختلف أصحاب المصلحة. كذلك أشارت إلى أن الحكومة المركزية والبلديات هي المؤسسات المسؤولة عن تنفيذ الإجراءات الأمنية المتعلقة بتكنولوجيا المعلومات والاتصالات، وذلك بمشاركة المؤسسات التعليمية والبحثية وكذلك المنظمات غير الحكومية والإعلام. كما أوضحت الاستراتيجية الأولويات التي يجب التركيز عليها.

وجدير بالذكر أن الحكومة اليابانية تعمل على تقييم الاستراتيجية سنوياً، ونشر نتائج التقييم، وتحديد برنامجها وأولوياتها للسنة التالية بناءً على ذلك التقييم. وقد أجرت الحكومة اليابانية التقييم الأول في عام 2007، أي بعد وضع الاستراتيجية بسنة واحدة، وتقييماً آخر في عام 2008.

2- التجربة التونسية في مجال حماية الفضاء السيبراني[42]

تعتبر التجربة التونسية من التجارب الرائدة في المنطقة العربية في مجال حماية الفضاء السيبراني وتعزيز أمنه[43]. فقد تنبهت الحكومة التونسية منذ نهاية عام 1999 إلى أهمية حماية البنى الأساسية لتكنولوجيا المعلومات والاتصالات وأمن المعلومات[44]. فقامت وزارة تكنولوجيات الاتصال بتعيين وحدة وطنية خاصة لحماية تكنولوجيا المعلومات، وذلك من أجل توعية أصحاب القرار والكوادر الفنية حول مسائل الحماية. كما أنشأت أول مجموعة عمل وطنية للخبراء المتخصصين بحماية تكنولوجيا المعلومات ومراقبة أمن البنى الأساسية والتطبيقات الوطنية الأكثر حرجاً.

---

(42) انظر موقع وزارة تكنولوجيات الاتصال التونسية www.infocom.tn، وموقع الوكالة الوطنية للسلامة المعلوماتية (National Agency for Computer Security): www.ansi.tn.

(43) *Implementing a National Strategy: the case of the Tunisian CERT*. http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/zouari-incident-response-tunisia-doha-feb-07.pdf.

(44) http://www.ansi.tn/en/aboutnacs.htm.

وفي نهاية عام 2002، أقرت الحكومة التونسية ضرورة حماية تكنولوجيا المعلومات، واعتبرتها مكوناً أساسياً من مكونات مجتمع المعلومات. وعمدت الوحدة الخاصة إلى صياغة استراتيجية وطنية وخطة عمل في مجال حماية تكنولوجيا المعلومات، وذلك بناءً على نتائج مسح وطني ساعد في تحديد الأولويات وحجم العمل المطلوب والاحتياجات اللوجستية والأدوات المساعدة اللازمة.

وفي مطلع عام 2003، أصدر مجلس الوزراء قراراً حول المعلوماتية وأمن تكنولوجيا المعلومات. وقد نص هذا القرار على إنشاء وكالة وطنية متخصصة بأمن تكنولوجيا المعلومات، وإنشاء هيئة المراقبين المعتمدين في مجال أمن تكنولوجيا المعلومات على المستوى الوطني. كما نص على اتخاذ عدد من الإجراءات الخاصة بأمن تكنولوجيا المعلومات على المستوى الوطني. وصدر عدد من القوانين ذات الصلة، منها القانون المتعلق بالتوقيع الإلكتروني والتجارة الإلكترونية (قانون رقم 8-2000)، وقانون مكافحة الجرائم السيبرانية (قانون رقم 89-1999، البند 199)، وقانون حماية المستهلك واحترام الملكية الفكرية (قانون رقم 36-1994)، وقانون حماية الخصوصية والبيانات الشخصية (قانون رقم 63-2004).

وفي شباط/فبراير 2004، نُشِر قانون خاص بالسلامة المعلوماتية (قانون رقم 5-2004) إضافة إلى مراسيمه التشريعية الثلاثة. ويجبر هذا القانون جميع المؤسسات الوطنية على مراقبة أمن تكنولوجيا المعلومات والاتصالات وحمايتها دورياً، من خلال الاعتماد على مجموعة المراقبين المعتمدين وطنياً، وإنشاء الوكالة الوطنية للسلامة المعلوماتية تحت إشراف وزارة تكنولوجيات الاتصال. وحدد القانون المهام الأساسية التي تضطلع بها هذه الوكالة ودورها على المستوى الوطني، وطلب من جميع المؤسسات الكبيرة المستخدمة لتكنولوجيا المعلومات والاتصالات التصريح عن جميع الحوادث التي تعرض فيها أمن هذه التكنولوجيا للاختراق. كما أوكلت إلى الوكالة مهمة تقديم المساعدة الآنية لمعالجة طوارئ أمن الحاسوب والشبكات المعلوماتية، والتأكد من حماية الفضاء السيبراني الوطني مع تيسير تقديم الخدمات الوطنية الحرجة بشكل متواصل في حالات اختراق أمن الشبكات الحاسوبية، وكذلك تقديم تدريب رفيع المستوى.

وقد أُطلق فريق الاستجابة لطوارئ الحاسوب رسمياً في أيلول/سبتمبر 2005 ضمن الوكالة الوطنية للسلامة المعلوماتية، وأُسند إليه العديد من مهام الوكالة، ومن أهمها ما يلي:

(أ) الدعم في مواجهة الأخطار[45]

نص القانون رقم (5-2004) على التزام شركات ومؤسسات القطاعين العام والخاص بإعلام فريق الاستجابة لطوارئ الحاسوب في مركز التنسيق التونسي بأي خطر تتعرض له شبكاتها الحاسوبية أو فضاؤها المعلوماتي السيبراني. ويحفظ الفريق سرية هذه المعلومات، ويحاول معالجة الأخطار ومتابعة تقديم جميع الخدمات الحرجة التي تحددها الدولة، مثل شبكة الاتصالات وشبكة الكهرباء. وقد استُحدثت خدمة خط الاتصال العاجل، وهي تقدم الخدمات على مدار الساعة وطيلة أيام الأسبوع، وتمكن الفنيين والشركات والمؤسسات من إعلام فريق الاستجابة لطوارئ الحاسوب في مركز التنسيق التونسي بالأخطار فور حدوثها. كما أنشأ الفريق مكتب المساعدة الوطنية من أجل مساعدة جميع المستخدمين، بمن فيهم الأشخاص في المنازل، على حماية حواسيبهم وأنظمتهم الحاسوبية من الأخطار الخارجية، عبر الاتصال الهاتفي، أو

(45) http://www.ansi.tn/en/about_cert-tcc.htm، مرجع سبق ذكره.

بإحضار حاسوبهم الشخصي إلى المكتب حيث يتم تزويده بالأدوات المساعِدة اللازمة، أو تصليحه في حال وجود أعطال.

واستحدث فريق الاستجابة لطوارئ الحاسوب في مركز التنسيق التونسي نظام ساهر (Saher) الذي يجيز توقع الأخطار المحيقة بشبكات الاتصالات والبنى الأساسية للفضاء السيبراني المحلي وتقييمها. وقد استُحدِث هذا النظام بالاعتماد على أدوات وبرمجيات المصدر المفتوح. وهو يسمح برصد أمن الفضاء السيبراني المحلي بالزمن الحقيقي والتصدي للهجمات العنيفة وهي بعدُ في مراحلها الأولى.

وأعد الفريق خطة للتصدي سريعاً للهجمات القوية التي قد تطال الفضاء السيبراني. وتقوم الخطة على إنشاء خلايا متناسقة للطوارئ على جميع المستويات ولجميع الجهات الفاعلة والمؤثرة في شؤون الفضاء السيبراني، مثل شركات تقديم خدمات الإنترنت ومزودي الاتصال وشركات الشبكات الضخمة. وتم اختبار هذه الخطة من خلال تنظيم هجوم كبير للديدان، ثم استُخدمت لاحقاً في مناسبات عدة كانت تونس تستضيف خلالها مؤتمرات حول تكنولوجيا المعلومات والاتصالات.

(ب) التعاون على الصعيدين الدولي والمحلي

انضم فريق الاستجابة لطوارئ الحاسوب في مركز التنسيق التونسي إلى عضوية منتدى الفرق المعنية بالأمن والاستجابة للحوادث[46] في أيار/مايو 2007. وهو يتعاون مع المراكز الوطنية لطوارئ الحاسوب من أجل تطوير الإجراءات المعتمدة في معالجة الأخطار على المستويين الإقليمي والدولي، وتبادل المعلومات حول المخاطر والأحداث الطارئة، وتقديم العون في التحري عن مصادر أخطار الحاسوب. كما يشجع هذا الفريق المجتمع المحلي على إنشاء تجمعات مهنية متخصصة في أمن شبكات الحواسيب وحمايتها، ويدعم أنشطة هذه التجمعات المهنية غير الرسمية. وهو يتعاون مع القطاع الخاص ولا سيما مع الشركات التي تقدم حلولاً برمجية للتصدي للأخطار السيبرانية.

(ج) التنبيه إلى الأخطار والتوعية

يقوم فريق الاستجابة لطوارئ الحاسوب في مركز التنسيق التونسي بالتحري عن الأخطار، وجمع المعلومات المتعلقة بها ونشرها عبر إعلام مديري النظم والشبكات ومستخدميها. ويحلل الفريق الأخطار المحتملة من خلال مراقبة العديد من المصادر من أجل تحديد كيفية التصدي للأخطار المحتملة.

كذلك يسعى الفريق إلى تعزيز الوعي بالممارسات الفضلى المعتمدة في حماية النظم المعلوماتية وضمان أمنها. وقد نشر عدداً من الأدلة والتوجيهات الموجهة إلى الأفراد والمؤسسات والمسؤولين عن تشكيل النظم المعلوماتية.

(46) http://www.first.org/، مرجع سبق ذكره.

ثالثاً- المسائل القانونية المرتبطة ببناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا

يجمع الباحثون المهتمون بتطور العصر الرقمي ومجتمع المعلومات على أهمية الإطار التشريعي والقانوني في بناء الثقة بالخدمات الإلكترونية. فالثقة والأمن يمثلان أهم عوامل التحول من النمط التقليدي إلى النمط الإلكتروني في اكتساب المعلومات والمعرفة وتوظيفها، وفي أنماط الأداء المتصلة بمختلف أنشطة البيئة الرقمية، وتحديداً الأنشطة التجارية والاستثمارية[47].

ونظراً إلى أهمية تطوير مجتمع المعلومات في المنطقة العربية، والاندماج في المجتمع الدولي للمعلومات، كان لا بد من تحديد الدور الذي تؤديه التشريعات السيبرانية (بوصفها القوانين المعنية بتكنولوجيا المعلومات والاتصالات واستخداماتها المختلفة) في بناء الثقة بالفضاء السيبراني والتطبيقات والخدمات الإلكترونية المتوفرة فيه، وفي تكريس هذه الثقة. كما يجب تحديد البنية الملائمة لهذه القوانين والتشريعات، وبيان محتواها وبنودها لتحقيق الهدف المرجو منها.

وتستنتج الدراسة التي أعدتها الإسكوا حول التشريعات السيبرانية[48]، ومثلها المناقشات والاجتماعات التي نظمتها الإسكوا[49] في عامي 2007 و2008 في هذا الصدد، أن البلدان العربية في المنطقة قد بذلت جهوداً متواضعة وسنت قوانين ترعى عدداً محدوداً من مواضيع التشريعات السيبرانية. فهذه الجهود لا تزال غير كافية لبناء ثقة المستخدمين بالفضاء السيبراني في العالم العربي وضمان أمنه. ويفسر هذا الوضع جزئياً قلة التطبيقات المهنية والخدمات الإلكترونية الموجهة إلى المستخدمين في المنطقة العربية من ناحية، وعزوف المواطنين عن استخدام التطبيقات والخدمات العملية المتوفرة عبر الإنترنت من ناحية أخرى.

ويعتمد هذا الفصل النهج القائم على التحليل الوصفي، والمقارنة، والتحليل التاريخي لأن مادته تتضمن عدداً من مدونات التشريع الدولية والوطنية، وتتناول التجربة التشريعية ذات الصلة بالبيئة الرقمية عموماً وبالخدمات الإلكترونية خصوصاً. ويرتكز الفصل على تحليل التشريعات ذات الصلة وفقاً لمعايير نظرية وعملية، وعلى عدد كبير من الدراسات النظرية والحالات التطبيقية التي أنجزها بعض بلدان المنطقة خلال العقدين الأخيرين.

ألف- التشريعات السيبرانية لبناء الثقة بالخدمات الإلكترونية وتعزيز أمنها

ظهرت الحاجة إلى التشريعات السيبرانية بعد نشوء مسائل قانونية مستجدة نتيجة استخدام الحاسوب في تخزين المعلومات ومعالجتها ونشرها وإدارتها واستحصالها، ومن جراء استخدام الوسائل الرقمية والإنترنت لتقديم الخدمات الإلكترونية. وتتميز هذه القوانين بتغطيتها فروعاً قانونية عديدة ضمن تقسيمات القانون التقليدية، ومسائل التعاقد والإثبات والضرر والملكية الفكرية والمصارف والجزاء والمنازعات ومسائل أخرى.

---

(47) تستند هذه الفقرة إلى مجموعة من المصادر التي تتناول الثقة والأمن في البيئة الرقمية، وهي واردة ضمن قائمة المراجع العامة المرفقة.

(48) E/ESCWA/ICTD/2007/8، مرجع سبق ذكره.

(49) الإسكوا، تقرير اجتماع الخبراء الاستشاري حول تشريعات الفضاء السيبراني، عمان 11-12 كانون الأول/ديسمبر 2007؛ وتقرير ورشة عمل حول التشريعات السيبرانية وتطبيقها في منطقة الإسكوا، بيروت، 15-16 كانون الأول/ديسمبر 2008.

أما أبرز التحديات القانونية فقد تمثل في سوء استخدام المعلومات الذي يضر بمصالح الأفراد والمؤسسات، وفي تحديد ما إذا كانت هذه الإساءة في استخدام الحاسوب والاعتداء على البيانات بمثابة مسؤولية قانونية، أم أنها مجرد فعل غير مقبول به أخلاقياً، وما إذا كان ينبغي تنظيم استخدام الحاسوب. وقد أثيرت هذه الأسئلة في سياق الموضوعين التاليين: (أ) المسؤولية عن المساس بالأفراد والمؤسسات عند إساءة التعامل مع بياناتهم الشخصية المخزنة في نظم الحاسوب وحقهم في الخصوصية؛ (ب) المسؤولية عن الأفعال التي تمس المعلومات ونظمها أو تعتدي عليها، خصوصاً المعلومات ذات الصلة بأموال الأفراد ومصالحهم، وكذلك حق الأفراد في الوصول إلى المعلومات ذات القيمة الاقتصادية. ويشير البحث في هذين الحقلين إلى أن القوانين المعنية بهذه المسائل هي القوانين المتعلقة بالخصوصية والحق في الوصول إلى المعلومات[50] وجرائم الحاسوب والإنترنت[51].

ومع تزايد الوعي بأهمية برامج الحاسوب، شهد مطلع السبعينات جدلاً واسعاً حول موقع حماية هذه البرامج، وتساؤلات حول ما إذا كان يندرج ضمن قوانين براءات الاختراع، بوصف البرنامج من المصنفات القابلة للاستثمار الصناعي، أم ضمن تشريعات حق المؤلف، باعتبار البرنامج في الأساس ترتيباً منطقياً لأوامر مكتوبة ونتاج إبداع فكري. وتم الاتفاق على إدراج البرمجيات وقواعد البيانات ضمن قوانين حماية الملكية الفكرية المتصلة بتقنية المعلومات[52]. ويدور النقاش حالياً حول الحماية القانونية لأسماء مواقع الإنترنت ومحتواها الرقمي.

ومع استخدام تكنولوجيا المعلومات والاتصالات كوسيلة لنشر المعلومات، وتقديم الخدمات الحكومية وخدمات التجارة الإلكترونية، وإتاحة العديد من العمليات الأخرى إلكترونياً، اتضحت ضرورة وضع تشريعات أخرى. ونذكر منها على سبيل المثال التشريعات المعنية بالحق في الوصول إلى المعلومات[53]، أي معلومات السجلات الحكومية وسجلات القطاع الخاص، والتشريعات الخاصة بالمعاملات والتجارة الإلكترونية[54] بمختلف أجزائها، والتي تتضمن تسديد الفواتير إلكترونياً. وتجدر الإشارة إلى أن البلدان المتقدمة سنت عدداً من التشريعات المعنية بتقنيات الأعمال المصرفية، أو بحجية الإثبات بالوسائل الإلكترونية، وحجية مستخرجات الحاسوب، وتنظيم النقل الإلكتروني للبيانات قبل سنها التشريعات المعنية بالحقول الأخرى في المداولات الإلكترونية وذلك لأن الحاسوب يستخدم في المصارف منذ فترة طويلة. وقد تميز هذا الحقل التشريعي بوضعه مفاهيم شاملة جديدة في حقل الخدمات الإلكترونية واحتياجاتها (تحديداً التجارة الإلكترونية، والمصارف الإلكترونية، ولاحقاً في الحكومة الإلكترونية). وقد شملت هذه المفاهيم التصدي لسائر المسائل القانونية المطروحة في ميدان تكنولوجيا المعلومات والاتصالات، ومنها حماية المستهلك وتنظيم العلاقات بين المؤسسات التجارية.

---

(50) انظر مجموعة المصادر التي تتناول الخصوصية والحق في الوصول إلى المعلومات ضمن قائمة المراجع المرفقة بهذا التقرير.

(51) انظر مجموعة المصادر التي تتناول جرائم الحاسوب والإنترنت موضوعياً وإجرائياً ضمن قائمة المراجع المرفقة بهذا التقرير.

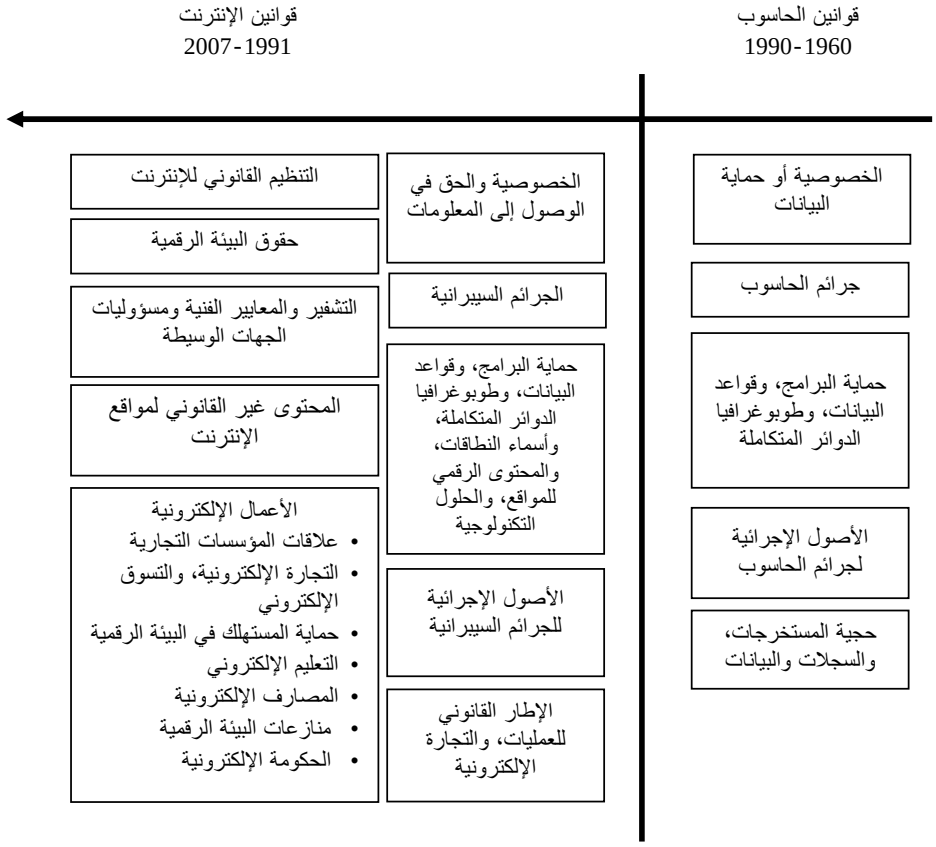
(52) انظر مجموعة المصادر التي تتناول الملكية الفكرية المتصلة بتقنية المعلومات ضمن قائمة المراجع المرفقة بهذا التقرير.

(53) انظر التذييل 50 أعلاه.

(54) انظر مجموعة المصادر التي تتناول الأعمال الإلكترونية وتطبيقاتها ضمن قائمة المراجع المرفقة بهذا التقرير.

وتؤدي حزمة تشريعات تكنولوجيا المعلومات والاتصالات دوراً حاسماً في قبول هذه التكنولوجيا وبناء الثقة بها وببيئتها وبتطبيقاتها. وهي تنظم المسائل الفنية، والنزاعات الناتجة عن الانتقال إلى الفضاء الرقمي. ولا يمكن أن يكون للخدمات الإلكترونية وجود، أياً كان التعريف المعتمد لتوصيفها، في غياب ثقة المستخدم بها ومن دون حمايته. وما من وسيلة أفضل من القانون لتوفير هكذا ثقة وحماية. فالقانون هو الأداة التي تضمن قبول الإنسان للتكنولوجيا، مع إدراكه لنتائجها، ووسائل حماية مصالحه، وسبل تفهم المسؤوليات المترتبة على إقرار القانون[55]. ويبين الشكل 1 الحركة التاريخية لنشوء قانون تكنولوجيا المعلومات والاتصالات ومواطن عمل فروعه.

الشكل 1- قانون تكنولوجيا المعلومات والاتصالات (التشريعات السيبرانية)



تتناول قوانين تكنولوجيا المعلومات والاتصالات المصالح الجديدة التي تنشأ في بيئة مجتمع المعرفة أو مجتمع المعلومات. ففي إطار الحماية القانونية للمعلومات، يجب أن يحمي القانون حق الأفراد في الوصول إلى المعلومات، وحقهم في سلامة ومشروعية التعامل مع بياناتهم الشخصية، وحقهم في الحفاظ على ثمرة إبداع عقولهم وهي مصنفة ضمن قواعد الملكية الفكرية، وحق مالكي المعلومات بأشكالها المختلفة،

(55) انظر المراجع المتخصصة بالقوانين والتشريعات السيبرانية ضمن قائمة المراجع المرفقة بهذا التقرير.

المصنفة أو الخاصة، في نشاطهم الاستثماري أو التجاري. وتتمثل هذه المصالح أيضاً في حق الفرد في سلامة المعلومات التي يتعامل معها، سواء تلك التي يرسلها أو يستقبلها، أم تلك المخزنة في النظم الحاسوبية.

ويشير تحويل هذه الحقوق إلى مسميات قانونية إلى أن بناء الثقة بالفضاء السيبراني يتطلب وضع تشريعات سيبرانية ترعى الحق في المعلومات، والحق في الخصوصية المعلوماتية أو الرقمية، والحق في حماية أمن المعلومات، والحق في حماية الإبداعات الفكرية المتصلة بتكنولوجيا المعلومات والاتصالات، والحق في إدارة المعلومات وفي الاستثمار المعلوماتي، وفي صحة الأعمال والعمليات الإلكترونية بجميع أشكالها، مع ضمان حقوق جميع المستفيدين منها والمستثمرين فيها.

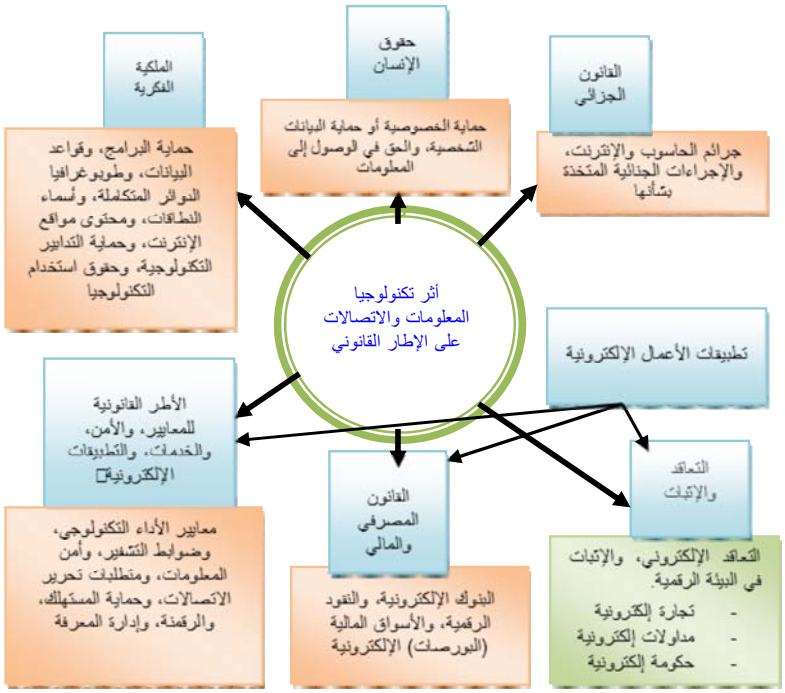
باء- علاقة قوانين تكنولوجيا المعلومات والاتصالات بالقوانين العامة الأخرى

لقد أثرت تكنولوجيا المعلومات والاتصالات وتطبيقاتها واستخداماتها على مختلف الفروع التقليدية في القانون، وأهمها قانون حقوق الإنسان، والقانون الجنائي، والقانون المدني، والقانون التجاري، وقانون الملكية الفكرية وما إليها. لذلك لا بد من إعادة تقييم القواعد القانونية والإجرائية في العديد من فروع القانون من أجل التعامل مع المستجدات في أنماط السلوك والعلاقات القانونية في البيئة الإلكترونية. فالاعتراف بالحق في الحياة الخاصة للأفراد، مثلاً، وحمايتها من مخاطر عملية جمع البيانات ومعالجتها تحتاج إلى اتخاذ تدابير تشريعية أدت إلى سن ما يُعرف بقانون الخصوصية. وإلى جانب مسألة الخصوصية طُرح موضوع الحق في الوصول إلى المعلومات، لا سيما منها محفوظات القطاع الحكومي. وهذان الموضوعان يتصلان بفرع قانون حقوق الإنسان وقواعده الدستورية.

وقد أثرت تكنولوجيا المعلومات على القواعد الموضوعية والإجرائية في القانون الجنائي، خصوصاً في ما يتعلق بحماية المعلومات وأمن نظمها. أما أبرز آثار التكنولوجيا فيتمثل في طرق التعامل مع الأنماط المستجدة من الجرائم والوسائل المتبعة لارتكاب أفعال إجرامية تقليدية في البيئة الرقمية. وتستهدف هذه الأفعال بيانات مثل مكان الجريمة، وهي تستغل التكنولوجيا كأداة لتسهيل ارتكاب الجرائم التقليدية. وقد أدى ذلك كله إلى ولادة مفهوم جرائم الحاسوب، بشقيه الموضوعي والإجرائي، وإلى تطوره لاحقاً ليصبح مفهوم الجرائم الإلكترونية أو الجرائم السيبرانية.

كما أثرت تكنولوجيا المعلومات على العلاقات التعاقدية فاستلزمت بالتالي إيجاد أنماط جديدة للتعبير عن الإرادة، والتعاقد في ميدان المعاملات المدنية والتعاملات التجارية في مختلف القطاعات. وقد أدى ذلك إلى نشوء مفهوم التجارة الإلكترونية، ومفهوم جديد عام للمعاملات بات يُعرف بالمداولات الإلكترونية، ومفهوم ونمط جديد للخدمات المصرفية والمالية بات يُعرف بالمصارف الإلكترونية. وفي هذا السياق، ظهر تأثير التكنولوجيا على سائر الخدمات الإلكترونية، وفي مقدمتها الخدمات الحكومية، وعلى العمل الحكومي وعلاقته بالأفراد والأعمال. ويبين الشكل 2 أثر تكنولوجيا المعلومات والاتصالات على القوانين التقليدية.

الشكل 2- العلاقات والقواعد والتشريعات القانونية المتأثرة بتكنولوجيا المعلومات



جيم- واقع التشريعات السيبرانية في المنطقة العربية

تناولت الدراسة التي أعدتها الإسكوا للعام 2007 حول تشريعات الفضاء السيبراني[56] واقع الحال في المنطقة العربية عموماً، وفي بلدان الإسكوا خصوصاً. كما عرضت قائمة بالتشريعات التي وضعتها المنطقة العربية. فخلال السنتين الماضيتين، قامت دول عدة بسن تشريعات وقوانين جديدة، وإعداد مسودات لمشاريع قوانين ترعى الفضاء السيبراني[57]. ويبين المرفق بهذه الدراسة الخصائص الأساسية لواقع المنطقة في نهاية عام 2008.

وفي ما يلي أبرز الاستنتاجات التي توصلت إليها الدراسة المسحية والشاملة للأدوات التشريعية ذات الصلة بالتشريعات السيبرانية القائمة في المنطقة العربية:

(أ) لم تبذل البلدان العربية جهداً كافياً في مجال القوانين والتدابير التشريعية ذات الصلة بتكنولوجيا المعلومات والاتصالات حتى الآن، ولا يزال الوعي بالدور الذي يؤديه التشريع وبأغراضه، وأدوات تنفيذه غير كاف. ولكن ينبغي ذكر الإنجازات المحرزة في عدد من المسائل الرئيسة، مثل حقوق الملكية الفكرية، التي تحققت بفضل التزام البلدان العربية الانضمام إلى منظمة التجارة العالمية، وبفضل متطلبات اتفاق

(56) E/ESCWA/ICTD/2007/8، مرجع سبق ذكره.

(57) تقرير اجتماع الخبراء الاستشاري حول تشريعات الفضاء السيبراني، مرجع سبق ذكره؛ وتقرير ورشة العمل حول التشريعات السيبرانية وتطبيقها في منطقة الإسكوا، مرجع سبق ذكره.

الجوانب التجارية لحقوق الملكية الفكرية، والإنجازات المحرزة في عدد من جوانب التجارة الإلكترونية والحكومة الإلكترونية (انظر المرفق)؛

(ب) لم تُتخذ التدابير اللازمة لتحقيق تنظيم متكامل وملائم، فمستوى التنظيم متباين بين البلدان العربية، وما من رؤية واضحة وشاملة. ويظهر توجه المؤسسات التشريعية في البلدان العربية نحو حلول جزئية لا تكفي لمواجهة التحديات الفنية والتطورات في الاحتياجات القانونية التي يفرضها العصر الرقمي؛

(ج) تفتقر بعض المساعي العربية إلى فهم حقيقي للمحتوى القانوني والتنظيمي للتشريعات السيبرانية، والقوانين والتدابير الدولية. ويظهر ذلك بوضوح عند نقل هذه القوانين وتطبيقها على المستوى المحلي. فاعتماد الحلول والتدابير القانونية الناجمة عن تجارب بلدان متقدمة سباقة في التنظيم يتطلب قراءة واعية لمدى كفاءة التطبيق استناداً إلى خصائص الواقع القانوني المحلي.

دال- الاستراتيجية التشريعية العربية المرجوة لتلبية احتياجات الخدمات الإلكترونية

ينبغي أن تتناول الاستراتيجية التشريعية المطلوبة مجموعة متكاملة من التشريعات السيبرانية، أو تشريعاً واحداً وشاملاً يتضمن أربعة عناصر أساسية:

(أ) اعتراف القانون بالمعلومات ووسائل حمايتها المدنية والجزائية في النظام القانوني. وتتضمن هذه الركيزة مجموعة من التشريعات المعنية بالأمن، والخصوصية، والسرية، وبناء قواعد البيانات، ومواقع الإنترنت، بالإضافة إلى قواعد إجرائية، وقواعد الإثبات المتصلة بالنزاعات والدعاوى الملازمة لهذه المواضيع؛

(ب) تنظيم وسائل التكنولوجيا ومعاييرها ومواصفاتها. ويشمل هذا التنظيم المسائل المتصلة بتوظيف التكنولوجيا في الخدمات الحكومية، واستثمارها، والتداول بها، وتوريد الخدمات، وضمان استدامتها إنتاجاً ونقلاً وتبادلاً. وترد في إطار هذا التنظيم قواعد المنافسة المشروعة في القطاع؛

(ج) الاعتراف القانوني بصلاحية الوسائل الإلكترونية في بيئة الأعمال والخدمات والاستثمار، أي الاعتراف بالإطار القانوني للعمليات الإلكترونية بجميع تطبيقاتها، وأهمها التجارة الإلكترونية، والحكومة الإلكترونية، والمصارف الإلكترونية، وما إليها؛

(د) الاعتراف القانوني بمصالح المستهلك أو المستخدم، وتوفير حماية قانونية له من عيوب ومخاطر التكنولوجيا وتطبيقاتها، مثل حماية سريته وخصوصيته وضمان أمنه، من أجل تعزيز ثقته باستخدام التطبيقات الإلكترونية.

ويتعين كذلك البحث في التشريعات الاستراتيجية في سياق الاستراتيجيات الوطنية المعنية بالمعلومات، وتكنولوجيا المعلومات والاتصالات ونظمها. وينبغي أن ينطلق البحث من رغبة سياسية حقيقية في وضع تشريعات وتدابير ذات أثر حقيقي وكفاءة عالية. لذا تقف جميع البلدان أمام خيارين، فإما أن تضع مجموعة من التشريعات التي تغطي جميع مسائل الفضاء السيبراني، وإما أن تضع تشريعاً واحداً وشاملاً يغطي جميع المسائل السيبرانية في إطار ما يسمى بقانون تكنولوجيا المعلومات والاتصالات، أو قانون الفضاء السيبراني. وتجدر الإشارة إلى أن كلا من الخيارين سليم إذا تم الوفاء بالتزاماته ومتطلباته.

وقد يفيد وضع تشريع واحد، أكثر من مجموعة متكاملة من التشريعات في تسهيل الأمور في المنطقة العربية، وذلك لاعتبارات عدة. فوضع تشريع واحد سيحقق توحيد تعاريف جميع المصطلحات والمفاهيم التكنولوجية والقانونية التي قد تتعارض في ما بينها في حال تعدد التشريعات. كما يسهل التشريع الواحد وضع إطار تنظيمي وإشرافي واحد يشمل مسائل التشريعات السيبرانية كلها، ويوائم بين الحلول القانونية والأحكام القائمة ضمن المدونة التشريعية الواحدة. ويسهل التشريع الواحد أيضاً، مادياً وتنظيمياً، إيجاد الحلول ووضع قواعد التنفيذ، وذلك من خلال تحديد جهة واحدة لإنفاذ القانون، وجهة واحدة للاختصاص القضائي والضبط العدلي، وغيرها من أجهزة العدالة.

وأما خيار وضع مجموعة من التشريعات فقد يكون صائباً وملائماً في حال تحقيق تناغم بين محتوى مختلف التشريعات، وإجراء تنسيق شامل بين الجهات المعنية بوضع كل تشريع من هذه التشريعات. فينبغي لهذه التشريعات المتعددة أن تضمن حماية المصالح المكفولة في هذا الفرع وتحقق توازنا بينها في حالات التعارض.

هاء- بنية ومحتوى التشريعات السيبرانية الخاصة ببناء الثقة بالخدمات الإلكترونية وتعزيز أمنها

تشير هذه الفقرة إلى الأسس التي ينبغي أن يرتكز عليها المحتوى النموذجي للتشريعات في جميع مجالات التشريعات السيبرانية، وإلى القواعد القانونية التي يتعين أن يتضمنها كل تشريع خاص، أو أقله الجزء المعني بمجال محدد في التشريع السيبراني الواحد.

وبهدف الإحاطة بجميع المسائل الخاصة بالفضاء السيبراني، وبحث محتوى القوانين ذات الصلة وبنيتها، يمكن تقسيم مواضيع الفضاء السيبراني على الشكل التالي:

(أ) الحق في الوصول إلى المعلومات في البيئة الرقمية؛

(ب) الخصوصية وحماية البيانات الشخصية؛

(ج) جرائم الحاسوب والإنترنت موضوعياً وإجرائياً: وهي تتضمن المسائل المتصلة بإساءة استخدام البريد الإلكتروني، والمحتوى الضار، والنشر غير القانوني على مواقع الإنترنت؛

(د) الملكية الفكرية للمصنفات، والحقوق المتصلة بتكنولوجيا المعلومات، وحماية المحتوى الرقمي وأسماء النطاقات؛

(•) الأعمال الإلكترونية: وهي تتضمن مسائل العمليات الإلكترونية، والحكومة الإلكترونية، والتجارة الإلكترونية، والمصارف الإلكترونية، وحماية المستهلك.

1- الحق في الوصول إلى المعلومات[58]

(58) انظر التذييل 50 أعلاه.

يشكل الحق في الوصول إلى المعلومات ضمانةً للشفافية والمشاركة العامة والرقابة الفاعلة على الحكومة، وأداةً لحماية الحق في الرأي والتعبير والإعلام. وقد كُرس هذا الحق في الإعلان العالمي لحقوق الإنسان، والعهد الدولي الخاص بالحقوق المدنية والسياسية، والاتفاقية الأوروبية لحماية حقوق الإنسان، والحريات الأساسية، وفي عدد كبير من الصكوك الدولية والدساتير الوطنية.

(أ) الحقائق القانونية ذات الصلة بقانون الحق في الوصول إلى المعلومات

بعد قراءة مختلف النماذج الدولية والوطنية للوثائق القانونية، وفي ضوء تحليل التشريعات الملائمة لتوفير البيئة الرقمية عموماً، وتطبيقات الخدمات الإلكترونية خصوصاً، يمكن استخلاص ما يلي:

- يهدف مفهوم الحق في الوصول إلى المعلومات إلى تمكين الأفراد من الوصول إلى المعلومات والوثائق والسجلات المحفوظة لدى السلطات والهيئات العامة في الدولة، وكذلك إلى تنظيم الحق في الوصول إلى سجلات ومعلومات القطاع الخاص، مع مراعاة التباين في طبيعة هذا الحق بين القطاعين العام والخاص وغرضه ونطاق استخدامه، وذلك من أجل تعزيز الشفافية؛

- لم يلق موضوع حق الفرد في الوصول إلى المعلومات الحماس نفسه الذي أبدته الحكومات أو مؤسسات في قطاعات الأعمال تجاه تفعيل غيره من حقوق الإنسان؛

- كان لتكنولوجيا المعلومات والاتصالات أثر كبير على تمكين الأفراد من الوصول إلى المعلومات، بعد توفر قدر كبير من البيانات والمعلومات والوثائق عبر مواقع الإنترنت؛

- يفقد الحق في الوصول إلى المعلومات قيمته إذا كثرت القيود أو الاستثناءات عليه بهدف حظر الوصول إلى معلومات أو سجلات ووثائق محددة. ومن هنا تكتسب التشريعات أهميتها الاستثنائية، حيث تخلق توازناً معقولاً ومشروعاً بين اعتبارات الحفاظ على سرية معلومات معينة لأغراض تتعلق بالأمن، وبين الحق في الوصول إلى المعلومات.

(ب) أهداف القانون وإطاره القانوني

يهدف هذا القانون عموماً إلى تكريس الحق الدستوري في الوصول إلى المعلومات وإلى إنفاذه. كما يهدف إلى تحديد نطاق الاستثناءات المقررة لهذا الحق بما لا يتعارض مع الحق نفسه، ويتناسب مع موجبات الطبيعة السرية لبعض البيانات والوثائق. ويهدف أيضاً إلى إحداث توازن وإزالة أي تناقض بين هذا الحق وسائر حقوق الإنسان المعترف بها ضمن التزامات الدولة وقواعدها الدستورية، وتحديداً الحق في التعبير، وفي حرية الرأي، وفي المشاركة، وفي الخصوصية.

ويجب أن يوضح هذا القانون كيفية تنفيذ التزامات الدولة تجاه المجتمع الدولي بشأن تكريس حقوق الإنسان، وكيفية التحقيق الفعلي والميسر للحق في الوصول إلى المعلومات بأقل كلفة ممكنة وعلى قاعدة المساواة، والتبرير المشروع للموافقة على إعمال هذا الحق أو رفضه. وينبغي أن يتناول هذا الحق كذلك الآلية اللازمة لتحقيق الالتزام بالشفافية، وتحديد مسؤوليات جميع الهيئات والأجهزة في القطاعين العام

والخاص تجاه هذا الالتزام، وتعزيز الثقافة الوطنية في ما يتصل بالحقوق والإلتزامات، وإدراك الواجبات الوظيفية لتعزيز المشاركة العامة، وتفعيل ممارسة حرية الرأي والتعبير.

ويجب أن يشير القانون المعني بالحق في الوصول إلى المعلومات، عند صياغته، إلى المحاور الأساسية التي تتضمن التعاريف القانونية الأساسية مثل السجلات، والمعلومات الشخصية، وآليات الوصول إلى المعلومات. وينبغي أن يبين القانون نطاق عمله، فيحدد ما إذا كان يطبق على المعلومات والسجلات والوثائق الحكومية، أو على سجلات القطاع الخاص أو في الحالتين معاً. ويفترض أن ينص القانون كذلك على الأهداف المرجوة منه كما ورد أعلاه، وعلى أحكام الحق في الوصول إلى السجلات الحكومية والعامة وتنظيم مسائلها. كذلك ينبغي أن يتضمن الإعتراضات الإدارية، والطعون في قرارات الموظف المسؤول عن المعلومات، إضافة إلى المسؤوليات القانونية والمخالفات.

2- الحق في الخصوصية أو حماية البيانات الشخصية[59]

وأما الخصوصية فهي حق الأفراد في حمايتهم من التدخل في حياتهم الخاصة، وحقهم في التحكم بدورة المعلومات التي تتعلق بهم. وقد مر تطور مفهوم الخصوصية تاريخياً بثلاث محطات رئيسية. ففي المحطة الأولى تم الاعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم، وهي ما يَعرف بالخصوصية المادية. أما المحطة الثانية فتناولت حماية القيم والعناصر المعنوية، وهي تُعرف بالخصوصية المعنوية. وفي المحطة الثالثة اعتُبرت الخصوصية حقاً عاماً لحماية الفرد من جميع أوجه الاعتداء والتدخل في حياته، مادية كانت أم معنويَة. ومع بلوغ الخصوصية محطتها الأخيرة هذه، ارتدى هذا المفهوم حلةً جديدة ترتبط بأثر تكنولوجيا المعلومات على الحياة الخاصة، وتتمثل في خصوصية المعلومات، وفي حق الأفراد في السيطرة على المعلومات والبيانات الرقمية الخاصة بهم.

(أ) الحقائق القانونية ذات الصلة بتشريعات الخصوصية وحماية البيانات الشخصية

لقد أقرت البلدان المتقدمة بمعظمها، وكذلك عدد كبير من البلدان النامية، بشكل أو بآخر، الحق في الخصوصية. وتكرس هذا الحق في النصوص الدستورية، كالدساتير الأوروبية التي نصت صراحة (في تسعينات القرن الماضي) على الحق في وصول الفرد إلى بياناته الشخصية وتحكمه بها.

وأقرت صكوك ووثائق عالمية وإقليمية إجراءات قانونية لحماية الخصوصية عبر أحكام قضائية تصدرها المحاكم العليا والدستورية. وتمثلت قوانين حماية الخصوصية بنموذجين. ويتمثل النموذج الأول في القوانين الشاملة التي تعترف بالحق وتقر بمبادئه الأساسية، وتقدم الإطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات، أو حماية البيانات المتصلة بالأفراد وحياتهم الخاصة (البيانات الشخصية). أما النموذج الثاني فيتمثل في قوانين قطاعية ترعى البيانات المتصلة بقطاعات محددة، مثل البيانات الصحية والمالية وبيانات الأحوال المدنية وغيرها، مع مراعاة التناغم بين أحكامها. وأما مدونات السلوك فتكمل القوانين، وترعى قطاعات معينة كقطاعي الصناعة أو الخدمات الفنية، في ما يعرف بوسيلة التنظيم القانوني الذاتي للقطاعات أو السوق.

(59) انظر التذييل 50 أعلاه.

أما الهدف من هذا القانون فيتمثل في حماية البيانات الشخصية للفرد من إساءة استخدامها بأي شكل كان. ولكي يقوم مفهوم حماية البيانات على أسس سليمة، يجب أن تستوفي البيانات الشخصية الشروط التالية: (1) أن يكون الحصول عليها قد تم بطريقة مشروعة وقانونية؛ (2) أن تُستخدم للغرض الأصلي المعلن والمحدد، وألا تُكشف لغير المخولين بالاطلاع عليها؛ (3) أن تتصل بالغرض المقصود من جمعها وألا تتجاوزه؛ (4) أن تكون صحيحة، وأن يجري تحديثها وتصحيحها؛ (5) أن يتمتع صاحبها بالحق في الوصول إليها، والحق في أن يَبلغ بأنشطة معالجتها أو نقلها، والحق في تصحيحها وتعديلها، وحتى في طلب إلغائها؛ (6) أن تحفظ بسريةٍ وأن تُحمى سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المعالجة؛ (7) أن تخضع لضوابط حماية الحق فيها، ومنع الضرر عند نقلها وتبادلها خارج نطاق الحدود الجغرافية؛ (8) أن تُتلف عند استيفاء الغرض من جمعها.

ولكي يتسم قانون الخصوصية بالفعالية المرجوة، ينبغي إنشاء جهة محايدة ومستقلة تراقب أداء جميع الجهات، وتشكل مرجعية لحل الشكاوى والاعتراضات كافةً.

(ب) أهداف قانون الخصوصية وحماية البيانات الشخصية

يهدف القانون إلى حماية الحياة الخاصة للأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، لا سيما مع ازدياد أنشطة جمع البيانات وتخزينها وتبادلها ونقلها عبر استخدام تكنولوجيا المعلومات والاتصالات. ويهدف القانون كذلك إلى توفير نظام يضمن مراقبة الجهات المعنية بجمع البيانات الشخصية ومعالجتها في القطاعين العام والخاص والتزام هذه الجهات بالضوابط والمعايير المشروعة لحماية الحق في الخصوصية. ويسمح القانون في الوقت نفسه بالقيام بأنشطة هذه القطاعات طالما امتثلت للمعايير المقررة، كما يضع ضوابط ملائمة لا تتعارض مع الحق.

ويحرص هذا القانون على تكريس المبادئ الأساسية المتعلقة بالممارسات العادلة والمقبولة والنزيهة في نطاق خصوصية المعلومات، وحماية البيانات الشخصية في بيئة الخدمات الإلكترونية والبيئة الرقمية عموماً. وهذه المبادئ هي الإبلاغ والإخطار[60]، والاختيار[61]، والوصول إلى البيانات[62]، والأمن[63]، وآليات إنفاذ القانون[64].

وينبغي أن يوفر هذا القانون نطاقاً موضوعياً وإجرائياً للقواعد القانونية الإدارية (التنظيمية) والمدنية والجزائية المتعلقة بالبيانات الشخصية، والحق في الخصوصية، وإشاعة الثقة بالبيئة الرقمية ومختلف

(60) يعني هذا المبدأ أن يقوم مزود الخدمة أو صاحب الموقع بإبلاغ المستخدم بما إذا كان الموقع نفسه أو مقتضيات الخدمة تتطلب جمع بيانات شخصية، وبمدى جمع هذه البيانات واستخدامها.

(61) يلزم هذا المبدأ الشركات صاحبة المواقع أو مزودة الخدمة بتوفير خيار للمستخدم حول استخدام بياناته على نحو يتجاوز الغرض المبدئي من جمعها.

(62) يمنح هذا المبدأ المستخدمين القدرة على الوصول إلى بياناتهم والتثبت من صحتها وتحديثها.

(63) يتعلق هذا المبدأ بمسؤوليات الجهات المعنية بجمع البيانات (أي أصحاب المواقع ومزودي الخدمات) ومعايير الأمن اللازم تطبيقها لضمان سرية البيانات وسلامة استخدامها وحظر الوصول غير المصرح به إليها. وهي تتضمن كلمات السر والتشفير وغيرها من وسائل أمن المعلومات.

(64) يتعلق هذا المبدأ بالآليات المناسبة واللازمة لفرض جزاءات على الجهات غير الملتزمة بالمبادئ المتقدمة، وما يتصل بها من ممارسات نزيهة بشأن جمع البيانات الشخصية في البيئة الرقمية.

تطبيقاتها، وسائر الخدمات الإلكترونية ومشاريع توظيف التكنولوجيا، وإزالة أي اعتقاد بالتهديد الشخصي والناشئ عن الاستغلال غير المشروع للبيانات الشخصية.

وعند صياغة قانون الخصوصية وحماية البيانات الشخصية، يجب أن يحدد القانون تعاريف المفاهيم الأساسية، كتعريف البيانات الشخصية، وصاحب البيانات ومستخدمها، ونظام المعالجة الإلكترونية. كما يجب أن يحدد نطاق القانون وأغراضه، والمبادئ العامة لحماية البيانات الشخصية، أو التزامات الجهة المعنية بمعالجة البيانات الشخصية. ويجب أن يشير كذلك إلى الجهة المشرفة على حماية البيانات وقواعدها التنظيمية وقواعدها الخاصة.

3- جرائم الحاسوب والإنترنت أو الجرائم السيبرانية[65]

تشكل جرائم الحاسوب والإنترنت أو الجرائم السيبرانية ظاهرة إجرامية حديثة نسبياً. وقد نشأت هذه الظاهرة في مطلع سبعينات القرن العشرين، ورافقت نشوء نظم الحاسوب والشبكات ونموها وتطورها، وثورة تكنولوجيا المعلومات والاتصالات. وتنطوي هذه الظاهرة على مخاطر جمة حيث تُلحق بالمؤسسات والأفراد خسائر فادحة، باعتبارها تعتدي على البيانات بدلالتها الفنية الواسعة، أي البيانات والمعلومات والبرامج على اختلاف أنواعها، وتطال البيانات المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات. كما أنها تطال الحق في الوصول إلى المعلومات، والأموال والحقوق المالية والابتكار، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتكنولوجيا، وتهدد إبداع العقل البشري.

ويؤدي نظام الحاسوب عموماً ثلاثة أدوار في ارتكاب الجرائم، ودوراً رئيساً في اكتشافها. فالحاسوب يؤدي أدواراً في ارتكاب الجرائم في الحالات التالية: **(أ)** عندما يكون الحاسوب هدفاً للجريمة، أي عندما تستهدف الأفعال غير المشروعة سرية البيانات وتكاملها وتوفرها. وتتضمن هذه الأفعال الإجرامية الدخول غير المصرح به إلى النظام الهدف، وهي تُعرف اليوم بأنشطة المخترقين لأنها كناية عن فعل اختراق النظام؛ (ب) عندما يكون الحاسوب أداة لارتكاب جرائم تقليدية، أي في حال استغلال الحاسوب مثلاً للاستيلاء على الأموال عبر إجراء تحويلات غير مشروعة أو عمليات تزييف وتزوير، أو الاستيلاء على أرقام بطاقات الائتمان؛ (ج) عندما يكون الحاسوب بيئة للجريمة، أي عند استخدامه لنشر المواد غير القانونية، أو أداة اتصال لإبرام صفقات ترويج المخدرات، وأنشطة الشبكات الإباحية، وما إلى ذلك. ويؤدي الحاسوب دوراً في اكتشاف الجريمة عندما تستخدمه الجهات المعنية بتنفيذ القانون على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، بدل أن تعتمد على النظم التكنولوجية في إدارة المهام، وذلك من خلال قواعد البيانات التابعة لجهاز إدارة العدالة.

(أ) الحقائق القانونية ذات الصلة بتشريعات جرائم الحاسوب والإنترنت

يشير تحليل الجهود الدولية واتجاهات القانون المقارن بشأن جرائم الحاسوب والإنترنت إلى أن أكثر قضايا جرائم الحاسوب والإنترنت إثارة للجدل هي تلك التي تتعلق بوضع قائمة بالأفعال التي يتعين تجريمها، وتحديد أنماط السلوك الإجرامي والأفعال المكونة له. وقد دار جدل حول مدى انطباق نصوص القوانين

(65) انظر التذييل 51 أعلاه.

الجنائية التقليدية على هذه الجرائم، خصوصاً في السنوات الأولى من بروز الظاهرة، ثم حَسم الجدل بالتأكيد على عدم كفاءة النصوص الجنائية القائمة في تنظيم هذه الأنماط الجديدة من الجرائم.

وتستند ضرورة وضع قانون لمعالجة الجرائم السيبرانية موضوعياً وإجرائياً إلى الحقائق القانونية الثلاث التالية: (1) إن طبيعة جرائم الحاسوب معنوية وليست مادية، كما هو الحال في الجرائم التقليدية. فعندما يكون الحاسوب مثلاً هدفاً للجريمة، تكون المعلومات المخزنة فيه أو المنقولة منه أو إليه هي هدف الفعل الإجرامي؛ (2) يمنع مبدأ الشرعية الجنائية المساءلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بوجود مثل هذا النص. وعندما لا يتوفر النص المتصل بتجريم تلك الأفعال التي لا تطالها النصوص القائمة، تُنتفى المسؤولية ويقع قصور في مكافحة تلك الجرائم؛ (3) لا يمكن تطبيق القياس على أنماط جرائم الحاسوب، على خلاف الجرائم التقليدية التي تستهدف الأموال والأشخاص مادياً. فالقياس في النصوص الجنائية الموضوعية محظور وغير جائز.

وتجدر الإشارة إلى أن الاعتداءات التي تستهدف الأجهزة والمواد ذات الوظيفة التكنولوجية أو الإلكترونية، مثل نظم الحاسوب والشبكات، تخرج عن نطاق جرائم الحاسوب حيث تطبق عليها نصوص التجريم التي تستهدف المال المادي المنقول.

(ب) إطار قانون الجرائم السيبرانية وأهدافه

تتمثل الأغراض الأساسية لهذا القانون في حماية المصالح الناشئة في نطاق تكنولوجيا المعلومات والاتصالات والبيئة الرقمية، كالحق في المعلومات واستثمارها، وتعزيز القواعد والمعايير المتصلة بأخلاق تكنولوجيا المعلومات والاتصالات، وتوفير الحماية القانونية للأفراد والمؤسسات من جميع أنشطة الاعتداء على البيانات ونظمها في مختلف مراحل معالجتها واستخدامها.

ويهدف هذا القانون إلى تجريم الحد الأدنى من أشكال الاعتداء في البيئة الرقمية، من خلال توفير نظام تدريجي للعقوبات يساهم في ردع المخالفين، ويعزز الثقة بالتكنولوجيا ونظمها وتطبيقاتها. ويهدف القانون إلى الالتزام بعدد من المعايير لحماية تبادل البيانات ونقلها، لبناء ثقة البلدان الأخرى بالإطار القانوني الوطني، وتحقيق معايير تبادل البيانات ونقلها، ونقل المعرفة والاستثمار المعلوماتي الداخلي. ويسعى هذا القانون كذلك إلى تحقيق تكامل الحماية الجزائية من أنشطة استهداف البيانات، بحيث تتكامل قواعد هذا التشريع ضمن تشريعات الملكية الفكرية مع قواعد الأحكام الجزائية الموضوعية في التشريعات المتعلقة بالخصوصية، وتلك المتعلقة بحماية المصنفات الرقمية، والحقوق المعنوية ذات الصلة بالخدمات الإلكترونية وبيئتها.

ويهدف الإطار الإجرائي للقانون إلى ضمان فعالية نصوص التجريم من خلال توفير قواعد ترعى مسائل التفتيش والضبط والملاحقة والتحقيق والاختصاص القضائي فيما يتعلق بهذه الجرائم ومكافحتها، وتحدث توازناً مع القواعد الخاصة بحقوق المتهم، وتسهل وتشجع التنسيق والتعاون، بما في ذلك آليات التعاون القضائي وتبادل المعلومات، على الصعيدين الإقليمي والدولي بشأن مكافحة هذه الجرائم.

ويجب أن يتضمن قانون الجرائم السيبرانية التعريفات الأساسية الضرورية (حول نظام الحاسوب، ومزودي الخدمات، والبيانات الشخصية وشبكات الحواسيب مثلاً) ونطاق القانون وأغراضه. ويجب أن يشمل قواعد تحديد الأفعال الإجرامية وعقوباتها، ونصوصاً موضوعية خاصة بالمساهمة الجرمية ومسؤولية

الشخص المعنوي، والنصوص الإجرائية ذات الصلة بالجرائم الإلكترونية، وكذلك المبادئ العامة لحماية البيانات الشخصية أو التزامات الجهة القائمة بمعالجة البيانات الشخصية. ومن المفيد أن يشير القانون إلى الجهة المشرفة على حماية البيانات والقواعد التنظيمية الخاصة بعملها.

4- الملكية الفكرية المتصلة بتكنولوجيا المعلومات والاتصالات والخدمات الإلكترونية[66]

تتعلق الملكية الفكرية بالحقوق الملازمة لنِتاج الإبداع الإنساني، سواء اتخذت صفة مصنف ذي وجود مادي، كالكتاب أو اللوحة الفنية أو برنامج الحاسوب، أم ارتبطت بإيصال هذا الإبداع إلى الجمهور، كالأداء التمثيلي والغناء والبث الإذاعي للمصنف. وترتبط الملكية الفكرية أيضاً بالعناصر المميزة للمشاريع الاقتصادية، كالعلامة التجارية أو الاسم التجاري أو غيرها.

ومنذ بدايات التنظيم القانوني الدولي للملكية الفكرية، صنفت الإبداعات ضمن مجموعتين: (أ) مجموعة الملكية الفكرية الأدبية أو الفنية، وتشمل ما يُعرف بحق المؤلف والحقوق المجاورة؛ (ب) مجموعة الملكية الفكرية الصناعية، وتضم الابتكارات القابلة للاستغلال الصناعي والتجاري، كبراءات الاختراع والرسوم والنماذج الصناعية، وكذلك عناصر التميز الخاصة بالمشروع التجاري مثل العلامة التجارية، وعلامة المنشأ، أو السر التجاري. ولا تنضوي جميع عناصر الملكية الفكرية وأقسامها ضمن اتفاقية دولية واحدة أو قانون وطني واحد . فالملكية الفكرية فرع قانوني شامل ذو عناصر متميزة ونظريات خاصة، غير أن كل مجال من مجالاته يشكل فرعاً خاصاً بنظريات وبنود متميزة.

(أ) الحقائق القانونية ذات الصلة بتشريعات الملكية الفكرية

الإبداع في مجال تكنولوجيا المعلومات والاتصالات هو مصدر وجودها، وهو أساسي لنموها وتطورها، في المجالات كافة من أدبية وفنية وصناعية وتجارية. ويحتاج بناء الثقة بهذه التكنولوجيا بجميع وجوهها إلى حماية قانونية لجميع منتجات الإبداع والابتكار في مجال تكنولوجيا المعلومات والاتصالات، وفي مقدمتها:

- مختلف برامج الحاسوب والحلول الإلكترونية الناتجة من عمليات البرمجة؛
- قواعد البيانات؛
- البيانات الضرورية لإدارة الحقوق، مثل النشر الإلكتروني والمحتوى الرقمي الإلكتروني؛
- الوسائط المتعددة بمختلف أنواعها وعناصر تكوينها؛
- عناصر المنافسة الخاصة بتميز المشروع التجاري الرقمي، والمعلومات السرية أو الأسرار التجارية ذات العلاقة بالمشاريع الرقمية في مجالي الخدمات والاستثمارات، وضوابط نقل التكنولوجيا وتوظيفها؛

(66) انظر التذييل 52 أعلاه.

- أسماء المواقع أو النطاقات الإلكترونية؛

- تصاميم الدوائر المتكاملة ذات الوظيفة الإلكترونية.

وقد انطلقت حركة التشريع الدولية والوطنية لحماية الملكية الفكرية من خلال تحديد تشريعات وطنية يمكن تعديلها لتتضمن حماية الملكية الفكرية الملائمة لتكنولوجيا المعلومات والاتصالات، وليس من خلال وضع قانون خاص بالملكية الفكرية الإلكترونية. وتمت حماية البرامج وقواعد البيانات والوسائط المتعددة ضمن التشريعات المعنية بحقوق المؤلف في معظم البلدان، إن لم يكن في جميعها. وتستثنى منها الولايات المتحدة الأمريكية وعدة بلدان أوروبية حيث تُحمى برامج الحاسوب أيضاً بموجب قوانين براءات الاختراع. وأما الأسرار التجارية ذات الصلة بمشاريع تكنولوجيا المعلومات والاتصالات فتحمى بموجب تشريعات الأسرار التجارية. وتُحمى العلامات الفارقة ذات الطبيعة الإلكترونية بموجب قوانين العلامات التجارية. وفي بعض البلدان، وُضعت أدوات تشريعية خاصة لأسماء مواقع الإنترنت وأسماء النطاقات، وفي عدد من البلدان نُظمت ضمن نصوص محددة في قوانين العلامات التجارية.

ولا يعيب تعدد قوانين الحماية التشريعية للملكية الفكرية نظام الحماية، لكنه يفرض التزاما جوهرياً بأن تكون الحماية شاملة، وأن يتحقق التناغم والانسجام بين هذه القوانين المتعددة نظراً إلى ارتباطها ببيئة واحدة هي البيئة الرقمية. ويمكن أن تستفيد البلدان النامية من التوجه نحو توحيد الأداة التشريعية للملكية الفكرية في قانون واحد من حيث تيسير إدارة شؤون هذه الحقوق وتبسيط قواعد المقاضاة وتوحيدها. كما يضمن هذا التوحيد الانسجام والشمول والبساطة والوضوح وتيسير الإنفاذ. ويبقى وجود أداة واحدة ليس مهما بقدر أهمية الحماية الشاملة للعناصر مهما تعددت أدواتها.

ومن المؤكد أن تحقيق حماية فاعلة للملكية الفكرية عموماً، وفي البيئة الرقمية خصوصاً، غير ممكن ما لم تنسجم الجهود الوطنية مع الجهود والاتفاقيات والمدونات التشريعية الدولية. فالتشريع الدولي يشكل بأدواته والتزاماته نطاقاً دولياً للحماية، وتتوحد نظرياته أكثر من أي موضوع قانوني آخر رغم اختلاف النظم القانونية. ولهذا، يُعتبر فهم النظام الدولي المتعلق بحماية الملكية الفكرية والانسجام معه، وتوفير الأداة التشريعية الوطنية الملائمة له ضمن النظام القانوني للدولة المعنية من أهم عناصر نجاح نظام الحماية الوطني للملكية الفكرية في مجال تكنولوجيا المعلومات والاتصالات.

(ب) إطار القوانين المنظمة للملكية الفكرية في البيئة الإلكترونية وأهدافها

تمثل حماية الإبداع الهدف الأساسي من استخدام أي أداة تشريعية لحماية أي مصنف رقمي أو حماية الحق المعنوي في أي من عناصر المشاريع الرقمية عموماً، ومشاريع الخدمات والأعمال الإلكترونية خصوصاً.

وتشجع حماية الحقوق المعنوية لمنتجات الإبداع والابتكار في البيئة الرقمية التوجه نحو مشاريع الاستثمار المعلوماتي ومشاريع التطبيقات الإلكترونية بأنواعها. كما تساهم في نجاح سياسات واستراتيجيات نقل المعرفة وتوظيفها اجتماعياً وثقافياً واقتصادياً في الدولة. ويساعد نظام الحماية الملائم والمتوازن والفعال في جذب الاستثمارات الأجنبية والاستفادة منها في خدمة الاقتصاد الوطني.

وتساهم تشريعات حماية الملكية الفكرية في الوفاء بالتزامات الدولة بحكم عضويتها في منظمة التجارة العالمية، أو التزاماتها المقررة بموجب الاتفاقيات الدولية التي تتيح تيسير التجارة البينية والخارجية في البضائع والخدمات، وتيسير انتقال المعرفة وتوظيفها.

وعند صياغة بنود قانون حماية الملكية الفكرية المتصلة بتكنولوجيا المعلومات والاتصالات، يجب أن تشير هذه البنود إلى كيفية حماية برامج الحاسوب وقواعد البيانات بمختلف أشكالها، وأن تتضمن معلومات عن كيفية إدارة الحقوق الإلكترونية، وعن الوسائط الرقمية المتعددة وحمايتها، وعن الأسرار التجارية وقمع المنافسة غير المشروعة، وعن قواعد حماية عناوين المواقع الإلكترونية.

5- الإطار التشريعي للأعمال الإلكترونية بمختلف أشكالها[67]

مع توجه الشركات والهيئات والحكومات والأفراد إلى الاستثمار في البيئة الرقمية لتقديم خدمات جديدة، والتسويق لمنتجات جديدة وبيعها، وإدارة مشاريع تجارية جديدة في ظل توفر آليات تسمح بتسديد المدفوعات إلكترونياً، وتلائم مشاريع التجارة والأعمال والخدمات الإلكترونية، برزت جملة تحديات قانونية لجميع النظم القانونية القائمة. وتشبه هذه التحديات تلك التي رافقت ظهور العلاقات القانونية في البيئة العادية، والتحديات التي فرضتها الطبيعة الخاصة للتطبيقات الإلكترونية بأدواتها ونطاقها. ومن أهم هذه التحديات:

- التوقيع الإلكتروني وآليات تنفيذه ومدى تحقيقه وظيفة التوقيع اليدوي التقليدي؛
- أدوات ووسائل الإثبات الإلكتروني المتصلة بالمتعاقد، ومدى قدرة العقود والسجلات والرسائل الإلكترونية على تحقيق مفهوم المحررات الكتابية والأصل والعقد الموقع؛
- الشفافية المطلوبة لتقديم الخدمات الحكومية الإلكترونية بصورة فعالة وملائمة؛
- الإطار القانوني المنظم للربط الأفقي والعمودي بين مواقع الخدمات الحكومية كمفهوم متطور للحكومة الإلكترونية؛
- التعبير عن الإرادة والتعاقد في البيئة الرقمية، ومدى تمكنهما من تحقيق شروط التعبير عن الإرادة والتعاقد في البيئة التقليدية؛
- مسؤولية الوسطاء ودور الجهات المعنية بتوثيق المراسلات والتواقيع الإلكترونية، والإطار القانوني المنظم لعملها (من هيئات توثيق وشهادات توثيق)؛
- الضرائب في البيئة الرقمية وفي أعمال التجارة الإلكترونية؛
- حماية حقوق المستهلك في البيئة الرقمية، خصوصاً في حالة التعاقد لشراء الخدمات والبضائع المتصلة مباشرة بالتجارة الإلكترونية والحصول عليها؛

(67) انظر التذييل 54 أعلاه.

- تحديات التنازع بشأن الاختصاص القضائي، وبشأن القانون الواجب تطبيقه؛

- تحديات حماية البيانات الشخصية التي يضعها المستهلك بتصرف مواقع الأعمال الإلكترونية، وخصوصاً في حالات التجارة الإلكترونية، والمصارف الإلكترونية، والحكومة الإلكترونية؛

- تحديات ومخاطر الاعتداء على البيانات في البيئة الرقمية وعلى الحقوق المتصلة بالمداولات الإلكترونية، ومنها الاعتداءات التي تستهدف مواقع الأعمال الإلكترونية أو قواعد بيانات العملاء.

(أ) الحقائق القانونية ذات الصلة بتشريعات الأعمال الإلكترونية وتطبيقاتها المختلفة

تناول هذا الفصل في فقرات سابقة التحديات الأربعة التي تتناولها بنود خاصة بمواضيع الحق في الوصول إلى المعلومات، والخصوصية، والجرائم السيبرانية، وحماية الملكية الفكرية. وينبغي تنظيم هذه المواضيع تنظيما شاملاً، بحيث تُخصص لها تشريعات منفصلة أو تدرج ضمن تشريع واحد. وعندئذ، يتحقق الهدف المتمثل في تنظيم الأعمال والخدمات الإلكترونية وبناء الثقة بها. وعندما تكون هذه المواضيع الأربعة محل تنظيم قائم بذاته، سيظهر عدد من الأفعال الجديدة التي تستهدف أدوات الأعمال الإلكترونية، مثل الإخلال بالتزامات سلطات التوثيق أو الاعتداءات المتصلة بالتوقيع الإلكتروني وموثوقيته. وقد تظهر بعض الممارسات، كاستغلال البيانات الشخصية لأغراض التسويق الإلكتروني من دون رضا المستخدم، وهي تفرض حمايتها في إطار الحق في التصرف بالبيانات الشخصية. وتعالج هذه المسائل ضمن الفروع المعنية عبر إدخال بنود تتلاءم مع تطورات الأعمال الإلكترونية وتطبيقاتها، أو ضمن تشريعات الأعمال الإلكترونية لسد النقص القائم في تشريعات الفروع الأخرى المعنية.

وقد اختارت بلدان عدة أن تنظم العلاقات القائمة في بيئة التجارة الإلكترونية ضمن خانة العمليات الإلكترونية، باعتبارها أشمل وأوسع من التجارة الإلكترونية. فهي تضم العمليات الإلكترونية، والحكومة الإلكترونية، والعلاقات التعاقدية الإلكترونية المدنية، والعلاقات في بيئة الأعمال الإلكترونية الحكومية وغير الحكومية، وكذلك المسائل ذات الصلة بتحويل الأموال إلكترونياً كجزء من قضايا المصارف الإلكترونية أو العمليات المالية الإلكترونية، وأنشطة المضاربات المالية مع الأسواق المالية العالمية وعبر المنصات الإلكترونية. وعملياً، يمكن تقسيم العمليات الإلكترونية إلى ثلاثة أشكال رئيسة وهي الحكومة الإلكترونية، والتجارة الإلكترونية، والمصارف الإلكترونية.

وقد بينت الممارسات العملية أن الاعتراف بصلاحية أدوات التجارة الإلكترونية وأنماطها وطابعها القانوني وحجيتها لا يكفي لقبولها وتعميمها. فالتجارة الإلكترونية تتطلب ثقة المستهلكين والتجار ومؤسسات الأعمال بهذا النمط المستجد من العلاقات التجارية والتعاملات التعاقدية، والاقتناع بعدم وجود مخاطر تهدد الحقوق والأموال، وتفوق المخاطر التي يألفها المتعاملون في البيئة العادية غير الرقمية. ويرتبط هذا الأمر بتقديم حماية قانونية لنظم المعلومات والشبكات، وحماية حقوق المستهلك، وفي مقدمتها حقه في الخصوصية وفي الدفاع عن حقوقه في سياق إجراءات مقاضاة ملائمة وبعيدة عن التعقيدات الناتجة عن التنازع لتحديد الاختصاص والقانون الواجب تطبيقه. ويشير الإطار 2 إلى أن التجارة الإلكترونية سرعت عملية وضع التشريعات السيبرانية في المنطقة العربية وكانت المحفز الرئيس لها.

الإطار 2- التجارة الإلكترونية وراء إصدار التشريعات السيبرانية في المنطقة العربية

بدأت البلدان العربية بتنظيم المواضيع القانونية ذات الصلة بتكنولوجيا المعلومات والاتصالات قبل ظهور التجارة الإلكترونية وشيوعها، باستثناء تدخلها المحدود في حماية برامج الحاسوب وقواعد البيانات ضمن تشريعات الملكية الفكرية . فبالرغم من انطلاق أنشطة توظيف الحاسوب على نطاق واسع في البلدان العربية خلال ثمانينات وتسعينات القرن الماضي، ومع أن الإنترنت اقتحمت الفضاء العربي منذ منتصف تسعيناته، وبرغم النمو الملحوظ في سوق الهواتف الخلوية، خلت خارطة التشريعات العربية قبل شيوع التجارة الإلكترونية دولياً من التشريعات ذات الصلة بفروع تكنولوجيا المعلومات ومواضيعها. لقد بحثت دراسات في عوامل ومعوقات تشجيع التجارة الإلكترونية، وتوسيع نطاق توظيفها وتبني المستهلك أو مؤسسات الأعمال هذه التجارة الإلكترونية. وقد أجمعت كلها على أن بناء الثقة هو أهم عناصر النجاح في تحقيق القبول بالتجارة الإلكترونية واعتمادها، وأن إمكانيات المساس بالخصوصية ومخاطر الجرائم الإلكترونية هي أبرز العناصر التي قد تهدد هذه الثقة. وقد أدت مداولات التجارة الإلكترونية إلى وضع تشريعات سيبرانية في عدد كبير من المناطق، ومنها المنطقة العربية، وكان أبرزها في بلدان الخليج العربية.

وتعود ضرورة اتخاذ تدابير تشريعية في ميدان التجارة الإلكترونية إلى ثلاثة عوامل رئيسة. أما العامل الأول فموضوعي ويتمثل في تسارع نمو أنماط التطبيقات الإلكترونية، وظهور فرص استثمار في البيئة الرقمية لإنشاء مشاريع الأعمال الأمر الذي يستدعي تنظيمها ضمن أطر قانونية. أما العامل الثاني فيشكل ضرورة حتمية تتمثل في الانضمام إلى منظمة التجارة العالمية. وأما العامل الثالث فقد نتج عن التجارة الإلكترونية التي أوجدت تحديات قانونية لم يسبق للنظم القانونية العربية أن تصدت لها أو وضعت تشريعات تتعامل معها ضمن الأطر القانونية، خصوصا في مجالي حماية الخصوصية والحماية من الجرائم الإلكترونية.

وأما المصارف الإلكترونية فهي الشكل التطبيقي الذي يشمل مختلف حلول التكنولوجيا المصرفية أو الصيرفة الإلكترونية. ولا تعمل المصارف الإلكترونية على نقل الخدمات المصرفية إلى البيئة الرقمية وحسب، إنما تهدف إلى إيجاد نمط مختلف للأداء يقوم على التفاعل بين العميل والمصرف وجميع الخدمات المصرفية، وذلك لإدارة النشاط المالي عن بعد بكل سهولة وشمولية.

وضمن نطاق التنظيم القانوني للمصارف الإلكترونية، لا بد من الإجابة على جملة تساؤلات وأبرزها ما يلي: هل تغطي تشريعات العمل المصرفي تقنيات المال الإلكتروني والأرصدة الإلكترونية؟ وهل يتم تنظيم مختلف أنواع البطاقات المالية والعلاقات والالتزامات القانونية ذات الصلة بها بالفعالية المطلوبة؟ وهل تتفق قواعد المسؤولية المدنية والجزائية القائمة مع طبيعة علاقات الأطراف المشاركة في عملية استخدام بطاقات الائتمان، وتسديد الفواتير إلكترونياً، وبطاقات إدارة الحسابات، ومع الآثار المترتبة عليها؟ وهل يعرف النظام القانوني عن المسؤوليات الناشئة في ميدان نظم التحويل، وتسديد الفواتير إلكترونياً ويرعاها؟ وماذا عن المصارف الافتراضية؟ هل تخضع لمعايير المصارف العادية في نشاطها وخدماتها وإطارها القانوني وقواعد الإشراف عليها؟ وهل انتهى عصر البنوك المركزية التي تؤدي دور المشرف القانوني، أم أن دورها أصبح أكثر أهمية في عصر المال الرقمي والخدمات المصرفية الإلكترونية؟ وماذا عن ضرورة التدخل من أجل وضع تشريعات البنوك المركزية؟ وهل التقاص الإلكتروني، وهو أحد أهم وسائل تسوية الحسابات في النطاق المصرفي، منظم بصورة شاملة

(ب) أهداف الإطار القانوني المنظم للأعمال الإلكترونية والتطبيقات ذات الصلة

إن لتشريع الأعمال الإلكترونية أهدافا شاملة تتصل بالتطبيقات كلها، وأهدافاً خاصة بكل تطبيق على حدة. وأما الأهداف العامة فيجب أن تحدد القواعد القانونية التي تكفل الثقة بالأعمال الإلكترونية وتطبيقاتها، وفي مقدمتها التجارة الإلكترونية، والمصارف الإلكترونية، والحكومة الإلكترونية، وأن تعزز نموها وشيوعها. وينبغي أن تكون هذه القوانين متكاملة مع القواعد القانونية القائمة التي توفر بيئة آمنة للنشاط الإلكتروني في مختلف القطاعات، وأن تضمن حماية حقوق جميع الأطراف ذات الصلة.

ومن ناحية أخرى، يجب التنبه إلى الدور الذي يمكن أن تؤديه هذه القوانين والتشريعات لتشجيع الاستثمار في البيئة الرقمية وتنفيذ مشاريعها، وتسهيل أدوات ووسائل إعمال الحقوق وإدارة العدالة في نطاق الأعمال الإلكترونية وتبسيطها.

وينبغي أيضاً وضع قواعد قانونية لتحقيق تعاون دولي أوسع نطاقاً، ودعم الجهود الدولية الرامية إلى توحيد التدابير القانونية المتصلة بالأعمال الإلكترونية والتوفيق بينها. وينبغي أن تتميز هذه القواعد القانونية بالمرونة والمواءمة مع طبيعة الأعمال الإلكترونية المتغيرة، وأن تواكب عصر الإبداع المعلوماتي، وتساهم في تعزيز الأداء الرقمي الإبداعي وإنمائه.

ويجب أن ينص أي تشريع على الغاية الأساسية منه. ففي حالة تشريعات الأعمال الإلكترونية، ينبغي أن تتناول هذه التشريعات، أكانت منفصلة أم موحدة، الغاية منها في المجالات الثلاثة التالية، أي الحكومة الإلكترونية، والتجارة الإلكترونية، والمصارف الإلكترونية.

فالغاية من التشريعات على صعيد الحكومة الإلكترونية هي توفير مختلف الخدمات الحكومية في البيئة الإلكترونية، وتعزيز الشفافية والمشاركة في صنع القرارات ووضع السياسات. وقد تكون الغاية أيضاً تحقيق الاتصال والتفاعل بين الأجهزة الحكومية ذاتها أفقياً وعمودياً لضمان فعالية الخدمات الإلكترونية وجودتها، وتطوير الأداء الحكومي الداخلي، وليس فقط الواجهة الإلكترونية الأمامية للخدمات الحكومية. ويضاف إلى ذلك الهدف الأساسي، وهو إشاعة الأمن والثقة وتعزيز العمليات الإلكترونية.

أما الغاية من التشريعات على صعيد التجارة الإلكترونية فهي تيسير التعامل التجاري على صعيد بيع الخدمات والبضائع وشرائها في البيئة الرقمية وعبر الوسائل الإلكترونية، والمساواة بين وسائل التعاقد والتبادل التجاري وأدوات إثباته المستخدمة في البيئتين العادية والإلكترونية. كما يجب أن تكون غاية القانون تحقيق أمن المداولات التجارية الإلكترونية، وإشاعة الطمأنينة حيال استخدامها، وتيسير الإجراءات القضائية وإعمال الحقوق في بيئتها.

أما الغاية من التشريعات على صعيد المصارف الإلكترونية فهي الاعتراف بمختلف وسائل العمل المصرفي الإلكتروني وتطبيقاته وحلوله، وتيسير سائر الخدمات المصرفية في البيئة الإلكترونية. كما يجب أن تكون الغاية منها ضمان أمن محتوى البيانات المتبادلة ذات الطبيعة المالية وسلامته، وتعزيز الثقة بالبيئة وخدماتها وتطبيقاتها، وكذلك تعزيز التعامل التفاعلي بين العميل ومواقع المصارف والخدمات المالية الإلكترونية.

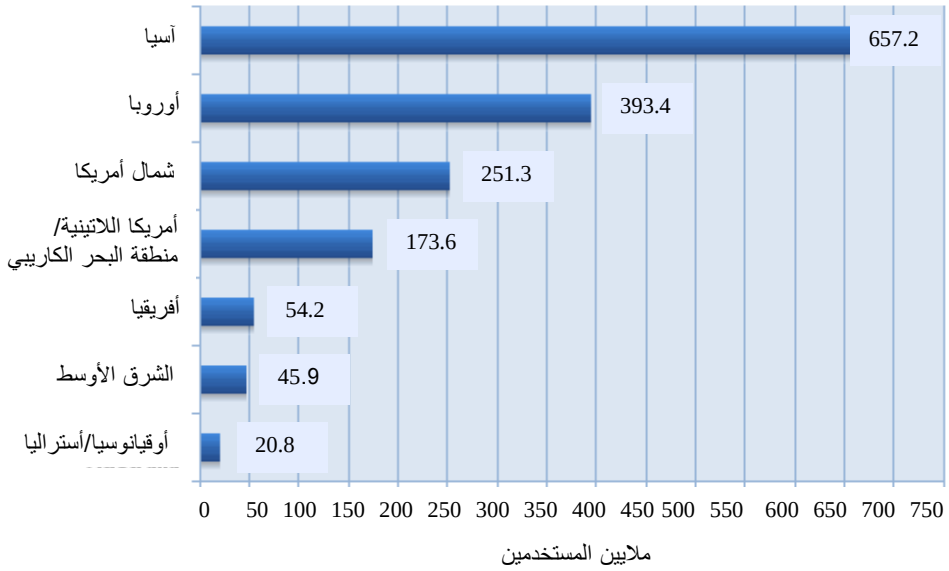
وينبغي أن يتضمن قانون الأعمال الإلكترونية تعريفات للأعمال الإلكترونية بمختلف أشكالها، وأن ينص على نطاق تطبيق القانون واستثناءاته، وغايات القانون، وقواعد الاعتراف بسلامة الوسائل الإلكترونية وحجيتها في التعاقد والإثبات، ومعايير وقواعد اعتماد الإرسال والاستقبال، ومعايير تحقق التعاقد على صعيد

الزمان والمكان المحددين لإرسال البيانات الإلكترونية واستلامها. كما يجب أن يشمل تنظيم سلطات وجهات التوثيق أو التصديق وصلاحياتها، وإحالة إلى التشريعات الأخرى الخاصة بحماية البيانات الشخصية والجرائم السيبرانية.

رابعاً- المستلزمات التقنية للأمن والحماية في الخدمات الإلكترونية

يؤول النجاح الكبير الذي حققته البرمجيات القائمة على شبكة الإنترنت خلال السنوات القليلة الماضية إلى نشوء نموذج الخدمات الإلكترونية كوسيلة لتلبية احتياجات المواطنين وتقديم الخدمات إلكترونياً عبر الشبكة. وقد شهد القرن الحادي والعشرون نمواً متصاعداً في أعداد مستخدمي شبكة الإنترنت، وانتشاراً ملحوظاً لتطبيقاتها في مجالات الأعمال والتجارة والخدمات الحكومية والتعليم والمعرفة والترفيه والسياحة والرعاية الصحية، وغيرها من الأنشطة الاقتصادية والاجتماعية والثقافية. ويعود ذلك إلى ما تقدمه هذه البرامج من مرونة في التعامل إلى حدٍ يمكن اعتبارها فيه وسيطاً يسهل التواصل بين المتعاملين، وييسر إجراء التعاقدات، وإبرام الاتفاقات التجارية، وتبادل المستندات والمدفوعات والرسائل في أي وقت وأي مكان، وبكلفة أدنى بكثير من كلفة البدائل الأخرى. فقد بلغ عدد المشتركين في شبكة الإنترنت أكثر من 542 مليون مشترك، منهم أكثر من 351 مليون مشترك في الشبكات العريضة الحزمة (Broad Band)، في حين تجاوز عدد مستخدمي الإنترنت 1.4 مليار مستخدم، بنسبة 22 في المائة من السكان، وذلك طبقاً لإحصاءات الاتحاد الدولي للاتصالات لعام 2007.

الشكل 3- استخدام الإنترنت في العالم وفقاً للمناطق



المصدر: Internet Usage Statistics. The Internet Big Picture. World Internet Users and Population Stats. Internet World Stats. www.internetworldstats.com/stats.htm.

التقديرات حول عدد مستخدمي الإنترنت هي كما يلي: 1 596 270 108 مستخدماً حتى 31 آذار/مارس 2009.

وبالرغم من الفرص التي يوفرها النمو المستمر في أعداد مستخدمي شبكات الاتصالات والإنترنت، والانتشار المتزايد للعمليات والخدمات الإلكترونية، تظهر أخطار وتحديات تهدد تلك العمليات وتقوض الثقة بها. أما هذه المخاوف والتهديدات الجديدة فهي ناتجة عن افتقار هذه التقنيات إلى الحصانة أمام المسيئين

والمتلاعبين، الأمر الذي أصبح يهدد القدرة على الاستمرار في تقديمها. ومن هنا الحاجة إلى بيئة آمنة تعزز ثقة المواطنين والجهات العامة والخاصة بهذه الخدمات الإلكترونية والاطمئنان إلى استعمالها.

وينطبق ذلك بشكل خاص على منطقة الإسكوا، حيث تتفاوت مستويات الاعتماد على تكنولوجيا المعلومات والاتصالات، ومستويات استعمال الخدمات الإلكترونية. ولكن البلدان الأعضاء تحتاج جميعها إلى بيئة آمنة لبناء الثقة بالخدمات الإلكترونية وتعزيز أمن هذه الخدمات. ويعرض هذا الجزء من الدراسة أبرز المخاطر التي تتعرض لها الحواسيب والمعلومات المسجلة بداخلها، والشبكات والتطبيقات والخدمات الإلكترونية. كما يشير إلى أهم الحلول التقنية الممكن توظيفها لرفع مستوى الأمن، ودعم الثقة بالمداولات والخدمات الإلكترونية.

ويتناول هذا الفصل العوامل الرئيسة التي تجعل من ضمان أمن تكنولوجيا المعلومات والاتصالات وسلامتها عملية صعبة ودقيقة، خصوصاً وأن الصعوبة تكمن في عناصر البنية الأساسية لهذه الشبكات. ويعرض هذا الفصل كذلك التحديات والأخطار التي تهدد الحواسيب وموارد المعلومات لدى الأفراد وضمن شبكة الإنترنت. كما يتوقف عند الأخطار التي تطال البنى الأساسية الحيوية الحرجة، كالطاقة والماء والنقل والاتصالات والمصارف والخدمات الحكومية والصحية. ويقدم الفصل عدداً من الحلول الفنية المقترحة، والمعايير الدولية المعتمدة في مجال إدارة نظم أمن المعلومات والتي تسمح، لدى تطبيقها وإدارتها بطريقة سليمة، بضمان مستوى مقبول من الأمن على الشبكات الإلكترونية ومواردها وتطبيقاتها. ويشير الفصل في جزئه الأخير إلى عدد من التجارب والمبادرات التي قامت بها بلدان عربية وأجنبية في مجال أمن تكنولوجيا المعلومات والاتصالات.

ألف- صعوبة ضبط أمن تكنولوجيا المعلومات والاتصالات

تعود صعوبة ضبط الأمن في استعمال الخدمات الإلكترونية إلى طبيعة التقنيات المستخدمة في عالم تكنولوجيا المعلومات والاتصالات بصورة عامة، وفي الفضاء السيبراني القائم على هذه التكنولوجيا بصورة خاصة. فحيث يكون بإمكان المستخدم أن يزور العالم الافتراضي وينجز أعماله عن بعد، وأحيانا من دون الكشف عن هويته، تتضافر هذه العوامل لتشكل مكونات لصعوبات محتملة في تصميم هذه النظم المعقدة أو تنفيذها أو إدارتها ومراقبتها. وتضاف إلى هذه المعادلة احتمالات الفشل والأخطاء البشرية، وأحيانا الكوارث الطبيعية، ويصبح معها ضبط الأمن في استعمال الخدمات الإلكترونية عبر شبكة الإنترنت عملية صعبة ومعقدة جداً. ويشير الشكل 4 إلى مصادر عدد من المشاكل التي يمكن أن تطرأ على بنية الإنترنت[68].

تتعدد السبل التي يلجأ إليها المهاجمون لاستغلال الثغرات ونقاط الضعف في شبكات تكنولوجيا المعلومات والاتصالات. وفي ما يلي عدد من أهم العوامل التي تيسر اختراق هذه الثغرات:

- الافتراضية والعالم الافتراضي: لا شك في أن تحرير المداولات والخدمات المختلفة من الإطار المادي والممارسات التقليدية لكي تصبح افتراضية، وتتم إلكترونياً عبر شبكة الإنترنت، يتيح فرصة لعدد كبير من المجرمين للاستفادة من تقنيات الاتصال المتقدمة، مثل تشفير المعلومات، وإغفال هوية المصدر والمواراة (Steganography)، والتعاون مع بعضهم البعض عبر الحدود بلا حاجة إلى الاجتماع فعلياً؛

(68) *Cybersecurity guide for developing countries*. ITU Edition 2007. www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf.

- تشبيك الموارد: إن تشبيك شبكات الحاسوب وموارد المعلومات على نطاق واسع يجعل منها أهدافاً تستقطب الجرائم الاقتصادية الإلكترونية، وذلك باستخدام التقنيات الحديثة. وتتصف جميع هذه الجرائم بانخفاض مستوى الخطر الجنائي الذي يتعرض له مرتكبوها من حيث إلحاق الضرر بهم، وذلك بسبب التعقيد الفني للهجمات وضعف الإجراءات القانونية عبر الحدود؛

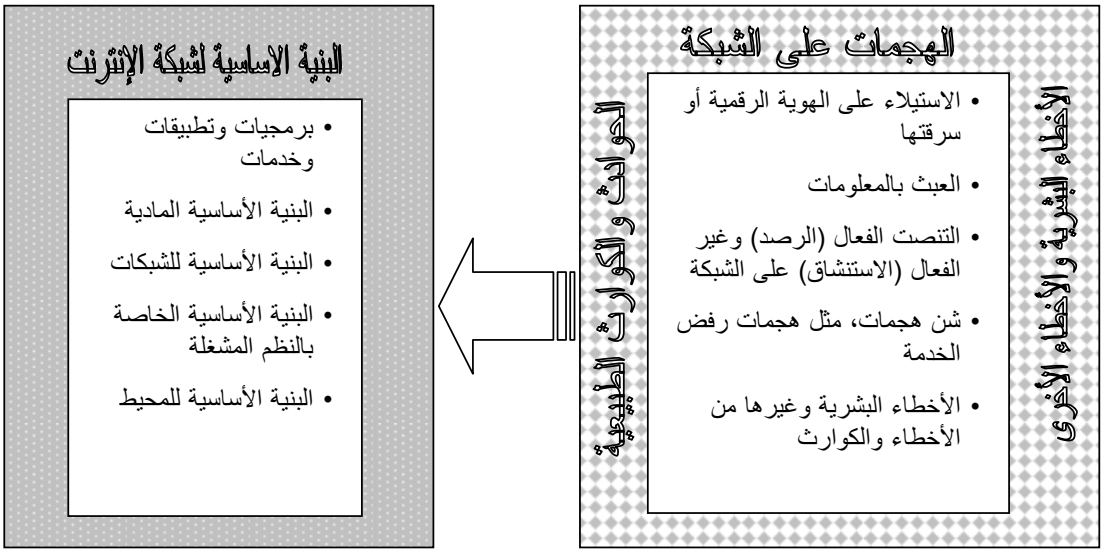
- انتشار المخترقين (Hackers): يستغل مخترقو شبكة الإنترنت الثغرات الأمنية في النظم والشبكات بغية التخطيط لجرائمهم. ولا شك في أن انتشارهم الواسع، وتوثيق أعمالهم في مكتبات خاصة، وأرشفة معلومات تتعلق بجرائمهم بغية بناء "المعرفة" حول هذا الموضوع كلها أمور تؤدي إلى تسهيل مهامهم التخريبية؛

- الثغرات والأخطاء: يستثمر المجرمون الأخطاء الفنية، وثغرات الإنترنت، وغياب إطار تشريعي موحد بين البلدان، وضعف التعاون الأمني بينها للقيام بأعمال إجرامية، مثل تبييض الأموال، والابتزاز، وسرقة حيز من زمن نظام المعالِج، وسرقة شيفرة المصدر، وقواعد البيانات؛

- صعوبة ملاحقة الجرائم: تعتبر الجرائم الحاسوبية متطورة جداً، وغالباً ما تتجاوز الحدود الجغرافية للدول بحيث تصبح ملاحقة مرتكبيها وتتبع آثارهم عملية صعبة ومعقدة، لا سيما بسبب صعوبة جمع الأدلة الجنائية؛

- ضعف الإطار القانوني: تصعب متابعة مرتكبي الجرائم الإلكترونية بسبب غياب الإطار التشريعي والقانوني الذي يسمح بذلك في عدد من الدول.

الشكل 4- الخرق الأمني على شبكة الإنترنت



باء- الأخطار المحدقة بالخدمات الإلكترونية

بهدف تحليل المخاطر التي تواجهها شبكات الحواسيب وموارد المعلومات والتطبيقات والخدمات المتوفرة عبرها ودراستها، ينظر الخبراء إلى هذه الأخطار من حيث طريقة تنظيمها وطريقة تنفيذها فنياً.

1- **من الناحية التنظيمية**، يمكن التمييز بين نوعين من الأخطار:

(أ) أخطار غير منظمة: وهي عشوائية ومحدودة الأثر، وتتحقق بتمويل محدود وبمهارات قليلة. ولا يمثل هذا النوع تهديداً للأمن الوطني؛

(ب) أخطار منظمة: وهي أشد خطراً، وتقوم بها جهات مدعومة مالياً، فتوظف أشخاصاً ذوي مهارات عالية. وقد يخدم هذا النوع من الأخطار أغراض التجسس الصناعي أو أغراضاً إجرامية أخرى.

وتتميز هذه الأخطار، المنظمة منها وغير المنظمة، بسرعتها في التطور الناجم عن سرعة تطور التكنولوجيا وصعوبة تحديد الثغرات الأمنية فيها، وإغفالها هوية مرتكبيها، واستخدامها برامج ووسائل مؤتمتة وتقنيات معقدة تتسبب جميعها بأضرار فادحة.

2- **من الناحية الفنية**: وهنا يعمل الخبراء في الأمن السيبراني على تصنيف الأخطار الإلكترونية على الشكل التالي:

(أ) أخطار فردية: وهي تستهدف الحاسوب الفردي للمستخدم، ومنها:

(1) سرقة كلمات المرور بهدف الدخول إلى نظم بعض الأفراد. ويمكن تحقيق ذلك بالتخمين، والانتحال، واستخدام أحصنة طروادة، وتحطيم التشفير المتبع لتخزين كلمة المرور، أو التجسس على المستخدم؛

(2) البريد الدعائي (Spam)، حيث تُرسلُ كمية كبيرة من البريد الإلكتروني بدون طلب المستخدم، لأغراض تجارية أو دعائية. وقد يكون هذا البريد وسيلة لنقل البرمجيات الخبيثة (Malware) التي تسبب الأذى للحاسوب المستقبل. ويَعد البريد الدعائي من مصادر الإزعاج الأولى التي يعاني منها الأفراد، حيث يَؤدي إلى ملء صناديق البريد وزيادة العبء على المخدمات. وبالرغم من بذل محاولات فنية عديدة لمنع انتشاره، كان البريد الدعائي في عام 2003 يمثل 54 في المائة من البريد الإجمالي. وفي عام 2005، تجاوز عدد الرسائل الدعائية في الولايات المتحدة الأمريكية 12 مليار رسالة، أي ما يمثل 38.7 في المائة من إجمالي الرسائل فيها[69].

(69) *Cybersecurity guide for developing countries*. ITU Edition 2007. www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf.

وللحد من البريد الدعائي، يستطيع الأفراد استخدام القوائم السوداء التي تسمح بتصنيف البريد حسب المخدم المرسِل، أي حسب عنوان بروتوكول الإنترنت (IP Address)، واستخدام المرشحات التي تحتاج إلى كلمات مفتاحية، واستخدام تقنية الملاءمة حسب الحاجة (Profiling) لتحديد ملامح محتوى الرسالة ومقارنتها بقاعدة بيانات المحتوى وفق تقنيات التنقيب عن البيانات؛

(3) البرمجيات الخبيثة: ويبدو أن عدد البرمجيات الخبيثة المنفذة على حواسيب الأفراد من دون علمهم في ازدياد. وهي موزعة إلى عدة أنواع، ومنها ما يلي:

أ- برمجيات التحميل (Downloaders)، وهي تُستخدم لتحميل البرامج عن بُعد؛

ب- برمجيات تسجيل الإدخال إلى الشبكة (key loggers)، حيث يتم تسجيل المحارف المدخلة عبر لوحة المفاتيح؛

ج- الروبوتات: وتسمى أيضاً الزومبي، وهي البرامج التي تسمح بالتحكم بالنظام عن بُعد بغية بناء جيش لامرئي من الحواسيب. ويتم الكشف يومياً عما يقارب 50 روبوتاً جديداً. وفي عام 2005، ألقت الشرطة الهولندية القبض على ثلاثة رجال يشتبه بإدارتهم شبكة تضم مئة ألف جهاز كمبيوتر من الروبوتات المجهزة لشن هجوم رفض الخدمة (DoS)، وهجمات أخرى تستهدف حسابات تسديد الفواتير إلكترونياً، وحسابات الشراء الإلكتروني الخاصة بضحاياهم (PayPal, eBay). وتشير توقعات إلى أن الهجوم بالروبوتات الشبكية (Botnets) سيصبح أكثر تنظيماً[(70)]؛

د- برمجيات التجسس (Spyware)، وهي تسجل المعلومات من دون علم المستخدم؛

•- برمجيات الدعاية (Adware)، وهي نوع من أنواع برامج التجسس التي تجمع معلومات عن المستخدم من أجل عرض الإعلانات في مستعرض الشبكة (Web Browser)، استناداً إلى البيانات التي تم جمعها من خلال أنماط الصَفحات التي يتصفحها المستخدم عادة؛

و- الفيروسات (Virus)، وتتكون من شيفرات خبيثة تُسقط نفسها على نظام المستخدم من دون معرفته. وتعتبر الفيروسات برامج ضارة لأنها قادرة على تكرار ذاتها لمرات عديدة، وقد يكون التكرار أو النسخ غير مطابق للأصل (Polymorphous). وتهاجم الفيروسات الحاسوب المصاب وبيئته المحيطة عبر نقل العدوى، والانتشار سريعاً في أجهزة أخرى. ويعتمد الفيروس في انتشاره على نظرية الاستنساخ والنشر، بالانتقال من حاسوب إلى آخر، أو إرفاق نسخ عنه مع برامج أخرى، وخصوصاً عبر البريد الإلكتروني. ويؤثر الفيروس على سلامة مصادر البيانات الموبوءة إلى حد قد يؤدي في بعض الأحيان إلى فقدان هذه المعلومات وإلى متاحية

(70) *Source*: Clusif. *Panorama de la cybercriminalit. 2005*: www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf.

النظام بأسره. وتشير التقديرات إلى وجود 000 50 من الفيروسات الجديدة المتداولة[71]. وهي تنتشر بسرعة فائقة عبر شبكة الإنترنت. ففيروس HTML_NETSKY.P مثلاً ضرب منذ عام 2004 حوالى 244 855 جهازاً. وتتكبد المؤسسات والشركات حوالى 42 مليون دولار للقضاء على الفيروسات؛

ز- الديدان (Worms): وهي جزء من رماز (Bits) الحاسوب. وهي تعبر الشبكة من دون تدخل المستخدم، وتعمل على إشغال موارد الحاسوب، مثل المعالج والذاكرة، فتجعل الحاسوب غير متاح للاستعمالات الأخرى. وتسمح الديدان أيضاً بالتحكم بالحاسوب عن بُعد أو بإشغال موارد الشبكة؛

ح- أحصنة طروادة (Trojans): وهي مخبأة داخل البرامج التقليدية أو ملفات المساعدة، وتسمح بالدخول إلى النظم وتحاول السيطرة عليها لسرقة زمن المعالجة وتغيير البيانات أو تدميرها. ويمكن أن تقوم أيضاً بالتجسس على الحاسوب، وقد تبقى في وضع النائم إلى حين حدوث الهجوم؛

ط- القنابل المنطقية (Logic Bombs): وهي فيروسات تُفعل عند وقوع حدث معين لمهاجمة النظام المضيف؛

ي- التصيّد (Phishing): وهو هجوم يستخدم برامج البريد الإلكتروني لكي يخدع مستخدمي الشبكة ويدفعهم إلى الكشف عن معلوماتهم الشخصية بحيث يمكن استثمارها لأغراض إجرامية.

ولمكافحة البرمجيات الخبيثة، على المستخدم أن يكون حذراً عند إرسال عنوانه الإلكتروني عبر الإنترنت. وعليه ألا يفتح الرسائل التي ترده من مصدر مجهول، وأن يحذف البريد الدعائي من دون قراءته وألا يجيب عليه، وألا ينقر على الروابط الواردة من صفحات الإنترنت وغير الموثوقة أو المجهولة المصدر. ويبين الإطار 3 أحد التهديدات الخارجية الخطرة، وهي سرقة الهوية الرقمية.

الإطار 3- سرقة الهوية الرقمية

تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الإنترنت ومستقبل الخدمات الإلكترونية. فقد تتعرض بيانات المستخدم الشخصية للسرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله، أو للزج باسمه في مداولات مشبوهة أو غير قانونية. ويستعين سارق الهوية عادة بمعلومات موجودة بالفعل على الإنترنت، وخصوصاً في مواقع شبكات التواصل الاجتماعية والمهنية المفتوحة، مثل MySpace وYouTube وLinkedin وFacebook أو الشبكات الخاصة بالخدمات الحكومية، مثل خدمات الضمان الاجتماعي، وشبكات الرعاية الصحية، ومواقع التجارة الإلكترونية، والأسواق الافتراضية، وشبكات المدفوعات الإلكترونية، والصارفات الآلية. فمن خلال تلك المواقع والشبكات، يسهل الوصول إلى أسماء الافراد، وإلى معلومات عنهم، وإلى عناوين إقامتهم، وتاريخ ميلادهم، وأصدقائهم، وصورهم الشخصية، وأرقام بطاقات الهوية، وبطاقات الضمان الاجتماعي، وما إليها[*].

وفي حالات سرقة الهوية الرقمية وانتحال الشخصية في ارتكاب فعل فاضح أو عمل مخالف للقانون، قد يتعرض الشخص المتضرر لمتاعب قانونية أو اجتماعية نتيجة عجزه عن إثبات براءته. ولا يتوقف ضرر سرقة الهوية الرقمية عند فقدان الأموال فحسب، بل قد يتعدى ذلك إلى الزج باسم الضحية في جرائم منظمة، وعمليات تمويل تنظيمات إرهابية

(71) *Source*: IPA/ISEC Computer virus incident report.

والإتجار بالمخدرات.

(*) http://edition.cnn.com/2006/TECH/internet/06/12/idtheft.internet/index.html.

(ب) التهديدات الشبكية: يتسم عصر المعلوماتية بربط مختلف الحواسيب بعضها ببعض من خلال الشبكات بحيث تكون قادرة على احتضان كميات كبيرة من البيانات[72]. ويتوقع ازدياد الاعتماد على الشبكات السلكية واللاسلكية في المستقبل إلى حدٍ تصبح معه هذه الشبكات معممة (Pervasive) وتزداد معه احتمالات المخاطر الأمنية. وتتنوع الهجمات التي تهدد الشبكات، ونذكر منها:

(1) عمليات الاختراق (Hacking): وهي عبارة عن سلسلة من العمليات المستخدمة في خرق نظم تكنولوجيا المعلومات. وأما المخترقون فهم الأفراد القادرون على اختراق هذه النظم. ويمكن تصنيف المخترقين حسب الفئات التالية:

أ- المخترقون المهنيون: ويمكن إدراج المرتزقة أو الجهات المنافسة للمؤسسة المستهدفة في هذه الخانة؛

ب- المخترقون الهواة، ومنهم:

'1' الفنيون الراغبون في إظهار مهارات فنية عالية؛

'2' صغار المبرمجين (Script Kiddies)، وهم غالباً صغار السن نسبياً. ويمارسون أولى درجات الاختراق، ويعملون عن طريق التطفل. فيقومون بتحميل البرامج المتاحة من الإنترنت بدلاً من كتابة الرماز الخاص بهم؛

'3' مخترقو الشبكة الناشطون (Hacktivisit)، وهم يستخدمون الهجمات الحاسوبية لأغراض سياسية أو دينية. فيطبقون تقنيات الاختراق على مواقع محددة من الإنترنت للتأثير على عملها، من دون إلحاق أضرار كبيرة بها. ومن الأمثلة على هذا النوع من الاختراق نذكر القنابل المؤتمتة عبر البريد الإلكتروني، والفيروسات، والديدان؛

'4' المحطمون (Crackers)، وهم يحاولون تحطيم أحد البرامج أو إحدى الشبكات بطريقة غير شرعية. وتطلق عليهم أيضاً تسمية المخترقين ذوي القبعات السوداء؛

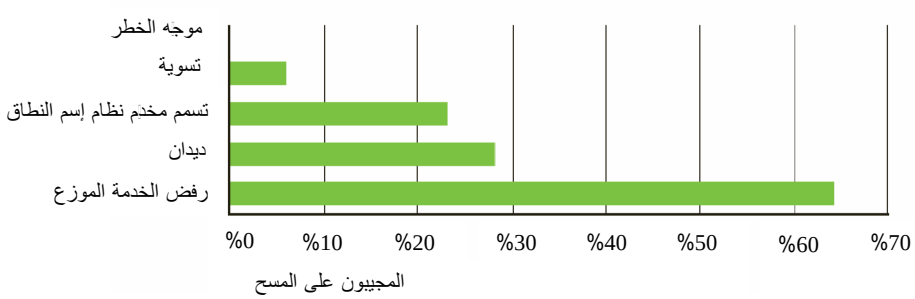
'5' المحطمون الطيبون (Sneakers)، وهم المخترقون ذوو القبعات البيضاء. ويحاولون اختراق النظم أو الشبكات للسماح لمالكي النظم باكتشاف الثغرات الأمنية فيها؛

'6' الأشخاص المضطربون نفسياً؛

(72) International Telecommunication Union. WSIS Thematic Meeting on Cybersecurity. *Background paper: A comparative analysis of cybersecurity Initiatives worldwide*. Geneva, 28 June-1 July 2005. www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

(2) رفض الخدمة (Denial of Service (DoS)): وهو يعني الهجوم على موقع محدد من حاسوب معين أو عدة حواسيب. ويهدف إلى زيادة الحمل على المخدمات بطلبات متكررة وعلى نحو يفوق قدرة المخدم على تلبيتها بحيث يتسببون بانهيار النظام الذي يصبح عاجزاً عن أداء عمله حسب الغاية التي صمم لأجلها. ويمكن توجيه هذه الطلبات من عدة أماكن موزعة وتسمى حينئذ بالهجوم الموزع (Distributed Denial of Service (DoS. ووفقاً لاستبيان قام به فريق الاهتمام الخاص المعني بالاتصالات الرقمية في عام 2005 والذي شمل 36 مزوداً للخدمة، تحتل هجمات رفض الخدمة المرتبة الأولى في قائمة الهجمات (انظر الشكل 5) حيث يتعرض كل مزود لما يقارب 40 هجوماً شهرياً يؤثر بشكل مباشر أو غير مباشر على عملائه؛

الشكل 5- أهم المخاطر التي يواجهها مزودو الخدمة[73]



(3) تغيير الأثر (Defacement): وهو يهدف إلى تغيير صفحة الإنترنت واستبدالها بصفحة جديدة ذات محتوى مختلف؛

(4) انتحال (Spoofing): وهو يتم باختطاف جلسة اتصال معتمدة على بروتوكول التحكم في الإرسال، أو ما يسمى ببرتوكول مراقبة الإرسال، وبالتالي استخدام أرقام البوابات، والدخول عبر الجدران النارية، وإنشاء وصلة "آمنة" بين المخترق والهدف. وعند استخدام بروتوكول برقية بيانات المستخدِم، يمكن أن يتعرض النظام لتهديدات أمنية أشد خطورة. وبنتيجة ممارسات الانتحال هذه، يتم السطو على عنوان بروتوكول الإنترنت عن طريق جهاز مخول دخول الشبكة، واستخدام العنوان المذكور لاختراق الشبكة والنظم. ويتمكن المعتدون على الشبكات ومستخدمو هذه البروتوكولات من تنفيذ عدة أعمال تخريبية مثل شل الشبكة، أو توجيه الحزم إلى أجهزة أخرى غير الأجهزة المقصودة (كأجهزة المعتدين مثلاً)، أو تحميل النظم على الشبكة تحميلاً زائداً، وذلك بإغراقها بالرسائل غير المرغوب فيها، أو منع المرسل من نقل البيانات عبر الشبكة، أو السيطرة على تدفق الحزم وإعاقة حركة المرور عبر الشبكة، وهذا يؤثر سلباً على أدائها وبالتالي على موثوقيتها؛

(73) C. Labovitz. D. McPherson. 2005. *SP Infrastructure Security Survey Results*. www.nanog.org/mtg-0510/pdf/labovitz.pdf.

(ج) التهديدات المحدقة بالبنى الأساسية الحيوية الحرجة: تشن على الفضاء السيبراني هجمات لأغراض إرهابية تطال بعض المواقع الحساسة التي تُعد جزءاً من البنى الأساسية الحيوية في الدولة والمجتمع، مثل قطاعات الطاقة، والماء، والنقل، والاتصالات، والصحة، والخدمات الحكومية والقطاع المصرفي. ويستغل المعتدون على هذه المواقع نقاط الضعف في هذه البنى الحيوية الحرجة، خصوصاً بعد أن أصبحت جميعها تعتمد في عملها على تكنولوجيا المعلومات والاتصالات، وبعد أن أصبحت متاحة للجمهور عبر الإنترنت. ونظراً إلى أهمية هذه البنى من الناحية الاستراتيجية، ينبغي تشديد الحماية على البوابات (Gateways) التي تسمح بالوصول إلى شبكات المنشآت الحرجة. فيتعين على الهيئات الإقليمية والوطنية إنشاء فرق للإشراف على حماية هذه البنى الأساسية الحيوية الحرجة، وذلك من خلال تصميم خطط للصيانة وتنسيقها، وإدراج الحلول الأمنية اللازم اعتمادها في حالات الطوارىء، وعندما تهاجَم هذه المنشآت أو البنى الأساسية جميعها في وقت واحد. وتُصنف الأحداث الضارة بالبنى الأساسية للمعلومات ضمن ثلاثة أنواع:

(1) الإخفاق (Failure): ويمكن أن يحدث بسبب عجز في النظام بحد ذاته، أو بتأثير عنصر خارجي يعتمد عليه النظام، أو بسبب أخطاء في تصميم البرمجيات، أو بسبب تردي الأجهزة المستخدمة، أو نتيجة أخطاء بشرية، أو بيانات فاسدة تولد داخل النظام؛

(2) الحوادث: وهي أحداث غير متوقعة وتطرأ عشوائياً، مثل الكوارث الطبيعية؛

(3) الهجمات: وغالباً ما تكون أحداثاً يقودها "عدو" خارجي. ولكن الإحصاءات تشير إلى أن المصادر الداخلية هي أحد أهم مصادر هذه الهجمات. وتتمثل بالأفراد الذين يعملون أو كانوا يعملون في المؤسسة والمخولون استخدام نظم المعلومات فيها؛

(د) أخطار التطبيقات: وهي جرائم اقتصادية تساهم شبكة الإنترنت في انتشارها الواسع وعدم خضوعها للقيود الجغرافية للدول بسبب طبيعتها الافتراضية. ونذكر منها تبييض الأموال، أي نقل الأموال الناتجة عن نشاط غير قانوني إلى نشاط قانوني، وبيع سلع وهمية وممارسة ألعاب الرهان.

جيم- حماية الفضاء السيبراني والحلول الفنية

1- المتطلبات العامة لحماية الفضاء السيبراني

تساهم الحلول الأمنية في تلبية الحد الأدنى من معايير أمن المعلومات مثل توفر البيانات ومتاحيتها وتكاملها وسلامتها وسريتها، والتعرف والاستيقان (Authentication) للتحقق من الهوية، وعدم الإنكار (Non Repudiation) للتحقق من وقوع الأحداث فعلياً.

وينبغي أن تضمن الحلول الفنية لمواجهة التهديدات الإلكترونية توفير الخصائص الضرورية لأمن المعلومات والخدمات[74]. وهي كما يلي:

(أ) **الحماية المادية**: أي حماية المواقع المادية التي تحتوي على المخدمات، ومنابع الطاقة، والتكييف، والموارد المختلفة من العبث ومن النفاذ غير المخول إليها؛

(ب) **المتاحية**: أي تأمين متاحية البيانات، واستمرارية الخدمات والنظم والبيانات ومكونات البنية الأساسية للنظم. وتقاس المتاحية بالمدة التي تبقى فيها الخدمة (أو المورد) متاحة ومشغلة بدون توقف. وترتبط المتاحية ارتباطاً وثيقاً بإمكانية الوصول إلى الخدمة (أو المورد)؛

(ج) **تكامل البيانات وسلامتها**: ويقصد بها سلامة البيانات والخدمات، وحمايتها من التغيير الطارئ، المتعمد وغير المتعمد، ومن العبث والتدمير. ويتم توفير هذه الحماية عبر بعض التقنيات كالتلبيد (Hash)، وتشفير البيانات، والحماية من الفيروسات والديدان وأحصنة طروادة، ومن خلال ضبط النفاذ إلى الخدمة؛

(د) **السرية**: وتعني حماية المعلومات والمداولات والخدمات من اطلاع غير المخولين عليها، وذلك عبر التشفير وضبط النفاذ. فالتشفير يساعد على حماية سرية المعلومات خلال تنقلها عبر الشبكات وفي أثناء تخزينها؛

(•) **التعرف والاستيقان**: وهو التحقق من هوية كيان محدد عبر خدمة استيقان معينة، أو كلمة مرور، أو شهادات المصادقة. وتسمح إجراءات التعرف والاستيقان بضمان سرية البيانات وسلامتها، بحيث يقتصر النفاذ إلى أي مورد على الأشخاص المخولين ويستوجب التعرف عليهم. كما تسمح إجراءات التعرف والاستيقان بضمان عدم التنصل والإنكار في المداولات الإلكترونية، وتحديد الكيانات المتعاملة مع بعضها البعض، وتتبع الرسائل والتأكد من وجهتها؛

(و) **عدم الإنكار**: ويرتبط هذا المفهوم بمفهوم المحاسبة والملاحقة والتدقيق، حيث تستوجب بعض الحالات التأكد من حدوث مداولة أو حدث معين عبر الشبكة الإلكترونية. فتحديد المسؤولية يفترض مسبقاً وجود آليات تسمح بالتعرف على هوية الأفراد وعلى أعمالهم، وتتيح تسجيل مجريات الأحداث بطرق سليمة.

2- حلول فنية لمواجهة التحديات الإلكترونية

في ضوء الواقع اليومي للمشاكل الأمنية التي تواجهها البنى الأساسية بمعظمها، ونظراً إلى توفر العديد من الحلول الفنية المقترحة، وازدهار سوق الأمن ومفاهيمه في الفضاء السيبراني، تطرح الأسئلة التالية نفسها:

(أ) هل تتلاءم الحلول الأمنية المقترحة مع المتطلبات الأساسية لحماية الفضاء السيبراني؟

(74) Alexander NTOKO. *E-government and IP symposium for the Arab Region. Building Trust and Security for e-Government.* ITU. 2004. www.ituarabic.org/Previous_Events/.../01-ITU%20BDT-Building%20Trust%20and%20Security%20for%20egovt.

(ب) هل يتم إعداد هذه الحلول وإدارتها بشكل صحيح؟

(ج) هل يمكن استخدام هذه الحلول بصيغتها المقترحة، أم يجب تكييفها أو تطوريها بشكل ديناميكي حسب البيئة المعنية بها؟

(د) هل يمكن أن تصلح هذه الحلول للحد من مركزية السلطة المسندة إلى مدير النظام؟

(•) كيف يمكن استخدام هذه الحلول لمعالجة المشاكل الأمنية التي تعزى إلى الإهمال، والأخطاء البشرية، وعيوب التصميم والتركيب؟ وهل تعود أساساً لمعالجة مشاكل في إدارة التكنولوجيا ومواطن الضعف فيها؟ أم أنها تعالج المشاكل التي تواجهها الحلول الأمنية بحد ذاتها؟

وبالرغم من هذه التساؤلات كلها، لا يمكن إلا الاعتراف بأن عدداً من الحلول الفنية المقترحة يسمح بضمان مستوى مقبول من أمن الشبكات الإلكترونية في حال تطبيقه وإدارته بطريقة سليمة. أما أكثر هذه الحلول الفنية شيوعاً فهي التالية:

(أ) **الحماية المادية**: تتم حماية المواقع المادية من العبث والنفاذ غير المخول إليها باستخدام تقنيات متعددة، مثل وضع نظم كاميرات مراقبة (Closed-Circuit Television Camera CCTV)، وأقفال إلكترونية تعتمد على كلمات مفتاحية أو بطاقات تعريف أو نظم تعريفية بيولوجية مختلفة (مثل بصمات أصابع اليد، أو العين، أو الصوت، وما إليها) للتعرف على الأشخاص المخولين الدخول إلى هذه المواقع. كما تستوجب الحماية المادية هذه تطبيق إجراءات الحماية من الكوارث الطبيعية كالصواعق والحرائق والزلازل؛

(ب) **المتاحية**: يستدعي تأمين متاحية الخدمات أولاً توفير الشروط التالية المتعلقة بمتاحية البنى المادية والتجهيزات التي تعتمد عليها هذه الخدمات، ومن ثم ضمان متاحية البيانات:

(1) التجهيزات والبنى الأساسية: لتأمين الطاقة الكهربائية بشكل دائم ومنتظم تستخدم عادة تقنيات التغذية المستمرة بالتيار الكهربائي (RAID Technologies). ولتأمين استمرارية العمل عند حدوث أعطال أو توقف بعض التجهيزات عن العمل، تُستخدمَ تقنيات تكرار التجهيزات والمخدمات ووحدات التخزين؛

(2) النظم والبيانات والخدمات: تستخدم تقنيات النسخ الاحتياطي الدوري للبيانات، كما تستخدم بعض التقنيات للحماية من عمليات الإختراق الأمني التي قد تؤدي إلى إيقاف الخدمة أو رفضها DoS؛

(ج) **تكامل البيانات وسلامتها**: يجب تأمين سلامة جميع البيانات، المتوفرة في وحدات التخزين أو المتبادلة عبر خطوط الشبكة. فقد جَهزت نظم التشغيل الحديثة بمعظمها بتقنيات تجيز التحقق من سلامة البيانات المتاحة في وحدات التخزين، ومنها تقنيات الحفظ الاحتياطي (Backup)، والكشف عن الأخطاء (Checksum)، والمصفوفات المتكررة من الأقراص المستقلة (RAID). وأما ضمان سلامة المعلومات المتبادلة عبر خطوط الشبكة فيتم عن طريق تقنيات مختلفة ترتكز على عدد من بروتوكولات وخدمات الاتصال المستخدمة[75].

(75) www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf، مرجع سبق ذكره.

بروتوكول الإنترنت - النسخة 4 (IPV4): تقوم هذه النسخة من بروتوكول الإنترنت بكبسلة البيانات المراد إرسالها عبر الإنترنت ضمن رزم من بروتوكولات الإنترنت، بحيث يمكن تسييرها عبر الشبكة إلى الوجهة المطلوبة. وتحتوي كل رزمة على عنوان بروتوكول الإنترنت العائد إلى الجهة المرسلة وذلك العائد إلى الجهة المستقبلة. ولا يتضمن هذا البروتوكول أي آلية لضمان أمن الخدمات لأنه لا يحتوي على أي وسيلة لاستيقان مَصدر الرزمة أو وجهتها، أو لضمان سرية البيانات المنقولة أو عناوين برتوكولات الإنترنت الداخلة في تحويل المعلومات بين الكيانين (أي بين المرسل والمتلقي). ولذلك، لا يمكن التحقق مما إذا كانت المعلومات متسلسلة بالشكل الصحيح. إلا أن هذا البرتوكول لا يزال قيد الاستخدام في الاتصال عبر الإنترنت. ومن هنا، كان لا بد من إضافة نظم لحماية التطبيقات عند استخدامه. ولمواجهة هذا النقص في نوعية الخدمة التي توفرها هذه النسخة من بروتوكول الإنترنت، يقترح الخبراء تثبيت بروتوكول مراقبة الإرسال في نهاية النظام لكي يوفر خدمة نقل يمكن الاعتماد عليها. ويبقى استخدام هذا البروتوكول غير آمن بالكامل.

بروتوكول الإنترنت - النسخة 6 (IPV6): يتميز هذا البروتوكول باتساع مجال العناوين المتاحة بسبب ترميز العنوان على 128 بت، بدلاً من 32 بت. وهو يسمح بإنشاء شبكات افتراضية، ويدعم الاستيقان وتقنيات التشفير، والتحقق من سلامة البيانات، ويجيز تبسيط عمليات التسيير (Routing) بفضل الترويسة السهلة للرزم. غير أن استخدام هذه النسخة من بروتوكول الإنترنت لا يزال محدوداً، ولم تصدر أي توصيات دولية لدعم انتشاره. ولهذا السبب، وبهدف ضمان مستوى معين من الأمن على الشبكات، شاع استخدام حل وسط، وهو أمن بروتوكول الإنترنت الذي يتوافق مع النسختين 4 و6 من بروتوكول الإنترنت.

أمن بروتوكول الإنترنت (IPSec): يسمح هذا البروتوكول بالحفاظ على سرية المعلومات المخزنة داخل الرزم، فهو يسمح بالاستيقان عبر حقول الترويسة، ويحقق وصلة "آمنة" بين المرسل والمستقبل. وتسمح ترويسة الاستيقان بالتحقق من أن البيانات لم تتغير أثناء النقل، وأن عنوان المصدر هو ذاته المذكور في الرزمة. كما تسمح ترويسة كبسلة الحمل الأمني ((Security Payload Header Encapsulating (ESP) بتنفيذ آليات التشفير، مثل خوارزمية معيار تشفير البيانات أو شفرة "ريفيست 5" (RC-5) أو الخوارزمية الدولية لتشفير البيانات. ويمكن تضمين جميع وظائف هذا البرتوكول في النسخة 6 من بروتوكول الإنترنت، وهو يستخدم أيضاً في دعم التجهيزات والتطبيقات التي لا تزال تعتمد على النسخة 4 من بروتوكول الإنترنت.

طبقة المقبس الآمنة ((Secure Sockets Layer (SSL) أو أمن طبقة النقل (Transport Layer Security ((TLS): وهي وسيلة بديلة للبروتوكولات الآمنة، واستخدامها واسع الانتشار في العمليات التجارية عبر الإنترنت. كما أنها تضمن أمن عملية التبادل بين التطبيقات حيث يجري استيقان الكيانين المتخاطبين وفق إجراءات الشهادات والجهة الثالثة الموثوقة. ويتم تشفير البيانات المرسلة عبر قناة اتصال طبقة المقبس الآمنة. وقد اعتُمد الجيل الثالث من هذه الطبقة كمعيار دولي، وأطلقت عليه تسمية أمن طبقة النقل.

بروتوكول النقل الآمن للنصوص المترابطة (S-HTTP): وهو حل بديل لطبقة المقبس الآمنة، ويقدم الإمكانات الأمنية نفسها مع شروط منح الشهادات، ولكنه لا يدعم إلا التدفق عبر بروتوكول نقل النصوص المترابطة ولم يلق هذا البرتوكول استحساناً لدى التقنيين، فاستخدم عوضاً عنه بروتوكول النقل الآمن للنصوص المترابطة الذي يعتمد على قواعد برتوكول أمن طبقة النقل لحماية صفحات الإنترنت.

برتوكول تعادل الخصوصية السلكي ((Wired Equivalency Privacy (WEP) وبروتوكول النفاذ المحمي ((Wi-Fi Protected Access (WPA) من إنتاج مجموعة واي-فاي: ويستخدم هذان البرتوكولان لضمان أمن الاتصالات اللاسلكية المحلية التي تعتمد على قواعد وتقنيات واي-فاي. إلا أن برتوكول تعادل الخصوصية السلكي يعاني من ثغرات أمنية كبيرة وهو سهل الاختراق، لذلك لا ينصح باستخدامه حالياً، ويعتبر بروتوكول النفاذ المحمي الجيل البديل عنه.

ونلاحظ أن العديد من برتوكولات النقل الآمن تتضمن تطبيقا لخوارزميات تشفير، إضافة إلى نظم للتحكم بالنفاذ، حيث تتحقق السرية من خلال تطبيق التشفير على البيانات. وسوف يتم شرح أهم هذه التقنيات لاحقاً في هذا الفصل.

ولا يكفي استخدام البروتوكولات لحماية البيانات عبر شبكة الإنترنت ومنع المخاطر. فقد تحتاج المؤسسة إلى وضع سياسة للتحكم بالتدفق الصادر من شبكتها ومواردها أو الوارد إليها لضمان أمنها بطريقة شبه كاملة، وذلك عبر استخدام تقنيات الجدران النارية.

الجدران النارية (Firewalls): وهي نظام لترشيح تدفق البيانات، ومنعها في بعض الحالات. وهي تحلل التدفق وتجيز عبوره إذا كان يستوفي عدداً من الشروط المسبق تحديدها، وهذا الأمر يسمح بتجزئة بيئة بروتوكول الإنترنت إلى مناطق عدة تختلف بحسب درجة الأمن المطبقة عليها. وأما أنواع الجدران النارية فعديدة، وهي تُصنف حسب مستوى ترشيح البيانات الذي توفره، ونذكر منها الطبقة 3 (بروتوكول الإنترنت IP)، والطبقة 4 (بروتوكول التحكم بالإرسال/بروتوكول برقية معطيات المستخدم TCP/UDP) والطبقة 7 (بروتوكول نقل الملفات/بروتوكول نقل النصوص المترابطة FTP/HTTP). ولجعل البيئة الداخلية لمؤسسة ما أكثر أمناً، يمكن استخدام جدار ناري للتطبيقات، أو ما يسمى بوكيل إنترنت Proxy، وهو يمثل نقطة عبور إلزامية لكافة التطبيقات التي تتطلب النفاذ إلى الإنترنت. إلا أن الجدار الناري لا يحقق الحماية المطلقة للموارد في المؤسسة بالرغم من كل ما يقدمه من أمان في عملية الترشيح.

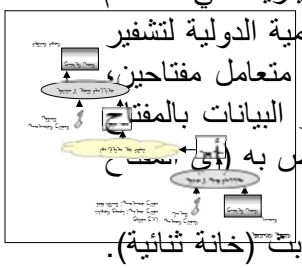
ضبط النفاذ (Access Control): لعل استيقان الشخص، أي التأكد من هويته باعتماد إحدى التقنيات كرقم التعريف السري، أو السمات البيولوجية للمستخدم مثل شبكة العين أو البصمة أو الصوت، أو مزيج من هذه التقنيات، يشكل أهم مكونات أمن المعلومات والخدمات. ويجب تشديد الحماية على مخدم الاستيقان كي لا يكون عرضة لأي ثغرة تهدد أمنه، لأن مصير البنية الأساسية للاتصالات والمعلومات رهن به. وعند تخزين السمات البيولوجية، يجب التأكد من عدم العبث بها. كما ينبغي التنبه إلى طبيعة هذه السمات التي تتيح في بعض الأحيان مجالاً للشك في هوية المستخدم (مثل تشابه الصوت في حالة التوائم).

حماية مخدمات نظام إسم النطاق ((Domain Name System (DNS): تعتمد جميع التطبيقات على هذه المخدمات التي تؤدي دوراً أساسياً في ترجمة عناوين النطاقات إلى عناوين شبكية، وفي تسيير البيانات. ويطبق على هذا النوع من المخدمات عدد من آليات الأمن، مثل ضبط النفاذ، والاستيقان، وقيد الدخول، والتكرار، والانسجام، وتشفير الطلب، والاستجابة.

تشفير البيانات[76] **(Encryption)**: تساهم هذه التقنيات في المحافظة على سرية البيانات، والتأكد من سلامتها، والتحقق من هوية المتعاملين بها. ويمكن التمييز بين نوعين رئيسين من تقنيات التشفير هما التشفير المتناظر (Symmetric) والتشفير اللامتناظر (Asymmetric)، وذلك باستخدام ما يسمى بالمفاتيح

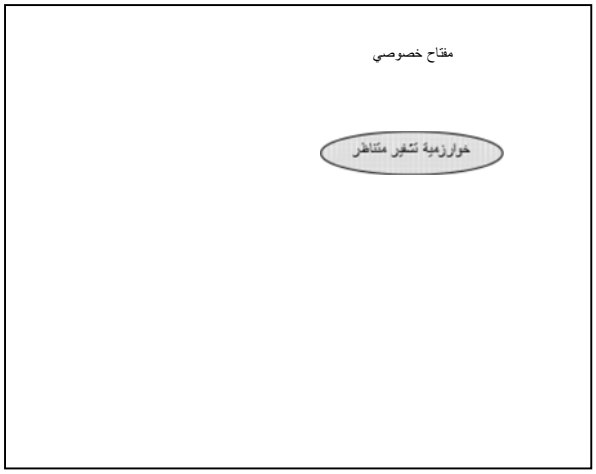
(76) www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf، مرجع سبق ذكره.

الخصوصية والمفاتيح العمومية. ويتوقف مستوى الأمن في هذه التقنيات على قدرة خوارزميات التشفير على إدارة هذه المفاتيح بطريقة آمنة، وعلى طول تركيبة المفتاح الذي تحدده هذه الخوارزميات. ويعتمد التشفير المتناظر على تقانات المفتاح الواحد الذي يستخدم للتشفير ولفك التشفير. وتمتاز هذه التقنية بسرعة أداء عالية إلا أن استخدامها يتطلب توفير آلية آمنة لتبادل المفاتيح. ومن أهم الخوارزميات المعيارية التي تستخدم للتطبيقات العامة والتجارية نذكر معيار تشفير البيانات 3 ومعيار التشفير المتقدم والخوارزمية الدولية لتشفير البيانات (AES, 3DES, IDEA). وأما التشفير اللامتناظر، فيعتمد على امتلاك كل شخص أو متعامل مفتاحين، مفتاحاً عاماً أو معلناً يستخدم للتشفير ومفتاحاً خاصاً لفك التشفير. ويقوم المرسل بتشفير البيانات بالمفتاح المعلن للمستقبل (أي المفتاح العام)، بينما يقوم المستقبل بفك التشفير باستخدام المفتاح الخاص به (أي المفتاح الخاص). ويوضح الشكل 6 آليات التشفير المتناظر والتشفير اللامتناظر.



وتستخدم خوارزميات التشفير اللامتناظر مفاتيح يتراوح طولها بين 512 و1024 بت (خانة ثنائية). ومن أشهرها خوارزمية "ريفيست" و"شامير" و"أديلمن" (Rivest Shamir Adleman RSA) وخوارزمية ديفي-هيلمن (Diffie-Hellman) وخوارزمية الجمال (El-Gamal). وتمتاز هذه التقنية بالتغلب على مشكلة تبادل المفاتيح، ولكن ليس على مشكلة الاستيقان والتأكد من صحة المتخاطبين، خصوصاً في حال سرقة المفاتيح. وقد ولدت هذه التقنية الحاجة إلى نظام لإدارة المفاتيح، وتخزين المفاتيح العمومية وإدارتها بشكل آمن وغير قابل للاختراق.

الشكل 6- التشفير المتناظر والتشفير اللامتناظر



البنية الأساسية للمفاتيح العمومية: تستخدم البنية الأساسية لإدارة المفاتيح لتنفيذ نظم التشفير اللامتناظر، حيث تتعاون مع بعضها البعض عدة مكونات هي سلطة المصادقة، وسلطة التسجيل، ودليل شهادات المصادقة الصالحة والملغاة، ونظام حفظ شهادات المصادقة والمستخدمين النهائيين. ويعمل نظام إدارة المفاتيح على توليد زوج فريد من المفاتيح وحفظه واسترجاعه، وإدارة الشهادات الرقمية وتجديدها وإصدارها وإلغائها، وتزويد الجهات المعنية بالمفاتيح العمومية والمصادقة عليها، وتوقيع الشهادة الرقمية.

الشهادات الرقمية[77]: تسمح هذه التقنيات بالتحقق من هوية الأفراد والتعرف عليهم (Non Repudiation). وتعتبر الشهادة الرقمية بطاقة الهوية الرقمية لكيان مادي أو اعتباري أو لمورد ما، وهي تحتوي على اسم السلطة المانحة، ومعلومات عن حامل الشهادة والمفتاح العام، والتوقيع الإلكتروني لسلطة المصادقة. ويقدم المعيار X.509 إطار عمل بنيوي لإنشاء خدمة الاستيقان بالاعتماد على الشهادات الرقمية، ويحدد بنية الشهادة الرقمية. ويبين الشكل 7 العناصر الرئيسة التي تتكون منها الشهادة الرقمية.

ويمكن التأكد من صحة الشهادة عند استيقان المفتاح العمومي للمرسل وتطبيق خوارزمية التلبيد. وبالمقابل، يمكن معرفة صحة الشهادة كما يمكن إلغاؤها إذا أصبحت البيانات التي تحتويها قديمة. وفي هذه الحالة، يجب إبلاغ كافة الجهات المصادقة.

الشكل 7- العناصر الرئيسة للشهادة الرقمية[78]

النسخة
الرقم التسلسلي
خوارزمية التوقيع
إسم الجهة المانحة
يجب أن يكون الزوج المركب من الرقم التسلسلي والجهة المانحة فريداً
الصلاحية
إسم الكيان
المفتاح العمومي للكيان
معلومات إضافية حول الكيان أو آليات التشفير
توقيع الشهادة
خوارزمية ومعايير التوقيع والتوقيع الفعلي

وتمثل شهادة المصادقة هوية المستخدم على الإنترنت، وتسمح بخلق جو من الثقة بين شخصين أو مخدمين أو مسيِّرين (Routers). وتسمح المصادقة الرقمية عموماً بالتحقق من الهوية، ونشر قيم المفاتيح العمومية والمعلومات المرتبطة بها. وتمثل المصادقة الرقمية سجلاً إلكترونياً، وهي تصدر عن جهة موثوقة تسمى سلطة المصادقة التي تعد مسؤولة عن صحتها. ويَربط المفتاح العمومي بشهادة المشترك وباسمه. وتُطلق على هذه السلطة عموماً تسمية الجهة الثالثة الموثوقة، كما تسمى أحياناً بسلطة التسجيل.

وتهدف هذه السلطة إلى إصدار رقم تشفير وشهادة مصادقة بعد التوثق من طلب العميل. وهي تسمح أيضاً بالتوثق من صحة البيانات وبتحقيق ميزة عدم الإنكار. ونظراً إلى تعدد سلطات المصادقة، تظهر بعض المشكلات التي تتعلق بضمان توافق هذه السلطات مع بعضها. وتتولى سلطة المصادقة إصدار الشهادات والتحقق من صحتها. أما السلطة الجذر فتعمل على تحديد سياسة المصادقة. وتضطلع سلطات التسجيل بمهمة التحقق، كما يهتم مزودو خدمة المصادقة بإصدار الشهادات. ويمكن التمييز بين ثلاثة أنواع من الشهادات:

(77) www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf، مرجع سبق ذكره.

(78) www.itu.int/ITUD/cyb/publications/2007/cgdc-2007-e.pdf، مرجع سبق ذكره.

- الشهادة الشخصية: وهي تضم إسم الشخص والمفتاح العمومي. وتفيد هذه الشهادة في تشفير الرسائل الإلكترونية، والتأكد من هوية الشخص عند اتصاله بالمؤسسات التي تقدم خدماتها إلكترونياً، كالمصارف مثلاً؛

- شهادة المخدم: وهي تضمن أمن الاتصالات بين المخدم والعميل؛

- شهادة الشبكات الافتراضية الخصوصية ((Virtual Private Network (VPN): وهي تتيح الاتصال الآمن بين مركز المؤسسة وفروعها.

مستخلص الرسالة والتوقيع الإلكتروني: تستند هذه الخدمة، التي تضمن عدم الإنكار وتكامل البيانات والاستيقان، إلى معيار شهادات المصادقة X.509. وتعتمد هذه الطريقة على توليد مستخلص الرسالة Digest من الوثيقة، وتشفيره بالمفتاح الخاص للمرسل، وإرساله مع الوثيقة. ويتم توليد مستخلص الرسالة باستخدام عملية التلبيد، ثم يَطبق هذا المستخلص على البيانات، بحيث يعيد المستقبِل حساب قيمة التلبيد من البيانات السابقة باستخدام العملية ذاتها. ويَستخرج مستخلص الرسالة عند الاستقبالَ من التلبيد بعد فك تشفيره بالمفتاح المعلن للمرسل. وأما عدم تطابق التشفير مع المفتاح المعلن فيدل على تغيير في البيانات. ومن أشهر عمليات التلبيد المعتمدة في هذا المجال خوارزمية التلبيد الآمن[79] ((Secure Hash Algorithm (SHA) وخوارزمية النسخة 5 من مستخلص الرسالة[80] ((Message Digest Algorithm 5 (MD5). ويشكل ناتج تشفير مستخلص الرسالة بالمفتاح الخاص للمرسل التوقيع الرقمي للمرسل، حيث يعبر عن الشخص المرسِل، ويضمن تكامل البيانات المرسلة، الأمر الذي يعزز الثقة بالرسالة. ويتطلب فك الرسالة عندئذ استخدام المفتاح العمومي.

أمن التطبيقات: يرعى كل تطبيق من تطبيقات الخدمات الإلكترونية قواعد أمن عامة وخاصة، وهي تختلف باختلاف نوع الخدمات التي يقدمها ومدى حساسية المعلومات المتبادلة. وأما طبقة المقبس الآمنة[81] فهي أحد أهم النظم التي تعزز أمن تنفيذ التطبيقات على شبكة الإنترنت، لا سيما تلك المرتبطة بأمن الخدمات الإلكترونية المالية. ويتميز هذا النظام بانتشاره الواسع وسهولة استخدامه. فهو لا يشكل عبئاً على حاسوب العميل، ويبني الثقة بينه وبين البائع. وتعتمد طبقة المقبس الآمنة على التشفير في نقل البيانات بين متصفح الإنترنت والمخدم، ولا يمكن تغيير البيانات المرسلة أو اعتراضها أثناء النقل. وهي تسمح باستيقان التاجر عبر شهادة المخدم SSL. وتجدر الإشارة إلى المداولة الإلكترونية الآمنة[82] (Secure Electronic Transaction ((SET) التي تشكل حلاً آخر إنما أكثر تعقيداً، لأنها تعتمد على شهادات المصادقة الرقمية وعلى التوقيع الإلكتروني، وتتطلب برمجيات معقدة. فهذا النظام لم يحقق انتشاراً واسعاً بالرغم من مستوى الأمن المتقدم الذي يضمنه.

أمن البريد الإلكتروني: اعتمد البريد الإلكتروني على البروتوكول البسيط لنقل البريد (SMTP) الذي استُخدم لنقل الرسائل إلكترونياً، وجرى تعديله لدعم امتدادات بريد الإنترنت الآمنة والمتعددة الأهداف

---

(79) SHA h*ash functions*. Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/SHA1.

(80) MD h*ash Algorithm. Version* 1.0, http://www.w3.org/TR/1998/REC-DSig-label/MD5-1_0.

(81) www.itu.int/ITUD/cyb/publications/2007/cgdc-2007-e.pdf، مرجع سبق ذكره.

(82) http://searchfinancialsecurity.techtarget.com/sDefinition/0,,sid185_gci214194,00.html.

(S/MIME). ولا تتضمن جميع هذه البرتوكولات الخدمات الأمنية للبريد الإلكتروني، وهي سهلة الاختراق. وقد اعتمد المجلس المعني بالأنشطة عبر شبكة الإنترنت ضمن معايير البروتوكولات الرسمية برتوكول البريد المعزز الخصوصية[83] (Privacy-Enhanced Mail (PEM)) لتوفير بريد إلكتروني آمن عبر الإنترنت يحقق خصائص التشفير والاستيقان وتكامل البيانات، إضافة إلى إدارة المفاتيح. كما يتوفر البروتوكول غير المعياري حول الخصوصية الحسنة[84] (Pretty Good Privacy (PGP)) الذي يحقق خصائص أمن البريد الإلكتروني من نواحي التشفير والاستيقان وتكامل البيانات، إلا أنه يعتمد الطريقة الموزعة في إدارة المفاتيح ولا يعتمد مركز مصادقة؛

الإطار 4- سرقة أرقام بطاقات الائتمان

يشكل تعرض الأدوات والنظم المستخدمة في إجراء المداولات الإلكترونية للسرقة أو التخريب خطراً كبيراً على مصالح المستخدمين ومستقبل الخدمات الإلكترونية. وقد انتشرت مؤخراً حوادث سرقات أرقام بطاقات الائتمان، إما مباشرة من أصحابها عن طريق دفعهم إلى إجراء تعاملات من خلال مراسلات بريد إلكتروني خادع أو عبر صفحات ومواقع إنترنت وهمية (التصيد)، أو عن طريق اختراق قواعد بيانات العملاء الخاصة بالمصارف وبمؤسسات المداولات الإلكترونية مثل VISA, MasterCard, American Express. ونذكر على سبيل المثال الحادثة التي تعرض لها مركز معالجة بيانات مداولات إلكترونية في الولايات المتحدة الأمريكية في عام 2005، ونتج عنها تسرب بيانات أكثر من 40 مليون بطاقة ائتمان[أ]. كما يمكن أن تتم السرقة باختراق قواعد بيانات عملاء المتاجر الكبيرة، وهنا نذكر مثلاً القضية الشهيرة[ب] التي حدثت في عام 2007 والتي تناولتها المحاكم الأمريكية[ج] وانتهت في آب/أغسطس 2008 بإدانة عصابة دولية مكونة من ثلاثة أفراد من الولايات المتحدة الأمريكية، وثلاثة أفراد من أستونيا، وثلاثة آخرين من أوكرانيا، وفردين من الصين، وفرد من بيلاروس. فقد قامت تلك العصابة بسرقة أرقام أكثر من 45 مليون بطاقة ائتمان (في حين قدر بعض الخبراء أن هذا العدد قد يتجاوز 94 مليون بطاقة ائتمان)[د]، علاوة على بيانات الهوية الشخصية لعملاء تسعة من أكبر متاجر التجزئة الأمريكية (TJX) ومنها Marshall's وT.J. Maxx وBJ's Wholesale Club وOfficeMax وBarnes وNoble Sports Authority. وقد استخدمت الأرقام المسروقة، قبل أن يتم اكتشاف السرقات[•]، في 13 بلداً لإجراء العديد من المداولات الإلكترونية، كان بينها إصدار بطاقات هدايا بقيمة 8 ملايين دولار أمريكي. وقدرت الخسائر المبدئية لسرقة البطاقات التابعة لمؤسستي VISA وMaster Card في هذه القضية بمئات الملايين من الدولارات، وهذا ما جعل تلك القضية أكبر قضية من نوعها في العالم.

(أ) http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061701031.html.

(ب) http://www.boston.com/business/ticker/2007/03/tjx_breach_invo.html.

(ج) http://edition.cnn.com/2008/CRIME/08/05/card.fraud.charges/index.html.

(د) http://www.channelregister.co.uk/2007/10/24/tjx_breach_estimate_grows/.

(•) http://www.eweek.com/c/a/Database/Stolen-TJX-Data-Used-in-8M-Scheme-Before-Breach-Discovery/.

(83) Network Working Group. *Privacy Enhancement for Internet Electronic Mail. Part IV: Key Certification and Related Services.* www.ietf.org/rfc/rfc1424.txt.

(84) http://en.wikipedia.org/wiki/Pretty_Good_Privacy.

أمن خدمات الحكومة الإلكترونية: الحكومة الإلكترونية هي البيئة التي تعتمد على شبكات المعلومات والاتصال عن بعد لتقديم الخدمات إلى المواطنين والرد على استعلاماتهم، والاضطلاع بأنشطة الدوائر الحكومية. وتقدم الحكومة الإلكترونية خدمات داخل الدوائر التابعة لها، وهذا ما يسمى بالخدمات من الحكومة إلى الحكومة، وخدمات إلى المواطنين، وهذا ما يسمى بالخدمات من الحكومة إلى المواطن، وأخرى إلى قطاعات الأعمال التجارية، وهذا ما يسمى بالخدمات من الحكومة إلى قطاعات الأعمال التجارية، وخدمات إلى الموظفين، وهذا ما يسمى بالخدمات من الحكومة إلى الموظف. ونظراً إلى أهمية خدمات الحكومة الإلكترونية، يعتبر موضوع أمنها من البنود الأساسية في بنية هذه الخدمات. وتعتمد هذه الخدمات في ضمان أمنها على إنشاء مركز وطني لإصدار الشهادات يشمل سلطة المصادقة، وسلطة التسجيل، ودليل شهادات المصادقة الصالحة والملغاة، ونظام حفظ شهادات المصادقة والمستخدمين النهائيين، ووضع سياسة تحدد العلاقات بين مختلف المكونات. وتدعم هذه البنية استحداث زوج فريد من المفاتيح، وحفظ المفاتيح وإجراءات الاسترجاع، وإدارة الشهادات الرقمية وتجديدها وإصدارها وإلغاءها، وتزويد الجهات المخولة بالمفاتيح العمومية والمصادقة عليها، وتوقيع الشهادات الرقمية. وتستخدم هذه الشهادات في مرحلة التعرف خلال عملية النفاذ إلى الخدمات، وفي ضمان أمن التعامل بين مختلف القطاعات حيث تقوم سلطة المصادقة بإصدار رقم تشفير، وشهادة مصادقة بعد التوثق من طلب العميل. كما أنها تسمح بالتوثق من صحة البيانات، وبتحقيق ميزة عدم الإنكار، واستخدام بعض أنواع التشفير المعتمد في تبادل المعلومات الخاصة أو السرية.

ويبين الشكل 8 بعض البرمجيات والآليات الأكثر شيوعاً في مجال حماية نظم المعلومات وأمنها، وتأثيرها على احتياجات الأمن الإلكتروني الأكثر أهمية بالنسبة إلى الأفراد والمؤسسات والشركات.

الشكل 8- برمجيات وآليات لضمان الأمن الإلكتروني(85)

التكنولوجيات المعتمدة لضمان الأمن الإلكتروني				
احتياجات الأمن / برمجيات وآليات	تكامل البيانات وسلامتها	السرية	التعرف والاستيقان	عدم الإنكار
مضادات الفيروسات	√			
الجدران النارية		√	√	
ضبط النفاذ		√	√	
التشفير		√		
البنية الأساسية للمفاتيح العمومية	√	√	√	√

دال- المعايير الدولية في إدارة نظم أمن المعلومات

تبين هذه الفقرة الاهتمام الدولي والجهود المبذولة لإيجاد معايير موحدة يمكن الارتكاز عليها في عملية إدارة نظم أمن المعلومات. فقد صدر عن معهد المعايير البريطانية، في عام 1995، المعيار

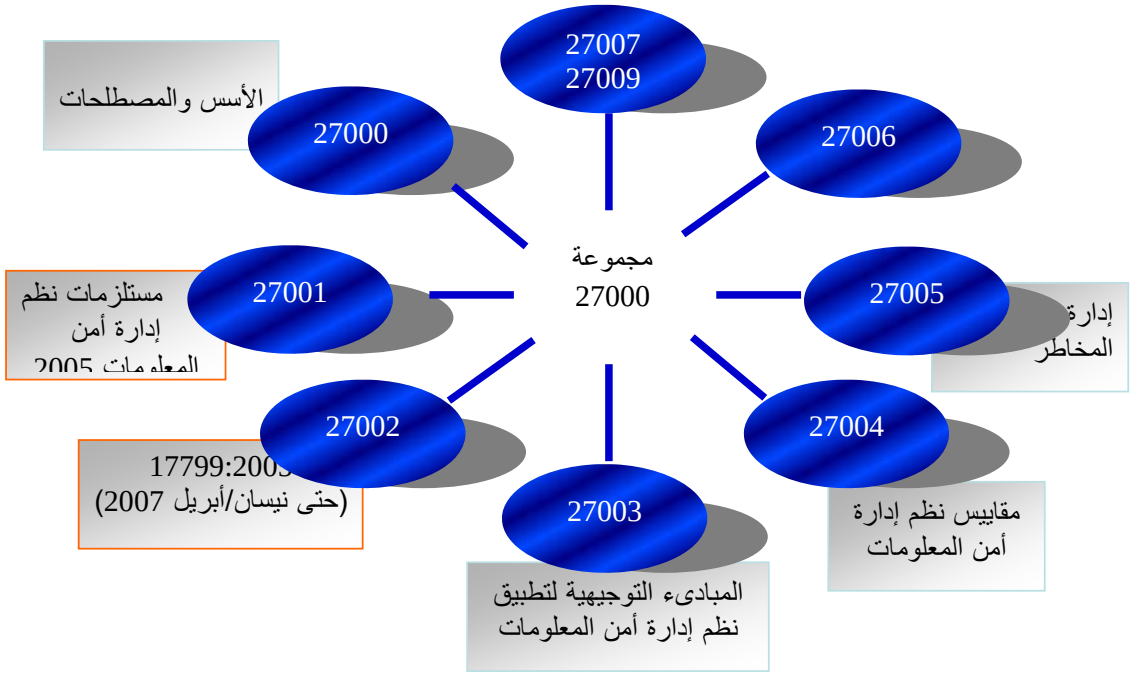
(85) http://www.itu.int/ITU-D/treg/Events/Seminars/2006/subregional_clmv/docs/2-5-1-ntoko.pdf, p.44.

BS 799[86] الذي يتضمن قسمين أساسيين[87]. ويتعلق القسم الأول بقانون الممارسة، والثاني بتوصيف نظام إدارة أمن المعلومات، وهو الذي يؤهل المؤسسة الحصول على الاعتماد. وفي عام 2000، اعتمدت المنظمة الدولية لتوحيد المقاييس الجزء الأول تحت تسمية ISO/IEC 17799، واعتمدت في عام 2005 الجزء الثاني تحت تسمية ISO27001. ويقترح المعيار ISO/IEC 17799، الذي يمكن اعتماده كمرجع عند إعداد السياسة المتعلقة بضمان الأمن، قواعد لممارسة إدارة الأمن، ومربع تحكّم لتحليل المخاطر والتدقيق في مسألة ضمان الأمن. وتكمن أهمية هذا المعيار في تطرقه إلى الجوانب التنظيمية والبشرية والقانونية والتقنية. أما المعيار ISO27001 فيركز على تقييم المخاطر وتحليلها، وإدارة الأصول والموارد، وإدارة الحوادث الطارئة.

ومما لا شك فيه أن تطبيق هذه المعايير يفيد في توعية العاملين في المؤسسات، ورفع مستوى إدارة الأمن فيها، وهذا الأمر يعزز الثقة بخدماتها في الأسواق التجارية وبين المتعاملين.

وقامت المنظمة الدولية لتوحيد المقاييس خلال السنوات الأخيرة بوضع مخطط لسلسلة من المعايير المتعلقة بأمن المعلومات وإدارة المخاطر، وأنشأت مجموعة متكاملة من معايير أمن المعلومات عرفت بمجموعة المعايير المعنية بنظم إدارة أمن المعلومات أو ISO27k، وهي مبينة في الشكل 9.

الشكل 9- مجموعة معايير ISO27K



(86) http://en.wikipedia.org/wiki/BS7799.

(87) Technical report. *The Information Security Breaches Survey 2006*. (ISBS 2006), www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf.

أنجز عدد من هذه المعايير والعمل جارٍ على إنجاز المعايير المتبقية[88]:

المعيار ISO/IEC 27000: وهو يتضمن شرحاً تعريفياً بهذه السلسلة من المعايير، ويبين هدف كل منها وارتباطه بالأجزاء الأخرى من السلسلة. كما يتضمن تعريفاً للعديد من المصطلحات العلمية المتعلقة بأمن المعلومات وحمايتها؛

المعيار ISO/IEC 27001: وهو يتضمن طرق تطبيق نظام إدارة أمن المعلومات والتحكم بها؛

المعيار ISO/IEC 27002: وهو يتضمن قواعد التطبيق وإرشادات حول استخدام الممارسات الفضلى في مجال إدارة نظم أمن المعلومات. وقد عَرِف هذا المعيار بتسميتين في السابق، أولاً BS7799 Part1 ثم تلتها ISO 17799. وقد تم تحديثه في عام 2005، ثم تعديل رمزه في تموز/يوليو 2007 بحيث أصبح يعرف بالمعيار ISO/IEC27002:2005؛

المعيار ISO/IEC 27003: وهو يعتبر دليلاً مرشداً لتطبيق نظام أمن المعلومات في المؤسسة، حيث يشرح البنود الواجب تطبيقها ضمن خطوات عملية؛

المعيار ISO/IEC 27004: وهو معيار لم ينجز بشكله النهائي بعد، ويتضمن شرحاً حول كيفية قياس مستوى إدارة الأمن في النظام؛

المعيار ISO/IEC 27005: وهو يتضمن الخطوات الرئيسة الواجب اتخاذها لضمان أمن النظم بطريقة سليمة، وبناءً على نظم إدارة المخاطر. وقد صدرت النسخة الأولى من هذا المعيار في عام 2008؛

المعيار ISO/IEC 27006: يتضمن هذا المعيار الذي صدر في عام 2007 دليلاً مرشداً حول الإجراءات المعتمدة في إصدار الشهادات، وعمليات التسجيل الإلكتروني، وحول تجنب المخاطر في إصدار الشهادات.

المعيار ISO/IEC 27007: وهو يتضمن دليلاً مرشداً حول الخطوات المتخذة في مراقبة نظم إدارة أمن المعلومات والتدقيق فيها، ويركز على النواحي الإدارية في عمليات المراقبة والتدقيق، إلا أنه لم يصدر بشكله النهائي بعد.

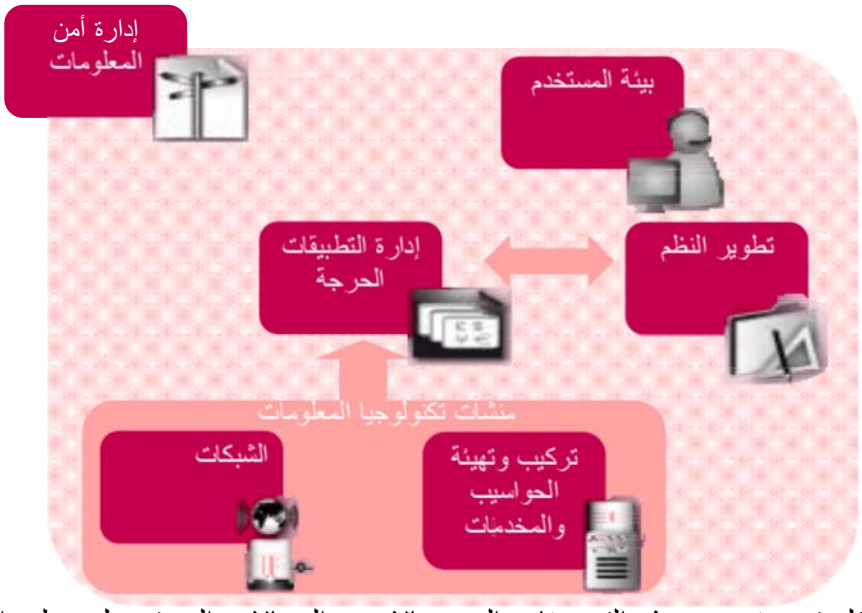
إضافة إلى المعايير الصادرة عن المنظمة الدولية لتوحيد المقاييس، صدر عن منتدى أمن المعلومات[89] في عام 1996 معيار الممارسات السليمة ((Standard of Good Practice (SoGP). ويضم هذا المعيار، الذي يتم تحديثه كل عامين، مجموعة من الوثائق التفصيلية للإجراءات الفضلى، والممارسات الواجب اتباعها من أجل حماية المعلومات والنظم الحاسوبية على المستويين المؤسسي والفردي. ويعتمد هذا المعيار على تقسيم إجراءات أمن المعلومات إلى ستة تصنيفات رئيسة هي: (أ) إدارة أمن المعلومات على المستوى المؤسسي؛ (ب) إدارة التطبيقات الحرجة؛ (ج) تهيئة وتركيب الحواسيب والمخدمات التي تتضمن

(88) http://www.iso27001security.com/html/iso27000.html.

(89) Information Security Forum. Protecting Business Information. *The Standard of Good Practice for Information Security*. http://www.isfsecuritystandard.com.

أكثر من تطبيق؛ (د) الشبكات الحاسوبية؛ (•) تطوير النظم؛ (و) بيئة المستخدم. ويبين الشكل 9 التصنيفات الستة الرئيسة التي يعتمد عليها معيار الممارسات السليمة.

الشكل 10- التصنيفات الأساسية في معيار الممارسات السليمة(90)



ويقسم كل تصنيف من هذه التصنيفات إلى مجالات، والمجالات إلى فصول، على النحو المبين في الشكل 11. وتتضمن وثائق الفصول تفاصيل عن الممارسات والإجراءات الفضلى الواجب القيام بها بخصوص كل موضوع من مواضيع الفصل.

الشكل 11- مجالات وفصول التصنيفات الستة الخاصة بمعيار الممارسات السليمة

التصنيفات	عدد المجالات	عدد الفصول
إدارة أمن المعلومات	7	36
إدارة التطبيقات الحرجة	6	25
تركيب الحواسيب والمخدمات	6	31
الشبكات	5	25
تطوير النظم	6	23
بيئة المستخدم النهائي	6	26
المجموع	**36**	**166**

وجدير بالذكر أن وثائق معيار الممارسات السليمة متاحة مجاناً عبر الإنترنت على موقع منتدى أمن المعلومات(91).

(90) *The Six aspects of Information Security*. https://www.isfsecuritystandard.com/SOGP07/index.htm.

(91) https://www.isfsecuritystandard.com.

ويلاحظ أن المعايير الدولية المعتمدة في إدارة نظم أمن المعلومات حديثة العهد ولم تستكمل بعد. وينبغي القيام بمتابعة دورية لتحديث المعايير الدولية لمواجهة الاختراقات الجديدة، مع أخذ المستجدات في نظم المعلومات في الاعتبار وتطبيق أحدثها.

هاء- أمن المداولات الإلكترونية: بعض الممارسات ودراسات حالة

1- تجربة الإمارات العربية المتحدة

أحرزت الإمارات العربية المتحدة تقدماً كبيراً في الانتقال إلى مجتمع المعلومات، وذلك بفضل امتلاكها بنية أساسية متقدمة في مجال الاتصالات، وتوفر إطار قانوني وقواعد ترعى المداولات الإلكترونية. والإمارات العربية المتحدة هي من بين البلدان السباقة في الشرق الأوسط إلى وضع إطار قانوني يحكم المداولات الإلكترونية. وقد اتخذت مبادرات عديدة للانتقال من العمل الورقي إلى العمل اللاورقي، واستحدثت عدداً من النظم لأتمتة إجراءات العمل بهدف التخفيف من العمل اليدوي والورقي. وتحتل الإمارات العربية المتحدة حالياً المرتبة 21 من بين 190 دولة من حيث أداء الحكومة الإلكترونية. ومن أهم المبادرات التي قامت بها في السنوات الأخيرة خدمة الرخصة الإلكترونية لمعالجة الوثائق e-permit، وإدارة تدفق الأعمال المتعلقة بترخيص البناء، وخدمة الموقع الإلكتروني، وهو نظام معلومات جغرافية GIS خاص بمفتشي مواقع البناء، وخدمة العرض الإلكتروني e-bid التي تسمح بالتفاوض مع مقدمي العروض للحصول على عقود لتنفيذ المشاريع الضخمة. وتجدر الإشارة إلى أن تطبيقات الحكومة الإلكترونية بدأت تنتشر منذ عام 1997، وكانت وزارة المالية رائدة في وضع معلومات عنها على المواقع، وتم لاحقاً العمل على دمجها ضمن بوابة واحدة.

وفي مجال التطبيقات المالية، وضعت خدمة الدرهم الإلكتروني، وهي أداة لتسديد الفواتير إلكترونياً وضعتها الحكومة لتسهيل جمع الإيرادات، وتزويد الحكومة والجهات الحكومية بأداة مريحة وآمنة لتسديد الفواتير. وقد صممت هذه الخدمة أساساً بغرض جمع إيرادات الحكومة الاتحادية، ولكنها أصبحت تُستخدم لاحقاً لخدمة الحكومات المحلية، والمنظمات شبه الحكومية، وبعض الشركات الخاصة. لقد بدأ استخدام هذه الخدمة في 3 شباط/فبراير 2001، وكانت الإمارات العربية المتحدة البلد الرائد في المنطقة العربية في استخدام مثل هذه الأدوات. ومن ثم ازداد انتشار أداة الدرهم الإلكتروني وأصبح لها العديد من القنوات المخصصة للدفع، مثل مطاريف نقاط البيع الإلكترونية e-POS، وبوابة الدفع عبر الإنترنت، والطابع الإلكتروني. وتتوفر اليوم خدمة العملاء بالصوت التفاعلي IVR، وهي خدمة مجانية تخول المواطن الاطلاع على رصيده، أو إلغاء بطاقة مفقودة، أو تغيير رقم التعريف الشخصي PIN، أو شحن البطاقات بخدمة ذاتية (مثل الصراف الإلكتروني e-Saraf) عبر الآلات المصرفية. وأصبحت جميع هذه الخدمات متوفرة عبر شبكة الإنترنت على الموقع التالي: www.e-dirham.gov.ae. ويمكن اعتبار البطاقات المستعملة في هذه الخدمة محفظة إلكترونية آمنة e-purse، وهي متوفرة بشكلين أساسيين:

- بطاقة ثابتة القيمة يمكن شراؤها من أي مصرف مشترك في خدمة الدرهم الإلكتروني، ولا يمكن إعادة شحنها، وإنما يستطيع المستخدم استعمال عدة بطاقات لتسديد مبلغ محدد؛

- بطاقة العميل الحكومي (Government Customer Card (GCC))، وهي بطاقة أطلقتها الحكومة في حزيران/يونيو 2001 لمستخدمي الخدمات الحكومية. وتتميز هذه البطاقة بكونها مخصصة

لشخص معين لا يمكن لغيره استخدامها، حيث يجري إصدارها مع رقم تعريف شخصي يُرسل إلى المستخدم داخل ظرف آمن. ويمكن تعبئة هذه البطاقة من أي مصرف مشترك في الخدمة.

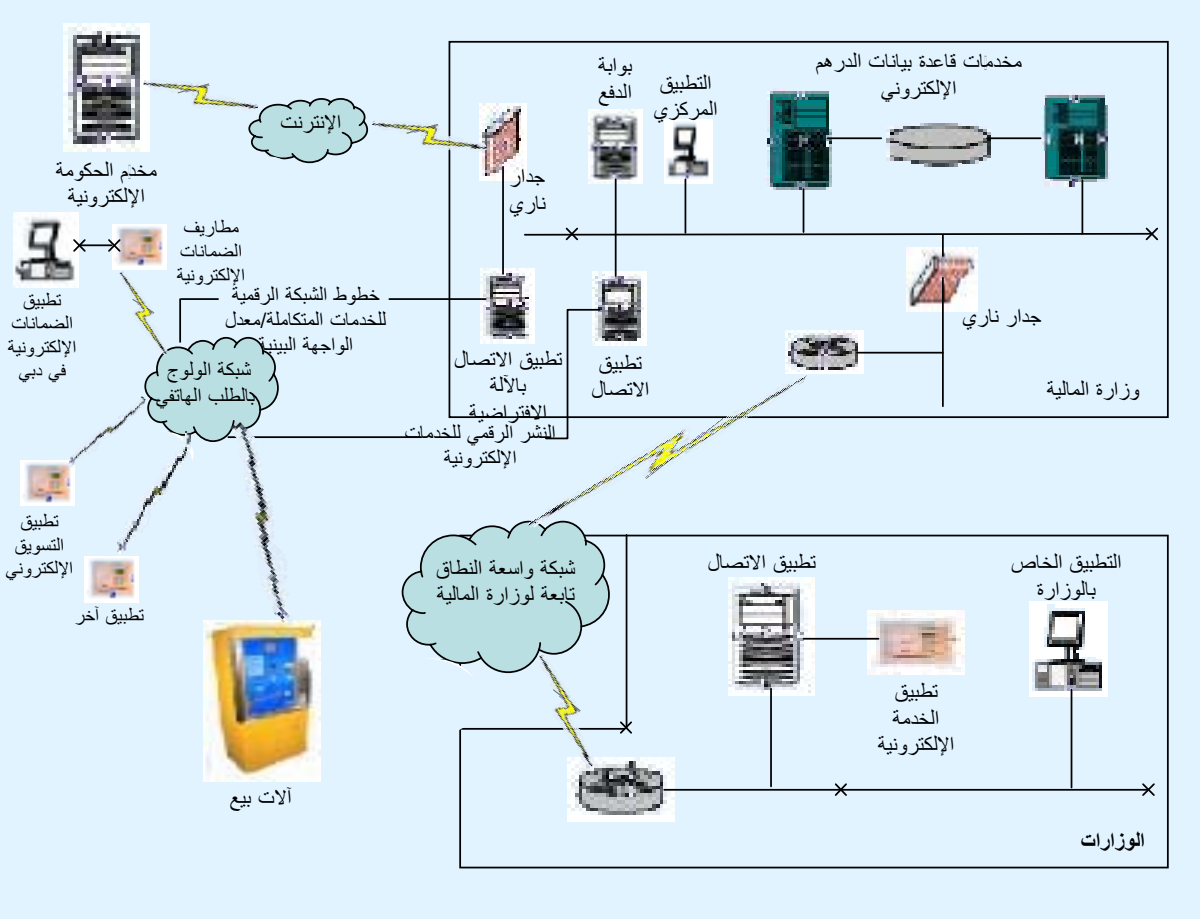
تسمح خدمة الدرهم الإلكتروني بتيسير عملية التحصيل من المواطن لأنها متاحة على مدار الساعة وطوال أيام الأسبوع. وقد حققت هذه الخدمة منافع للحكومة التي استطاعت تحويل الموظفين الذين كانوا مخصصين للتحصيل إلى وظائف أخرى. ويبين الشكل 12 المخطط العام لبنية خدمة الدرهم الإلكتروني.

وانطلاقاً من خدمة الدرهم الإلكتروني، جرت عملية التحول من التحصيل التقليدي إلى التحصيل الإلكتروني، وذلك بالاعتماد على مبدأ المشاركة والشراكة مع مزودي الخدمة والمصارف. كما أطلقت حملات توعية للعملاء، وجرى تسويق الخدمة في المجتمع على اختلاف شرائحه. وتشير التقديرات إلى أن متوسط عدد العمليات الجارية عبر هذه الخدمة هو 000 35 عملية يومياً. وأما الإيرادات المحصلة بهذا الأسلوب فتُقدر بنسبة 85 في المائة من الإيرادات الحكومية الإجمالية.

ولتحقيق مزيد من الأمن في المداولات الإلكترونية، أنشأت هيئة تنظيم الاتصالات في الإمارات العربية المتحدة مركز الاستجابة لطوارئ الحاسب الآلي. ويهدف هذا المركز الوطني إلى مكافحة الجرائم الحاسوبية، والتنبيه إلى حوادث الأمن الإلكترونية على شبكة الإنترنت واكتشافها، والعمل على منعها. كما يعمل على بناء القدرات الوطنية، ونشر التوعية والمعلومات حول التهديدات والثغرات الأمنية. وبالرغم من هذه المحاولات الهادفة إلى تعزيز أمن استعمال الخدمات الإلكترونية، لم ينتشر مفهوم خصوصية المعلومات على المستوى الوطني، وما زال بإمكان هيئة تنظيم الاتصالات وضع الأطر والإجراءات المتعلقة باستخدام معلومات المستهلك. ويضاف إلى ذلك أن معظم الشركات لا تعتمد في إدارة أمن معلوماتها المعيار ISO 27001 الذي يعتبر شرطاً أساسياً لانتشار المؤسسات وتوسع أعمالها على المستويين العالمي والإقليمي. وهو يتضمن جميع الإجراءات والطرق التي تتبعها المؤسسات لتطبيق نظام إدارة أمن معلوماتها والتحكم بها، كما يعرض هذه الإجراءات على العالم الخارجي. أما المشاكل الرئيسة التي ما زالت هذه الشركات تواجهها فتتمثل في الفيروسات، والبريد الدعائي، والأخطار الداخلية.

الشكل 12- بنية خدمة الدرهم الإلكتروني[92]

(92) K. Al-Bustani. *How ICT change the way governments deliver services: e-dirham, Case Study: e-dirham.* Abu-Dhabi Summit. March 2006.



2- تجربة تونس

صدر في تونس مؤخراً عدد من القوانين والمراسيم التي تحدد التنظيم على المستويين الإداري والمالي، والأدوار المضطلع بها في الوكالة الوطنية لأمن المعلوماتية، والوكالة الوطنية للمصادقة الإلكترونية، إضافة إلى واجبات سلطات التسجيل، ومزودي خدمة المصادقة[93]. وتتناول هذه القوانين والمراسيم موضوع حماية الخصوصية، وشروط استخدام أدوات التشفير وتحديد التعاريف الخاصة بالوثائق الرقمية، وشهادات المصادقة الرقمية، والتوقيع الإلكتروني. وقد أنشئت الوكالة الوطنية للمصادقة الإلكترونية بموجب القانون 2000-83 المؤرخ 9 آب/أغسطس 2000 والمتعلق بتنظيم المداولات الإلكترونية، والتجارة الإلكترونية[94]. وقد كلفت الوكالة بمنح شهادات المصادقة الرقمية أو تجديدها أو إلغائها، والترخيص لمزودي خدمة المصادقة، والتوثق من صحة شهادات المصادقة الأجنبية، وتقييم أجهزة التشفير. وقد وضعت البنية الأساسية للمفاتيح العمومية التي تضم سلطة مصادقة مركزية يتبعها عدد من السلطات الفرعية الموزعة

(93) N. Boudriga. *Digital Certification Practice and Achievements in Tunisia*. May 2003. www.iit.cnr.it/Tiwis 2003/documenti/day1/pres-N.Boudrigua.pdf.

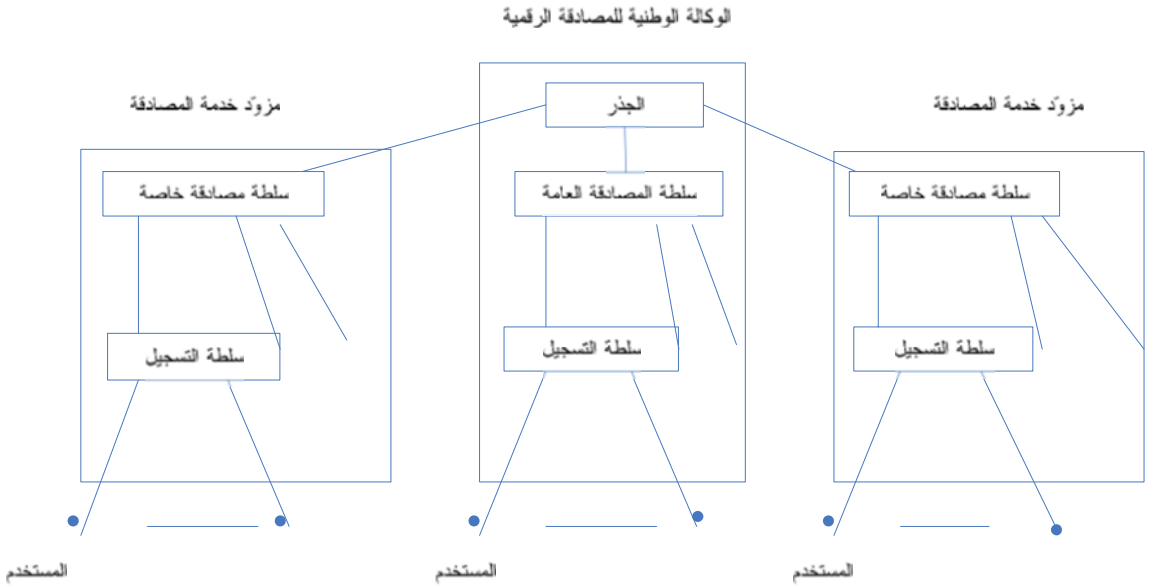
(94) National Digital Certification Agency. Agence Nationale de Certification Electronique. http://www. certification.tn.

جغرافياً. وتؤدي الوكالة الوطنية للمصادقة الإلكترونية دور السلطة الجذر، وهي تتمتع بأعلى درجات الموثوقية في مجال المصادقة الرقمية، وأمن المداولات الإلكترونية في تونس. وتُناط بها الخدمات التالية:

- ضمان أمن المداولات الإلكترونية في مجالي التجارة الإلكترونية والحكومة الإلكترونية؛
- إدارة الشهادات الرقمية؛
- منح مزودي خدمة المصادقة الترخيص اللازم؛
- وضع الحلول المتعلقة بالتوقيع الإلكتروني وبضمان أمنه؛
- التأهيل في مجال التوقيع الإلكتروني.

وتعمل الوكالة الوطنية للمصادقة الإلكترونية في تونس على تزويد الجهات الحكومية والعامة بشهادات المصادقة، وهي المسؤولة عن التحقق من الشهادات بالتقاطع مع الهيئات العالمية. ويشير الشكل 13 إلى هيكلية سلطات المصادقة الرقمية في تونس.

الشكل 13- البنية العامة لسلطات المصادقة الرقمية في تونس[95]



من جهة أخرى، ودائماً في سياق ضمان أمن المداولات الإلكترونية، تنتشر في تونس عملية التعامل بالنقود الافتراضية، والمقصود بها الدينار الإلكتروني تحديداً[96]. وهي تعتمد على طبقة المقبس الآمن، وعلى شهادات المصادقة الصادرة عن المكتب المختص. وتتضمن عملية تسديد الفاتورة مرحلة التعرف على بطاقة العميل وتليها مرحلة تخويل هذا العميل تسديد الفاتورة. وقد اعتُمدت هذه الخدمة في البريد التونسي[97]، وأصبحت تُستخدم لإجراء ما يزيد على 85 في المائة من المداولات الوطنية.

(95) Public Key Infrastructure, The Tunisian Infrastructure.

(96) http://www.e-dinar.poste.tn.

(97) Kooli, Interview, e@Work newsletter, UNCTAD, WTO, September 2007.

وقد ساعد اعتماد شهادات المصادقة على انتشار عدد من التطبيقات الإلكترونية، كتسجيل الطلاب عن بعد، واستعمال خدمات الحكومة الإلكترونية، والتصريح عن الضرائب وتسديدها إلكترونياً. واستطاعت تونس بفضل اعتماد شهادات المصادقة تطوير هذه التطبيقات والخدمات بشكل آمن، وبالتالي نشر خدماتها الإلكترونية عبر شبكة الإنترنت في مجالات عدة كالتجارة الإلكترونية، وتسديد الفواتير إلكترونياً والحكومة الإلكترونية، والصحة الإلكترونية، والتعليم الإلكتروني، والصيرفة الإلكترونية، وغيرها من العمليات المتطورة. وفي إطار تعزيز أمن المداولات الإلكترونية وثقة المستخدمين بها، تعمل تونس على تنفيذ عدة مشاريع مستقبلية نذكر منها المشاريع التالية:

- تنسيق الإطار القانوني على المستوى الإقليمي؛
- بناء قدرات صانعي القرار والمستخدمين على تغطية المعايير الأمنية؛
- إنشاء مخزن لشهادات المصادقة الجذرية؛
- إنشاء مخزن لجميع شهادات المصادقة المسلمة في البلد؛
- نشر الوعي بالبنية الأساسية، وقضايا الأمن وخدماتها؛
- التركيز على التشغيل البيني من خلال الشراكة مع المنتديات الإقليمية؛
- استخدام تقنيات التشفير لحماية البيانات والوثائق عند نقلها بالبريد الإلكتروني.

وبالإضافة إلى تجربة الإمارات العربية المتحدة وتجربة تونس في مجال تعزيز أمن استخدام بعض الخدمات الإلكترونية، يشير الإطار 5 إلى عدد من الأنشطة والمبادرات التي قامت بها الدانمرك وهنغاريا في نطاق ضمان أمن تكنولوجيا المعلومات والاتصالات.

الإطار 5- بعض الممارسات في مجال أمن تكنولوجيا المعلومات والاتصالات في الدانمرك وهنغاريا[أ]

تجربة الدانمرك

أقرت الدانمرك رسمياً في عام 2005 سياسة أمنية لتكنولوجيا المعلومات والاتصالات في 90 في المائة من الهيئات الحكومية، وقد جرى تنسيقها على المستويين المحلي والإقليمي.

وواجهت الإدارات الحكومية في الدانمرك في عام 2005 عدة أخطار، منها الفيروسات، بنسبة 31 في المائة، تلتها هجمات رفض الخدمة، ثم نقص التخزين الاحتياطي، ثم النفاذ غير المخول، وأخيراً سوء استخدام تكنولوجيا المعلومات والاتصالات.

وقد اعتُمد التوقيع الإلكتروني على نطاق واسع في عام 2005. ويشكل النفاذ عبر رقم التعريف الشخصي نسبة 28 في المائة من المداولات.

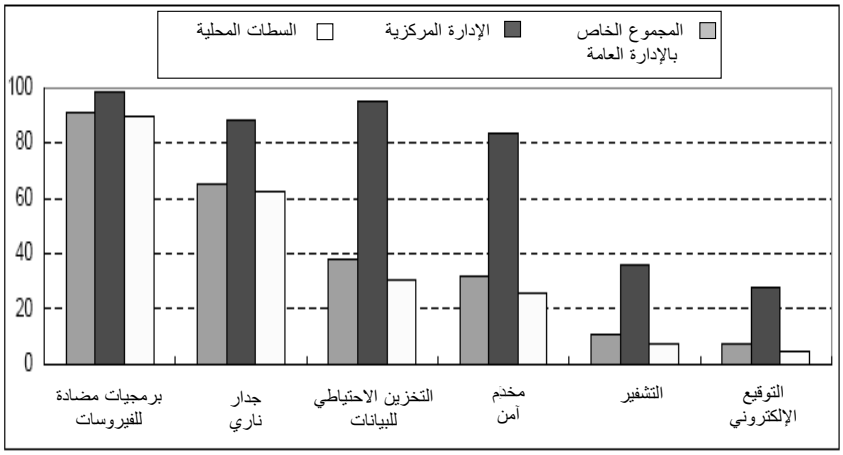
الإطار 5 (تابع)

تجربة هنغاريا

يعد استخدام البرامج المضادة للفيروسات أمراً شبه معمم في جميع الإدارات الحكومية، بخلاف الجدران النارية التي يعتبر استخدامها أقل انتشاراً. وأما التوقيع الإلكتروني، فليس على الدرجة نفسها من الانتشار كما في الدانمرك. وتنتشر تقنية التشفير بنسبة 11.6 في المائة من إجمالي الإدارات الحكومية. ويبين الشكل 14 نسبة انتشار بعض

الإجراءات المعتمدة في هنغاريا بشأن أمن التعاملات الإلكترونية.

الشكل 14- إجراءات ضمان أمن التعاملات الإدارية الحكومية في هنغاريا(ب)



(أ) Organisation for Economic Co-operation and Development (OECD). Working Party on Indicators for the Information Society. *Measuring Security and Trust in the Online environment: A view using official data*. DSTI/ICCP/IIS(2007)4/Final, January 2008, www.oecd.org/dataoecd/47/18/40009578.pdf.

(ب) Security Measures in place in the Public Administration in Hungary. 2005، مرجع سبق ذكره.

خامساً- التوعية بأهمية حماية استخدام تكنولوجيا المعلومات والاتصالات وضمان أمنها

تعتبر المعلومات عنصراً أساسياً في حياة الأفراد والمنظمات، ورأس مال لا غنى عنه بالنسبة إلى المؤسسات التجارية في عالمنا اليوم القائم على تكنولوجيا المعلومات والاتصالات. فنظم تكنولوجيا المعلومات تؤدي دوراً رئيساً في ربط الشبكات الداخلية داخل المؤسسات والمنظمات، أو عبر تأمين الاتصال مع عدد كبير من الموردين والشركاء والعملاء والأسواق. وتساهم هذه النظم، في حال كانت المعلومات المتوفرة بشأنها كاملة ودقيقة ومحدثة، في تحسين عملية اتخاذ القرارات الإدارية. وأما ضمان تقديم معلومات بهذه الجودة الرفيعة، فلا يمكن أن يتم إلا عن طريق الحد من هامش الخطأ. ومن هنا تظهر الحاجة إلى ضمان أمن نظم المعلومات عبر التصدي للأخطار التي تهدد سرية المعلومات وتوفرها وتكاملها.

ولا يكفي وضع سياسة تضمن أمن المعلومات، أو الاستثمار في عدد من المعدات أو التكنولوجيات للحد من المخاطر التي تتعرض لها الشبكة الإلكترونية، أو نظم المعلومات، وإنما يجب إدخال ثقافة أمن المعلومات في صلب السلوك اليومي للأفراد والعاملين كي تصبح جزءاً لا يتجزأ من ثقافة الشركات.

وقد حظيت التوعية بأمن تكنولوجيا المعلومات والاتصالات واستخداماتها المختلفة وحمايتها باهتمام خاص من المجتمع الدولي والمنظمات الإقليمية والدولية. ويشير هذا الفصل إلى التوجيهات الدولية في هذا المجال، كما يعرض ملخصاً عن الدليل الذي أصدرته وكالة أمان الشبكات والمعلومات الأوروبية[98] حول كيفية رفع مستوى الوعي بأمن الشبكات والنظم المعلوماتية. فهو يشكل أساساً لوضع استراتيجية، وخطة عمل لتنظيم مبادرات التوعية في مجال أمن المعلومات والنظم والشبكات وتنفيذها. كما يتضمن هذا الفصل مبادرات قامت بها بلدان عربية وأجنبية في مجال التوعية.

ألف- توجيهات دولية وإقليمية لنشر ثقافة حماية الفضاء السيبراني وتعزيز أمنه

مع بروز الأخطار التكنولوجية التي تهدد استخدام تكنولوجيا المعلومات والاتصالات وانتشار هذه الأخطار، تنبه المجتمع الدولي إلى أهمية حماية الفضاء السيبراني واستخداماته وتعزيز أمنه، وإلى ضرورة توعية جميع الشركاء وأصحاب المصلحة في مجتمع المعلومات حول هذه الأخطار، ونشر ثقافة حماية تكنولوجيا المعلومات والاتصالات. وفي هذا السياق، أصدرت الجمعية العامة للأمم المتحدة في دورتها السابعة والخمسين في عام 2002 القرار 239/57 المتعلق بإنشاء ثقافة أمنية عالمية للفضاء الحاسوبي[99]. فقد أدركت الجمعية العامة أن ضمان الأمن السيبراني ليس مجرد مسألة حكومية، وأن هذا الأمن لا يتحقق عبر ممارسات أو قوانين وتشريعات خاصة في هذا المجال وحسب، وإنما من خلال دعم الوقاية في المجتمع بأسره.

(98) http://aitnews.com/news/9772.html، مرجع سبق ذكره.

(99) www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf، مرجع سبق ذكره.

ولا تستطيع التكنولوجيا وحدها أن تكفل أمن الفضاء السيبراني، إنما يفترض بالمجتمع الدولي أن يضع التخطيط لإدارة هذه العملية في صلب أولوياته. وعلى كافة الجهات المعنية والمشتركين[100] في بناء مجتمع المعلومات والاتصالات، من حكومات ومؤسسات أعمال ومنظمات وأفراد ومستخدمين لتكنولوجيا المعلومات، أن يدركوا حجم المخاطر التي تهدد أمن معلوماتهم بشكل خاص، وأمن الفضاء السيبراني الذي يعملون في أرجائه ويتعاملون من خلاله بشكل عام. كما عليهم أن يتحملوا مسؤولياتهم في هذا المجال، جاهدين لاتخاذ التدابير الوقائية والتخطيط للإجراءات اللازمة بغية تعزيز أمن هذه المعلومات والتكنولوجيات. وقد ركز قرار الأمم المتحدة على أهمية التعاون الدولي من أجل تحقيق ضمان أمن الفضاء السيبراني من خلال دعم الجهود الوطنية الرامية إلى تعزيز القدرات البشرية، وزيادة فرص العمل والتعلم، وتحسين الخدمات العامة، وبالتالي تحسين نوعية الحياة عن طريق الاستفادة من استخدام تكنولوجيا المعلومات والاتصالات المتقدمة والآمنة واستعمال الشبكات الإلكترونية، وتعزيز حصول جميع فئات المجتمع عليها بالشكل الموثوق.

وبهدف خلق ثقافة عالمية حول أمن الفضاء السيبراني، ركزت الجمعية العامة للأمم المتحدة في قرارها المذكور على تسعة عناصر متكاملة. وينبغي أن يلتزم بهذه العناصر جميع المشتركين في مجتمع المعلومات والاتصالات وأن يطبقوها، كل حسب مجالات عمله ومسؤولياته. وقد أُرفق بالقرار ملحق تضمن ملخصاً عن تعاريف هذه العناصر التسعة الأساسية.

وبالتوازي مع أعمال منظمة الأمم المتحدة، قامت منظمة التعاون والتنمية في الميدان الاقتصادي[101] بالتأكيد على هذه العناصر من أجل بناء ثقافة أمن استخدام نظم المعلومات والشبكات، وأصدرتها على شكل مبادئ توجيهية تهدف إلى ما يلي:

- تعزيز ثقافة الأمن لدى جميع المشتركين في مجتمع المعلومات والاتصالات كوسيلة لحماية نظم وشبكات المعلومات؛

- رفع مستوى الوعي بمخاطر نظم المعلومات والشبكات، وبالسياسات والممارسات والتدابير والإجراءات المتاحة لمواجهة تلك المخاطر، وبضرورة الاعتماد على هذه السياسات والممارسات وتطبيقها؛

- وضع إطار مرجعي عام يساعد المشتركين على فهم قضايا الأمن، واحترام القيم الأخلاقية لدى وضع السياسات والممارسات والإجراءات الهادفة إلى ضمان أمن نظم المعلومات والشبكات، ولدى تطبيق هذه السياسات والإجراءات؛

- تشجيع التعاون وتبادل المعلومات، حسب الاقتضاء، بين جميع المشتركين لدى وضعهم السياسات والممارسات والإجراءات المتعلقة بأمن المعلومات والشبكات القائمة على تكنولوجيا المعلومات والاتصالات وسلامتها، ولدى تطبيقهم إياها.

---

(100) يقصد بكلمة مشتركين "الحكومات والأعمال التجارية والمنظمات الأخرى وفرادى المستخدمين الذين يطورون ويمتلكون ويديرون ويخدمون ويستخدمون نظم وشبكات المعلومات"، قرار الأمم المتحدة 239/57 المؤرخ 31 كانون الثاني/يناير 2003.

(101) Organisation for Economic Co-operation and Development. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. 2002.

وتتوجه هذه المبادئ التوجيهية إلى جميع العاملين في نظم المعلومات والشبكات والمشتركين في الخدمات الإلكترونية على جميع المستويات، بدءاً بواضعي السياسات والعمليات، ووصولاً إلى المستخدمين النهائيين للموارد والخدمات. وتحدد هذه المبادئ المسؤوليات التي يضطلع بها كافة المشتركين في مجتمع المعلومات والاتصالات. وتوصي المبادئ التسعة المقترحة ببذل الجهود اللازمة لضمان قيم الديمقراطية في المجتمع، وخصوصاً حرية تدفق المعلومات ونشرها، وأسس الخصوصية الشخصية. وتتوزع هذه المبادئ إلى ثلاث مجموعات: (أ) مجموعة المبادئ الأساسية التي تشمل التوعية، والمسؤولية والاستجابة؛ (ب) مجموعة المبادئ الاجتماعية التي تشمل الأخلاقيات والديمقراطية؛ (ج) مجموعة مبادئ دورة الأمن التي تضم تقييم المخاطر، وتصميم الخطط المتعلقة بالأمن وتنفيذها، وإدارة الأمن، وإعادة تقييم الخطط. وهذه المجموعات مفصلة على الشكل التالي:

1- مجموعة المبادئ الأساسية، وهي تشمل:

(أ) **التوعية**: فعلى المشتركين أن يدركوا مدى الحاجة إلى ضمان أمن نظم المعلومات والشبكات، وأن يعملوا جادين لتعزيز هذا الأمن. فتعزيز الوعي بالمخاطر وبالضمانات المتاحة يعتبر خط الدفاع الأول في عملية حماية أمن نظم المعلومات والشبكات التي تتأثر بالتهديدات الخارجية والداخلية على حد سواء. ولذلك، يوصي هذا المبدأ بأهمية توعية المشتركين بالنظم التي يعملون عليها، وتعريفهم بهيكلياتها، وتدريبهم على الممارسات الفضلى المتاحة؛

(ب) **المسؤولية**: ويعتبر هذا المبدأ جميع المشتركين مسؤولين عن أمن نظم المعلومات والشبكات. فينبغي على كل شخص يعمل من خلال شبكة داخلية أو مرتبط بشبكات اتصالات عالمية أن يدرك مسؤوليته تجاه حماية أمن هذه النظم وشبكات المعلومات، وأن يحاسب وفقاً لهذا المبدأ. ويتطلب ذلك من العاملين في بيئة معينة أن يعيدوا النظر بشكل دوري ومنتظم في ممارساتهم وتدابيرهم وإجراءاتهم، وأن يقيموها لمعرفة مدى تلاؤمها مع بيئتهم. فيتعين مثلاً على مصممي المنتجات والخدمات التي تعتمد على تكنولوجيا المعلومات والاتصالات وموردیها أن يفصلوا نظم الحماية والأمن وفقاً لمنتجاتهم، بما في ذلك آخر التطورات والتحديثات، كي يتسنى للمستخدمين فهمَ وظيفة الأمن الخاصة بمنتجاتهم وخدماتهم بشكل أفضل، وتحمل مسؤولياتهم المرتبطة بها؛

(ج) **الاستجابة**: ويشدد هذا المبدأ على وجوب التعاون بين جميع المشتركين في الوقت المناسب من أجل منع حوادث الأمن أو كشفها أو الرد عليها، نظراً إلى سرعة انتشارها وخطورتها على النظم والمعلومات المحلية، وعلى سائر النظم والشبكات المترابطة. ومن هنا تظهر الحاجة إلى تبادل المعلومات والمعارف حول مكامن الأخطار والضعف في النظم، واتخاذ الإجراءات اللازمة بحيث يكون التعاون بين المشتركين سريعاً وفعالاً وقادراً على منع أي حادث قد يخرق أمن النظم والمعلومات، أو كشفه أو معالجته. وفي بعض الأحيان، يمكن أن تتعاون جهات متباعدة جغرافياً وعبر الحدود في تنسيق هذه التدابير، وتبادل المعلومات.

2- مجموعة المبادىء الاجتماعية، وهي تشمل:

(أ) **الأخلاقيات**: ويشدد هذا المبدأ على ضرورة احترام المشتركين مصالح الآخرين. فأمام انتشار الشبكات ونظم المعلومات وكثرة المشتركين فيها، ينبغي على كل مستخدم أن يتنبه إلى تصرفاته من خلال

هذه الشبكات بحيث لا يضر بمصلحة سائر المشتركين. وقد أصبح السلوك الأخلاقي أمراً محتماً على هذه الشبكات. فعلى المشتركين أن يعملوا بجهد من أجل وضع الممارسات الفضلى واعتمادها، وتعزيز السلوكيات الأخلاقية التي تضمن الأمن وتحترم مصالح الآخرين المشروعة؛

(ب) **الديمقراطية**: ينبغي أن تتوافق عملية ضمان أمن نظم المعلومات والشبكات مع القيم الأساسية التي يستند إليها المجتمع الديمقراطي، وأن تراعي القيم المعترف بها في المجتمعات الديمقراطية، بما في ذلك حرية تبادل الأفكار والآراء، والتدفق الحر للمعلومات، وضمان سرية المعلومات والاتصالات، وحماية الخصوصية والبيانات الشخصية والشفافية في التعاملات والاتصالات.

3- مجموعة مبادئ دورة الأمن، وهي تشمل:

(أ) **تقييم المخاطر**: على المشتركين أن يجروا عمليات تقييم للمخاطر بغية تحديد التهديدات ومواطن الضعف الرئيسة في النظم المستخدمة، والعوامل الداخلية والخارجية المؤثرة مثل التكنولوجيا والعوامل المادية والبشرية والسياسات والخدمات. وتسمح عملية تقييم هذه المخاطر بتحديد مستوى المجازفة المقبول، واختيار الضوابط المناسبة لإدارة الأخطار التي تهدد ضمان مستوى الأمن المطلوب في نظم وشبكات المعلومات؛

(ب) **تصميم الخطط المتعلقة بضمان الأمن وتنفيذها**: على المشتركين أن يدرجوا الأمن كعنصر أساسي في النظم والشبكات المخصصة لإدارة البيانات. وعلى القيمين على تصميم هذه النظم وتنفيذها أن يركزوا على تصميم واعتماد الضمانات المناسبة، والحلول الملائمة لتجنب الأضرار المحتمل وقوعها بسبب الثغرات أو مكامن الخطر المعروفة أو للحد منها. وتشمل الضمانات المتعلقة بالأمن وضع الحلول الفنية المناسبة، وتوفير بيئة للعمل، وحجم الشبكات ونظم المعلومات المتوفرة فيها. وبذلك تصبح خطط الحماية والحلول جزءاً لا يتجزأ من هيكلية النظم، وعنصرا أساسيا في تصميمها؛

(ج) **إدارة الأمن**: إلى جانب تقييم المخاطر، يجب أن تتميز عملية إدارة أمن شبكات ونظم المعلومات بالدينامية، وأن تشمل جميع الأنشطة وعمليات المشتركين على كافة المستويات. ويجب أن تركز إدارة الأمن على توفير ردود سريعة ومناسبة لمعالجة التهديدات أو الوقاية منها، والكشف عن الحوادث والاستجابة بسرعة لدى وقوعها، ومراجعة هذه المراحل باستمرار بغية تحديثها وتطويرها. وبالتالي، تصبح جميع السياسات والممارسات والإجراءات التي تعتمد على نظم المعلومات والشبكات متناسقة ومتكاملة بحيث تضمن قيام نظام أمني متماسك؛

(د) **إعادة تقييم الخطط**: نظراً إلى طبيعة التهديدات المتغيرة والمتطورة باستمرار، يشدد هذا المبدأ على أهمية مراجعة عملية إدارة أمن نظم المعلومات والشبكات، وإعادة تقييمها، وإجراء التعديلات الضرورية والمناسبة في السياسات والخطط والممارسات والتدابير والإجراءات المنفذة لهذه الغاية.

وتجدر الإشارة هنا إلى أن مجموعة إدارة الأمن ترتبط بالأعمال التي تقوم بها مراكز الاستجابة لطوارئ الحاسوب المنتشرة في عدد من بلدان العالم.

باء- خطة عمل للتوعية حول ضمان الأمن في استخدام تكنولوجيا المعلومات والاتصالات

يعتبر المحللون والخبراء أن العنصر البشري يبقى الحلقة الأضعف في أي إطار أو مخطط لمعالجة مسألة أمن المعلومات. ومن هنا، برزت أهمية تعزيز ثقافة المستخدمين والمؤسسات من أجل درء المخاطر والتقليل من التعديات على أمن الشبكات والنظم والمعلومات. وفي هذا المجال، أصدرت وكالة أمان المعلومات والشبكات الأوروبية في عام 2006 دليلاً حول كيفية رفع مستوى الوعي بأمن المعلومات[102]. وكان هدف الوكالة تقديم المساعدة إلى البلدان الأعضاء من أجل رفع مستوى الوعي، ونشر مفهوم استخدام تكنولوجيا المعلومات والاتصالات بشكل آمن ومسؤول.

ويهدف الدليل إلى وضع استراتيجية مفصلة ودقيقة حول كيفية التخطيط لأي مبادرة توعية وطنية بشأن أمن المعلومات وتنظيمها وإدارتها، وإلى إبراز المخاطر التي قد تواجهها مبادرات التوعية في محاولة لتجنبها. كما يتضمن الدليل إطاراً عاماً لتقييم فعالية مبادرات التوعية، ويعرض نماذج حول كيفية إجراء هذا التقييم.

1- الفئات المستهدفة بمبادرات التوعية حول أمن تكنولوجيا المعلومات والاتصالات

يتوجه هذا الدليل إلى فئتين أساسيتين في المجتمع، هما فئة المستخدمين المنزليين وفئة المستخدمين في الشركات الصغيرة والمتوسطة الحجم. ونستعرض فيما يلي هاتين الفئتين واحتياجاتهما تفصيلاً:

(أ) فئة المستخدمين المنزليين: وتشمل جميع المواطنين، على اختلاف أعمارهم ودرجة معرفتهم وكفاءتهم الفنية، الذين يستخدمون تكنولوجيا المعلومات والاتصالات لأغراض شخصية في أي مكان خارج بيئة العمل. وتنقسم هذه الفئة إلى المجموعات الثلاث التالية:

(1) **مجموعة الشباب**: وتضم الشباب الذين تتراوح أعمارهم بين 7 سنوات و15 سنة، المتملكين من تكنولوجيا المعلومات والاتصالات، وإن بمستويات متفاوتة، لأنهم نشأوا منذ صغرهم في هذه البيئة ويملكون قدرة كبيرة على التعلم؛

(2) **مجموعة البالغين**: وتضم الذين تجاوزوا السادسة عشرة عاماً من العمر، ونشأوا جزئياً في بيئة تكنولوجيا المعلومات والاتصالات. وهذه المجموعة هي على الأرجح الأكثر تنوعاً من حيث مستويات المهارات والمعارف في هذا المجال. وتضم هذه المجموعة الأهالي والأشخاص العاديين الذين يمارسون مهناً مختلفة؛

(3) **مجموعة المبحرين الفضيين**: وتضم المتقدمين في السن الذين كبروا في بيئة لا تتعامل مع تكنولوجيا المعلومات والاتصالات، وهم بالتالي يجهلون هذا المجال ولا يثقون به.

---

(102) *A Users' Guide: How to Raise Information Security Awareness*. Enisa. June 2006.

وفي المنطقة العربية، يمكن أن تنضم إلى هذه المجموعة فئات أخرى مثل القاطنين في المناطق النائية البعيدة عن استخدامات التكنولوجيا[103]؛

(ب) **فئة المستخدمين في الشركات الصغيرة والمتوسطة الحجم**: وتضم أصحاب العمل والموظفين على حد سواء. وتنقسم هذه الفئة إلى المجموعات الأربع التالية:

(1) **مجموعة أرباب العمل أو المدراء**: وتعتبر هذه المجموعة من أهم الفئات المستهدفة لأنها تملك قرارات الاستثمار أو عدم الاستثمار في أمن المعلومات والشبكات التابعة للشركة؛

(2) **مجموعة موظفي إدارة تكنولوجيا المعلومات**: يملك أفراد هذه المجموعة عادة المعرفة التقنية لكنهم ليسوا بالضرورة خبراء في أمن النظم والمعلومات، وهنا تكمن حاجتهم إلى فهم بروتوكولات أمن المعلومات والشبكات بغية تطبيقها بالشكل السليم؛

(3) **مجموعة موظفي المصالح الإدارية**: تتألف هذه المجموعة من موظفي الدوائر والمصالح الإدارية المعنيين بتنفيذ الإجراءات الإدارية. يجب تثقيف أفراد هذه المجموعة وتلقينهم أسس أمن المعلومات وأهميتها والدور الذي تؤديه في ضبط مجالات أعمالهم ومراقبتها لأنهم لا يملكون عادة المعرفة التكنولوجية الضرورية؛

(4) **مجموعة الموظفين والعمال**: تعتبر هذه المجموعة من أكبر المجموعات المستهدفة ضمن فئة الشركات، إن لم تكن أهمها. فالأبحاث تشير إلى أن معظم التهديدات والاختراقات التي تتعرض لأمن نظم المعلومات والشبكات ناتجة عن أخطاء وأعمال بشرية.

2- الاستراتيجية المقترحة لتصميم مبادرات التوعية حول أمن المعلومات وتنفيذها

يتضمن دليل المستخدم المتصل بكيفية رفع مستوى الوعي بأمن المعلومات استراتيجيةً شاملة للتوعية. وتتناول هذه الاستراتيجية أبرز العمليات الضرورية للتخطيط لبرامج التوعية حول أمن المعلومات والشبكات وتنظيمها وإدارتها، بدءاً من تقييم الاحتياجات ورسم الخطط وتنفيذها، ووصولاً إلى تقييمها وتعديلها في بعض الحالات. ويمكن اعتبار هذه الاستراتيجية المقترحة إطاراً عاماً وشاملاً يمكن الاعتماد عليه لتنفيذ أنشطة التوعية الخاصة بأمن المعلومات والاتصالات وتحديد النطاقات المتخصصة فيها والفئات المستهدفة.

وتنقسم هذه الاستراتيجية إلى ثلاث مراحل أساسية مبينة في الشكل 15: (أ) تقييم الاحتياجات ورسم الخطة؛ (ب) تنفيذ الخطة وإدارتها؛ (ج) تقييم الخطة وتعديلها. وتحدد الاستراتيجية عدة أنشطة وعمليات يجب العمل على تنفيذها في كل مرحلة من المراحل.

(أ) المرحلة الأولى: تقييم الاحتياجات ورسم خطة العمل، وتتضمن تنفيذ النشاطات التالية:

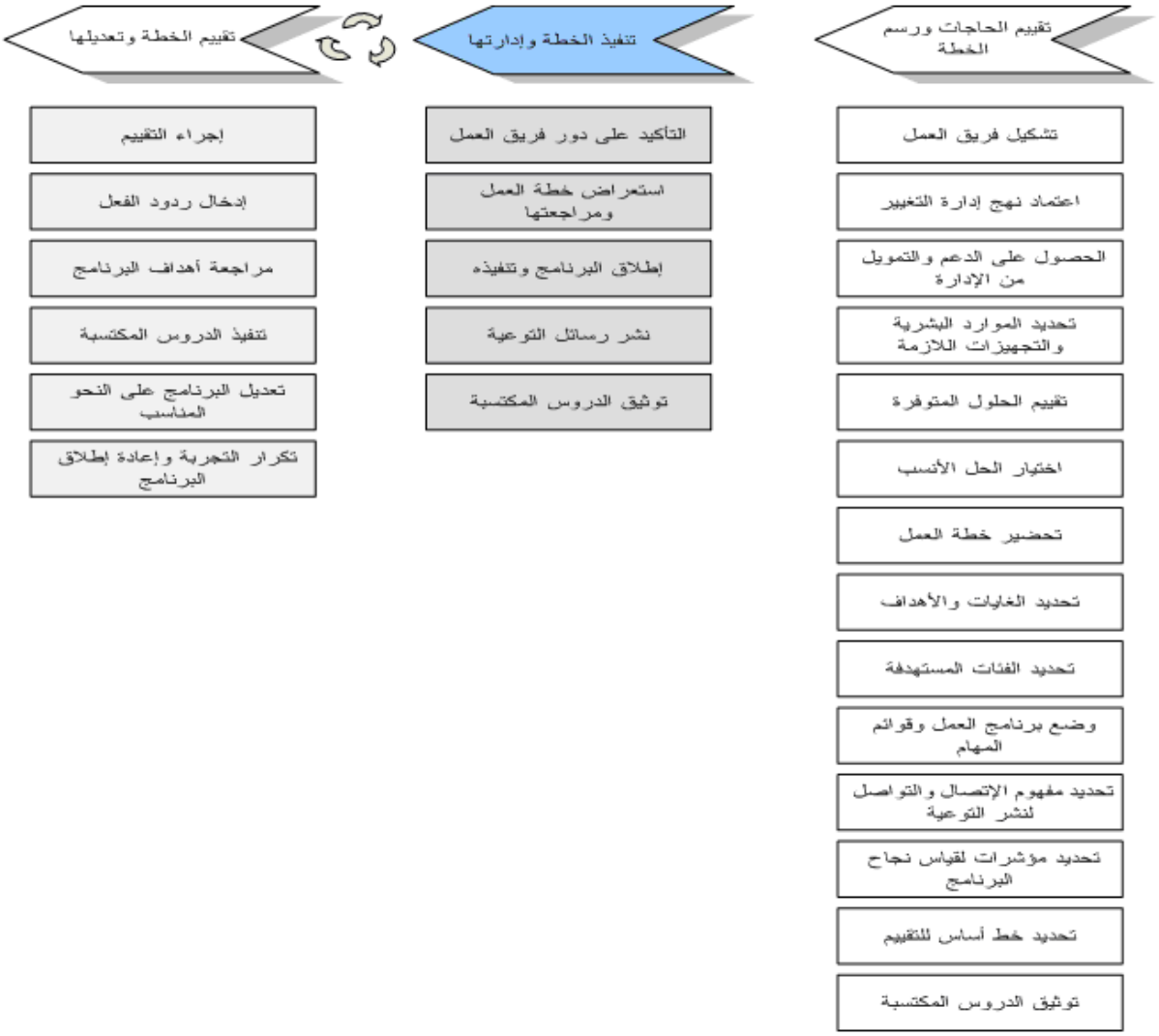
(103) تعبر هذه الفقرة عن رأي معدي هذا التقرير، وهي لم ترِد في الدليل الصادر عن وكالة أمان المعلومات والشبكات الأوروبية.

(1) **تشكيل فريق العمل المعني بإعداد برنامج التوعية** للبدء بعملية التخطيط للمبادرة وتنظيمها. ويفضل أن يكون أعضاء الفريق من ذوي الخبرة في إعداد برامج التوعية والتدريب في مجال تكنولوجيا المعلومات والاتصالات واستخداماتها، ومن ذوي الخبرة في المجال الإعلامي؛

(2) **اعتماد نهج إدارة التغيير** لدعم برنامج التوعية وضمان استمراريتها في المستقبل. لذا، يجب الاتفاق على بعض المبادئ، ومن أهمها: إشراك أصحاب المصلحة الرئيسين في عمليات صنع القرار والتخطيط والتنفيذ والتقييم، وتحديد الأدوار والمسؤوليات بوضوح، وإدارة المخاطر، وتذليل العوائق التي تحول دون التغيير، وتقديم الدعم والتدريب والتطوير لضمان إحداث تغيير في السلوك والثقافة، والتعلم من التجارب السابقة والحالية، وغيرها من المبادىء التي تضمن عملية التغيير في الإدارة؛

الشكل 15- العمليات الضرورية للتخطيط لبرامج التوعية بأمن المعلومات والشبكات وتنظيمها وإدارتها[104]

(104) *.A Users' Guide: How to Raise Information Security Awareness*. enisa. Phase I. Plan and Assess, p. 14



(3) **الحصول على الدعم والتمويل اللازمين من الإدارة،** وذلك عبر ترسيخ مفهوم أهمية برامج التوعية بأمن المعلومات التي تتوجه إلى الجهات المعنية وأصحاب القرار والإداريين. وينبغي في هذه المرحلة تحديد التكاليف الضرورية لتنفيذ مبادرة التوعية، حيث يتعين رصد موازنة خاصة لبرنامج التوعية بأمن المعلومات، وذلك من أجل تغطية تكاليف رواتب الموظفين أي مدير برنامج التوعية ومساعديه وجميع العاملين على مبادرات التوعية، وتكاليف مواد التوعية والترويج والإعلانات وطباعة الملصقات وغيرها من المواد التي ستستخدم في البرنامج.

وللحصول على الدعم على المستويين الإداري والمادي، من الضروري تحديد المنافع والأهداف المبتغاة من جراء تنفيذ برنامج التوعية. ومن أهم فوائد برنامج التوعية التدريب والتعليم في مجال أمن المعلومات، ونشر المبادىء التوجيهية والممارسات المتميزة لضمان أمن موارد المعلومات، وتحفيز الاشخاص على تبنيها، وتزويد الأشخاص بمعلومات عامة حول أهم المخاطر والضوابط الخاصة بأمن المعلومات،

وحث المعنيين على إدراك مسؤولياتهم والالتزام بها في هذا الصدد، وتعزيز ثقافة أمن المعلومات والالتزام بها، والتقليل من عدد الانتهاكات التي يتعرض لها أمن نظم المعلومات ومواردها وحجم هذه الانتهاكات، وبالتالي تقليل التكاليف المباشرة (الناتجة مثلاً عن تدمير الفيروسات بعضَ البيانات) والتكاليف غير المباشرة (عبر خفض عدد المخالفات، وتسهيل التحقيق فيها وحلها مثلاً)؛

(4) **تقييم الحلول المتوفرة واختيار الحل الأنسب** عبر دراسة الحلول والمقترحات المتوفرة في الأسواق وتحليلها لتنفيذ مبادرة توعية حول أمن نظم المعلومات وشبكاتها؛

(5) **تحضير خطة عمل** لتحديد الأنشطة والموارد، والجداول الزمنية الضرورية لتنفيذ برنامج التوعية. وتجدر الإشارة إلى أهمية وضع خطة العمل هذه، وضرورة مراجعتها بشكل دوري وتعديلها عند الحاجة؛

(6) **تحديد الغايات والأهداف المرجوة من برنامج التوعية**: وهي الغايات المزمع بلوغها عبر تنفيذ برنامج التوعية حول أمن المعلومات والشبكات والخدمات الإلكترونية؛

(7) **تحديد الفئات المستهدفة** من أجل تبيان الفئات الخاصة التي يستهدفها برنامج التوعية. ولهذه الغاية، يجب طرح عدة أسئلة، ومنها ما يلي: إلى من يتوجه برنامج التوعية هذا؟ هل تتطابق حاجات الفئات المستهدفة أم تختلف؟ كيف تنظر كل فئة إلى مفهوم ثقافة أمن استخدام تكنولوجيا المعلومات والاتصالات؟

(8) **وضع برنامج العمل وتحديد الأولويات، حيث** ينبغي وضع لائحة كاملة بالمواضيع التي سيتناولها تنفيذ برنامج العمل، وتقييمها، وتصنيفها بحسب أهميتها تمهيداً لتحديد الأولويات وتحسين شروط التنفيذ؛

(9) **تحديد أدوات الاتصال والتواصل لنشر التوعية**: ففي هذه المرحلة، يعمل الفريق المعني برفع مستوى الوعي حول أمن المعلومات على تحديد الرسائل الأساسية التي يجب نشرها عبر برنامج التوعية واختيار قنوات النشر الملائمة (كالنشرات، والجرائد، والتلفاز، والإنترنت) لكل فئة من الفئات المستهدفة. وبالإضافة إلى هذه القنوات، يمكن الاعتماد على عدد من الشركاء في المجتمع من أجل إيصال رسالة التوعية إلى أكبر شريحة ممكنة من المجموعات المستهدفة في برنامج التوعية. ومن بين هؤلاء الشركاء، يمكن ذكر المصارف، ومراكز التنمية المحلية، والمدارس والثانويات والمعاهد والجامعات في المناطق، ومراكز بيع الحواسيب، ومزودي خدمة الإنترنت، والمكتبات، والجمعيات الأهلية والاتحادات الصناعية والتجارية، وغيرها من المؤسسات العاملة في المجتمع المحلي. ويشير الإطار 6 إلى الإجراءات المتخذة من أجل وضع خطة عمل لتنفيذ برنامج توعية حول أمن استخدام تكنولوجيا المعلومات والاتصالات؛

الإطار 6- نموذج عن الإطار المعتمد في عمليات رفع مستوى الوعي بأهمية حماية الخصوصية والبيانات الشخصية(*)

الجمهور المستهدف	احتياجات الجمهور	رسالة التوعية	قنوات النشر	المسؤولون	الأهداف المرجوة	التوقيت والتواتر	الأدوات المستخدمة في ردود الفعل
من تستهدف رسالة التوعية؟	ما هي احتياجات الجمهور؟	ما هو محتوى الرسالة؟	ما هو شكل الرسالة؟	من المسؤول عن نشر الرسالة؟	ماذا نأمل بعد تحقيق هذه المبادرة؟	في أي وقت يجب إطلاق المبادرة؟	ما هي الأدوات التي سيتم استخدامها لجمع ردود فعل الجمهور؟
المبحرين الفضيين	مستوى المعرفة لدى هذه الفئة منخفض أو حتى معدوم	حماية الخصوصية والبيانات الشخصية في أثناء استخدام الإنترنت	توزع المعلومات من خلال برامج الرعاية الصحية	فريق عمل برنامج التوعية	زيادة فهم الفئات المستهدفة للحلول المتوفرة	ينبغي أن تتزامن مع الأسبوع الوطني لكبار السن	البريد الإلكتروني
	انعدام الثقة بالتكنولوجيا واستخداماتها		بالتعاون مع مراكز ومؤسسات الضمان الاجتماعي				الهاتف

(*) *A Users' Guide: How to Raise Information Security Awareness*. Develop Detailed Communication Plan. European Network and Information Security Agency (enisa), 2006, p. 33.

(10) **تحديد مؤشرات لقياس نجاح البرنامج**: فبهدف قياس الوعي بأمن استخدام تكنولوجيا المعلومات والاتصالات، ينبغي وضع مؤشرات تتعلق بأربعة عناصر رئيسة هي: تحسين العمليات، ومقاومة الهجمات، والكفاءة والفعالية، والحماية الداخلية. ويعرض الإطار 7 أمثلة حول هذه المؤشرات؛

الإطار 7- مؤشرات لقياس نجاح برنامج التوعية

بهدف قياس أداء الجهات المشرفة على خطة التوعية الوطنية حول حماية استخدام تكنولوجيا المعلومات والاتصالات وأمنها وكفاءتها في تطوير التوجيهات المتعلقة بأمن استخدام هذه التكنولوجيا ونشرها وتطبيقها، يمكن وضع مؤشرات على المستوى الوطني وعلى مستوى الشركات. وفيما يلي بعض الأمثلة على كل منها:

1- **على المستوى الوطني**:

- وجود مبادرة تقوم بها السلطات العامة (لوحدها أو بالتعاون مع القطاع الخاص) لتوعية عامة الناس حول أمن المعلومات والشبكات؛
- وجود مبادىء واضحة وموجزة لمبادرة التوعية الوطنية؛
- النسبة المئوية للأفراد الذين يعلمون بإطلاق مبادرة التوعية الوطنية؛
- النسبة المئوية للأفراد الذين يملكون معلومات حول أهداف مبادرة التوعية الوطنية وتوجهاتها؛

- النسبة المئوية للأفراد الذين يملكون معرفة تامة بالإجراءات الصحيحة التي يجب اتخاذها، أو بالجهة التي ينبغي الاتصال بها في حال وقوع حادث ما؛
- نسبة الأفراد الذين تابعوا برنامج التوعية؛
- نسبة الأفراد الذين زودوا أجهزتهم الحاسوبية ببرامج فحص الفيروسات.

2- **على مستوى الشركات الصغيرة والمتوسطة الحجم**:

- وجود سياسة خاصة بأمن المعلومات والشبكات؛
- نسبة الموظفين الذين يعلمون بوجود سياسة خاصة بأمن المعلومات على مستوى الشركة؛
- نسبة الموظفين الذين قرأوا سياسة الشركة الخاصة بأمن المعلومات، ويعملون على تطبيق بعض العمليات المقترحة فيها؛
- نسبة الموظفين الذين يعلمون بالجهة التي ينبغي الاتصال بها في حال وقوع أي حادث؛
- وجود برنامج توعية يستهدف الموظفين؛
- نسبة الموظفين الذين تابعوا برنامج التوعية حول أمن المعلومات.

(11) تحديد خط أساس للتقييم: ينبغي تقييم الوضع قبل البدء بتنفيذ برنامج التوعية للتمكن من استخدام المؤشرات الموضوعة لقياس فعالية هذا البرنامج وأثره؛

(12) توثيق الدروس المكتسبة: يمكن استنباط بعض المواقف والظروف التي مر بها فريق العمل خلال مرحلة تقييم الحاجات والتخطيط للبرنامج وتوثيقها واستخدامها في برامج مستقبلية؛

(ب) **المرحلة الثانية: تنفيذ الخطة وإدارتها**، وتتضمن تنفيذ خمسة أنشطة:

(1) **التأكيد على دور فريق العمل المخصص للقيام ببرنامج التوعية**: أي العمل على تنفيذ الأنشطة من أجل رفع مستوى التوعية حول أمن استخدام تكنولوجيا المعلومات والاتصالات، حيث ينبغي على كل عضو في الفريق أن يؤدي دوره بامتياز وأن يتحمل مسؤوليات التنفيذ والنتائج المرتقبة؛

(2) **استعراض بنود خطة العمل ومراجعتها**: قبل البدء الفعلي بالتنفيذ، يستحسن مراجعة بنود خطة العمل وتعديلها أو استكمالها ببعض البنود الضرورية كي تتماشى أكثر مع الأهداف والغايات واحتياجات الموازنة؛

(3) **إطلاق برنامج التوعية وتنفيذه**: في هذه المرحلة، يبدأ فريق العمل بتنفيذ أنشطة التوعية بسلاسة وفعالية بفضل الإجراءات التي سبقت التنفيذ، من تحديد للاحتياجات، ووضع للحلول المناسبة؛

(4) **نشر رسائل التوعية**: تنفيذ خطة الاتصال والتواصل ونشر الرسائل التي يتضمنها برنامج التوعية لرفع مستوى الأمن في استخدام المعلومات والشبكات الإلكترونية. ومن المهم في هذه المرحلة جمع التعليقات والملاحظات وردود الفعل والاستفادة منها في تنفيذ الدورات المقبلة من البرنامج؛

(5) **توثيق الدروس المكتسبة**: توثيق الدروس المستخلصة من هذه المرحلة الثانية؛

(ج) **المرحلة الثالثة: تقييم الخطة وتعديلها**: وتتضمن ستة أنشطة:

(1) **تقييم برنامج التوعية**: فقد أظهرت تجارب بعض البلدان إمكانية قياس فعالية برامج التوعية من حيث قدرتها على تحسين أمن المعلومات، وذلك بالرغم من بعض الادعاءات المعاكسة. فبتحديد خط الأساس، يمكن إعطاء صورة كاملة عما كانت عليه حالة الفئات المستهدفة قبل تنفيذ البرنامج. وبمتابعة استبيانات المسح الشامل وعمليات المتابعة الدورية، يمكن تتبع التقدم المحرز في مجال التوعية حول أمن استخدام تكنولوجيا المعلومات والاتصالات؛

(2) **أخذ ردود الفعل بعين الاعتبار**: ينبغي الأخذ بردود الفعل الواردة من الفئات التي شملها برنامج التوعية، وإدراجها في البرامج اللاحقة؛

(3) **مراجعة أهداف البرنامج** في ضوء النتائج الصادرة عن تقييم فعالية البرنامج؛

(4) **تنفيذ الدروس المكتسبة**: بعد تقييم الدروس المكتسبة من برنامج التوعية، ينبغي العمل على تطبيق هذه الدروس وتكرارها لإنجاح البرنامج في المستقبل، وتعزيز فعاليته؛

(5) **تعديل البرنامج على النحو المناسب**: توفر الخبرات المكتسبة منذ بدء تطبيق البرنامج، والمعارف الضرورية لتعديل البرنامج، وتعزيز فرص نجاحه. ويمكن أن تطال هذه التعديلات أي نشاط أو مهمة في البرنامج من دون المس بأهدافه وغاياته الأساسية؛

(6) **تكرار التجربة وإعادة إطلاق البرنامج**: وذلك بإعادة المراحل السابقة بدءاً من المرحلة الثانية، واستغلال هذه الفرصة لتعزيز المواضيع التي يشملها البرنامج وتطويرها.

جيم- مبادرات ناجحة للتوعية في عدد من البلدان العربية والأجنبية

قامت بلدان عديدة بإعداد برامج للتوعية في مجال أمن المعلومات والشبكات، واستخدام التطبيقات الإلكترونية وتنفيذها. وفي هذا الصدد، تستعرض هذه الدراسة التجربتين التونسية والسعودية، إضافة إلى تجربة أستراليا وماليزيا.

1- مبادرات التوعية في تونس

تعنى الوكالة الوطنية لأمن المعلوماتية في تونس[105] بالتوعية. وهي تتخذ مبادرات عدة لإطلاع كافة شرائح المجتمع على قضايا الأمن والمخاطر، والحلول والمواقف التي يمكن أن تعزز أمن النظم والشبكات. كما تهتم الوكالة بإنشاء منتديات للمناقشة يشارك فيها المهنيون والخبراء، وتساهم في إنشاء جمعيات تعنى بأمن الحواسيب. وبهدف رفع مستوى الوعي بأمن استخدام تكنولوجيا المعلومات والاتصالات، تقوم الوكالة بنشر عدة برامج للتوعية بأمن نظم المعلومات والشبكات عبر موقعها الإلكتروني وتستهدف من خلالها الأهالي والأطفال بصورة خاصة[106]. فيجد الآباء مثلاً بعض النصائح التي يفيد التذكير بها، وبعض الاحتياطات البسيطة التي تساهم في حماية أطفالهم من المخاطر المحتملة على شبكة الإنترنت، وتسمح لهم بالسيطرة على استخدام أولادهم للإنترنت.

ويقدم الموقع أيضاً نصائح حول استخدام التقنيات الخاصة بترشيح البريد الإلكتروني الخاص وحمايته من البريد الدعائي. ويقدم البرمجيات المضادة التي يمكن تحميلها من الموقع مباشرة[107]، كما يعرض دليلاً مفصلاً حول طريقة استخدام هذه البرمجيات والتحكم بها.

وفي إطار تعزيز أنشطة التوعية، تصدر الوكالة الوطنية لأمن المعلوماتية في تونس مطبوعات متخصصة عديدة في هذا المجال.

2- موقع إلكتروني للتوعية في المملكة العربية السعودية

يعمل المركز الوطني الإرشادي لأمن المعلومات التابع لهيئة الاتصالات وتقنية المعلومات في المملكة العربية السعودية[108] على رفع مستوى وعي الأفراد والمؤسسات بالأخطار التي تهدد أمن المعلومات. ويتعاون المركز مع أعضائه وشركائه في المملكة وخارجها لتنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة.

ويتضمن موقع المركز على شبكة الإنترنت[109] مركزاً إلكترونياً للتوعية في مجال المعلومات والشبكات. كما يتوجه إلى المنظمات والمؤسسات والمستخدمين العاديين، وينشر مقالات متخصصة لرفع مستوى وعي المستفيدين من خلال برامج ومواضيع توعية تتعلق بقضايا الأمن المعلوماتي وسبل معالجتها. كما يقوم المركز ببناء القدرات المحلية عبر تنظيم دورات تدريبية ومؤتمرات وورش عمل يتم خلالها توزيع مطويات ومطبوعات. وتتضمن المطوية الصادرة عن المركز الوطني الإرشادي لأمن المعلومات في المملكة العربية السعودية ثماني نصائح لحماية الجهاز الشخصي من مخاطر الإنترنت.

3- مبادرات التوعية في أستراليا

(105) http://www.ansi.tn/ar/index_ar.htm.

(106) *Conseils pratiques pour parents*, http://www.ansi.tn/fr/parents_enfants/conseils_pour_parents.htm.

(107) http://www.ansi.tn/fr/outils_domestique.htm.

(108) http://www.cert.gov.sa.

(109) http://www.cert.gov.sa/index.php?option=com_content&task=blogsection&id=18&Itemid=109.

أنجزت الهيئة الأسترالية للاتصالات والإعلام[110] مشروع توعية محلية موجه إلى الأطفال، وأطلقت عليه تسمية الإبحار الآمن للأطفال عبر الإنترنت (Cybersmart Kids Online)[111]. ويهدف المشروع إلى تزويد الأهالي والأطفال بالمعلومات والأدوات التي يمكن أن تساعدهم على أن يكونوا آمنين خلال استخدامهم شبكة الإنترنت. ويتوجه هذا الموقع بشكل خاص إلى الأطفال والشباب الذين تقل أعمارهم عن 18 سنة. كما يقدم لهم مواد للتوعية ومواد تعليمية بطريقة ترفيهية تتناسب مع مختلف مراحل نموهم. ويشتمل الموقع على دليل للشباب يتضمن عدداً من التوصيات والمبادئ التي تعلمهم التعامل بذكاء وبأمان مع شبكة الإنترنت، سواء للإبحار في صفحات الإنترنت، أو لتصفح بريدهم الإلكتروني، أو للدردشة. كما يعرض بعض الفصول الخاصة بالأهالي والمعلمين، حيث يتوجه إليهم بعدد من التوجيهات والنصائح للتمتع باستعمال الإنترنت وخدماته بشكل آمن. ويدعم الموقع نشاط معلمي المدارس في عملية تدريب طلابهم وتوعيتهم على التصرف الذكي والسليم في العالم السيبراني، ويقدم لهم برامج تدريبية وموارد إلكترونية وواجبات منزلية. ويقدم الموقع أيضاً في قسم خاص نصائح حول ضمان استخدام الهاتف المحمول بطريقة سليمة وآمنة.

4- تجربة ماليزيا في بناء ثقافة الأمن في الفضاء السيبراني

يمكن اعتبار تجربة ماليزيا في بناء ثقافة الأمن في الفضاء السيبراني من أغنى تجارب البلدان في هذا المجال. فقد أُدرج مفهوم ثقافة الأمن وبناء القدرات كبند أساسي في الإطار الوطني لأمن الفضاء السيبراني، بهدف تطوير ثقافة الأمن على المستوى الوطني وتعزيز وضمان استمراريتها. وتحقق ذلك عبر توحيد وتنسيق الجهود المبذولة لرفع مستوى التوعية، وإنشاء آلية فعالة لنشر المعرفة المتعلقة بالأمن على شبكة الإنترنت.

ولتحقيق هذه الأهداف، أنشأت ماليزيا بوابة معلومات متخصصة في مواضيع الأمن الإلكتروني[112]، وهي تتوجه إلى جميع فئات المجتمع من أطفال وشباب وأهالي ومستخدمين ومنظمات. وتقدم البوابة معلومات شاملة وتفصيلية عن جميع المشاكل والأخطار التي من الممكن أن تتعرض لها هذه الفئات لدى استعمالها شبكة الإنترنت وخدماتها. كما تقدم البوابة النصائح والقواعد والتعاريف وأفلام الفيديو والمقالات التي يمكن الاعتماد عليها لبناء المعرفة، والتصدي لمثل هذه الأخطار أو الوقاية منها. وتتطرق بوابة المعلومات إلى كيفية إعداد السياسات المتعلقة بالأمن السيبراني في المنظمات والمؤسسات وتطبيقها. كما تعرض عينات أو نماذج عن سياسات مثيلة يمكن الاعتماد عليها كدليل في عملية بناء سياسات الأمن المعلوماتي.

---

(110) The Australian Communications and Media Authority (ACMA). *eSecurity-Towards Building A Security Culture*. http://www.acma.gov.au/WEB/HOMEPAGE/PC=HOME.

(111) http://www.cybersmartkids.com.au/about-us.htm.

(112) http://www.esecurity.org.my.

سادساً- منهجيات تطوير خدمات إلكترونية موثوقة

أصبح من المؤكد أن استخدام تكنولوجيا المعلومات والاتصالات يؤثر إيجاباً على تقديم الخدمات الإدارية والصحية والتعليمية والتجارية لجميع فئات المجتمع، من أفراد وطلاب وأصحاب أعمال وعاملين في الدولة. لكن كثيرين ما زالوا يفضلون الحصول على الخدمات بالطرق التقليدية لأسباب متعددة، منها صعوبة النفاذ إلى الخدمات الإلكترونية أو عدم القدرة على استثمارها، أو عدم الثقة بها وبنتائجها. ومن هنا تبرز أهمية تصميم الخدمات الإلكترونية وتطويرها بطرق ابتكارية تثير اهتمام المستخدمين وتحظى بثقتهم، بحيث تزودهم بقيم مضافة مقارنة مع الطرق التقليدية. وبالتالي، يجب أن يكون الهدف الرئيس وراء تطوير أي نظام للخدمات الإلكترونية بشكل أساسي تعزيز كفاءة أداء الخدمات الإلكترونية، وتسهيل الحصول عليها.

ويحتاج تطوير الخدمات الإلكترونية إلى استثمار جيد في تكنولوجيا المعلومات والاتصالات ونظمها وقواعد بياناتها، ويتطلب وضع آليات تفاعل يثق بها المستخدم النهائي ويسهل عليه استعمالها. وينبغي معالجة الخدمات الإلكترونية وتطويرها بما يتلاءم مع البيئة الرقمية، وبما يتناسب مع السياق الاجتماعي والنفسي للمستخدمين، ومن خلال نهج للتطوير يركز على المستخدم النهائي وعلى ثقته بالخدمة الإلكترونية وبمزودها.

ويشير هذا الفصل إلى عدد من المنهجيات التي يجب أخذها في الاعتبار عند تطوير الخدمات الإلكترونية وتقديمها، وبعض خصائص الخدمات الإلكترونية التي تساعد في بناء ثقة المستخدمين بها. وتجدر الإشارة إلى أن الخصائص العامة للخدمات الإلكترونية الموثوقة هي حصيلة الدراسات التي أُعدت في إطار مشروع تراست غايد (Trustguide)[113] الذي تم تنفيذه في المملكة المتحدة.

ألف- تقديم خدمات ذات قيمة مضافة

أظهرت الدراسات والأبحاث أن نجاح نظام الخدمات الإلكترونية يتطلب تحقيق قيمة مضافة واضحة للمستخدمين، مثل توفير الوقت والكلفة والجهد، وتقديم خدمات غير تقليدية يصعب على العملاء العاديين الحصول عليها. ومن هذه الخدمات غير التقليدية نذكر مثلاً خدمات المعلومات والاستشارات المالية، والخدمات الإلكترونية على مدار الساعة وطوال أيام الأسبوع وخلال العطلات. كما يحتاج نجاحها إلى تحقيق قيمة مضافة واضحة لمقدم الخدمة أيضاً، مثل خفض كلفة أداء الخدمات للعملاء، وكلفة تسيير الأعمال الداخلية والخارجية، وكلفة نقل النقد الورقي وحفظه وتداوله. ويحتاج نجاحها كذلك إلى زيادة القدرة التنافسية لمقدم الخدمة وجذب المزيد من العملاء، وزيادة أنشطة العملاء الحاليين عن طريق تطوير باقة الخدمات المقدمة إليهم وقنوات التواصل معهم.

ولتحقيق قيمة مضافة واضحة للمؤسسة المسؤولة عن تقديم الخدمة الإلكترونية، يجب أن يهتم مطورو الخدمات الإلكترونية بدراسة باقة الخدمات الإلكترونية التي يمكن أن يوفرها مقدم الخدمة، وحساب كلفة القيام بها والمخاطر المرتبطة بها، وما يمكن أن يحققه بتوسيع نطاق خدماته وبزيادة عملائه وزيادة حجم تعاملاتهم، وخفض نفقات خدمة العملاء ونفقات توسيع الفروع وزيادة عددها. كما يجب دراسة كلفة إنشاء

(113) تراست غايد (Trustguide) هو مشروع مشترك بين مجموعة بريتيش تلكوم (British Telecom) ومختبرات هوليت باكرد (Hewlett Packard)، ومدعوم من المركز المعني بأمن المعلومات والأبحاث في جامعة بلايماوث (Plymouth) في المملكة المتحدة - www.trustguide.org.uk.

البنية الأساسية للخدمات التي تشمل نظم المعلومات والشبكات والاتصالات، وقواعد البيانات ونظم تأمين الشبكات والآليات وقنوات التواصل مع العملاء. كما يجب الاهتمام بإعداد الكوادر البشرية والخبرات اللازمة لتفعيل نظام العمليات والخدمات الإلكترونية وحمايتها. ومن المفيد الاستعانة بخبراء واستشاريين متخصصين في التقنيات المستخدمة وفي نظم العمليات الإلكترونية وأنماطها، وتوعية المستخدمين بما توفره الخدمة الإلكترونية لهم من مزايا، وإشراكهم والأخذ برأيهم عند طرح البدائل لتطوير الخدمات الإلكترونية واختيارها.

باء- الإلتزام بتقديم الخدمة إلكترونياً

يبدأ نجاح تطوير نظام الخدمات الإلكترونية وتفعيله بإنشاء قيادة تعي ما يقدمه ذلك النظام من إضافات ومزايا لمختلف الأطراف، وما يرتبط بها من تقنيات وآليات، وما تتطلبه من عناصر. ويجب التمييز بين الاستعانة بالتكنولوجيا، كالحواسيب والشبكات من أجل تحسين أداء العمليات والخدمات، وبين استحداث نموذج جديد للعمليات يوظف تلك التكنولوجيات لصالح المستخدم والمؤسسة بصورة غير مسبوقة وغير تقليدية.

وينبغي للجهة المزودة للخدمات أن تتنبه إلى عدد من الممارسات حين تقرر تطوير نظام الخدمات الإلكترونية، ومنها عدم الاحتفاظ بممارسات تقليدية تفصل الإدارات التكنولوجية عن إدارات تطوير العمليات والخدمات. فالنظام المتكامل لتأمين قنوات أداء الخدمات الإلكترونية ليس مجموعة من الأجهزة والنظم الهادفة إلى حماية الحواسيب وقواعد البيانات، ومنع اختراق الشبكات وتتبعها وحسب، وإنما هو مسؤولية مشتركة بين عدة إدارات، ومنها إدارة الأمن، وإدارة نظم المعلومات، والإدارة القانونية، وإدارة خدمة العملاء، وإدارة التدريب والتوعية. وبالتالي، يجب أن يجري تقديم الخدمات الإلكترونية وضمان حمايتها وأمنها وفق رؤية استراتيجية تعكس مصداقية المؤسسة المزودة للخدمات بوجه عام، وتنمي الثقة بالخدمات المقدمة إلكترونياً بوجه خاص.

وينبغي أن تدرك المؤسسة أيضاً أن أي خلل في نظام خدمة العملاء سيكون له أثر سلبي بالغ على نجاح نظام الخدمات الإلكترونية. فالتعامل الإلكتروني يتم "عن بعد" من دون تدخل شخصي مباشر، وبالتالي لا يستطيع العميل إتمام معاملته الإلكترونية بالشكل المطلوب عند حدوث خلل في الخدمة الإلكترونية. فإذا فشل العميل في سحب أمواله من صراف آلي لتسديد ثمن مشترياته، أو في إتمام عملية تحويل إلكتروني بشأن صفقة يقوم بها، وتعرض بالتالي لحرج بالغ أو خسارة فادحة، فَقَد حتماً ثقته بالخدمات الإلكترونية. فالعميل يتوقع خدمة ذات كفاءة عالية وقادرة على دعمه وحل أي مشكلة تصادفه في أي وقت، سواء كانت الخدمة مقدمة إلكترونياً أم بالوسائل التقليديةً.

ويجب على المؤسسة المقدمة للخدمات الإلكترونية ألا تتجاهل المخاطر التي قد يتعرض لها نظام الخدمات الإلكترونية من اختراق أو تعطيل أو ما إليها من صعوبات. فعلى الرغم من توخي الدقة، والاستعانة بالخبرات والأطر التنظيمية والحلول التقنية اللازمة، يبقى احتمال الأخطار قائماً، ولا يمكن الافتراض بأن أي نظام هو آمن كلياً من أخطار الاختراق أو العطب. ولذلك، ينبغي أن يضع مقدم الخدمة الآليات المناسبة للتأمين ضد المخاطر والحوادث تقنياً وإجرائياً، وأن يعمل على إعداد خطط بديلة لإدارة العمليات في حالات الطوارئ وتفعيل تلك الخطط، وإخطار عملائه عندما يشك في تضرر مداولاتهم.

جيم- بناء الثقة بالخدمات والتطبيقات الإلكترونية

حددت إحدى الدراسات التي أعدها مشروع تراست غايد[114] المسائل الأساسية المتعلقة ببناء الثقة وضمان الأمن والخصوصية في الخدمات والتطبيقات التي تعتمد على استخدام تكنولوجيا المعلومات والاتصالات، وذلك من وجهة نظر المستخدم بشكل أساسي. وقد اعتُبرت الثقة شرطاً أساسياً، فهي تكتسب أهمية خاصة في العلاقات التجارية، وفي جميع أنواع العلاقات التي تتضمن بعض المخاطر، لا سيما إذا كان وسيط العلاقة يعتمد على تكنولوجيا المعلومات والاتصالات التي يغيب عنها التواصل المباشر، والتي تتم من دون التعرف على أطراف هذه العلاقة.

ومن أجل استخلاص الشروط العامة المتعلقة بالثقة والأمن والخصوصية في التطبيقات والخدمات الإلكترونية، نَظّم القيّمون على مشروع تراست غايد عدداً كبيراً من ورش العمل التي شملت مجموعة واسعة من شرائح المجتمع بهدف إجراء حوار بين مصممي الخدمات الإلكترونية وبين جمهور العموم حول تعزيز الثقة بالخدمات الإلكترونية. ومن أهم الإنجازات التي حققها العاملون في هذا المشروع تقديم توصيات، ودليل عمل يحمل عدداً من المبادئ التوجيهية العامة التي يجب أخذها في الاعتبار لتطوير وتقديم خدمات إلكترونية بشكل موثوق. وتتضمن هذه المبادئ التوجيهية العناصر الستة الأساسية التالية:

1- التعليم والتوعية

أظهرت نتائج ورش العمل التي نظمت خلال تنفيذ مشروع "تراست غايد" أن أفضل وسائل التوعية في مجال تكنولوجيا المعلومات والاتصالات هي تلك التي تعتمد على التعلم الذاتي، والتي يقوم من خلالها الأفراد باستخدام تجهيزاتهم من أجل التعرف على تكنولوجيا المعلومات والاتصالات وخدماتها الإلكترونية. كما أشارت الاستطلاعات إلى أن الاستعانة بالأقران الموثوق بهم، كالأساتذة والمدربين أو الأقارب والأصدقاء من ذوي الخبرة، طريقة هامة للحصول على معرفة موثوقة. وتبين كذلك أن التعليم التفاعلي، الذي يستطيع من خلاله المتدربون طرح الأسئلة والتحاور، يؤثر إيجاباً على مستخدمي هذه التكنولوجيا وعلى ثقتهم بها وبخدماتها. ومن هنا تبرز أهمية تنظيم دورات تدريبية تفاعلية للأفراد بشكل منتظم حول استخدامات تكنولوجيا المعلومات والاتصالات، وأهمية التدريب في المدارس والجامعات لأن الأطفال والطلاب في مختلف المراحل هم من أكثر الفئات استخداماً لشبكة الإنترنت وتطبيقاتها. وبما أن التلفاز يعتبر وسطاً موثوقاً بالنسبة إلى الأطفال، فقد تكون توعية هذه الشريحة فعالة عن طريق البرامج التلفزيونية، ولا سيما بالاعتماد على الصور والألعاب.

2- إمكانية المحاولة والتعلم من التجربة

أظهرت نتائج الدراسة أهمية الاكتشاف الذاتي من خلال التجربة لدى غالبية البالغين والمراهقين، فالثقة تُبنى عادة لدى الأفراد من خلال تجربة خدمة معينة. ويجب أن يشكل عنصرا التجربة والاختبار جزءاً لا يتجزأ من عملية تعليمية متكاملة تؤدي إلى بناء علاقات قوية بين المستخدم وخدمات الإنترنت. كما أن تجربة الخدمات الإلكترونية في بيئة محدودة المخاطر (كالمعاملات المالية من دون أي التزام بتقديم البيانات الشخصية) أمر بغاية الأهمية لتحقيق المشاركة على المدى الطويل حيث تسمح هذه التجربة للمستخدم باكتشاف منفعتها والمشاركة في تقييمها في جو آمن.

---

(114) Trustguide: Final Report. October 2006. http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf، انظر التذييل 115 أعلاه.

3- توفير تدابير الاسترداد

يعتبر توفير تدابير الاسترداد للمستخدم دافعاً قوياً إلى قبوله بالخدمات الإلكترونية واعتمادها. فهذه التدابير، مثل إمكانية استعادة آخر حالة قبل حدوث المعاملة، تؤثر إيجاباً على التعاطي مع المخاطر المتصورة. وتشجع إتاحة عملية الاسترداد المستخدم على تعزيز ثقته بالمداولات الإلكترونية، لأن أثر نتائج المخاطرة المحتملة قد حُجم بشكل فعال. وقد أظهرت الدراسة أن الأشخاص لا يجرون المداولات الإلكترونية الحرجة إلا إذا كانوا على ثقة تامة بأنها ستلبي توقعاتهم (كأن تتم عملية الدفع الإلكتروني بدقة وسرية أو أن يتم تسليم البضائع وفق الجودة المتوقعة)، وبالتالي فإن إتاحة تدابير للاسترداد تمكن من تخفيف أي خطر ناتج عن خطأ ما بإعادة العملية إلى وضعها الأول مع ضمان عدم تكبيد الفرد أي خسارة.

وقد أظهرت نتائج الدراسة أيضاً أن ثقة الأفراد بإجراء مداولات تجارية عبر الإنترنت تتعزز في حال تعهد طرف ثالث، مثل المؤسسة المصرفية أو شركة بطاقة الائتمان التي يتعاملون معها، بعدم تكبدهم أي خسارة مالية نتيجة وقوع أي خطأ. وفي تلك الظروف، يمكن تقليص المخاطر المحتملة بدرجة كبيرة نظراً إلى أن الخطر لم يبلغ بل تحول إلى طرف ثالث. وبالتالي فإن دعم الخدمات الإلكترونية بتدابير تمكن من الاسترداد أو إدخال وسيط موثوق يعزز ثقة المستخدمين بالخدمات الإلكترونية، ويشجعهم على اتخاذ القرار باستثمار هذه الخدمات.

4- توفير الضمانات وتعزيز الثقة في حال الشروع في المعاملة

إن تصريح مقدم الخدمة بتوفير ضمانات مادية أو معنوية للمستخدم عند استخدامه الخدمات الإلكترونية يدعم عملية صنع القرار، حيث تساعد هذه الضمانات المستخدم على تفسير درجة المخاطرة التي يواجهها في المداولات الإلكترونية والنتيجة التي يتوقعها. وتدل الضمانات على نية مقدم الخدمة الوفاء بالتزاماته وعلى مدى موثوقيته. ولكي تكون الضمانات فعالة، يجب أن يحدد مقدم الخدمة بصراحة العناصر التي يمكن ضمانها في العمليات الإلكترونية وتلك التي لا يمكن ضمانها. أما العامل الآخر المهم فيتمثل في طريقة مناقشة الضمانات مع المستخدم النهائي وكيفية التقيد بها على شبكة الإنترنت. وهذا ما يدل على أن الأهمية لا تكمن في التكنولوجيا بحد ذاتها، بل في الطريقة التي تدار بها بحيث تؤثر على قبولها واعتمادها واستخدامها. كذلك، تجدر الإشارة إلى أهمية العلامة التجارية، فقيمتها ترتبط ارتباطاً شديداً بمدى تحقيقها توقعات المستهلكين وهي تولد بالتالي الثقة بها والولاء لها.

وتعمل الضمانات بطريقة مشابهة لعملية الاسترداد. فهي تشمل تعويض المخاطر المحتملة، والمساعدة على إدارة التوقعات، وتقديم أدلة على مدى صدق مقدم الخدمة عندما يعد بمساعدة المستخدم في اتخاذ قرارات مدروسة من خلال تعزيزها الثقة بالنتائج المتوقعة.

5- زيادة الشفافية بهدف تعزيز الثقة

لقد أثبتت الدراسات أن الإفراط في طلب بيانات شخصية في الخدمات الإلكترونية، وتخزين هذه البيانات إلكترونياً لدى مقدمي الخدمة، وخصوصاً في قواعد البيانات المركزية، يعزز الشكوك لدى المستخدمين ويشعرهم بأنهم أكثر عرضة للخطر. وهذا الشعور ناجم عن ضعف السيطرة على الأشخاص الذين يقومون بجمع المعلومات، أو الذين يستطيعون الحصول عليها وبالتالي استخدامها. وتتفاقم هذه المشكلة عندما يتعامل المستخدمون مع هذا الإفراط في طلب البيانات الشخصية بتزويد قواعد البيانات بمعلومات

خاطئة عن أنفسهم. وتعزز هذه العوامل إدراك مخاطر الأنشطة التي تعتمد على تكنولوجيا المعلومات والاتصالات، وتسلط الضوء على أهمية الثقة بين طرفي العلاقة.

وقد أظهرت الدراسة أن اعتماد الشفافية، وتوضيح أسباب طلب معلومات محددة من المستخدمين، وتحديد كيفية استخدام هذه البيانات كلها عوامل أساسية في تعزيز الثقة لدى هؤلاء المستخدمين. كما تبين أن تعزيز الشفافية وثقة المستخدمين يتم عبر معالجة المسائل المتعلقة بحماية بياناتهم الشخصية، وتوفير إمكانية نفاذهم إلى هذه البيانات والتحكم بها بأمان، أي تصحيحها وحتى إزالتها. وينبغي أن يتم هذا بالتزامن مع تقديم ضمانات قوية حول كيفية استخدام البيانات الشخصية وتخزينها والوصول إليها، مع إدراك مدى صعوبة توفير الضمانات عبر الحدود الدولية.

6- نشر السياسات الخاصة بتقديم الخدمات والحفاظ على المعلومات

من الواضح أن المستخدمين يترددون في قبول الشروط والأحكام التي يجب عليهم القبول بها للاستفادة من خدمة معينة متاحة عبر شبكة الإنترنت. فقد أظهرت النتائج أن العديد من الأشخاص يمتنعون عن الاشتراك في خدمات الإنترنت بسبب عدم موافقتهم على الشروط والأحكام الخاصة بها. ويمكن تحقيق الانفتاح المرجو من خلال نشر السياسة المتبعة في تقديم الخدمة والحفاظ على المعلومات الشخصية، وعبر إتاحة إمكانية التجربة والاسترداد وتقديم الضمانات. فجميع هذه الإجراءات تساهم في تحقيق الانفتاح وفي بناء ثقة المستخدمين. ولكن من المهم أيضاً أن يكون مقدمو الخدمة صادقين، وأن يقدموا ضمانات يستطيعون الإلتزام بها لاحقاً.

الإطار 8- أمثلة للحفاظ على الخصوصية في المواقع الإلكترونية

من المؤكد أن نشر سياسة الموقع بشأن الخصوصية، وتوضيح شروط استخدام المواقع الإلكترونية يزيد من ثقة المستخدمين بهذه المواقع. فمن أجل كسب هذه الثقة، تنشر معظم مواقع التجارة الإلكترونية العالمية المعروفة مثل Amazon.com وHotels.com، وكذلك تلك التي انطلقت من العالم العربي مثل tejari.com، السياسة التي تعتمدها للحفاظ على الخصوصية، وتبين شروط استخدامها والتفاعل معها.

ويبين إشعار الخصوصية المنشور عبر موقع Amazon.com المعلومات التي يجمعها الموقع من المستخدمين. وهذه المعلومات نوعان: معلومات يدخلها المستخدم بذاته (كالإسم والعنوان البريدي والعنوان الإلكتروني)؛ ومعلومات يستنتجها الموقع آلياً من حاسوب المستخدم مثل عنوان بروتوكول الإنترنت IP، ونسخة عن نظام الاستثمار على حاسوبه. كما يبين إشعار الخصوصية كيفية استخدام الموقع للمعلومات الخاصة بالمستخدمين من أجل التفاعل معه، أو لإجراء إحصاءات عامة، أو من أجل تحديد ملامح المستخدم. ويوضح إشعار الخصوصية كذلك الحالات التي يستثمر فيها طرف ثالث معلومات الموقع، أكان هذا الطرف مزود خدمة، أم مصرفاً وسيطاً للدفع الإلكتروني، أم جهات أخرى. ويحدد الإشعار المذكور نوع المعلومات المسموح لهذه الأطراف باستثمارها.

ويوضح إشعار الخصوصية في موقع Amazon.com أيضاً الآليات والبرامج المعتمدة في الموقع لحماية المعلومات الشخصية للمستخدمين. ويبين كذلك الخيارات المتاحة للتفاعل مع الموقع بهدف تعديل البيانات الشخصية أو بيان المجالات والمواضيع الهامة.

ويتضمن موقع hotels.com بياناً للخصوصية يشبه من حيث مضمونه، إلى حد ما، مضمون إشعار الخصوصية في موقع Amazon.com ولكنه أبسط منه.

وتجدر الإشارة إلى أن شروط استخدام هذه المواقع تبين الحالات التي يمكن فيها إلغاء عملية الشراء أو البيع، والرسوم المترتبة على تلك العملية، وكيفية استرداد المبالغ المقتطعة.

المصدر: www.amazon.com, www.hotels.com, www.tejari.com.

سابعاً- التوصيات

لقد أثبتت الدراسات والوقائع والأرقام أن بناء مجتمع المعلومات، والانتقال إلى أسلوب العمل الإلكتروني يعودان على أبناء المجتمع بالنمو والازدهار والمعرفة، ويساهمان في نمو البلدان والمجتمعات على الصعد الاقتصادية والاجتماعية والثقافية. وبوجود هذه المنافع، يتحول المجتمع نحو بيئة العمل الرقمي، مع التنبه إلى المخاطر المعلوماتية، ومحاولة خلق بيئة رقمية محصنة وآمنة وموثوقة يطمئن إليها الأفراد وأصحاب الأعمال. ومن هنا تأتي أهمية هذا التقرير، الموجه خصوصاً إلى الجهات المعنية ببناء مجتمع المعلومات وتطويره في المنطقة العربية.

وقد أشار هذا التقرير إلى الأبعاد الأساسية في أمن استخدامات تكنولوجيا المعلومات والاتصالات، ولا سيما الخدمات الإلكترونية، وإلى بناء الثقة بها. كما أوضح الإشكاليات الفنية والقانونية والتطبيقية التي تواجهها البيئة الرقمية بأسرها. فالجهات المعنية كلها، من بلدان ومؤسسات وأفراد، تواجه التهديدات المعلوماتية ذاتها، وإن اختلفت أساليب الوقاية التي تعتمدها في مواجهتها. فليس بالإمكان توفير حماية مطلقة لأمن مجتمع المعلومات الرقمي، وإنما يمكن تخفيف أثر الأخطار المحتملة إلى حدٍ بعيد.

ويبين التقرير أن موضوع أمن استخدام تكنولوجيا المعلومات والاتصالات وبناء الثقة بها يختلف عن غيره من المواضيع المتعلقة ببناء مجتمع المعلومات، نظراً إلى ارتباطه بجميع أصحاب المصلحة والشركاء في هذا المجتمع وتأثره بهم. فكل جهة معنية باتخاذ القرار، أو بتشغيل البنى الأساسية، أو بتطوير البرمجيات أو بتشغيلها أو باستثمارها، تتأثر بشكل أو بآخر بضمان أمن الخدمات الإلكترونية وبناء الثقة بها.

وتلخص هذه التوصيات الإطار الوطني العام لضمان أمن استخدام تكنولوجيا المعلومات والاتصالات وتعزيز الثقة بها. كما توضح المواضيع الأساسية التي يجب أن يعالجها هذا الإطار، وتشير إلى المهام الأساسية الملقاة على عاتق أصحاب المصلحة والشركاء في مجتمع المعلومات.

(أ) إن وضع إطار وطني عام لبناء الثقة بمجتمع المعلومات وتعزيز أمنه هام لخلق بيئة رقمية موثوقة وآمنة، وللتشجيع على استخدام وتطوير التطبيقات والخدمات الإلكترونية في مختلف نواحي الأنشطة الإدارية، والحكومية، والعملية، والتجارية، والثقافية، والتعليمية؛

(ب) إن وضع استراتيجية وطنية لضمان أمن استخدام تكنولوجيا المعلومات والاتصالات وتعزيز الثقة بها ضروري لتحديد الأهداف الوطنية في هذا المجال، وتحديد المحاور الأساسية التي تعنى بها الدولة على المستوى الوطني، وكذلك لبيان الأولويات وتحديد مسؤوليات مختلف أصحاب المصلحة وشرح آليات التنفيذ. كما تتمثل ضرورته في توضيح تقاطع الاستراتيجية مع الاستراتيجيات التنموية الأخرى، ومع الاتفاقيات والمعاهدات الدولية؛

(ج) وفي ما يلي أبرز المحاور التي ينبغي معالجتها ضمن الاستراتيجية الوطنية، أو الإطار الوطني العام:

(1) تحديد البنى الأساسية في الدولة التي يعتمد تشغيلها على تكنولوجيا المعلومات والاتصالات، ووضع خطط عملية كفيلة بحماية هذه البنى من المخاطر المعلوماتية؛

(2) وضع خطط عمل مرنة وقابلة للتحديث من أجل حماية البنى الأساسية، والنظم والتطبيقات والخدمات المعلوماتية في مؤسسات القطاع العام، وشركات القطاع الخاص (وخصوصاً المؤسسات أو الشركات التي تقدم خدمات الإنترنت، ومراكز المعلومات). وباعتماد هذا النوع من الخطط، يمكن حماية هذه المكونات من الأخطار الخارجية وبناء ثقة الأفراد وأصحاب الأعمال بهذه الخدمات؛

(3) وضع إطار تنظيمي لحماية أمن الفضاء السيبراني في ضوء التجارب الدولية، وإنشاء نظام وطني لتعزيز أمن الفضاء السيبراني وحماية الخدمات الإلكترونية. وكذلك تحديد جهة مركزية (أو إنشاء فرق عمل أو مركز أو مؤسسة وطنية) تنسق الجهود المبذولة على المستوى الوطني لبناء الثقة بالخدمات الإلكترونية وضمان أمنها. ويجب أن تعتمد هذه الجهة أحدث الحلول التكنولوجية، وأن تتبع المعايير الدولية في مجال تعزيز أمن الفضاء السيبراني والثقة به، وأن تشكل مرجعاً وطنياً في جميع الشؤون الفنية ذات الصلة؛

(4) تحديث الإطار القانوني بما يتلاءم مع احتياجات البيئة الرقمية وتطبيقاتها، أي وضع التشريعات السيبرانية ولوائحها التنفيذية، واتخاذ الإجراءات اللازمة لتطبيق هذه القوانين على المستوى الوطني، بما فيها تدريب القضاة والمحامين على تطبيق التشريعات السيبرانية. وأما أبرز المحاور التي تدخل في حماية البيئة الرقمية وضمان أمنها والثقة بها فهي حماية الخصوصية والبيانات الشخصية، والتصدي للجرائم السيبرانية، وحماية الملكية الفكرية وحماية المستهلك؛

(5) تشجيع القطاعين العام والخاص على التعاون من أجل حماية الشبكات والنظم المعلوماتية الوطنية والفضاء السيبراني وضمان أمنها. فغالباً ما يكون القطاع الخاص سباقاً في استثمار التكنولوجيا الحديثة، وامتلاك أدواتها، ومعرفة طرق تشغيلها. وأما القطاع العام، وبحكم مسؤوليته عن العديد من البنى الأساسية الحساسة في الدولة، وخصوصاً في منطقة الإسكوا، فعليه أن يتعاون مع القطاع الخاص للاستفادة من خبراته ومهاراته ومرونته في التعامل. ومن جهة أخرى، ونظراً إلى افتقار العديد من مؤسسات القطاع العام إلى الخبرات التكنولوجية العالية، يحبذ إنشاء شراكات بين مؤسسات القطاعين العام والخاص، أو إبرام عقود بينها لحماية البنى الأساسية ونظم المعلومات في مؤسسات القطاع العام وضمان أمنها؛

(6) إطلاق برامج توعية عامة حول أهمية ضمان أمن الخدمات الإلكترونية وتعزيز ثقة أصحاب القرار بها، وأخرى خاصة بالعاملين في القطاع العام وأصحاب الأعمال والأفراد والأسر والأطفال حول آليات الحماية في البيئة الرقمية، وأساليب التفاعل الآمن مع الفضاء السيبراني وتطبيقاته وخدماته، واستخدام جميع وسائل الاتصال الممكنة للقيام بحملات التوعية هذه؛

(7) تشجيع أنشطة البحث والتطوير القائمة على برمجيات المصدر المفتوح في مجال حماية تكنولوجيا المعلومات والاتصالات وضمان أمنها، وبناء الثقة بالخدمات الإلكترونية في الجامعات ومراكز البحوث الوطنية، والتشجيع على إيجاد حلول تقنية موثوقة لحماية البنى الأساسية الحساسة في الدولة، والبنى والنظم والتطبيقات داخل المؤسسات؛

(8) توجيه الجامعات نحو إعداد متخصصين في مجال أمن الفضاء السيبراني وحمايته، وفي وضع تطبيقات معلوماتية آمنة، وإطلاق برامج تدريبية متخصصة لطلاب الجامعات والعاملين في القطاعين العام والخاص الذين يشرفون على تشغيل النظم المعلوماتية وحمايتها وضمان أمنها بهدف كسب ثقة المستخدمين، من أفراد وأصحاب أعمال ومواطنين، بالنظم المعلوماتية؛

(د) إن التعاون الدولي هام جداً في مجال ضمان أمن الفضاء السيبراني وحمايته وعلى صعيد بناء الثقة بالخدمات الإلكترونية، نظراً إلى الطبيعة الكونية التي تتميز بها البيئة الرقمية. ويتجلى التعاون الدولي في تبادل المعلومات حول الأخطار الخارجية وكيفية مواجهتها على المستوى القانوني حيث يستعان بالاتفاقيات والمعاهدات الدولية أو الإقليمية في مجال التشريعات السيبرانية من أجل وضع التشريعات السيبرانية المحلية، والإلتزام بها إذا كان ذلك ملائماً. وتجدر الإشارة إلى أن تبادل التجارب الناجحة والآليات بين البلدان، ولا سيما تلك المتشابهة من حيث نظمها الإدارية والقانونية، له أثر إيجابي؛

(•) إن لتبادل المعلومات حول الأخطار المعلوماتية وحول طرق مجابهتها بين المؤسسات والشركات على المستوى الوطني أهمية كبيرة لمجابهة الأخطار الخارجية. كذلك، من المفيد تحديد إحدى الجهات في الدولة كي تؤدي دور المنسق في مجال تبادل المعلومات حول أمن تكنولوجيا المعلومات والاتصالات وحمايتها؛

(و) إن توفير خدمات إلكترونية موثوقة يتطلب اعتماد منهجيات مستحدثة تيسر تقديم الخدمات إلى المستخدمين إلكترونياً، وتأتيهم بقيمة مضافة جديدة. ومن المجدي وضع توجيهات حول كيفية تطوير تطبيقات وخدمات إلكترونية آمنة ومحصنة ضد الأخطار الخارجية، وحول الخصائص الضرورية لهذه التطبيقات بغية كسب ثقة المستثمر النهائي وطمأنته، وحول الشروط الفنية لتشغيل هذه الخدمات وطريقة تعامل الأفراد المسؤولين عن تشغيلها بما يحفظ خصوصية البيانات الشخصية.

ويتطلب العمل على المحاور السابقة تعاوناً بين مختلف أصحاب المصلحة والشركاء في مجتمع المعلومات، كما بينت الدراسات والتوجيهات الدولية والإقليمية والتجارب الناجحة في البلدان. وفيما يلي الأدوار التي ينبغي أن يؤديها أصحاب المصلحة الأساسيون في تحقيق الاستراتيجية الوطنية أو الإطار الوطني لبناء الثقة بالخدمات الإلكترونية وضمان أمن البيئة الرقمية وحمايتها.

ويتمثل دور الدولة في ما يلي:

(أ) وضع الإطار الوطني العام لضمان أمن الفضاء السيبراني وحمايته، ولبناء الثقة بالخدمات الإلكترونية، والعمل على تنفيذ هذا الإطار وتطبيقه؛

(ب) تحديث الإطار التشريعي بما يتلاءم مع احتياجات استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها، ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية، وذلك بالتعاون مع الجهات المعنية وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، والاسترشاد بالخبرات والتجارب والمبادرات الدولية ذات الصلة من أجل صياغة اللوائح التنفيذية التشريعية لمواجهة الجرائم المعاصرة؛

(ج) التحفيز على التعاون مع البلدان الصديقة والمنظمات الدولية ذات الصلة لتبادل الخبرات ودعم الخدمات الإلكترونية وتنميتها، ولمكافحة الجرائم السيبرانية التي لا تعترف بالحدود الجغرافية أو السياسية؛

(د) وضع وتنفيذ خطط وحملات لتوعية المجتمع حول الفرص والمزايا التي تقدمها الخدمات الإلكترونية للأفراد والمؤسسات، وحول أهمية ضمان أمن هذه الخدمات وحمايتها من المخاطر والتحديات التي قد تواجهها؛ ويفترض بهذه الخطط والحملات أن تشمل مختلف القطاعات وشرائح المجتمع على اختلاف مستوياتها، لأن تحقيق النجاح المنشود في التحول نحو استعمال الخدمات الإلكترونية يحتاج إلى ثقة المجتمع وتكاتفه.

أما الدور الذي يؤديه القطاع الخاص فيتمثل بشكل أساسي في الاضطلاع بالمهام التالية:

(أ) استحداث خدمات إلكترونية ذات كفاءة عالية بالاعتماد على تكنولوجيا المعلومات والاتصالات، وتقديم خدمات جديدة تتيحها هذه التكنولوجيا مع أخذ مستلزمات جذب المستخدمين النهائيين، وضمان ثقتهم بعين الاعتبار، وذلك من خلال الخدمات الإلكترونية التي يقدمها هذا القطاع مباشرة إلى المواطنين، أو من خلال تطوير تطبيقات الخدمات الإلكترونية؛

(ب) تقييم التكنولوجيات الجديدة واعتمادها على المستوى الوطني، والمساهمة في تقييم الأخطار المعلوماتية المتجددة وفي إيجاد الحلول الفنية والتنظيمية لمواجهتها، وتشجيع أنشطة البحث والتطوير في مجال ضمان أمن تكنولوجيا المعلومات والاتصالات وحمايتها؛

(ج) التعاون مع القطاع العام في ضمان أمن الشبكات والنظم الحاسوبية والتطبيقات على المستويين الوطني والمؤسسي وحمايتها، وتبادل المعلومات والتجارب الناجحة حول الأخطار وأساليب مواجهتها؛

(د) إدراج منظومات آمنة وموثوقة لتكنولوجيا المعلومات والاتصالات وتطبيقاتها في جميع المشاريع التي يقدمها هذا القطاع إلى المجتمع.

وتؤدي المنظمات غير الحكومية دوراً في نشر ثقافة أمن الفضاء السيبراني وتعزيز ثقة المواطنين بالتطبيقات والخدمات الإلكترونية عبر مشاركتها الفعالة في تنفيذ حملات التوعية في هذا المجال.

وأما دور المستخدم النهائي فيتمثل في ما يلي:

(أ) الإلتزام بالتوصيات المتعلقة بضبط الأمن في مجال استخدام تكنولوجيا المعلومات والاتصالات، وتنفيذ أساليب الحماية الفنية، والتعامل بأخلاقية ومسؤولية في الفضاء السيبراني؛

(ب) المشاركة في ورش التوعية وندوات التدريب التي تتناول آليات ضمان الأمن في استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها بهدف تكوين المعرفة في هذا الموضوع أو تطويرها وتحديثها وفقاً للمستجدات التكنولوجية.

المرفق

واقع التشريعات السيبرانية في المنطقة العربية حتى نهاية عام 2008

تضمنت الدراسة التي قامت بها الإسكوا في عام 2007 حول نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا مسحاً لكافة التشريعات ذات الصلة بتكنولوجيا المعلومات في مختلف فروع هذا القانون (وقد أدخلت عليه بعض التعديلات منذ تاريخ انتهاء هذه الدراسة). وقد أظهرت الدراسة قصوراً واضحاً وعدم كفاءة عدد من هذه التشريعات بعد انقضاء سنوات على سنها.

وفي ضوء هذه الدراسة والأبحاث المتخصصة المنجزة في مختلف فروع هذا الحقل، يمكن تلخيص أبرز الإنجازات وأوجه القصور والنقص، في الواقع العربي عموماً وفي منطقة الإسكوا خصوصاً، بالموجز الوارد في الجدولين الأول والثاني، كالتالي:

الجدول الأول: حول واقع الأداء التشريعي العربي في المسائل التالية:

(1) الحق في الوصول إلى المعلومات (الحقوق في البيئة الرقمية).

(2) الخصوصية وحماية البيانات الشخصية.

(3) جرائم الحاسوب أو الجرائم الإلكترونية (الجرائم السيبرانية) من الناحيتين الموضوعية (نصوص التجريم) والإجرائية (قواعد الأصول الجزائية أو الإجراءات المتعلقة بالجرائم).

(4) الملكية الفكرية للمصنفات الرقمية.

(5) المعايير الفنية ومعايير الأداء في الخدمات الإلكترونية (بما فيها التشفير وأمن المعلومات).

(6) حماية المستهلك الرقمي (التي قد تشمل في بعض مواضيعها تشريعات المعايير الفنية من خلال تنظيم مسؤوليات مزودي الخدمات والجهات الوسيطة، وقد تكون منفصلة عنها).

الجدول الثاني: حول واقع الأداء التشريعي العربي في مسائل العمليات الإلكترونية بمختلف تطبيقاتها:

(7) المداولات والتجارة الإلكترونية.
(8) المصارف الإلكترونية.
(9) المضاربات المالية الإلكترونية (البورصات الخارجية).
(10) الحكومة الإلكترونية.

تتعلق مواضيع الجدول الأول بكافة أوجه التطبيقات والأنشطة الإلكترونية، الفردية منها أو المؤسسية، في القطاعين العام والخاص، المتصلة وغير المتصلة بالأعمال، وفي مقدمتها الخدمات الإلكترونية. وتجدر الإشارة إلى أن مسألة أمن المعلومات الفنية غير مدرجة ضمن مسائل جرائم الحاسوب التي تتعلق بالنظام القانوني للجريمة لا للخدمة، بل أُدرجت ضمن المعايير الفنية للتعامل مع المعلومات وخدماتها.

وأما الجدول الثاني فيبحث في تطبيقات العمليات الإلكترونية، ويتناول ضمن الموضوع الأول والمعنون "المداولات والتجارة الإلكترونية" التعليم الإلكتروني والصحة الإلكترونية والتوظيف الإلكتروني والنشر الإلكتروني والتسويق الإلكتروني وغيرها. وأما المصارف الإلكترونية، والنشاط المالي الإلكتروني الخاص بمضاربات البورصة والمزادات الإلكترونية، والحكومة الإلكترونية، فقد فصلت عن المداولات الإلكترونية لأن كل تطبيق من هذه التطبيقات ينفرد بمميزات تحتاج إلى مسائل تشريعية مستقلة عن سائر العمليات الإلكترونية. غير أن جميع التطبيقات في الجدول الثاني تقع ضمن نطاق المفهوم الشامل والواسع للعمليات الإلكترونية. وتجدر الإشارة إلى أن موضوع المشتريات الحكومية قد أُدرج ضمن تطبيق الحكومة الإلكترونية لأنه يتعلق بعمليات تكون فيها الحكومة طرفاً. ويشكل الاختصاص القضائي والقانون الواجب تطبيقه أحد المواضيع

القانونية ذات الصلة بالعلاقات الإلكترونية وجميع تطبيقاتها. ولذلك، كان الاتجاه الدولي والوطني نحو إدراج النصوص الخاصة به ضمن قوانين التجارة الإلكترونية.

الجدول 1- الإنجازات ومواطن القصور والنقص في تشريعات البيئة الرقمية والخدمات الإلكترونية في العالم العربي

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
(1) الحق في الوصول إلى المعلومات	1- أنشئت في جميع البلدان العربية مراكز وطنية أو قومية للمعلومات، وهي تتباين من حيث استقلاليتها والجهات المرتبطة بها. كما أنشئت هيئات أخرى معنية بالمعلومات والوثائق كالأرشيف الوطني والمكتبة الوطنية وغيرها. وبعد تكريس مسألة الوصول إلى المعلومات كحق من حقوق الإنسان، وجب تكريس الحق في الوصول إلى السجلات الحكومية والعامة والحق في طلب مختلف أنواع المعلومات، عدا تلك المتعلقة بالأمن القومي والمصنفة كمعلومات ووثائق سرية. ومع تنامي نظم المعلومات ونشوء الشبكات، أصبح لزاماً تنظيم هذا الحق وتكريسه، وتنظيم آليات تتعلق بحصول المواطن على المعلومات. 2- وضع الأردن مؤخراً تشريعاً خاصاً نص على إنشاء مجلس للمعلومات ونظم الحق في تقديم طلبات للحصول عليها. غير أن هذا التشريع لم يحقق الهدف الرئيس منه، حيث أُسندت رئاسة المجلس إلى ممثل جهة حكومية (وهي دائرة المكتبة الوطنية التابعة لوزارة الثقافة)، ومعها مهمة الإشراف على الجهاز التنفيذي. فمثل هذا التشريع يستمد قوته وفعاليته من استقلالية الهيئة المناط بها رعاية هذا الحق وحياديتها. فأساس وجوده هو الحد من سيطرة الحكومات على مصادر المعلومات، وليس بالتالي من الملائم إسناد قيادة المجلس ومهامه إلى جهات حكومية بالرغم من أن التشريع نص على استقلال عملها. 3- وباستثناء هذا التدخل الرسمي، وبعض النصوص المتناثرة في التشريعات المعنية بالوصول إلى السجلات الحكومية وقوانين جهات الإحصاء، وفي ما خلا بعض القواعد الخاصة التي لا تتلاءم مع البيئة الرقمية، في تونس تحديداً، لا تتوفر تشريعات عربية في هذا الحقل. 4- وتجدر الإشارة إلى أن الحق في الوصول إلى المعلومات يعتبر في الظاهر حقاً متناقضاً مع الحق في الخصوصية أو معاكساً له، في حين أن الأخير يعتبر استثناء عليه. كذلك يحظر الحق في الوصول إلى المعلومات الحصول على أسرار الأمن القومي، والمساس بالبيانات الخاصة خارج نطاق المعايير التي تحمي هذا الحق.
(2) الخصوصية وحماية البيانات الشخصية	1- وعلى المستوى العربي، نجحت تونس في سن القانون رقم 63 لسنة 2004 حول الخصوصية وحماية البيانات الشخصية. 2- ووضعت إمارة دبي تشريعاً لحماية البيانات الشخصية (القانون رقم 1 لسنة 2007)، وهو شامل من حيث محتواه وقواعده، إلا أنه خاص بمركز دبي المالي العالمي دون سواه. 3- ويحتوي قانون المداولات الإلكترونية رقم 2008/69 على نصوص محدودة في حقل حماية البيانات الشخصية (الفصل السابع)، وهو لا يشمل جميع المبادئ الموضوعية والقواعد الإجرائية الخاصة بحماية البيانات الشخصية المختلفة، وينحصر نطاق عمله بالتزامات مزودي خدمات التصديق وبالمداولات الإلكترونية فقط. 4- وباستثناء ما تقدم، تعاني البيئة العربية من قصور عام في هذا الحقل، وهو انعدام التشريعات الشاملة وعدم كفاية بعض النصوص المتناثرة في التشريعات القائمة لتغطية

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	المحاور المتعلقة بحماية الخصوصية ومواضيعها على نحو يحقق الثقة بالتكنولوجيا عموماً، وبالخدمات الإلكترونية خصوصاً.
(3) جرائم الحاسوب موضوعياً وإجرائياً	1- وضعت الإمارات العربية المتحدة والمملكة العربية السعودية نظام الجرائم المعلوماتية، ووضعت تونس تشريعات خاصة بجرائم الحاسوب من الناحية الموضوعية (نصوص التجريم). وقامت عمان بتعديل قانون الجزاء كي يتضمن بعضاً من أشكال جرائم الحاسوب، وخصوصاً إساءة استخدام بطاقات الائتمان. وفي الأردن والجزائر، وغيرهما من البلدان العربية، سنّت مشاريع قوانين بهذا الشأن. 2- ونصت تشريعات المداولات الإلكترونية في الأردن والبحرين ودبي وعمان على تجريم بعض صور الجرائم في البيئة الرقمية، لكن أياً منها لا يَعد تشريعاً شاملاً يكفي لتغطية هذا الحقل من حقول قانون تكنولوجيا المعلومات. 3- ولم يعمد أي من البلدان العربية إلى تطوير تشريعات الإجراءات الجنائية بالشكل الذي يتناسب مع الجرائم الإلكترونية وتحدياتها في مجالات ضبط الأدلة، والتفتيش، والاختصاص، وغيرها من المسائل الإجرائية الناشئة عن هذه الأنماط الجديدة من الجرائم، رغم أن غالبية هذه البلدان أفردت أقساماً خاصة ضمن أجهزة الضابطة العدلية أو الضابطة القضائية (أجهزة الشرطة). وتتولى هذه الأقسام أنشطة الاستدلال بشأن الجرائم الإلكترونية، لكن التجارب متفاوتة من حيث فعاليتها وجديتها وتميزها. ولعل أقدم هذه الأقسام قسم جرائم الحاسوب التابع للأدلة الجرمية في الأمن العام الأردني. ولكن عمل هذه الأجهزة لا يتعدى كونه عملاً إدارياً في غياب غطاء تشريعي، ومن دون تطوير نصوص الإجراءات الجنائية، وهو لا يحقق الغرض المأمول في خدمة جهاز العدالة بفعالية لمكافحة هذه الجرائم. 4- ونظمت في البلدان العربية برامج تدريب وتأهيل عديدة حول الأمن والإجرام المعلوماتي (أكثرها في منطقة الإسكوا)، لكن نتائجها ليست كافية. فهي تفتقر كلها إلى الطابع المؤسسي، وكذلك إلى البعد التطبيقي العملي في غالبيتها. كما يتحسس المتدربون عدم فعالية محتواها في غياب مرجعيات العمل، وفي مقدمتها الأدوات التشريعية التي تحسم الجدل النظري حول هذا الموضوع، وعدم تنفيذ توصيات ورش العمل والأنشطة العلمية والتدريبية. 5- ويعد القصور في وضع تشريعات الجرائم الإلكترونية (الموضوعية والإجرائية) الأوضح من بين مواطن القصور في قانون تكنولوجيا المعلومات، مع أن مئات التوصيات قد صدرت عربياً بهذا الشأن منذ ما يقارب 15 سنة. وتواجه البيئة العربية أكثر فأكثر المخاطر وحالات الاعتداء والمنازعات الفعلية التي أحيلت إلى القضاء من دون غطاء تشريعي، وذلك بالرغم من أهمية هذا الغطاء في خلق الثقة والشعور بالأمن، وكلاهما يشجعان على تقبل البيئة الرقمية والتعامل معها.
(4) الملكية الفكرية للمصنفات الرقمية	1- قررت غالبية البلدان العربية، بما فيها جميع بلدان الإسكوا، أن تدرج ضمن قوانين حماية حق المؤلف حماية برامج الحاسوب وحماية قواعد البيانات (حماية التبويب والبناء وليس المحتوى)، بوصفها مصنفات أدبية مسايرة لمنهج القانون النموذجي لحماية برامج الحاسوب الذي وضعه خبراء المنظمة العالمية للملكية الفكرية في عام 1978. 2- وقرر كل من الأردن وتونس وعمان ومصر حماية تصاميم أو طوبوغرافيا الدوائر المتكاملة. وقد وضعت هذه البلدان، وبلدان أخرى في الخليج، إطاراً قانونياً بشأن المنافسة

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	غير المشروعة والأسرار التجارية. 3- وباستثناء الأردن، لم يقم أي من البلدان العربية بإقرار أي قواعد في نطاق تشريعات حماية حق المؤلف لجهة حماية التدابير التكنولوجية الفعالة والبيانات الإلكترونية المتعلقة بإدارة الحقوق، علماً أنهما من المسائل التي تضمنتها اتفاقية المنظمة العالمية للملكية الفكرية في شأن حق المؤلف التي اعتُمدت في عام 1996، والمعروفة باتفاقية الحقوق الرقمية (مع أنها لم تغط سائر الحقوق الرقمية). 4- كما طورت بعض التشريعات الجمركية، أو استخدمت كمصدر لإقرار تعليمات ونظم بشأن التدابير الجمركية لحماية الملكية الفكرية (وتعليمات الجمارك الأردنية هي أبرز مثال على ذلك). وساهمت هيئات الجمارك في أنشطة وحملات ملاحقة النسخ المقرصنة من البرمجيات والمصنفات الموسيقية والأفلام. 5- ونظم عدد من بلدان غربي آسيا حملات لملاحقة المصنفات المقرصنة، كان أبرزها في الأردن ودبي والمملكة العربية السعودية، ولكن الجهد الأكبر انصب في ملاحقة المصنفات الموسيقية والأفلام. وفي إطار الجهود الإدارية الرامية إلى إنفاذ حقوق الملكية الفكرية، أنشئت أقسام متخصصة في بعض أجهزة الشرطة العربية لتولي مخالفات الملكية الفكرية. 6- وأما فيما يتعلق بالمصنفات الرقمية فتتولى هيئات مراقبة الإعلام المرئي والمسموع (التي تقع بغالبيتها ضمن ملاك وزارات ومجالس الإعلام أو الثقافة، وليس الاتصالات وتكنولوجيا المعلومات) مهام إجازة عرض المصنفات (الأقراص المدمجة على أنواعها). وتجدر الإشارة إلى أن مصنفات الألعاب الإلكترونية التي تسوق كأقراص مدمجة هي من ضمن برامج الحاسوب لا المصنفات الموسيقية. 7- وترتبط إجازة النشر، بما فيه محتوى النشر الإلكتروني، بدوائر المطبوعات والصحافة والنشر التي تتبع غالباً وزارات الثقافة، أو تتبع وزارات الإعلام بالنسبة إلى النشاط الصحفي. 8- وفي جميع بلدان غربي آسيا نظم إدارية ومراكز وطنية أو قومية للمعلومات تسند إليها مهام تسجيل أسماء النطاقات ضمن البناء التنظيمي لهيئات الاتصالات، أو هيئات تكنولوجيا المعلومات أو الهيئات التي تتولى شؤون القطاعين، لكنها جميعها لا تستند إلى تشريع كافٍ وشاملٍ بل إلى تعليمات وقرارات وزارية. 9- وفي البلدان العربية، ومنها بلدان غربي آسيا، أطر قانونية قديمة نسبياً لتسجيل براءات الاختراع والعلامات التجارية وحمايتها. وقد عدلت لمواكبة اتفاقية الجوانب التجارية لحقوق الملكية الفكرية في إطار متطلبات الانضمام إلى منظمة التجارة العالمية. وشملت هذه التعديلات حماية العلامات التجارية المشهورة (كما في الأردن)، وإقرار نظام لقمع المنافسة غير المشروعة في العلامات التجارية، وضوابط جديدة بشأن عدم تسجيل العلامات التي تعتبر ترجمتها إلى لغة أخرى اعتداء على علامة مسجلة أو مشهورة، وتوسيع نطاق الحماية في البراءات ليشمل طريقة الإنتاج والمنتج النهائي. 10- ولا يتضمن الإطار القانوني العربي عموماً أي نصوص تتعلق بحماية محتوى المواقع الإلكترونية والحلول التقنية على المواقع لأن التعامل مع المحتوى يتم على أساس اعتباره مفردات مستقلة عن بعضها. فالبرامج والمواد الأدبية أو الفنية مشمولة

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	بالتشريعات التي تحمي حق المؤلف. وأما استغلال براءة اختراع (صناعية) فيدرج ضمن حماية نظام براءات الاختراع، وتُدرج العلامات التجارية ضمن نظام العلامات التجارية وليس كشعارات مميزة للموقع، كما يدرج الاسم التجاري ضمن قوانين حماية الأسماء التجارية. 11- ويتمثل القصور الأبرز في عدم إقرار إطار قانوني موحد يواكب الموقف الدولي حول حماية أسماء النطاقات والعلاقة بين أسماء النطاقات والعلامات التجارية. كذلك لا تخضع جهات الاستضافة لتشريعات المعايير الفنية والتقنية ومسؤوليات الهيئات الوسيطة التي تندرج ضمن تشريعات التنظيم الإداري لمعايير الخدمة التقنية، وليس ضمن تشريعات الملكية الفكرية (أنظر الحكومة الإلكترونية). 12- ويجب إقرار نظام الحماية المتعلق بمعلومات إدارة الحقوق والتدابير التكنولوجية الفعالة في ظل اتساع النشر الإلكتروني، واعتماد النظم المؤتمتة لتبادل المعلومات والمصنفات الفنية. أما موضوع النشر الإلكتروني فيستعرض ضمن مواضيع الجدول الثاني نظراً إلى ارتباطه بالملكية الفكرية من حيث المحتوى، لأنه يمثل أحد أبرز تطبيقات العمليات الإلكترونية.
(5) المعايير التقنية وأمن المعلومات	1- تشمل هذه التدابير التشريعية القواعد الخاصة بتوحيد التدابير والحلول التقنية، وإدارة المعلومات المتبعة في مختلف النظم التقنية في القطاع الحكومي، وتلك الواجب توفرها لدى شركات تقديم الخدمات التقنية، كمزودي خدمات الإنترنت، وشركات الاتصالات وتبادل البيانات، وشركات استضافة المواقع الإلكترونية وتصميمها، وغيرها من شركات التكنولوجيا والاتصالات. وتشمل كذلك موضوع التشفير بوجه خاص من بين الحلول التقنية، وضوابطه واستخدامه ونقله وتبادله، وكذلك القواعد القياسية الخاصة بمعالجة المعلومات وحفظها ونقلها وتبادلها، بما فيها الضوابط والحلول المتصلة بأمن المعلومات في القطاعين العام والخاص. وتصبح هذه المعايير التقنية ذات أهمية قصوى حين يتعلق الأمر برخص تقديم الخدمات، كرخص تقديم خدمات التوثيق الإلكتروني أو توريد خدمة الإنترنت أو تراسل البيانات أو الاستضافة أو حتى خدمات الهواتف الخلوية والاتصالات على أنواعها، وإن كانت هذه لا تزال تخضع في العالم العربي لقوانين الاتصالات وللشروط العقدية لرخص تشغيلها، مثل خدمات البريد. ويمتد نطاق هذا القانون إلى مسؤوليات جهات تقديم الخدمة ومسؤوليات الجهات الوسيطة، وذلك في غياب تشريع خاص ينظم هذا المجال. فقد يكون هذا الموضوع مشمولاً بتشريعات حماية المستهلك أو التشريعات ذات العلاقة بترخيص العمل إذا كانت مستقلة، وإلا فإنه يدرج في القانون الخاص بالخدمات الإلكترونية. وفي هذا السياق، تجدر الإشارة إلى أن هذا التشريع يشمل تقديم خدمات الإنترنت إلى العموم عبر مقاهي ومراكز الإنترنت، فتأتي الواجبات والمسؤوليات المتصلة بهذا الجانب لتضاف إلى المعايير والمواصفات الخاصة بمحتوى الخدمة. وفي المقابل، تشمل بعض التشريعات الأخرى ضوابط المحتوى الرقمي الخاص بمواقع الإنترنت، وقواعد البيانات المفتوحة للجمهور. وتترك نظم أخرى هذا الأمر لتشريعات النشر أو لتشريعات جرائم المعلومات، حيث تجرم المحتوى الضار وتتطرق إلى معايير وضوابط المحتوى الرقمي. 2- ولا وجود لتشريعات (قوانين) شاملة في البيئة العربية بل عدد محدود من التعليمات الحكومية والقرارات الوزارية المتناثرة بخصوص ضوابط التعامل مع المعلومات، وقواعد البيانات في القطاع الحكومي أو في القطاع المصرفي، أو لدى الهيئات العامة وليس في سائر القطاعات. وهنا تكمن خطورة هذا التناثر في توزع الضوابط القانونية، لأن هذا

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	التشريع يهدف إلى ضبط التقنية ضمن معايير تلائم الاستراتيجيات الوطنية وأهدافها، وتشجع على التوجه نحو الخدمة الإلكترونية، وتيسر توظيف التكنولوجيا ومواردها، وتعزز نفاذ التشريعات الأخرى ذات العلاقة. ولكن هذا التباين بين الضوابط يؤدي إلى ظهور مشاكل تحول دون تحقيق جميع هذه الأهداف. 3- وحين اتجه الأردن إلى وضع قانون لتوظيف موارد التكنولوجيا، بدا وكأنه يسعى إلى وضع تشريع يشمل المواضيع المشار إليها في البند 1 أعلاه، ولكن الواقع كان غير ذلك. فقد تبين أنه مجرد إطار تنظيمي لعمل مركز المعلومات الوطني الذي أنشئ قبل إصدار هذا القانون. 4- ويمتد القصور في وضع هذه التشريعات الشاملة إلى البلدان العربية كافة. والمطلوب هو إما اتخاذ تدبير شامل على مستوى عمل قطاعات الدولة كافة، الحكومية منها والأهلية والخاصة، أو على الأقل ضبط اتجاهات القرارات والتعاميم والتعليمات القطاعية ومحتواها. وتجدر الإشارة إلى أن وجود تلك التعاميم والتعليمات والقرارات لا يغطي جميع المواضيع المذكورة سابقاً. 5- وفي البلدان التي كلفت وزارة واحدة بقطاع تكنولوجيا المعلومات والاتصالات، كما هو الحال في الأردن ومصر وغيرهما، يصبح هذا التشريع ضرورة ملحة في ظل الدور الذي تضطلع به هيئات تنظيم قطاع الاتصالات في تولي أنشطة ترخيص شركات الخدمات الإلكترونية وشركات الاتصالات، وفي ظل حالات التكامل والاندماج الحاصلة بين أنشطة هذه الشركات. 6- ويتمثل أحد أهم أسباب عدم تحقيق إنجاز على الصعيد القانوني في توزيع جهات الإشراف على قطاع تكنولوجيا المعلومات والاتصالات على جهات ووزارات وهيئات عديدة في البلدان العربية. فليس معروفاً ما إذا كانت تختص بمتابعته والعمل عليه مراكز المعلومات الوطنية أو القومية، أم وزارات الاتصالات، أم وزارات وهيئات التكنولوجيا، أم الوزارات التي تتولى الأمرين معاً، أم هيئات تنظيم الاتصالات حين تكون مستقلة عن وزارات الاتصالات، أم الجهات التي تحتكر تشغيل الخدمة، أم وزارات الثقافة، أم الإعلام، أم غيرها. واللافت هو التداخل في كثير من المسائل ذات الارتباط بين وزارات الاتصالات والإعلام والثقافة، وتفشيه في معظم بلدان غربي آسيا. ففي الأردن مثلاً، تشرف وزارة الثقافة على دائرة المكتبة الوطنية التي تشرف بدورها على مجلس المعلومات، تليها دائرة المطبوعات التي تشرف على النشر بأنواعه. وتؤدي وزارة الاتصالات وتكنولوجيا المعلومات دوراً إشرافياً. أما مركز المعلومات الوطني، وهو الذراع الأساسي في توظيف موارد التكنولوجيا وفقاً للقانون الذي يحمل المسمى نفسه، فهو مستقل، ويضطلع بنشاط مشترك مع الجمعية العلمية الملكية غير التابعة لأي جهة. وأما المجلس الأعلى للإعلام، فمسؤول عن الإعلام المرئي والمسموع ومصنفاته وإجازته، وعن إجازة البث الفضائي والإذاعي، بما في ذلك المستخدم عبر الإنترنت. ويتجه الأردن نحو دمج نشاطه مع وزارة الاتصالات وتكنولوجيا المعلومات عبر تعديل تشريعي مقترح، وإن كان ذلك لا يحل مشكلة التداخل الحاصل بينهما وبين وزارة الثقافة. وأما هيئة تنظيم قطاع الاتصالات فهي الجهة المستقلة المعنية بمنح رخص الاتصالات والخدمات الإلكترونية الخاصة بالبيانات على أنواعها. وتنشأ بين هذه الأطر وبين المشغلين الأساسيين في قطاعي الاتصالات والبريد تداخلات يصعب حصرها في هذا المقام، لكنها مثال واضح على الخلل الناجم عن تشتت جهات الإشراف المعنية بالخدمات الإلكترونية وإدارة المعلومات في البلد إلى درجةٍ يصعب معها تحديد الجهة المسؤولة عن توحيد معايير التقنية، وأمن المعلومات، وأدوات قياسها.

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
(6) حماية المستهلك الرقمي	1- ورغم كثرة الدعوات إلى حماية المستهلك في البيئة الرقمية، لا وجود لتشريع عربي في هذا الحقل حتى الآن. 2- ويشمل هذا التشريع عدة عناصر، أهمها مسؤوليات الجهات التي تقدم الخدمات الإلكترونية على أنواعها، والجهات الرئيسة والوسيطة المسؤولة عن أي خلل في مستوى الخدمة وعن أنشطة التسويق والإعلام المخادع. وحتى إذا أُدرج هذا الموضوع ضمن تشريعات المعايير التقنية ومعايير الأداء في الخدمات الإلكترونية على أنواعها، يظل تنظيم قواعد حماية المستهلك ضرورياً لأن الاعتداء على حقوقه في البيئة الرقمية ليس من ضمن مسؤوليات مقدمي الخدمات الإلكترونية أو الجهات المعنية بإدارة المواقع الإلكترونية وإنشائها وحسب، بل يندرج أيضاً ضمن مسؤولية جهات إيصال المنتجات المتعاقد عليها، وجهات التسويق وإرسال الرسائل الاقتحامية، أو جهات الاعتداء على الخصوصية وغيرها. 3- ولا يشتمل الإطار القانوني في غالبية البلدان العربية حتى الآن على قانون يحمي المستهلك في البيئة العادية وليس الرقمية. ففي الأردن، لم يصدر حتى الآن مثل هذا القانون مع أن إعداده وتقديمه قد أُنجز منذ فترة غير قصيرة. وفي الجمهورية العربية السورية، أدرج هذا القانون ضمن اَلتشريعات الحديثة. ولكنه، على حداثته، لم يراع حقوق المستهلك في البيئة الرقمية، حتى وإن كانت قواعده العامة لا تتضمن ما يحول دون تغطية الأخطار التي يتعرض لها المستهلك في هذه البيئة. 4- وشكلت حماية المستهلك في الأطر القانونية الأجنبية، وتحديداً الأوروبية، المحرك الرئيس لاتجاهات الأحكام القضائية في ما يتصل بالاختصاص القضائي والقانون الواجب تطبيقه في منازعات البيئة الرقمية، وذلك من أجل حماية مصالح المستهلك الأوروبي من الخضوع لنظم قانونية خارجية. ويشير ذلك إلى مدى أهمية هذا القانون. فإذا لم تنظم أمور الاختصاص وتنازع القوانين ضمن قوانين المداولات الإلكترونية بصورة تحمي المستخدم العربي، وتيسر إحقاق الحق في نطاق منازعات البيئة الرقمية، فقد تدرج في قانون حماية المستهلك الرقمي.

الجدول 2- الإنجازات ومواطن القصور والنقص في تشريعات البيئة الرقمية والخدمات الإلكترونية في العالم العربي (خاص بتطبيقات العمليات الإلكترونية)

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
(7) المداولات والتجارة الإلكترونية (العمليات الإلكترونية)	1- أنجز كل من الأردن والبحرين وتونس ودبي وعمان ومصر والمملكة العربية السعودية وضع قوانين المداولات الإلكترونية. ونظمت كلها، باستثناء مصر، السجلات الإلكترونية، ورسالة المعلومات وزمن ومكان إرسالها، والعقود الإلكترونية والتواقيع الإلكترونية ضمن هذه القوانين. كما نصت على سلطات التوثيق، وعلى تجريم بعض أشكال الأفعال ذات الصلة بالجرائم الإلكترونية. وأما مصر فقد حصرت القانون بالتوقيع الإلكتروني، لافتراضها بأن التعاقدات الإلكترونية لا تختلف عن المداولات العادية إلا في شق الإثبات. وفي بقية البلدان العربية، تختلف درجة إنجاز مشاريع القوانين الموضوعة في هذا الصدد. 2- وتضمنت قوانين المداولات الإلكترونية العربية في الأردن نصوصاً بشأن تحويل الأموال بالوسائل الإلكترونية. وقد وضع البنك المركزي الأردني تعليمات تتعلق بتحويل الأموال بالوسائل الإلكترونية في الأسواق الأردنية. ولكن هذا التنظيم اقتصر على الأدوات القائمة، ولم يشمل أبرز تطبيقات المصارف الإلكترونية أو مكوناتها أي النقل

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	الرقمي للأموال. وقد استعرضناه بشكل مفصل لاحقاً ضمن هذا الجدول. 3- أما في موضوع سلطات التوثيق فقد كانت تجربة تونس هي الأنضج بإنشائها وكالة وطنية للتوثيقات الإلكترونية. وقد أقر الأردن في عام 2001 قانوناً نص على وجوب إصدار نظام لإنشاء سلطة التوثيق، ولكن هذا النظام لم يصدر حتى اليوم. وفي بعض البلدان المشار إليها أنشئت مجالس أو هيئات متصلة بتكنولوجيا المعلومات، كما هو الحال في مصر، وفي أماكن أخرى، مثل دبي، أُسندت المهمة إلى أطر قائمة بالفعل. 4- وتتباين التشريعات المعنية بالمداولات الإلكترونية العربية بخصوص نطاق هذه المداولات ومحتواها ومدى شمولها. ويعود هذا التباين إلى ضعف التنسيق بين الجهات التي وضعت هذه التشريعات والجهات العاملة على برامج الحكومة الإلكترونية، إن داخل الدولة الواحدة أو بين الدول. وفي معظم الدول، أُطلقت على هذه القوانين تسمية قوانين المداولات الإلكترونية، ولم تُحصر بالتجارة الإلكترونية. 5- وبالإضافة إلى المصارف الإلكترونية والحكومة الإلكترونية، يرد النشر الإلكتروني بجوانبه الإدارية والمدنية والجزائية بين العمليات الإلكترونية وتطبيقاتها. ولكنه ما زال يمثل أحد اهتمامات تشريعات الصحافة والمطبوعات، باعتبار أن الإنترنت واسطة للنشر. وتتوزع المسائل القانونية للنشر الإلكتروني، وخصوصاً الصحافة الإلكترونية، بين تشريعات الملكية الفكرية وتحديداً حق المؤلف، وتشريعات الخدمات التقنية، وتحديداً المعايير ومسؤوليات الجهات الوسيطة، وتشريعات الحماية الجزائية، وتحديداً جرائم الحاسوب. ولكنها ترتبط كلها بتشريعات حماية البيانات الشخصية. وبما أن الصحافة هي جزء رئيس من هذا النشر، نجد أن تشريعات المطبوعات والنشر والصحافة ذات علاقة وثيقة بهذا الجزء أيضاً. ولم تتحقق حتى الآن أي إنجازات على صعيد تطوير هذه التشريعات لتغطية مسائل النشر الإلكتروني. 6- وفي إطار الخلل في فهم الأدوات التشريعية ومحتواها ودورها، تضمنت تشريعات المداولات الإلكترونية المشار إليها أعلاه نصوصاً تهدف إلى سد النقص في بقية فروع قانون تكنولوجيا المعلومات. وبالرغم من النوايا الحسنة، جاءت هذه المحاولة ناقصة وفي الوقت نفسه معطلة للهدف المرجو، كما هو الحال في الأردن. فبهدف تضمين القانون نصوصاً جزائية تساعد على مواجهة جرائم الحاسوب، أقر الأردن نصاً عاماً، هو المادة 38، حيث جرم أي شخص يرتكب جريمة تقليدية بوسائل إلكترونية. وجاء النص قاصراً عن مواجهة جرائم الحاسوب التي لا وصف لها في القانون التقليدي، ومعطلاً لوضع قانون جرائم الحاسوب في الوقت نفسه، باعتبار أنه مشمول بقانون المداولات الإلكترونية. والأمر سيان بالنسبة إلى القانون العماني حول حماية البيانات الشخصية التي أُفرد لها فصل في قانون المداولات الإلكترونية رقم 2008/69، على غرار قانون تونس الخاص بالمداولات الإلكترونية، وذلك قبل تعديله. وكان القانون في تونس يعالج البيانات الشخصية ضمن ثلاث مواد أُلغيت لاحقاً عندما وضع تشريع شامل لحماية البيانات الشخصية، كما ورد أعلاه. وأما في الأردن، فقد اتجهت السلطات التشريعية نحو تغطية البيانات الشخصية ضمن مواد خاصة لم تشمل هذا الفرع، الأمر الذي سيحول دون وضع قانون شامل لحماية الخصوصية، باعتبار أن الموضوع منظم بالفعل. وينطبق الأمر نفسه على الجرائم الإلكترونية. فقد أغفل قانون المداولات الإلكترونية في الأردن النص المقرر سابقاً في قانون الجزاء، والذي يجرم مجموعة من الجرائم، وأقر قانون جديد تجريم أشكال أخرى من العمليات، الأمر الذي أحدث تباينا في الأدوات التشريعية ونطاق التطبيق. وفي الوقت نفسه، لم تفِ التجربتان بمتطلب وضع قانون شامل لمكافحة الجرائم الإلكترونية. 7- لم تقدم التشريعات العربية حلولاً للاختصاص القضائي والقانون الواجب تطبيقه عند

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	تعارض القوانين المعنية بالمنازعات حول المداولات الإلكترونية. واكتفت جميع التشريعات بتناول مسألة الزمان والمكان المعتمد لصدور رسالة المعلومات وإنشائها، وفق المضمون نفسه الذي أقره القانون النموذجي بشأن التجارة الإلكترونية الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي. وإذا كان صحيحاً أن تحديد معيار الزمان والمكان كاف لتحديد قاعدة الإسناد التي يجري تطبيقها، والتي تشكل إحدى قواعد القانون الدولي الخاص التقليدية، فإن وضع قواعد حول الاختصاص وتنازع القوانين في البيئة الرقمية هو الشغل الشاغل لجميع النظم القانونية الدولية منذ عقدين، وهو الدافع وراء استحداث معايير جديدة مختلفة عن تلك التي وضعها القضاءان الأمريكي والأوروبي لضمان حماية المستخدم في أمريكا وأوروبا عندما يكون طرفا في منازعة رقمية.
(8) المصارف الإلكترونية	1- استخدم عدد كبير من البلدان العربية أدوات تشريعية يمكن وصفها بالقاصرة، مثل التعاميم والقرارات والتعليمات والنظم في أحسن الأحوال، لمعالجة بعض تطبيقات الصيرفة الإلكترونية، وتحديداً البطاقات المالية والمقاصة الإلكترونية للشيكات المتداولة بين المصارف وعبر غرف المقاصة في البنوك المركزية. وباستثناء الأردن وتونس، لم تتم معالجة التحويل الإلكتروني للأموال عبر رسالة البيانات حتى الآن. ومع ذلك، لم تضع جميع البلدان العربية، وحتى تلك التي وضعت تشريعات في حقل المداولات الإلكترونية، التشريع الملائم والكافي لتغطية محتوى المصارف الإلكترونية وتطبيقاتها. فلدى هذه البلدان اعتقاد واهم وخاطئ بأن التعليمات والنظم المشار إليها كافيةٌ، أو بأن مضمون نصوص قوانين المداولات الإلكترونية قادر على تغطية تحويل الأموال إلكترونياً، أو تنظيم المال النقدي الإلكتروني. 2- ولم يصدر أي تشريع عربي متكامل وشامل حول الإطار القانوني لبطاقات الائتمان، بل مجموعة من الأدوات التشريعية التي ترعى جانباً منه فحسب. وهذا الإطار واسع النطاق في دبي ولبنان رغم كونه عبارة عن عدد من التعليمات والتعاميم وليس قانوناً. وهو ضيق وغير كاف في بلدان أخرى مثلما هو الحال في الأردن. 3- وفيما يتصل بالمقاصة الإلكترونية، طبق كل من الأردن ودبي وعمان ولبنان والمملكة العربية السعودية نظماً تعالج نقل صورة الورقة المالية (أي الشيك غالباً) ولا تشمل المعالجة الرقمية للحسابات، أو عمليات التقاص المباشر، أو الشيك الرقمي. 4- ورغم كثرة الحديث عن البوابات المخصصة لتسديد الفواتير إلكترونياً، تحققت التجربة الأبرز في دبي رغم استمرار الحاجة إلى تطويرها. ولكن الإطار القانوني لهذه البوابات لم ينجز حتى الآن في البلدان العربية، وهذا هو أهم أسباب التأخر في شيوع مختلف التطبيقات الإلكترونية التفاعلية في القطاع المصرفي. 5- وفي البلدان العربية، بما فيها بلدان غربي آسيا، يظل نطاق المصارف الإلكترونية بمعناه الشامل بعيداً عن التنظيم الملائم. كما يشكل التشتت في أدوات تنظيم بعض تطبيقات الصيرفة، والعمل المصرفي الإلكتروني مصدراً للإرباك أكثر منه لحل المشاكل.
(9) المضاربات المالية الإلكترونية والأسواق المالية العالمية	1- وفي البلدان العربية، لا سيما في الأردن ولبنان ومصر وغالبية بلدان الخليج، يضطلع العديد من المواطنين بأنشطة المضاربة الإلكترونية مع الأسواق العالمية، وذلك عبر المنصات الإلكترونية في مجال عقود النفط والعملات والذهب والأسهم والخيارات. ولكن أياً من البلدان العربية، ما عدا الأردن مؤخراً، لم يضع قانوناً لضبط هذه المداولات رغم حجم النشاط الهائل الذي تنطوي عليه، ورغم حجم المنازعات، ونطاق الأخطار القانونية المتزايدة.

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	2- ويجب التنبيه إلى أن المضاربات الإلكترونية المقصودة هنا تختلف عن المداولات المالية مع الأسواق المالية العالمية التي تجريها شركات الوساطة المنظمة والقائمة وفق قوانين الأسواق المالية العربية، كقانون الأوراق المالية في الأردن، وقانون سوق رأس المال في دبي وعمان ومصر وغيرها. ولكن أياً من هذه الأدوات التشريعية لا يتعامل مع المضاربات الإلكترونية عن بعد لمجرد أنها تشريعات ذات صلة بنشاط الأسواق المالية المحلية واستثماراتها العالمية التي تتخذ أشكالاً منظمة مغايرة لاستغلال الشبكات. وبالرغم من ذلك، يرد قسم من هذه الأنشطة ضمن بعض التعليمات والنظم والقرارات والتعاميم في هذه الأسواق المالية العربية، وخصوصاً مركز دبي المالي العالمي. وتجدر الإشارة إلى أن إعادة قراءة الاحتياجات التشريعية المتعلقة بالنشاط المالي الإلكتروني تشكل فرصة هامة لإعادة تقييم الأدوات التشريعية المالية العربية بوجه عام، لا سيما مع ظهور أوجه قصور في التعامل مع الأزمة المالية العالمية الأخيرة. 3- ولمواجهة ظاهرة تمتد منذ نحو عشر سنوات في ميدان أنشطة البورصة الأجنبية، ومعظمها في توظيف الأموال محلياً بحجة العمل بالبورصة الأجنبية، سن الأردن القانون المؤقت رقم 50 لسنة 2008، والذي صدر بموجبه قانون تنظيم التعامل في البورصات الأجنبية. وهذا القانون معروض حالياً على مجلس النواب بهدف إقراره كقانون دائم أو رده أو تعديله. ولم يستوف هذا القانون شرط التعامل مع الأسواق المالية العالمية، ولم يركز على أي من نطاقات التعامل الإلكتروني. وقد جاء هذا القانون كرد على أزمة التضييق على النشاط، وليس كقانون للتنظيم. 4- ولم يصدر تنظيم يرعى مسألة المزادات الإلكترونية التي تجري على منصات الشركات العالمية في البيئة الرقمية. ويمكن أن تكون هذه الأنشطة عموماً محلاً لتنظيم المداولات الإلكترونية، من دون حاجة لإفراد أداة تشريعية خاصة بكل تطبيق إلكتروني ما لم يحتج هذا التطبيق إلى قواعد قانونية خاصة، كما هو الحال في البنوك الإلكترونية أو في المضاربات الإلكترونية، وتحديداً في الشق المتعلق بالمال الإلكتروني وتداوله، والقواعد الخاصة بالمضاربات المالية وتغطيتها.
(10) الحكومة الإلكترونية	1- ومنذ عام 2000، بدأت غالبية البلدان العربية باعتماد خطط تتعلق بالحكومة الإلكترونية. وفي هذا الصدد، تحققت إنجازات متقدمة في عدد من البلدان، لا سيما في الإمارات العربية المتحدة ودبي تحديداً. وانطلق عدد من التجارب من رؤية شاملة نظرياً واستراتيجياً، رافقها قصور في التنفيذ، كما هو الحال في الأردن والمملكة العربية السعودية. 2- وتضمنت الاستراتيجيات وخطط العمل الوطنية العربية المعنية بالحكومة الإلكترونية عموماً، وتلك التي أقرتها جميع بلدان غربي آسيا، وجوب العمل على وضع التشريعات أو الإطار القانوني الملائم. ولكن القصور في تحديد هذا الإطار القانوني والتعامل مع موضوع الحكومة الإلكترونية بوصفه نقلاً للخدمات القائمة إلى البيئة الرقمية عبر تطبيقات إلكترونية ليس إلا، والتركيز على التطبيقات التقنية، كلها عوامل أدت إلى قصور واسع في توفير أهم دوافع الحكومة الإلكترونية، وهو التنظيم التشريعي لاحتياجاتها. 3- وأنشأت البلدان العربية مواقع حكومية شاملة كبوابات للخدمات الإلكترونية، وقسمت في غالبيتها الخدمات إلى ثلاث مجموعات، هي الخدمات الحكومية الموجهة إلى المواطن، والخدمات الحكومية الموجهة إلى قطاعات الأعمال التجارية، والخدمات الحكومية الموجهة إلى الحكومة. وقد تناولت جميع الاستراتيجيات وخطط العمل نظرياً مجالات الاهتمام لدى الحكومة الإلكترونية، مثل برنامج التطوير الإداري والتنفيذي، وبرنامج

الحقل/الفرع القانوني	الإنجازات ومواطن القصور
	تطوير التشريعات، وبرنامج تنمية الكوادر البشرية، وبرنامج التطوير الفني، وبرنامج الإعلام والتوعية، وبرنامج تطوير البنية المالية. وباشرت برامج الحكومة الإلكترونية العربية العمل عبر ثلاثة محاور، وهي التالية: النشر الإلكتروني عبر الإنترنت، وتقديم الخدمات الحكومية عبر الإنترنت، واعتماد أدوات القياس المتصلة بالمعايير التقنية لحفظ البيانات في المؤسسات الحكومية وتخزينها. أما من ناحية التطبيق، فقد حددت كل حكومة الخدمات التي ترغب في المباشرة بها، وبدأت مراحل تحويل المؤسسات القائمة بصورة جزئية تمهيداً لإحداث ربط شامل بين هذه المؤسسات وبوابة الخدمات الإلكترونية. 4- وبعيداً عن تقييم كفاءة الخطط من النواحي المالية والتقنية والإدارية التي لا تشملها هذه الدراسة، يتعلق القصور الواضح فيها بشق الإطار القانوني وتطوير التشريعات. ويتمثل أبرز مثال على أثر هذا القصور في غياب الإطار القانوني للمشتريات الحكومية الإلكترونية والمناقصات الحكومية الإلكترونية، وغياب الإطار القانوني لبوابة الدفع الإلكتروني الموحدة. 5- وأما من ناحية الرؤية، والتي يفترض أن تستند إليها التشريعات ذات الصلة لأنها الأدوات اللازمة لتحقيقها، فتجدر الإشارة إلى أن الخدمات الحكومية الإلكترونية لا تعني، ولا يمكن أن تعني، مجرد أتمتة للخدمة الحكومية. فالمقصود هو تحقيق تفاعل شامل بين متلقي الخدمة وأجهزة الحكومة، علماً أن هذا التفاعل لا يزال غائباً عن سائر تجارب الحكومات الإلكترونية العربية. 6- وقد اعتمد عدد من البلدان أدوات قياس البيانات أو القواعد المعنية بحفظها ومعالجتها واسترجاعها في نظم المؤسسات الحكومية كأداة قانونية. وصدرت قرارات وزارية بهذا الشأن، مثل قرار مجلس الوزراء السعودي رقم 40 والمؤرخ 27 آذار/مارس 2006 بشأن إقرار ضوابط تطبيق التعاملات الإلكترونية الحكومية في الجهات الحكومية. ولا شك في أن القرار الوزاري، وإن كان أداة قانونية ملائمة، يبقى قاصراً في نطاق الفكر المؤسسي الذي يتوقف نجاح الحكومة الإلكترونية على تعميقه وتكريسه. ومن ناحية أخرى، ليست المعايير التقنية رهناً بالمعايير الفنية المتخذة في المؤسسات الحكومية وحسب، بل ينبغي توفر معايير وأدوات للقياس في جميع موارد التكنولوجيا وتطبيقاتها. والأهم أن أمور التشفير ومسؤوليات الجهات الوسيطة تحتاج إلى تنظيم تشريعي وإلى ضوابط قانونية خاصة برخص وعقود امتياز تقديم الخدمات، وكلها تحتاج إلى إطار تشريعي شامل.

مراجع عامة

Australian Government. *Cyber Smart Kids Online*. Available at: http://www.cybersmartkids.com.au/about-us.htm.

Boudriga, N. *Digital Certification Practices and Achievement in Tunisia*. May 2003. Available at: http://www.iit.cnr.it/Tiwis2003/documenti/day1/pres-N.Boudrigua.pdf.

Critical Information Infrastructure Protection. *Management Framework for Organizing National Cyber security/CIIP Efforts*. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/richardson-cybersecurity-framework-and-readiness-assessment-CITEL-Mar-08.pdf.

European Network and Information Security Agency (enisa). 2006. Technical report. *The Information Security Breaches Survey* (ISBS 2006). Available at: http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf.

_____. 2006. *A Users' Guide: How to Raise Information Security Awareness, European Network and Information Security Agency*.

Final Acts of the Plenipotentiary Conference. 2006. *Resolution 130. Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies*. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf.

Information Security Forum. Protecting Business Information, *The Standard of Good Practice for Information Security*. Available at: http://www.isfsecuritystandard.com.

International Telecommunication Union (ITU). WSIS Thematic Meeting on Cybersecurity. June 2005. *Background paper: A Comparative Analysis of Cybersecurity Initiatives Worldwide*. Available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

_____. 2006. Available at: http://www.itu.int/ITU-D/treg/Events/Seminars/2006/subregional_clmv/docs/2-5-1-ntoko.pdf.

_____. 2007. *Cybersecurity guide for developing countries*. Available at: http://www.itu.int/ITU-D/cyb/publications/2007/ cgdc-2007-e.pdf.

_____. 2008. *National Cyber Security/CIIP Self-Assessment Tool*. January 2008 Draft.

National Agency for Computer Security. Agence Nationale de la Sécurité Sociale (ANSI). Available at: http://www.ansi.tn.

National Digital Certification Agency. Tunisia. Available at: http://www.certification.tn.

National Information Security Center (NISC). Available at: http://www.nisc.go.jp/eng/index.html.

Ntoko, A. 2004. E-government and IP symposium for the Arab Region, *Building Trust and Security in e-Government*. ITU. Available at: www.ituarabic.org/PreviousEvents/.../01-ITU%20BDT-Building%20Trust%20and %20Security%20for%20egovt.

Organisation for Economic Co-operation and Development (OECD). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Available at: http://www.oecd.org/document/ 42/0,3343,en_2649_34255_15582250_1_1_1_37441,00.html.

_____. *Recommendation on Electronic Authentication and Guidance for Electronic Authentication.* Available at: http://www.oecd.org/document/7/0,3343,en_2649_34255_38909639_1_1_1_1,00.html.

_____. 2002. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.

_____. 2008. Working Party on Indicators for the Information Society. *Measuring Security and Trust in the Online Environment: A view Using Official Data*. DSTI/ICCP/IIS(2007)4/Final. January 2008. Available at: http://www.oecd.org/dataoecd/47/18/40009578.pdf.

Trustguide. 2006. *Final Report*. October 2006. Available at: http://www.trustguide.org.uk/Trustguide%20-%20Final%20 Report.pdf.

United Nations Interregional Crime and Justice Research Institute (UNICRI). Available at: http://www.unicri.it/wwd/ trafficking/legal_framework/docs/convention_on_cybercrime.pdf.

مجلس أوروبا، اتفاقية بشأن الجريمة السيبرانية، بودابست، 21 تشرين الثاني/نوفمبر 2001. http://www.unicri.it/wwd/trafficking/legal_framework/docs/convention_on_cyber_crime.pdf.

اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، E/ESCWA/ICTD/2007/8، 27 حزيران/يونيو 2007.

مراجع متخصصة بالقوانين والتشريعات السيبرانية

الثقة والأمن في البيئة الرقمية

Fischer-Hubner, S. 2006. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. Springer.

Kubota, T. 2007. *Cyberlaw for Global E-business: Finance, Payment, and Dispute Resolution.* Idea Group Inc. (IGI).

Marsden, C. 2000. *Regulating the Global Information Society (Warwick Studies in Globalization*. Harvard University.

United Nations Conference on Trade and Development (UNCTAD). 1999. *Regional Round Tables on Electronic Commerce and Development. Building Confidence*. UNCTAD/SDTE/MISC.11.

قوانين تقنية المعلومات

Edwards, S., Ford II, H. 2001. *Information Technology and Economic Growth in the Emerging Economies.* University of California, Los Angeles (UCLA). September 2001. Available at: http://www.anderson. ucla. edu/faculty/sebastian.edwards.

Ferrera, G.R. Lichtenstein, S.D., Reder, M.E.K., Bird, R., et al. 2003. *Cyberlaw: Text and Cases*. Thomson Learning.

Helewitz, J.A. 2003. *Cyberlaw: Legal Principles of Emerging Technologies.* Pearson/Prentice Hall.

Kubota, T. 2007. *Cyberlaw for Global E-business: Finance, Payment, and Dispute Resolution.* Idea Group Inc (IGI).

Smith, G.J.H. 2007. *Internet Law and Regulation*, Sweet and Maxwell.

Reed, C., Angel, J. 2007. *Computer Law: The Law and Regulation of Information Technology*. Oxford University Press.

Tapper, C. 1982. *Computer Law*, Longman. (Original from the University of Michigan, Digitized 7 November 2007).

Trout, B.J. (Contributor Torke, K.). 2007. *Cyber Law: A Legal Arsenal for Online Business*. World Audience, Inc.

د. عرب، يونس، موسوعة القانون وتقنية المعلومات، الكتاب الأول، قانون الحاسوب، ط 1، منشورات إتحاد المصارف العربية، 2001، بيروت.

الخصوصية والحق في الوصول إلى المعلومات

Brooke, H. 2005. *Your Right to Know: How to Use the Freedom of Information Act and Other Access Laws*. Pluto Press.

Connolly, K.J. *Law of Internet Security and Privacy*. Aspen Publishers Online (ISBN 0735542732, 9780735542730).

Frackman, A., Martin C., R., Ray, C. 2002. *Internet and Online Privacy: A Legal and Business Guide.* ALM Publishing.

Garrett, B. 2001. *The Right to Privacy.* The Rosen Publishing Group.

Herold, R. 2002. *The Privacy Papers: Managing Technology, Consumer, Employee, and Legislative Actions*. CRC Press.

Holtzman, D.H. 2006. *Privacy Lost: How Technology is Endangering Your Privacy*, A Wiley Imprint.

Lintner, B., Coronel, S.S. 2001. *The Right to Know: Access to Information in Southeast Asia*. Philippines: Philippine Center for Investigative Journalism.

Westby, J.R. 2004. *International Guide to Privacy*. (American Bar Association Privacy & Computer Crime Committee, American Bar Association Section of Science & Technology Law). American Bar Association.

د. عرب، يونس، موسوعة القانون وتقنية المعلومات، الكتاب الثاني (دليل أمن المعلومات والخصوصية) الجزء الثاني: الخصوصية وحماية البيانات في العصر الرقمي، ط 1، منشورات إتحاد المصارف العربية، 2002، بيروت.

Budapest Convention on Cybercrime. CETS No.: 185. Opening for signature 23/11/2001. Entry into force 7 January 2004.

Casey, E. 2004. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press.

Herold, R. *Managing an Information Security and Privacy Awareness and Training Program*. Auerbach publication.

Toren, P. 2003. *Intellectual Property and Computer Crimes*, Law Journal Press.

Vacca, J.R. 2005. *Computer Forensics: Computer Crime Scene Investigation*. Charles River Media.

د. عرب، يونس، موسوعة القانون وتقنية المعلومات، الكتاب الثاني (دليل أمن المعلومات والخصوصية) الجزء الأول، جرائم الحاسوب والإنترنت، ط 1، منشورات إتحاد المصارف العربية، 2001، بيروت.

الملكية الفكرية المتصلة بتكنولوجيا المعلومات

Black, T. 2002. *Intellectual Property in the Digital Era*. Sweet and Maxwell.

Dreyfuss, R., Zimmerman, D.L., First, H. 2002. *Expanding the Boundaries of Intellectual Property: Innovation Policy for the Knowledge Society*. Oxford University Press.

Hoyenkamp, H., Janis, M.D., Lemley, M.A. Latest issue: 2005. *IP and Antitrust: An Analysis of Antitrust Principles Applied to Intellectual Property Law*. Aspen Publishers Online (ISBN 0735522073, 9780735522077).

Koo, D.-H. 2005. *Information Technology and Law: Computer Programs and Intellectual Property Law in the US, Europe, Japan, Korea*. Pakyoungsa 2005.

Nguyen, X.-T.N., Gomulkiewicz, R.W., Conway-Jones, D., 2006. *Intellectual Property, Software, and Information Licensing: Law and Practice*. BNA Books.

Torremans, P. 2008. *Intellectual Property Law*. Oxford University Press.

Wherry, T.L. 2002. *The Librarian's Guide to Intellectual Property in the Digital Age*: *Copyrights, Patents, and Trademarks*. ALA Editions.

المنظمة العالمية للملكية الفكرية (الوايبو) معاهدة بشأن حق المؤلف، 1996.

الوايبو، معاهدة بشأن الأداء والتسجيل الصوتي، 1996.

تشريعات الأعمال الإلكترونية وتطبيقاتها

Campbell, D., Woodley, S. 2003. *E-Commerce: Law and Jurisdiction*. Kluwer Law International.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. Directive on electronic commerce. Official Journal L 178, 17/07/2000 P. 0001-0016.

Grosse, R.E. 2004. *The Future of Global Financial Services*. Blackwell Publishing.

Gup, B.E. 2003. *The Future of Banking*. Greenwood Publishing Group.

Kehal, H.S., Singh, V.P. 2005. *Digital Economy: Impacts, Influences, and Challenges*. Idea Group Inc. (IGI).

Leroy Miller, R., Jentz G.A. 2005. *Business Law Today: The Essentials: Text & Summarized Cases – e-commerce, Legal, Ethical, and International Environment*. Thomson West.

Mills, J.E., Law R. 2005. *Handbook of Consumer Behavior, Tourism, and the Internet*. Haworth Press.

Pruski, A.H. 2005. *Assistive Technology: From Virtuality to Reality*. IOS Press.

Simmons & Simmons Communications Practice. 2001. *E-commerce Law: Doing Business Online.* Palladian Law.

The UCLA Online Institute for Cyberspace Law and Policy. *The Electronic Signatures in Global and National Commerce Act 2000* ("E-Sign"). Available at: http://www.gseis.ucla.edu/iclp/hp.html.

Todd, P. 2006. *e-Commerce Law*. New York: Routledge – Cavendish.

UCLA. The Internet Tax Freedom Act 1998. Available at: http://www.gseis.ucla.edu/iclp/hp.html.

لجنة الأمم المتحدة لقانون التجارة (اليونسترال)، القانون النموذجي للتجارة الإلكترونية، 1996؛ وقانون اليونسترال النموذجي للتواقيع الرقمية، 2001، إضافة إلى مختلف التشريعات والأدلة الإرشادية والنّماذج العقدية التي وضعتها اليونسترال والمتاحة على موقعها على الإنترنت: www.uncitral.org.