إرشادات الإسكوا للتشريعات السيبرانية

مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية

بيروت، ٢٠١٢

المحتويات

تمهيد

يشهد المجتمع اليوم تطوراً متسارعاً لتكنولوجيا المعلومات والاتصالات، كما يشهد تزايداً وتنوعاً في التطبيقات والخدمات الإلكترونية التي تعتمد الفضاء السيبراني أساساً لها. ولأن تكنولوجيا المعلومات والاتصالات أصبحت الركيزة الأولى لبناء مجتمع المعرفة ولبنة أساسية في نموه وازدهاره، يتطلع العديد من الدول اليوم، المتقدمة منها أو النامية، إلى بناء مجتمع معرفي جديد يعتمد على التنوع الاقتصادي، وعلى الابتكار والإبداع، وكذلك على التبادل المعرفي والفكري في المجالات الحيوية المختلفة.

لقد بينت التجارب العالمية والإقليمية أن بناء مجتمع معرفي مستدام يحتاج إلى بيئة قانونية وتنظيمية للفضاء السيبراني. وتُعتبر التشريعات السيبرانية التي تضع الأطر الناظمة لاستخدام الفضاء السيبراني وتعالج المسائل القانونية الناجمة عن استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها المختلفة في الحياة الاقتصادية والاجتماعية، ركيزة أساسية للبيئة التمكينية الضرورية لمجتمع المعرفة.

وبهدف المساهمة في تطوير البيئة التمكينية لبناء مجتمع المعرفة في المنطقة العربية، أدرجت اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) موضوع التشريعات السيبرانية في قائمة اهتماماتها منذ عام ٢٠٠٧، ونظمت في هذا الإطار عدداً من الأنشطة لعل أهمها مشروع «تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية» الذي يموله صندوق التنمية في الأمم المتحدة والذي بدأت الإسكوا بتنفيذه عام ٢٠٠٩. وقد أعدت الإسكوا في إطار هذا المشروع «إرشادات الإسكوا للتشريعات السيبرانية» التي تغطي ستة محاور أساسية هي: الاتصالات الإلكترونية وحرية التعبير، والمعاملات الإلكترونية والتوقيع الإلكتروني، والتجارة الإلكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، والجرائم السيبرانية، والملكية الفكرية في المجال المعلوماتي والسيبراني.

وقد جاء إعداد هذه الإرشادات استجابة لتطلعات المنطقة العربية في التحول إلى مجتمع المعرفة، ولجسر الثغرة القانونية الموجودة في دول المنطقة في مجال التشريعات السيبرانية. وتجدر الإشارة إلى أن جميع دراسات وأنشطة الإسكوا في مجال التشريعات السيبرانية أوصت بضرورة إعداد حزمة متكاملة من هذه التشريعات لتكون أداة مساندة للدول العربية في وضع قوانينها السيبرانية من ناحية، وأساساً للمواءمة والمجانسة فيما بين التشريعات السيبرانية في المنطقة العربية من ناحية أخرى.

وتم إعداد وصياغة هذه الإرشادات بالاعتماد على التجارب الدولية والإقليمية في مجال التشريعات السيبرانية، وخاصة تجربة المفوضية الأوروبية، وبعد الاطلاع على العديد من المراجع العلمية والبحثية والفقهية في هذا المجال. وتجدر الإشارة إلى أن المسودة الأولية لهذه الإرشادات نوقشت خلال اجتماع خبراء خصص لهذا الغرض وضم مجموعة من الخبراء من معظم الدول العربية. وقد أخذت الملاحظات التي أبداها الخبراء بعين الاعتبار عند صياغة النسخة النهائية من الإرشادات.

إن إرشادات الإسكوا للتشريعات السيبرانية هي ثمرة جهد مشترك ضمن إطار المشروع المذكور أعلاه. فقد أوصت اللجنة الاستشارية العليا للمشروع، والتي ضمت عدداً من المؤسسات الإقليمية العاملة في مجال التشريعات السيبرانية، بإعداد حزمة متكاملة من الإرشادات للتشريعات السيبرانية. وقد تعاونت الإسكوا في إعداد هذه الإرشادات مع الخبير الدولي السيد وسيم حرب وفريق عمله.

وقام فريق عمل من شعبة تكنولوجيا المعلومات والاتصالات بتنفيذ مشروع الإسكوا للتشريعات السيبرانية خلال الفترة ٢٠٠٩-٢٠١٢، وذلك بإدارة السيدة نبال إدلبي رئيسة قسم تطبيقات تكنولوجيا المعلومات والاتصالات في الشعبة، وبمشاركة كل من السيد جورج يونس والسيدة ميرنا بربر والسيدة هانيا الدياسي، وبدعم من السيد يوسف نصير المدير السابق للشعبة والسيد حيدر فريحات مديرها الحالي.

لقد أعدت الإسكوا هذه الإرشادات ليستعين بها المشرعون عند صياغة التشريعات السيبرانية، وليستفيد منها أصحاب القرار في الوزارات والمؤسسات الحكومية من أجل وضع قوانين جديدة أو تعديل القوانين النافذة، وليعتمد عليها القضاة والمحامون في معالجة المسائل القانونية المتعلقة بالفضاء السيبراني. وتتمنى الإسكوا أن يستفيد من هذه الإرشادات أيضاً الأكاديميون والباحثون والطلاب المهتمون بتنظيم الفضاء السيبراني، وكذلك الأفراد الذين يحلمون بأن يصبح الفضاء السيبراني فضاء آمناً وموثوقاً.

وأخيراً تأمل الإسكوا في أن تساهم هذه الإرشادات بتحفيز مجتمع المعرفة في المنطقة العربية.

مقدمة عامة حول إرشادات الإسكوا للتشريعات السيبرانية

لقد دخلت الدول العربية إلى عالم تشريع الفضاء السيبراني متأخرة بعض الشيء عن الدول الغربية، كما هو حال دول العالم الجنوبي عموماً، خاصة وأن بناء مجتمع المعلومات فيها قد أخذ فترة من الزمن، في حين بدأت مسيرته فعلياً في الدول المتقدمة في مطلع التسعينات. يضاف إلى ذلك أن الاعتماد على شبكات وأنظمة الحاسوب في المعاملات والتجارة وفي مجال القطاع العام ولدى المؤسسات والأفراد في الدول العربية، ليس بنفس الحجم الذي هو عليه في دول العالم الشمالي.

وعلى الرغم من ذلك، فإن استعمال أجهزة وأنظمة الحاسوب أخذ يتزايد يوماً بعد يوم في الدول العربية، وبالتالي ازدادت الحاجة إلى تنظيم قانوني لاستعمال هذه الأنظمة لاسيما بعد أن واكب القطاع الخاص والأفراد التطوّر وبدأ استعمال شبكة الإنترنت الفعلي لأجل القيام بعمليات مصرفية، أو معاملات وتعاقد عن بعد، أو حتى كتابة المدونات. لذا فإن المشرِّع في الدول العربية وجد أن توفر القوانين المُنظِّمة لموضوع الفضاء السيبراني يشكل ضرورة من الناحية القانونية بالنسبة للتعاملات بين الأفراد والمؤسسات، ومثال على ذلك الإثبات الإلكتروني والتعاقد والمراسلات والحد من الجرائم السيبرانية. وتُضاف إلى ذلك العوائق أمام التعاملات بين أفراد ومؤسسات عربية ونظيرتها في الدول الغربية حيث يتطلب مثل هذا التعاون وجود قواعد قانونية متوافقة بالحد الأدنى.

أمام هذا الغياب في التشريع السيبراني في الدول العربية، قامت بعض الدول في بداية الأمر باقتباس قوانين بعض الدول الأوروبية ومحاولة ملاءمتها مع الواقع القائم في الدول العربية المعنية لإقرار هذه القوانين، وقد تم أيضاً الاسترشاد بالمعاهدات والاتفاقيات الدولية والنماذج القانونية لمنظمات دولية مثل الأونيسترال UNCITRAL في ورشة التشريع العربية. وتختلف المقاربات التشريعية في الدول العربية لناحية تقنين مواضيع الفضاء السيبراني، ويتلخص ذلك بما يلي:

أ- وضع قانون خاص بكل موضوع من مواضيع الفضاء السيبراني[1].

ب- تعديل القوانين القائمة والسارية المفعول وإضافة مواد أو فصول عليها تتعلق بالفضاء السيبراني[2]. وتبين أن هذه الطريقة لا تلبي الحاجة التشريعية حيث اقتصر الأمر على بعض المواضيع مثل قانون حماية حق المؤلف، والإثبات الإلكتروني اللذين تم تناولهما ضمن إطار قوانين الإجراءات وأصول المحاكمات المدنية.

ج- وضع قانون موّحد يشمل مختلف مواضيع الفضاء السيبراني، ويكون نصاً واحداً مقسماً إلى أبواب يتعلق كل منها بموضوع من مواضيع الفضاء السيبراني.

١- اهتمام الإسكوا بالتشريعات السيبرانية

تعتبر التشريعات السيبرانية مكوناً أساسياً من مكونات البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات، كما تشكل عنصراً هاماً لتوفير الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الفضاء السيبراني. ومن هذا المنطلق، وبهدف تعزيز مجتمع المعرفة في المنطقة العربية والمساهمة في تحفيز التكامل الإقليمي، بدأ اهتمام اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) بتطوير التشريعات السيبرانية Cyber Laws كونها تشكل عنصراً أساسياً من عناصر البيئة التمكينية لمجتمع المعلومات ولبناء الاقتصاد المبني على المعرفة.

قامت منظمة الإسكوا منذ عام ٢٠٠٧ بإعداد عدة دراسات حول وضع التشريعات السيبرانية في الدول العربية[3]. كما قامت بتنظيم عدة اجتماعات خبراء لمناقشة هذه الدراسات وتحديد احتياجات المنطقة من أجل تحسين وضع التشريعات السيبرانية. وقد بينت جميع هذه الأنشطة الحاجة إلى إعداد إرشادات توجيهية للتشريعات السيبرانية لتطوير وتنسيق التشريعات السيبرانية في المنطقة العربية والتي من شأنها أن تساعد الحكومات العربية على سن أو تعديل تشريعاتها لتنظيم كل ما يتعلق بالفضاء السيبراني. كما أوضحت الدراسات واجتماعات الخبراء أهمية تنسيق التشريعات السيبرانية فيما بين بلدان المنطقة العربية من أجل تحسين التجارة الإلكترونية البينية ومواجهة الجرائم السيبرانية وبناء اقتصاد إقليمي مبني على المعرفة. وبناء على ذلك باشرت الإسكوا عام ٢٠٠٩ بإعداد وتنفيذ مشروع **"تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"**[4] للاستجابة لاحتياجات المنطقة العربية في مجال التشريعات السيبرانية.

يتضمن مشروع الإسكوا إعداد دراسات لتحديث وضع التشريعات السيبرانية في المنطقة العربية[5]، وصياغة إطار عام لتحسين وضع التشريعات السيبرانية في المنطقة العربية[6]. ومن أهم دراسات ومخرجات المشروع هذه الدراسة

التي تهدف إلى إعداد حزمة إرشادات للتشريعات السيبرانية تغطي ست محاور أساسية لتنظيم الفضاء السيبراني. ويتضمن مشروع الإسكوا كذلك تنظيم اجتماعات خبراء لمناقشة الدراسات الناتجة عنه، وتنظيم ورشات عمل للتوعية بناء القدرات على استثمار إرشادات الإسكوا للتشريعات السيبرانية. كما يتضمن تقديم خدمات استشارية للدول الأعضاء في الإسكوا والبلدان العربية الأخرى من أجل تطوير تشريعاتهم السيبرانية مع الأخذ بالاعتبار إرشادات الإسكوا للتشريعات السيبرانية. وبهدف ضمان استمرارية العمل على تطوير التشريعات السيبرانية في المنطقة تضمن مشروع الإسكوا إنشاء شبكة افتراضية للنقاش والحوار بحيث تشكل هذه الشبكة اللبنة الأساسية لتبادل المعرفة وأداة لاستدامة المشروع.

تسعى الإسكوا من خلال هذه الدراسة بشكل رئيسي إلى وضع أطر إرشادية خاصة بمواضيع الفضاء السيبراني، وتسمح للدول التي لم تسن قوانين تتعلق بالفضاء السيبراني أو ترى أن قوانينها بحاجة للتحديث من جهة والإكمال من جهة أخرى أن تسير في هذا الاتجاه. وتغطي هذه الإرشادات المواضيع التالية المتعلقة بالفضاء السيبراني: ١- الاتصالات الإلكترونية وحرية التعبير، ٢- المعاملات الإلكترونية والتواقيع الإلكترونية، ٣- التجارة الإلكترونية وحماية المستهلك، ٤- معالجة وحماية البيانات ذات الطابع الشخصي، ٥- الجرائم السيبرانية، ٦- الملكية الفكرية في المجال المعلوماتي والسيبراني.

إن هذه المقاربة في صياغة الإرشادات اعتمدت أسلوب التقنين المنفصل لمواضيع الفضاء السيبراني وذلك بغية توفير الحد الأقصى من الوضوح. وتقتضي الإشارة إلى أن إعداد الإرشادات التوجيهية تم بالاعتماد على أعمال بحثية تناولت مجموعة من السوابق والأدبيات التي عالجت بشكل أو بآخر، موضوع الفضاء السيبراني، سواء كانت اتفاقيات إقليمية أو قرارات وإرشادات وتوصيات إقليمية، أم تشريعات عربية وأجنبية، إضافة إلى المراجع الفقهية العربية والأجنبية.

في ضوء ما وفرته نتائج الأعمال البحثية، جرى إعداد الفهارس الموضوعية الستة، وقد تم الاستئناس بالإرشادات الأوروبية المتصلة بهذه المواضيع وكذلك ببعض النصوص القانونية القائمة في دول من العالم الشمالي، مع الأخذ بعين الاعتبار ما هو قائم في دول الإسكوا من تشريعات تتعلق من قريب أو من بعيد بالمواضيع الستة المختارة.

٢- منهجية إعداد إرشادات الإسكوا للتشريعات السيبرانية

تولي الإسكوا اهتماماً خاصاً للتجارب الدولية والإقليمية المتراكمة في مجال التشريعات السيبرانية وبخاصة تجربة الاتحاد الأوروبي والتي نتج عنها إصدار عدد من التوجيهات والإرشادات تشمل مواضيع الفضاء السيبراني لدول الاتحاد الأوروبي، كما تولي كذلك اهتماماً بالتجارب العربية سواء منها الإقليمية أو الوطنية. وبناء عليه اعتمدت في إعداد هذه الإرشادات على:

١) التجارب والأنشطة الدولية المنظمة للفضاء السيبراني[٧]، وأهمها: الاتفاقيات الإقليمية، والإرشادات والتوصيات الصادرة عن الاتحاد الأوروبي والقرارات الصادرة عن مجلس الأمم المتحدة والمجلس الأوروبي والاتحاد الدولي للاتصالات بالإضافة إلى القوانين الدولية النموذجية في هذا المجال؛

٢) التجارب والأنشطة العربية المتعلقة بالفضاء السيبراني[٨]، وأهمها: النصوص القانونية ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ والقرارات والقوانين النموذجية الصادرة من جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق؛

٣) مختارات من تشريعات وطنية من مختلف الدول الأجنبية[٩] التي نظمت المعاملات الإلكترونية وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الأسترالية والتشريعات الخاصة ببعض دول آسيا الوسطى؛

٤) أهم المراجع الفقهية العربية والأجنبية[١٠] التي تناولت التنظيم القانوني للفضاء السيبراني.

وكانت حصيلة أعمال الجمع على الشكل التالي:

- بلغ عدد الاتفاقيات الإقليمية والإرشادات الأوروبية والتنظيمات والقرارات والقوانين النموذجية ٥٧ نصاً؛
- بلغ عدد التشريعات الأجنبية ٥٢ نصاً؛
- بلغ عدد التشريعات العربية ٩٣ تشريعاً عربياً.

وقد تم الاسترشاد بالمراجع الفقهية العالمية العائدة لمؤلفين مشهود لهم في الأوساط المعلوماتية وأبرزها:

- Droit de L'internet, André Lucas

- Droit de L'informatique et Des Télécommunications, Jérôme Huet - Herbert Mais.

- Le droit de l'Internet : Lois, contrats et usages de Vincent Fauchoux, Pierre Deprez, et Jean-Michel Bruguière (Broché - 22 janvier 2009).

- Droit de l'Informatique, Vivant (M.) Lamy, 1998.

- Philosophie du droit d'auteur "On Line", Internet saisi par le Droit, Travaux de l'A.F.D.I.T, - Gautier (P.-Y), Editions des Parques, 1997.

- Business et Droit d'Internet, The Best of Mc Graw Hill, Hance (O.), 1996.

- Guerres dans le cyberspace, Services secrets et Internet, Guisnel (J.), Editions La Découverte, 1995.

- The Law of Electronic Commerce, EDL, E-mail, and Internet: Technologie, Proof and Liability, Wright (B.), 2nd Ed.,Boston, Little, Brown and Company, 1995.

- Traité de la propriété littéraire et artistique, Lucas (A) et Lucas (H), Paris, Litec, 1994.

- Lucas (A.), Résumé des débats du colloque: "Program copyright and moral rights: a culture clash?" Symposium de l'OMPI, Paris 1994: Computer and Law and Security report, 1994.

- Computers and the English Law of Evidence, Law, Computers & Artificial Intelligence, Hirst (M.), 1992.

- Bensoussan (A.) Contributions théoriques au droit de la prévue dans le domaine informatique: Aspects techniques et solutions juridiques, Gaz.Pal., 1991, 2.

- Bensoussan (A.), Le commerce électronique sur les autoroutes de l'information, Cahiers Juridiques et Fiscaux de l'Exportation, No 296/.

وبعد الانتهاء من تجميع المعلومات تمّت مقارنة التشريعات الدولية والإرشادات الأوروبية بالتشريعات العربية وتحليلها لرصد واستخلاص نقاط القوة والضعف الموجودة في هذه التشريعات. فكان التركيز على:

أ- وجود تشريعات وطنية خاصة تنظم الفضاء السيبراني؛
ب- مدى شمولية التشريعات للمواضيع الستة المذكورة أعلاه.

٣- طريقة البحث

تم البحث عن المعلومات والنصوص القانونية المطلوبة من خلال الاعتماد على وسيلتين أساسيتين، هما:
- البحث عبر شبكة الإنترنت؛
- البحث عبر المكتبات الورقية.

شمل البحث عبر شبكة الإنترنت، الاتفاقيات الدولية والإقليمية والإرشادات الأوروبية الخاصة بموضوع التشريعات السيبرانية، والتشريعات الأجنبية، بالإضافة إلى المراجع الفقهية العالمية والإقليمية، وذلك من خلال رصد المواقع الخاصة بالمصادر الأساسية للجهات الرسمية المعنية. ومن أهم المصادر المعتمدة:

الموقع الخاص بالاتحاد الأوروبي:
http://eur-lex.europa.eu
الموقع الخاص بالمجلس الأوروبي:
http://www.coe.int
الموقع الخاص باللجنة الأوروبية للعدالة:
http://ec.europa.eu/justice
الموقع الخاص بالأمم المتحدة:
http://www.un.org
الموقع الخاص بلجنة الأمم المتحدة للقانون التجاري الدولي:
http://www.uncitral.org
الموقع الخاص بمنظمة التعاون والتنمية والاقتصاد :
http://www.oecd.org
الموقع الخاص بالبنك الدولي:
http://www.worldbank.org
الموقع الخاص بوزارة العدل للولايات المتحدة:
http://www.cybercrime.gov
الموقع الخاص الرسمي لتشريعات فرنسا:
http://www.legifrance.gouv.fr
الموقع الخاص بالتشريعات الأمريكية:
http://www.uscode.house.gov , www.law.cornell.edu
الموقع الخاص بالمنظمة العالمية للملكية الفكرية:
http://www.wipo.int

بالإضافة إلى مواقع أخرى خاصة بوزارات العدل العربية، ووزارات التجارة والاتصالات الأجنبية والعربية.

شمل البحث عبر المكتبات الورقية، المكتبات المتوفرة التالية: مكتبة الدكتور وسيم حرب، مكتبة المركز العربي لتطوير حكم القانون والنزاهة، مكتبة الجامعة الأمريكية، مكتبة الجامعة العربية، مكتبة جامعة القديس يوسف.

٤- الوضع العام للتشريعات السيبرانية في المنطقة العربية

تبين دراسات الإسكوا وتحديث هذه الدراسات[١١] والذي أجري خلال الفترة الأولى من تنفيذ مشروع "تنسيق التشريعات السيبرانية لتعزيز مجتمع المعرفة في المنطقة العربية"[١٢] تزايد الاهتمام في المنطقة بالتشريعات السيبرانية وفي تطبيقها أيضاً. فقد شهدت السنوات الأخيرة إقرار عدد لا بأس به من التشريعات السيبرانية ومنها قانون المعاملات الإلكترونية في قطر في عام ٢٠١٠، وقانون الجرائم الإلكترونية في الأردن عام ٢٠١٠، وكذلك قانون التوقيع الإلكتروني وخدمات الشبكة في الجمهورية العربية السورية في عام ٢٠١٠.

تبين أثناء أعمال البحث أن معظم البلدان العربية، عملت على إصدار تشريعات خاصة وإقرار نظام للتعاملات الإلكترونية تهدف إلى ضبط التعاملات والتواقيع الإلكترونية وتنظيمها وتوفير الإطار التنظيمي لها، وذلك لإضفاء الحجية عليها، حيث تتم معاملة المستند الإلكتروني - متى توافرت فيه الشروط والمواصفات المطلوبة نظاماً - معاملة المستند الورقي المكتوب، لجهة ترتب الآثار النظامية عليه، وقبول حجيته في الإثبات وغير ذلك من الأمور النظامية التي

يتطلبها الوضع حتى يتم قبول هذه التعاملات والاعتماد عليها كوسيلة جديدة من وسائل التعامل. ويشمل نظام التعاملات الإلكترونية جميع المعاملات الإلكترونية.

وتجدر الإشارة إلى أن عدداً من الدول دمجت قانوني المعاملات والتجارة الإلكترونية في قانون واحد مثل الأردن والسعودية وعمان، بينما ذهبت بعض الدول الأخرى مثل البحرين وقطر والسودان إلى دمج التوقيع والمعاملات والتجارة الإلكترونية في قانون واحد. ومن المفيد الإشارة هنا إلى أن معظم قوانين المعاملات والتجارة الإلكترونية في المنطقة العربية لم تتضمن بنوداً خاصة بالدفع الإلكتروني والاستثناء على ذلك هو في اليمن ولبنان، حيث صدر في اليمن قانون خاص بالعمليات المصرفية الإلكترونية، أما في لبنان فقد أصدر مصرف لبنان المركزي العديد من القرارات التي تنظم عمليات الدفع الإلكتروني والصيرفة الإلكترونية.

كما تبين الدراسات التي قامت بها الإسكوا حول وضع التشريعات السيبرانية أن هناك عدداً قليلاً من البلدان العربية التي نظمت الجرائم التي تحدث خلال شبكة الإنترنت، بحيث أصدرت تشريعات خاصة تقضي بمكافحة الجرائم السيبرانية والمعلوماتية، ومنها دبي والسعودية والسودان والأردن. وعمدت بلدان على إلى تعديل تشريعاتها الجزائية لتشمل جرائم الحاسوب، مثال سلطنة عمان التي قامت بإصدار قانون تعديل قانون الجزاء العام[١٣] وإضافة مادة مكررة تتعلق بجرائم الحاسوب؛ بالإضافة إلى قيام بعض البلدان بإصدار عدة قرارات وتنظيمات إدارية في هذا المجال، وخاصة في مصر[١٤] ولبنان[١٥].

وتكاد تكون القوانين الخاصة بحماية البيانات الشخصية في الفضاء السيبراني شبه معدومة في منطقة الإسكوا فما عدا قانون صادر عن مركز التجارة العالمي في دبي لا يوجد أي قانون خاص بهذا المجال. أما دول شمال أفريقيا فقد أصدرت كل من تونس والمغرب قوانين خاصة بحماية البيانات الشخصية.

أما فيما يتعلق بموضوع حماية الملكية الفكرية، فقد عمدت بعض البلدان العربية إلى تطبيق أحكام قوانين حقوق المؤلف الخاصة، والبعض الآخر إلى تعديل قوانينه المعتمدة لتشمل حماية حقوق المؤلف عبر شبكة الإنترنت وحماية البرامج والحاسوب، أو من خلال إصدار نصوص تنظيمية خاصة لحماية البرامج والحاسوب، مثال تعميم صادر عام ٢٠٠٦ لحماية برامج المعلوماتية ومكافحة القرصنة في لبنان. ولا بد من الإشارة، ضمن هذا المجال، إلى أن جامعة الدول العربية قامت بإصدار القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة[١٦]، حيث تناول أحكاماً حول حجية الكتابة والمحرّرات والتواقيع الإلكترونية، والهيئة المختصّة، ووجهة التوثيق الإلكتروني المنظمة لشهادات التوثيق الإلكتروني والجرائم المرتكبة في هذا المجال وعقوباتها. وتبنت جامعة الدول العربية أيضاً عام ٢٠٠٣، بقرارها رقم ٤١٧، قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات[١٧] وما في حكمها.

وبالرغم من هذه الجهود الواعدة، فإن هذه التشريعات السيبرانية فيما بين الدول العربية ما زالت غير متجانسة، مما يعقد القيام بالتعاملات الإلكترونية عبر الحدود على الرغم من أهمية هذه التعاملات لتطوير الاقتصاد العربي وتعزيز مجتمع المعلومات العربي.

هوامش

١- صدر قانون خاص لتنظيم المعاملات الإلكترونية في جميع الدول العربية باستثناء العراق ولبنان وفلسطين والكويت التي هي بصدد إعداد ودراسات لمشاريع قوانين في هذا المجال.

٢ – قامت سلطنة عمان بإصدار مرسوم سلطاني رقم ٢٠٠١/٢٧ يقضي بتعديل بعض أحكام قانون الجزاء العماني وذلك بإضافة المادة ٢٧٦ مكرر وهي تتضمن أحكاما حول جرائم الحاسوب. قامت دبي بإصدار قانون رقم ٣٦ لسنة ٢٠٠٦ بتعديل بعض أحكام قانون الإثبات في المعاملات المدنية والتجارية (١٩٩٢)- مثال المادة ١٧ لتتناسب وأحكام الإثبات الالكتروني.
قامت فلسطين أيضا بتعديل قانون البيانات في المواد المدنية والتجارية رقم (٤) لسنة ٢٠٠١م – المادة ١٩ ليشمل الإثبات عبر البريد الالكتروني.

٣- نماذج التشريعات السيبرانية في منطقة الإسكوا، E/ESCWA/ICTD/2007/8

٤- http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

٥- دراسات المشروع الخاصة بوضع التشريعات السيبرانية في المنطقة العربية (٤ دراسات شارك بإعدادها كل من: د. يونس عرب، د. عمر الشريف، د. سامي شرف، د. حسين الغافري).

٦- دراسة "نحو الانفتاح على التواصل مع الواقع القانوني للفضاء السيبراني في المنطقة العربية"، إعداد الدكتور عبد الحي السيد، ٢٠١١.

٧ – تراجع لائحة الاتفاقيات الإقليمية والإرشادات الأوروبية – ملحق رقم ١.

٨ – تراجع لائحة التشريعات العربية – ملحق رقم ٢.

٩ – تراجع لائحة تشريعات الدول الأجنبية – ملحق رقم ٣.

١٠ – تراجع لائحة المراجع الفقهية العربية والأجنبية المجمعة على الإنترنت ومن المكتبات الورقية – ملحق رقم ٣.

١١- دراسات المشروع الخاصة بوضع التشريعات السيبرانية في المنطقة العربية (أربع دراسات شارك بإعدادها كل من: د. يونس عرب، د. عمر الشريف، د. سامي شرف، د. حسين الغافري).

١٢- http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

١٣- مرسوم سلطاني رقم ٢٠٠١/٢٧ يتعلق بتعديل بعض أحكام قانون الجزاء العماني، إضافة المادة ٢٧٦ مكرر حول جرائم الحاسوب.

١٤- قرار وزاري بإنشاء إدارة متخصصة لمكافحة جرائم الحواسيب والشبكات بوزارة الداخلية تسمى "إدارة مباحث مكافحة جرائم الحاسبات الإنترنت".

١٥- تعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥ يتعلق بحماية برامج المعلوماتية ومكافحة القرصنة في لبنان.

١٦- القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، اعتمده مجلس وزراء العدل العرب بقرار رقم ٧٧١/د٢٤ – ٢٠٠٨/١١/٢٧.

١٧ – قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنيات المعلومات وما في حكمها، اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بقرار رقم ٤٩٥ – د١٩– ٢٠٠٣/١٠/٨، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم ٤١٧– د٢١/٢٠٠٤.

الإرشـاد الأول

الاتصالات الإلكترونية وحرية التعبير

١

الورقة البحثية الخلفية لإرشاد الاتصالات الإلكترونية وحرية التعبير

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع الاتصالات الإلكترونية وحرية التعبير في الدول العربية ورصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية. وبالتالي تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بالاتصالات الإلكترونية وحرية التعبير.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالاتصالات الإلكترونية وحرية التعبير.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) نقل المعلومات إلى الجمهور: يتناول أحكاماً عامةً حول مبدأ حرية نقل المعلومات إلى الجمهور عبر وسائل إلكترونية، والقيود المفروضة على هذا المبدأ، ودور مزود خدمات الشبكة ومستضيف البيانات فيما يتعلق بنقل المعلومات إلى الجمهور.

٢) النظام القانوني لمزودي خدمات الشبكات الإلكترونية: يتضمن الأحكام القانونية المنظّمة لنشاط مزودي خدمات الشبكات الإلكترونية وموجباتهم ومسؤولياتهم وتعاونهم مع السلطات العامة الأمنية والقضائية في سبيل المصلحة العامة وترسيخ العدالة.

٣) تشفير المعلومات: يتناول تراخيص استعمال وسائل التشفير واستيرادها وتصديرها ومسؤولية مزودي وسائل التشفير فيما يتعلق بخصوصية المعلومات والحالات التي يجب إفشاؤها بموجب حكم قضائي، ومسؤولية مزودي وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة.

٤) التنصت على الاتصالات الخاصة والشخصية: يتناول أحكاماً من شأنها منع التنصت أو المراقبة أو الاعتراض أو الإفشاء في ما خص الاتصالات الشخصية والخاصة. وإباحة التنصت في أحوال خاصة وفق القانون وبعد إجازة السلطات الدستورية والقضائية المختصة.

٥) أحكام جزائية: يتناول الأفعال موضوع التجريم والعقوبات المفروضة عند ارتكاب هذه الجرائم.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن المجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Directive 2002/58/EC of the European Parliament and of 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).

- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

- Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997.

- 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").

- DECLARATION on freedom of communication on the Internet (*Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies*).

- Online Privacy: Using the Internet Safely Privacy Rights Clearinghouse / UCAN. Posted July 1995. Revised December 2010.
http://www.privacyrights.org/fs/fs18-cyb.htm

- Privacy and Telecommunications: Do We Have the Safeguards? By Prashant Iyengar and Elonnai Hickok in Privacy — Nov 22, 2010.
http://www.cis-india.org/advocacy/igov/privacy-india/privacy-telecommunications

- Protecting communications against forgery, by Daniel J. Bernstein.
http://cr.yp.to/antiforgery/forgery-20080501.pdf

- Practical attacks against WEP and WPA, by Martin Beck, Erik Tews, November 8, 2008.
http://dl.aircrack-ng.org/breakingwepandwpa.pdf

- Security of the WEP algorithm, by Nikita Borisov, Ian Goldberg, and David Wagner.
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

- The Wireless Application Protocol (WAP), by Dave Singel´ee, Bart Preneel, September 2003.
http://www.citeseerx.ist.psu.edu

- The Status of Voice over Internet Protocol (VOIP) Worldwide, by the International Communication Union, 2006.
http://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf

- Wiretapping and Electronic Eavesdropping, Olmstead v. United States, Olmstead, Berger v. New York, Katz v. United States.
http://law.jrank.org/pages/19166/Wiretapping-Electronic-Eavesdropping.html

- Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping by Gina Marie Stevens and Charles Doyle American Law Division.
http://www.fas.org/sgp/crs/intel/98-327.pdf

- Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, 2009.
http://epic.org/privacy/wiretap/2005_wiretap_report.pdf

- Telecommunications Security Guidelines for Telecommunications Management Network, John Kimmins, Charles Dinkel, and Dale Walters. U.S. Department of Commerce.
http://csrc.nist.gov/publications/nistpubs/800-13/sp800-13.pdf

- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services.

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

- Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorizations and individual licenses in the field of telecommunications services.

٢) وتناولت أعمال البحث أيضا مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة عالجت تنظيم الاتصالات الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، الفنلندية، السويسرية، البريطانية، والأسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول آسيا الوسطى.

٣) كما تم الاسترشاد بالمراجع الفقهية العالمية والعربية الخاصة بالاتصالات الإلكترونية وحرية التعبير وخصوصية البيانات:

- Encryption over IP-proof.
http://www.frequentis.com/NR/rdonlyres/7A85E0DD-518B-429C-9E18-BC6FC3D6758A/0/Frequentis_Line_Encryption.pdf

- The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy, by Jim Dempsey , September 22, 2010.
http://www.cdt.org/testimony/electronic-communications-privacy-act-promoting-security-and-protecting-privacy

-Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010.
http://judiciary.house.gov hearings/pdf/Blaze100624.pdf

- "Lex Nokia" And Confidentiality In Electronic Communications In Finland, Posted July 26, 2010 *By Eija Warma, of Castren & Snellman, Helsinki, Finland*.
http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland/

- Optimizing Cost and Performance in Online Service Provider Networks, by Zheng Zhang Purdue University, Ming Zhang Microsoft Research, Albert Greenberg Microsoft Research, Y. Charlie Hu Purdue University, Ratul Mahajan Microsoft Research, Blaine Christian Microsoft Corporation.
http://research.microsoft.com/en-us/um/people/ratul/papers/nsdi2010-entact.pdf

- Data Encryption- Post note by UK Parliamentary Office of Science and Technology, October 2006, available:
http://www.parliament.uk/documents/post/postpn270.pdf

- IS Auditing Procedure: P9 Evaluation of Management Controls Over Encryption Methodologies, by Information Systems Audit and control Association,
http://www.isaca.org/Knowledge-Center/Standards/Documents/P9EvalofMgmtControlsOverEncryptionMethodologie.pdf

- محاضرات الدكتور وسيم حرب – الدراسات العليا في القانون، كلية الحقوق - الجامعة اللبنانية، ١٩٩٥-٢٠٠٥، مكتب المحاماة والاستشارات القانونية والتحكيم.

- تشفير الاتصال باستخدام معايير WEP & WPA، للمؤلفة عالية تركي عبد الرحمن الحربي
http://coeia.edu.sa/images/stories/PDFs/Encrypted_communication_using_criteria_WEp__WPA.pdf

- أمن الشبكات اللاسلكية – توجيهات التمارين التطبيقية، إعداد: ألبيرتو إسكوديرو باسكال، T+46، النسخة العربية: أنس طويلة.
http://www.itrainonline.org/itrainonline/mmtk/wireless_ar/15_Wireless_Security/15_ar_mmtk_wireless_security_exercisesguidelines.doc

٥) وقد تم الاسترشاد أيضاً بالدراسات التي أعدتها منظمة الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق، ٢- وضع التشريعات السيبرانية في سلطنة عمان، دولة الإمارات العربية المتحدة، دولة قطر، ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٦) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق، وأبرزها الاستراتيجيات العربية والوطنية الخاصة بتكنولوجيا الاتصالات والمعلومات، ونذكر بعضها:

- الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات (٢٠٠٧-٢٠١٢).
http://www.aticm.org.eg/upload/ICTJuly2008.doc

- الإستراتيجية الوطنية لمجتمع عمان الرقمي (سلطنة عمان).
http://www.ita.gov.om/ITAPortal_AR/Services/eoman_strategy_C3.aspx?NID=110

- الاستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات (فلسطين).
http://www.mtit.gov.ps/index.php?option=com_content&task=view&id=28&Itemid=56

- استراتيجية تقانات الاتصالات والمعلومات للتنمية الاقتصادية والاجتماعية حتى ٢٠١٣ (سوريا).
http://www.reefnet.gov.sy/home/StrategySummary.doc

- الخطة الوطنية لتكنولوجيا المعلومات والاتصالات (السعودية).
http://coeia.edu.sa/index.php/ar/about-coeia/strategic-plan.html

- الرؤية الإستراتيجية لوزارة الاتصالات وتقنية المعلومات ٢٠٠١- ٢٠٢٥ (اليمن).
http://www.ptc.gov.ye/

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم الاتصالات الإلكترونية ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شمولية النقاط التي يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- التشريعات الوطنية الخاصة بالاتصالات الإلكترونية وحرية التعبير في منطقة الإسكوا

تبين أثناء أعمال البحث أن دول الإسكوا عملت على إصدار تشريعات خاصة بتنظيم الاتصالات، وهي التالية:

١- الاردن:

- قانون الاتصالات رقم (١٣) لسنة ١٩٩٥
http://www.trc.gov.jo/index.php?option=com_content&task=view&id=144&Itemid=378&lang=arabic

٢- الإمارات العربية المتحدة:

قانون اتحادي رقم (٣) لسنة ٢٠٠٣م وتعديلاته بشأن تنظيم الاتصالات
http://www.theuaelaw.com/vb/showthread.php?t=711

٣- البحرين:
- مرسوم بقانون رقم ٤٨ لسنة ٢٠٠٢ باصدار قانون الاتصالات
http://www.legalaffairs.gov.bh/htm/L4802.htm

- مرسوم سلطاني رقم ٣٠/ ٢٠٠٢ الخاص بانشاء "هيئة تنظيم الاتصالات"

٤- سلطنة عمان:
- قانون تنظيم الاتصالات بموجب المرسوم السلطاني رقم ٣٠ لسنة ٢٠٠٢ الخاص بتنظيم الاتصالات
http://www.tra.gov.om/newsite1/telecomActAr.aspx?Menu_ID=67&Lang=2

٥- سوريا:
- قانون رقم ١٨ لسنة ٢٠١٠ الخاص بالاتصالات
http://www.qun-engineer.org.sy/docs/communicationlaw.pdf

٦- السودان:
- قانون الاتصالات لسنة ٢٠٠١
http://www.moj.gov.sd/laws_3/10/5.htm

٧- العراق:
- قانون الاتصالات اللاسلكية رقم (١٥٩) لسنة ١٩٨٠
http://www.iraq-ild.org/PDF/1980/z1392.pdf

٨- فلسطين:
- قانون الاتصالات الفلسطيني لسنة ٢٠٠٥
http://www.pogar.org/publications/other/laws/media/telecomm-pal-05-a.pdf

٩- قطر:
- مرسوم بقانون رقم ٣٤ لسنة ٢٠٠٦ باصدار قانون الاتصالات
http://www.ict.gov.qa/files/law(1).pdf

١٠- الكويت:
- مشروع قانون الاتصالات الكويتي عام ٢٠١٠
http://www.eastlaws.com/News/News.aspx?ID=3928

١١- لبنان:
قانون تنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية رقم ٤٣١ - صادر في ٢٢/٧/ ٢٠٠٢
http://www.tra.gov.lb/Library/Files/Uploaded%20files/Law431/Law-431.htm

- نظام التراخيص الممنوحة لمقدمي الخدمات
http://www.tra.gov.lb/Licensing-regulation-AR

١١-مصر:
- قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣
http://www.pogar.org/publications/other/laws/media/telecommorg-egy-03-a.pdf

١٣- السعودية:
- مرسوم ملكي رقم م/١٢ الصادر في ١٤٢٢/٣/١٢ هـ الخاص بنظام الاتصالات
http://www.mcit.gov.sa/NR/rdonlyres/8E82B7E1-DAB5-4386-ABD8-2CAC7601FAA6/0/TeleAct1.pdf

- لائحة النظر في مخالفات نظام الاتصالات
http://www.citc.gov.sa/NR/rdonlyres/0D52804A-BE7C-4E8B-A54C-74D800CF5862/0/Laeehat_AlNadhar.pdf

١٤- اليمن:
مشروع قانون الاتصالات وتقنية المعلومات
http://www.mtit.gov.ye/index.php?q=news_d&id=342

ب - شمولية التشريعات الوطنية الخاصة

لقد كرست جميع الدساتير العربية مبدأ سرية المراسلات والاتصالات السلكية وحدد بعضها مبدأ عدم جواز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي. مثال الدستور اليمني حيث نصت المادة ٥٣ منه: "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي".

أكدت بعض قوانين الاتصالات الوطنية الخاصة على سرية وخصوصية الاتصالات. مثال: قانون البحرين رقم ٤٨ لسنة ٢٠٠٢ الخاص بتنظيم الاتصالات حيث نصت المادة ٣ منه: "أن من مهام وصلاحية هيئة تنظيم الاتصالات حماية البيانات الخاصة وخصوصية الخدمات".

وقد حدد القانون السعودي لتنظيم الاتصالات الصادر عام ٢٠٠١ في المادة ٩ منه: "أن سرية المكالمات الهاتفية والمعلومات التي يتم إرسالها أو استقبالها عبر شبكات الاتصالات العامة مصونة. ولا يجوز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات التي تبينها الأنظمة".

كما وحدد قانون الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣ في البند ٦ من المادة ٥ منه. أن من مهام الجهاز القومي لتنظيم الاتصالات : "٦- وضع القواعد التي تضمن حماية المستخدمين بما يكفل سرية الاتصالات وتوفير أحدث خدماتها.."

أما القانون السوري الصادر عام ٢٠١٠ فقد نص في المادة ٣ منه، على أن من مهام الهيئة الناظمة لقطاع الاتصالات، (الفقرة (و) من البند ٤) "الحفاظ على سرية المعلومات الناجمة عن تقديم الخدمات وخصوصيتها". كما وأفرد هذا القانون باباً خاصاً لحماية البيانات والخصوصية والأمن القومي. فقد ورد في المادة ٥٠: " (أ)...تكون للاتصالات بين المستخدمين صفة الخصوصية. (ب) يتخذ كل مرخص له جميع الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين لديه. (ج) تحدد اللائحة التنفيذية لهذا القانون شروط حماية خصوصية بيانات الحركة وخصوصية بيانات موقع المشترك".

وعملت قوانين أخرى خاصة بتنظيم الاتصالات على فرض عقوبات عند مخالفة هذه الأحكام وخرق أمن شبكة الاتصالات، مثال الإمارات العربية المتحدة حيث جاء في المادة ٧٢ من قانون تنظيم قطاع الاتصال لسنة ٢٠٠٣: "يعاقب بالحبس مدة لا تزيد عن كل من استغل أجهزة الاتصالات في الإساءة أو الإزعاج أو إيذاء مشاعر الآخرين أو لغرض أخر غير مشروع. كل من نسخ أو أفشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية أو أي من خدمات الاتصالات".

أما القانون المصري الخاص بتنظيم الاتصالات فقد نص في المادة ٧٣ منه "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تزيد كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال التالية: ١ - إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها. ٢- إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات. ٤- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق".

واكتفت بعض الدول العربية بالإحالة إلى قوانين عامة عند خرق مبدأ سرية الاتصالات، مثال قانون العقوبات اللبناني حيث جاء في الفصل الثاني من الباب الثامن: "في الجرائم الواقعة على الحرية والشرف" وقد تضمّن هذا الفصل نبذة خاصة عنوانها "في إفشاء الأسرار" (المواد من ٥٧٩ إلى ٥٨١).

كما وحددت القوانين الخاصة بتنظيم الاتصالات مسؤولية وواجبات مقدمي خدمات الاتصالات في المحافظة على سرية المعلومات، ونذكر منها على سبيل المثال: قانون قطر رقم ٣٤ لسنة ٢٠٠٦ الخاص بإصدار قانون الاتصالات والذي نص في المادة ٥٢ منه: (حماية معلومات العملاء) "على مقدمي الخدمة عند إدارة شبكاتهم ومرافقها والأنظمة المتصلة بها مراعاة حقوق الخصوصية للعميل. وتقع عليهم مسؤولية حفظ المعلومات والبيانات الخاصة بالعميل وباتصالاته التي تكون بحيازتهم، وعليهم توفير الحماية الكافية لها، ولا يجوز لمقدم الخدمة جمع أي معلومات أو استعمالها أو الاحتفاظ بها أو إعلانها عن أي عميل إلا بموافقته أو وفقاً لما يسمح به القانون.

وعلى مقدمي الخدمة التأكد من أن المعلومات المقدمة صحيحة وكاملة وصالحة لغرض استعمالها. وللعملاء الحق في أن يطلبوا تصحيح أو حذف أي معلومات خاصة بهم . وليس في أحكام هذه المادة ما يمنع السلطات المختصة من الحصول على أي معلومات سرية أو اتصالات خاصة بالعملاء وفقاً للقانون".

كما ونص القانون اللبناني رقم ٤٣١ لسنة ٢٠٠٢ الخاص بتنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية، في المادة ٣٨ – (إجراءات المراقبة والتفتيش): "تعتبر المعلومات التي يطلع عليها المراقبون والمفتشون في معرض تنفيذهم لمهامهم سرية ولا يجوز لهم البوح بها إلا أمام رؤسائهم التسلسليين أو بناءً على طلب المرجع القضائي المختص. كما تطبق أحكام السرية على كل من يطلّع على هذه المعلومات بحكم عمله في الهيئة أو الوزارة".

كما وأكدت الاستراتيجيات الوطنية لتكنولوجيا المعلومات والاتصالات على السرية وحماية خصوصية البيانات، ونذكر ما ورد في بعض منها على سبيل المثال:

- الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات - بناء مجتمع المعلومات حتى ٢٠١٢، التي خصصت المحور الرابع منها لبناء الثقة والأمن في استخدام تكنولوجيا الاتصالات والمعلومات.

وفيما يلي الخطوط الرئيسية لتنفيذ هذا المحور: "

- المساهمة في تأمين وإدارة حقوق النشر الرقمية على شبكة الإنترنت وصياغة السياسات الملزمة لمكافحة التعدي على حقوق الملكية الفكرية.
- التعاون على المستوى الدولي لمكافحة جرائم الفضاء الالكتروني وإساءة استخدام تكنولوجيا الاتصالات والمعلومات.
- وضع وتفعيل تشريعات حماية البيانات وحماية خصوصية المواطن العربي.
- توفير أمن المعلومات والشبكات لضمان خصوصية المستخدم.
- إصدار قوانين وتشريعات تجرم اختراق الشبكات".

- الاستراتيجية الوطنية لمجتمع عمان الرقمي (سلطنة عمان): "إضافة إلى ذلك فقد تم إنشاء مركز البيانات الوطني ومقره هيئة تقنية المعلومات وذلك بالتنسيق مع الجهات الحكومية المهتمة ليعمل على ضمان استمرارية العمل وتحسين الكفاءة وتقليل التكلفة إلى جانب توفير بيئة آمنة للوصول للخدمات الإلكترونية على مدار الساعة والمحافظة على البيانات والمعلومات من حيث سريتها وسلامتها وحماية خصوصيتها."

- الاستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات (فلسطين)، التي حددت ضمن أهدافها العامة:
"٨. تسهيل الوصول إلى المعلومات والمعرفة واستخدام الإنترنت بشكل سريع وآمن لجميع شرائح المجتمع.
١١. حماية البيانات الفردية وخصوصيات الأفراد."

- استراتيجية تقانات الاتصالات والمعلومات للتنمية الاقتصادية والاجتماعية حتى ٢٠١٣ (سوريا)، حيث نصت على ما يلي: "برنامج بناء قطاع تقانة المعلومات: الذي يقوم على الإسراع بنشر الإنترنت في سورية؛ وعلى وضع قانون حديث لقطاع المعلوماتية، يعالج مواضيع خصوصية المعلومات، وحق الحصول على المعلومة العامة، وحقوق المعاملات والتوقيع الإلكتروني، والقواعد المتعلقة بالجرائم الإلكترونية؛ وعلى تنظيم المهنة".

- الخطة الوطنية لتكنولوجيا المعلومات والاتصالات (السعودية)، التي نصت على ما يلي: " بالإضافة إلى ذلك سيعمل مركز التميز لأمن المعلومات على تعليم مهندسين مؤهلين ليكونوا متخصصين في مجال أمن المعلومات و تشجيع الأفراد الموهوبين وكذلك الأفكار المتعلقة بمجال أمن المعلومات ليتم تحويلها إلى مشاريع ومنتجات تحت مسمى (صنع في المملكة العربية السعودية)".

هوامش

١– تراجع لائحة تشريعات الدول الأجنبية.

مقدمة إرشاد الاتصالات الإلكترونية وحرية التعبير

يرتدي الإرشاد الخاص بالاتصالات الإلكترونية وحرية التعبير أهمية خاصة بالنسبة لمجموع التشريعات السيبرانية، نظراً لأنه يتناول الجانب التقني والعملي الخاص بتحديد هويات الأطراف التي تقوم بتزويد خدمات الاتصال ونوعية ومدى مسؤوليتها. ولأن تحديد التبعة القانونية الناجمة عن أي مخالفة أو التعرض للاتصالات الإلكترونية يجب أن يستند إلى أدلة إلكترونية أو رقمية بشكل أساسي، ولتحديد مهام الأطراف المعنية بتلك الاتصالات، كان لا بد من تقنين جوانب الاتصالات الإلكترونية كافة.

مع تزايد وتنوع عدد المشتركين المتصلين بالإنترنت، ومع التطور الحاصل في إمكانية التواصل بوسائل إلكترونية بين المشتركين، فقد أصبح نقل المعلومات والبيانات الرقمية بواسطة الشبكات الإلكترونية أمراً شائعاً[1] مستعملاً على نطاق واسع في جميع الأنشطة الاقتصادية والاجتماعية والرسمية والخاصة[2]، نظراً لسرعة وسهولة التواصل بهذه الطريقة ولسهولة الولوج إلى البيانات على شبكة الانترنت. وللبيانات الرقمية المنقولة في بعض الأحيان أهمية خاصة، بحيث يؤدي إفشاؤها أو التعرض لها أو تحريفها إلى أضرار كبيرة ومسؤولية قانونية تترتب على عدد من الجهات غير المرتبطة مباشرةً بمن قام بأفعال الإفشاء أو التعرض أو التحريف. كما قد تشكل هذه البيانات المخزّنة أو المنقولة إلى الجمهور تعدياً على حقوق بعض الأشخاص، كحالة التعدي على الملكية الفكرية، ومن قبيل ذلك النسخ غير المشروع للأفلام أو الأغاني أو القدح والذم على موقع معين بحق شخص معين أو الترويج لنشاطات إجرامية ممنوعة. كما قد تكون الأدلة الإلكترونية حاسمة في إثبات عناصر بعض الجرائم الجزائية والوقائع المادية لا سيما تلك الجرائم المرتكبة بوسائل إلكترونية أو بواسطة شبكة الإنترنت أو التي يكون فيها جهاز الحاسوب أو برمجياته محلاً لها. ويقتضي إثبات هوية مُرسل الرسالة الإلكترونية أو مصدرها أو تاريخ إرسالها أو استلامها وتحديد الحاسب الخادم[3] الذي صدرت عنه. وقد نشأ بالتالي تخوف من وسائل نقل المعلومات بالطرق الإلكترونية، مما قد يحدو البعض إلى تقييدها بشكل مطلق وعدم السماح بها إلا بموجب تراخيص وحالات خاصة.

في مواجهة التحديات المذكورة الناشئة عن نقل المعلومات والبيانات بوسائل إلكترونية وتخزينها مؤقتاً لهذا الغرض، يلجأ المتعاملون عادةً إلى بعض الوسائل التقنية لحماية أنفسهم كتشفير[4] المعلومات المنقولة[5] لحفظ سريتها أو ضمان موثوقيتها، أو منع مزودي خدمات الإنترنت إظهار بعض المواقع المحظورة أو المسيئة أو قيام مستضيفي البيانات بحفظ معلومات كافية عن الأشخاص الذين يستضيفون بياناتهم. إلا أن هذه الحماية التقنية هي استنسابية وخاصة، أي أنها قد لا تكون شاملة وبالتالي فهي غير كافية ولا تُغني عن الحماية القانونية[6]. ويفترض تدخل المشترع لسن تشريعات واضحة تؤكد على مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية، ولكن ضمن ضوابط تتعلق بالنظام العام والسلامة العامة. كما تنظم هذه التشريعات عمل مزودي خدمات الاتصال ومستضيفي البيانات وموجباتهم ومسؤولياتهم لاسيما لجهة محتوى ومشروعية المعلومات المنقولة والمخزّنة من قبلهم، وإلزامهم بحفظ البيانات التقنية ومعلومات حركة البيانات والمعلومات التي تبين هوية الناشرين لديهم، وتقديمها للسلطات الأمنية والقضائية للمساعدة في التحقيقات وكشف الأدلة حول الجرائم. وتنظم التشريعات وسائل التشفير والترخيص لها ومنع إساءة استعمالها لارتكاب جرائم أو للمس بالأمن الوطني. كما تؤكد هذه التشريعات على خصوصية الفرد، بحيث تمنع التنصّت على الاتصالات الخاصة والشخصية إلا ضمن الضوابط التي يضعها القانون وتحت رقابة السلطات الدستورية والقضائية في الأحوال التي يجيزها القانون.

يأتي هذا الإرشاد حول الاتصالات الإلكترونية وحرية التعبير ليشكل إطاراً قانونياً متكاملاً في هذا المجال. وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام ٢٠٠٠ المتعلق بالتجارة الإلكترونية، وبالقانون الفرنسي رقم ٢٠٠٤/٥٧٥ الصادر بتاريخ ٢٠٠٤/٦/٢١ حول الثقة في الاقتصاد الرقمي، وبالقوانين الأسترالية حول تنظيم الاتصالات (قانون عام ١٩٧٩ وقانون عام ١٩٩٧) وبالقوانين الأجنبية والوطنية المختلفة في حقل إعداد نصوص الإرشاد الحالي الموجه للدول العربية حول الاتصالات الإلكترونية وحرية التعبير.

لقد تم تقسيم القانون الاسترشادي المُقترح على خمسة أبواب تتناول مسائل الاتصالات الإلكترونية وحرية التعبير وخصوصية البيانات، وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: النظام القانوني لمزودي خدمات الشبكات الإلكترونية.
الباب الثالث: تشفير المعلومات.
الباب الرابع: التنصّت على الاتصالات الخاصة والشخصية.
الباب الخامس: أحكام جزائية.

شروحات حول الإرشاد المتعلق بالاتصالات الإلكترونية وحرية التعبير

يتضمن **الباب الأول** المعنون «أحكام عامة» تعاريف لبعض المصطلحات التقنية والمفاهيم المُستعملة في متن الإرشاد. وكذلك يورد الباب الأول مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية ويضع لهذا المبدأ ضوابط. وتضع المادة ١ من الإرشاد تعاريف لنقل المعلومات للجمهور بوسيلة إلكترونية ولنقل المعلومات للجمهور على الخط ولمزود خدمات الشبكات الإلكترونية ولمزود خدمة الاتصال ولمستضيف البيانات وللمعلومات المتعلقة بحركة البيانات ولتخزين المعلومات مؤقتاً وانتقالياً ولتشفير المعلومات ولوسائل تشفير المعلومات.

تعرّف المادة ١ من الإرشاد نقل المعلومات للجمهور بوسيلة إلكترونية، فهو كل وضع بتصرف الجمهور أو فئات منه، بواسطة وسائل اتصالات إلكترونية، لإشارات أو كتابات أو صور أو أصوات أو رسائل من أية طبيعة كانت، والتي ليس لها طابع المراسلات الخاصة. فالعناصر التي تؤلف هذا المفهوم هي: الوضع بتصرف الجمهور لرسائل أياً كانت طبيعتها، واستعمال وسائل اتصالات إلكترونية، وأن لا يكون للرسائل طابع المراسلات الخاصة. أما نقل المعلومات للجمهور على الخط، فهو كل نقل، بناء لطلب فردي، لبيانات أو لمعلومات رقمية ليس لها طابع المراسلات الفردية، بواسطة وسائل اتصالات إلكترونية، تسمح بتبادل المعلومات بين المُرسل والمُستقبل. فهنا يجب أن يكون إرسال المعلومات بناء لطلب يُرسل من شخص معين. وهذا وجه الاختلاف مع المفهوم الأول. ويمكن أن يتم إرسال واستقبال المعلومات بشكل تفاعلي Interactive. ويُعرّف مزود خدمات الشبكات الإلكترونية[٧] بأنه إما مزود خدمة الاتصال أو مستضيف للبيانات. مزود خدمة الاتصال هو من يتيح للمستخدم الدخول إلى شبكة اتصالات ويمكّنه من نقل المعلومات عبرها. أما مستضيف البيانات، فهو من يتولى تخزين المعلومات العائدة للغير لديه، ولحساب هذا الغير، مقابل بدل مادي أو مجاناً. كما يتولى وضع هذه المعلومات بتصرف الجمهور من خلال استخدام شبكات الاتصال. بالتالي، على سبيل المثال، على كل شخص يرغب في التصفح على الإنترنت، الحصول على خدمة الوصول إلى شبكة الإنترنت والدخول إليها من خلال مزود خدمة الاتصال. أما الشخص الراغب في إنشاء موقع له على الإنترنت، فعليه وضع معلومات محتوى موقعه على الحاسب الخادم لدى مستضيف البيانات، للتمكّن من عرضها على شبكة الإنترنت.

وتعرّف المادة ١ من الإرشاد المعلومات المتعلقة بحركة البيانات[٨] بأنها أية معلومات تتعلق بعملية نقل للبيانات أو اتصال عبر شبكة إلكترونية، ينتجها النظام المعلوماتي المرتبط بالشبكة الإلكترونية، وتحدد هذه المعلومات مصدر الاتصال أو مُرسل البيانات والمُرسل إليه أو المُتلقي وخريطة طريق إرسال المعلومات ووقت الإرسال وتاريخه وحجم البيانات المُرسلة ومدة الإرسال وغيرها من المعلومات التقنية. فهذه المعلومات هي معلومات تقنية غير مرئية من قبل المستخدم العادي، ولا تهمه في المبدأ، ولا يعرف معظم المستخدمين بوجودها بالرغم من أنها تُحفظ لكل منهم على شبكات نقل المعلومات. وتشكل دليلاً أساسياً في التحقيقات القضائية الرامية إلى اقتفاء أثر الرسائل الإلكترونية المُرسلة على الشبكات الإلكترونية وتحديد مصدرها وهوية مُرسلها. ويقتضي تحديد المقصود بتخزين المعلومات انتقاليا ومؤقتاً وتمييزه عن التخزين النهائي للمعلومات الذي يتم بقصد الحفظ النهائي لسنوات عديدة وبقصد الاسترجاع لاحقاً، إذ أن التخزين الانتقالي أو المؤقت يتمّ بقصد نقل المعلومات كون وتيرة النقل لا تستوعب كل المعلومات دفعة واحدة، مما يحتّم إرسال المعلومات على دفعات، ومما يفرض تخزينها مؤقتاً لحاجات النقل. إن تخزين المعلومات انتقالياً ومؤقتاً يعني أن التخزين يخدم حصرياً تنفيذ عملية نقل هذه المعلومات على شبكة الاتصالات، ويشترط أن لا تزيد مدة التخزين عن الوقت المعقول اللازم لنقل المعلومات. فعمليات نقل المعلومات تشمل بطبيعتها التخزين الآلي المؤقت والوسيط أو الانتقالي للمعلومات المُرسلة ضمن الشرطين المذكورين أعلاه[٩].

تعرّف المادة ١ من الإرشاد وسائل تشفير المعلومات[١٠] بأنها تعني التجهيزات أو البرامج المعدّة من أجل تحويل البيانات، عبر اتفاقات سرية، أو من أجل تحقيق العملية المعاكسة. تهدف وسائل التشفير إلى ضمان سرية المعلومات المخزّنة أو المُرسلة أو تأمين سلامتها أو موثوقيتها. وإن تشفير المعلومات[١١] هو عملية تحويل المعلومات عبر اتفاقات سرية إلى رموز غير مفهومة بحيث ينبغي إعادتها إلى حالتها الأصلية لأجل قراءتها وفهمها. فالتشفير وفك التشفير يجريان بالاستناد إلى اتفاق سري يُبرم بين مُستقبل الرسالة ومُرسلها، بحيث إذا علم بهذا الاتفاق شخص ثالث تمكّن من قراءة محتوى الرسالة المُشفّرة[١٢]. فالرسالة المُشفرة تكون غير مفهومة من قبل الغير حتى لو تمكّن من اعتراضها. فعلى سبيل المثال البدائي عن التشفير، يقوم مُرسل الرسالة بتشفير الرسالة عبر كتابة الكلمات معكوسة بينما يفك مُستقبل الرسالة التشفير عبر عكس كل كلمة لاستعادة صيغتها الأصلية[١٣].

وحفاظاً على الحريات العامة وتحفيزاً للنشاط الاقتصادي والثقافي، تعلن المادة ٢ من الإرشاد مبدأ حرية نقل المعلومات للجمهور بوسيلة إلكترونية. فيمكن بالتالي استعمال شبكة الإنترنت بشكل حر لإنشاء المواقع عليها وعرض المعلومات والخدمات الإلكترونية ضمن أحكام القانون. ولكن المادة ٢ تضع لهذا المبدأ قيوداً، فلا يمكن الحد من ممارسة هذه الحرية إلا ضمن حدود احترام كرامة الإنسان وحرية الغير وملكيته وتعدد الآراء، ومن جهة أخرى ضمن حدود حماية النظام العام وحاجات الدفاع الوطني ومتطلبات المرافق العامة والمتطلبات التقنية لوسائل الاتصال. وأن تحترم حرية التعبير نظام حماية البيانات الشخصية.

يتضمن **الباب الثاني** المعنون «النظام القانوني لمزودي خدمات الشبكات الإلكترونية» الأحكام القانونية المنظّمة لنشاط مزودي خدمات الشبكات الإلكترونية وموجباتهم[١٤] ومسؤولياتهم[١٥] وتعاونهم مع السلطات العامة الأمنية والقضائية في سبيل المصلحة العامة وترسيخ العدالة.

تنظّم المادة ٣ مسألة تقييد الوصول إلى بعض المواقع والخدمات الإلكترونية وذلك حمايةً لبعض المعتقدات أو لحماية الأطفال[١٦] أو لحصر استخدام الإنترنت في الشركات والمؤسسات للعمل دون اللهو، وغيرها من الأمور. وبالتالي يجب بالتالي على مزود خدمة الاتصال أن يُعلم المستخدمين بوجود وسائل تقنية تسمح بتقييد الوصول إلى بعض المواقع الإلكترونية أو الخدمات الإلكترونية أو بالاختيار منها. وعلى مزود خدمة الاتصال تقديم هذه الوسائل للمستخدمين. وهذا الموجب هو موجب أساسي يقع على عاتق مزود خدمة الاتصال.

تعرض المادة ٤ من الإرشاد مسألة مدى إلزام مزود خدمة الاتصال ومستضيف البيانات بإجراء رقابة على المعلومات[١٧]. فهذا الأمر قد يكون صعباً لا بل مستحيلاً من الناحية التقنية بالنظر لحجم المعلومات الهائل وغير المحدود. وبالنظر للطابع المعقّد لهذه المعلومات كتعدد اللغات وأشكال المستندات، وبالنظر للطابع الدائم التغيّر لهذه المعلومات. وبالتالي فقد أعفت التشريعات الحديثة مزودي خدمة الاتصال ومستضيفي البيانات من إجراء رقابة مستمرة على جميع المعلومات المنقولة أو المخزّنة. إلا أنه يتوجب عليهم مراقبة بعض المعلومات أو المواقع الإلكترونية المحدّدة لفترة معينة وذلك بناءً لقرار قضائي[١٨]. وفي هذا السياق، لا تُخضع المادة ٤ من الإرشاد مزود خدمة الاتصال ومستضيف البيانات لموجب رقابة على مضمون المعلومات التي يرسلها أو يخزنها، ولا لموجب عام بالبحث عن الأعمال المتعلقة بنشاطات غير مشروعة[١٩]. يُستثنى من ذلك حالة صدور قرار قضائي يُلزم مزود خدمة الاتصال أو مستضيف البيانات بإجراء مراقبة مؤقتة ومحدودة لمعلومات محدّدة. إلا أن انتفاء موجب الرقابة على مستضيف البيانات لا يعفيه من موجب التصرف في حال علم بطابعها غير المشروع. فهو يبقى غير مسؤول طالما لم يكن يعلم بالطابع غير المشروع للمعلومات، ويصبح مسؤولاً إذا علم بهذا الطابع ولم يقدم فوراً على سحب هذه المعلومات أو جعل الوصول إليها مستحيلاً[٢٠]. وقد أثار المجلس الدستوري الفرنسي بموجب قراره رقم ٤٩٦ تاريخ ١٠ حزيران ٢٠٠٤ إشكالية وجوب كون الطابع غير الشرعي للمعلومات ظاهراً أو مُسنداً إلى قرار قضائي بسحب المعلومات، ولا يكفي إدلاء شخص ثالث بعدم مشروعية المعلومات. كذلك، يكون مزود خدمة الاتصال مسؤولاً إذا لم يمحُ المعلومات المخزّنة مؤقتاً بناءً على طلب مُرسلها، وكذلك بناءً لقرار صادر عن المحاكم. وهذا النظام لمسؤولية مزود خدمة الاتصال ينبع من الطابع المؤقت للتخزين مع انتفاء موجب الرقابة على المعلومات.

تنظّم المادة ٥ إجراءات إبلاغ مستضيف البيانات بالطابع غير المشروع للمعلومات، بحيث إذا تمت هذه الإجراءات وفق الأصول، اعتبرت معرفة مستضيف البيانات للطابع غير المشروع متحققة وفعلية، وترتبت عليه المسؤولية من جراء ذلك. فالمعطيات المطلوب إبلاغها هي: تاريخ التبليغ، عناصر التعريف عن هوية المُبلّغ، اسم المُرسل إليه ومقره، وصف الأعمال المُنازع بها ومكان تمركزها، الأسباب التي تدعو لسحب المعلومات مع ذكر القواعد القانونية والتعليل[٢١].

تتناول المادة ٦ من الإرشاد كيفية تحديد هوية الناشر بوسائل إلكترونية وذلك لتمكين الغير من مداعاته في حال ارتكابه فعلاً ضاراً به أو جرماً جزائياً كالقدح أو الذم أو انتهاك حقوق الملكية الفكرية. وتفرّق المادة ٦ في هذا الصدد بين الناشر المحترف والناشر غير المحترف. فيحق للأخير فقط إبقاء هويته سرية شرط تقديم عناصر التعريف الشخصية عنه لمستضيف البيانات الذي يخزّن معلوماته، وشرط تقديم عناصر التعريف العائدة لمستضيف البيانات للجمهور. وفي هذه القاعدة نجد تسهيلاً على الأفراد ولكن في نفس الوقت حفظاً لحقوق الغير. أما الناشر المحترف، فيُلزم دوماً بنشر عناصر التعريف العائدة له، ضماناً لشفافية معاملاته الكثيرة والمتكررة مع الغير، وتمكيناً لهذا الغير من تقدير كفاءة المحترف ومن مساءلته مباشرةً عند إخلاله بواجباته. ويجب على مستضيف البيانات أن يحتفظ بالبيانات التي تعرّف بهوية كل ناشر لمدة لا تقل عن عشر سنوات، وذلك حتى يستطيع تقديمها في كل نِزاع مستقبلي قد يثار حول

المعلومات المنشورة. أخيراً، بطبيعة الحال، وبالنظر لخصوصية المعلومات المُسلّمة إليه، يخضع مستضيف البيانات لموجب السر المهني بخصوص عناصر التعريف الشخصية، باستثناء حالة وجود قرار قضائي.

توجب المادة ٧ على كل من مزود خدمة الاتصال ومستضيف البيانات حفظ المعلومات المتعلقة بحركة البيانات والعائدة لجميع المستخدمين الذين يستفيدون من خدماته وذلك لمدة لا تقل عن خمس سنوات، إلا أنه لا يخضع لموجب الحفظ مضمون المعلومات ذاتها المُرسلة أو المخزّنة، أو المراسلات المُتبادلة. فغالباً ما تحتاج التحقيقات الإدارية والقضائية إلى مثل هذه المعلومات، ولكن لا يستطيع مزودو خدمات الشبكات الإلكترونية تقديمها لعدم أخذهم أي احتياط بحفظها. وكان لا بد من فرض ذلك بموجب نص قانوني مُلزم لهم، إذ غالباً ما يُهمل مزودو خدمات الشبكات الإلكترونية حفظ هذه المعلومات أو لا تكون لديهم مصلحة هامة بحفظها. وبطبيعة الحال، وتبعاً لخصوصية هذه المعلومات واتصافها بالطابع الشخصي كونها تحدّد بشكل مباشر أو غير مباشر أنشطة الشخص وعاداته واهتماماته وأشغاله وأمكنة تواجده، أخضعت المادة ٧ مزودي خدمة الاتصال ومستضيفي البيانات لموجب السر المهني بخصوص معلومات حركة البيانات، باستثناء حالة وجود قرار قضائي. كذلك ألزمتهم المادة ٧ بصون المعلومات حول حركة البيانات من التدمير أو المحو أو التعديل أو الإفشاء. وأخيراً فرضت عليهم محوها بعد انقضاء مدة الحفظ القانونية المحدّدة بخمس سنوات.

فرضت المادة ٨ على مزودي خدمة الاتصال ومستضيفي البيانات تقديم معلومات حركة البيانات وهوية الأشخاص الذين يستفيدون من خدماتهم للسلطات القضائية والأمنية العاملة تحت إشرافها، وكذلك تمكين هذه السلطات من الوصول إلى المعلومات المنوه عنها وفقاً لوقت الإرسال الحقيقي لها عند حصول أي عملية اتصال. فالمعلومات المنوه بها لا تتوفر إلا لدى مزودي خدمة الاتصال ومستضيفي البيانات، إلا أنها هامة جداً في إجراء التحقيقات وجمع الأدلة، ويقتضي بالتالي إلزامهم بتقديمها ضماناً لحسن سير التحقيقات[٢٢].

تأتي المادة ٩ من الإرشاد في نفس سياق المادة ٨ السابقة، لجهة مساهمة مزود خدمة الاتصال ومستضيف البيانات في مكافحة بعض الجرائم. فوفقاً للمادة ٩، يجب أن يساهم كل من مزود خدمة الاتصال ومستضيف البيانات بمحاربة الجرائم ولاسيما الجرائم ضد الإنسانية أو جرائم الإباحية للقاصرين أو التحريض على العنف أو التعرض لكرامة الإنسان. وعلى مزود خدمة الاتصال أو مستضيف البيانات بالتالي أن يضع بتصرف الجمهور آلية واضحة وسهلة للإبلاغ عن الأفعال المذكورة في هذه المادة، وعليه بعد حصول التبليغ إعلام السلطات العامة بذلك. وهذه المادة تطبيق لمبدأ عام هو واجب كل مواطن وشخص في مؤازرة عمل القضاء وتقصي الجرائم، لاسيما إذا كان ممتهناً وتتوفر له كل الوسائل التقنية لهذه المؤازرة.

تتناول المادة ١٠ من الإرشاد المسؤولية التعاقدية لكل من مزود خدمة الاتصال ومستضيف البيانات. وهي تستعيد المبادئ العامة الواردة في النظرية العامة للعقود وتطبقها على هذه الحالة الخاصة. فوفق المادة ١٠ المذكورة، يكون مزود خدمة الاتصال ومستضيف البيانات مسؤولاً عن حسن تنفيذ موجباته المنصوص عنها في العقود الموقّعة مع عملائه. ويجب أن تتضمن هذه العقود تحديداً لنوعية الخدمة المقدمة ولمواصفاتها ولمدتها، وتنتفي مسؤولية مزود خدمة الاتصال ومستضيف البيانات إذا أثبت أن عدم تنفيذ العقد تجاه عميله أو سوء تنفيذه هو ناتج عن خطأ العميل أو عن القوة القاهرة أو عن فعل الغير. إن هذه المادة هي كلاسيكية وفق قواعد القانون المدني، إذ أن كل شخص يقدم خدمة ما يكون مسؤولاً عن حسن تقديمها.

تنظّم المادة ١١ من الإرشاد حق الرد للشخص المعني المذكور في عملية نقل للمعلومات للجمهور، إذ يتمتع كل شخص تم ذكر اسمه في عملية نقل للمعلومات إلى الجمهور بحق الرد، مع عدم الإخلال بطلبات التصحيح أو الإلغاء التي يستطيع توجيهها لمزود الخدمة. توجه طلبات ممارسة حق الرد خلال ثلاثة أشهر من تاريخ النشر إلى مدير النشرة، وفي حال عدم إفشائه لاسمه للجمهور، توجه الطلبات المنوه عنها إلى مستضيف البيانات الذي يخزّن المعلومات موضوع طلب الرد، وعلى مستضيف البيانات إرسال طلب الرد دون تأخير إلى مدير النشرة. فحق الرد هو تطبيق لمبدأ عام بحفظ حق الدفاع وتمكين كل شخص من إبداء وجهة نظره حول معلومات خاصة به، لاسيما أن مدى الضرر الناتج عن النشر الإلكتروني يفوق بأضعاف ذاك الناشئ عن النشر الورقي تبعاً لإمكانية الوصول لعدد غير محدود من الأشخاص عبر الشبكات الإلكترونية.

ينظم **الباب الثالث** المعنون «تشفير المعلومات» هذه المسألة لجهة تراخيص استعمال وسائل التشفير[٢٣] واستيرادها وتصديرها ولجهة مسؤولية مزودي وسائل التشفير.

تتناول المادة ١٢ من الإرشاد إجراءات الترخيص لاستعمال وسائل التشفير[٢٤] وتقديمها واستيرادها وتصديرها، ويُراعى في ذلك خطورة وسائل التشفير واستعمالاتها المزدوجة

المدنية والعسكرية وإمكانية استخدامها لارتكاب جرائم أو للتواصل مع العدو أو بين العصابات الإجرامية[٢٥]. ففي المبدأ، إن استعمال وسائل التشفير هو حر. لكن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن فقط وظيفة التوثيق أو تأمين سلامة المعلومات تخضع للترخيص أمام السلطات الرسمية المختصة. وللتخفيف من قسوة المبدأ المذكور، يمكن أن تحدّد كل دولة وسائل التشفير التي لا تخضع لأية معاملة رسمية، وذلك في ضوء متطلبات الحفاظ على الدفاع الوطني والأمن الداخلي والخارجي. كما أن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن وظيفة سرية المعلومات تخضع للترخيص من السلطات الرسمية المختصة. في جميع الأحوال، يجب أن يحدد طالب الترخيص المواصفات التقنية لوسائل التشفير.

تتطرق المادة ١٣ من الإرشاد إلى مسؤولية مزودي وسائل التشفير تبعاً للضرر الذي يمكن أن ينجم عن انكشاف البيانات المشفرة أو الاتفاقات السرية المتعلقة بها. وبطبيعة الحال، وتبعاً لخصوصية المعلومات المعنية، يخضع مزوّدو وسائل التشفير لموجب السرية إلاّ في حالة صدور قرار قضائي. باستثناء الحالة التي يثبتون فيها عدم حصول خطأ مقصود أو إهمال، وبالرغم من كل نص مخالف، يُسأل مزودو وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة. إنّ هذه المادة قلبت عملياً عبء الإثبات، وذلك لصعوبته من قبل المستخدمين بوجه طرف مُمتهن كمزود وسائل التشفير، إذ تكون مسؤولية مزود وسائل التشفير مُفترضة، إلا أنه يستطيع التحلل منها بإثبات عدم ارتكابه خطأ مقصوداً أو إهمالاً.

يتعرض **الباب الرابع** المعنون «التنصّت على الاتصالات الخاصة والشخصية» لحماية الاتصالات الخاصة والشخصية من التنصّت[٢٦]، وإباحة التنصّت في أحوال خاصة وفق القانون وبعد إجازة السلطات الدستورية والقضائية المختصة[٢٧].

فوفق المادة ١٤ من الإرشاد، يمنع التنصّت أو المراقبة أو الاعتراض أو الإفشاء في ما خص الاتصالات الشخصية والخاصة إلا في الأحوال التي يجيزها القانون. وقد أجازت المادة ١٥ من الإرشاد التنصّت أو مراقبة أو اعتراض اتصالات خاصة وشخصية[٢٨] بإذن قضائي من أجل ضرورات التحقيقات القضائية الجزائية، أو بإذن من السلطات الأمنية أو الدستورية المختصة، من أجل تجميع المعلومات لمكافحة الإرهاب والجرائم الواقعة على أمن الدولة والجرائم المنظّمة[٢٩]. فالمبدأ هو منع التنصّت على الاتصالات الخاصة والشخصية، والاستثناء هو السماح به لضرورات الأمن العام والسلامة العامة[٣٠]. إذ أن حماية خصوصية الفرد وحميميته هي هامة، وهامة جداً، إلا أنها لا يمكن أن تعلو على المصلحة العامة للمجتمع في أمنه وسلامته واستقراره بتأمين العدالة فيه.

يتناول الباب الخامس المعنون «أحكام جزائية» النصوص العقابية التي تضمن فعالية تطبيق هذا الإرشاد والتزام الفرقاء بالموجبات التي أنشأها على عاتقهم[٣١]. فالمادة ١٦ من الإرشاد تحدد الأفعال الواجبة التجريم وهي: فعل عدم تعاون مزود خدمات الشبكات الإلكترونية مع القضاء بتقديم معلومات حركة البيانات أو بسحب بيانات أو بمنع الوصول إليها متى طلب منه ذلك، وفعل مزود خدمة الاتصال أو مستضيف البيانات بعدم حفظ معلومات حركة البيانات وبيانات التعريف الشخصية وفق ما يفرضه القانون[٣٢]. وفعل شخص بتقديم معلومات غير صحيحة عن قصد لمزود خدمات الشبكات الإلكترونية لحمله على سحب معلومات أو منع الوصول إليها، وفعل عدم قيام مدير النشرة بنشر رد الشخص المعني وفقاً للمادة ١١ من هذا الإرشاد، وفعل تقديم أو تصدير أو استيراد وسائل تشفير بصورة غير مشروعة دون الحصول على الترخيص المطلوب من السلطات الرسمية، وفعل التنصّت على الاتصالات الإلكترونية الخاصة والشخصية بصورة غير مشروعة خارج الحالات التي يجيزها القانون[٣٣].

إن غاية النصوص العقابية المنوه بها هي ردع المعنيين عن مخالفة مضمون هذا الإرشاد وحثهم على تلبية متطلباته. ويعود لكل دولة عضو أن تحدد العقوبات الرادعة وفق سلم العقوبات المعتمد لديها مع الأخذ بعين الاعتبار الأضرار الكبيرة الناجمة عن الجرائم المنوه عنها.

هوامش

1- See ITU World Telecommunication/ICT Indicators database, available:
http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

- The number of Internet users has doubled between 2005 and 2010.
- In 2010, the number of Internet users will surpass the two billion mark, of which 1.2 billion will be in developing countries.
- A number of countries, including Estonia, Finland and Spain have declared access to the Internet as a legal right for citizens.
- With more than 420 million Internet users, China is the largest Internet market in the world.
- While 71% of the populations in developed countries are online, only 21% of the populations in developing countries are online. By the end of 2010, Internet user penetration in Africa will reach 9.6%, far behind both the world average (30%) and the developing country average (21%).
- By the end of 2010, there will be an estimated 5.3 billion million cellular subscriptions worldwide, including 940 million subscriptions to 3G services.
- Access to mobile networks is now available to 90% of the world population and 80% of the population living in rural areas.
- See Key Global Telecom Indicators for the World Telecommunication Service Sector, by International Telecommunication Union (2005-2010), available: http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html
- See OECD Broadband statistics, June 2010, available: http://www.oecd.org/dataoecd/21/35/39574709.xls

2- See Testimony of Prof. Matt Blaze, House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, June 24, 2010, available: http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf

3- Server: A network device that provides service to the network users by managing shared resources. Note 1- The term is often used in the context of a client-server architecture for a local area network (LAN). Note 2- Examples are a printer server and a file server. Available: http://myrtle.forest.net/

٤- راجع تشفير الاتصال باستخدام معايير WEP & WPA، للمؤلفة عالية تركي عبد الرحمن الحربي.
http://coeia.edu.sa/images/stories/PDFs/Encrypted_communication_using_criteria_WEp__WPA.pdf
التشفير هو عملية تحويل البيانات إلى طلاسم حتى إذا استطاع المهاجمون (Attackers) الوصول إلى البيانات المنقولة عبر الشبكة لا يستطيعون الاستفادة من هذه البيانات.

٥- يمكن اعتبار أن أولى استعمالات وسائل التشفير الكهربائي والميكانيكي في آن في العصر الحديث يعود إلى آلات Enigma الخاصة بالجيش الألماني أبان الحرب العالمية الثانية، والتي أدى فك تشفيرها من قبل الحلفاء إلى تسريع انتصارهم في الحرب.
http://en.wikipedia.org/wiki/Enigma_machine

6- See "Lex Nokia" And Confidentiality In Electronic Communications In Finland, July 26, 2010, available:
http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland/

In Finland, the Constitution guarantees everyone a basic right of privacy, and specifically states that "The secrecy of correspondence, telephony and other confidential communication is inviolable".

7- See Service Provider Designation of Agent to Receive Notification of Claims of Infringement, by United States Copyright Office, available: http://www.copyright.gov/onlinesp/
A "service provider" is defined as a provider of online services or network access, or the operator of facilities therefore, including an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
8- See the Internet Traffic Report (11/01/2001), available: http://www.internettrafficreport.com/
The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections.

9- See the Commonwealth Telecommunications (Interception and Access) Act 1979 (TIA Act) amended on 13 June 2006, is to protect the privacy of individuals who use the Australian telecommunications system, available: http://www.efa.org.au/Issues/Privacy/tia.html#storedcomms

Definition of Stored Communications

The TIA Act states:
Stored communication means a communication that:

(a) is not passing over a telecommunications system; and
(b) is held on equipment that is operated by, and is in the possession of, a carrier; and
(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

10- See Data Encryption- Postnote by UK Parliamentary Office of Science and Technology, October 2006, available: http://www.parliament.uk/documents/post/postpn270.pdf
Encryption is increasingly used to protect digital information, from personal details held on a computer to financial details transmitted over the Internet. Encryption has many benefits but can also be used to conceal criminal activity. This POSTnote outlines encryption techniques, their applications and their reliability. It also discusses controversial government proposals to give public authorities new powers under the Regulation of Investigatory Powers Act, relating to the handling of encrypted data in criminal investigations.

١١- يوجد عالمياً عدد كبير من وسائل التشفير، ومنها / GnuPG، Open VPN، Trucrypt، Nagra Vis، Conax، Beta Crypt، Irdeto، Viaccess
PGP، OpenSSL الخ. . .

12- Pretty Good Privacy (PGP) is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route. Available both as freeware and in a low-cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations. Developed by Philip R. Zimmermann in 1991, PGP has become a de facto standard for e-mail security. PGP can also be used to encrypt files being stored so that they are unreadable by other users or intruders. Available: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214292,00.html

13- *Communication Protocols:*
- Voice over Internet Protocol (VoIP) is referred to as and broadly includes Voice over Broadband (VoB), Voice over Digital Subscriber Line (DSL), Voice over Internet (VoI), Voice over Wireless Local Area Network and Internet telephony. http://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf

- *WEP Wired Equivalent Privacy*, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security. http://www.webopedia.com/TERM/W/WEP.html

- *WAP Wireless Application Protocol*, a secure specification that allows users to access information instantly via sand the low-bandwidth constraints of a wireless-handheld network. Although WAP supports HTML and XML, the WML language (an XML application) is specifically devised for small screens and one-hand navigation without a keyboard. WML is scalable from two-line text displays up through graphic screens found on items such as smart phones and communicators. WAP also supports WMLScript. It is similar to JavaScript, but makes minimal demands on memory and CPU power because it does not contain many of the unnecessary functions found in other scripting languages. Because WAP is fairly new, it is not a formal standard yet. It is still an initiative that was started by Unwired Planet, Motorola, Nokia, and Ericsson. http://www.webopedia.com/TERM/W/WAP.html

14- See Common Charter of Telecom Services, by Association of Unified Telecom Service Providers of India (AUSPI) 2005, available: http://www.auspi.in/pdf/Common-Charter-of-Telecom-Services-2005.pdf

15- See Data protection in the electronic communications sector, available: http://europa.eu/legislation_summaries/information_society/l24120_en.htm
The provider of an electronic communications service must protect the security of its services by:

- ensuring personal data is accessed by authorized persons only;
- protecting personal data from being destroyed, lost or accidentally altered;
- ensuring the implementation of a security policy on the processing of personal data.

In the case of an infringement of personal data, the service provider must inform the person concerned, as well as the National Regulatory Authority (NRA).

16- See US Code § 2258A. Reporting requirements of electronic communication service providers and remote computing service providers, available: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002258---A000-.html

17- See US Code 18 U.S.C. § 2511 (2)(A)(i) "It shall **not be** unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks." Available: http://www.cybertelecom.org/security/ecpaisp.htm

18- See Telecommunication Act of Australia 1997, available: http://www.acma.gov.au/WEB/STANDARD/pc=PC_100073
Section 324 of the Act requires an ISP to be able to intercept a communication passing over the ISP's network or facility in accordance with an interception warrant under the *Telecommunications (Interception) Act 1979*. In practice, when served with an interception warrant, the ISP will be required to intercept all traffic transmitted, or caused to be transmitted, to and from the identifier of the target service (for example, an electronic mail address) used by the interception subject and described on the face of the warrant. The ISP will need to deliver the intercepted communications to an agreed delivery point from which the intercepting agency may access those communications.

The ISP must also provide access to the traffic-related data generated to process the traffic. For interception of Internet traffic, traffic-related data will be the signaling information contained within the IP datagrams and, where applicable, the calling line identifier of the telephone service used by the interception subject to connect to the ISP.

19- See US Code 18 § 2258B. Limited liability for electronic communication service providers, remote computing service providers, or domain name registrar, available: http://www.law.cornell.edu/uscode/18/usc_sec_18_00002258---B000-.html

20- See Declaration on freedom of communication on the Internet, (Adopted by the Council of Europe Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers′ Deputies), available: https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031

Principle 6: Limited liability of service providers for Internet content
Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity. Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet. In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information. In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

21- See US Code 18 § 2258A. Reporting requirements of electronic communication service providers and remote computing service providers, available: http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002258---A000-.html

22- See Declaration on freedom of communication on the Internet, (Adopted by the Council of Europe Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers′ Deputies), available: https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031

Principle 7: Anonymity
In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

23- See Protecting communications against forgery, by Daniel J. Bernstein, available: http://cr.yp.to/antiforgery/forgery-20080501.pdf

24- See IS Auditing Procedure Evaluation of Management Controls over encryption methodologies, available: http://www.isaca.org/Knowledge-Center/Standards/Documents/P9EvalofMgmtControlsOverEncryptionMethodologie.pdf
Risk Assessment in use of Encryption - The most critical aspect of encryption is the determination of what data should be encrypted and where and when it should be encrypted.

25- In a *New York Times* article by Charlie Savage (September 27, 2010) news that the Obama administration is proposing new legislation that would provide the U.S. Government with direct access to all forms of digital communication, «including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct `peer to peer′ messaging like Skype to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.» In other words, the U.S. Government is taking exactly the position of the UAE and the Saudis: no communications are permitted to be beyond the surveillance reach of U.S. authorities. The new law would not expand the Government's legal authority to eavesdrop -- that's unnecessary, since post-9/11 legislation has dramatically expanded those authorities -- but would require all communications, including ones over the Internet, to be built so as to enable the U.S. Government to intercept and monitor them at any time when the law permits. In other words, Internet services could legally exist only insofar as there would be no such thing as truly private communications; all must contain a «back door» to enable government officials to eavesdrop.

Available: http://boingboing.net/2010/09/27/obama-administration.html

- The FRA law (*FRA-lagen* in Swedish) is a Swedish legislative package that authorizes the state to warrantlessly wiretap all telephone and Internet traffic that crosses Sweden′s borders. It was passed by the Parliament of Sweden on June 18, 2008, by a vote of 143 to 138 (with one delegate abstaining and 67 delegates not present) and took effect on January 1, 2009. In more detail, «FRA-law» is the common name for a new law as well as several modifications to existing laws, formally called Government proposal 2006/07:63 – Changes to defence intelligence activities (Swedish *proposition 2006/07:63 – En anpassad försvarsunderrättelseverksamhet*). It was introduced as anti-terrorism legislation, and gives the government agency Swedish National Defence Radio Establishment (FRA, Swedish *Försvarets radioanstalt*) the right to conduct signals intelligence on - to intercept - all internet exchange points that exchange traffic that crosses Swedish borders, though experts argue that it is impossible to differentiate between international traffic and traffic between Swedes. Available: http://en.wikipedia.org/wiki/FRA_law
See Figure of Signals Intelligence according to the «FRA-law».

26- See:
- US Code Chapter 119 § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited, available: http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002511----000-.html
- US Patriot Act 2001, available: http://epic.org/privacy/terrorism/hr3162.html

27- See The Finnish Electronic Communications Privacy Act (516/2004), available: http://www.technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland

The 2002 directive was enacted in Finland in 2004 by the Act. The purpose of the Act is to guarantee confidentiality in electronic communications and define specific circumstances when confidentiality is allowed to be breached. According to the Act, a breach is permissible in the following situations: 1) by consent of a sender or recipient, 2) to facilitate handling of providing and using services, 3) to allow handling for billing purposes, 4) to allow handling for marketing purposes by the service provider, 5) handling for the purposes of technical development, 6) handling for the purpose of detecting a technical fault or error; and 7) handling in cases of misuse.

28- See Wiretap report 2009 - US courts - Table 4 Summary of Interceptions of Wire, Oral, or Electronic communications, January 1 through December 31, 2009, available: http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table4.pdf

A total of 2,376 intercepts authorized by Federal and state courts were completed in 2009. The number of applications for orders by federal authorities was 663. The number of applications reported by state prosecuting officials was 1,713, with 24 states providing reports, two more than in 2008. Installed wiretaps were in operation an average of 42 days per wiretap in 2009, compared to 41 days in 2008. The average number of persons whose communications were intercepted rose from 92 per wiretap order in 2008 to 113 per wiretap order in 2009. The average percentage of intercepted communications that were incriminating remained unchanged at 19 percent in 2009.

Public law 106-197 amended 18 U.S.C § 2519 (2) (b) to required that reporting should reflect the number of wiretap applications granted for which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2009, one instance was reported of encryption encountered during a state wiretap; however, this did not prevent the officials from obtaining the plain text of the communications.

29- See Comprehensive Counter-Terrorism Act of 1991 (Introduced in Senate - IS) Subtitle B--Electronic Communications SEC. 2201. Cooperation of Telecommunications Providers with Law Enforcement, available: http://thomas.loc.gov/cgi-bin/query/F?c102:1:./temp/~c102zN0Wau:e30557

It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.

30- See Electronic communication Flow Chart, available: http://www.plymouth.gov.uk/eleccomm3.pdf

31- See:
- US Code Chapter 119 § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited, available: http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002511----000-.html
- US Patriot Act, 20001 available: http://epic.org/privacy/terrorism/hr3162.html

32- See Telecommunications (Interception and Access) Act 1979 (C′th), available: http://www.efa.org.au/Issues/Privacy/tia.html#scw

Prohibition on Access to Stored Communications. Section 108 states:

(1) A person commits an offence if:

(a) the person:
(i) accesses a stored communication; or
(ii) authorizes, suffers or permits another person to access a stored communication; or
(iii) does any act or thing that will enable the person or another person to access a stored communication; and

(b) the person does so with the knowledge of neither of the following:
(i) the intended recipient of the stored communication;
(ii) the person who sent the stored communication.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

Note: This section does not prohibit accessing of communications that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient.

(1A) Without limiting paragraph (1)(b), a person is taken for the purposes of that paragraph to have knowledge of an act referred to in paragraph (1)(a) if written notice of an intention to do the act is given to the person.

33- See Electronic Communications Privacy Act (ECPA) enacted by the US Congress in 1986, available: http://www.fas.org/sgp/crs/intel/98-327.pdf
Title III/ECPA bars the use of any mechanism (device), tape recorder included, to intentionally capture the spoken word or any communication being transmitted electronically (intercept wire, oral, or electronic communications) without the consent of one of the participants or a court order, 18 U.S.C. 2511(1)(a),(b). This applies to all telephone conversations whether a cell telephone is involved or not. It likewise applies to all face to face conversations unless they occur in a public place or under other circumstances where the speakers should reasonably have expected that their conversation would be overheard.

نص إرشاد الاتصالات الإلكترونية وحرية التعبير

الباب الأول: أحكام عامة

المادة ١: تعاريف

نقل المعلومات للجمهور بوسيلة إلكترونية: هو كل وضع بتصرف الجمهور أو فئات منه، بواسطة وسائل اتصالات إلكترونية، لإشارات أو كتابات أو صور أو أصوات أو رسائل من أية طبيعة كانت، والتي ليس لها طابع المراسلات الخاصة.

نقل المعلومات للجمهور على الخط: هو كل نقل، بناء لطلب فردي، لبيانات أو لمعلومات رقمية ليس لها طابع المراسلات الفردية، بواسطة وسائل اتصالات إلكترونية، تسمح بتبادل المعلومات بين المُرسل والمُستقبِل.

مزوِّد خدمات الشبكات الإلكترونية: يكون مزود خدمات الشبكات الإلكترونية إما مزود خدمة الاتصال أو مستضيفاً للبيانات.

مزوِّد خدمة الاتصال: هو من يتيح للمستخدم الدخول إلى شبكة اتصالات ويمكّنه من نقل المعلومات عبرها.

مستضيف البيانات: هو من يتولى تخزين المعلومات العائدة للغير لديه، ولحساب هذا الغير، مقابل بدل مادي أو مجاناً، كما يتولى وضع هذه المعلومات بتصرف الجمهور من خلال استخدام شبكات اتصال.

المعلومات المتعلقة بحركة البيانات: هي أية معلومات تتعلق بعملية نقل للبيانات أو اتصال عبر شبكة إلكترونية، ينتجها النظام المعلوماتي المرتبط بالشبكة الإلكترونية، وتحدد هذه المعلومات مصدر الاتصال أو مُرسل البيانات والمُرسل إليه أو المُتلقي وخريطة طريق إرسال المعلومات ووقت الإرسال وتاريخه وحجم البيانات المُرسلة ومدة الإرسال وغيرها من المعلومات التقنية.

تخزين المعلومات انتقالياً ومؤقتاً: إن تخزين المعلومات انتقالياً ومؤقتاً يعني أن التخزين يخدم حصرياً تنفيذ عملية نقل هذه المعلومات على شبكة الاتصالات، ويشترط أن لا تزيد مدة التخزين عن الوقت المعقول اللازم لنقل المعلومات. فعمليات نقل المعلومات تشمل بطبيعتها التخزين الآلي المؤقت والوسيط أو الانتقالي للمعلومات المُرسلة ضمن الشرطين المذكورين أعلاه.

وسائل تشفير المعلومات: تعني وسائل التشفير التجهيزات أو البرامج المعدّة من أجل تحويل البيانات، عبر اتفاقات سرية، أو من أجل تحقيق العملية المعاكسة. تهدف وسائل التشفير إلى ضمان سرية المعلومات المخزّنة أو المُرسلة أو تأمين سلامتها أو موثوقيتها.

تشفير المعلومات: عملية تحويل المعلومات عبر اتفاقات سرية إلى رموز غير مفهومة بحيث يجب إعادتها إلى حالتها الأصلية لأجل قراءتها وفهمها.

المادة ٢: حرية نقل المعلومات للجمهور بوسيلة إلكترونية

إن نقل المعلومات للجمهور بوسيلة إلكترونية هو حر.
لا يمكن الحد من ممارسة هذه الحرية إلا ضمن حدود احترام كرامة الإنسان وحرية الغير وملكيته وتعدد الآراء، ومن جهة أخرى ضمن حدود حماية النظام العام والآداب العامة وحاجات الدفاع الوطني ومتطلبات المرافق العامة والمتطلبات التقنية لوسائل الاتصال. كما وأن حرية التعبير يجب أن تحترم نظام حماية البيانات الشخصية.

الباب الثاني: النظام القانوني لمزودي خدمات الشبكات الإلكترونية

المادة ٣: تقييد الوصول إلى بعض المواقع والخدمات الإلكترونية

يجب على مزود خدمة الاتصال أن يُعلم المستخدمين بوجود وسائل تقنية تسمح بتقييد الوصول إلى بعض المواقع الإلكترونية أو الخدمات الإلكترونية أو بالاختيار منها، وعلى مزود خدمة الاتصال تقديم هذه الوسائل التقنية للمستخدمين.

المادة ٤: رقابة مزود خدمة الاتصال ومستضيف البيانات على المعلومات

لا يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب رقابة على مضمون المعلومات التي يرسلها أو يخزنها، ولا لموجب عام بالبحث عن الأعمال المتعلقة بنشاطات غير مشروعة. يُستثنى من ذلك حالة صدور قرار قضائي يُلزم

مزود خدمة الاتصال أو مستضيف البيانات بإجراء مراقبة مؤقتة ومحدودة لمعلومات محدّدة.
ولا يكون مستضيف البيانات مسؤولاً عن المعلومات المخزّنة:

- إذا لم يكن يعلم بطابعها غير المشروع الظاهر.
- أو إذا أقدم على سحب هذه المعلومات أو جعل الوصول إليها مستحيلاً منذ اللحظة التي يعلم فيها بطابعها غير المشروع الظاهر.

يكون مزود خدمة الاتصال مسؤولاً إذا لم يمحُ المعلومات المخزّنة مؤقتاً بناءً على طلب مُرسل هذه المعلومات، وكذلك بناءً لقرار قضائي.

المادة ٥: إجراءات الإبلاغ بعدم مشروعية المعلومات

يُعتبر مستضيف البيانات أنّه قد عَلِمَ بالطابع غير المشروع للمعلومات التي يخزّنها عندما يتم إبلاغه المعلومات التالية:

- تاريخ التبليغ
- إذا كان المُبلّغ شخصاً طبيعياً: اسمه ومهنته ومقره وجنسيته وتاريخ ومكان الولادة
- إذا كان المُبلّغ شخصاً معنوياً: شكله القانوني، مركزه القانوني، واسم المفوض بتمثيله
- اسم المُرسل إليه ومقره
- وصف الأعمال المُنازع بها ومكان تمركزها
- الأسباب التي تدعو لسحب المعلومات مع ذكر القواعد القانونية والتعليل.

المادة ٦: عدم إفشاء هوية الناشر وحفظ بيانات التعريف الشخصية له

يحق لكل شخص ينشر معلومات، بصفة غير مهنية أو غير محترفة، للجمهور عبر الاستفادة من خدمات مستضيف بيانات، أن يبقي هويته سرية وأن يقدم إلى الجمهور عناصر التعريف العائدة فقط لمستضيف البيانات، شرط تقديم عناصر التعريف الشخصية عنه لمستضيف البيانات.
أما الناشر المحترف، فيجب عليه دوماً تقديم عناصر التعريف الشخصية به للجمهور.

يجب على مستضيف البيانات أن يحتفظ بالبيانات التي تعرّف بهوية كل ناشر لمدة لا تقل عن عشر سنوات.

كما يخضع مستضيف البيانات لموجب السر المهني بخصوص عناصر التعريف الشخصية باستثناء حالة وجود قرار قضائي.

المادة ٧: حفظ معلومات حول حركة البيانات

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات حفظ المعلومات المتعلقة بحركة البيانات والعائدة لجميع المستخدمين الذي يستفيدون من خدماته، وذلك لمدة لا تقل عن خمس سنوات. لا يخضع لموجب الحفظ مضمون المعلومات ذاتها المُرسلة أو المخزّنة أو المراسلات المُتبادلة.

يخضع مزود خدمة الاتصال ومستضيف البيانات لموجب السر المهني بخصوص معلومات حركة البيانات باستثناء حالة وجود قرار قضائي.

يلتزم مزود خدمة الاتصال ومستضيف البيانات بصون المعلومات حول حركة البيانات من التدمير أو المحو أو التعديل أو الإفشاء، كما يلتزم بمحوها بعد انقضاء مدة الحفظ القانونية المحدّدة بخمس سنوات.

المادة ٨: تقديم معلومات حركة البيانات للسلطات القضائية والأمنية

يجب على كل من مزود خدمة الاتصال ومستضيف البيانات تقديم المعلومات المتعلقة بحركة البيانات وبهوية الأشخاص الذين يستفيدون من خدماتهم، وذلك إلى السلطات القضائية والأمنية المختصة العاملة تحت إشرافها. وكذلك يجب عليهم تمكين هذه السلطات من الوصول إلى المعلومات المنوه عنها وفقاً لوقت الإرسال الحقيقي لها عند حصول أي عملية اتصال.

المادة ٩: مساهمة مزود خدمة الاتصال ومستضيف البيانات في مكافحة بعض الجرائم

يجب أن يساهم كل من مزود خدمة الاتصال ومستضيف البيانات بمحاربة الجرائم ولاسيما الجرائم ضد الإنسانية أو الجرائم الإباحية للقاصرين أو بالتحريض على العنف أو التعرض لكرامة الإنسان. وعلى مزود خدمة الاتصال أو مستضيف البيانات بالتالي أن يضع بتصرف الجمهور آلية واضحة وسهلة للإبلاغ عن الأفعال المذكورة في هذه المادة، وعليه بعد حصول التبليغ إعلام السلطات العامة بذلك.

المادة ١٠: المسؤولية التعاقدية لمزود خدمة الاتصال ومستضيف البيانات

يكون كل من مزود خدمة الاتصال ومستضيف البيانات مسؤولاً عن حسن تنفيذ موجباته المنصوص عنها في

العقود الموقّعة مع عملائه. ويجب أن تتضمن هذه العقود تحديد نوعية الخدمة المقدمة ومواصفاتها ومدتها.

تنتفي مسؤولية مزود خدمة الاتصال ومستضيف البيانات إذا أثبت أن عدم تنفيذ العقد تجاه عميله أو سوء تنفيذه هو ناتج عن خطأ العميل أو عن القوة القاهرة أو عن فعل الغير.

المادة ١١: حق الرد للشخص المعني المذكور في عملية نقل المعلومات للجمهور

يتمتع كل شخص تم ذكر اسمه في عملية نقل للمعلومات إلى الجمهور على الخط بحق الرد، مع عدم الإخلال بطلبات التصحيح أو الإلغاء التي يستطيع توجيهها لمزود الخدمة. توجه طلبات ممارسة حق الرد خلال ثلاثة أشهر من تاريخ النشر إلى مدير النشرة. وفي حال عدم إفشائه لاسمه للجمهور، توجه الطلبات المنوه عنها إلى مستضيف البيانات الذي يخزّن المعلومات موضوع طلب الرد. وعلى مستضيف البيانات إرسال طلب الرد دون تأخير إلى مدير النشرة.

الباب الثالث: تشفير المعلومات

المادة ١٢: استعمال وسائل التشفير وتقديمها واستيرادها وتصديرها

إن استعمال وسائل التشفير هو حر.

إن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن فقط وظيفة التوثيق أو تأمين سلامة المعلومات يخضع للترخيص من قبل السلطات الرسمية المختصة. يمكن أن تحدّد كل دولة وسائل التشفير التي لا تخضع لأية معاملة رسمية، وذلك في ضوء متطلبات الحفاظ على الدفاع الوطني والأمن الداخلي والخارجي.

إن تقديم ونقل واستيراد وتصدير وسائل التشفير التي تؤمن وظيفة سرية المعلومات يخضع للترخيص من قبل السلطات الرسمية المختصة.

في جميع الأحوال، يجب أن يحدد طالب الترخيص المواصفات التقنية لوسائل التشفير.

المادة ١٣: مسؤولية مزودي وسائل التشفير

يخضع مزوّدو وسائل التشفير لموجب السرية باستثناء حالة صدور قرار قضائي.

باستثناء الحالة التي يثبتون فيها عدم حصول خطأ مقصود أو إهمال. وبالرغم من كل نص مخالف، يُسأل مزودو وسائل التشفير لضمان سرية المعلومات عن الضرر اللاحق بالأشخاص الذين يعهدون إليهم بإدارة اتفاقاتهم السرية المتعلقة بالتشفير، وذلك في حال حصول تعرض لسلامة أو سرية البيانات المحوّلة بواسطة الاتفاقات المذكورة.

الباب الرابع: التنصّت على الاتصالات الخاصة والشخصية

المادة ١٤: عدم جواز التنصّت على الاتصالات الخاصة والشخصية

تضمن الدول الأعضاء الحق في سرية الاتصالات الإلكترونية الخاصة والشخصية، بحيث لا تخضع هذه الاتصالات لأي نوع من أنواع التنصّت أو المراقبة أو الاعتراض أو الإفشاء إلا في الأحوال التي يجيزها القانون.

المادة ١٥: جواز التنصّت بإذن قضائي أو لضرورات الأمن الوطني

يمكن لكل دولة عضو أن تجيز التنصّت أو مراقبة أو اعتراض أو إفشاء اتصالات خاصة أو شخصية في الحالتين التاليتين:

- بإذن قضائي، من أجل ضرورات التحقيقات القضائية الجزائية.

- بإذن من السلطات الأمنية أو الدستورية المختصة تحت إشراف القضاء، من أجل تجميع المعلومات لمكافحة الإرهاب والجرائم الواقعة على أمن الدولة والجرائم المنظّمة.

الباب الخامس: أحكام جزائية

المادة ١٦: أحكام جزائية

ضماناً للفعالية في تطبيق أحكام هذا الإرشاد، تحرص الدول الأعضاء على تجريم الأفعال التالية:

- عدم تعاون مزود خدمات الشبكات الإلكترونية مع القضاء بتقديم معلومات حركة البيانات أو بسحب بيانات أو بمنع الوصول إليها متى طُلب منه ذلك.

- فعل مزود خدمة الاتصال أو مستضيف البيانات بعدم حفظ معلومات حركة البيانات وبيانات التعريف الشخصية وفق ما يفرضه القانون.

- قيام شخص بتقديم معلومات غير صحيحة عن قصد لمزود خدمات الشبكات الإلكترونية لحمله على سحب معلومات أو منع الوصول إليها.

- عدم قيام مدير النشرة بنشر رد الشخص المعني وفقاً للمادة ١١ من هذا الإرشاد.

- تقديم أو تصدير أو استيراد وسائل تشفير بصورة غير مشروعة دون الحصول على الترخيص المطلوب من السلطات الرسمية.

- التنصّت على الاتصالات الإلكترونية الخاصة والشخصية بصورة غير مشروعة خارج الحالات التي يجيزها القانون.

الإرشاد الثاني

المعاملات الإلكترونية والتواقيع الإلكترونية

٢

الورقة البحثية الخلفية لإرشاد المعاملات الإلكترونية والتواقيع الإلكترونية

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع المعاملات والتواقيع الإلكترونية في الدول العربية، رصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية، وبالتالي تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار تشريعات أو تنظيمات خاصة تتعلق بالمعاملات والتواقيع الإلكترونية.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالمعاملات والتواقيع الإلكترونية.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) السندات والتواقيع الإلكترونية والإثبات الإلكتروني: تنظيم السندات الإلكترونية العادية والرسمية، النسخ في السندات الإلكترونية، تحديد الشروط القانونية للاعتراف بالكتابة الإلكترونية وقوتها الثبوتية، والشروط الأساسية لصحة التوقيع الإلكتروني، تحديد البيانات والآليات اللازمة لإنشاء التوقيع إلكتروني، موثوقية التوقيع الإلكتروني وحمايته من التقليد والتزوير، حفظ السندات الإلكترونية والشروط المطلوبة لصحتها.

٢) واجبات ومسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعوّل: تحديد وتنظيم مسؤوليات مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة باعتبار أنها تتمتع بقرينة الموثوقية، ومسؤوليته عن سلامة منظومة التوقيع الإلكتروني الخاصة به وعن سريتها، الآلية المتبعة لإصدار شهادات التصديق وموثوقيتها، ومفاعيل إلغاء شهادة المصادقة؛ مسؤولية صاحب شهادة المصادقة عن صحة المعلومات المتعلقة به المقدمة إلى مزود خدمات المصادقة وتحديثها؛ بالإضافة إلى مسؤولية الطرف المعوّل عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني أو للتحقق من صلاحية الشهادة أو وقفها أو إلغائها أو وجود قيود عليها.

٣) الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية: تعتبر شهادات المصادقة الإلكترونية الأجنبية الموصوفة معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني في حالات معينة، من شأنها أن تساعد على حل الإشكاليات الناشئة عن تجاوز التعاملات الإلكترونية الحدود الوطنية بفعل الإنترنت، والمساهمة في توحيد المتطلبات التي يخضع لها مزودو خدمات المصادقة وشهادات المصادقة.

٤) العمليات المصرفية: تشمل أوامر الدفع والتحاويل الإلكترونية للأموال النقدية، بطاقات الدفع والسحوبات المصرفية الآلية، بالإضافة إلى النقود والشيكات الإلكترونية؛ تحديد مواصفات الأنظمة الإلكترونية المستعملة في العمليات المتعلقة بأوامر الدفع والتحاويل الإلكترونية؛ مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية؛ ومسؤولية المصرف أو المؤسسة المالية المحافظة على سلامة حساب العميل ونظام الدفع الإلكتروني.

قسمت أعمال البحث إلى قسمين أساسيين: القسم الأول تناول الناحية القانونية لموضوع المعاملات الإلكترونية أي الإرشادات والقوانين النموذجية الأجنبية والعربية، والتشريعات الأجنبية والعربية بالإضافة إلى المراجع الفقهية المرتبطة، والقسم الثاني شمل الناحية التقنية لهذا الموضوع وخاصة فيما يتعلق بأنظمة التشفير (encryption systems) وفكها والمفاتيح العامة (Public Key) والمفاتيح الخاصة (Private Key)، بالإضافة إلى بعض أسماء مزودي خدمات التصديق في الدول الأوروبية.

القسم الأول: أبرز ما تناولته أعمال البحث في هذا القسم:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي، المتعلقة بهذا المجال، ومنها:

- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

- 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").

- Model Law 56/80 on Electronic Signatures, adopted by the United Nations Commission on International Trade Law.

- UNCITRAL Legislative Guide on Secured Transactions, Supplement on security Rights in Intellectual Property, United Nations Commission on International Trade Law. Pre-release (15 July 2010).

- OECD Guidelines for Cryptography Policy, 27 March 1997.

- OECD Recommendation on Electronic Authentication, and OECD Guidance for Electronic Authentication.

- Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 C4-0648/97).

- Commission recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder.

- Commission Recommendation 87/598/EEC of 8 December 1987, concerning a European code of conduct relating to electronic payments .

- Commission Decision of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

٢) بالإضافة إلى ذلك تناولت أعمال البحث مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم المعاملات الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الأسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول آسيا الوسطى.

٣) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية الخاصة بالمعاملات الإلكترونية.

- قيمة مستخرجات التقنيات العلمية الحديثة ومدى حجيتها في الإثبات، أسامة أحمد شوقي المليجي، دراسة، مؤتمر معالجة المعلومات القانونية في القرن ٢١ وتحدياتها، بيروت، ٧-٢٠٠١/٢/٩.

- التنظيم القانوني لشبكة الإنترنت، الدكتور طوني عيسى، أطروحة دكتوراة، الجامعة اللبنانية، ٢٠٠٠.

- الإثبات الإلكتروني للقاضي وسيم شفيق حجار، بيروت ٢٠٠٧.

- الإثبات الإلكتروني في القانون اللبناني للقاضي سامي منصور، مجلة العدل، ٢٠٠١.

- الدليل الكتابي وحجية الكمبيوتر في الإثبات في المواد المدنية والتجارية ، بحث، مؤتمر القانون والكمبيوتر والإنترنت، ١-٢٠٠٠/٥/٣.

- La signature Electronique, Transactions et confiance sur Internet, par Arnaud-F. Fausse, Paris 2001.

- De L'Ecrit Electronique et des signatures qui s'y attachent, 14 Juin 2000.

- Le droit de la preuve est un Totem Moderne (Le commerce électronique), par Cyrille Charbonneau et Frédéric-Jérôme Pansier, Avril 2000.

- Hirst (M.): Computers and the English Law of Evidence, Law, Computers & Artificial Intelligence, 1992.

- Bensoussan (A.) Contributions théoriques au droit de la prevue dans le domaine informatique: Aspects techniques et solutions juridiques, Gaz.Pal., 1991,2.

- The Legal and Market Aspects of Electronic Signatures by the European Commission - DG Information, Society final version.
http://ec.europa.eu/information_society/eeurope/ 2005/all_about/security/electronic_sig_report.pdf

- Commission welcomes new legal framework to guarantee security of electronic signatures, Brussels, 30 November 1999.
http://ec.europa.eu/dg15en/media/sign/index.htm

- Digital Signature Guidelines Tutorial, American Bar Association.
http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

- Cryptographie et signature Electronique, Aspects Juridiques; Alain Bensoussan, Yves le Roux, Hermes, 1999.

- How Encryption Works by Jeff Tyson published on. http://computer.howstuffworks.com/encryption1.htm

- Digital Signatures and European Laws, by Mirella Mazzeo, 26 Jan 2004.
http://www.symantec.com/connect/articles/digital-signatures-and-european-laws

- Cryptography for Network and Information Security.
http://technet.microsoft.com/en-us/library/cc962027.aspx

- Cryptography Policy, by Lance J. Hofjhan, Fam A. Ali, Steven L. HeAle+, Am Huybredtts, September 1994.
http://www.cspri.seas.gwu.edu/Mazz.%20Papers/p109-hoffman%20Crypto%20Policy%20CACM.pdf

- Data Encryption Standard (DES), Federal Information, Processing Standards Publication 46-2, 1993 December 30.

- Advanced Encryption Standard (AES), Federal Information, Processing Standards Publication 197, November 26, 2001.

- The National Strategy to Secure Cyberspace, the White House Washington- February 2003.

- Privacy and Encryption controls: A Crypto Trilogy (Bernstein, Junger & Karn), by Keith Aoki. This module has been revised to reflect the state of affairs as of August 24, 2000. The earlier 1999 version of this model is superceded

- The Codebreakers: The Story of Secret Writing (1973; rev. ed, 1996); by David Kahn
http://www.britannica.com/dday/article-7517

- Data Encryption for QUB Confidential Data, Security Policy User Guide1, Queen's University, Belfast.23 February 2009.
http://www.qub.ac.uk/directorates/InformationServices StaffComputing/ITServices/FileStoresecuritypolicies/word/Filetoupload,140675,en.doc

- Information Privacy in Cyberspace Transactions by Jerry Kang, April 1998
http://www.ntia.doc.gov/ntiahome/privacy/files/cprivacy.pdf

- Les enjeux de la cryptographie, Lionel Thoumyre, November 1998.
http://www.juriscom.net//espace2/crypto2.htm

٤) وقد تم الاسترشاد أيضاً بالدراسات التي أعدتها الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق. ٢- وضع التشريعات السيبرانية في سلطنة عمان ، دولة الإمارات العربية المتحدة ، دولة قطر. ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٥) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم المعاملات الإلكترونية؛ ومدى شمولية هذه التشريعات النقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بالمعاملات الإلكترونية والتواقيع الإلكترونية:

تبين أثناء أعمال البحث أن معظم دول الإسكوا، عملت على إصدار تشريعات خاصة وإقرار نظام للتعاملات الإلكترونية، بحيث تهدف هذه التشريعات إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير الإطار النظامي لها، وإضفاء الحجية عليها. حيث تتمّ أيضاً معاملة المستند الإلكتروني - متى توافرت فيه الشروط والمواصفات المطلوبة نظاماً - معاملة المستند الورقي المكتوب، لجهة ترتب الآثار النظامية عليه، وقبول حجيته في الإثبات وغير ذلك من الأمور النظامية والقانونية لقبول هذه المعاملات والاعتماد عليها كوسيلة جديدة من وسائل التعامل.

إن دول الإسكوا التي أصدرت تشريعات خاصة بالمعاملات الإلكترونية هي التالية:

١- الأردن:
قانون رقم الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الإلكترونية.
http://www.lob.gov.jo/ui/laws/search_no.jsp?no=85&year=2001

٢- الإمارات العربية المتحدة:
قانون رقم (٢) صادر في ٢٠٠٢/٠٢/١٢ بشأن المعاملات والتجارة الإلكترونية.
http://www.theuaelaw.com/vb/showthread.php?t=1137

٣- البحرين:
مرسوم بقانون رقم ٢٨ الصادر بتاريخ ١٤ سبتمبر ٢٠٠٢ بشأن المعاملات الإلكترونية وتعديلاته.
http://www.moic.gov.bh/MoIC/Ar/Industry/ResourcesLaws/CommerceLaw/eLaw/

٤- سوريا:
قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الإلكتروني وخدمات الشبكة.
http://www.moct.gov.sy/moct/?q=ar/node/69

٥- السودان:
قانون المعاملات الإلكترونية لسنة ٢٠٠٧.
http://www.cbos.gov.sd/node/281

٦- سلطنة عمان:
قانون رقم ٦٩ لسنة ٢٠٠٨ بشأن المعاملات الإلكترونية.
http://www.ita.gov.om/ITAPortal_AR/Businesses/Businesses_Projects.aspx?NID=97

٧- قطر:
قانون المعاملات والتجارة الإلكترونية تاريخ ١٩ اغسطس ٢٠١٠.
http://www.ict.gov.qa/files/images/e-commerce_law_updated.pdf

٨- مصر:
قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الإلكتروني.

٩- السعودية:
مرسوم ملكي رقم ١٨ لسنة٢٠٠٧ خاص بنظام التعاملات الإلكترونية.
http://www.ncda.gov.sa/low21/7.pdf

١٠- اليمن:
قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن انظمة الدفع والعمليات المالية والمصرفية الإلكترونية.
http://www.centralbank.gov.ye/ar/CBY.aspx?keyid=80&pid=74&lang=2&cattype=1

واقر مجلس الوزراء الكويتي مؤخراً "مشروع قانون المعاملات الإلكترونية" الذي تسري أحكامه على المعاملات الإلكترونية والدفع الإلكتروني والرسالة الإلكترونية والأنظمة المؤتمتة. وينص المشروع للمرة الأولى على أنه "لا يجوز إغفال الأثر القانوني للتوقيع الإلكتروني من حيث صحته وإمكان العمل به لمجرد وروده في شكل إلكتروني، ويكون للتوقيع الإلكتروني المحمي في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيع الكتابي المنصوص عليها في أحكام قانون الإثبات في المواد المدنية والتجارية، متى روعي في إنشائه وإتمامه الضوابط الفنية الواردة في هذا القانون ولائحته التنفيذية".

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالمعاملات الإلكترونية، وهي: لبنان، وفلسطين[٢] التي قامت بإعداد مشروع قانون المبادلات والتجارة الإلكترونية الصادر عام ٢٠٠٣.

من ناحية أخرى، نفيد ضمن هذا المجال أن جامعة الدول العربية قد قامت بإصدار القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة[٣]، وقد تناول هذا القانون أحكاماً حول حجية الكتابة والمحرّرات والتواقيع الإلكترونية، والهيئة المختصّة، وجهة التوثيق الإلكتروني المنظمة لشهادات التوثيق الإلكتروني والجرائم المرتكبة في هذا المجال وعقوباتها. كما وأصدرت القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية، الذي تناول أحكاماً حول رسالة البيانات، والعقود الإلكترونية، والدفع الإلكتروني، والعقوبات التي تفرض عند مخالفة هذه الأحكام بالإضافة إلى القانون الواجب تطبيقه والمحكمة المختصة.

ب - شمولية التشريعات الوطنية الخاصة

إزاء التطور والتغيير الكبير الحاصلين في مجال تقنيات المعلومات والتغييرات الحاصلة في أشكال المعاملات الإدارية والتجارية من خلال استعمال الوسائل الإلكترونية والشبكات والوسائط المعلوماتية، عملت جميع الدول العربية على تنظيم موضوع التعاملات الإلكترونية ضمن إطار تشريعي متكامل. فقام بعضها بإصدار تشريعات تشمل في آن المعاملات والتواقيع الإلكترونية بالإضافة إلى التجارة الإلكترونية، ولم تخصص لها تشريعات منفردة ومستقلة، باستثناء بعض النصوص القانونية الوطنية التي تراعي أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية كما هو الحال في اليمن؛ والقرارات الإدارية أو تعاميم المصرف المركزي فيما يتعلق بالتحاويل الإلكترونية، والعمليات المالية والمصرفية بالوسائل الإلكترونية والصراف الآلي وبطاقات الإئتمان والوفاء كما هو الحال في لبنان.

عالجت التشريعات الوطنية العربية ونظمت: الكتابة والسندات الإلكترونية والرسائل والسجلات وآثارها القانونية؛ التواقيع الإلكترونية، آلية إنشاء التوقيع الإلكتروني، قوته

الثبوتية وحمايته؛ واجبات ومسؤولية وسيط الشبكة الإلكترونية؛ واجبات ومسؤولية مزودي خدمات المصادقة الإلكترونية، مسؤولية صاحب الشهادة والجهات المختصة لتنظيم نشاطات تقديم خدمات التوقيع الإلكتروني، منح وإلغاء الترخيص الخاص بممارسة نشاطهم؛ إبرام العقود والتعبير عن الإيجاب والقبول وأثره القانوني عند إبداء النوايا؛ التحاويل الإلكترونية للأموال وأنظمة الدفع وشروطه والشيكات الإلكترونية وحجية الوفاء الإلكتروني ووسائله؛ والعقوبات التي تفرض عند مخالفة نظم المعلومات وارتكاب أعمال التزوير أو التحريف أو التعديل في السندات الإلكترونية، ومخالفة الأحكام الخاصة بمنظومة التوقيع الإلكتروني وصحته، الخ.

أصدرت مملكة البحرين المرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ الخاص بالمعاملات الإلكترونية، وهو قانون شامل إذ أنه يغطي معظم الجوانب المتعلقة بالمعاملات الإلكترونية، بحيث تطرق إلى كيفية إبرام العقود وصحة انعقادها ودور الوكلاء الإلكترونيين في إبرام العقود، الإسناد الإلكتروني وإثباته، السجلات الإلكترونية، الإقرار بتسلمها، وقت ومكان إرسال وتسلم السجلات الإلكترونية وقوتها الثبوتية، اعتماد مزودي خدمة الشهادات الوطنيين والخارجيين واجباتهم ومسؤولياتهم، بالإضافة إلى أحكام خاصة بمستندات نقل البضائع، وأحكام خاصة بتسجيل أسماء النطاق وتنظيم تسجيل واستعمال اسم النطاق (Domain Name)، بالإضافة إلى كيفية الطعن في صحة السجلات والتوقيعات الإلكترونية.

انفردت سلطنة عمان ضمن مرسومها السلطاني رقم ٢٠٠٨/٩٦ المتعلق بإصدار قانون المعاملات الإلكترونية بتخصيص فصل يتعلق بطرق حماية المعاملات الإلكترونية التي لم تتطرق إليها ولم تعالجها باقي الدول العربية، فنصت على أحكام تقضي باستخدام التشفير كوسيلة لحماية المعاملات الإلكترونية بهدف المحافظة على سرية المعلومات أو البيانات التي تحويها الرسالة الإلكترونية، وتحديد الطرق الخاصة بحماية نظم المعلومات أي اعتماد التشفير بطريق المفتاح العام، الجدران النارية (Fire Wall)، مرشحات المعلومات، البرامج المضادة للديدان (worm) والفيروسات (Viruses)، الخ.

كما قامت السعودية بإصدار ضوابط لتطبيق التعاملات الإلكترونية الحكومية من شأنها المحافظة على المعلومات والبيانات الحكومية، حيث تقوم كل جهة حكومية بإدارة وحفظ وتوثيق البيانات التابعة لها، وإتاحة البيانات المشتركة منها إلكترونياً للجهات الحكومية الأخرى المستفيدة لتأمين تكامل البيانات بين الأجهزة الحكومية وذلك ضمن الالتزام بمعايير محددة لحماية الخصوصية والمعلومات بالإضافة إلى معايير استرشادية تعدها الجهة المعنية.

نظمت إمارة دبي أيضاً بقانونها رقم ٢ لسنة ٢٠٠٢ الخاص بالمعاملات والتجارة الإلكترونية الاستخدام الحكومي للسجلات والتوقيعات الإلكترونية وقبول وإيداع المستندات والإصدار الإلكتروني للمستندات، وتطرقت في إحدى مواد القانون إلى التوقيع الإلكتروني المحمي دون أن تفرد له أحكاماً خاصة بحمايته عبر استعمال وسيلة التشفير.

أما اليمن فعملت على تضمين قانونها رقم (٤٠) لسنة ٢٠٠٦ ما يتعلق بأنظمة الدفع والعمليات المالية والمصرفية والإلكترونية، وهو ينظم بشكل مفصل أنظمة الدفع وتحويل الأموال إلكترونياً، والآثار المترتبة على كل من السجل والعقد والرسالة والتوقيع الإلكتروني، كما نظم تداول الوثائق والسجلات والرسائل الإلكترونية بإنشائها وإرسالها واستلامها، ونظم أيضاً إجراءات توثيق السجل والتوقيع الإلكتروني، وهو ما كان ضروريا لسد النقص في تنظيم هذه المسائل خصوصاً مع غياب التنظيم التشريعي الكامل لها.

لا بد من الإشارة إلى أنه، وبالرغم من أن جميع الدول العربية باستثناء أربع دول قد أصدرت قوانين خاصة بالمعاملات والتواقيع والتجارة الإلكترونية، إلا أنها لم تعالج بشكل تفصيلي جميع النقاط التي يجب أن تتضمنها هذه التشريعات. نقدم أمثلة على ذلك:

- لم تصدر الدول العربية أنظمة أو أحكاماً خاصة بوسائل حماية المستندات والمعاملات والتواقيع الإلكترونية وأنواعها وإجراءاتها مثال التشفير باستثناء سلطنة عمان وإمارة دبي. إلا أن هذه الأخيرة قد ذكرتها في مادة واحدة ولم تخصص لها فرعاً أو فصلاً، أي أنها لم تعالجها بشكل تفصيلي.

- لم تتطرق بعض الدول العربية ضمن تشريعاتها الخاصة بالمعاملات الإلكترونية إلى عمليات التحاويل والدفع الإلكتروني مثال: سلطنة عمان، السعودية، البحرين، وسوريا، وهذه العمليات تحتاج بلا شك إلى تنظيم قانوني لما تنطوي عليه من أهمية بالغة. إلا انه بالمقابل أصدرت اليمن نصاً خاصاً يراعي أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية؛ وأصدر لبنان عدداً من القرارات الإدارية أو تعاميم المصرف المركزي المتعلقة بالتحاويل الإلكترونية، والعمليات

المالية والمصرفية بالوسائل الإلكترونية والصراف الآلي وبطاقات الائتمان والوفاء.

القسم الثاني: تناولت أعمال البحث في هذا القسم بعض أنظمة حماية المعلومات، وبعض أنظمة التشفير المعتمدة، وبعض أسماء مزودي خدمات التصديق وذلك من أجل إتاحة المجال أمام المشترع العربي للاطلاع على هذه الوثائق ومساعدته في وضع التشريعات المناسبة آخذاً بعين الاعتبار المعطيات التقنية المطلوبة، وأبرزها:

١) بعض أنظمة حماية المعلومات:

- Guidelines on Firewalls and Firewall Policy.
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

- Payment Application Data Security Standard.
https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

- Methods, software programs, and systems for electronic information security.
http://www.freepatentsonline.com/7395436.html

- Secured electronic mail system and method.
http://www.freepatentsonline.com/y2002/0007453.html

- Creating, verifying, managing, and using original digital files.
http://www.freepatentsonline.com/y2002/0055942.html

٢) بعض أنظمة التشفير المعتمدة في العالم وأبرزها:

- DES-Data Encryption Standard.
http://www.itl.nist.gov/fipspubs/fip46-2.htm

- AES-Advanced Encryption Standard.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

- RSA's security system.
http://ecommerce.hostip.info/pages/914/RSA-Data-Security.html

- BLOWFISH encryption algorithm.
http://www.schneier.com/blowfish.html

- IDEA International Data Encryption Algorithm.
http://www.quadibloc.com/crypto/co040302.htm

- SEAL encryption algorithm.
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_se.html#wp1027129

- RC4 encryption algorithm.
http://www.codeproject.com/KB/recipes/rc4csharp.aspx

- The CSS Decryption Algorithm.
http://www.cs.cmu.edu/~dst/DeCSS/Gallery/plain-english.html

- PHP – Simple Encryption and Decryption algorithm.
http://flax.ie/php-simple-encryption-and-decryption-algorithm/

- CAS Central Authentication Service project.
http://www.jasig.org/cas

٣) أسماء بعض مزودي شهادات التصديق:

- List of European Service Providers Issuing Qualified Certificates.
http://eu.adr.eu/html/en/adr/electronic_signatures/PDF1.pdf

- Global List of PCI DSS Validated Service Providers.
http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf

- Qualified Security Assessor (QSA) companies.
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

- قائمة مزودي خدمات التصديق في السعودية:
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/DSPs-ISPs-List

- المركز الوطني للتصديق الرقمي، وزارة الاتصالات وتقنية المعلومات في السعودية:
http://www.mcit.gov.sa/arabic/NationalCenter

- مزودو خدمات التصديق الإلكتروني في دولة الإمارات
http://www.tra.gov.ae/news100-A.php

٤) لائحة ببعض أسماء الشركات مزودي خدمات التشفير:

- http://searchmobilecomputing.bitpipe.com/data/olist?iStart=1&t=itmgmt_10_50_20_28_2

- Protectyon, established in Haarlem (the Netherlands). As a team of web designers, software developers and application engineers we have been fighting copyright infringement since day one, which gave us the idea to provide a new innovative service to fight online piracy.
http://www.protectyon.com/about.php

- Verisign company.
http://www.verisign.com/

هوامش

١- تراجع لائحة تشريعات الدول الأجنبية - ملحق رقم ٥ من التسليم الاول.

٢- راجع مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني المنشور على الموقع الالكتروني:
http://www.pita-palestine.org/PITA%20files/proposed%20e_commerce%20law.doc

٣- القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، أعتمده مجلس وزراء العدل العرب بقرار رقم ١٧٧/د٢٤ - ٢٧/١١/٢٠٠٨

مقدمة إرشاد المعاملات الإلكترونية والتواقيع الإلكترونية

تعاظم حجم التعاملات الإلكترونية في ظل تطور التقنيات وتنامي استعمال الحاسوب والإنترنت وانتشار ثقافة المعلوماتية بين الجمهور.

عند بداية الثمانينيات من القرن العشرين بدأ استعمال الحاسوب من قبل القطاع الخاص، إلا أن استعماله في المعاملات اقتصر على إدخال البيانات واستخراجها وطباعة المستندات آلياً مما شكل نقلة نوعية عن الطباعة على الآلة الكاتبة أو عن حفظ الملفات ورقياً وبواسطة أنظمة أرشفة تقليدية.

أدى السماح للجمهور باستعمال شبكة الإنترنت في بدايات التسعينيات من القرن الماضي، إلى ظهور أنواع جديدة من إمكانيات الاتصال والتعامل والتعاقد. وقد أدّى بالتالي إلى إمكانية تبادل المعلومات في بداية الأمر ثم إلى تبادل الرسائل والمعاملات في وقت لاحق واستّعمل كوسيلة لتسليم بعض المنتجات ذات الطابع الإلكتروني، وهو ما أصبح يعرف بالمعاملات الإلكترونية. وهنا برزت إشكالية صحة وسلامة كلّ من المستند الإلكتروني غير المطبوع ورقياً والتوقيع. فنسخ التوقيع الخطي وإيراده إلكترونياً لا يحقق ذات القوة الثبوتية للتوقيع الخطي على ركيزة ورقية، ذلك أن حماية الصورة المنسوخة قد تتعرض للانتهاك.

يشكل المستند الورقي وسيلة حفظ وإثبات وحجة على من وقعه أو صاغه وله قوة ثبوتية شاملة نظراً لأنه يسمح لأي شخص كان، حتى ولو لم يكن يتمتع بمعرفة تقنية أو خبرة، باكتشاف أي تعديل يطرأ على المستند أو مضمونه. فإن مجرد النظر بالعين المجردة إلى أي مستند ورقي يمكّن الناظر من ملاحظة أي حشو أو إضافة أو تشطيب، أو قطع أو تمزيق أو محو، مما يفيد الناظر بأن المستند لم يعد بحالته السليمة ومما يفيد بأن هذه التغييرات من شأنها المساس بالقوة الثبوتية أو بصلاحية المستند الورقي لإنتاج الآثار القانونية الناجّة عنه وعن مضمونه لو كان بقي سليماً. لذا فإن القانون قد فرض التوقيع مجدداً فوق كل تمحية أو حشو وذلك لإضفاء المشروعية على مثل هذا التعديل ليعود المستند الورقي سليماً ومنتجاً لآثار القانونية.

من هنا يبرز الفرق بين المستند الورقي والمستند الإلكتروني، إذ إن المستند الإلكتروني لا يسمح عادة بفعل طبيعته الإلكترونية (أي أنه مؤلف من كتابة وفقاً للنظام الثنائي ٠١٠١٠٠١) باكتشاف أي تعديل أو تغيير فيه، لأن طبيعة حفظه بصورة إلكترو-مغناطيسية تسمح بتعديله بدون أن يتمكن من يعاينه من اكتشاف أي تعديل طرأ عليه منذ صياغته الأولى "الأساسية".

من هنا كان لا بد من وضع معايير لحماية المستند الإلكتروني مثل التشفير والصعوبات التقنية الأخرى التي تمنع الولوج إليه، وقد تم كذلك وضع برمجيات قادرة على كشف أي خرق أو تلاعب بسلامته. فضلاً عن ذلك، فإن إسناد المستند الإلكتروني إلى من صاغه هو أمرٌ لا بد من التأكد منه. من هنا كانت الحاجة إلى أن يجري توقيع المستند الإلكتروني بطريقة تلائم طبيعته غير الملموسة. يُعرف التوقيع عادةً بأنه إشارة أو رسم أو كتابة بخط يد شخص ما، تعبر عن هوية ومصدر ونية وموافقة صاحب التوقيع على مضمون ما وقعه. يتمتع التوقيع بقوة ثبوتية قانونية نظراً لأنه صادر عن شخص طبيعي معين، ويعتبر التوقيع إقراراً من الموقع على مضمون ما تم توقيعه، وهو الوسيلة القانونية المثلى لنسبة مستند مكتوب وموقّع إلى شخص الموقِع.

لذا كان لا بد من إيجاد بديل إلكتروني للتوقيع الخطي اليدوي. وهنا نشأ التوقيع الإلكتروني الذي يعرّف بأنه بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وهي تستعمل كوسيلة لتأكيد الموثوقية.

يتمتع التوقيع الإلكتروني بعدد من الإجراءات التقنية التي تسمح باعتماده والتأكد من صحته ومن صدوره عن الشخص المعني به، وتعرف هذه الوسائل بآليات إنشاء التوقيع الإلكتروني والتحقق من صحته.

ومع تطور عالم المعلوماتية واعتماد الحاسوب من قبل القطاع الخاص، تطورت الأساليب التجارية واتجهت أكثر نحو استعمال الإنترنت كوسيلة اتصال وكوسيلة تبادل للأموال لا سيما عندما أصبحت المصارف تقبل الحوالات النقدية الإلكترونية. تساهم المعاملات الإلكترونية[1] في النمو الاقتصادي الوطني، مما يعكس اهتمام مختلف الدول بتحفيزها وتنظيمها. إلا أن هذه المعاملات تثير إشكاليات جديدة يعجز النظام القانوني السائد حالياً[2] عن إيجاد حلول وافية لها في ظل قوانين لم تلحظ الطابع الإلكتروني كركيزة يمكن استعمالها مكان

الركيزة الكتابية أو الورقية، ومن هذه الإشكاليات عدم الاعتراف بالقوة الثبوتية للسندات الإلكترونية وعدم اعتماد وقبول التواقيع الإلكترونية وعدم الركون إلى موثوقيتها. يُضاف إلى ذلك وجود تفاوت واضح في المعرفة التقنية بين الممتهن والمتعامل العادي، مما قد يُضاعف أخطار التلاعب في المعاملات الإلكترونية، وممّا قد يدفع المتعاملين إلى الإحجام عن التعاملات الإلكترونية، الأمر الذي سيؤدي إلى الإضرار بالاقتصاد الوطني. وبالتالي كان لا بد من وضع إطار قانوني لتنظيم المعاملات الإلكترونية ومسائل الإثبات الإلكتروني، ولاسيما التواقيع الإلكترونية وموثوقيتها، وذلك لتدعيم الثقة بالتقنيات الجديدة وتحفيز قبول الجمهور لها وإعطائها نفس القوة الثبوتية التي تُعطى للتعاملات الجارية بالأساليب التقليدية أي الخطية.

كان لا بد إذاً من توفير الحماية القانونية اللازمة للسند الإلكتروني كما هي الحال للسند العادي أي الورقي. إذ أن إمكانية ضبط وكشف أي تعديل أو تحريف يجري على السند الخطي، هي سهلة وواضحة للعين المجردة. فالشخص المعني يستطيع بسهولة التمييز بين السند الأصلي والسند المحرّف. لذا كان لا بد عند إضافة أي تعديل أو حشو على المستند الخطي، من أن يوقع الفرقاء عليه لإعطائه المصداقية والقوة الثبوتية. إلا أن هذا الأمر يستحيل تطبيقه في السند الإلكتروني إذ ليس هناك من إمكانية تسمح بذلك في إحدى مكونات الحاسوب وذاكرته. لهذا السبب، اقتضى وجود أنظمة توفر الحماية القانونية للسند الإلكتروني ومنع أي وصول غير مشروع أو تعدي على سريته وكشف ما قد يصيبه من تعديلات بصورة غير مشروعة. من هنا بروز أهمية تطبيق وسائل التشفير[٣] وتطوير تقنياته وأنظمته[٤] لأجل توفير سرية المعلومات وصحتها، بالإضافة إلى تطوير أنظمة تسمح برصد وكشف ما إذا كان قد حصل أي تعديل غير مشروع على السند الإلكتروني. وبرز اتجاهان في مجال التشفير، فالاتجاه الأول اكتفى باللجوء إلى تطبيق وسائل التشفير في التشريع العام دون التدخل في أنظمته الخاصة لأنها قابلة التعديل، أما الاتجاه الثاني فقد حدد ضوابط تقنيات التشفير في التشريع الخاص على أن يتم تعديلها عند تغيير هذه التقنيات.

ويبرز الطابع الدولي للمسألة من خلال تخطي المعاملات الإلكترونية الحدود الجغرافية للدول، حيث أصبحت تتم على نطاق واسع كالمعاملات التي تحصل من بلد إلى بلد أو التي تتضمن عنصراً أجنبياً، بالرغم من عدم انسجام التشريعات الوطنية في هذا المجال وفي بعض الأحيان تناقضها. كما يقتضي هذا الطابع الدولي للمسألة تأمين تناسق منتجات التواقيع الإلكترونية بين مختلف الدول، ولاسيما توحيد الشروط الفنية التي تخضع لها، مما يساهم في تأمين حرية تبادلها بين الدول دون أية عوائق، الأمر الذي يدعو أيضاً إلى وضع إطار قانوني للمعاملات الإلكترونية يأخذ بطابعها الدولي ويسعى إلى تأمين الانسجام بينها.

لقد ظهر جهد واضح على الصعيد الدولي في مجال إقرار الإرشادات والتوجيهات والقوانين والقواعد المنظّمة في هذا المجال. فلقد أصدر البرلمان الأوروبي[٥] في ١٩٩٩/١٢/١٣ إرشاداً يتعلق بالتواقيع الإلكترونية. كما اعتمدت لجنة القانون التجاري الدولي لدى الأمم المتحدة في العام ٢٠٠١ قانون الأونسيترال النموذجي حول التواقيع الإلكترونية. وعلى الصعيد الوطني، لقد حدّثت الكيبيك-كندا منذ العام ١٩٩٣ قانونها من أجل الاعتراف بالقوة الثبوتية للتسجيلات المعلوماتية. كما أقرت بريطانيا في العام ١٩٩٥ قانوناً يعترف بالسند الإلكتروني، وأتبعته عام ٢٠٠٠ بقانون حول الاتصالات الإلكترونية يتضمن التوقيع الإلكتروني والتخزين الإلكتروني للمعلومات. وأصدر الرئيس الأميركي في ٢٠٠٠/٦/٣٠ قانوناً فديرالياً حول التوقيع الإلكتروني في مجال التجارة الداخلية والدولية. وأقر المشرع الفرنسي بتاريخ ٢٠٠٠/٣/١٣ القانون رقم ٢٠٠٠/٢٣٠ حول تكييف الإثبات مع تقنيات المعلوماتية وحول تعلّقه بالتواقيع الإلكترونية.

كما وظهرت معايير وبروتوكولات عديدة تهدف إلى تنظيم المعاملات الإلكترونية وتوفير الحماية والأمان للجهات الراغبة بالتواصل عبر شبكات الانترنيت وأهمها بروتوكولات التشفير[٦] وبروتوكولات التصديق[٧]. قامت بعض الدول العربية في منطقة الإسكوا بوضع تشريعات تتعلق بالمعاملات والتواقيع الإلكترونية، ومنها من وضع أيضاً لوائح تنظيمية لهذه القوانين. إلا أنه وعلى رغم مرور بضع سنوات على تلك التشريعات، ما زالت الاجتهادات المرتبطة بتلك التشريعات قليلة ولم تؤدِ بعد أي دور فعال في سبيل تطوير هذه القوانين.

وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام ١٩٩٩ المتعلق بالتواقيع الإلكترونية وبقانون الأونسيترال النموذجي حول التواقيع الإلكترونية وبالقوانين الوطنية المختلفة، في إعداد نصوص الإرشاد الحالي الموجه إلى الدول العربية حول المعاملات الإلكترونية والتواقيع الإلكترونية والإثبات الإلكتروني.

لقد تم تقسيم القانون الاسترشادي المُقترح على خمسة أبواب تتناول مختلف جوانب المعاملات الإلكترونية والتواقيع الإلكترونية والإثبات الإلكتروني. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: السندات والتواقيع الإلكترونية.
الباب الثالث: مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعوّل/المعتمد
الباب الرابع: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية.
الباب الخامس: العمليات المصرفية.

يتضمن **الباب الأول** المعنون "أحكام عامة" تحديداً لنطاق تطبيق القانون وتعاريف للمصطلحات الواردة في القانون وعرضاً للمبادئ الخاصة بالأسواق الداخلية التي يطبق عليها القانون. تحدّد المادة الأولى منه هدف القانون. فهو يرمي إلى تسهيل استخدام التواقيع الإلكترونية والاعتراف القانوني بها. وإلى حسن سير المعاملات من خلال وضع إطار قانوني للتواقيع الإلكترونية وبعض خدمات المصادقة. إلا أن الإرشاد لا يغطي الجوانب المتعلقة بإبرام وبصحة العقود أو غيرها من الموجبات القانونية عندما يكون هناك متطلبات شكلية بموجب القوانين الوطنية. ولا يمس هذا الإرشاد القواعد والقيود التي تنظم استخدام المستندات الواردة في القوانين الوطنية. فالقانون الحالي لا يسعى إلى تعديل القواعد القانونية التقليدية المختصة بالعقود والمستندات. بل إلى إدخال السندات والتواقيع الإلكترونية إلى النظام القانوني وتأمين الاعتراف بها. أما المادة ٢ من القانون. فتتضمن تعاريف لمختلف المصطلحات الواردة فيه باعتبار أن هذه المصطلحات هي إما تقنية معقدة. تتطلب بياناً لشروطها ومواصفاتها. وإما قانونية لها معانٍ خاصة يقتضي توضيحها. فالسند الإلكتروني هو القيدً أو العقد أو المراسلة التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم. والتوقيع هو علامة مميزة تسمح بتحديد هوية الشخص الموقع وتعبر عن رضاه والتزامه بمضمون السند الموقَع. أما التوقيع الإلكتروني[٨] فهو بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى. وهي تخدم كوسيلة لتأكيد الموثوقية. إن وظيفة التوقيع الإلكتروني هي. كما الحال في التوقيع اليدوي. التعريف عن هوية صاحب التوقيع وتأكيد موافقته على محتوى السند الموقّع. إلا أن شكل وآليات وضع التوقيع الإلكتروني والتحقق منه تختلف. وقد ميّز كل من التوجيه الأوروبي[٩] وقانون الأونيسترال حول التواقيع الإلكترونية بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم. إذ أن الأمر يعود إلى التقنية المستعملة لضمان سلامة التوقيع وصدوره عن الشخص الموقع.

والتوقيع الإلكتروني المتقدم هو التوقيع الرقمي المستند إلى التشفير[١٠] عبر مفتاح غير متماثل.

لا يمكن فهم التواقيع الإلكترونية دون التطرق إلى التشفير. إذ أن التوقيع بالمفاتيح العمومية والخصوصية يرتكز على وسائل التشفير؛ فالتواقيع الإلكترونية تشكل إحدى تطبيقات التشفير[١١]. التوقيع الإلكتروني يسمح بالتأكد من هوية الموقع ومن صحة المعلومات. بينما يستخدم التشفير لضمان سرية المعلومات والاتصالات. بعد توقيع السند الإلكتروني. يقتضي نقله إلى الشخص المقصود بطريقة آمنة. عبر تحويله إلى شكل غير مفهوم إلا من قبل هذا الأخير. وبالتالي فان التوقيع الإلكتروني المتقدم هو التوقيع الذي يلبي متطلبات إضافية مجتمعة تعزز من موثوقيته: منها أن يكون مرتبطاً فقط بالموقّع. وأن يسمح بتحديد الموقّع. وأن يُنشأ بوسائل تكون تحت رقابة الموقّع الحصرية. وتكون مرتبطة بالبيانات المُوقّعة ارتباطاً يجعل كل تعديل لاحق في البيانات الموقعة قابلاً للاكتشاف. وبالتالي. وبالنظر لهذه المتطلبات. يُعرف التوقيع الإلكتروني المتقدم من قرينة الموثوقية بالمقارنة مع التوقيع الإلكتروني العادي الذي يجب إثبات موثوقيته من قبل من يتمسك به. الموقّع هو كل شخص يحوز آلية لإنشاء توقيع ويتصرف إما لحسابه الخاص أو لحساب شخص طبيعي أو معنوي يمثّله. أما الطرف المعوّل أي الطرف المعتمد فهو كل شخص يجوز أن يتصرف استناداً إلى شهادة مصادقة إلكترونية أو إلى توقيع إلكتروني. الطرف المعول/المعتمد قد يكون مُستقبل الرسالة الإلكترونية الموقّعة أو حتى الأشخاص الثالثين الذين يستندون على التزام الموقع بفعل توقيعه الإلكتروني وذلك في تصرفاتهم القانونية.

إن البيانات اللازمة لإنشاء توقيع إلكتروني هي بيانات فريدة. مثل رموز أو مفاتيح تشفير خاصة[١٢]. يستخدمها الموقّع لإنشاء توقيع إلكتروني[١٣]. ويقتضي الانتباه إلى عمليات حفظ هذه البيانات أو نسخها باعتبار أنها تعرض هذه البيانات لخطر الاختراق من قبل الغير. أما الآلية لإنشاء توقيع إلكتروني. فهي برنامج معلوماتي أو تجهيزات معلوماتية معدة لتضع موضع التطبيق البيانات اللازمة لإنشاء توقيع إلكتروني. يقتضي التفريق بين الآلية العادية لإنشاء التواقيع الإلكترونية والآلية الآمنة لإنشاء التواقيع إلكترونية التي يجب أن تلبي متطلبات إضافية. تخولها بالتالي. خلافاً لتلك العادية. الاستفادة من قرينة الموثوقية. والمتطلبات الإضافية هي الوسائل التقنية والإجراءات الملائمة التي تضمن عدم مصادفة بيانات إنشاء التوقيع إلكتروني إلا مرة واحدة وكذلك سريتها. وتضمن عدم إيجاد بيانات إنشاء التوقيع بالاستنتاج

وحمايته من التزوير والتقليد[14]، وحماية بيانات إنشاء التوقيع من أي استخدام من قبل الغير، وعدم تعديل آلية التوقيع الآمنة للبيانات الموقعة. أما البيانات اللازمة للتحقق من التوقيع الإلكتروني، فهي بيانات، مثل رموز أو مفاتيح تشفير عامة[15]، تستخدم للتحقق من توقيع إلكتروني. وتُعرّف الآلية للتحقق من توقيع إلكتروني[16] بأنها برنامج أو تجهيزات معلوماتية معدة من أجل وضع بيانات التحقق من التوقيع الإلكتروني موضع التطبيق. يورد القانون في مادته الثانية عند تعريف آلية التحقق من توقيع إلكتروني قواعد موجهة لضمان فعالية هذه العملية، ولاسيما التأكد من أن البيانات المُستخدمة من أجل التحقق من التوقيع تُطابِق البيانات المعروضة بوجه المُتحقِّق المُتعامل الآخر، وأنه يمكن التحقق من التوقيع بطريقة أكيدة، وأن نتيجة التحقق تُعرض بطريقة صحيحة، وأن المُتحقِّق المُتعامل الآخر يستطيع بشكل أكيد، عند الاقتضاء، تحديد مضمون البيانات الموقّعة، وأنه يمكن التحقق من مصداقية الشهادة وصحتها، التي تكون لازمة للتحقق من التوقيع الإلكتروني، وأنه تعرض بشكل صحيح نتيجة عملية التحقق من التوقيع الإلكتروني وهوية الموقّع، وأنه يذكر بشكل واضح أنه تم استعمال اسم مستعار، وأن كل تعديل له تأثير على الأمان قابل للاكتشاف. إن ذكر اسم مستعار في شهادة المصادقة لا يعفي مزود خدمات المصادقة من الاستحصال على الهوية الحقيقية لتقديمها للسلطات عند الحاجة.

أما شهادة المصادقة الإلكترونية[17]، فهي شهادة إلكترونية تربط بين بيانات التحقق من التوقيع الإلكتروني وشخص معين وتؤكد هوية هذا الشخص. فلكل شخص نوعان من البيانات: بيانات لإنشاء التوقيع وبيانات للتحقق من هذا التوقيع. يستعمل المُوقّع بيانات إنشاء التوقيع للتوقيع، وتكون هذه البيانات محمية وتحت سلطة المُوقّع الحصرية مخافة أن يستعملها الغير للتوقيع عن المُوقّع. أما بيانات التحقق من التوقيع فهي متاحة لكل شخص ليستعملها للتحقق من صحة توقيع المُوقّع. إن بيانات الإنشاء وبيانات التحقق تكون مترابطة، إلا أنه لا يمكن استنتاج إحداها من الأخرى. يتدخل شخص ثالث[18] مستقل وحيادي ومُفترض أنه موثوق للتعريف عن المُوقّع وللمصادقة على كون بيانات معينة للتحقق من التوقيع تعود لهذا المُوقّع، وتكون شهادة المصادقة الإلكترونية موصوفة عندما تلبي بعض الشروط لجهة مشتملاتها ولجهة صدورها عن مزود خدمات مصادقة إلكترونية يلبي بدوره شروطاً خاصة. تستفيد شهادة المصادقة الإلكترونية الموصوفة بدورها من قرينة الموثوقية. يجب أن تشتمل الشهادة الموصوفة على: ذكر بأنها شهادة موصوفة، تحديد مزود خدمات المصادقة الإلكترونية والبلد الذي يقيم فيه، اسم الموقّع، صفة خاصة للموقّع، بيانات التحقق من التوقيع الإلكتروني، تحديد بداية مدة صلاحية الشهادة وانتهائها، رقم الشهادة، التوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية، حدود استخدام الشهادة، القيمة القصوى للمعاملات التي يمكن استخدام الشهادة فيها. أما الشروط الإضافية المطلوبة لمزود خدمات المصادقة الإلكترونية الصادرة عنه شهادة المصادقة الموصوفة، فهي: تقديم الإثبات على موثوقيته، تقيده بالقواعد القانونية الموضوعة لحماية البيانات ذات الطابع الشخصي، تأمين خدمة سريعة وأكيدة لدليل للشهادات وخدمة أكيدة وآنية لإلغاء الشهادات، إتاحة المجال لتحديد تاريخ ووقت إصدار الشهادة وإلغائها بشكل دقيق، التحقق بوسائل ملائمة ومتوافقة مع القوانين الوطنية من هوية ومن الصفات الخاصة للشخص الذي صدرت له الشهادة، استخدام عناصر بشرية كفوءة ومتخصصة، تطبيق إجراءات وطرق إدارية منطبقة على المعايير المتعارف عليها، استخدام أنظمة ومنتجات موثوق بها، اتخاذ تدابير ضد تزوير وتقليد الشهادات، توفير موارد مالية كافية للعمل، تسجيل جميع المعلومات الملائمة المتعلقة بالشهادة الموصوفة خلال المدة المفيدة، عدم حفظ وعدم نسخ بيانات إنشاء التوقيع الإلكتروني، التقيد بموجب إعلام المتعاملين معه، استخدام أنظمة موثوق بها من أجل حفظ الشهادات في شكل قابل للتحقق منه وفق شروط معنية.

أما مزود خدمات مصادقة إلكترونية، فهو كل هيئة أو شخص طبيعي أو معنوي يسلّم شهادات إلكترونية أو يقدم خدمات إلكترونية أخرى مرتبطة بالتواقيع الإلكترونية. يُعرّف منتوج توقيع إلكتروني بأنه كل منتوج تجهيزات أو برامج أو عنصر خاص من هذا المنتوج، معدّة للاستخدام من قبل مزود خدمات مصادقة إلكترونية من أجل تقديم خدمات التواقيع الإلكترونية، أو معدّة للاستخدام من أجل إنشاء التواقيع الإلكترونية أو التحقق منها. يُنشىء القانون الحالي نظاماً للاعتماد الاختياري لمزودي خدمات المصادقة الإلكترونية في حال تلبيتهم الشروط القانونية المطلوبة، وذلك للتشجيع على تعزيز موثوقية خدمات المصادقة المقدمة. لكن هذا النظام لا يمنع مزودي خدمات المصادقة غير المُعتمدين من العمل، بل يترك تقدير موثوقية الشهادات الصادرة عنهم وفق كل حالة للإثباتات المقدّمة. ويُعرّف الاعتماد الاختياري بأنه كل ترخيص يحدد الحقوق والموجبات الخاصة بتقديم خدمات المصادقة الإلكترونية، يُعطى، بناءً لطلب مزود خدمات المصادقة الإلكترونية المعني، من قبل هيئة عامة أو خاصة مكلفة بوضع هذه الحقوق والموجبات وبمراقبة احترامها. وتستكمل المادة ٢ التعاريف الواردة في القانون

بتعريف المصطلحات الخاصة بالعمليات المصرفية. فأمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية هو الأمر الذي ينظم كلياً أو جزئياً بوسيلة إلكترونية، ويفوض بموجبه العميل مصرفاً أو مؤسسة مالية، بإجراء دفع إلكتروني أو تحويل إلكتروني للأموال النقدية أو إتمام قيد دائن أو مدين على حسابه. أما بطاقة الدفع أو السحب المصرفية فهي أداة صادرة عن مصرف أو عن مؤسسة مالية، وهي تتيح لصاحبها سحب الأموال وتحويلها، أو سحبها فقط. والنقود الإلكترونية تتكون من وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية لمدة محددة، وتصدر مقابل نقد تتم مبادلته فوراً، بنفس القيمة ونفس العملة، وتتيح للغير دون المصدر إتمام عمليات دفع. والشيك الإلكتروني هو الشيك الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً.

أما المادة ٣ من القانون، فهي تعطي لكل دولة عضو الحق بتطبيق تشريعاتها الوطنية، التي تقرها وفقاً لهذا الإرشاد، على مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها وعلى الخدمات التي يقدمونها. كما تسمح هذه المادة بتداول منتجات التواقيع الإلكترونية المنطبقة على هذا الإرشاد بكل حرية في الأسواق الداخلية. والهدف هو تشجيع المعاملات الإلكترونية من خلال حرية تداول منتجات التواقيع الإلكترونية.

أما **الباب الثاني** المعنون "السندات والتواقيع الإلكترونية"، فإنه يتناول بالتفصيل السندات والتواقيع الإلكترونية. فالمادة ٤ من القانون تنظّم مسألة مدى انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المحددة لها في هذا القانون، وتُعطي صلاحية التحقق من ذلك لأجهزة عامة أو خاصة، وتكون نتيجة هذا التحقق مُعترفاً بها من قبل جميع الدول الأعضاء. فآليات إنشاء التواقيع الإلكترونية تشكل الضمانة التقنية لموثوقية التواقيع، وينبغي التحقق منها من قبل جهاز متخصص وموثوق. تجيز المادة ٥ فرض متطلبات إضافية لاستخدام التواقيع الإلكترونية في القطاع العام، على أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة. وهذه المتطلبات الإضافية مبررة بالنظر للثقة المُفترضة في صحة التعاملات العامة الناجمة عن تدخل طرف رسمي محايد مكلف بمهمة خدمة عامة، ولا يجب تقويض هذه الثقة من خلال تواقيع إلكترونية معرّضة ولو بشكل بسيط للتلاعب.

أما المادة ٥ من القانون، فهي تعرّف الكتابة وتضع الشروط القانونية للاعتراف بالكتابة الإلكترونية وبقوتها الثبوتية. وهذه الشروط تختصر بتحديد الشخص صاحب الكتابة وبإنشاء الكتابة وحفظها في ظروف تضمن سلامتها. إنّ الكتابة على دعامة إلكترونية تتمتع بنفس القوة الثبوتية للكتابة على دعامة ورقية. فمفهوم الكتابة هو واحد، أنّه تدوين سلسلة حروف أو أرقام أو أشكال أو أي رموز لها معنى مفهوم، أياً كانت الدعامة المستعملة ووسائل نقل المعلومات. ويقتضي التفريق بين الدعامة أو الركيزة التي توضع عليها الكتابة، والمختلفة بين ورقية أو إلكترونية، والكتابة بحد ذاتها. وتزيل المادة ٥ الالتباس الحاصل بالخلط بين الكتابة ودعامتها.

تشرّع المادة ٦ من القانون تنظيم السندات الإلكترونية العادية وكذلك الرسمية، إلا أنها تعطي الدول الخيار بحظر السندات الرسمية الإلكترونية أو بعض الفئات منها أو وضع متطلبات إضافية بخصوصها، وذلك تبعاً للاعتبارات التي جرى ذكرها أعلاه في سياق شرح المواد السابقة.

كما تتعرض المادة ٦ في فقرتها الثانية لإشكالية تعدّد النسخ في السندات الإلكترونية، إذ تختلط النسخة بالأصل في حالة السند الإلكتروني. فالنسخة هي تكرار تام للأصل، وهي مطابقة كلياً له، وقد يستحيل التمييز بينهما. لذلك، تُعتبر قاعدة تعدد النسخ الأصلية، المعمول بها بالنسبة للعقود المتبادلة المنظمة بشكل سندات عادية، مُستوفاة عندما تُنظّم وتُحفظ السندات العادية الإلكترونية وفق شروط الموثوقية المنصوص عليها في هذا الإرشاد وعندما تسمح الآليات لكل طرف بالحصول على نسخ عن السندات أو بالوصول إليها.

تقر المادة ٧ من القانون الآثار القانونية للتواقيع الإلكترونية، فهي، إذا كانت موثوقة، معادلة للتوقيع اليدوي. وتكون في جميع الحالات مقبولة أمام القضاء كوسيلة إثبات، إلا أن موثوقيتها تختلف باختلاف الوسائل التي اعتمدت لإنشائها، ويعود للمحكمة تقدير موثوقيتها من خلال الاستعانة بالخبرة الفنية. ويمكن لأشخاص يستعملون نظاماً مغلقاً لتبادل المعلومات أن يبرموا اتفاقات خطية خاصة حول الآثار القانونية لجهة الإثبات للتواقيع الإلكترونية وفق ما يرتأونه، لكن ضمن هذا النظام. وتضع المادة ٨ الشروط الأساسية للتوقيع الإلكتروني[١٩]، فهو يستلزم استخدام وسائل أو إجراءات موثوق بها من شأنها تأمين التعريف بصاحب التوقيع وتأكيد الصلة بين التوقيع والسند الذي يتعلق به. وتعطي المادة ٨ التواقيع الإلكترونية المتقدمة، والمُسندة إلى شهادات موصوفة والمُنشأة بواسطة آلية آمنة لإنشاء التواقيع موثوقية مفترضة، تُعفي من يتمسك بها من عبء

إثبات موثوقيتها. ويجب على الخصم هدم هذه القرينة بإثبات عدم الموثوقية.

تتناول المادة ٨ من القانون موضوع تزوير السندات الإلكترونية. فتنص على أنه في حال أنكر الخصم السند الإلكتروني أو التوقيع الإلكتروني أو ادعى تزويرهما، يتحقق القاضي من توفر شروط الموثوقية المنصوص عليها في هذا الإرشاد. ويمكن للقاضي الاستعانة بالخبرة الفنية من أجل التحقق من توفر هذه الشروط. يستفيد التوقيع الإلكتروني المتقدم من قرينة الموثوقية، إلا أنه يعود للقاضي، في ضوء العناصر التي تتوفر له، تقرير زوال هذه القرينة. فالتحقق من وجود تزوير يتم من خلال التثبت من توفر شروط الموثوقية المنصوص عليها في هذا القانون، والتي تضفي موثوقية مفترضة على التوقيع الإلكتروني، وكذلك من خلال التقنيات المستعملة التي يتم فحصها من قبل خبير فني متخصص.

أما المادة ٩ من القانون، فتعالج مسألة حفظ السندات الإلكترونية والشروط المطلوبة لصحة عملية الحفظ وتلافي أي تلاعب في الحفظ. فعملية الحفظ هي صحيحة عندما يتم التأكد من سلامة المعلومات واكتمالها منذ وقت بدء إنشاء هذه المعلومات لحين حفظها بالشكل الإلكتروني. لا تشكل التعديلات والمستجدات على المعلومات مساساً بسلامتها إذا تم توثيقها وفق الأصول القانونية. كذلك يُشترط لصحة عملية الحفظ أن تتم بشكلٍ يسمح بالرجوع إلى المعلومات لاحقاً وعرضها بشكل مفهوم، وأنه قد تم حفظ البيانات التقنية التي تبين منشأ المعلومات ومصدرها والجهة المرسلة إليها وتاريخ إرسالها ووقته وكذلك استلامها.

تتناول المادة ١٠ من القانون مسألة الآثار الإلكترونية والوثيقة الورقية المطبوعة عن السند الإلكتروني. فهي تعتبر الآثار الإلكترونية الصادرة عن شخص ما بمثابة بدء بينة خطية بوجه الشخص المذكور، وتعتبر الوثيقة الورقية المطبوعة عن السند الإلكتروني كصورة السند الورقي. وتتمتّع الآثار الإلكترونية بأهمية خاصة في مسائل الإثبات الإلكتروني، فكثيراً ما يشغّل المتعامل الحاسوب ويعمل على بعض الأنظمة المعلوماتية، ولكن دون التعبير صراحةً عن مراده بكتابة أو رسالة واضحة، بل يترك آثاراً لدخوله بعض البرامج أو لاستخدامها. وهذه الآثار قد تشكل دليلاً ولو غير كامل ضده.

بالانتقال إلى **الباب الثالث** المعنون "مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعول/المعتمد"، يتبيّن أنه ينظم مسؤولية كل من مزود خدمات المصادقة الإلكترونية وصاحب شهادة المصادقة والطرف المعول/المعتمد. فالمادة ١١ تضع القواعد الخاصة بمزودي خدمات المصادقة الإلكترونية، الذين لا يخضعون في المبدأ لأي ترخيص لممارسة نشاطهم، إلا أنه من الممكن إنشاء أنظمة اختيارية للاعتماد لرفع مستوى خدمات المصادقة الإلكترونية المقدمة، على أن تكون جميع المعايير المتعلقة بهذه الأنظمة موضوعية وشفافة ومتناسبة وغير مميِّزة، وعلى أن يخضع مزوّدو خدمات المصادقة المعتمدون لنظام ملائم للمراقبة. لا يعني نظام الاعتماد الاختياري بالطبع حظر مزودي خدمات المصادقة غير المُعتمدين، بل يبقى هؤلاء مجبرين على تقديم الإثباتات على موثوقية وسائلهم وموثوقية شهادات المصادقة الصادرة عنهم.

تحدد المادة ١٢ من القانون مسؤوليات مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة باعتبار أنها تتمتع بقرينة الموثوقية. فمزود خدمات المصادقة مسؤول في هذه الحالة عن الضرر الواقع على كل شخص طبيعي أو معنوي، يثق بشكل معقول بهذه الشهادة في ما خص صحة جميع المعلومات الواردة فيها وكفايتها. وهو مسؤول عن تكامل بيانات إنشاء التوقيع الإلكتروني وبيانات التحقق منه، إلا إذا أثبت أنه لم يرتكب أي إهمال. تنشأ مسؤولية مزود خدمات المصادقة من واقع أنه يتوجب عليه جمع كل المعلومات المطلوبة لإصدار شهادة المصادقة الإلكترونية وكذلك التحري عن صحة المعلومات الواردة في شهادة المصادقة وأخيراً المصادقة على أن بيانات التحقق من التوقيع تعود لشخص معين يحوز بيانات إنشاء توقيع مقابلة للنوع الأول من البيانات. كما يكون مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة، مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يستند بشكل معقول على هذه الشهادة، وذلك من أجل عدم تسجيل إلغاء الشهادة، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال. فإلغاء شهادة المصادقة يرتب زوال الموثوقية عن كل توقيع إلكتروني يتم بالاستناد إلى بيانات إنشاء التوقيع، ويفترض بالمتعامل مع الموقّع أن يكون على علم بهذا الأمر حتى يحتاط له. من هنا ينشأ موجب مزود خدمات المصادقة بتسجيل إلغاء الشهادة فوراً ونشر ذلك. كذلك يعود لمزود خدمات المصادقة الإلكترونية، وفق المادة ١٢ من القانون، أن يذكر في شهادة موصوفة القيمة القصوى للمعاملات التي يمكن استعمال الشهادة فيها، بشرط أن تكون هذه القيمة القصوى ظاهرة للغير. ولا يكون مزود خدمات المصادقة الإلكترونية مسؤولاً عن الأضرار التي تنتج عن تخطي هذه القيمة القصوى. فقد يرغب شخص معنوي بتحديد الصلاحيات المالية لممثليه بالتوقيع عنه وفق سقوف معينة كما هي حال المديرين في الشركات التجارية.

أو قد يحتاط شخص في تعامله على الإنترنت مخافة إساءة استعمال توقيعه ويفرض سقفاً لقيمة معاملاته. وفي جميع الأحوال يجب أن تظهر للمتعاملين بشكل واضح القيمة القصوى لأي معاملة إلكترونية للمُوقِّع يرغب بتوقيعها إلكترونياً، وذلك لحماية مصالحهم.

في المقابل، وفق المادة ١٣ من القانون تترتب مسؤولية على صاحب شهادة المصادقة عن صحة المعلومات المتعلقة به المقدمة إلى مزود خدمات المصادقة وتحديثها، وعن عدم اتخاذ التدابير الضرورية، كإعلام مزود خدمات المصادقة، في حال تعرض بيانات إنشاء التوقيع لما يثير الشبهة أو للانكشاف، وعن استعمال شهادة مصادقة إلكترونية موقوفة أو مُلغاة أو عن استعمال شهادة خلافاً لشروطها. ففي هذه الحالات، يكون الضرر عائداً بشكل واضح إلى فعل خاطئ صادر عن صاحب شهادة مهمل أو سيء النية.

تتعرض المادة ١٤ من القانون إلى مسؤولية الطرف المعوّل/المعتمد، فهو يكون مسؤولاً عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني أو للتحقق من صلاحية الشهادة أو وقفها أو إلغائها أو وجود قيود عليها. ففي هذه الحالات يكون الطرف المعوّل/المعتمد قد ارتكب خطأً كبيراً أو إهمالاً فاضحاً يشكل مانعاً لمسؤولية أي طرف آخر كمزود خدمات المصادقة الإلكترونية. فمن أولى البديهيات قيام الطرف المعوّل/المعتمد بالتحقق من موثوقية التوقيع الإلكتروني ومن الشهادة العائدة له، إذ أن آلية التوقيع الإلكتروني كلها، من بيانات إنشاء التوقيع إلى بيانات التحقق من التوقيع، قد صُمّمت لتمكين الطرف المعوّل/المعتمد من إجراء التحقق.

يتطرق **الباب الرابع** المعنون "الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية" إلى مفعول شهادات المصادقة الإلكترونية الصادرة في دولة أجنبية. وتعتبر المادة ١٥ من القانون شهادات المصادقة الإلكترونية الأجنبية الموصوفة معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني في إحدى ثلاث حالات: حالة تلبية الشهادة ومزود خدمات المصادقة الإلكترونية الشروط المذكورة في هذا الإرشاد مع وجود ترخيص للمزود في إحدى الدول الأعضاء، وحالة ضمان الشهادة من قبل مزود خدمات مصادقة إلكترونية وطني يلبي المتطلبات الواردة في هذا الإرشاد، وحالة كون الشهادة أو مزود خدمات المصادقة الإلكترونية معترفاً بهما تطبيقاً لاتفاق ثنائي أو متعدد الأطراف بين الدولة العضو ودول أخرى أو منظمات دولية. إن توضيح الوضعية القانونية لشهادة مصادقة إلكترونية أجنبية هو ضروري لحل الإشكاليات الناشئة عن تجاوز التعاملات الإلكترونية الحدود الوطنية بفعل الإنترنت، كما أن من شأن ذلك المساهمة في توحيد المتطلبات التي يخضع لها مزودو خدمات المصادقة وشهادات المصادقة.

ينظم **الباب الخامس** المعنون "العمليات المصرفية" هذه العمليات، أي تلك المتعلقة بأوامر الدفع والتحويل الإلكتروني للأموال النقدية وبالبطاقات المصرفية وبالنقود الإلكترونية وبالشيكات الإلكترونية.

تتناول المادة ١٦ مسألة إصدار أوامر الدفع والتحويل الإلكتروني للأموال النقدية. فحتى يكون كل طرف على بينة من حقوقه وموجباته ومن الجدوى الاقتصادية من العقد، ولحماية العميل الطرف غير الممتهن في العقد وهو الأضعف، توجب المادة ١٦ أن يتم إبرام اتفاق واضح ومفصل مسبق بين العملاء والمصارف والمؤسسات المالية على الشروط التنظيمية لأوامر الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية[٢٠]. ويجب أن تتضمن هذه الشروط تعيين تاريخ نفاذ أوامر التحويل الصادرة والواردة والعمولات المستوفاة وقيمة العملية المنجزة وحقوق فريقي العقد وموجباتهما والقواعد المختصة بالأخطاء في القيود أو القيود غير المشروعة وطرق الاعتراض المتاحة للعميل والإجراءات المتبعة في حال الدخول غير المشروع على حساب العميل وسعر الصرف المعتمد للعملة الأجنبية والقيود على العمليات. وضمانةً لحقوق فرقاء العقد وتجنباً لحدوث أي إلباس في بيان موجبات وحقوق كل طرف، تشترط المادة ١٦ أن يكون الأمر بتحويل الأموال النقدية خطياً على دعامة ورقية أو إلكترونيةً، وإذا كان الأمر صادراً بالصورة الإلكترونية، يجب التصديق عليه من قبل هيئة رسمية أو خاصة تعتمدها كل دولة عضو.

تحدد المادة ١٧ مواصفات الأنظمة الإلكترونية المستعملة في العمليات المتعلقة بأوامر الدفع والتحاويل الإلكترونية، والضمانات التقنية والقانونية المقدمة لسلامة هذه العمليات. فالأنظمة الإلكترونية يجب أن تكون قادرة على نقل أمر دفع إلكتروني أو تحويل إلكتروني للأموال النقدية مع قدرتها على تخزين البيانات المتعلقة بالأمر للتمكن من الرجوع إليه. ويجب أن تتضمن هذه البيانات تحديداً للجهة المُرسلة وإسم العميل وقيمة المبالغ وغيرها من العناصر المهمة. كما يجب أن تتيح هذه الأنظمة الإلكترونية للطرف الآمر بالدفع أو بالتحويل معرفة نتيجة هذا الأمر فوراً لجهة القبول أو الرفض وأسباب هذا الرفض.

تتكلم المادة ١٨ من القانون عن مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية. فلا يكون العميل مسؤولاً عن أي قيد جرى على حسابه ناتج عن تحويل إلكتروني للأموال النقدية، بعد قيامه بإبلاغ المصرف أو المؤسسة المالية عن وجود إمكانية لدخول الغير إلى حسابه دون وجه حق، أو عن فقدان بطاقته المصرفية أو احتمال معرفة الغير لرمز التعريف الخاص به. وعلى العميل اتباع الأصول والإجراءات المتفق عليها مع المصرف أو المؤسسة المالية بشأن معاملة التبليغ. لا يستطيع العميل أن يلغي أو يرجع أمر تحويل إلكتروني للأموال النقدية صادر عنه بعد سحب المبلغ من حسابه. فالعميل المتنبه إلى مصالحه يفترض أن يبادر إلى إبلاغ المصرف في حال وجود خطر عليها وذلك عبر إتباع طرق التبليغ المتفق عليها، ويكون حينها قد أتم واجباته، ويعود للمصرف أو للمؤسسة المالية التصرف على أساس التبليغ الحاصل.

تتعرض المادة ١٩ لمسؤولية المصرف أو المؤسسة المالية عن عدم تنفيذ أمر تحويل عميله، ولاعتراض العميل ولموجب تقديم معلومات مفصّلة له. ففي الحالة الأولى، يتحمل المصرف أو المؤسسة المالية مسؤولية عدم تنفيذ أمر التحويل كلياً أو جزئياً أو سوء تنفيذه. يتوجب عليه حينها، بالإضافة إلى التعويضات، إعادة المبالغ إلى العميل الآمر بالتحويل، إلا إذا كان عدم التنفيذ ناجماً عن خطأ أو نقص في التعليمات المعطاة من قبل الأخير.

في الحالة الثانية، أي في حال اعتراض العميل على عملية دفع إلكتروني أو تحويل إلكتروني للأموال النقدية، يتوجب على المصرف أو المؤسسة المالية أن تثبت أنه قد جرى قيد هذه العملية أصولاً وأنها لم تتعرض لأي خلل تقني في النظام المعلوماتي. ويُمنع تحميل العميل أية فوائد أو عمولات بغية تصحيح الأخطاء في قيود عمليات الدفع الإلكترونية أو قيود التحاويل الإلكترونية للأموال النقدية.

وفي جميع الأحوال، يجب على المصرف أو المؤسسة المالية تقديم معلومات منتظمة مفصلة لعملائها عن عمليات الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية.

تتناول المادة ٢٠ مسألة تعديل شروط التعاقد. فقد اشترطت قيام المصرف أو المؤسسة المالية قبل ١٠ أيام على الأقل بإبلاغ العميل صراحةً بأي تعديل مُقترح على شروط التعاقد. إلا أنه في الحالات الاستثنائية، مثل تلك المتعلقة بالحفاظ على سلامة حساب العميل أو نظام الدفع الإلكتروني، يمكن للمصرف أو المؤسسة المالية فرض قيود على الخدمة المقدمة للعميل شرط أن يصار إلى إبلاغه فوراً بالقيود ودون تحميله أية أعباء مالية من جراء ذلك. وتوازن هذه المادة من جهة بين مبدأ حماية العميل وعدم مفاجأته بشروط جديدة دون أن يكون لديه الوقت الكافي لدراستها ومن جهة ثانية بين ضرورات حماية حساب العميل بفرض قيود فورية على خدمة العميل، على أن يصار إلى إعلامه فوراً بهذه القيود. ولا ينتظر المصرف أو المؤسسة المالية في الحالات الاستثنائية موافقة العميل على فرض الإجراءات بسبب ضرورة الإسراع بالتصرف صوناً لسلامة حسابه.

تفرض المادة ٢١ من القانون أن يكون طلب الحصول على بطاقة مصرفية أو على العقد العائد لإصدارها خطياً على دعامة ورقية أو إلكترونية، وذلك منعاً لأي التباس حول مضمون العقد.

تفصل المادة ٢٢ من القانون مسؤوليات المصرف أو المؤسسة المالية عند إصدار بطاقات مصرفية، فكلاهما ملزم بموجب الإعلام تجاه أصحاب البطاقات المصرفية، وبإعطاء معلومات التعريف لأصحاب البطاقات لتمكينهم من استخدامها مع الحفاظ على السرية، وبحفظ كشوفات مفصلة عن عشر سنوات، بوضع وسائل ملائمة للإبلاغ عن فقدان البطاقة أو سرقتها، وبمنع استخدام البطاقة بعد حصول هذا الإبلاغ. كذلك، يكون المصرف أو المؤسسة المالية مسؤولين عن عدم تنفيذ الأوامر الصادرة عن صاحب البطاقة أو عن سوء تنفيذها، وكذلك عن العمليات المنفذة دون موافقته وعن الأخطاء في قيود حسابه. وعلى المصرف أو المؤسسة المالية أن يدفعا لصاحب البطاقة المبالغ المسحوبة من حسابه دون مبرر مشروع.

تفصل المادة ٢٣ من القانون مسؤوليات صاحب البطاقة المصرفية لجهة كيفية استعمال البطاقة ولجهة الاعتراض على عمليات الدفع ولجهة إبلاغ المصرف بفقدان البطاقة أو بسرقتها. فقد ورد فيها أنّ صاحب البطاقة المصرفية يلتزم باستعمال بطاقته وفق الشروط المتفق عليها ويتخذ كل الاحتياطات اللازمة لحماية البطاقة ومعلومات التعريف التي تتيح استعمالها. ولا يمكن لصاحب البطاقة المصرفية أن يرجع عن أمر الدفع الإلكتروني الصادر بواسطة هذه البطاقة. ولا يحق لصاحب البطاقة المصرفية أن يعترض على أي عملية دفع إلا في حال تعرضت بطاقته أو معلومات التعريف التي تتيح استعمالها للفقدان أو السرقة أو الاستعمال غير المشروع أو الاحتيالي أو في حال الخطأ الحاصل من قبل الجهة المصدرة للبطاقة. ويجب على صاحب البطاقة المصرفية، فور معرفته، إبلاغ المصرف أو المؤسسة بفقدانه بطاقته أو بسرقتها، وبأي عملية تمت دون موافقته.

وبأي خطأ في كشف حسابه. ويتحمل صاحب البطاقة المصرفية، حتى تاريخ إبلاغه المصرف أو المؤسسة المالية، نتائج فقدان البطاقة أو سرقتها، وذلك في حدود سقف تعينه كل دولة. لكن هذا السقف لا يطبق في حال ارتكاب صاحب البطاقة المصرفية خطأ فادحاً أو إهمالا كبيراً، أو في حال عدم قيامه بالإبلاغ وفق الفقرة السابقة ضمن مهلة معقولة.

وقد أعفت المادة ٢٣ من القانون صاحب البطاقة المصرفية من المسؤولية في عدة حالات: حالة حصول عمليات دفع بعد تقدمه باعتراض، حالة عمليات الدفع غير المشروعة المنفذة عن بعد دون تقديم البطاقة مادياً، حالة تزوير البطاقة المصرفية. وفي مثل هذه الحالات، يتولى المصرف أو المؤسسة المالية إعادة قيد المبالغ المعترض عليها في حساب صاحب البطاقة دون استيفاء أي عمولة أو نفقة، وذلك في خلال مهلة شهر من تاريخ استلام اعتراض صاحب البطاقة.

تنظم المادة ٢٤ من القانون النقود الإلكترونية، فتنص على أنها تصدر عن المصرف المركزي في دولة عضو أو عن مؤسسة مالية مرخص لها بذلك، وذلك بناءً على عقد يبرم مع العميل، على أن يتضمن العقد حقوق والتزامات الفريقين بشكل واضح. وتشكل وحدات النقود الإلكترونية ديناً على مُصدرها، يسقط بانقضاء مدة صلاحيتها، ويبرئ بالتالي ذمة مُصدرها.

تتناول المادة ٢٥ الشيك الإلكتروني محددةً مشتملاته والضمانات الخاصة به. إذ يجب أن يتضمن جميع البيانات المطلوبة قانوناً، ويعود لكل دولة عضو أن تحدد ضمانات تقنية لضمان موثوقية الشيك الإلكتروني وصحته وكذلك أن تضع قواعد تنظيمية مفصلة لكيفية استعماله. ويمكن للمصارف في الدول الأعضاء التعامل بالشيكات الإلكترونية.

تحدد المادة ٢٦ الأخيرة تحت عنوان أحكام ختامية مبدأ حق الوصول إلى المعلومات العامة. وعلى الدولة أن تضمن هذا الحق شريطة أن لا يؤدي ذلك إلى التعرض للأمن الوطني أو سلامة الدولة أو الحياة الخاصة للأفراد أو الأسرار المحمية بموجب نصوص قانونية خاصة أو أن ينتهك النظام العام في الدولة."

هوامش

1- Information Privacy in Cyberspace Transactions by Jerry Kang 1998: http://www.ntia.doc.gov/ntiahome/privacy/files/cprivacy.pdf
«Cyberspace transaction» means an interaction with an individual through cyberspace for the purposes of satisfying, accepting, or completing an individual's request, offer, lease, financing, rental, purchase, sale, or exchange of information, services, or goods. A «cyberspace transaction» specifically includes the browsing of a World Wide Web page through the hypertext transfer protocol and its subsequent extensions, regardless of whether any money is exchanged. A «cyberspace transaction» specifically excludes any portion of an interaction that is a message from an individual to an individual in a noncommercial context, or to a publicly accessible forum.

٢- أي قبل وضع تشريع ينظم المعاملات إلكترونيا"

٣ - يراجع الإثبات الالكتروني، للقاضي وسيم شفيق حجار: "ان التشفير هو من أقدم العلوم التقنية، يعود على الأقل لأربعة آلاف سنة، وقد بدأ على الأرجح حوالي عام ٢٠٠٠ قبل الميلاد في مصر الفرعونية، حيث استعمل لتزيين قبور الحكام والملوك، ليس بغرض إخفاء محتوى النصوص، بل بهدف جعلها أكثر فخامة وقدسية. في الهند استخدمت رموز سرية في العصور الغابرة للتواصل بين الحكام وجواسيسهم. كما طور اليونانيون والاسبرطيون أنظمة التشفير، ولجأت الجيوش الرومانية إلى تقنيات معينة في الكتابة من اجل تبادل رسائل مشفرة غير مفهومة من العدو. تقدم التشفير في العصور الوسطى خصوصاً في ايطاليا فينيس، حيث كرس لأهداف الاتصال بالسفراء، ووضع الكاهن الألماني Trithemius نظاماً جديداً للتشفير وترك خمس كتب حول هذا الموضوع عام ١٥١٨. في القرن السابع عشر، أنشئت في معظم الدول الأوروبية ما يعرف بالغرف السوداء Black Chambers لاستنباط تقنيات التشفير وتفكيك شيفرات الدول الأخرى. ومن ثم عرف علم التشفير خطوات أخرى، منها ابتكار دولاب التشفير الذي يتكون من عدة دوائر برّامة في قالب واحد تحتوي كل منها على الأحرف الأبجدية. وظهر بعد ذلك الدوار الكهربائي Rotor، الذي يتلقى النص غير المشفر من لوحة المفاتيح لينتج الموجة الكهربائية المناسبة على لوحة التشفير التي تخرج النص المشفر. ومع اختراع التلغراف عام ١٨٤٤، وأجهزة البث اللاسلكية عام ١٨٩٥، تم اللجوء إلى تقنيات التشفير لتوفير سرية الاتصالات".
كمثال على التشفير البدائي في تلك الحقبة، كانت الرسالة تكتب على ورق يلف حول دعامة، وحتى تفك الرسالة، يقتضي إعادة وضعها على دعامة بنفس القطر، لتأمين ترابط الكلمات والجمل وتسلسلها.

– نرفق بهذا الإرشاد رسومات لعملية التشفير بهدف مساعدة المشترع في فهم التقنية الدقيقة لهذه العملية،

-How encryption works: http://computer.howstuffworks.com/encryption1.htm

The Greek historian Plutarch wrote, for example, about Spartan generals who sent and received sensitive messages using a scytale, a thin cylinder made out of wood. The general would wrap a piece of parchment around the scytale and write his message along its length. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense. But if the other general receiving the parchment had a scytale of similar size, he could wrap the paper around it and easily read the intended message.

٤ – راجع:

– نظام DES-Data Encryption Standard http://www.itl.nist.gov/fipspubs/fip46-2.htm

DES – Data Encryption Standard http://www.cypher.com.au/crypto_history.htm
In 1972 the US National Bureau of Standards began the search for an encryption algorithm that could be tested and certified. After several false starts in 1974 IBM offered the US government an algorithm which was based on the early 1970's LUFICER algorithm. The offer was accepted and the algorithm was tested and 'adjusted' by the NSA and eventually released as a federal standard in 1976.

DES is a Symmetric block cypher based on a 64 bit block. The user feeds in a 64 block of plain text and is returned 64 bits of cyphertext. The same algorithm and key are used for the encrypt and decrypt operations.

Since its release in 1976 the key has remained fixed at 56 bits (reduced from a 128 bit key as part of the NSA 'adjustment') although it was possible to 'build' DES with a 128 bit key, exporting it from the US was banned. Recently however this key length restriction was removed by the US Government.

– نظام AES-Advanced Encryption Standard المرفق بهذا التقرير http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

AES - Advanced Encryption Standard, The Latest Encryption Algorithm http://cyberstephanians.blogspot.com/2008/02/advanced-encryption-standard-latest.html
Advanced Encryption Standard (AES) is the latest encryption standard used to protect confidential information like financial data for government and commercial use. It is a stronger symmetric encryption algorithm that was approved by NIST (National Institute of Standards and Technology) to replace the Data Encryption Standard (DES) and Triple DES encryption algorithm. DES is arguably the most important and widely used cryptographic algorithm in the world. However, its usefulness is now quite limited after years of advances in computational technology. A DES key can now be easily cracked after several hours of number crunching. By using dedicated hardware, Electronic Frontier Foundation manages to break it in 22 hours (http://www.rsasecurity.com/rsalabs/des3/).

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor,[3] the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages.

– بالإضافة الى الغوريتميات Algorithms أخرى مثال:

3-Way • ABC • Akelarre • Anubis • ARIA • BaseKing • BassOmatic • BATON • BEAR and LION • CAST-256 • CIKS-1 • CIPHERUNICORN-A • CIPHERUNICORN-E • CLEFIA • CMEA • Cobra • COCONUT98 • Crab • Cryptomeria/C2 • CRYPTON • CS-Cipher • DEAL • DES-X • DFC • E2 • FEAL • FEA-M • FROG • G-DES • GOST • Grand Cru • Hasty Pudding cipher • Hierocrypt • ICE • IDEA NXT • Intel Cascade Cipher • Iraqi • KASUMI • KeeLoq • KHAZAD • Khufu and Khafre • KN-Cipher • Ladder-DES • Libelle • LOKI97 • LOKI89/91 • Lucifer • M6 • M8 • MacGuffin • Madryga • MAGENTA • MARS • Mercy • MESH • MISTY1 • MMB • MULTI2 • MultiSwap • New Data Seal • NewDES • Nimbus • NOEKEON • NUSH • Q • RC6 • REDOC • Red Pike • S-1 • SAFER • SAVILLE • SC2000 • SHACAL • SHARK • SMS4 • Spectr-H64 • Square • SXAL/MBAL • Threefish • Treyfer • UES • Xenon • xmx • XXTEA • Zodiac.

5- The legal and market aspects of electronic signature, Study for the European Commission- DG Information Society http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

٦– لقد ظهرت عدة آليات معلوماتية (بروتوكولات) Protocole للتعامل الآمن في السوق التجاري في السنوات الأخيرة، نذكر منها:
١ . نظام PGP (Pretty good Privacy) الذي ابتكره Phil Zimmermann، وهو بسيط وسهل، إلا أن استعماله يخضع لقيود في أوروبا وأميركا. ٢ . نظام S-HTTP الذي يعتمد عدة تقنيات تشفير، ويسمح بتوقيع الرسالة البيانية بعد تشفيرها. ٣ . نظام SSL (Secure Socket layer) الذي تم تطويره من قبل شركة Netscape، وهو قابل للتطبيق فقط على المعاملات عبر شبكة الانترنت. ٤ . نظام SET (Secure Electronic Transaction) الذي وضع عام ١٩٩٦ من قبل شركتي Visa وMasercard بالاشتراك مع شركات Microsoft وIBM وNetscape، حيث يهدف هذا النظام إلى تأمين التعامل عبر استعمال البطاقة المصرفية. Francis Balle، Laurent Cohen-Tanugi، Dictionnaire du Web، 2001، Dalloz، p70

7- See Authentication Protocols, available: http://www.comptechdoc.org/independent/networking/protocol/protauthen.html
An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely:

CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP. Authentication Protocol.
EAP - Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used.
PAP - Password Authentification Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.
SPAP - Shiva PAP. Only NT RAS server supports this for clients dialing in.
DES - Data Encryption Standard for older clients and servers.
RADIUS - Remote Authentication Dial-In User Service used to authenticate users dialing in remotely to servers in a organization's network.
S/Key - A one time password system, secure against replays. RFC 2289. Authentication Protocol.
TACACS - Offers authentication, accounting, and authorization. Authentication Protocol.
MS-CHAP (MD4) - Uses a Microsoft version of RSA message digest 4 challenge and reply protocol. It only works on Microsoft systems and enables data encryption. Selecting this authentification method causes all data to be encrypted.
SKID - SKID2 and SKID3 are vulnerable to a man in the middle attack.

8- UNCITRAL Model Law on Electronic Signatures (2001), available: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

- "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

- A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html

- Methods, software programs, and systems for electronic information security http://www.freepatentsonline.com/7395436.html FIG. 3A shows a diagram of digital signature creation

9- European law (directive n.93/1999) provides three kinds of electronic signatures, each with different juridical value: 1- electronic signature (also called a weak electronic signature or light electronic signature); 2- advanced electronic signature; 3- advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (also called a secure digital signature, strong digital signature, or qualified digital signature).
http://www.symantec.com/connect/articles/digital-signatures-and-european-laws

10- OECD Guidelines for Cryptography Policy:
«Cryptography» means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.

«Encryption» means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality. http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html

١١- راجع كتاب الإثبات الالكتروني للقاضي وسيم حجار:
يفترض التشفير عنصرين: آلية التشفير Algorithm ومفتاح التشفير Clé، وإن هناك نوعين من التشفير، أو من آلية التشفير بتعبير أدق:
١. التشفير عبر المفتاح السري Clé Secrète à، أو المفتاح المتماثل Symétrique وهو يتم بتشفير المعلومات وفك تشفيرها عبر استعمال مفتاح واحد. لذا، يصبح هذا النظام أكثر عرضة للاختراق عند تعدد المستخدمين، حيث سيشترك في مفتاح التشفير هؤلاء المستخدمون جميعاً. يتم تشفير النص المنوي تشفيره مقطعاً تلو الآخر، حيث يُقسم هذا النص الى وحدات ذات حجم معين. تجدر الإشارة أخيراً إلى ان النظام الأكثر شهرة بالنسبة لهذه التقنية هو نظام DES (Data Encryption Standard) وRC4. يرتكز هذا النوع من التشفير على عمليتي استبدال حرف بآخر وتغيير تسلسل الأحرف، حيث يكون مفتاح التشفير عبارةً عن أرقام جزافية ذات طول معين Nombres Pseudoaléatoires، تنتج من برنامج معلوماتي بالاستناد الى نواة محددة Semence مثل ساعة وتاريخ إنتاج المفتاح. يُفترض هذا الأسلوب أن يكون المفتاح سرياً وغير معروف إلا من المرسل والمستقبل، وتكمن الصعوبة في نقل المفتاح الى المرسل إليه، وتتم عملية النقل هذه عادةً وفق آلية متفق عليها.

٢. التشفير عبر المفتاح العمومي (العام) Clé Publique à، أو المفتاح غير المتماثل: Asymétrique. في هذه الحالة، يُستعمل مفتاحان، واحدٌ للتشفير وآخر لفك التشفير. المفتاحان مرتبطان حسابياً، فما يمكن تشفيره بأحدهما يُمكن فكه بالآخر. يعمد المُرسِل الى تشفير الرسالة مستعملاً المفتاح العمومي للمُستقبل (هذا المفتاح معلومٌ من الجميع)، في حين يقوم المرسل إليه بحل التشفير، بعد استلامه الرسالة المُشفرة، بواسطة مفتاحه الخاص المحفوظ لديه، والذي لا يتشاركه مع احد، ولا يمكن فك التشفير إلا بواسطة المفتاح المذكور المملوك فقط من المُرسل إليه. هكذا، لا يعود ضرورياً تبادل المفاتيح عبر الشبكة المشرعة للعموم وتحمُل إمكانية اعتراض هذه المفاتيح من قبل الغير وكشفها. يستعمل هذا التشفير معادلاتٍ حسابية مقعدة، ولتبسيط الأمور يرتكز نظام إنتاج المفاتيح على حاصل ضرب رقمين أوليين بحجم كبير p و q ضمن شروطٍ حسابية معينة.

ترتبط مناعة نظام التشفير بطول المفتاح المُستعمل، الذي يُقاس بوحدة، تُسمى بيت Bit، وكلما كبُر المفتاح ازدادت صعوبة اختراقه، إلا أن إطالة المفتاح دونها سلبيات، فالمعلومات المُشفرة تكون في المبدأ أكبر حجماً من المعلومات الأساسية قبل تطبيق التشفير عليها، وتنعكس زيادة طول مفتاح التشفير على حجم المعلومات المُشفرة، فكلما ازداد طول المفتاح زاد حجم المعلومات، وبما ان نقل المعلوماتٍ يتم بوتيرة معينة b/s هي سعة خط النقل الممكنة، فإن إطالة مفتاح التشفير تستلزم وقتاً أطول لإتمام عملية نقل المعلومات بعد تشفيرها، مما يعني بطءاً في الأنظمة المعلوماتية، وارتفاعاً في كلفة النقل عبر الشبكات.

- Methods, software programs, and systems for electronic information security: http://www.freepatentsonline.com/7395436.pdf

12- An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group. www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

A system of encryption where both the encoding and decoding keys are privately held by the sender and receiver.
www.utexas.edu/lbj/21cp/ebt/glossary.htm

13- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as «public key cryptography,» which employs an algorithm using two different but mathematically related «keys;» one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an «asymmetric cryptosystem.»

14- The European Commission welcomes new legal framework to guarantee security of electronic signatures, Brussels, 30 November 1999
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/99/915&format=HTML&aged=1&language=EN&guiLanguage=en

15- Public key cryptography is a widely adopted cryptographic system used to encrypt data. Unlike symmetric cryptography, which utilizes a single key, this type of system is considered asymmetric because it relies on a pair of keys. Public key cryptography was originally introduced in the 1970s by cryptographers Whitfield Diffie and Martin Hellman. Such cryptography systems are often referred to as Diffie-Hellman encryption as a way of paying homage to the inventors.
http://www.wisegeek.com/what-is-public-key-cryptography.htm

16- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as «verified» if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

17- Entrust Securing Digital Identities & Information: http://www.entrust.com/digital-certificates.htm
Digital certificates are the evolving, current-day standard to help solve the growing concerns regarding secure online communication and the protection of sensitive data. This is particularly the case with transactions where financial institutions and their clients similarly contend that the leading impediment to online banking is security. Since traditional security measures like firewalls, anti-virus software, and login/password user authentication are no longer sufficient to address the increasing number of sophisticated online attacks, digital certificates were implemented as an alternative to basic authentication security practices

18- Entrust Securing Digital Identities & Information: http://www.entrust.com/certification-authority.htm
A certification authority is a trusted third party organization that issues digital certificates to requesting organizations after a process of verifying (or certifying as the name implies) their credentialing information. As a part of this process, an issued digital certificate contains some of that information for identification purposes: such as the certificate holder's name, organization, address, etc. By issuing the digital certificate, the certification authority attests to the organization's identification contained therein, confirming that it is a legitimate entity.

19- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signe's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.

20- 97/489/EC: Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997H0489:EN:HTML

نص الإرشاد المتعلق بالمعاملات الإلكترونية والتواقيع الإلكترونية

الباب الأول: أحكام عامة

المادة ١: نطاق التطبيق

إن الهدف من الإرشاد هو تسهيل استخدام التواقيع الإلكترونية والسندات والكتابة الإلكترونية والاعتراف القانوني بها. ويشكل الإرشاد بالتالي إطاراً قانونياً للتواقيع الإلكترونية وبعض خدمات المصادقة من أجل ضمان حسن سير المعاملات.

لا يغطي الإرشاد الجوانب المتعلقة بإبرام وبصحة العقود أو غيرها من الموجبات القانونية عندما يكون هناك متطلبات شكلية بموجب القوانين الوطنية. ولا يمس هذا الإرشاد بالقواعد والقيود التي تنظم استخدام المستندات الواردة في القوانين الوطنية.

المادة ٢: تعاريف

١. **السند الإلكتروني:** هو القيد أو العقد أو المراسلة التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم.

٢. **التوقيع:** هو علامة مميزة تسمح بتحديد هوية الشخص الموقع وتعبر عن رضاه والتزامه بمضمون السند المُوقَّع.

٣. **توقيع إلكتروني[1]:** هو بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وهي تخدم كوسيلة لتأكيد الموثوقية.

٤. **توقيع إلكتروني متقدم:** هو توقيع إلكتروني يلبي المتطلبات التالية مجتمعةً:
- أن يكون مرتبطاً فقط بالمُوقّع.
- أن يسمح بتحديد المُوقع.
- أن يُنشأ بوسائل تكون تحت رقابة المُوقّع الحصرية.
- أن يكون مرتبطاً بالبيانات المُوقّعة بشكل أن كل تعديل لاحق في البيانات المُوقّعة يكون قابلاً للاكتشاف.

٥. **مُوقّع:** هو كل شخص يحوز آلية لإنشاء توقيع ويتصرف إما لحسابه الخاص أو لحساب شخص طبيعي أو معنوي يمثّله.

٦. **طرف معوّل/معتمد:** هو كل شخص يجوز أن يتصرف استنادا إلى شهادة مصادقة إلكترونية أو إلى توقيع إلكتروني.

٧. **بيانات لازمة لإنشاء توقيع إلكتروني:** هي بيانات فريدة، مثل رموز أو مفاتيح تشفير خاصة، يستخدمها المُوقّع لإنشاء توقيع إلكتروني.

٨. **آلية لإنشاء توقيع إلكتروني:** هي برنامج معلوماتي أو تجهيزات معلوماتية معدة لتضع موضع التطبيق البيانات اللازمة لإنشاء توقيع إلكتروني.

٩. **آلية آمنة لإنشاء توقيع إلكتروني:** هي آلية لإنشاء توقيع إلكتروني تلبي المتطلبات التالية مجتمعةً، بحيث تضمن على الأقل بوسائل تقنية وبإجراءات ملائمة أن:
- البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن عملياً مصادفتها إلا مرة واحدة وأن سريتها هي مؤمنة بصورة معقولة.
- تكون هناك ضمانة كافية أن البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن إيجادها بالاستنتاج وأن يكون التوقيع محمياً من أي تزوير أو تقليد بوسائل تقنية متاحة فعلياً.
- البيانات المستخدمة لإنشاء توقيع إلكتروني هي محمية بطريقة موثوقة من قبل المُوقّع الشرعي من أي استخدام من قبل الغير.
- الآلية الآمنة للتوقيع الإلكتروني لا تعدل البيانات الموقّعة، ولا تمنع أن تعرض هذه البيانات على الموقّع قبل التوقيع.

١٠. **بيانات لازمة للتحقق من التوقيع الإلكتروني:** هي بيانات، مثل رموز أو مفاتيح تشفير عامة، تستخدم للتحقق من توقيع إلكتروني.

١١. **آلية للتحقق من توقيع إلكتروني:** هو برنامج أو تجهيزات معلوماتية معدة من أجل وضع بيانات التحقق من التوقيع الإلكتروني موضع التطبيق عند التحقق من توقيع إلكتروني، من المناسب التأكد مما يلي:
- أن البيانات المُستخدمة من أجل التحقق من توقيع، تُطابق البيانات المعروضة بوجه المُتحقِّق المُتعامل الآخر.

- إمكانية التحقق من التوقيع بطريقة أكيدة والتأكد من أن نتيجة التحقق تُعرض بطريقة صحيحة.
- أن المُتحقِّق المُتعامل الآخر يستطيع بشكل أكيد، عند الاقتضاء، تحديد مضمون البيانات الموقّعة.
- إمكانية التحقق من مصداقية الشهادة وصحتها، وهو أمر ضروري للتحقق من التوقيع الإلكتروني.
- إمكانية تعرض نتيجة عملية التحقق من التوقيع الإلكتروني وهوية الموقّع بشكل صحيح.
- أن يتم التنويه وبشكل واضح أنه تم عن استعمال اسم مستعار.
- أن كل تعديل له تأثير على الأمان قابل للاكتشاف.

١٢. **شهادة مصادقة إلكترونية:** هي شهادة إلكترونية تربط بين بيانات التحقق من التوقيع الإلكتروني وبين شخص معين وتؤكد هوية هذا الشخص.

١٣. **شهادة مصادقة إلكترونية موصوفة:** هي شهادة إلكترونية تشتمل على التالي:
- إشارة إلى أنها شهادة موصوفة.
- تحديد مزود خدمات المصادقة الإلكترونية والبلد الذي يقيم فيه.
- اسم الموقّع.
- صفة خاصة للموقّع عند الاقتضاء في ضوء كيفية استخدام شهادة المصادقة.
- بيانات التحقق من التوقيع الإلكتروني والتي تقابل بيانات إنشاء التوقيع الإلكتروني. الموضوعة تحت رقابة الموقّع.
- تحديد بداية مدة صلاحية الشهادة وانتهائها.
- رقم الشهادة.
- التوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية الذي أصدر الشهادة.
- حدود استخدام الشهادة.
- القيمة القصوى للمعاملات التي يمكن استخدام الشهادة فيها.

كما يجب أن تكون الشهادة صادرة من قبل مزود خدمات مصادقة إلكترونية يلبي الشروط التالية:
- أن يقدم الإثبات أنه موثوق كفاية لتقديم خدمات المصادقة الإلكترونية.
- أن يتقيد بالقواعد القانونية الموضوعة لحماية البيانات ذات الطابع الشخصي.
- أن يؤمن خدمة سريعة وأكيدة لدليل الشهادات وخدمة أكيدة وآنية لإلغاء الشهادات.
- أن يسهر على أنه يمكن تحديد تاريخ ووقت إصدار الشهادة وإلغائها بشكل دقيق.
- أن يتحقق، بوسائل ملائمة ومتوافقة مع القوانين الوطنية، من هوية ومن الصفات الخاصة للشخص الذي صدرت له الشهادة.
- أن يستخدم عناصر بشرية، تكون لديها المعارف المتخصصة والخبرات والمؤهلات الضرورية لتقديم الخدمات، وعلى وجه الخصوص، مؤهلات على مستوى الإدارة، معارف متخصصة في تكنولوجيا التواقيع الإلكترونية وممارسة جيدة لإجراءات الأمان الملائمة. وكذلك أن يطبق إجراءات وطرقاً إدارية منطبقة على المعايير المتعارف عليها.
- أن يستخدم أنظمة ومنتجات موثوقاً بها، تكون محمية من التعديلات وتوفر الأمان التقني والتشفيري للوظائف التي تنفذها.
- أن يتخذ تدابير ضد تزوير وتقليد الشهادات، وفي حالة كان ينتج بيانات لإنشاء التوقيع الإلكتروني، أن يؤمن السرية خلال عملية الإنتاج.
- أن تكون لديه موارد مالية كافية للعمل وفق متطلبات هذا الإرشاد، وعلى وجه الخصوص لتحمل المسؤولية عن الأضرار من خلال توفير ضمانات مناسبة.
- أن يسجّل جميع المعلومات الملائمة المتعلقة بشهادة موصوفة خلال المدة المفيدة، ولاسيما من أجل تقديم الدليل على الشهادة أمام القضاء. هذه التسجيلات ممكن أن تتم بطرق إلكترونية.
- أن لا يحفظ أو ينسخ بيانات إنشاء التوقيع الإلكتروني التي قدم لها خدمات إدارة المفاتيح.
- قبل التعاقد مع شخص يطلب شهادة، أن يعلم فيها هذا الشخص بشروط وبكيفية استخدام الشهادة، ولاسيما القيود على الاستخدام، وبإجراءات المطالبة وتسوية النِزاعات. هذه المعلومات، التي من الممكن نقلها بوسائل إلكترونية، يجب أن تكون خطية وفي لغة مفهومة بسهولة. إن بعض هذه المعلومات الملائمة يجب - أن توضع بتصرف الغير، بناءً لطلب، واستناداً إلى الشهادة.
- أن يستخدم أنظمة موثوق بها من أجل حفظ الشهادات في شكل قابل للتحقق منه وفق الشروط التالية:
- وحدهم الأشخاص المرخص لهم قادرون على إدخال معلومات وتعديلها.
- المعلومات تخضع للرقابة لجهة مصداقيتها.

الشهادات لا تكون متاحة لأبحاث الجمهور إلا بعد موافقة صاحب الشهادة.
- كل تعديل تقني يتعرّض لمتطلبات الأمان يكون ظاهراً للمشغل.

١٤. **مزود خدمات مصادقة إلكترونية[٢٢]:** هو كل هيئة أو شخص طبيعي أو معنوي يسلّم شهادات إلكترونية أو يقدم خدمات إلكترونية أخرى مرتبطة بالتواقيع الإلكترونية.

١٥. **منتوج توقيع إلكتروني:** هو كل منتوج تجهيزات أو برامج أو عنصر خاص من هذا المنتوج، معدّة للاستخدام من قبل مزود خدمات مصادقة إلكترونية من أجل تقديم خدمات التواقيع الإلكترونية، أو معدّة للاستخدام من أجل إنشاء التواقيع الإلكترونية أو التحقق منها.

١٦. **الاعتماد الاختياري:** هو كل ترخيص يحدد الحقوق والموجبات الخاصة بتقديم خدمات المصادقة الإلكترونية، يُعطى، بناءً لطلب مزود خدمات المصادقة الإلكترونية المعني، من قبل هيئة عامة أو خاصة مكلفة بوضع هذه الحقوق والموجبات وبمراقبة احترامها.

١٧. **أمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية:** هو الأمر الذي ينظم كلياً أو جزئياً بوسيلة إلكترونية، ويفوض بموجبه العميل مصرفاً أو مؤسسة مالية، بإجراء دفع إلكتروني أو تحويل إلكتروني للأموال النقدية أو إتمام قيد دائن أو مدين على حسابه.

١٨. **بطاقة الدفع أو السحب المصرفية:** هي أداة صادرة عن مصرف أو عن مؤسسة مالية، وهي تتيح لصاحبها سحب الأموال وتحويلها، أو سحبها فقط.

١٩. **النقود الإلكترونية:** تتكون من وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية لمدة محددة، وتصدر مقابل نقد تتم مبادلته فوراً، بنفس القيمة ونفس العملة، وتتيح للغير دون المصدر إتمام عمليات دفع.

٢٠. **الشيك الإلكتروني:** هو الشيك الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً.

المادة ٣: مبادئ متعلقة بالأسواق الداخلية

تطبق كل دولة عضو التشريعات الوطنية التي تقرها وفقاً لهذا الإرشاد، على مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها وعلى الخدمات التي يقدمونها.
تسهر الدول الأعضاء على إمكانية تداول منتجات التواقيع الإلكترونية المنطبقة على هذا الإرشاد بكل حرية في الأسواق الداخلية.

الباب الثاني: السندات والتواقيع الإلكترونية[٢٣]

المادة ٤: الآليات الآمنة لإنشاء التوقيع الإلكتروني

إن انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المبيّنة في التعاريف أعلاه تحدد من قبل أجهزة مختصة، عامة أو خاصة، تعيّن من قبل الدول الأعضاء.

إن التحقق من انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المعينة في التعاريف أعلاه يكون معترفاً به من قبل مجموع الدول الأعضاء في الإسكوا[٢٤].
يمكن أن تخضع الدول الأعضاء استخدام التواقيع الإلكترونية في القطاع العام لمتطلبات إضافية، هذه المتطلبات يجب أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة.

المادة ٥: مفهوم الكتابة الإلكترونية والآثار القانونية للسندات والكتابة الإلكترونية

الكتابة هي تدوين سلسلة حروف أو أرقام أو أشكال أو أي رموز لها معنى مفهوم، أياً كانت الدعامة المستعملة ووسائل نقل المعلومات. تعتمد الكتابة والسندات بالشكل الإلكتروني تماماً كالكتابة والسندات على دعامة ورقية، شرط تحديد الشخص الصادرة عنه؛ على أن تُنشأ وتحفظ في ظروف من شأنها أن تضمن سلامتها. ويكون للكتابة والسندات على دعامة إلكترونية نفس القوة الثبوتية للكتابة والسندات على دعامة ورقية.

المادة ٦: السندات العادية والرسمية الإلكترونية

يمكن تنظيم السندات العادية والسندات الرسمية بالشكل الإلكتروني، إلا أنه يعود للدول الأعضاء عدم اعتماد السندات الرسمية الإلكترونية أو بعض الفئات منها، كما يعود لها فرض متطلبات إضافية بالنسبة لها.

إن قاعدة تعدد النسخ الأصلية المعمول بها بالنسبة للعقود المتبادلة المنظمة بشكل سندات عادية تُعتبر مستوفاة عندما تُنظّم وتُحفظ السندات العادية الإلكترونية وفق شروط الموثوقية المنصوص عليها في هذا الإرشاد وعندما تسمح الآليات المعتمدة لكل طرف بالحصول على نسخ عن السندات أو بالوصول إليها.

المادة ٧: الآثار القانونية للتواقيع الإلكترونية

يستلزم التوقيع الإلكتروني استخدام وسائل أو إجراءات موثوق بها من شأنها تأمين التعريف بصاحب التوقيع وتأكيد الصلة بين التوقيع والسند الذي يتعلق به. تسهر الدول الأعضاء على أن تكون التواقيع الإلكترونية المتقدمة، والمُسندة إلى شهادات موصوفة والمُنشأة بواسطة آلية آمنة لإنشاء التواقيع:

- تلبي متطلبات القانون لناحية وجود توقيع في ما خص البيانات الإلكترونية، تماماً كالتوقيع اليدوي في ما خص البيانات المكتوبة أو المطبوعة على الورق.
- تكون مقبولة كوسيلة إثبات أمام القضاء.
- تستفيد من قرينة الموثوقية.

بخصوص التوقيع الإلكتروني، تسهر الدول الأعضاء على أن لا ترفض فعاليته القانونية وقبوله كوسيلة إثبات لمجرد:

- أن التوقيع هو بشكل إلكتروني.
- أو أن التوقيع لا يستند إلى شهادة موصوفة.
- أو أن التوقيع لا يستند إلى شهادة موصوفة صادرة عن مزود خدمات مصادقة إلكترونية مُرخص له.
- أو أن التوقيع غير مُنشأ بواسطة آلية آمنة لإنشاء التواقيع.

المادة ٨: التحقق من صحة وموثوقية السندات والتواقيع الإلكترونية

في حال أنكر الخصم السند الإلكتروني أو التوقيع الإلكتروني أو ادعى تزويرهما، يتحقق القاضي من توفر شروط الموثوقية المنصوص عنها في هذا الإرشاد. ويمكن للقاضي الاستعانة بالخبرة الفنية من أجل التحقق من توفر هذه الشروط.

يستفيد التوقيع الإلكتروني المتقدم من قرينة الموثوقية، إلا أنه يعود للقاضي القول، في ضوء العناصر التي تتوفر له، بزوال هذه القرينة.

المادة ٩: حفظ السندات الإلكترونية

عندما يشترط القانون حفظ سند أو معلومات، تكون عملية الحفظ بالشكل الإلكتروني صحيحة إذا:

- تم التأكد من سلامة المعلومات واكتمالها منذ وقت بدء إنشاء هذه المعلومات لحين حفظها بالشكل الإلكتروني. لا تشكل التعديلات والمستجدات على المعلومات مساساً بسلامة المعلومات إذا تم توثيقها وفق الأصول القانونية.
- تم حفظ المعلومات بشكلٍ يسمح بالرجوع إليها لاحقاً وعرضها بشكل مفهوم.
- تم حفظ البيانات التقنية التي تبين منشأ المعلومات ومصدرها والجهة المرسلة إليها وتاريخ إرسالها ووقته وكذلك استلامها.

المادة ١٠: الآثار الإلكترونية والوثيقة الورقية المطبوعة عن السند الإلكتروني

تعتبر الآثار الإلكترونية الصادرة عن شخص ما بمثابة بدء بينة خطية بوجه الشخص المذكور.

تكون للوثيقة الورقية المطبوعة عن السند الإلكتروني الآثار القانونية نفسها لصورة السند الورقي.

الباب الثالث: مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعول/ المعتمد

المادة ١١: مزودو خدمات المصادقة الإلكترونية

لا تُخضع الدول الأعضاء تقديم خدمات المصادقة لأي ترخيص مسبق. مع مراعاة الفقرة الأولى، يمكن للدول المتعاقدة أن تعتمد أنظمة اختيارية تهدف إلى رفع مستوى خدمات المصادقة الإلكترونية المقدمة. جميع المعايير المتعلقة بهذه الأنظمة يجب أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة.

تسهر كل دولة عضو على وضع نظام ملائم لمراقبة مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها والذين يصدرون شهادات مصادقة إلكترونية موصوفة للجمهور.

المادة ١٢: مسؤوليات مزود خدمات المصادقة الإلكترونية

تسهر الدول الأعضاء على أن مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة أو يضمن مثل هذه الشهادة، يكون مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يثق بشكل معقول بهذه الشهادة في ما خص:

- صحة جميع المعلومات الواردة في الشهادة الموصوفة في التاريخ الذي صدرت فيه، وتضمن الشهادة جميع المعلومات المفروضة قانوناً.
- ضمان أن بيانات إنشاء التوقيع الإلكتروني وبيانات التحقق منه قابلة للاستعمال بشكل متكامل، في الحالة التي ينتج مزود خدمات المصادقة هذين النوعين من البيانات، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال.

أن مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة، يكون مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يستند بشكل معقول على هذه الشهادة، وذلك من أجل عدم تسجيل إلغاء الشهادة، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال.

يعود لمزود خدمات المصادقة الإلكترونية أن يذكر في شهادة موصوفة القيمة القصوى للمعاملات التي يمكن استعمال الشهادة فيها، بشرط أن تكون هذه القيمة القصوى ظاهرة للغير.

لا يكون مزود خدمات المصادقة الإلكترونية مسؤولاً عن الأضرار التي تنتج عن تخطي هذه القيمة القصوى.

المادة ١٣: مسؤولية صاحب شهادة المصادقة

يكون صاحب شهادة المصادقة مسؤولاً:
- عن صحة المعلومات المتعلقة به والتي قدمها لمزود خدمات المصادقة وكذلك عن تحديثها عند الاقتضاء.
- عن عدم اتخاذ التدابير الضرورية في حال تعرض بيانات إنشاء التوقيع لما يثير الشبهة أو للانكشاف، ولاسيما عن إعلام مزود خدمات المصادقة بذلك.
- عند استعماله شهادة مصادقة إلكترونية موقوفة أو مُلغاة أو عن استعمال شهادة خلافاً لشروطها.

المادة ١٤: مسؤولية الطرف المعوّل/المعتمد

يكون الطرف المعوّل/المعتمد مسؤولاً:
- عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني.
- عن عدم اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مُسنداً إلى شهادة مصادقة إلكترونية، لأجل التحقق من صلاحية الشهادة أو وقفها أو إلغائها وكذلك من وجود أي قيود على استعمال الشهادة.

الباب الرابع: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية

المادة ١٥: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية

إن شهادات المصادقة الإلكترونية المُسلَّمة على أنها موصوفة من قبل مزود خدمات مصادقة إلكترونية في بلد أجنبي، تُعتبر معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني:
- إذا كانت الشهادة ومزود خدمات المصادقة الإلكترونية يلبيان الشروط المذكورة في هذا الإرشاد وقد جرى الترخيص للمزود اختيارياً في إحدى الدول الأعضاء.
- أو إذا ضمنت الشهادة من قبل مزود خدمات مصادقة إلكترونية وطني، يلبي المتطلبات الواردة في هذا الإرشاد.
- أو إذا كانت الشهادة أو مزود خدمات المصادقة الإلكترونية معترفاً بهما تطبيقاً لاتفاق ثنائي أو متعدد الأطراف بين الدولة العضو ودول أخرى أو منظمات دولية.

الباب الخامس: العمليات المصرفية

المادة ١٦ : إصدار أوامر الدفع والتحويل الإلكترونية للأموال النقدية

يجب أن يسبق أية عملية دفع أو تحويل إلكتروني وضع اتفاق واضح ومفصل بين العملاء والمصارف والمؤسسات المالية على الشروط التنظيمية لأوامر الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية. ويجب أن تتضمن هذه الشروط تعيين تاريخ نفاذ أوامر التحويل الصادرة والواردة والعمولات المستوفاة وقيمة العملية المنجزة وحقوق فريقي العقد وموجباتهما والقواعد المختصة بالأخطاء في القيود أو القيود غير المشروعة وطرق الاعتراض المتاحة للعميل والإجراءات المتبعة في حال الدخول غير المشروع على حساب العميل وسعر الصرف المعتمد للعملة الأجنبية والقيود على العمليات.

يجب أن يكون الأمر بتحويل الأموال النقدية خطياً على دعامة ورقية أو إلكترونية. وإذا كان الأمر صادراً بالصورة الإلكترونية، يجب التصديق عليه من قبل هيئة رسمية أو خاصة تعتمدها كل دولة عضو.

المادة ١٧: الأنظمة الإلكترونية لأوامر الدفع أو التحاويل الإلكترونية

يجب أن تكون الأنظمة الإلكترونية المُستعملة قادرة على نقل أمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية وعلى تخزين البيانات المتعلقة بالأمر للتمكن من الرجوع إليه. ويجب أن تتضمن هذه البيانات تحديداً للجهة المُرسلة واسم العميل وقيمة المبالغ وغيرها من العناصر المهمة اللازمة للتأكد من صحة أمر الدفع. كما يجب أن تتيح هذه الأنظمة الإلكترونية للطرف معطي الآمر بالدفع أو بالتحويل معرفة نتيجة هذا الأمر فوراً لجهة القبول أو الرفض وأسباب هذا الرفض.

المادة ١٨: مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية

لا يكون العميل مسؤولاً عن أي قيد جرى على حسابه

ناتج عن تحويل إلكتروني للأموال النقدية، بعد قيامه بإبلاغ المصرف أو المؤسسة المالية عن وجود إمكانية لدخول الغير إلى حسابه دون وجه حق، أو عن فقدان بطاقته المصرفية أو احتمال معرفة الغير لرمز التعريف الخاص به. وعلى العميل اتباع الأصول والإجراءات المتفق عليها مع المصرف أو المؤسسة المالية بشأن معاملة التبليغ. لا يستطيع العميل أن يلغين يرجع أأ أمر تحويل إلكتروني للأموال النقدية صادراً عنه بعد سحب المبلغ من حسابه.

المادة ١٩: مسؤولية المصرف أو المؤسسة المالية عن أوامر الدفع أو التحاويل الإلكترونية

يتحمل المصرف أو المؤسسة المالية مسؤولية عدم تنفيذ أمر التحويل كلياً أو جزئياً أو سوء تنفيذه، يتوجب عليه حينها، بالإضافة إلى التعويضات، إعادة المبالغ إلى العميل الآمر بالتحويل، إلا إذا كان عدم التنفيذ ناجماً عن خطأ أو نقص في التعليمات المعطاة من قبل الأخير.

في حال اعتراض العميل على عملية دفع إلكتروني أو تحويل إلكتروني للأموال النقدية، يتوجب على المصرف أو المؤسسة المالية أن تثبت أنه قد جرى قيد هذه العملية أصولاً وأنها لم تتعرض لأي خلل تقني في النظام المعلوماتي. ويُمنع تحميل العميل أية فوائد أو عمولات بغية تصحيح الأخطاء في قيود عمليات الدفع الإلكترونية أو قيود التحاويل الإلكترونية للأموال النقدية.

يجب على المصرف أو المؤسسة المالية تقديم معلومات منتظمة مفصلة لعملائها عن عمليات الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية.

المادة ٢٠: تعديل شروط التعاقد

يجب على المصرف أو المؤسسة المالية أن يبلغ العميل صراحة، قبل ١٥[١٠] أيام على الأقل، عن رغبته بإجراء أي تعديل على شروط التعاقد لا سيما تلك المتعلقة بالعمولات أو القيود على العمليات.

إلا أنه في الحالات الاستثنائية، مثل تلك المتعلقة بالحفاظ على سلامة حساب العميل أو نظام الدفع الإلكتروني، يمكن للمصرف أو المؤسسة المالية فرض قيود على الخدمة المقدمة للعميل شرط أن يصار إلى إبلاغه فوراً بالقيود ودون تحميله أية أعباء مالية من جراء ذلك.

المادة ٢١: إصدار بطاقة مصرفية

يجب اعتماد الصيغة الخطية على دعامة ورقية أو إلكترونية لطلب الحصول على بطاقة مصرفية أو على العقد العائد لإصدارها.

المادة ٢٢: مسؤوليات المصرف أو المؤسسة المالية في ما خص البطاقات المصرفية

يجب على المصرف، أو المؤسسة المالية التي تصدر بطاقات مصرفية:

١- أن تُعلم صاحب البطاقة المصرفية بخصائص هذه البطاقة وبنظام استعمالها.

٢- أن تعطي صاحب البطاقة المصرفية معلومات التعريف التي تخوله استعمالها، مع ضمان سرية هذه المعلومات.

٣- أن تحفظ كشوفات مفصلة عن العمليات المنجزة بواسطة البطاقة في السنوات العشر الأخيرة.

٤- أن تتيح لصاحب البطاقة المصرفية إبلاغها عن فقدان البطاقة أو سرقتها وذلك بوسائل ملائمة.

٥- أن تمنع أي استخدام للبطاقة المصرفية فور الإبلاغ عن فقدانها أو سرقتها.

يقوم صاحب البطاقة بالتأشير على حسن إعلامه واستلامه الخصائص والمعلومات الخاصة بالبطاقة عبر توقيعه على وثيقة تفيد بذلك، وعليه أن يضع عبارة "عُلم مع الموافقة" بخط يده.

يكون المصرف أو المؤسسة المالية مسؤولين عن عدم تنفيذ الأوامر الصادرة عن صاحب البطاقة أو عن سوء تنفيذها، وكذلك عن العمليات المنفذة دون موافقته وعن الأخطاء في قيود حسابه. وعليهما أن يدفعا لصاحب البطاقة المبالغ المسحوبة من حسابه دون مبرر مشروع، أو بخلاف ما هو متفق عليه بالعقد.

المادة ٢٣: مسؤوليات صاحب البطاقة المصرفية

يلتزم صاحب البطاقة المصرفية باستعمال بطاقته المصرفية وفق الشروط المتفق عليها وبأن يتخذ كل الاحتياطات اللازمة لحماية البطاقة ومعلومات التعريف التي تتيح استعمالها.

لا يمكن لصاحب البطاقة المصرفية أن يرجع عن أمر الدفع الإلكتروني الصادر بواسطة هذه البطاقة.

لا يحق لصاحب البطاقة المصرفية أن يعترض على أي عملية دفع إلا في حال تعرضت بطاقته أو معلومات التعريف التي تتيح استعمالها للفقدان أو السرقة أو الاستعمال غير المشروع أو الاحتيالي أو في حال الخطأ الحاصل من قبل الجهة المصدرة للبطاقة.

يجب على صاحب البطاقة المصرفية، فور معرفته بذلك، إبلاغ المصرف أو المؤسسة بفقدانه بطاقته المصرفية أو بسرقتها، وبأي عملية تمت دون موافقته، وبأي خطأ في كشف حسابه . يتحمل صاحب البطاقة المصرفية، حتى تاريخ إبلاغه المصرف أو المؤسسة المالية، نتائج فقدان البطاقة أو سرقتها، وذلك في حدود سقف يتم تعيينه في التشريع الوطني. لكن هذا السقف لا يطبق في حال ارتكاب صاحب البطاقة المصرفية خطأ فادحاً أو إهمالا كبيراً، أو في حال عدم قيامه بالإبلاغ وفق الفقرة السابقة ضمن مهلة معقولة. لا يكون صاحب البطاقة المصرفية مسؤولاً عن:

١- عمليات الدفع المجراة بعد اعتراضه على استخدام البطاقة المصرفية.
٢- عمليات الدفع المنفذة عن بعد بشكل غير مشروع أو احتيالي، دون تقديم البطاقة المصرفية مادياً أو تحديد هوية الآمر بالدفع.
٣- تزوير البطاقة المصرفية إذا كانت مادياً في حيازته لدى إجراء العملية المعترض عليها.

وفي مثل هذه الحالات، يتولى المصرف أو المؤسسة المالية إعادة قيد المبالغ المعترض عليها في حساب صاحب البطاقة دون استيفاء أي عمولة أو نفقة، وذلك في خلال مهلة شهر من تاريخ استلام اعتراض صاحب البطاقة.

المادة ٢٤: النقود الإلكترونية

تصدر النقود الإلكترونية عن المصرف المركزي في الدولة أو عن مؤسسة مالية مرخص لها بذلك، وذلك بناءً لعقد يبرم مع العميل، على أن يتضمن العقد حقوق والتزامات الفريقين بشكل واضح.

تشكل وحدات النقود الإلكترونية ديناً على مُصدرها، يسقط بانقضاء مدة صلاحيتها، ويبرئ بالتالي ذمة مُصدرها.

المادة ٢٥: الشيك الإلكتروني

يجب أن يتضمن الشيك الإلكتروني جميع البيانات المطلوبة قانوناً بحسب القوانين المالية أو المصرفية، ويعود لكل دولة عضو أن تحدد ضمانات تقنية لضمان موثوقية الشيك الإلكتروني وصحته، وكذلك وضع قواعد تنظيمية مفصلة لكيفية استعماله. يمكن للمصارف العاملة في الدولة التعامل بالشيكات الإلكترونية.

المادة ٢٦: أحكام ختامية

على الدولة أن تضمن للإفراد حق الوصول إلى المعلومات العامة والمستندات الموجودة لدى المؤسسات والإدارات العامة، شرط أن لا يؤدي ذلك إلى التعرض للأمن الوطني أو سلامة الدولة أو علاقاتها الخارجية لدولة ذات الطابع السري أو مصالحها الاقتصادية العليا أو الحياة الخاصة للأفراد أو الأسرار المحمية بموجب نصوص قانونية خاصة أو أن ينتهك ذلك النظام العام في الدولة.

هوامش

٢١- التوقيع الالكتروني = التوقيع الرقمي

٢٢- مزود خدمات مصادقة الكترونية = مقدم خدمات التصديق (السعودية/سلطنة عمان/دبي)؛ مزود خدمات التصديق الالكتروني (سوريا)، مزود خدمة شهادات معتمد (البحرين)

٢٣- إن الإرشاد الحاضر هو في الأصل موجه إلى الدول الأعضاء في الإسكوا حتى تلك التي وضعت تشريعات خاصة بها للفضاء السيبراني

٢٤- ١٠ أيام هي المدة المُقترحة ويمكن تعديلها زيادةً او نقصاناً على ألا تقل عن الفترة اللازمة لتمكين صاحب العلاقة من تعديل شروط التعاقد.

الإرشاد الثالث

التجارة الإلكترونية وحماية المستهلك

٣

الورقة البحثية الخلفية لإرشاد التجارة الإلكترونية وحماية المستهلك

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع التجارة الإلكترونية وحماية المستهلك في الدول العربية الأعضاء في الإسكوا. رصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية. وبالتالي تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بالتجارة الإلكترونية وحماية المستهلك.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والاقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالتجارة الإلكترونية وحماية المستهلك.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) الخطابات أو الرسائل الإلكترونية التجارية: تتناول إسناد الرسائل الإلكترونية وإشعارات استلام الرسائل الإلكترونية وزمان ومكان استلام وتسليم الرسالة الإلكترونية والمعلومات الواجب تقديمها في هذا المجال والخطابات أو الرسائل التجارية غير المرغوب بها والمهن المنظّمة بقانون والشروط والقيود والضوابط المفروضة على الخطابات والرسائل الإلكترونية بهدف حماية المستهلك.

٢) العقود الإلكترونية: تتناول مسألة الاعتراف القانوني بهذه العقود وإشكالية استخدام أنظمة الرسائل المعلوماتية الآلية في تكوين العقود والمعلومات الواجب تقديمها وكيفية إجراء طلبية ووجوب تحديد الأسعار وإتاحة المجال للمستهلك للعدول عن طلبه ومسؤولية المحترف.

٣) قواعد التصرف والحلول غير القضائية للنزاعات والمراجعات القضائية: تتناول القواعد والمبادئ التي تهدف إلى حماية المستهلك وتنظيم الاتصالات والعقود التجارية.

وتتضمن الحلول غير القضائية للنزاعات في مجال التجارة الإلكترونية كالوساطة والتحكيم عبر الشبكة الإلكترونية من اجل تسوية الخلافات بالطرق السريعة التي تتناسب مع متطلبات التجارة الإلكترونية.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي المتعلقة بهذا المجال ومنها:

- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996 with additional article 5 bis as adopted in 1998.

- UNCITRAL Model Law on International Commercial Arbitration, 1994.

- United Nations Convention on the Use of Electronic Communications in International Contracts.

- Convention on the Recognition and Enforcement of Foreign Arbitral Awards - the "New York" Convention, June 1958 adopted by uncitral.
http://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/1958_NYC_CTC-e.pdf

- Directive 97/55/EC of European Parliament and of 6 October 1997 amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising.

- 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").

- Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

- OECD guidelines for Consumer protection in the context of Electronic commerce
http://www.oecd.org/dataoecd/18/29/34023811.pdf

- Green Paper on European Union Consumer Protection COM(2001) 531, October 2001

- GREEN PAPER on alternative dispute resolution in civil and commercial law, Brussels, 19.04.2002 COM(2002) 196 final
http://eur-lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0196en01.pdf

- Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Official Journal L 012 , 16/01/2001 P. 0001 - 0023
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:HTML

- Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters of 27 September 1968,
http://curia.europa.eu/common/recdoc/convention/en/c-textes/brux-idx.htm

٢) بالإضافة إلى ذلك تناولت أعمال البحث بعض قواعد التصرف والاتفاقيات الجماعية التي تحكم العلاقة التجارية فيما بين المهنيين والمستهلكين والتي تهدف إلى حماية المستهلك:

- Uniform Rules of conduct for Interchange of Trade Data by Teletransmission (UNCID)
http://www.unece.org/trade/untdid/texts/d220_d.htm

- FEDMA Code on E-commerce & Interactive marketing, Federation of European Direct Marketing, 5 September 2000
http://www.fedma.org/getfile.php/342989.1014.xdpffdbpwd/Code_of_conduct_for_e-commerce.pdf

- APTICE Code of Practice for e-commerce and e-government, 2001. Spain.
http://www.agace.org/en/pdfs/AGACE_code_of_practice.pdf

- Canadian Code of Practice for Consumer Protection In Electronic Commerce,
http://www.cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00072.html

- The Australian Guidelines for Electronic Commerce , Commonwealth of Australia 2006
http://www.treasury.gov.au/documents/1083/PDF/australian_guidelines_for_electronic_commerce.pdf

- Collective Agreement between the Business Practices & Consumer Protection Authority (The "Employer") and the B.C. Government and Service Employees' Union (BCGEU), Effective from April 1, 2006 to March 31, 2010
http://www.bcgeu.ca/files/Business_Practices_2006_2010.pdf

٣) وتناولت أعمال البحث أيضا مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم التجارة الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الاسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول آسيا الوسطى.

٤) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية الخاصة بالتجارة الإلكترونية والتحكيم الالكتروني:

- International Trade Law, by Indira Carr, 3rd Edition, Cavendish publishing.
http://books.google.com/

- Electronic Transactions: Jurisdictional Issues in the European Union, by E. GUSAKOVA, 2004
http://www.elsa.org/fileadmin/user_upload/elsa_international/PDF/SPEL/SPEL04_1GUSAKOVA.pdf

- Wright (B.): The Law of Electronic Commerce, EDL, E-mail, and Internet: Technologie, Proof and Liability, 2nd Ed., Boston, Little, Brown and Company, 1995.

- Bensoussan (A.), Le commerce électronique sur les autoroutes de l'information, Cahiers Juridiques et Fiscaux de l'Exportation, No 2/96.

- Protecting consumers Online, A Report from the Federal Trade Commission Staff, December 1999
http://www.ftc.gov/os/1999/12/fiveyearreport.pdf

- Online dispute resolution ODR http://en.wikipedia.org/wiki/Online_dispute_resolution#cite_note-42
Online Arbitration: Admissibility within the current legal framework, by Rafal Morek rafalmorek@uw.edu.pl,
http://www.odr.info/Re%20greetings.doc

- International Commercial Arbitration: Electronic Arbitration (New York: United Nations Conference on Trade and Development, 2003), by O. Cachard
http://www.unctad.org/en/docs/edmmisc232add20_en.pdf> at 1.

- Online Dispute Resolution – More Than The Emperor's New Clothes By Julia Hornle, 2003,
http://www.odr.info/unece2003/pdf/Hornle.pdf

- Online Arbitration: Binding or Non-Binding?, (2002) ADR online Monthly 11, by T. Schultz, online:
http://www.ombuds.org/center/adr2002-11-schultz.html

- Alternative Dispute Resolution in the European Union, by Julia Hörnle - Research Fellow in E-commerce Law, IT Law Unit, CCLS, Queen Mary College, University of London, j.hornle@qmw.ac.uk

- Dispute Resolution in Cyberspace by Devashish Bharuka and William Fisher, last modified: June 25, 2001
http://cyber.law.harvard.edu/ilaw/Jurisdiction/

- Consumer Confidence Alternative Dispute Resolution, September 14, 2001, by Carleton S. Fiorina, Global Business Dialogue on Electronic Commerce
http://www.gbd-e.org/pubs/Tokyo_Recommendations_2001.pdf

- Fourth Annual Conference of the Global Business Dialogue on Electronic Commerce (GBDe), Brussels, 29th October 2002
http://www.gbd-e.org/pubs/BrusselsDeclaration_2002.pdf

- Electronic Commerce: On-line Contract Issues, by Fred M. Greguras,
<http://www.batnet.com/oikoumene/ec_contracts.html>

- محاضرات الدكتور وسيم حرب – الدراسات العليا في القانون، كلية الحقوق-الجامعة اللبنانية، ١٩٩٥- ٢٠٠٥، مكتب المحاماة والاستشارات القانونية والتحكيم.

- التحكيم الإلكتروني للدكتور نبيل زيد – مقابلة - مستشار وحدة التحكيم الالكتروني في الجمعية العربية لقانون الانترنت، ٢٠٠٧ .
http://www.arab-elaw.com/show_similar.aspx?id=81

- بحث في التحكيم في عقود التجارة الإلكترونية، للدكتور عمر فارس، دكتوراه في قانون الأعمال في فرنسا.
http://www.mn940.net/forum/forum30/thread8339.html

- إجراءات التحكيم عبر الإنترنت، القاضي محمد حته
http://kenanaonline.com/users/hetta11/posts/81161

- قوانين الاستثمار والتحكيم الجديدة..القاضي الدكتور محمد وليد منصور
http://sarab.cz.cc/montada-f67/toc-t7714.htmpi

٥) بالإضافة إلى ذلك تناولت أعمال البحث مراكز التحكيم الدولية والعربية، وأبرزها:

- ICC International Court of Arbitration,
http://www.iccwbo.org/court/arbitration/

- AAA American Arbitration Association, Disputes Alternatives Resolutions
http://www.adr.org/

- Cyber tribunal II,
http://www.cybertribunal.org

- WIPO Arbitration and Mediation Center,
http://www.wipo.int/amc/en/index.html

- GCC commercial Arbitration Center,
http://www.gcac.biz

- الاتحاد العربي للتحكيم الدولي،
www.auica.com

- غرفة التحكيم العربية
http://www.arado.org.eg/ .

٦) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم المعاملات الإلكترونية، ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شموليتها للنقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بالتجارة الإلكترونية وحماية المستهلك

التجارة الإلكترونية:

تبين أثناء أعمال البحث أن معظم الدول العربية عملت على إصدار أحكام تنظم التجارة الإلكترونية ضمن تشريعات هي نفسها التشريعات المتعلقة بالمعاملات الإلكترونية، فكان أن أصدرت الدول العربية المعنية في هذه الدراسة، تشريعات موحدة تضم أحكاماً تتعلق بالمعاملات والتجارة الإلكترونية، حيث جمعت بين العقود الإلكترونية وكيفية انتشائها وصحتها ومفاعيلها القانونية وطرق إثباتها وسائر

المعاملات الإلكترونية والتواقيع الرقمية وشهادات المصادقة الإلكترونية.

التشريعات العربية المتعلقة بالمعاملات والتجارة الإلكترونية هي التالية:

١- الإمارات العربية المتحدة:
قانون رقم (٢) صادر في ٢٠٠٢/٠٢/١٢ بشأن المعاملات والتجارة الإلكترونية
http://www.theuaelaw.com/vb/showthread.php?t=1137

٢- البحرين:
مرسوم بقانون رقم ٢٨ الصادر بتاريخ ١٤ سبتمبر ٢٠٠٢ بشأن المعاملات الإلكترونية وتعديلاته
http://www.moic.gov.bh/MoIC/Ar/Industry/ResourcesLaws/CommerceLaw/eLaw/

٣- سلطنة عمان:
قانون رقم ٦٩ لسنة ٢٠٠٨ بشأن المعاملات الإلكترونية
http://www.ita.gov.om/ITAPortal_AR/Businesses/Businesses_Projects.aspx?NID=97

٤- قطر:
قانون المعاملات والتجارة الإلكترونية تاريخ ١٩ أغسطس ٢٠١٠
http://www.ict.gov.qa/files/images/e-commerce_law_updated.pdf

٥- السعودية:
مرسوم ملكي رقم ١٨ لسنة ٢٠٠٧ خاص بنظام التعاملات الإلكترونية
http://www.ncda.gov.sa/low21/7.pdf

أما الدول التي غابت عنها الأحكام الخاصة بالتجارة الإلكترونية (أي التي تتضمن مواد خاصة بالعقود الإلكترونية وصحتها وطرق إثباتها) وان كانت قد أصدرت تشريعات متعلقة بالمعاملات الإلكترونية، فهي:

١- الأردن:
قانون رقم الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الإلكترونية
http://www.lob.gov.jo/ui/laws/search_no.jsp?no=85&year=2001

٢- سوريا:
قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الالكتروني وخدمات الشبكة
http://www.moct.gov.sy/moct/?q=ar/node/69

٣- الكويت:
مشروع قانون المعاملات الإلكترونية.

٤- مصر:
قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الالكتروني

٥- اليمن:
قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية
http://www.centralbank.gov.ye/ar/CBY.aspx?keyid=80&pid=74&lang=2&cattype=1

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالمعاملات والتجارة الإلكترونية، وهي: لبنان، وفلسطين[1] التي قامت بإعداد مشروع قانون المبادلات والتجارة الإلكترونية الصادر عام ٢٠٠٣.

أما العراق فهو البلد الوحيد الذي لم يعالج موضوع المعاملات والتجارة الإلكترونية ولم يصدر أية تشريعات في هذا المجال.

من ناحية أخرى، نفيد ضمن هذا المجال أن جامعة الدول العربية قد قامت بإصدار القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية، الذي تناول أحكاماً حول العقود الإلكترونية، وشروط صحة التعاقد وحجيته وإمكانية العدول عن العقد، بالإضافة إلى أحكام حول عقود نقل البضائع الكترونياً، والعقوبات التي تفرض عند مخالفة هذه الأحكام، بالإضافة إلى القانون الواجب تطبيقه والمحكمة المختصة.

حماية المستهلك

نجد أيضاً أن معظم الدول العربية المعنية قد أصدرت تشريعات خاصة بحماية المستهلك من الغش والإعلان الخادع والحؤول دون استغلاله وتأمين شفافية المعاملات الاقتصادية التي يكون المستهلك أحد أطرافها، وهي التالية:

١- الإمارات:
القانون الاتحادي رقم (٢٤) لسنة ٢٠٠٦ (قانون حماية المستهلك)
http://www.economy.ae/

٢- البحرين:
مرسوم بقانون رقم (١١) لسنة ١٩٧٧ بتعديل المرسوم بقانون

رقم (١٨) لسنة ١٩٧٥ بتحديد الأسعار والرقابة عليها
http://www.mohamoon-bh.com/Default.aspx?action=LegsCates&FIID=2190

٣- سوريا:
قانون رقم /٢/لعام ٢٠٠٨ بشأن حماية المستهلك
http://www.dcc-sy.com/files/laws/protect%20law.doc

٤- العراق:
قانون حماية المستهلك رقم ١ لسنة ٢٠١٠

٥- سلطنة عمان:
مرسوم سلطاني رقم ٢٠٠٢/٨١ بإصدار قانون حماية المستهلك
http://www.mocioman.gov.om/MOCI/getdoc/970be5be-beca-4c6e-b026-cdd7bd28df26/customer-law.aspx

٦- فلسطين:
قانون رقم ٢١ لسنه ٢٠٠٥ بشأن حماية المستهلك.
http://muqtafi.birzeit.edu/pg/getleg.asp?id=15136

٧- قطر:
قانون رقم (٨) لسنة ٢٠٠٨ بشأن حماية المستهلك
http://www.alarab.com.qa/details.php?docId=13023&issueNo=141&secId=16

٨- الكويت:
قانون رقم (٢) لسنة ١٩٩٥ في شأن البيع بالأسعار المخفضة والدعاية والترويج للسلع والخدمات.
http://www.moci.gov.kw/

٩- لبنان:
مرسوم رقم ١٣٠٦٨ تاريخ ٥ آب ٢٠٠٤ المتعلق بحماية المستهلك
http://www.consumerslebanon.org/

١٠- مصر:
قانون رقم ٦٧ لسنة ٢٠٠٦ بإصدار قانون حماية المستهلك
http://www.cpa.gov.eg/doc/Law.doc

١١- السعودية:
المرسوم الملكي رقم م/١٩والتاريخ: ١٤٢٩/٤/٢٣هـ بالموافقة على نظام مكافحة الغش التجاري
http://www.mci.gov.sa/circular/23-1.asp#16

١٢ - اليمن:
القانون رقم (٤٦) لسنة ٢٠٠٨م بشأن حماية المستهلك
http://consumeryemen.org/yacp/index.php?option=com_content&view=article&id=12&Itemid=9

ومن الدول التي تعمل على صياغة مشروع قانون لحماية المستهلك الأردن التي أصدرت: مشروع قانون رقم ( ) لسنة ٢٠٠٦ (قانون حماية المستهلك)
http://www.mit.gov.jo/

ب - شمولية التشريعات الوطنية الخاصة:

التجارة الإلكترونية

كما ذكرنا أعلاه، نجد أن معظم الدول العربية لجأت إلى إصدار قانون موحد يضم أحكاماً تنظم المعاملات والتواقيع الإلكترونية بالإضافة إلى أحكام خاصة حول العقود التجارية وعقود نقل البضائع الكترونياً. وهذه الدول العربية هي الإمارات العربية المتحدة، سلطنة عمان، السعودية، البحرين، وقطر. فقد تناولت هذه التشريعات ضمن أحكامها مواد تتعلق بإبرام العقود التجارية الكترونياً، والتعبير عن الإيجاب والقبول وكافة الأمور المتعلقة بإبرام العقد والعمل بموجبه، بما في ذلك أي تعديل أو عدول أو إبطال للإيجاب أو القبول عن طريق السجلات الإلكترونية، والآثار القانونية لهذه العقود من حيث الإثبات والصحة والقابلية للتنفيذ، بالإضافة إلى دور الوكلاء الالكترونيين في إبرام العقود وإبطالها، والعقوبات المفروضة في حال مخالفة الأحكام المرعيّة الإجراء بموجب هذه التشريعات. كما ويتضمن بعضها أحكاماً حول الإجراءات والمستندات المطلوبة فيما يتعلق بعقد نقل البضائع الكترونياً.

وقد انفردت الإمارات العربية المتحدة بأن خصصت مادة للتحكيم الإلكتروني حيث جاء في المادة ٣٧ من قانون المعاملات والتجارة الإلكترونية: "يجوز للرئيس تشكيل محاكم أو هيئات تحكيم خاصة للفصل في القضايا والمنازعات الناشئة عن هذا القانون".

كما وعمدت دولة قطر ضمن قانونها الخاص بالمعاملات والتجارة الإلكترونية على وضع مواد قانونية حول تشكيل هيئة مختصة للنظر في النزاعات التي تنشأ عن هذه المعاملات وتعرف بـ "لجنة التظلمات وتسوية المنازعات" وهي تختص بفض المنازعات التي تنشأ بين مقدمي الخدمات أو بين مقدمي الخدمات والمتعاملين.

أما بالنسبة للدول العربية التي أصدرت قوانين خاصة بالمعاملات الإلكترونية دون التطرق إلى معالجة العقود الإلكترونية، فسنورد بعض الشروحات حول ما تتضمنه قوانينها هذه، وأهمها مثلاً:

- أصدرت دولة مصر قانوناً خاصاً بالتواقيع الإلكترونية (قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الالكتروني) حيث اقتصرت أحكامه على إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات ومهامها ونظام عملها وعلى التوقيع الالكتروني وآثاره القانونية وحجيته وإصدار شهادات التصديق الالكتروني. ولم تعالج أحكامه العقود الإلكترونية وكيفية إبرامها وصحتها.

- كذلك الأمر بالنسبة لسوريا التي أصدرت قانون التوقيع الإلكتروني (قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الالكتروني وخدمات الشبكة) حيث تناولت أحكامه فقط التوقيع الالكتروني وحجيته، وواجبات ومسؤولية وسيط الشبكة الإلكترونية ومقدم الخدمات، بالإضافة إلى إنشاء الهيئة الوطنية لخدمات الشبكة ومهامها ونظام عملها.

- أما التشريع الذي أصدرته اليمن (قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن انظمه الدفع والعمليات المالية والمصرفية الإلكترونية)، فاقتصرت أحكامه أيضاً على أنظمة الدفع والتحاويل الإلكترونية، وشروط قابلية السند الالكتروني للتحويل وإجراءات الدفع الالكتروني، وتوثيق السجل والتوقيع الالكتروني. وقد غابت الأحكام المتعلقة بتنظيم العقود التجارية وصحتها.

حماية المستهلك

بالرغم من شيوع استخدام تقنيات المعلومات والاتصالات في إنجاز الأعمال الإلكترونية وإبرام العقود وتنفيذها عبر شبكة الإنترنت، لم يخصص المشرع العربي في التشريعات الخاصة بحماية المستهلك المذكورة أعلاه، مواد قانونية خاصة بحماية العمليات التي يجريها المستهلك عن بعد أو عبر شبكة الإنترنت، باستثناء ثلاثة دول عربية وهي لبنان، مصر وقطر.

خصص لبنان ضمن قانونه الخاص بحماية المستهلك فصلاً (الفصل العاشر) يتعلق بـ "العمليات التي يجريها المحترف عن بعد أو في محل إقامة المستهلك"، حيث حدد فيه أن جميع الأحكام الواردة في هذا القانون تطبق على المعاملات التي يجريها المستهلك عن بعد أو عبر شبكة الإنترنت. فقد جاء في **المادة ٥١:** " ترعى أحكام هذا الفصل العمليات التي يجريها المحترف عن بُعد أو في محل إقامة المستهلك، لا سيما تلك التي تتم في مكان إقامة المستهلك أو عبر الهاتف أو الإنترنت، أو أية وسيلة أخرى معتمدة لذلك. لا تراعي أحكام هذا الفصل العمليات المالية والمصرفية والبيع بالمزاد العلني والعمليات التي تتناول أموالاً غير منقولة".

المادة ٥٢: "يجب تزويد المستهلك، في الحالات المنصوص عليها في المادة ٥١، بمعلومات واضحة وصريحة تتناول المواضيع التي تمكنه من اتخاذ قراره بالتعاقد، لاسيما:

- تعريف المحترف وإثمه وعنوانه ورقم ومكان تسجيله، وبريده الإلكتروني، بالإضافة إلى أية معلومات تتيح تعريف المحترف.
- السلعة والخدمة المعروضة وكيفية استعمالها والمخاطر التي قد تنتج عن هذا الاستعمال.
- مدة العرض.
- ثمن السلعة أو الخدمة والعملة المعتمدة وكافة المبالغ التي قد تضاف إلى الثمن لا سيما الرسوم والضرائب والمصاريف أياً كانت، وكيفية تسديد هذه المبالغ.

وأوردت مصر ضمن قانون حماية المستهلك مادة تفرض على المورد أن يضع على جميع مراسلاته بما فيها المراسلات الإلكترونية بيانات تحدد شخصيته ونشاطه بهدف حماية المتعاملين معه، حيث نصت المادة الرابعة من هذا القانون: "على المورد أن يضع على جميع المراسلات والمستندات والمحررات التي تصدر عنه في تعامله أو تعاقده مع المستهلك، بما في ذلك المحررات والمستندات الإلكترونية - البيانات التي من شأنها تحديد شخصيته، وخاصة بيانات قيده في السجل الخاص بنشاطه وعلامته التجارية إن وجدت."

أما قطر فقد خصصت فصلاً ضمن قانون المعاملات والتجارة الإلكترونية لحماية المستهلك من الغش الذي قد يحصل أثناء العمليات الإلكترونية، حيث نصت المادة ٥١: "مع عدم الإخلال بقانون رقم ٨ لسنة ٢٠٠٨ بشأن حماية المستهلك يجب على مقدم الخدمة أن يوفر لمستهلكي خدماته ولأي جهة حكومية مختصة، في الشكل وبالطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، المعلومات التالية."

هوامش

١- تراجع لائحة تشريعات الدول الأجنبية.

٢- راجع مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني المنشور على الموقع الالكتروني:
http://www.pita-palestine.org/PITA%20files/proposed%20e_commerce%20law.doc

مقدمة إرشاد التجارة الإلكترونية وحماية المستهلك

تشكل التجارة الإلكترونية نشاطاً اقتصاديا أساسياً نشأ وتعاظم في ظل تطور وسائل الاتصال واتساع شبكة الإنترنت وعدد المتعاملين عليها. تطور مفهوم التجارة الإلكترونية على مدى الثلاثين عاماً المنصرمة. فكانت البداية عبر تسهيل التواصل عن بعد عن طريق إمكانية وقبول إرسال واستلام المستندات بوسيلة إلكترونية أو برقية مثل صور الفواتير أو أوامر الدفع. ومن ثم أدى تطور التواصل والمراسلات عن بعد، لاسيما بواسطة طرق الاتصالات الإلكترونية الحديثة وأهمها شبكة الإنترنت، إلى إمكانية أوسع للتبادل التجاري بوسائل إلكترونية.

إن سهولة معاينة السلع وطلبها والخدمات على شبكة الإنترنت وإمكانية الدفع الإلكتروني مع إمكانية تسليم المنتجات والسلع إلكترونياً عبر شبكة الإنترنت، وتوافر شروحات وافية حول المواصفات والمنتجات وأنواعها، قد دفع إلى نشوء أسلوب جديد من أساليب التعامل التجاري، وهو ما يُعرف بالتجارة الإلكترونية. وقد تجاوزت التجارة الإلكترونية الحدود الوطنية إلى العالمية في ظل زوال الحواجز بين الدول وتقليص دور الأبعاد الجغرافية بفضل شبكة الإنترنت[1]. وأصبحت شبكة الإنترنت تستخدم كسوق كونية إلكترونية[2] (e-marketplace) لترويج السلع وتقديم الخدمات. بذلك، أصبح تطور التجارة الإلكترونية يساهم بشكل فعال في زيادة القدرة التنافسية للشركات الوطنية على صعيد العالم ككل، وفي خلق فرص جديدة للعمل على الصعيد الوطني. فالتجارة الإلكترونية أصبحت في أساس نمو الاقتصاد الوطني وازدهاره.

إن التجارة الإلكترونية، وفق التعريف المُعطى في هذا الإرشاد، هي نشاط اقتصادي يعرض بموجبه، أو يؤمن عن بعد وبوسائل إلكترونية، تقديم الأموال أو الخدمات أياً كان نوعها أو طبيعتها. ويدخل أيضاً في إطار التجارة الإلكترونية خدمات تقديم المعلومات مباشرةً على الخط وخدمات الاتصالات التجارية وأدوات البحث واسترجاع المعلومات، وخدمات تأمين الوصل بشبكة اتصال أو استضافة البيانات.

وقد عرف سوق التجارة الإلكترونية نمواً مطّرداً منذ الثمانينات[3] مع ازدياد عدد آلات الصراف الآلي ATM وإمكانية إرسال نسخ المستندات برقياً والكترونياً عبر وسائل الاتصال عامةً. وقد ازداد حجم التجارة الإلكترونية بشكل كبير عام ١٩٩١، حين رفعت شركة NSF كل تقييد للاستعمال التجاري لشبكة الإنترنت في الولايات المتحدة الأميركية، واكتمل تحرير الشبكة في أوروبا عام ١٩٩٤. ففي مطلع القرن الحالي وتحديداً في العام ٢٠٠٣، بلغ حجم التجارة الإلكترونية ١٤٠٠ مليار دولار على صعيد العالم، وقد تضاعف منذ ذلك الوقت. في الوقت الحاضر يوجد حوالي ٣٦٥ مليون اسم موقع على الإنترنت حوالي ٢٣٤ مليون موقع يمكن الولوج إليه، ويبلغ عدد مستعملي شبكة الإنترنت حوالي ١,٩٦ مليار شخص حول العالم[4]، وهذه الأرقام على تزايد بنسبة تتراوح بين ١٧ و٢٠ ٪ سنوياً.

الوضع القانوني والحاجة إلى التشريع

في ظل تنامي التجارة الإلكترونية ووجود عوائق قانونية ناجمة عن اختلاف التشريعات الوطنية وعدم توفر الحماية القانونية للتعاملات التجارية التي تجري عن بعد وخارج النطاق المحلي للقوانين الوضعية، بالإضافة إلى احتمال تعرض المتعاملين لإشكاليات وعمليات تلاعب غير قانونية، ولاسيما بفعل حصول التعامل عن بعد ومع شريك أجنبي وفي أغلب الأوقات غير معروف من الشريك الأول الذي قد يقع في دولة أخرى، أضف إلى ذلك ضرورة أن تشمل القوانين الضريبية الإعمال التجارية التي تجري عن بعد. في ضوء ذلك كله، وجد المشترع نفسه قاصراً عن إمكانية وضع تشريع يمكن تطبيقه على التعاملات التجارية الجارية في نطاق أكثر من دولة وذلك بسبب إقليمية تطبيق القوانين.

من هنا كان لا بد من حلول بديلة عن التشريع بالمعنى الضيق، إذ لا يمكن ترك التعاملات التجارية خارجة عن أي تنظيم قانوني ولا يمكن في الوقت نفسه تقنينها من قبل أي مشرِّع نظراً لعدم اختصاص أية جهة بذلك. حيث يشكل الفضاء السيبراني إطاراً فيزيائياً جديداً يتخطى الجغرافيا الدولية وبالتالي لا يخضع لأي سيادة وطنية محددة على الخريطة، مما يجعله خارجاً عن إمكانية تطبيق أية شريعة أو قانون وضعي، إذ يتعذر على المشرع الوطني ممارسة سلطته على هذا الفضاء. ولما كان توسع الفضاء السيبراني ما زال مستمراً لم يعد بإمكان أية دولة أن تضع حدوداً لهذا التوسع، خاصةً وأنه آخذٌ في التزايد بسرعة كبيرة[5].

هذا الأمر أدى إلى استحداث قواعد قانونية نموذجية على صعيد التجارة الإلكترونية تحظى بسيادة عالمية لتطبيقها

على شبكة الإنترنت، بهدف تنظيم هذا القطاع وحماية المستهلكين والمتعاملين[6]. في هذا السياق، أصدرت لجنة القانون الدولي لدى الأمم المتحدة بتاريخ ١٩٩٧/٦/١٢ قانوناً نموذجياً للتجارة الإلكترونية، يمكن اعتماده من قبل الدول لتوحيد الحلول القانونية في هذا المجال وتأمين التناسق بين التشريعات. كما أقر البرلمان الأوروبي بتاريخ ٢٠٠٠/٦/٨ إرشاداً حول التجارة الإلكترونية.

بالإضافة إلى ذلك تم إنشاء أنظمة تمكّن المستهلك من حماية حقوقه نظراً لأنه الفريق الأضعف في التعامل مع المحترف، لاسيما عندما يكون المحترف بعيداً وغير معروف شخصياً و خارجاً عن النطاق الإقليمي للقانون الذي يسود مكان وجود المستهلك. وكذلك جاءت العقود والاتفاقات الجماعية[7] وقواعد حسن التصرف[8] Codes of Conduct لتشكل ضمانة أولية للمستهلك.

يأتي هذا الإرشاد حول التجارة الإلكترونية وحماية المستهلك ليشكل إطاراً قانونياً متكاملاً في هذا المجال. وقد تم الاسترشاد بالإرشاد الأوروبي[9] الصادر عام ٢٠٠٠ المتعلق بالتجارة الإلكترونية، وبقانون الأونسيترال النموذجي حول التجارة الإلكترونية[10] لعام ١٩٩٧ وببعض القوانين الوطنية الأجنبية والعربية المختلفة، وذلك في سبيل إعداد نصوص الإرشاد الحالي الموجه للدول العربية حول التجارة الإلكترونية وحماية المستهلك. وكذلك تم الاستئناس بالقانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية الذي أصدرته جامعة الدول العربية.

لقد تم تقسيم القانون الاسترشادي المُقترح على أربعة أبواب تتناول مختلف جوانب التجارة الإلكترونية وحماية المستهلك. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: الخطابات أو الرسائل الإلكترونية التجارية.
الباب الثالث: العقود الإلكترونية.
الباب الرابع: أحكام ختامية.

يتضمن **الباب الأول** المعنون "أحكام عامة" تحديداً لأهداف الإرشاد ولنطاق تطبيقه وكذلك تعريفاً لبعض المصطلحات المستعملة في هذا الإرشاد. وأخيراً يورد الباب الأول قاعدة حرية التجارة الإلكترونية مع بعض الضوابط. فالإرشاد الحالي يهدف إلى المساهمة في ازدهار الأسواق الداخلية من خلال تأمين الانتقال الحر لخدمات مجتمع المعلومات (الخدمات الإلكترونية) بين الدول. فالخدمات الإلكترونية المتاحة على الشبكات الإلكترونية، ولاسيما شبكة الإنترنت، تشكل التجارة الإلكترونية. والمبدأ هو حرية التجارة الإلكترونية سعياً لازدهارها، إلا أنه من الممكن فرض ضوابط وقيود قانونية لحماية المصالح العليا للدولة ولحماية المستهلك[11].

تضع المادة ٢ من الإرشاد تعاريف لمختلف المصطلحات المستعملة فيه. فالرسالة الإلكترونية هي المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية، بما في ذلك على سبيل المثال البريد الإلكتروني. ويتم تبادل الرسالة الإلكترونية بين مُرسِل ومُرسَل إليه. فمُرسل الرسالة الإلكترونية هو الشخص الذي أنشأ هذه الرسالة أو أرسلها قبل تخزينها من قبل المرسل إليه أو الغير، ولا يشمل الشخص الذي يتصرف كوسيط. أما المُرسل إليه، فهو الشخص الذي قصد المُرسل أن يتسلم الرسالة الإلكترونية، ولا يشمل أيضاً الشخص الذي يتصرف كوسيط. والوسيط هو الشخص الذي يقوم، نيابة عن شخص آخر، بإرسال أو استلام أو تخزين رسالة إلكترونية أو بتقديم خدمات أخرى فيما يتعلق بهذه الرسالة.

كذلك كان من الضروري تعريف الخدمة الإلكترونية باعتبارها موضوع التجارة الإلكترونية. فالخدمة الإلكترونية هي كل خدمة، عادةً لقاء مقابل، مقدّمة عن بعد بواسطة وسائل معلوماتية لمعالجة وتخزين البيانات، وذلك بناءً لطلب فردي من المتعامل. وتتضمن الخدمات الإلكترونية، المعروفة أيضاً بخدمات مجتمع المعلومات، نشاطات اقتصادية عديدة تتم على الخط مباشرةً مثل بيع السلع عن بعد. ولا تقتصر الخدمات الإلكترونية على النشاطات التي يتم فيها إبرام عقود إلكترونية، بل تمتد إلى خدمات دون مقابل مادي، مثل خدمات تقديم المعلومات على الخط أو الخطابات أو الاتصالات التجارية، وخدمات محركات البحث أو الوصول إلى المعلومات أو نقلها بواسطة شبكة إلكترونية، وكذلك خدمات الربط بشبكة اتصال إلكترونية وخدمات استضافة البيانات وخدمات مشاركة الملفات[12]. إن خدمات التلفزيون والراديو لا تدخل ضمن خدمات مجتمع المعلومات، بمفهوم هذا الإرشاد، ما خلا طبعاً حالة المواقع الإلكترونية التي تبث صوتاً و/أو صورة على الإنترنت مقابل ثمن عادةً ما يكون مدفوعاً سلفاً[13]. كذلك إن استعمال البريد الإلكتروني أو غيره من وسائل الاتصال الفردية من قبل أشخاص طبيعيين، لغايات لا تدخل في نطاق نشاطاتهم التجارية أو المهنية، لا ينضوي أيضاً ضمن خدمات مجتمع المعلومات بمفهوم هذا الإرشاد. كون هذه التصرفات ليست من صلب النشاطات التجارية أو المهنية لهؤلاء الأشخاص. كما أن النشاطات التي بطبيعتها لا يمكن تحقيقها عن بعد أو بوسيلة إلكترونية لا تشكل خدمة إلكترونية.

كما تعرّف المادة ٢ من الإرشاد العقد الإلكتروني الذي سيطبق عليه هذا الإرشاد، وذلك لتمييزه عن العقد المُبرم بالوسائل التقليدية غير الخاضع لهذا الإرشاد. والعقد الإلكتروني هو عقد نظّم بوسيلة إلكترونية. إن هذا التعريف هو مبسط ومقتضب ويستوعب أية صيغة إلكترونية يبرم بها العقد، كتبادل القبول أو الإيجاب على الإنترنت أو على شبكة تجارية مقفلة أو الدخول في مزاد علني على شبكة الإنترنت وغيرها.

تتم التجارة غالباً بين مستهلك ومورد نسميه محترفاً لكونه يحترف الأعمال التجارية أو أعمال التوريد ويلم بمواصفات البضائع وخصائصها وكيفية استعمالها. والمستهلك هو كل شخص طبيعي أو معنوي أو مجموعة معينة يجمع بينها حاجة أو سعي إلى نوع من المنتجات أو الخدمات وتتصرف كجسم واحد من ناحية الطلب على هذه المنتجات أو الخدمات، يشتري سلعة أو خدمة أو يستأجرها أو يستعملها أو يستفيد منها، وذلك لأغراض لا تدخل في نطاق نشاطه المهني أو التجاري. أما المحترف، فهو الشخص الطبيعي أو المعنوي الذي يحترف نشاطاً معيناً كبيع السلع أو توزيعها أو تأجيرها أو تقديم الخدمات. إن نشوء العلاقة بين المحترف والمستهلك وإتمام تعامل تجاري إلكتروني يستلزمان حصول خطابات أو اتصالات تجارية. فالخطابات أو الاتصالات التجارية هي كل شكل اتصال مخصص لترويج - بشكل مباشر أو غير مباشر- الأموال أو السلع أو الخدمات أو صورة شركة أو مؤسسة أو شخص يمارس نشاطاً تجارياً أو صناعياً أو حرفياً أو يمارس مهنة منظمة بقانون. لكن لا تشكل اتصالات إلكترونية بمفهوم هذه المادة: المعلومات التي تسمح بالوصول المباشر إلى نشاطات الشركة أو المؤسسة أو الشخص، لاسيما إسم الموقع أو عنوان البريد الإلكتروني، وكذلك الاتصالات المتعلقة بالأموال أو بالخدمات أو بصورة الشركة أو المؤسسة أو الشخص، المُجراة بشكل مستقل، لاسيما عندما تقدم بدون مقابل مادي. ولما كانت بعض التعاملات الإلكترونية تتم أحياناً من خلال نظام رسائل معلوماتي آلي، فقد أقتضى تعريف هذا النظام بأنه برنامج أو وسيلة إلكترونية تُستخدم لاستهلال إجراء ما أو للاستجابة كلياً أو جزئياً للرسائل الإلكترونية أو لعمليات تنفيذها، وذلك دون مراجعة أو تدخل من شخص طبيعي في كل مرة يستهل النظام إجراء ما أو يطلق استجابة ما.

تؤكد المادة ٣ المبدأ الأساسي في هذا الإرشاد، وهو حرية التجارة الإلكترونية ضمن حدود القانون، وذلك لتعزيز التبادل التجاري بين الدول الأعضاء ورفع حجم التجارة الإلكترونية الجارية بينهم. فلا يمكن للدول الأعضاء تقييد الانتقال الحر لخدمات مجتمع المعلومات (الخدمات الإلكترونية) من دولة عضو إلى دولة عضو أخرى. وتُمارس التجارة الإلكترونية بحرية ضمن نطاق القوانين النافذة. لكن الدول المتعاقدة تستطيع أن تأخذ في صدد خدمة معينة لمجتمع المعلومات تدابير تحد من حرية التجارة الإلكترونية والانتقال الحر للخدمات الإلكترونية، عندما تكون هذه التدابير ضرورية للحفاظ على الصحة العامة وعلى الأمن العام والدفاع الوطني وعلى النظام العام، ولاسيما الوقاية أو التحقيق أو الاكتشاف أو الملاحقة في المسائل الجزائية، وحماية القاصرين ومسائل التمييز العنصري أو الجنسي أو الديني أو التعرض لكرامة الإنسان، وكذلك لحماية المستهلكين والمستثمرين. تجدر الإشارة هنا إلى أن القيود المذكورة آنفاً لا تعطّل الممارسات المشروعة في إطار التجارة الإلكترونية، وهي الغالبة، مما يبقي تأثير هذه القيود محدوداً على حجم التجارة الإلكترونية. كما أن الإرشاد الحالي لا يحول دون تطبيق القواعد القانونية الأخرى، ذات الطابع الحمائي، المتعلقة بالصحة العامة أو بحماية المستهلك و/أو المحترف.

يضع **الباب الثاني** المعنون "الخطابات أو الرسائل الإلكترونية التجارية" تنظيماً لهذه الخطابات، فهو يتناول إسناد الرسائل الإلكترونية وإشعارات استلام الرسائل الإلكترونية وزمان ومكان استلام وتسليم الرسالة الإلكترونية والمعلومات الواجب تقديمها في هذا المجال والخطابات أو الرسائل التجارية غير المرغوب بها والمهن المنظّمة بقانون. في مجال تحديد كيفية إسناد الرسائل الإلكترونية، أي تحديد الشخص الذي صدرت عنه الرسالة الإلكترونية، فهذه الأخيرة تعتبر صادرة عن المرسل إذا أرسلها شخص مكلّف من قبله أو نظام معلوماتي مُبرمج من قبله أو من قبل شخص مكلّف من قبله للعمل تلقائياً. إن توضيح هذا الأمر هو ذو أهمية في مجال التعامل الإلكتروني، لأنه يتم عن بعد دون حضور الفرقاء في مجلس واحد، ولأن المُرسل قانوناً للرسالة الإلكترونية قد لا يكون هو المُرسل الفعلي لها.

تعطي المادة ٥ من الإرشاد إشعارات الرسالة الإلكترونية مفعولاً قانونياً تماماً كإشعارات استلام الرسائل الورقية. فمن الممكن أن يُصدر مزود خدمات إيصالاً تبعاً لتقديم خدمة مدفوعة منه على الخط. إلا أن استلام إشعار إلكتروني إثباتاً لإرسال رسالة إلكترونية أو لاستلامها لا يعني حكماً مطابقة المعلومات التي تم استلامها للمعلومات التي تم إرسالها. وهذا الأمر بديهي لأن الإشعار يثبت واقعة إرسال الرسالة أو استلامها فقط ولا يثبت مضمونها، إذا لم تتم المصادقة على هذا المضمون من قبل طرف ثالث موثوق، أو لم يتم استعمال وسائل حماية تقنية في الرسالة تمنع أي تحوير فيها.

تحدد المادة ٦ من الإرشاد الوقت[١٧] الذي تُعتبر فيه الرسالة الإلكترونية قد أُرسلت إلى المرسل إليه، كما تعيّن الوقت الذي تُعتبر فيه الرسالة قد تم استلامها من قبله[١٨]. إن تحديد الأوقات ضروري لتبيان ما إذا كان الإجراء قد تم ضمن المهل المفروضة. كذلك قد لا يستلم المرسل إليه الرسالة فعلاً بسبب عطل تقني أو بسبب إهماله استخراجها. إلا أن المرسل يكون قد نفذ قانوناً موجباته بإرسال الرسالة عند دخولها في نظام معلوماتي خارج سيطرته، وتعد الرسالة قد استلمت قانوناً كذلك عندما تدخل النظام المعلوماتي المحدّد مسبقاً. وفي حال عدم تحديد مثل هذا النظام، عندما تدخل نظاماً معلوماتياً تابعاً للمُرسل إليه. كما تُحدد المادة ٦ المكان[١٩] المفترض لإرسال الرسالة الإلكترونية وكذلك المكان المفترض لاستلامها. وهذا الأمر مهم لتحديد مكان حصول التعاقد وتحديد المحكمة المختصة عند حدوث نِزاع قضائي، وكذلك القانون الواجب التطبيق. وتضع المادة ٦ بالتالي قواعد موضوعية تنظم زمان ومكان إرسال الرسالة الإلكترونية. إلا أن هذه القواعد هي مكملة لإرادة الفرقاء، فلا تطبق إلا عند عدم وجود اتفاق مخالف لها بينهم.

إن الخطابات أو الاتصالات التجارية هي ضرورية لتموين خدمات مجتمع المعلومات وتطوير مجموعة متنوعة من الخدمات الإلكترونية الجديدة، ولكن، من أجل حماية المستهلكين وموثوقية المعاملات الإلكترونية، يجب أن تخضع هذه الخطابات لقيود تتعلق بالشفافية. في هذا الإطار، تضع المادة ٧ شروطاً للخطابات أو للاتصالات الإلكترونية تبيّن ماهيتها والشخص الطبيعي أو المعنوي الذي تتم لصالحه والحسومات والعروض وشروط المشاركة بين بعضهم البعض. إن هذه البيانات تهدف إلى حماية الشخص - وهو في كثير من الأحيان المستهلك- الذي توجه إليه هذه الخطابات أو الاتصالات، وذلك بإعطائه معلومات كافية غير ملتبسة ليستطيع تقدير موقفه.

لم تحظّر المادة ٨ من الإرشاد الاتصالات أو الخطابات التجارية غير المرغوب بها[٢٠]، بل وضعت ضوابط وقيوداً لها. هذا مع العلم بأن إرسال هذه الخطابات قد يكون غير مناسب للمستهلكين ولمزودي الخدمات التقنية ومن شأنه إعاقة حسن عمل الشبكات التبادلية أو الحوارية Interactive. ولهذا السبب تعتمد المؤسسات والشركات آليات لتصفية الرسائل الإلكترونية. تبعاً لذلك، يجب أن تُبيّن ماهية الاتصالات الإلكترونية غير المرغوب بها من أجل الشفافية ومن أجل تسهيل عمل آليات تصفية الرسائل المعتمدة من قبل الشركات. كما يجب أن لا يتم تحميل المُرسل إليه أية نفقات إضافية عند إرسال الخطابات التجارية غير المرغوب بها. في هذا الإطار، ألزمت المادة ٨ مزودي الخدمات التقنية مسك سجلات متاحة للجمهور، يمكن أن يتسجل فيها كل شخص يرغب بإيقاف إرسال الخطابات التجارية غير المرغوب بها. على أن يوقف مزود الخدمات التقنية إرسال الخطابات المنوه عنها لكل من عبر عن رغبته بذلك.

تتطرّق المادة ٩ إلى موجبات الأعضاء في المهن المنظمة بقانون، الذين يتولون تقديم خدمات إلكترونية عبر استعمال الخطابات أو الاتصالات التجارية. فهذه الخطابات تكون مسموحة شرط احترام القواعد المهنية التي تتعلق باستقلالية المهنة وبكرامتها وبشرفها وكذلك السر المهني والإخلاص تجاه الزبائن والأعضاء الآخرين في المهنة، ولاسيما حماية المستهلك والصحة العامة.

يشكّل **الباب الثالث** المعنون "العقود الإلكترونية" صلب هذا الإرشاد والباب الأبرز فيه. فهو يتناول مسألة الاعتراف القانوني بهذه العقود وإشكالية استخدام أنظمة الرسائل المعلوماتية الآلية في تكوين العقود والمعلومات الواجب تقديمها وكيفية إجراء طلبية ووجوب تحديد الأسعار وإتاحة المجال للمستهلك للعدول عن طلبه ومسؤولية المحترف.

تطلق المادة ١٠ من هذا الإرشاد المبدأ الأساسي، وهو يتضمن الاعتراف القانوني بالعقود الإلكترونية، واعتمادها في التعاملات بين الأشخاص الطبيعيين والمعنويين كالعقود الورقية. وهذا المبدأ هو ضروري لازدهار التجارة الإلكترونية التي تستند أساساً إلى عقود إلكترونية تبرم عن بعد على الإنترنت وباستعمال وسائل معلوماتية[٢١]. فعلى النظام القانوني أن يسمح بإبرام العقود بوسائل إلكترونية، وأن لا يشكل عائقاً أمام استعمال العقود الإلكترونية، وأخيراً أن لا يحرم هذه العقود من الآثار والاعتراف القانوني لمجرد أنها منظمة بوسيلة إلكترونية. كما يجوز استخدام الرسائل الإلكترونية للتعبير عن العروض وقبول العروض. إلا أنه بالنظر لعدم اعتياد العامة كافة على استخدام المعلوماتية وللطابع الذي تتسم به بعض العقود وعلى الأخص العقود الرسمية التي تفترض حضور الشخص أمام المأمور الرسمي، فإنه يمكن استثناء بعض العقود أو فئات منها من الشكل الإلكتروني، وهذه العقود تشمل: العقود التي تنشأ أو تنقل حقوقاً على أموال عقارية، باستثناء عقود الإيجار، والعقود التي من أجلها يتطلب القانون تدخل المحاكم أو السلطات العامة أو مهناً تمارس سلطة عامة من أجل إنتاج مفاعيل بحق الغير كالمصادقة القانونية أو الشهادات، وعقود الضمان المقدمة من قبل أشخاص يتصرفون لغايات لا تدخل ضمن إطار نشاطاتهم المهنية أو التجارية، والعقود التي

تتعلق بقانون العائلة أو قانون الإرث. أخيراً، إن اعتماد الشكل الإلكتروني للعقد لن يغير في شروطه ومفاعيله القانونية وفي النظرية العامة للعقود، إذ تبقى أحكام القانون المدني والتجاري تطبق على العقود الإلكترونية في كل ما لا يتعارض مع أحكام هذا الإرشاد. ويخضع بالتالي العقد الإلكتروني، بالإضافة إلى النظرية العامة للعقود، إلى الأحكام الواردة في هذا الإرشاد المتعلقة بالشكل الإلكتروني.

يمكن في بعض الأحيان إبرام عقود بواسطة نظام آلي معلوماتي للرسائل الإلكترونية، عبر تبادل رسائل العروضات والقبول معها. إن هذا النظام يكون في الواقع مُبرمجاً من قبل العارض، وهو شخص طبيعي أو معنوي، أو من قبل شخص مكلّف من قبله، أو يكون خاضعاً لسيطرة العارض. وبالتالي، إن شروط العروض ومواصفاتها تحدد من قبل العارض الشخص الطبيعي أو المعنوي، والذي يحدد أيضاً متى يجب أن يصدر النظام الآلي رسالة العرض أو رسالة القبول ومتى يرفض ذلك. فالإرادة في النهاية هي إرادة العارض ولا يتعدى النظام المعلوماتي الوسيلة التقنية المعتمدة للتعامل مع كثرة الطلبات الواردة والتي يمكن توحيد طرق التعامل معها وفق معايير معينة. فالمادة ١١ من الإرشاد الحالي تعترف بصحة العقد الذي يتكون بالتفاعل بين نظام معلوماتي آلي وشخص طبيعي أو بالتفاعل بين نظاميين معلوماتيين آليين، وذلك بالرغم من عدم مراجعة شخص طبيعي المسائل التالية: الأفعال التي قامت بها الأنظمة المعلوماتية للرسائل الآلية، والعقد الناتج عن تلك الأفعال، وتدخله فيها، بغية حماية المستهلكين والعملاء[٢٣]. أوجبت المادة ١٢ على مزود الخدمات تقديم معلومات معينة لعملائه عن خدماته، ليكونوا على بينة من أمرهم حين طلبهم هذه الخدمات. وهذه المعلومات تتضمن: اسم مزود الخدمات وشهرته ومقامه واسم ممثله التجاري ومركزه وعنوانه التجاري وسجله التجاري وعنوان بريده الإلكتروني وأرقام هاتفه، والمراحل التقنية المختلفة الواجب إتباعها من أجل إبرام العقد، وأرشفة العقد وإمكانية الوصول إليه أم لا، والوسائل التقنية من أجل تحديد وتصحيح الأخطاء المرتكبة في إدخال المعلومات، واللغات المقترحة لإبرام العقد. كذلك يجب أن يحدد مزود الخدمات قواعد التصرف الملائمة التي يخضع لها وكذلك المعلومات حول طريقة استعراض هذه القواعد بوسائل إلكترونية. هذا وإن قواعد التصرف تنظّم طريقة عمل مزود الخدمات والأصول التي يخضع لها بصورة تفصيلية وكيفية سير إجراءاته واستجابته لطلبات المتعاملين. ويلتزم مزود الخدمات أن تكون البنود التعاقدية والشروط العامة المقدمة للعميل محققة بشكل يسمح له بحفظها وبنسخها. كما يلتزم مقدم العرض بعرضه طالما بقي ممكناً الوصول إلى هذا العرض بالطرق الإلكترونية. على أن الفقرتين ١ و٢ من هذه المادة لا تطبقان على العقود التي تبرم حصراً من خلال تبادل بريد إلكتروني أو من خلال اتصالات فردية متوازية. إن أحكام هذه المادة تعتبر أيضاً مكملة لإرادة الفرقاء المحترفين فقط، أي أنه في حال وجود اتفاق مخالف بين المحترفين فهو الذي يطبق.

تستعرض المادة ١٣ من الإرشاد الأصول والمبادئ المطبقة عند إجراء طلبية من قبل العميل بوسيلة إلكترونية. فمزود الخدمات يجب أن يعلم عن استلام طلبية العميل دون تأخير غير مبرر بوسائل إلكترونية. كما يكون الأطراف الموجّهة إليهم الطلبية أو الإشعار بالاستلام قد استلموها عندما يمكن لهم أن يصلوا إليها. كما يضع مزود الخدمات بتصرف العميل وسائل تقنية ملائمة وفعالة وممكن الوصول إليها، تسمح له بتحديد الأخطاء المرتكبة في إدخال المعلومات وبتصحيحها وذلك قبل إجراء الطلبية. على أن الفقرتين ١ و٢ من هذه المادة لا تطبقان على العقود التي تبرم حصراً من خلال تبادل بريد إلكتروني أو من خلال اتصالات فردية متوازية. إن أحكام هذه المادة تعتبر أيضاً مكملة لإرادة الفرقاء المحترفين فقط، أي أنه في حال وجود اتفاق مخالف بين المحترفين فهو الذي يطبق.

تنظم المادة ١٤ من الإرشاد كيفية عرض الأسعار[٢٤]. فهذه يجب أن تذكر بطريقة واضحة، وأن تحدد ما إذا كانت الضرائب ونفقات التسليم مشمولة بالسعر أم لا. كما يجب أن تكون وسيلة الدفع المعتمدة آمنة وسهلة الاستعمال، وأن يُعلم المحترف المستهلك بالشروط المطبقة على وسيلة الدفع والعملة التي يتم بها الدفع. تتناول المادة ١٥ من الإرشاد حق الرجوع الممنوح للمستهلك عن طلبه ضمن مهلة محددة[٢٥]، حتى يتمكن من إعادة النظر في السلعة والخدمة المقدمة إليه ومدى انطباقها على المواصفات وعلى حاجاته الفعلية. وهذا الحق يتعلق بالنظام العام طالما أنه يتعلق بحماية المستهلك، وقد أكدت هذه المادة على ذلك من خلال عبارة "خلافاً لأي نص آخر". ويحق للمستهلك العدول عن قراره بشراء سلعة أو استئجارها أو الاستفادة من الخدمة في خلال مهلة عشرة أيام تسري اعتبارا من تاريخ العقد بالنسبة للخدمات ومن تاريخ التسليم بالنسبة للبضائع والسلع. يمكن للأطراف الاتفاق على مهلة معينة بإيراد بند خاص في العقد. وفي بعض الحالات لا يحق للمستهلك ممارسة حق الرجوع، بالنظر لطبيعة السلعة أو البضاعة أو لافتراض موافقة المستهلك الصريحة أو الضمنية عليها أو تحديد مواصفاتها مسبقاً أو لنشوء العيب نتيجة فعل صادر عنه. وهذه الحالات هي: حالة استفادته من الخدمة أو

استعمال السلعة قبل انقضاء مهلة العشرة أيام أو المهلة المتفق عليها، وحالة البضائع أو السلع المصُنعة بناءً لطلبه أو وفقاً لمواصفات محددة، وحالة الأشرطة أو الأسطوانات أو الأقراص المدمجة أو البرامج المعلوماتية في حال تم إزالة غلافها، وحالة شراء الصحف والمجلات والمنشورات لاسيما الكتب، وحالة ظهور عيب في السلعة من جراء سوء حيازتها أو حفظها من قبل المستهلك، وحالة تقديم خدمات إيواء أو نقل أو إطعام أو لهو تقدّم في تاريخ معين أو بصورة دورية محددة، وحالة تحميل برامج عبر الإنترنت إلا إذا وجد عيب في البرنامج منع حصول التحميل. وعند ممارسة المستهلك حقه بالعدول، يتوجب على المحترف إعادة المبالغ التي قبضها من المستهلك إليه، على أن يتحمل الأول مصاريف التسليم.

جاءت المادة ١٦ لتطبق المبدأ الذي أوردته المادة ١٠ على الأعمال المتعلقة بعقد نقل البضائع[٢٦]، إذ يمكن استخدام الرسالة الإلكترونية لتنظيم عقد نقل البضائع أو أي مستند يتعلق بفعل مرتبط به أو أي مستند يتم تنفيذاً له، بما في ذلك على سبيل المثال لا الحصر بيانات مواصفات البضاعة وأعدادها وكميتها أو علاماتها وإيصال البضائع وتأكيد تحميل البضاعة وإصدار التعليمات إلى الناقل والمطالبة بتسليم البضاعة والإذن بالإفراج عن البضائع والإخطار بوقوع هلاك أو تلف في البضاعة وجميع الإخطارات والإشعارات المتعلقة بالعقد أو بتنفيذه ومنح حقوق على البضاعة أو اكتسابها أو التنازل عنها أو نقلها والتعهد بتسليم البضاعة إلى شخص معين[٢٧].

تضع المادة ١٧ من هذا الإرشاد القواعد القانونية المتعلقة بمسؤولية المحترف، وهذه لا تختلف عن المبادئ الأساسية للقواعد العامة في المسؤولية التعاقدية. إذ يُسأل كل من يمارس التجارة الإلكترونية تجاه العميل أو المشتري عن حسن تنفيذ موجباته الناجمة عن العقد. ولا يمكن إعفاؤه من المسؤولية كلياً أو جزئياً إلا إذا أثبت أن عدم تنفيذ العقد أو سوء تنفيذه يعود للعميل أو للمشتري أو للقوة القاهرة أو لفعل الغير.

يتضمن **الباب الرابع** المعنون "أحكام ختامية" أحكاماً تتعلق بقواعد التصرف[٢٨]، وبالحلول غير القضائية للنِزاعات وبالمراجعات القضائية وبالتعاون بين الدول الأعضاء وبالعقوبات.

وفقاً للمادة ١٨، تقوم الهيئات أو المنظمات المهنية[٢٩] أو العائدة للشركات أو للمستهلكين بوضع قواعد للتصرف تهدف إلى حسن تطبيق أحكام هذا الإرشاد. وبعرض هذه القواعد بالوسائل الإلكترونية على الجمهور. إن قواعد التصرف[٣٠] تضع الأصول التطبيقية والتفسيرية والإجرائية لأحكام هذا الإرشاد. كما من الممكن أن تضيف على أحكامه بشرط أن تبقى منسجمة معه. تشكل قواعد التصرف الأداة الأنسب لتحديد القواعد الأدبية المطبّقة على الاتصالات التجارية. إن قواعد التصرف لها الصفة الاختيارية حيث يعود للفرقاء المعنيين بها أن يقرروا الالتزام بها أو عدمه. وحتى تكون قواعد التصرف ملائمة وفعالة ومتوازنة تجاه المصالح المتعارضة كافة، يفترض أن تشارك الهيئات والمنظمات التي تمثل المستهلكين في وضع وتطبيق قواعد التصرف المنوه عنها.

تتطرق المادة ١٩ للحلول غير القضائية للنِزاعات بين مزودي خدمات مجتمع المعلومات (الخدمات الإلكترونية) والعملاء. وهذه الحلول تهدف إلى تسريع الفصل والتخفيف من تعقيدات الإجراءات وأحياناً الاستعانة بخبرات متخصصة. وتتضمن الحلول غير القضائية للنِزاعات الوساطة والتحكيم[٣١]، وهي تتلاءم مع متطلبات التجارة الإلكترونية، التي تقوم على السرعة وتتسم بطابع دولي[٣٢]. وتتيح المادة ١٩ للفرقاء استعمال آليات الحلول غير القضائية من أجل تسوية الخلافات[٣٣]، وذلك من خلال وسائل إلكترونية ملائمة، وباتفاق الفرقاء[٣٤]، على أن يتم تأمين الضمانات الإجرائية الملائمة للأطرف المعنية[٣٥]، لاسيما في مسائل حماية المستهلك، كحفظ حق الدفاع والوجاهية والتقاضي على درجتين وتعليل القرارات.

تتناول المادة ٢٠ من الإرشاد المراجعات القضائية، وتقضي بأن تسمح الإجراءات القضائية المطبّقة على خدمات مجتمع المعلومات (الخدمات الإلكترونية) باتخاذ تدابير سريعة، لاسيما عبر أمر على عريضة، لوقف كل انتهاك وللوقاية من كل تعد جديد على المصالح المعنية.

لا تكون الضوابط المعتمدة للتجارة الإلكترونية في دولةٍ ما فعالة إلا إذا امتد أثرها إلى الدول الأخرى، وكانت منسجمة بين الدول المختلفة، وذلك بالنظر للطابع الدولي لهذه التجارة. لذلك، كان لا بد من إيلاء التعاون بين الدول الأعضاء أهمية قصوى. تتناول المادة ٢١ من الإرشاد هذه المسألة، وهي تلزم الدول الأعضاء باعتماد وسائل للمراقبة وللتحقيق لازمة لتطبيق فعال للإرشاد الحالي وبالسهر على أن يقدم لها مزود الخدمات المعلومات المطلوبة. وعليها أيضاً أن تتعاون لضمان تطبيق فعال للإرشاد الحالي، وأن تسمي فيما بينها أشخاصاً مفوضين للاتصال بهم.

وفقاً للمادة ٢٢ من الإرشاد، ينبغي على الدول مراجعة قوانين حماية المستهلك الوطنية وملاءمتها بالحد الأدنى مع

القواعد المشار إليها في هذا الإرشاد عندما يكون التعامل بين المستهلك والمحترف قد تم عن بعد أو بوسائل إلكترونية على شبكة الإنترنت.

لا يتحقق فرض احترام أي قاعدة إلا إذا اقترنت مخالفتها بعقوبات رادعة ومناسبة. ويعود للدول، وفقاً للمادة ٢٣ من هذا الإرشاد، تحديد نظام العقوبات المطبق على مخالفة أحكامه ضماناً لفعاليتها ووجوب تطبيقها.

هوامش

1- See E-commerce Statistics Compendium, November 2009, available: http://econsultancy.com/uk/reports/e-commerce-statistics
- More than 85% of the world's internet users surveyed have purchased something online, according to the Nielsen Company. [Source, Nielsen, Feb 2008]
- UK shoppers will spend £13.16bn online in the last quarter of 2008, 15% more than Q4 2007. [Source: IMRG /Capgemini via Econsultancy blog, Nov 2008] – This equates to £215 for every person in the UK, but represents a slowdown compared with the 54% year-on-year increase in 2007
- Online retail sales in the UK are predicted to reach £44.9bn in 2012, up from £19.5bn in 2008. [Source: Verdict Research via eMarketer, Sept 2008]
- Online retail is still set to reach £31.2 bnby 2013, accounting for 10.0% of total retail spending. [Source: Verdict Research, June 2009]
- See E-commerce in Saudi Arabia: adoption and perspectives, September 2004, by Sadiq M. Sait 1 Khalid M. Al-Tawil 2 Syed Ali Hussain http://css.escwa.org.lb/SD/0977/b10.pdf
- See E-commerce in Bahrain, http://css.escwa.org.lb/SD/0977/c5.pdf
- See E-commerce in Palestine, published by ESCWA, available: http://css.escwa.org.lb/SD/0977/c6.pdf

2- See E-market place, available: http://www.idea.gov.uk/idk/core/page.do?pageId=82639

3- The Future of Internet Economy, A Statistical Profile, OECD ministerial meeting on the future of the internet economy, Seoul-Korea, 17-18 June 2008, available: http://www.oecd.org/dataoecd/44/56/40827598.pdf

4- See Internet Usage Statistics: Internet Usage and World Population Statistics are for June 30, 2010, available: http://www.internetworldstats.com/stats.htm

5- Bing Bang Theory, available: http://63.111.106.66/technology/whitepapers/bigbangtheory.pdf

6- See OECD guidelines for Consumer protection in the context of Electronic commerce is available online at: http://www.oecd.org/dataoecd/18/29/34023811.pdf

7- See example on Collective agreement: Collective agreement between the business practices & consumer protection authority (The «Employer») and the B.C. government and service employees' union (BCGEU), Effective from April 1, 2006 to March 31, 2010, available: http://www.bcgeu.ca/files/Business_Practices_2006_2010.pdf

8- See Decoding codes: The dialogue between consumers and suppliers through codes of conduct in the European Community, available: http://www.springerlink.com/content/r202h4651862u602/

The second Consumer Action Programme of the European Community (1981) has introduced the idea of a dialogue between producers and consumers, leading to voluntary agreements or codes of conduct. Today, several types of codes exist within the area of the European Community. They differ in their geographic origin, their adoption procedure and their modus operandi. Many codes are good examples of a new type of rule-making in European consumer affairs, namely sponsored regulation. In between the public and the private normative order, a grey area of paralegal norms is existing and developing steadily. The EC authorities often prefer to provide the conditions for rule-making by private parties instead of producing norms themselves. In those cases, codes of conduct may replace the law, substitute it, or add to it. Codes of conduct are not the only possible output of the dialogue between producers and consumers, nor are they the only example of sponsored regulation. Others are model contracts, complaint boards, and standardization institutes

- See A Unified Consumer Protection Code, By Kevin Hoy, September 09 2005, available: http://www.internationallawoffice.com/newsletters/detail.aspx?g=62d4ba76-b386-4a54-8f2e-4c07a52a2aac

9- See *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), published in Official Journal of the European Communities dated 17.7.2000, L 178/1, available: <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf>.

10- See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, United Nations, New-York 1999, available:
http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

11- See Protecting consumers Online, A Report from the Federal Trade Commission Staff, December 1999, available: http://www.ftc.gov/os/1999/12/fiveyearreport.pdf
«*In the electronic marketplace, frauds can appear suddenly, spread rapidly, and disappear without notice or warning. Law enforcement has to be just as fast. The FTC uses technology based tools -- some of which it pioneered -- to protect consumers. Among these tools are Consumer Sentinel, Internet "Surf Days," and the Internet Lab*».

12- File sharing

13- Prepaid TV

14- See OECD guidelines for Consumer protection in the context of Electronic commerce» (I. transparent and effective protection) «*Consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce*».
http://www.oecd.org/dataoecd/18/29/34023811.pdf

15- See *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* 1996 with additional article *5 bis* as adopted in 1998, articles 13, 14, and 15
http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

16- See International Trade Law, by Indira Carr, 3rd Edition, Cavendish publishing. Available: http://books.google.com/
«A problem normally voiced about electronic messages is the uncertainty in attributing messages to those who are supposed to have sent them. What guarantee is there that the electronic message is really sent by the person who is indicated as being the originator? One way of resolving this uncertainty would be to follow up the electronic message with a paper document. This defeat the advantages-speed, efficiency and economic benefits – normally advanced in favour of electronic communication. The EC model law handles this uncertainty by presuming that a data message under certain condition would be regarded as that of the originator. So where the originator and the addressee agreed upon an authentication procedure and that procedure is applied by the addressee, the message will be attributed to the originator according to article 13 (3-a) of the EC model law».

17- See UNCITRAL Model Law on Electronic Commerce, Article 15 (2)

18- UNCITRAL Arbitration Rules: Article 2 Notice and calculation of periods of time
«A notice shall be deemed to have been received on the day it is delivered in accordance with paragraphs 2, 3 or 4, or attempted to be delivered in accordance with paragraph 4. A notice transmitted by electronic means is deemed to have been received on the day it is sent, except that a notice of arbitration so transmitted is only deemed to have been received on the day when it reaches the addressee's electronic address».
http://www.uncitral.org/pdf/english/texts/arbitration/arb-rules-revised/arb-rules-revised-2010-e.pdf

19- See UNCITRAL Model Law on Electronic Commerce, Article 15 (3,4)

20- See the Canadian Code of Practice for Consumer Protection In Electronic Commerce, Principle7- Unsolicited E-mail available at: http://www.cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00072.html

> *7.1 Vendors shall not transmit marketing e-mail to consumers without their consent, except when vendors have an existing relationship with them. An existing relationship is not established by consumers simply visiting, browsing or searching vendors> Web sites.*
> *7.2 Any marketing e-mail messages vendors send shall prominently display a return e-mail address and shall provide in plain language a simple procedure by which consumers can notify vendors that they do not wish to receive such messages.*

21- The Electronic Commerce (EC Directive) Regulations 2002 -

8. Unsolicited commercial communications: A service provider shall ensure that any unsolicited commercial communication sent by him by electronic mail is clearly and unambiguously identifiable as such as soon as it is received.

22- See Business-to-Consumer E-commerce Statistics, Figure 1. B2C e-commerce indicators in selected OECD countries for 2000 or latest available year, available: http://www.oecd.org/dataoecd/34/36/1864439.pdf

٢٣- لقد ورد في المادة (٤) من القانون المصري رقم ٦٧ لسنة ٢٠٠٦ بإصدار قانون حماية المستهلك:
على المورد أن يضع على جميع المراسلات و المستندات والمحررات التي تصدر عنه في تعامله أو تعاقده مع المستهلك ، بما فى ذلك المحررات والمستندات الإلكترونية – البيانات التي من شأنها تحديد شخصيته، وخاصة بيانات قيده في السجل الخاص بنشاطه وعلامته التجارية إن وجدت.
كما ورد في الفصل العاشر، المادة ٥١ و٥٢ من القانون اللبناني مرسوم رقم ١٣٠٦٨ تاريخ ٥ آب ٢٠٠٤ المتعلق بحماية المستهلك:

المادة ٥١: « ترعى أحكام هذا الفصل العمليات التي يجريها المحترف عن بُعد أو في محل إقامة المستهلك، لا سيما تلك التي تتم في مكان إقامة المستهلك أو عبر الهاتف أو الإنترنت، أو أية وسيلة أخرى معتمدة لذلك. لا ترعى أحكام هذا الفصل العمليات المالية والمصرفية والبيع بالمزاد العلني والعمليات التي تتناول أموالاً غير منقولة».
المادة ٥٢: « يجب تزويد المستهلك، في الحالات المنصوص عليها في المادة ٥١ ، بمعلومات واضحة وصريحة تتناول المواضيع التي تمكنه من اتخاذ قراره بالتعاقد، لا سيما:
– تعريف المحترف واسمه وعنوانه ورقم ومكان تسجيله، وبريده الإلكتروني، بالإضافة إلى أية معلومات تتيح تعريف المحترف.
– السلعة والخدمة المعروضة وكيفية استعمالها والمخاطر التي قد تنتج عن هذا الاستعمال.
– مدة العرض.
– ثمن السلعة أو الخدمة والعملة المعتمدة وكافة المبالغ التي قد تضاف إلى الثمن لا سيما الرسوم والضرائب والمصاريف أياً كانت، وكيفية تسديد هذه المبالغ.
– الخ. . .

24- See The Australian Guidelines for Electronic Commerce, Commonwealth of Australia 2006, available at: http://www.treasury.gov.au/

25- Businesses engaged in electronic commerce should provide enough information about the terms, conditions and costs of a transaction to enable consumers to make informed decisions. 26. This information should be clear, accurate and easily accessible. It should be provided in a way that gives consumers an adequate opportunity for review before entering into the transaction and that allows consumers to retain a copy of the information. 28. All information referring to costs should indicate the applicable currency, including guidance on how to get information on exchange rates, or a link to a site where such information may be found. 31. The information should include a prominently displayed single-figure total minimum price for the product or service. All compulsory charges such as delivery, postage and handling charges should be included in this price. This does not preclude a business itemising the total costs to the consumer collected by the business.

See The Australian Guidelines for Electronic Commerce, Commonwealth of Australia 2006, available at: http://www.treasury.gov.au/

34. Businesses should put in place procedures that let consumers:
34.1 review and accept or reject the terms and conditions of the contract;
34.2 identify and correct any errors; and
34.3 confirm and accept or reject the offer.
35. Consumers should be able to retain a record of any order, transaction confirmation, or acceptance of any offer they make.

26- See The General Agreement on Tariffs and Trade (GATT) covers international trade in goods, available: http://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm

27- *«Businesses engaged in electronic commerce with consumers should provide accurate and easily accessible information describing the goods or services offered; sufficient to enable consumers to make an informed decision about whether to enter into the transaction and in a manner that makes it possible for consumers to maintain an adequate record of such information».* OECD guidelines for Consumer protection in the context of Electronic commerce (b. information about the goods or services). http://www.oecd.org/dataoecd/18/29/34023811.pdf

28- See Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID) http://www.unece.org/trade/untdid/texts/d220_d.htm
These rules aim at facilitating the interchange of trade data effected by teletransmission, through the establishment of agreed rules of conduct between parties engaged in such transmission. Except as otherwise provided in these rules, they do not apply to the substance of trade data transfers.

29- See FEDMA Code on E-commerce & Interactive marketing, Federation of European Direct Marketing, 5 September 2000, available at: http://www.fedma.org/getfile.php/342989.1014.xdpffdbpwd/Code_of_conduct_for_e-commerce.pdf

See APTICE Code of Practice for e-commerce and e-government, 2001. Spain, available at: http://www.agace.org/en/pdfs/AGACE_code_of_practice.pdf

30- See the directive on E-Commerce (2000/_/EC), article 16 states « Member States and the Commission shall encourage the drawing up of codes of conduct at Community level, by trade, professional and consumer associations and organisations, designed to contribute to the proper implementation of articles 5 to 15. »

31- See UNCITRAL Arbitration Rules (as revised 2010), available at: http://www.uncitral.org/pdf/english/texts/arbitration/arb-rules-revised/arb-rules-revised-2010-e.pdf

- UNCITRAL Model Law on International Commercial Arbitration, available at: http://www.uncitral.org/pdf/english/texts/arbitration/ml-arb/06-54671_Ebook.pdf

- Convention on the Recognition and Enforcement of Foreign Arbitral Awards, available at: <http://www.uncitral.org/english/texts/arbitration/NY-conv.htm>.

- European Convention on International Commercial Arbitration, United Nations, Treaty Series, vol. 484, p. 364 No. 7041 (1963-1964) entered into force in 1964. Currently, there are some works on possible revision of the convention. See: United Nations Economic and Social Council, Advisory Group to Consider Possible Revisions to the European Convention on International Commercial Arbitration of 1961, online: <http://www.unece.org/ie/Wp5/eucon.htm>. This opens the possibility to adapt the Convention to the needs of dispute settlement by means of electronic commerce.

32- Online dispute resolution (ODR) is a branch of dispute resolution which uses technology to facilitate the resolution of disputes between parties. It primarily involves negotiation, mediation or arbitration, or a combination of all three. In this respect it is often seen as being the online equivalent of alternative dispute resolution (ADR). However, ODR can also augment these traditional means of resolving disputes by applying innovative techniques and online technologies to the process.
http://en.wikipedia.org/wiki/Online_dispute_resolution#cite_note-42

33- See OECD guidelines for Consumer protection in the context of electronic commerce (B. alternative dispute resolution and redress) http://www.oecd.org/dataoecd/18/29/34023811.pdf
Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.

٣٤- لقد ورد في المادة ٨ من قانون التحكيم السوري الجديد رقم ٤ لعام ٢٠٠٨: « يجب أن يكون اتفاق التحكيم مكتوباً وإلا كان باطلاً، ويكون الاتفاق مكتوباً إذا ورد في عقد أو وثيقة . . . ، أو في أية رسائل متبادلة عادية كانت أو مرسلة بوسائل الاتصال المكتوب (البريد الإلكتروني، الفاكس، التلكس) إذا كانت تثبت تلاقي إرادة مرسليها على اختيار التحكيم وسيلة لفض النزاع».

35- See the Canadian Code of Practice for Consumer Protection In Electronic Commerce, Principle 6- Complaint Handling and Dispute Resolution available at: http://www.cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00072.html

6.1 Vendors shall provide consumers with access to fair, timely and effective means to resolve problems with any transaction.
6.2 Vendors shall offer an internal complaints-handling process that:

a) is easily accessible online and offline;
b) is available to consumers free of charge;
c) is easy to use;
d) acknowledges complaints within seven business days of receipt and endeavours to resolve or address these complaints within 45 days of acknowledgment; and
e) records and monitors complaints.

6.3 When a consumer and a vendor cannot resolve a complaint, the vendor is strongly encouraged to offer to refer matters to an appropriate third-party dispute resolution service, use of which shall be at the consumer>s discretion.
6.4 Any dispute resolution service(s) offered by the vendor in accordance with 6.3 shall:

a) be available to be initiated online and irrespective of consumers' location;
b) be easily accessible to consumers (e.g. via a hyperlink from vendors' Web sites);
c) be easy to use;
d) be offered at nominal or no cost to consumers;
e) be expeditious, with reasonable time limits for each stage of the process;
f) be fair (i.e. meet the standards of due process);
g) commit vendors to abide by awards when consumers agree to them;

h) be operated by an independent and impartial body; and
i) be transparent in all aspects of its operations, including services, procedures, governance structure, dispute resolution personnel, and the results of dispute resolutions. With respect to the last, the dispute resolution service provider shall make public its arbitration case results and detailed statistics on its confidential dispute resolution results covering the number and type of complaints and the proportion resolved in the customer's favour.

نص إرشاد التجارة الإلكترونية وحماية المستهلك

الباب الأول: أحكام عامة

المادة ١: أهداف الإرشاد ونطاق تطبيقه

يهدف هذا الإرشاد إلى وضع قواعد قانونية عامة من شأنها المساهمة في ازدهار الأسواق من خلال تأمين الانتقال الحر لخدمات مجتمع المعلومات (الخدمات الإلكترونية) بين الدول الأعضاء.

المادة ٢: تعاريف

التجارة الإلكترونية: هي نشاط اقتصادي يعرض بموجبه أو يؤمن عن بعد وبوسائل إلكترونية تقديم الأموال أو الخدمات. ويدخل أيضاً في إطار التجارة الإلكترونية خدمات تقديم المعلومات مباشرةً على الخط وخدمات الاتصالات التجارية وأدوات البحث واسترجاع المعلومات، وخدمات تأمين الوصل بشبكة اتصال أو استضافة البيانات.

رسالة إلكترونية: هي المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية، بما في ذلك على سبيل المثال البريد الإلكتروني.

مُرسِل الرسالة الإلكترونية: هو الشخص الذي أنشأ الرسالة الإلكترونية أو أرسلها قبل تخزينها من قبل المرسل إليه أو الغير، ولا يشمل الشخص الذي يتصرف كوسيط.

المُرسَل إليه: هو الشخص الذي قصد المُرسل أن يتسلم الرسالة الإلكترونية، ولا يشمل الشخص الذي يتصرف كوسيط.

الوسيط: هو الشخص الذي يقوم، نيابة عن شخص آخر، بإرسال أو إستلام أو تخزين رسالة إلكترونية أو بتقديم خدمات أخرى فيما يتعلق بهذه الرسالة.

خدمة إلكترونية: هي كل خدمة، عادةً لقاء مقابل، مقدّمة عن بعد بواسطة وسائل معلوماتية لمعالجة وتخزين البيانات، وذلك بناءً لطلب فردي من المتعامل.

عقد إلكتروني: هو عقد نظّم وتم توقيعه بوسيلة إلكترونية.

المستهلك: هو كل شخص طبيعي أو معنوي يشتري سلعة أو خدمة أو يستأجرها أو يستعملها أو يستفيد منها، وذلك لأغراض لا تدخل في نطاق نشاطه المهني أو التجاري.

المحترف: هو الشخص الطبيعي أو المعنوي الذي يحترف نشاطاً معيناً كبيع السلع أو توزيعها أو تأجيرها أو تقديم الخدمات.

خطابات أو اتصالات تجارية: كل شكل اتصال مخصص لترويج، بشكل مباشر أو غير مباشر، الأموال أو الخدمات أو صورة شركة أو مؤسسة أو شخص يمارس نشاطاً تجارياً أو صناعياً أو حرفياً أو يمارس مهنة منظمة بقانون. لا تشكل اتصالات إلكترونية بمفهوم هذه المادة:

- المعلومات التي تسمح بالوصول المباشر إلى نشاطات الشركة أو المؤسسة أو الشخص، لاسيما اسم الموقع أو عنوان البريد الإلكتروني؛
- الاتصالات المتعلقة بالأموال أو بالخدمات أو بصورة الشركة أو المؤسسة أو الشخص، المجراة بشكل مستقل، لاسيما عندما تقدم بدون مقابل مادي.

نظام رسائل معلوماتي آلي: هو برنامج أو وسيلة إلكترونية تُستخدم لاستهلال إجراء ما أو للاستجابة كلياً أو جزئياً للرسائل الإلكترونية أو لعمليات تنفيذها، وذلك دون مراجعة أو تدخل من شخص طبيعي في كل مرة يستهل النظام إجراء ما أو يطلق استجابة ما.

المادة ٣: حرية التجارة الإلكترونية

لا يمكن للدول الأعضاء تقييد الانتقال الحر لخدمات مجتمع المعلومات (الخدمات الإلكترونية) من دولة عضو إلى دولة عضو أخرى.

تُمارس التجارة الإلكترونية بحرية ضمن نطاق القوانين النافذة. لكن يمكن للدول المتعاقدة أن تأخذ في صدد خدمة معينة لمجتمع المعلومات تدابير تخالف الفقرة الأولى، عندما تكون هذه التدابير ضرورية:

للحفاظ على النظام العام، ولاسيما الوقاية أو التحقيق أو الاكتشاف أو الملاحقة في المسائل الجزائية، وحماية القاصرين

ومسائل التمييز العنصري أو الجنسي أو الديني أو التعرض لكرامة الإنسان.

- للحفاظ على الصحة العامة؛

- للحفاظ على الأمن العام والدفاع الوطني والنظام العام؛

- لحماية المستهلكين و/أو المستثمرين.

الباب الثاني: الخطابات أو الرسائل الإلكترونية التجارية

المادة ٤: إسناد الرسائل الإلكترونية

تعتبر الرسالة الإلكترونية قد صدرت عن المُرسل إذا أُرسلت:

من شخص مكلّف من قبله.

من نظام معلوماتي مُبرمج من قبل المُرسل أو من قبل شخص مكلف من قبله للعمل تلقائياً.

المادة ٥: إشعارات استلام الرسالة الإلكترونية

تكون إشعارات إرسال الرسائل الإلكترونية أو إشعارات استلامها مقبولة قانوناً في الدول الأعضاء. إلا أن استلام إشعار إلكتروني إثباتاً لإرسال رسالة إلكترونية أو لاستلامها لا يعني حكماً مطابقة المعلومات التي تم استلامها للمعلومات التي تم إرسالها.

المادة ٦: زمان ومكان إرسال واستلام الرسالة الإلكترونية

ما لم يتفق المُرسِل والمُرسَل إليه على خلاف ذلك، إن إرسال الرسالة الإلكترونية يتحقق في المبدأ عندما تدخل أول نظام معلوماتي لا يخضع لسيطرة المُرسل أو لسيطرة شخص مكلف من قبله، أو عند تلقيها من قبل المرسل إليه وذلك في حالة بقائها في ذات النظام المعلوماتي.

ما لم يتفق المُرسِل والمُرسَل إليه على خلاف ذلك، يتحدد وقت استلام الرسالة الإلكترونية على الشكل التالي:

- إذا كان المُرسَل إليه قد حدّد نظاماً معلوماتياً لاستلامها:

- يتم الاستلام وقت دخول الرسالة النظام المعلوماتي المحدّد؛
- أو وقت استخراج المُرسَل إليه للرسالة أو علمه بواقعة إرسال الرسالة على عنوان إلكتروني معين في حال إرسالها على نظام معلوماتي غير ذلك التي قد تم تعيينه.

- إذا لم يحدد المُرسَل إليه نظاماً معلوماتياً، يتم الاستلام عندما تدخل الرسالة الإلكترونية نظاماً معلوماتياً تابعاً للمرسل إليه.

ما لم يتفق المُرسِل والمُرسَل إليه على خلاف ذلك، تُعتبر الرسالة الإلكترونية قد أُرسلت من مكان مقر عمل المُرسِل، وتُعتبر أنها استلمت في مكان مقر عمل المُرسَل إليه. إذا كان للمُرسِل أو للمُرسَل إليه أكثر من مقر عمل واحد، كان مقر العمل هو المقر الذي له أوثق علاقة بالمعاملة المعنية، وإذا لم يوجد مثل هذه المعاملة، يُعتمد مقر العمل الرئيسي. إذا لم يكن للمُرسِل أو للمُرسَل إليه مقر عمل، يُعتمد محل إقامته المعتاد.

المادة ٧: المعلومات الواجب تقديمها

تحرص الدول الأعضاء على أن تكون الخطابات أو الاتصالات التجارية، التي تنضوي ضمن خدمات مجتمع المعلومات (الخدمات الإلكترونية)، تلبي على الأقل الشروط التالية:

- أن يكون الاتصال أو الخطاب التجاري معرّفاً كذلك بشكل واضح؛
- أن يحدّد بشكل واضح الشخص الطبيعي أو المعنوي الذي يتم لصالحه الخطاب أو الاتصال التجاري؛
- أن تكون الحسومات والعروض المحسومة محددة كذلك، وأن تكون شروط المشاركة فيها ظاهرة بشكل دقيق وغير ملتبس وممكن الحصول عليها.

المادة ٨: الاتصالات أو الخطابات التجارية غير المرغوب بها

على الدول الأعضاء التي تسمح بالاتصالات أو الخطابات غير المرغوب بها بواسطة البريد الإلكتروني أن تسهر على أن الاتصالات التجارية المنفّذة بواسطة مزود خدمات تقنية مقيم على أراضيها قابلة للتحديد بطريقة واضحة وغير ملتبسة منذ تلقيها من قبل المرسل إليه.

تتخذ الدول الأعضاء تدابير تضمن أن مزودي الخدمات التقنية الذين يرسلون بواسطة البريد الإلكتروني اتصالات تجارية غير مرغوب بها، يراجعون بشكل متواصل سجلات من الممكن أن يتسجّل فيها الأشخاص الطبيعيون الذين لا يرغبون باستلام هذا النوع من الاتصالات. وأخيراً أن يحترم مزودو الخدمات التقنية رغبات هؤلاء الأشخاص.

المادة ٩: المهن المنظمة بقانون

تحرص الدول الأعضاء على أن استعمال الخطابات أو

الاتصالات التجارية، التي تنضوي ضمن خدمات مجتمع المعلومات (خدمات إلكترونية) المقدّمة من قبل عضو في مهنة منظمة بقانون، يكون مسموحاً شرط احترام القواعد المهنية التي تتعلق باستقلالية المهنة وبكرامتها وبشرفها وكذلك بالسر المهني وبالإخلاص تجاه الزبائن والأعضاء الآخرين في المهنة.

تشجع الدول الأعضاء الهيئات والمؤسسات المهنية على وضع قواعد للتصرف بغية تحديد المعلومات الممكن إعطاؤها لغايات الاتصالات التجارية مع احترام القواعد المذكورة في الفقرة السابقة.

الباب الثالث: العقود الإلكترونية

المادة ١٠: الاعتراف القانوني بالعقود الإلكترونية

تحرص الدول الأعضاء على أن نظامها القانوني يسمح بإبرام العقود بوسائل إلكترونية، وأن النظام القانوني المطبّق على آليات التعاقد لا يشكل عائقاً أمام استعمال العقود الإلكترونية، ولا يحرم هذه العقود من الآثار والاعتراف القانوني لمجرد أنها منظّمة بوسيلة إلكترونية. يجوز استخدام الرسائل الإلكترونية للتعبير عن العروض وقبول العروض. يعود للدول الأعضاء أن تعتمد أن الفقرة السابقة لا تطبق على جميع العقود أو على البعض منها، ممّا يعود إلى الفئات التالية:

- العقود التي تنشىء أو تنقل حقوقاً على أموال عقارية، باستثناء عقود الإيجار؛
- العقود التي من أجلها يتطلب القانون تدخل المحاكم أو السلطات العامة أو مهناً تمارس سلطة عامة؛
- عقود الضمان المقدمة من قبل أشخاص يتصرفون لغايات لا تدخل ضمن إطار نشاطاتهم المهنية أو التجارية؛
- العقود التي تتعلق بقانون العائلة أو قانون الإرث.

تطبق على العقود الإلكترونية أحكام القانون المدني والتجاري في كل ما لا يتعارض مع أحكام هذا الإرشاد.

المادة ١١: استخدام أنظمة الرسائل المعلوماتية الآلية في تكوين العقود

لا يجوز إنكار صحة العقد الذي يتكون بالتفاعل بين نظام معلوماتي آلي وشخص طبيعي أو بالتفاعل بين نظامين معلوماتيين آليين، لمجرد عدم مراجعة شخص طبيعي المسائل التالية: الأفعال التي قامت بها الأنظمة المعلوماتية للرسائل الآلية، والعقد الناتج عن تلك الأفعال، وتدخله فيها.

المادة ١٢: المعلومات الواجب تقديمها

باستثناء الحالة التي يكون فيها الأطراف غير المعتبرين مستهلكين قد اتفقوا على العكس، تحرص الدول الأعضاء على أن يقدم مزود الخدمات على الأقل المعلومات التالية، مصاغة بشكل واضح، مفهوم وغير ملتبس، وقبل أن يجري العميل طلبيته:

- اسمه وشهرته ومقامه واسم ممثله التجاري ومركزه وعنوانه التجاري وسجله التجاري وعنوان بريده الإلكتروني وأرقام هاتفه.
- المراحل التقنية المختلفة الواجب اتباعها من أجل إبرام العقد.
- إذا كان العقد بعد إبرامه يُدخل ضمن الأرشيف أم لا من قبل مزود الخدمات وإذا كان ممكناً الوصول إليه أم لا.
- الوسائل التقنية من أجل تحديد وتصحيح الأخطاء المرتكبة في إدخال المعلومات قبل أن يتم إجراء الطلبية.
- اللغات المقترحة لإبرام العقد.

باستثناء الحالة التي يكون فيها الأطراف غير المعتبرين مستهلكين قد اتفقوا على العكس، تحرص الدول الأعضاء على أن يحدد مزود الخدمات قواعد التصرف الملائمة التي يخضع لها وكذلك المعلومات حول طريقة استعراض هذه القواعد بوسائل إلكترونية.

إن البنود التعاقدية والشروط العامة المقدمة للعميل يجب أن تكون بشكل يسمح له بحفظها وبنسخها. يلتزم مقدم العرض بعرضه طالما بقي ممكناً الوصول إلى هذا العرض بالطرق الإلكترونية. إن الفقرتين ١ و٢ من هذه المادة لا تطبقان على العقود التي تبرم حصراً من خلال تبادل بريد إلكتروني أو من خلال اتصالات فردية متوازية.

المادة ١٣: إجراء طلبية

باستثناء الحالة التي يكون فيها الأطراف غير المعتبرين مستهلكين قد اتفقوا على العكس، تحرص الدول الأعضاء على أنه عند إجراء العميل طلبيته بوسائل إلكترونية، أن تطبق المبادئ التالية:

- يجب على مزود الخدمات أن يفيد باستلام طلبية العميل دون تأخير غير مبرر بوسائل إلكترونية.
- يكون الأطراف الموجّهة لهم الطلبية أو الإشعار بالاستلام، قد استلموها عندما يمكنهم أن يصلوا إليها بوسائل إلكترونية.

باستثناء الحالة التي يكون فيها الأطراف غير المعتبرين مستهلكين قد اتفقوا على العكس، تحرص الدول الأعضاء

على أن يضع مزود الخدمات بتصرف العميل وسائل تقنية ملائمة وفعالة وممكن الوصول إليها، تسمح له بتحديد الأخطاء المرتكبة في إدخال المعلومات وبتصحيحها وذلك قبل إجراء الطلبية.

إن الفقرتين ١ و٢ من هذه المادة لا تطبقان على العقود التي تبرم حصراً من خلال تبادل بريد إلكتروني أو من خلال اتصالات فردية متوازية.

المادة ١٤: تحديد الأسعار

تحرص الدول الأعضاء على أن تذكر الأسعار بطريقة واضحة وأن تحدد ما إذا كانت الضرائب ونفقات التسليم مشمولة بالسعر أم لا.

يجب أن تكون وسيلة الدفع المعتمدة آمنة وسهلة الاستعمال، وأن يُعلم المحترف المستهلك بالشروط المطبقة على وسيلة الدفع.

المادة ١٥: حق الرجوع

خلافاً لأي نص آخر، يحق للمستهلك العدول عن قراره بشراء سلعة أو استئجارها أو الاستفادة من الخدمة في خلال مهلة عشرة أيام[1] تسري اعتبارا من تاريخ العقد بالنسبة للخدمات ومن تاريخ التسليم بالنسبة للبضائع والسلع. يمكن للأطراف الاتفاق على مهلة معينة بإيراد بند خاص في العقد.

إلا أنه لا يحق للمستهلك ممارسة حق الرجوع في الحالات التالية:

١- إذا استفاد من الخدمة أو استعمل السلعة قبل انقضاء مهلة العشرة أيام أو المهلة المتفق عليها.
٢- إذا كان موضوع العقد بضائع أو سلع صُنعت بناءً لطلبه أو وفقاً لمواصفات عيّنها بنفسه.
٣- إذا كان موضوع العقد أشرطة أو أسطوانات أو أقراصاً مدمجة أو برامج معلوماتية، في حال تم إخراجها من العبوة أو إزالة غلافها للمرة الأولى.
٤- إذا كان موضوع العقد شراء الصحف والمجلات والمنشورات لاسيما الكتب.
٥- إذا ظهر عيب في السلعة من جراء سوء حيازتها أو حفظها أو استعمالها من قبل المستهلك.
٦- إذا اشتمل العقد على تقديم خدمات إيواء أو نقل أو إطعام أو لهو تقدّم في تاريخ معين أو بصورة دورية محددة.
٧- إذا كان موضوع العقد خدمة تحميل برامج عبر الإنترنت إلا إذا وجد عيب في البرنامج منع حصول التحميل ولم يكن للمستهلك أي دور في إحداث العيب.

عند ممارسة المستهلك حقه بالعدول، يتوجب على المحترف إعادة المبالغ التي قبضها من المستهلك إليه، على أن يتحمل الأول مصاريف التسليم.

المادة ١٦: الأعمال المتعلقة بعقد نقل البضائع

يمكن استخدام الرسالة الإلكترونية لتنظيم عقد نقل البضائع أو أي مستند يتعلق بفعل مرتبط به أو أي مستند يتم تنفيذاً له، بما في ذلك على سبيل المثال لا الحصر بيانات مواصفات البضاعة وأعدادها وكميتها أو علاماتها وإيصال البضائع وتأكيد تحميل البضاعة وإصدار التعليمات إلى الناقل والمطالبة بتسليم البضاعة والإذن بالإفراج عن البضائع والإخطار بوقوع هلاك أو تلف في البضاعة وجميع الإخطارات والإشعارات المتعلقة بالعقد أو بتنفيذه ومنح حقوق على البضاعة أو اكتسابها أو التنازل عنها أو نقلها والتعهد بتسليم البضاعة إلى شخص معين.

المادة ١٧: مسؤولية المحترف

يُسأل كل من يمارس التجارة الإلكترونية تجاه العميل عن حسن تنفيذ موجباته الناتجة عن العقد. ولا يمكن إعفاؤه من المسؤولية كلياً أو جزئياً إلا إذا أثبت أن عدم تنفيذ العقد أو سوء تنفيذه يعود للعميل أو للقوة القاهرة أو لفعل الغير.

الباب الرابع: أحكام ختامية

المادة ١٨: قواعد التصرف

تشجع الدول الأعضاء أن تقوم الهيئات أو المنظمات المهنية أو العائدة للشركات أو للمستهلكين بوضع قواعد للتصرف تهدف إلى حسن تطبيق أحكام هذا الإرشاد، وبتسهيل الوصول إلى هذه القواعد بالوسائل الإلكترونية.

تشجع الدول الأعضاء الهيئات والمنظمات التي تمثل المستهلكين على المشاركة في وضع وتطبيق قواعد التصرف المنوه عنها، والتي لها تأثير على مصالحهم.

المادة ١٩: الحل غير القضائي للنزاعات

تحرص الدول الأعضاء، في حال الخلاف بين مزود خدمات مجتمع المعلومات (الخدمات الإلكترونية) والعميل، ألا تمنع قوانينها استعمال وسائل بديلة لحل النزاعات أو تسوية الخلافات، وذلك من خلال وسائل إلكترونية ملائمة.

تشجع الدول الأعضاء الأجهزة غير القضائية لتسوية النِزاعات، ولاسيما في مسائل حماية المستهلك، على تأمين الضمانات الإجرائية الملائمة للأطراف المعنية.

المادة ٢٠: المراجعات القضائية

تحرص الدول الأعضاء على أن الإجراءات القضائية المتاحة في القانون الوطني، والمطبقة على خدمات مجتمع المعلومات (الخدمات الإلكترونية)، تسمح باتخاذ تدابير سريعة، لاسيما عبر أمر على عريضة، لوقف كل انتهاك وللوقاية من كل تعدٍّ جديد على المصالح المعنية.

المادة ٢١: التعاون بين الدول الأعضاء

تعتمد الدول الأعضاء وسائل للمراقبة وللتحقيق لازمة لتطبيق فعال للإرشاد الحالي وتسهر على أن يقدم لها مزودو الخدمات المعلومات المطلوبة.

تتعاون الدول الأعضاء لضمان تطبيق فعال لهذا الإرشاد، وتسمي فيما بينها أشخاصاً مفوضين للاتصال بهم.

المادة ٢٢: حماية المستهلك

تحرص الدول الأعضاء على ملاءمة قوانينها المتعلقة بحماية المستهلك مع القواعد المشار إليها في الإرشاد الحاضر في ما يتعلق بحماية المستهلك عند إجراء أي تعامل بينه وبين المحترف عن بعد او على شبكة الإنترنت.

المادة ٢٣: العقوبات

تحدد الدول الأعضاء نظام العقوبات المطبق على مخالفة أحكام هذا الإرشاد. يجب أن تكون العقوبات فعالة ورادعة ومتناسبة مع حجم ومدى المخالفة.

هوامش

١- مدة مقترحة وغير ملزمة

الإرشاد الرابع

معالجة وحماية البيانات ذات الطابع الشخصي

٤

الورقة البحثية الخلفية لإرشاد معالجة وحماية البيانات ذات الطابع الشخصي

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع البيانات ذات الطابع الشخصي وحمايتها في الدول العربية، ورصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية، وبالتالي تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بحماية البيانات الشخصية.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بمعالجة وحماية البيانات ذات الطابع الشخصي.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) الشروط العامة المطلوبة لقانونية معالجات البيانات ذات الطابع الشخصي: تتناول مبادئ متعلقة بنوعية البيانات ذات الطابع الشخصي ومواصفاتها، ومبادئ متعلقة بقانونية معالجة البيانات أي الحالات التي يُسمح فيها بمعالجة بيانات ذات طابع شخصي، وتحديد فئات خاصة من المعالجات، بالإضافة إلى الموجبات المفروضة على المسؤول عن المعالجة أو ممثله، وحق الشخص المعني بالاطلاع على خصائص المعالجة المتعلقة به وعلى البيانات المتعلقة به، وطلب تصحيح أو محو أو منع الدخول إلى البيانات المتعلقة به، كذلك حق الشخص المعني بالاعتراض على معالجة البيانات ذات الطابع الشخصي المتعلقة به وذلك لأسباب مشروعة مرجحة وكذلك لغايات الترويج التجاري، أو الاعتراض على نقل هذه البيانات للغير لغايات الترويج التجاري. ويتناول هذا الموضوع أيضاً موجبات المسؤول عن المعالجة لجهة سرية وأمان المعالجات ولجهة استعمال وسائل تقنية وتنظيمية ملائمة من أجل حماية البيانات ذات الطابع الشخصي من التدمير العرضي أو غير المشروع والتعديل والبث أو الوصول غير المشروع والمعالجة غير المشروعة، وموجبات المسؤول عن المعالجة بالتقدم أمام سلطة الرقابة الرسمية المختصة للحصول على التصريح والترخيص المسبق منها، وتحديد بيانات التصريح المطلوبة ونشر المعالجات في سجل خاص للمعالجات مفتوح للاطلاع من قبل كل شخص.

٢) سلطة الرقابة الرسمية المختصة: تتناول إنشاء سلطة رقابة رسمية للسهر على حماية البيانات الشخصية، وتلقي التصاريح حول معالجة البيانات الشخصية وإعطاء التراخيص لتنفيذ هذه المعالجات، وصلاحيات سلطة الرقابة التحقيقية مثل جمع المعلومات والوصول للبيانات وصلاحيتها التنفيذية لجهة فرض عقوبات إدارية كغرامات أو منع الدخول أو محو البيانات أو وقف المعالجة مؤقتاً أو نهائياً، واللجوء إلى القضاء لتدابير أكثر فعالية. كما أعطيت سلطة الرقابة، بغية ضمان تطبيق عملي فعال للقانون، صلاحية تلقي أية طلبات أو شكاوى من الأفراد ومتابعتها مع ضرورة الالتزام بحفظ السر المهني.

٣) المراجعات القضائية، المسؤوليات والعقوبات: تتناول الحق لكل شخص بمراجعة المحاكم المختصة في حال التعرض لأي من حقوقه المتعلقة بمعالجة البيانات ذات الطابع الشخصي، وذلك بالإضافة إلى المراجعة الإدارية المتاحة أمام سلطة الرقابة الرسمية المختصة، وبالإضافة أيضاً إلى الحق في الحصول على تعويض من جراء أي عمل غير مشروع أو خاطئ، والحالات التي يعفى فيها المسؤول عن المعالجة كلياً أو جزئياً، والتدابير المناسبة لضمان تنفيذ أحكام حماية البيانات الشخصية.

٤) نقل البيانات ذات الطابع الشخصي إلى دول أجنبية: تتناول شروط نقل البيانات إلى بلد أجنبي، والمعايير المفروضة لتقويم مستوى حماية معالجة البيانات الشخصية، شرط موافقة الشخص المعني على نقل البيانات الخاصة به، والضمانات المفروض أن يقدمها المسؤول عن المعالجة لجهة حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

٥) قواعد التصرف وأحكام ختامية: تتناول ضرورة ووضع واعتماد قواعد للتصرف تساهم في حسن تطبيق أحكام حماية البيانات ذات الطابع الشخصي، بالإضافة إلى تسوية المعالجات المنفذة والمهلة المحددة لها كي تصبح متوافقة مع أحكام الإرشاد الخاص بها.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981
http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

- Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Approved by the Committee of Ministers, in Strasbourg, on 15 June 1999.
http://conventions.coe.int/Treaty/EN/Treaties/Html/108-1.htm

- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Strasbourg,8.XI.2001
http://conventions.coe.int/Treaty/EN/Treaties/Html/181.htm

- European Parliament and Council Directive 95/46/EC 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 [Official Journal L 281 of 23.11.1995].

- Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R1882:EN:HTML

- Council Decision 92/242/EEC of 31 March 1992 in the field of information security.

- COUNCIL RESOLUTION of 15 July 1974 on a Community policy on data processing.

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.

- Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:en:NOT

- COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries
http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

- The Bucharest Declaration on Combating Counterfeiting and Piracy, 1*2 July 2006*.
http://www.ccapcongress.net/archives/Regional/Files/Bucharest%20Declaration.pdf

- Recommendation No (87) 15 adopted on 17 September 1987 concerning the regulating of the use of personal data in the police sector.

- United Nations Guidelines for the regulation of computerized personal data files, A/RES/45/95, adopted by the General Assembly on 14 December 1990.
http://ec.europa.eu/justice/policies/privacy/instruments/un_en.htm

- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
http://www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part1

٢) بعض قواعد التصرف، والمبادئ التوجيهية ونماذج عقود حول نقل البيانات الشخصية لبلد أجنبي:

- Personal Data Security Breach Code of Practice [Approved by the Data ProtectionCommissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003]
http://dataprotection.ie/viewdoc.asp?DocID=1082

- Guidance Note for Data Controllers on Purpose Limitation and Retention
http://www.dataprotection.ie/viewdoc.asp?DocID=859&ad=1

- GUIDANCE NOTE FOR DATA CONTROLLERS ON THE RELEASE OF PERSONAL DATA TO PUBLIC REPRESENTATIVES
http://www.dataprotection.ie/viewdoc.asp?DocID=550&m=f

- Data security guidance
http://www.dataprotection.ie/viewdoc.asp?DocID=1091&ad=1

- Model Contracts for the transfer of personal data to third countries
http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

٣) مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم معالجة البيانات الشخصية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الاسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول أسيا الوسطى.

٤) كما تم الاسترشاد بالمراجع الفقهية العالمية الخاصة بحماية البيانات الشخصية وأهمها:

- Maitrise et protection de l'information, rédigé par CLUSIF juin 2006
www.cnisf.org/biblioth_cnisf/librairie/maitrise_protection_info.pdf

- Élaboration d'une politique de protection de la vie privée et d'une déclaration s'y rattachant
http://www.oecd.org/document/1/0,3746,fr_2649_34255_28878569_1_1_1_1,00.html

- Générateur de l'OCDE de déclaration de protection de la vie privée
http://www.oecd.org/document/42/0,3746,fr_2649_34255_28879786_1_1_1_1,00.html

- The Commerce Department's Latest Privacy Initiative on Data Privacy Day
http://www.commerce.gov/blog/2011/01/28/commerce-department%E2%80%99s-latest-privacy-initiative-data-privacy-day

- NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE. Enhancing Online Choice, Efficiency, Security, and Privacy, The white house, April 2011
http://www.nist.gov/nstic/

- National Security Strategy "The White House May 2010, p 27 Web 17 Dec 2010
http://www whitehouse gov/sites/default/files/rss viewer/national security strategy pdf

- Cyber space policy Review- Assuring a Trusted and Resilient Information and Communications Infrastructure
http://www.nist.gov/nstic/

- Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers, Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada 2011
http://www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=220

- Circle of Care: Sharing Personal Health Information for Health-Care Purposes, by Ann Cavoukian, Ph.D. Commissioner, September 2009
http://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=885

- How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice, by Ann Cavoukian, Ph.D. Commissioner, May 2007
http://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=621

- Privacy Breach Protocol- Guidelines for Government Organizations, Dec 01, 2006
www.ipc.on.ca

- André Lucas, Jean Devèse, Jean Frayssinet: Droit de L'Informatique et de L'internet, Thémis, Droit privé

- Vincent Fauchoux, Pierre Deprez, et Jean- Michel Bruguière: Le droit de l'Internet : Lois, contrats et usages de (Broché - 22 janvier 2009).

- Vivant (M.): Droit de l'Informatique, Lamy, 1998.

- محاضرات الدكتور وسيم حرب – الدراسات العليا في القانون، كلية الحقوق-الجامعة اللبنانية، ١٩٩٥- ٢٠٠٥، مكتب المحاماة والاستشارات القانونية والتحكيم.

- الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني، ورقة مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة ٢-٤ يونيو٢٠٠٨م
http://www.shaimaaatalla.com/vb/showthread.php?t=3945&page=1

٥) وتناولت أعمال البحث أخيراً التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية القليلة والخاصة بحماية البيانات ذات الطابع الشخصي؛ ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شمولها النقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بحماية البيانات ذات الطابع الشخصي

تبين أثناء أعمال البحث أن هناك نقصاً لدى الدول العربية في إصدار تشريعات أو تنظيمات قانونية تتعلق بكيفية معالجة البيانات الشخصية وحمايتها، وأن هناك فقط دولة الإمارات العربية المتحدة التي أصدرت تشريعاً خاصاً بذلك وباللغة الانكليزية، بالإضافة إلى سلطنة عمان التي أفردت ضمن قانونها الخاص بالمعاملات الإلكترونية باباً خاصاً يتناول حماية البيانات الشخصية، هذا بالإضافة إلى الكويت التي أفردت الفصل التاسع من مشروع قانونها الخاص بالمعاملات الإلكترونية لمعالجة البيانات الشخصية.

التشريعات العربية المتعلقة بحماية البيانات الشخصية هي التالية:

١- الإمارات العربية المتحدة: قانون لحماية البيانات الشخصية رقمه ١ صدر عام ٢٠٠٧ خاص بالمركز المالي الدولي لدبي DIFC.
http://dp.difc.ae/legislation/dp_protection/

٢- سلطنة عمان: قانون رقم ٦٩ لسنة ٢٠٠٨ بشأن المعاملات الإلكترونية.
http://www.ita.gov.om/ITAPortal_AR/Businesses/Businesses_Projects.aspx?NID=97

٣- الكويت: مشروع قانون المعاملات الإلكترونية.

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالبيانات الشخصية، مثال:

- سوريا[1]، التي قامت بأعداد مشروع قانون حماية البيانات الشخصية
- اليمن التي أصدرت مشروع قانون قانون لسنة ٢٠٠٩ م بشأن المعلومات
http://www.justice-lawhome.com/vb//archive/index.php?t-9166.html

ب - شمولية التشريعات الوطنية الخاصة

كما ذكرنا أعلاه، نجد أن دولة الإمارات، دون سواها، هي التي أصدرت تشريعا لمعالجة موضوع حماية البيانات الشخصية، علماً بأن هذا القانون جاء خاصاً بمركز دبي المالي العالمي وصدر فقط باللغة الإنكليزية، وشاملاً جميع المواضيع التي حددها الإرشاد الخاص بحماية البيانات ذات الطابع الشخصي بما يتناسب مع وضع مركز دبي المالي العالمي، حيث جاء القانون متضمناً ٣٥ مادة قانونية تتناول القواعد والمبادئ المتعلقة بجمع ومعالجة وإفشاء واستخدام البيانات الشخصية في مركز دبي المالي العالمي، وحقوق الأفراد في ما يتصل بالبيانات الشخصية، وموجبات مراقبي معالجة البيانات وصلاحية مركز دبي المالي العالمي في مراقبة كل ما يتعلق بالمسائل المتصلة بمعالجة البيانات الشخصية، فضلا عن إدارة وتطبيق القانون.

أما فيما يتعلق بقانون المعاملات الإلكترونية الخاص بسلطنة عمان فقد تضمن في الفصل السابع منه المواد ٤٣ إلى ٥١ وتتناول هذه المواد: جمع البيانات الشخصية، وضمان سرّيتها، والإعلام بإجراءات حماية البيانات الشخصية، وتمكين صاحب البيانات من النفاذ إليها، وحظر إرسال وثائق إلكترونية مرفوضة، وعدم جواز معالجة البيانات الشخصية، وتحويل البيانات الشخصية إلى الخارج؛ إلا انه لم يتطرق إلى إنشاء سلطة الرقابة الرسمية المختصة بالسهر على حماية البيانات الشخصية، وإلى تلقي التصاريح وإعطاء التراخيص لمعالجة البيانات الشخصية، وصلاحيات سلطة الرقابة التحقيقية مثل جمع المعلومات والوصول للبيانات وصلاحيتها التنفيذية لجهة فرض عقوبات إدارية كغرامات أو منع الدخول أو محو البيانات أو وقف المعالجة مؤقتاً أو نهائياً.

كما وعمدت اليمن في مشروع قانونها بشأن المعلومات إلى تحديد مبادئ الحق في الحصول على المعلومات، وطلب الحصول على المعلومات، وشروطه وإجراءاته، ونشر المعلومات المتعلقة بأنشطة الهيئات التمثيلية والنيابية والقضائية والوزارات والأجهزة والمؤسسات والمصالح المركزية والمحلية ووحدات القطاع العام والمختلط ونتائج أدائها لواجباتها الدستورية والقانونية؛ وتكلفة الحصول على المعلومات؛ والاستثناءات على حق الحصول على المعلومات في حدود ما يجيزه القانون ولمن يمنحه القانون وعلى النحو المحدد في النظم والإجراءات المعتمدة لدى كل مصدر من مصادر الحصول على المعلومات؛ وإدارة المعلومات ومهام الهيئة المختصة بالإشراف والتوجيه ورسم وإقرار السياسات والخطط في مجال المعلومات ومتابعة تنفيذها ودور هذه الهيئة في وضع أسس ومعايير معالجة البيانات والمعلومات؛ بالإضافة إلى تبادل المعلومات بين كافة أجهزة الدولة ووحدات القطاع العام والمختلط والخاص والشركات الأجنبية العاملة داخل

الجمهورية؛ والمعايير الأساسية لأمنية المعلومات وحماية أنظمتها؛ حماية خصوصية الأفراد؛ بالإضافة إلى المسؤوليات والعقوبات المفروضة عند خرق هذه المبادئ والأصول. وقد غاب عن مشروع القانون هذا موضوع نقل البيانات الخاصة وتحويلها إلى خارج البلاد.

أما بالنسبة إلى الكويت فقد خصصت في مشروع قانونها الخاص بالمعاملات الإلكترونية الفصل السابع منه لتنظيم مسألة الخصوصية وحماية البيانات، حيث نصت المواد القانونية (٣٥ إلى ٤٠) على عدم الجواز للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أي بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة معلوماتها الإلكترونية المتعلقة بالشؤون الوظيفية أو بالسيرة الاجتماعية أو بالحالة الصحية أو بعناصر الذمة المالية للأشخاص أو غير ذلك من المعلومات الشخصية، باستثناء بعض الحالات ولاعتبارات تتعلق بالأمن القومي للبلاد؛ وعدم جواز جمع أو تسجيل أو تجهيز أي معلومات أو بيانات شخصية مشار إليها بأساليب أو طرق غير مشروعة أو بغير رضاء الشخص أو من ينوب عنه واستخدام هذه المعلومات أو البيانات الشخصية والمسجلة لديها بسجلاتها أو بأنظمة معلوماتها في غير الأغراض التي جمعت من أجلها، وواجبات الجهات الحكومية والهيئات الأخرى المشار إليها أعلاه باتخاذ التدابير المناسبة لحماية البيانات، وحق الأفراد أن يطلبوا محو أو تعديل أي مما تقدم من البيانات أو المعلومات الشخصية المتعلقة بهم والتي تختزنها في سجلاتها أو أنظمة معلوماتها إذا تبين عدم صحة هذه البيانات أو عدم تطابقها مع الواقع، وكذلك لاستبدالها وفقا لما طرأ عليها مع تعديل.

كذلك الأمر بالنسبة لسوريا، حيث عالجت ضمن مشروع قانونها الخاص بحماية البيانات الشخصية مسألة جمع البيانات الشخصية ومعالجتها واستخدامها وحمايتها، وحق الوصول إلى المعلومات ذات الطابع الشخصي والتصحيح؛ نقل البيانات الخاصة وتحويلها إلى خارج البلاد؛ والجمع أو المعالجة دون ترخيص أو دون التقيد بالأحكام القانونية؛ وإفشاء البيانات أو نقلها للخارج دون إذن مسبق؛ ورفض تصحيح البيانات.

هوامش

١ – تراجع لائحة تشريعات الدول الأجنبية

٢– راجع مشروع قانون حماية البيانات الشخصية السوري المنشور على الموقع الالكتروني:
http://www.dp-news.com/pages/detail.aspx?l=1&articleId=58379

مقدمة إرشاد معالجة وحماية البيانات ذات الطابع الشخصي

تشكل حقوق الإنسان وحرياته المرجع الرئيسي لحماية حرمة حياته الشخصية. وهي تبعاً لذلك السند الأساسي لشرنقة الحقوق المتصلة بهذه الحرمة.

تطوّر هذا المفهوم منذ القدم وبشكل دائم. وقد صدرت بعض النصوص والوثائق مثل الماغنا كارتا عام ١٢١٥[١] التي وضعت حدوداً للسلطات السياسية. وتلتها بعد ذلك "المواد الإثنتي عشرة" عام ١٥٢٥ في ألمانيا[٢]. إلى إعلان الجمعية الوطنية الفرنسية[٣] حول حقوق الإنسان عام ١٧٨٩ كوليدة الثورة الفرنسية. وبعدها بعامين صدرت شرعة الحقوق في الولايات المتحدة الأميركية عام ١٧٩١[٤]. أدخلت هذه النصوص إلى المجتمع والفرد فكرة أن الحقوق الإنسانية تعتبر واجبة الاحترام من الغير ويجب حمايتها قانوناً. فبعد أن كان الإنسان سلعة يباع ويشترى جسدياً (العبودية) بدون الالتفات حتى إلى كرامته وفكره. أصبح هو ورأيه وكرامته واحترامه موجباً له على الغير وعلى السلطات الرسمية.

مع هذا الاهتمام المتزايد بحقوق الإنسان أوردت شرعة حقوق الإنسان الصادرة عن الأمم المتحدة في العام ١٩٤٨ بعد الحرب العالمية الثانية وبسبب مآسي هذه الأخيرة. مجموعة من الحقوق التي وقعتها الدول المنضمّة إلى الأمم المتحدة وباتت تعتبر قاعدة عامة تقتدي الدول بها. وقد ورد فيها إعلان واضح عن الاعتراف النهائي بالحقوق الفردية للإنسان. لا سيما في المادة ١٢ من الإعلان التي حددت أن حق الشخص بعدم التعرض الاعتباطي لخصوصيته مصان. كما لا يجوز التعرض لكرامته.

أمام هذا الواقع. وبعد تطوّر مفهوم الحرية الشخصية في العالم الغربي أولاً حيث تقر المجتمعات بقيمة الحياة الشخصية وحرمتها كإحدى القيم التي لا يجوز التعرض لها والتي يجب صونها. توسع هذا المفهوم أكثر في جميع المجتمعات وإن بنسب متفاوتة. مثل العالم العربي أو الشرقي حيث ما تزال العائلة بمختلف قيمها ركيزة احترام الحقوق والحريات الشخصية.

لذا. وإزاء هذا التطوّر. تبيّن منذ منتصف القرن الماضي. لا سيما في أوروبا. أنّه مع تزايد استعمال أنظمة الحاسوب والحواسيب الكبيرة الفائقة السرعة التي يمكنها حفظ كمية هائلة من البيانات وتداولها بسرعة ليس فقط ضمن إطار دولة واحدة إنما على مستوى دول العالم قاطبة بما في ذلك البيانات الخاصة بالأفراد مثل الاسم. الأصل. العنوان. الآراء والمعتقدات. التفاصيل الطبية تبيّن للمشترع أن إمكانية الكشف والتقاطع والمعالجة والتحليل لهذه البيانات يعرض الخصوصية الفردية لآثار سلبية. ويمكن التعسف في استعمال هذه الأنظمة وإساءة استخدام البيانات ذات الطابع الشخصي.

أحاطت فرنسا أولاً بالموضوع ووضعت تشريعاً خاصاً حوله. فقد صدر بتاريخ ٦ كانون الثاني ١٩٧٨ القانون رقم ١٩٧٨/١٧ المتعلق بالمعلوماتية وبالملفات وبالحريات متضمناً المبادئ الأساسية في هذا الإطار: مبادئ جمع المعلومات. التصريح عن غايات المعالجة. صفات المعلومات. حق الشخص المعني في الاطلاع وطلب التصحيح. كما أنشأ القانون هيئة إدارية مستقلة مهمتها السهر على حسن تطبيق القانون.

وقد اعتمد قانون ١٩٧٨ نموذجاً لاتفاقية المجلس الأوروبي لعام ١٩٨١ ولمعظم القوانين الصادرة في الدول الأوروبية لاحقاً.

تتالت بعد ذلك النصوص الأوروبية الوطنية حول الموضوع في السويد والمملكة المتحدة وخلافهما. وتلك الخاصة بالإتحاد الأوروبي كالقرارات والمعاهدات والإرشادات[٥].

إضافة إلى ذلك. ومع تعاظم حجم التجارة الإلكترونية واتساعها. اتضحت أيضاً القيمة التجارية للبيانات ذات الطابع الشخصي. وقد تدخل البرلمان الأوروبي لتفادي إقرار تشريعات متناقضة بين الدول الأوروبية قد لا تعتمد نفس مستوى الحماية القانونية للبيانات ذات الطابع الشخصي. ما قد يعرقل نقل مثل هذه البيانات بين الدول الأوروبية ولاسيما في مجال التجارة الإلكترونية. وكذلك لتأكيد كون أنظمة معالجات البيانات ذات الطابع الشخصي هي في خدمة الإنسان الذي يجب أن تُحترم حرياته الأساسية وحقوقه. ولاسيما الحياة الخاصة. مع الأخذ بعين الاعتبار ضرورة المساهمة في التطور الاجتماعي والاقتصادي. لذلك عمد البرلمان الأوروبي بتاريخ ٢٤ تشرين الأول ١٩٩٥ إلى إصدار إرشاد للدول الأوروبية يتعلق بحماية الأشخاص الطبيعيين لجهة معالجة البيانات ذات الطابع الشخصي ولجهة حرية نقل هذه البيانات. إن هذا الإرشاد جاء متوافقاً مع السياسة الأوروبية حول حقوق الإنسان كما هي محددة في المعاهدة

الخاصة بحماية حقوق الإنسان والحريات الأساسية لعام ١٩٥٠[٦] وكذلك مع التوجيهات الصادرة عن منظمة التعاون الاقتصادي والتطور OECD عام ١٩٨٠[٧] الخاصة بحماية البيانات ذات الطابع الشخصي ونقلها عبر الحدود. وقد عمدت فرنسا إلى إدخال الإرشاد الأوروبي المنوه عنه في نظامها القانوني بموجب القانون رقم ١٩٧٨/١٧ تاريخ ٦ كانون الثاني ١٩٧٨ المعدَّل بموجب القانون رقم ٢٠٠٤/٨٠١ تاريخ ٦ آب ٢٠٠٤ .

صدرت عن الإتحاد الأوروبي إرشادات[٨] وقرارات لاحقة للإرشاد رقم EC/46/95 مبنية عليه، وتتعلق بمعالجة أو نقل البيانات ذات الطابع الشخصي عبر الوسائل التقنية و\أو الإلكترونية. من خلال مراجعة هذه النصوص الأحدث نسبياً من الإرشاد المذكور تبيّن أنها تستند إلى الإرشاد رقم EC/46/95 من ناحية المبادئ العامة، إلا أنها تختلف عنه من ناحية بعض النقاط التقنية أو العملية الخاصة بطرق المعالجة أو النقل الخاصة .

وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام ١٩٩٥، المتعلق بحماية الأشخاص الطبيعيين لجهة معالجة البيانات ذات الطابع الشخصي ولجهة حرية نقل هذه البيانات وإضافةً إلى النصوص اللاحقة التي تكاملت معه، لدى إعداد نص الإرشاد الحالي حول معالجة البيانات ذات الطابع الشخصي، وذلك بالنظر للتراث الأوروبي العريق والتجربة الناجحة في مجال حماية حقوق الإنسان والحريات العامة، وبالنظر أيضاً إلى الانسجام العام بين القوانين الأوروبية ومعظم الأنظمة القانونية العربية، وهي ذات مصدر لاتيني مشترك.

أضف إلى كون الإرشاد الأوروبي المذكور قد شكل الركيزة القانونية لجميع دول الإتحاد الأوروبي وحتى للدول غير الأوروبية، فقد صدر "مبدأ الميناء الآمن"[٩] وهو مجموعة مبادئ تُشكل قواعد تصرف على الشركات الأميركية التقيّد بها عند نقل المعلومات إليها من إحدى الدول الأوروبية عندما تكون هذه المعلومات ذات طابع شخصي. إن مبدأ الميناء الآمن قد تم وضعه للتكيّف مع قواعد الإرشاد الأوروبي رقم EC/46/95 وهو يتلخص بأن متلقي البيانات ذات الطابع الشخصي إذا كان خارج الاتحاد الأوروبي (أي خارج نطاق تطبيق الإرشاد EC/46/95) فيجب عليه أن يؤمن مستوى حماية للبيانات ذات الطابع الشخصي ملائماً للإرشاد المذكور[١٠].

إضافةً إلى ما سبق، فقد تمت مراجعة عدد كبير من قوانين الخصوصية وحماية البيانات من حول العالم، وقد اتجه الرأي إلى اعتماد النص الأقرب إلى الواقع العربي والأكثر ملائمة للدول التي تسعى إلى وضع تشريع جديد يتعلق بحماية البيانات ذات الطابع الشخصي. فالإرشاد الأوروبي رقم EC/46/95 يعتبر من النصوص الواضحة نسبياً والتي يمكن أن تكون سهلة التطبيق محلياً لجهة كون مواد الإرشاد المذكور قواعد عامة بدون تفاصيل إجرائية كبيرة.

تمت أيضاً مقارنة بعض القوانين العربية مع الإرشاد الأوروبي رقم EC/46/95 وبخاصة منها قانون مركز دبي العالمي المالي حول حماية البيانات الشخصية لعام ٢٠٠٧. وقد تبيّن أن أكثر مواد القانون المذكور متلائمة إلى حدٍ بعيد مع الإرشاد الأوروبي رقم EC/46/95، إلا أن مواد الأخير بقيت أشمل من القانون المذكور.

إن أغلب الأحكام القضائية الصادرة في أوروبا حول موضوع حماية البيانات الشخصية، قد صدرت في ظل قوانين متلائمة مع الإرشاد الأوروبي، مما يسمح للدول العربية الراغبة بإصدار تشريع متعلق بحماية البيانات ذات الطابع الشخصي بأن تراجع نص الإرشاد وتطبيقه عملياً عبر الاجتهاد ومما يتيح للمشرع العربي الإحاطة بكل جوانب أصل النص وتطبيقاته عملياً.

من خلال العودة إلى الدساتير العربية لا سيما تلك الخاصة بدول منطقة الإسكوا، تبيّن أن جميع الدساتير كفلت الحرية الشخصية للمواطنين، إلا أن أغلبها بقي صامتاً من ناحية الخصوصية والحياة الشخصية، باستثناء الدستورين المصري والقطري حيث ورد صراحة في المادة ٤٥ من الدستور المصري أن لحياة المواطنين الخاصة حرمة يحميها القانون. وكذلك ورد في المادة ٣٧ من الدستور القطري (الجديد نسبياً والعائد لعام ٢٠٠٣) أن لخصوصية الإنسان حرمتها، فلا يجوز تعرض أي شخص لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته أو أية تدخلات تمس شرفه أو سمعته، إلا وفقاً لأحكام القانون وبالكيفية المنصوص عليها فيه. يتبيّن من نص الدستور القطري أنه جاء متوافقاً مع مبدأ حماية الخصوصية وتنظيم إمكانية التعرض لها قانوناً، مما يعني إقراراً بالمبادئ التي جاء الإرشاد الأوروبي رقم EC/46/95 ينص عليها.

تقسيم الإطار الإرشادي لحماية البيانات ذات الطابع الشخصي وعناوينه

لقد تم تقسيم الإطار الإرشادي على سبعة أبواب تتناول مختلف الأوجه القانونية لمعالجة البيانات ذات الطابع الشخصي. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: سلطة الرقابة الرسمية المختصة.
الباب الثالث: الشروط العامة المطلوبة لقانونية معالجات البيانات ذات الطابع الشخصي.
الباب الرابع: المراجعات القضائية، المسؤوليات والعقوبات.
الباب الخامس: نقل البيانات ذات الطابع الشخصي إلى دول أجنبية.
الباب السادس: قواعد التصرف[11].
الباب السابع: أحكام ختامية.

يتضمن **الباب الأول** الأحكام العامة المتعلقة بالفلسفة الأساسية الكامنة وراء إصدار هذا الإرشاد، وهي أنه يهدف إلى حماية الحريات والحقوق الأساسية للأشخاص الطبيعيين[12]، لاسيما تلك المتعلقة بحياتهم الشخصية وخصوصيتها، في موضوع معالجة البيانات[13] ذات الطابع الشخصي. كما يتضمن في المادة ٢ منه تعريفاً لمختلف المصطلحات المعتمدة في الإرشاد. فالبيانات ذات الطابع الشخصي هي أي بيانات تتعلق بشخص معروف أو قابل للتعريف مباشرة أو غير مباشرة لا سيما عبر رقم تعريف أو غير ذلك من الميزات الشخصية والجسدية والعقلية والاقتصادية والثقافية أو الهوية الاجتماعية أو عبر البيانات المحفوظة لدى "المراقب". وهذا التعريف يشمل أي نوع من المعلومات يساهم في تحديد هوية الشخص، وبالتالي يشمل الأصوات والصور. إن شمول الأصوات والصور أصبح من الأهمية بمكان تبعاً للتطور التقني ولظهور الملفات الرقمية المتضمنة صوراً وأصواتاً. ويقتضي الإشارة إلى أن البيانات التي تُحذف عناصر التعريف الشخصية منها تصبح بالتالي خارجة عن مفهوم البيانات ذات الطابع الشخصي المذكورة آنفاً وتخرج من دائرة الحماية القانونية. كما تم تعريف معالجة بيانات ذات طابع شخصي بأنها عملية أو مجموعة عمليات منفذة على البيانات الشخصية بوسيلة آلية أو غيرها مثل الجمع، التسجيل، التنظيم، التيويم، التعديل، الاسترجاع، المعاينة، الحفظ، الكشف بواسطة النقل، الضبط، الإفشاء أو بشكل عام العرض علانية، الدمج، المحو، منع الوصول أو الإلغاء. وهذا التعريف هو واسع يشمل جميع العمليات الممكن إجراؤها على البيانات ذات الطابع الشخصي والتي من الممكن أن تتعرض للحياة الخاصة ولخصوصية الفرد. كذلك لم يتم التفريق بين المعالجات الممكننة أو الآلية والمعالجات اليدوية غير الممكننة تبعاً لكون الوظائف والأهداف هي نفسها وإن اختلف أسلوب المعالجة من الجهة التقنية. وقد تم تعريف نظام حفظ البيانات ذات الطابع الشخصي: مجموعة بيانات شخصية منظمة بشكل يمكن الوصول إليها بناءً لمعايير معينة سواء كانت متعلقة بالشخص أو بأية إشارة للشخص وتكون جاهزة للقراءة حتى لو لم تكن معالجة بواسطة جهاز يعمل بأوامر أعطيت له لهذه الغاية. ويقتضي التنبيه إلى أن الإرشاد الحالي لا يطبق إلا على بيانات ذات طابع شخصي مسجلة في ملفات ذات هيكلية معينة، ولاسيما بالنسبة للمعالجات الورقية، وذلك تبعاً للسهولة في استثمار البيانات وفي الوصول إليها. ولا يمتد الإرشاد الحالي إلى البيانات غير المعطاة هيكلية معينة. كذلك يعرّف الإرشاد مراقب البيانات الذي هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية وغاية معالجة البيانات. ويقتضي الإشارة إلى أنه عند نقل رسالة متضمّنة بيانات ذات طابع شخصي بواسطة خدمة اتصال أو بريد إلكتروني، فإن الشخص الذي صدرت عنه الرسالة، وليس ذلك الذي يؤمن خدمة الاتصال، هو من يُعتبر المسؤول عن المعالجة، والمقصود هو "المراقب". ويميز الإرشاد بين المراقب والمعالج، فالمعالج هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يقوم منفرداً أو بالاشتراك مع آخرين بمعالجة البيانات لصالح المراقب؛ أما الغير فهو كل من يرد ذكره في القانون ولا يكون مراقب البيانات او معالج البيانات (أو أحد موظفيه) أو متلقي البيانات أو الشخص موضوع البيانات. كذلك فالمُرسل إليه او متلقي البيانات ذات الطابع الشخصي فهو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يتلقى البيانات أو الذي يستحصل على إذن بالإطلاع عليها ، والمُرسل إليه يختلف عن الشخص المعني بالمعالجة وعن المراقب وعن المعالج وعن تابعي الأخيرين. ولا تعتبر بمثابة مُرسل إليه السلطات المخولة قانوناً طلب بيانات من المراقب.

كذلك تم تحديد تعريف الإذن الذي يعطيه الشخص موضوع البيانات بأنه كل نوع من أنواع التعبير الحرّ والواضح والمحدد الذي يبديه الشخص موضوع البيانات بعد تلقيه المعلومات ويسمح بمعالجة بياناته الشخصية. وأخيراً تم تعريف سلطة المراقبة وهي السلطة أو الهيئة المعيّنة من قبل الحكومة لمراقبة معالجة البيانات وصحة استعمالها.

تجدر الإشارة إلى أن التعريفات هذه هي غير ملزمة للدول التي ستضع او تعدل تشريعاً خاصاً بها لحماية البيانات ذات الطابع الشخصي، فقد تزيد عليها أو تنقص.

وقد استثنى الإرشاد من نطاق تطبيقه بعض المعالجات، وهي المعالجات المنفذة التي يكون موضوعها السلامة العامة أو الدفاع الوطني أو سلامة الدولة وكذلك نشاطات الدولة

المتعلقة بالقانون الجزائي، وأيضاً المعالجات المنفذة من قبل شخص طبيعي لممارسة نشاطات تكون حصرياً شخصية ولحاجات خاصة، كمعالجات المراسلات الخاصة ومسك دليل بالعناوين.

ينشىء **الباب الثاني** هيئة رقابة رسمية للسهر على حسن تطبيق أحكام هذا الإرشاد، إذ أنه لا يمكن ضمان فعالية أي قانون إلا من خلال الآلية التي ترافقه لضمان التطبيق. وهذه الآلية تشمل الجهاز المكلف بالتطبيق والعقوبات الرادعة. وقد أعطيت هيئة الرقابة بموجب المادة ٤ من الإرشاد صلاحيات كافية للتمكن من التطبيق الجيد والفعال للقانون. فصلاحيات هيئة الرقابة تتناول تلقي التصاريح حول معالجات البيانات ذات الطابع الشخصي وإعطاء التراخيص أيضاً لتنفيذ المعالجات وكذلك اقتراح النصوص القانونية والتنظيمية وإعطاء استشارات في هذا المجال. وتولي عناية خاصة لصلاحية هيئة الرقابة التحقيقية مثل جمع المعلومات والوصول للبيانات ولصلاحيتها التنفيذية لجهة فرض عقوبات إدارية كالغرامات أو منع الدخول أو محو البيانات أو وقف المعالجة مؤقتاً أو نهائياً... كذلك يعود لهيئة الرقابة عند فشل التدابير المتخذة من قبلها أو عدم ملاءمتها اللجوء إلى القضاء لتدابير أكثر فعالية. كما أعطيت هيئة الرقابة لضمان تطبيق عملي فعال للقانون، صلاحية تلقي أية طلبات أو شكاوى من الأفراد ومتابعتها. وتبعاً لخصوصية المعلومات التي من الممكن أن يطلع عليها موظفو هيئة الرقابة أثناء قيامهم بعملهم، فقد فرض الإرشاد عليهم ضرورة الالتزام بحفظ السر المهني.

يتضمن **الباب الثالث** الشروط العامة المطلوبة لقانونية معالجات البيانات ذات الطابع الشخصي، وقد نظّم هذه الشروط في عدة فصول.

الفصل الأول المعنون "مبادئ متعلقة بنوعية البيانات ذات الطابع الشخصي"[١٤] يفصل، في المادة ٥، مواصفات البيانات ذات الطابع الشخصي. فهذه يجب أن تكون مُعالجة بشكل أمين ومشروع وقد جمعت لغايات محددة واضحة ومشروعة ولا يمكن معالجتها بشكل مخالف لهذه الغايات إلا لأهداف تاريخية أو إحصائية أو علمية، كما يجب أن تكون ملائمة وغير مفرطة بالنظر لغايات المعالجة، وكذلك صحيحة ومحدثة، وأخيراً محفوظة بشكل يسمح بتحديد الأشخاص المعنيين لمدة لا تتجاوز تلك اللازمة لتحقيق غايات المعالجة. وتفرض الدول الأعضاء ضمانات ملائمة للبيانات التي تحفظ لمدة تفوق تلك المحددة آنفاً لغايات تاريخية أو إحصائية أو علمية. إن تحديد المواصفات المذكورة للبيانات ذات الطابع الشخصي يهدف إلى وضع ضوابط شفافة للمعالجة وإلى الحؤول دون التوسع في جمع البيانات لأغراض مختلفة، أو إساءة استعمال البيانات المجمعة وتفادي تحريفها أو عدم تطابقها مع الواقع مما قد يلحق الضرر بالشخص المعني.

ضمن الفصل الثاني المعنون "مبادئ متعلقة بقانونية معالجات البيانات"[١٥]، تحدد المادة ٦ الحالات التي يُسمح فيها بمعالجة بيانات ذات طابع شخصي، وذلك بغية عدم إباحة المعالجات بشكل مطلق، الأمر الذي قد يؤدي إلى سوء استخدامها. فالمعالجات مباحة في حال موافقة الشخص المعني أو في حالة تنفيذ عقد أو تدابير قبل التعاقد أو لاحترام التزام قانوني أو لصيانة مصلحة حيوية للشخص المعني أو لتنفيذ مهمة متعلقة بالمصلحة العامة أو تدخل ضمن ممارسة السلطة العامة من قبل المراقب أو من قبل الغير المُرسلة إليه البيانات أو لتحقيق المصلحة المشروعة للمسؤول عن المعالجة أو للغير المُرسلة إليه البيانات.

في الفصل الثالث المعنون "فئات خاصة من المعالجات"، تورد المادة ٧ معالجات البيانات ذات الطابع الشخصي المحظّرة بغية المحافظة على كرامة الإنسان وعدم استعمال المعالجات للتمييز بين الأشخاص على أسس تناقض المفاهيم الديمقراطية والمساواة وحقوق الإنسان. وتتضمن المعالجات المحظورة تلك التي تكشف الأصل العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، الانتماء النقابي، كذلك معالجة البيانات المتعلقة بصحة الإنسان وبحياته الجنسية. لكن المادة ٧ تعطي أيضاً استثناء على المحظورات بحيث يسمح بالمعالجات المحظورة في حال موافقة الشخص المعني أو في حال تنفيذ التزامات في نطاق قانون العمل أو للدفاع عن المصالح الحيوية للشخص المعني أو في ما خص أعضاء وأشخاصاً مرتبطين بمؤسسات لا تتوخى الربح ولغايات سياسية أو دينية أو نقابية وشرط عدم نقل البيانات إلى الغير دون موافقة الأشخاص المعنيين أو في حالة البيانات العلنية للجمهور أو الضرورية لإثبات حق أو ممارسته أو للدفاع عنه أمام القضاء أو حالة البيانات الضرورية لغايات الطب الوقائي، التشخيص الطبي، المعالجات الطبية والمنفذة من أشخاص متخصصين. ولمزيد من المرونة في النص، أجازت الفقرة الثانية من المادة ٧ للدول المتعاقدة، لغايات المصلحة العامة الهامة، اعتماد استثناءات إضافية على أحكام الفقرة الأولى من هذه المادة مع مراعاة الضمانات الملائمة، تبعاً لأثرها على الأمن العام والمصلحة العامة. أخضعت الفقرة الأخيرة من المادة ٧ المعالجات المتعلقة بالجرائم الجزائية وبتدابير الأمن وبالعقوبات الإدارية وبالأحكام المدنية لرقابة السلطة العامة. أما المادة ٨ فقد أتاحت إعفاءات من أحكام

هذا الإرشاد في ما خص المعالجات المنفذة لغايات الصحافة أو التعبير الأدبي أو الفني شرط احترام الحياة الخاصة، وذلك لعدم تقييد حرية الصحافة والإبداع الفني والأدبي.

في الفصل الرابع من الباب الثاني المعنون "التزامات المراقب بإعلام الشخص المعني"، تفرض المادتان ٩ و١٠ على المراقب أو ممثله تقديم معلومات معيّنة حول هويته وخصائص المعالجة وحقوق الشخص المعني، وذلك في حالتين: حالة تجميع المعلومات لدى الشخص المعني وحالة تجميع المعلومات عن الشخص المعني لدى الغير. وفي الحالة الثانية وتبعاً لغايات المعالجة الإحصائية أو البحثية، وتيسيراً على المراقب، يعفى الأخير من الالتزام المذكور إذا كان إعلام الشخص المعني مستحيلاً أو يتطلب جهوداً غير متناسبة أو إذا كانت التشريعات الوطنية تسمح بتسجيل البيانات أو بنقلها.

في الفصل الخامس من الباب الثاني المعنون "حق الشخص المعني بالإطلاع على البيانات وبطلب تصحيحها"، منحت المادة ١١ الشخص المعني الحق بالإطلاع على خصائص المعالجة وعلى البيانات المتعلقة به، وكذلك الحق بطلب تصحيح أو محو أو منع الدخول إلى البيانات المتعلقة به، موضوع المعالجة غير القانونية وفق هذا الإرشاد، لاسيما إذا كانت البيانات غير كاملة أو غير صحيحة، وأخيراً طلب إبلاغ الغير البيانات المصححة. هذان الحقان هما من الحقوق الأساسية الممنوحة للأشخاص لضمان عدم الإساءة للأشخاص بحفظ معلومات عنهم غير صحيحة ولتمكين الأشخاص من مراقبة احترام المراقب للأحكام القانونية.

في الفصل السادس من الباب الثاني المعنون "حق الشخص المعني بالاعتراض على المعالجة"، أعطت المادة ١٣ للشخص المعني الحق بالاعتراض على معالجة البيانات ذات الطابع الشخصي المتعلقة به وذلك لأسباب مشروعة مرجحة وكذلك لغايات الترويج التجاري، أو على نقل هذه البيانات للغير لغايات الترويج التجاري. هذا الحق بالاعتراض يكفل صيانة الحياة الخاصة للفرد وعدم انتهاكها وممارسة رقابة للفرد على مدى انطباق المعالجة على الأحكام القانونية. وفي هذا السياق الحمائي، أتاحت المادة ١٤ للشخص المعني عدم الخضوع لأي قرار يُنتج آثاراً قانونية تجاهه، يستند على معالجة ممكننة للبيانات بهدف تقييم بعض خصائص شخصيته، كإنتاجيته المهنية أو مصداقيته أو تصرفاته... إلا أن المادة ١٤ أوردت بعض الاستثناءات في حالة اتخاذ القرار في إطار إبرام عقد أو تنفيذه أو في حالة الإجازة بموجب نص قانوني وفي مطلق الأحوال تحت شرط حماية المصالح المشروعة للشخص المعني.

في الفصل السابع المعنون "التزامات المراقب لجهة سرية وأمان المعالجات"، تتناول المادة ١٤ سرية معالجات البيانات ذات الطابع الشخصي، إذ تنص على أن كل شخص يعمل تحت سلطة المراقب، وكذلك المعالج ، لا يستطيع معالجة بيانات ذات طابع شخصي دون أمر من المراقب إلا في حال وجود نص قانوني مخالف. وهذا الأمر طبيعي كون المراقب هو الذي يحدد غايات المعالجة وأساليبها ويتحمل المسؤولية عنها. أما المادة ١٥ فتتعرض لأمان المعالجات، والتزامات المراقب لجهة استعمال وسائل تقنية وتنظيمية ملائمة من أجل حماية البيانات ذات الطابع الشخصي من التدمير العرضي أو غير المشروع، والتعديل والبث أو الوصول غير المشروع والمعالجة غير المشروعة. كما تشترط المادة ١٥ تنظيم العلاقة بين المراقب والمعالج بعقد خطي يتضمن بنوداً معينة صريحة، وذلك منعاً لأي إشكال في العلاقة بينهما وما قد ينتج عن ذلك من تعرض لحقوق الأشخاص.

في الفصل الثامن المعنون "التصريح أمام سلطة الرقابة الرسمية المختصة والترخيص المسبق منها"، تفرض المادة ١٦ على المراقب التقدم بتصريح مسبق أمام سلطة الرقابة الرسمية قبل تنفيذ المعالجة، ولا يمكن اعتماد إجراءات مبسطة للتصريح أو الإعفاء من التصريح إلا في حال عدم إمكانية التعدي على حقوق الأشخاص المعنيين أو حرياتهم تبعاً لطبيعة البيانات المُعالجة، أو في حال مسك سجل مخصص لإعلام الجمهور ومفتوح لاستشارته أو لكل شخص له مصلحة مشروعة مبررة، أو في حالة المعالجات المتعلقة بأعضاء أو بأشخاص مرتبطين بمؤسسات لا تتوخى الربح ولغايات سياسية أو دينية أو نقابية وشرط عدم نقل البيانات إلى الغير دون موافقة الأشخاص المعنيين، أو أخيراً في حالة المعالجات غير الممكننة. إن اشتراط التصريح ضروري لتمكين سلطة الرقابة الرسمية من مراقبة تنفيذ أحكام هذا الإرشاد ومدى تقيد المراقب بها، ولاكتشاف أي تحوير في المعالجة يجري لاحقاً خلافاً لمضمون التصريح. وقد عالجت المادة ١٧ مضمون التصريح والمعلومات التي يجب أن يحتويها وهي: اسم المراقب وعنوانه وكذلك اسم ممثله وعنوانه، غايات المعالجة، وصف لفئات الأشخاص المعنيين وللبيانات أو لفئات البيانات، المُرسل إليهم البيانات أو فئاتهم، نقل البيانات المقرر لبلدان أجنبية، وصف عام لوسائل الأمان المطبقة على المعالجات. أما المادة ١٨، فنظّمت مسألة الترخيص المسبق، من قبل سلطة الرقابة الرسمية أو حتى من قبل السلطة الرسمية العليا، لبعض المعالجات التي تمثل أخطاراً فريدة على حقوق الأشخاص المعنيين وحرياتهم. وهذه تشكل أعلى درجات المعالجات خطورةً على حقوق الأشخاص وحرياتهم، لذلك تم إخضاعها لدراسة مسبقة لوضعيتها ولترخيص

مسبق يصدر عن سلطة الرقابة الرسمية وأحياناً عن سلطة دستورية أعلى، كمجلس الوزراء أو رئيس الجمهورية، إلا أن أعداد هذه المعالجات يجب أن تكون محدودة قدر الإمكان لعدم إعاقة الأعمال. وأخيراً تتناول المادة ١٩ نشر المعالجات ومسك سلطة الرقابة الرسمية سجلاً للمعالجات مفتوحاً للإطلاع من قبل كل شخص.

في الفصل التاسع المعنون "استثناءات وقيود على الحقوق والالتزامات"، ورعايةً لبعض المصالح العليا في المجتمع كصيانة المصلحة الاقتصادية للدولة وأمن الدولة والدفاع الوطني وملاحقة الجرائم الجزائية والمخالفات المهنية وحماية للحقوق، أجازت المادة ١٢ للدول الأعضاء اتخاذ تدابير تشريعية لتقييد الحقوق والالتزامات الملحوظة في سياق هذا الإرشاد، لاسيما حق الشخص المعني بالإطلاع على البيانات المتعلقة به وكذلك التزامات المراقب.

في **الباب الرابع** المعنون "المراجعات القضائية، المسؤوليات والعقوبات"، تعطي المادة ٢١ الحق لكل شخص بمراجعة المحاكم المختصة في حال التعرض لأي من حقوقه المتعلقة بمعالجة البيانات ذات الطابع الشخصي، وذلك بالإضافة إلى المراجعة الإدارية المتاحة أمام سلطة الرقابة الرسمية المختصة. وهذه المادة هي تأكيد للحق البديهي لكل شخص بالتظلم أمام القضاء حامي الحريات والحقوق، فبالإضافة إلى المراجعة الإدارية أمام السلطة الإدارية، أي سلطة الرقابة الرسمية، توجد المراجعة القضائية أمام المحكمة المختصة. أما المادة ٢٢، فتؤكد على مبدأ عام راسخ في القانون المدني، وهو الحق في الحصول على تعويض من جراء أي عمل غير مشروع أو خاطئ، وهو قد يكون هنا إجراء معالجة غير قانونية أو أي عمل غير منطبق على هذا الإرشاد. ويمكن إعفاء المراقب جزئياً أو كلياً من المسؤولية إذا أثبت أن الفعل المسبّب للضرر لا ينسب إليه، وهي الشروط التقليدية لموانع المسؤولية الراسخة في القانون المدني. وضماناً لفعالية تطبيق هذا الإرشاد ومنعاً لأية إمكانية للتهرب من أحكامه، فقد أوصت المادة ٢٣ الدول الأعضاء باتخاذ التدابير المناسبة لضمان تطبيق أحكام هذا الإرشاد وتحديد العقوبات الواجبة التطبيق في حال مخالفة هذه الأحكام. كما أعطت المادة ٢٣ أمثلة عن أفعال توجب التجريم، كمعالجة بيانات ذات طابع شخصي دون تقديم تصريح أو دون الحصول على ترخيص، أو معالجة بيانات ذات طابع شخصي دون التقيد بأحكام هذا الإرشاد، أو إفشاء بيانات ذات طابع شخصي، أو رفض الجواب على طلب الشخص المعني بالإطلاع أو بالتصحيح، أو عرقلة عمل سلطة الرقابة الرسمية.

في **الباب الخامس** المعنون "نقل البيانات ذات الطابع الشخصي إلى دول أجنبية"، تشترط المادة ٢٤ لنقل البيانات ذات الطابع الشخصي، موضوع المعالجة، إلى بلد أجنبي، تأمين مستوى ملائماً من الحماية القانونية. وقد وضعت المادة ٢٤ معايير معينة لتقويم مستوى الحماية، وهذه المعايير هي: الظروف المتعلقة بالنقل، طبيعة البيانات، غاية المعالجة ومدتها، بلد المنشأ وبلد الوجهة النهائية، القواعد القانونية المطبّقة، القواعد المهنية ووسائل الأمان. وتهدف هذه المادة إلى تأمين تناسق التشريعات بين الدول المختلفة لتفادي أية إعاقة لنقل البيانات بينها، مما قد ينعكس سلباً على المعاملات الإلكترونية والتجارة الإلكترونية. فقد تختلف مفاهيم الحماية القانونية بين الدول، وقد يعمد بعضها إلى منع نقل البيانات إلى دول أخرى لأن مستوى الحماية فيها منخفض وفق تقديرها. لإضفاء مزيد من المرونة على المادة ٢٤ ولاستيعاب الحالات التي لا تؤمن مستوى ملائماً من الحماية بالرغم من عدم تعرض حقوق الأفراد وحرياتهم للخطر، فقد لحظت المادة ٢٥ إمكانية نقل البيانات إلى دولة أجنبية لا تؤمن مستوى ملائماً من الحماية القانونية، شرط موافقة الشخص المعني، أو كون النقل ضرورياً لإبرام أو تنفيذ عقد في مصلحة الشخص المعني بين المراقب والغير، أو كون النقل ضرورياً للحفاظ على مصلحة عامة هامة أو لإثبات حق أو ممارسته أو الدفاع عنه أمام القضاء، أو كون النقل ضرورياً للحفاظ على مصلحة حيوية للشخص المعني، أو كون النقل يتم انطلاقاً من سجل عام مخصص قانوناً لإعلام الجمهور ومفتوح لاستشارته أو لأي شخص له مصلحة مشروعة مبررة. كذلك، يمكن للدول المتعاقدة أن ترخص بنقل بيانات ذات طابع شخصي إلى بلد لا يؤمن مستوى ملائماً من الحماية القانونية، وذلك عندما يقدم المراقب ضمانات كافية لجهة حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص. هذه الضمانات يمكن أن تنتج عن بنود تعاقدية ملائمة.

في **الباب السادس** المعنون "قواعد التصرف"، وزيادةً في توضيح أحكام هذا الإرشاد وتأمين حسن تطبيقه، توصي المادة ٢٦ الدول المتعاقدة بوضع قواعد للتصرف تساهم في التطبيق الجيد لقواعد هذا الإرشاد.

أخيراً، في **الباب السابع** المعنون "أحكام ختامية"، تتعرض المادة ٢٧ للمعالجات المنفذة قبل تاريخ نفاذ هذا الإرشاد وتتيح تسوية وضعها خلال فترة ثلاث سنوات من التاريخ المذكور، على أن تصبح هذه المعالجات متوافقة مع أحكام هذا الإرشاد.

هوامش

1 - Magna Carta: http://en.wikipedia.org/wiki/Magna_Carta

2- Twelve Articles : http://en.wikipedia.org/wiki/Twelve_Articles

3- Déclaration de Droits de L'Homme et du Citoyen http://en.wikipedia.org/wiki/Declaration_of_the_Rights_of_Man_and_of_the_Citizen

4- United States Bill of Rights : http://en.wikipedia.org/wiki/United_States_Bill_of_Rights

5- Directive 95/46/EC of the European Parliament and of 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.

- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

6- http://conventions.coe.int/treaty/fr/Treaties/Html/005.htm

7- Guidelines on the Protection of Privacy and Transborder flows of Personal data, 1980, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

8- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

- Directive 2002/58/EC of the European Parliament and of 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).

9- Safe Harbour principle: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles : US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.

Intended for organizations within the EU or US that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive.

The process was developed by the US Department of Commerce in consultation with EU.

١٠– وضع الإتحاد الأوروبي نماذج لبنود تعاقدية تتعلق بنقل البيانات ذات الطابع الشخصي عبر الحدود.
http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm

١١ – استعملت بعض الدول العربية عبارة قواعد السلوك.

12 - Guidelines for the regulation of computerized personal data files, A/RES/45/95, adopted by the General Assembly on 14 December 1990.

13 - Data means information which:
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_todata_protection.pdf

14- Directive 95/46/EC of the European Parliament and of 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, Section 1, Article 6.

15- The principal risk is the risk that individuals will suffer harm because personal information about them is:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who ought not to have it;
- used in unacceptable or unexpected ways beyond their control; or
- not kept securely.

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_dps_final.pdf

نص إرشاد معالجة البيانات ذات الطابع الشخصي

الباب الأول: أحكام عامة

المادة ١: موضوع الإرشاد

إن الدول الأعضاء تؤمن، وفق أحكام هذا الإرشاد، حماية الحريات والحقوق الأساسية للأشخاص الطبيعيين، لاسيما تلك المتعلقة بحياتهم الخاصة، وفي موضوع معالجة البيانات ذات الطابع الشخصي.

المادة ٢: تعريف المصطلحات

لأغراض هذا الإرشاد، تعتمد التعاريف التالية:

- **بيانات ذات طابع شخصي:** أية بيانات تتعلق بشخص معروف أو قابل للتعريف مباشرة أو غير مباشرة لا سيما عبر رقم تعريف أو غير ذلك من الميزات الشخصية، الجسدية، العقلية، الاقتصادية، الثقافية، أو الهوية الاجتماعية أو عبر البيانات المحفوظة لدى "المراقب".

- **معالجة بيانات ذات طابع شخصي:** عملية أو مجموعة عمليات منفذة على البيانات الشخصية بوسيلة آلية أو غيرها مثل الجمع، التسجيل، التنظيم، التيويم، التعديل، الاسترجاع، المعاينة، الحفظ، الكشف بواسطة النقل، الضبط، الإفشاء أو بشكل عام العرض علانية، الدمج، المحو، منع الوصول أو الإلغاء.

- **ملف بيانات ذات طابع شخصي:** مجموعة بيانات شخصية منظمة بشكل يمكن الوصول إليها بناءً لمعايير معينة سواء متعلقة بالشخص أو بأية إشارة للشخص وتكون جاهزة للقراءة حتى لو لم تكن معالجة بواسطة جهاز يعمل بأوامر أعطيت له لهذه الغاية.

- **مراقب البيانات:** هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يقوم منفرداً أو بالاشتراك مع آخرين بتحديد كيفية وغاية معالجة البيانات.

- **معالج البيانات:** هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يقوم منفرداً أو بالاشتراك مع آخرين بمعالجة البيانات لصالح المراقب.

- **الشخص موضوع البيانات:** هو الشخص الطبيعي الذي هو موضوع البيانات، أي الذي يتم تجميع ومعالجة بياناته ذات الطابع الشخصي.

- **الغير:** هو الشخص الطبيعي أو المعنوي، السلطة العامة أو الهيئة، الذي يختلف عن الشخص المعني بالمعالجة وعن المراقب وعن المعالج وعن التابعين للأخيرين.

- **متلقي البيانات أو المرسل إليه:** هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه، الذي يتلقى البيانات أو الذي يستحصل على إذن بالإطلاع عليها.

- **الموافقة/الإذن:** كل نوع من أنواع التعبير بإرادة حرة والواضح والمحدد الذي يبديه الشخص موضوع البيانات بعد تلقيه المعلومات ويسمح بمعالجة بياناته الشخصية.

المادة ٣: نطاق تطبيق الإرشاد

يطبق الإرشاد على معالجة البيانات ذات الطابع الشخصي، المكننة كلياً أو جزئياً، وكذلك على المعالجات اليدوية غير المكننة. يُستثنى من تطبيق هذا الإرشاد المعالجات التالية:

- المعالجات المنفذة التي يكون موضوعها السلامة العامة أو الدفاع الوطني أو سلامة الدولة وكذلك نشاطات الدولة المتعلقة بالقانون الجزائي.

- المعالجات المنفذة من قبل شخص طبيعي لممارسة نشاطات تكون حصرياً شخصية ولحاجات خاصة.

الباب الثاني: هيئة الرقابة الرسمية المختصة

المادة ٤: تُنشئ كل من الدول المتعاقدة هيئة رقابة رسمية

تكون وظيفتها مراقبة حسن تطبيق أحكام هذا الإرشاد. تمارس هذه الهيئة المهام الموكلة إليها بكل استقلالية.

يتم استشارة هيئة الرقابة عند تحضير تدابير تنظيمية أو إدارية متعلقة بحماية حقوق وحريات الأشخاص بخصوص معالجة البيانات ذات الطابع الشخصي. يكون لهيئة الرقابة الصلاحيات التالية:

- صلاحيات تلقي التصاريح عن معالجات البيانات ذات الطابع الشخصي وكذلك إعطاء التراخيص في هذا المجال.

- صلاحيات التحقيق، مثل حق الوصول إلى البيانات موضوع المعالجات وجمع المعلومات الضرورية لتحقيق مهمتها الرقابية.

- صلاحيات التدخل وفرض عقوبات إدارية، مثل إبداء الرأي مسبقاً في المعالجات ونشر هذه الآراء، ومثل إعطاء الأمر بمنع الوصول أو محو أو تدمير بيانات، ومثل منع إجراء معالجة بشكل مؤقت أو نهائي، ومثل توجيه تنبيه أو إنذار إلى مراقب المعالجة.

- صلاحية المثول أمام القضاء في حال مخالفة أحكام هذا الإرشاد أو صلاحية رفع هذه المخالفات إلى السلطة القضائية المختصة.

- صلاحيات استشارية لجهة اقتراح النصوص القانونية والتنظيمية في مجال معالجة البيانات ذات الطابع الشخصي.

- صلاحيات التعاون مع الهيئات الأجنبية المختصة في الدول الأخرى في مجال معالجة البيانات ذات الطابع الشخصي.

تقبل قرارات هيئة الرقابة الرسمية الطعن أمام المرجع القضائي المختص. يمكن لكل شخص أو لمؤسسة تمثله، تقديم طلب إلى هيئة الرقابة الرسمية، بخصوص حماية حقوقه وحرياته في مجال معالجة البيانات ذات الطابع الشخصي، وعلى سبيل المثال تقديم طلب للتحقق من مشروعية المعالجة.

تضع هيئة الرقابة ضمن فترات زمنية منتظمة تقارير حول نشاطاتها، وتنشرها.

يخضع موظفو وأعضاء هيئة الرقابة، حتى بعد انتهاء مهامهم، لالتزام الحفاظ على السر المهني لجهة المعلومات السرية التي اطلعوا عليها خلال أو بسبب عملهم ضمن الهيئة.

الباب الثالث: الشروط العامة المطلوبة لقانونية معالجات البيانات ذات الطابع الشخصي

الفصل الأول: مبادئ متعلقة بنوعية البيانات ذات الطابع الشخصي

المادة ٥: تعتمد الدول الأعضاء في قوانينها، أن البيانات ذات الطابع الشخصي يجب أن تكون:
- مُعالجة بشكل أمين ومشروع.
- قد جُمِعت لغايات محددة وواضحة ومشروعة ولا يمكن معالجتها بشكل مخالف لهذه الغايات. إن المعالجة اللاحقة لغايات تاريخية أو إحصائية أو علمية لا تعتبر مخالفة للغايات الأصلية للمعالجة مع مراعاة وجود ضمانات ملائمة.

- ملائمة وغير مفرطة بالنظر لغايات المعالجة.

- صحيحة ومحدثة، بحيث يجب اتخاذ كل التدابير لمحو أو تصحيح البيانات الخاطئة أو الناقصة، وذلك بالنظر لغايات المعالجة.

- محفوظة بشكل يسمح بتحديد الأشخاص المعنيين بها لمدة لا تتجاوز تلك اللازمة لتحقيق غايات المعالجة. وتفرض الدول الأعضاء ضمانات ملائمة للبيانات التي تُحفظ لمدة تفوق تلك المحددة آنفاً لغايات تاريخية أو إحصائية أو علمية.

- يجب على مراقب معالجة البيانات ذات الطابع الشخصي ضمان احترام الأحكام الواردة في هذه المادة.

الفصل الثاني: مبادئ متعلقة بقانونية معالجات البيانات

المادة ٦: لا يمكن معالجة البيانات ذات الطابع الشخصي إلا في الحالات التالية:
١- إذا أعطى الشخص المعني موافقته.
أو
٢ - إذا كانت المعالجة ضرورية لتنفيذ عقد يكون فيه الشخص المعني طرفاً أو لتنفيذ تدابير قبل التعاقد تتخذ بناء لطلب الأخير.
أو
٣- إذا كانت المعالجة ضرورية لاحترام التزام قانوني مُلقى على عاتق مراقب المعالجة.
أو
٤- إذا كانت المعالجة ضرورية لصيانة مصلحة حيوية للشخص المعني.
أو
٥- إذا كانت المعالجة ضرورية لتنفيذ مهمة متعلقة بالمصلحة العامة أو تدخل ضمن ممارسة السلطة العامة من قبل مراقب المعالجة أو من قبل الغير المُرسلة إليه البيانات.
أو
٦- إذا كانت المعالجة ضرورية لتحقيق المصلحة المشروعة لمراقب المعالجة أو للغير المُرسلة إليه البيانات.

الفصل الثالث: فئات خاصة من المعالجات

المادة ٧: معالجات تقع على فئات خاصة من البيانات

تحظر معالجات البيانات ذات الطابع الشخصي التي تكشف الأصل العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، الانتماء النقابي، كذلك معالجة البيانات المتعلقة بصحة الإنسان وبحياته الجنسية. لكن لا يُعمل بالحظر الوارد في هذه المادة في الحالات التالية:

١- إذا أعطى الشخص المعني موافقته الصريحة على المعالجة.

أو

٢- إذا كانت المعالجة ضرورية لإحترام الالتزامات والحقوق القانونية الخاصة لمراقب المعالجة في نطاق قانون العمل.

أو

٣- إذا كانت المعالجة ضرورية للدفاع عن المصالح الحيوية للشخص المعني.

أو

٤- إذا كانت المعالجة تنفذ في إطار النشاطات المشروعة لمؤسسات لا تتوخى الربح ولغايات سياسية أو دينية أو نقابية، شرط أن تنحصر المعالجة بأعضاء المؤسسة أو بأشخاص يرتبطون بها بعلاقات منتظمة متعلقة بغايات المؤسسة، وشرط أن لا تنقل البيانات إلى الغير دون موافقة الأشخاص المعنيين.

أو

٥- إذا كانت المعالجة تنصب على بيانات جعلت علنية للجمهور من قبل الشخص المعني أو كانت ضرورية لإثبات حق أو ممارسته أو للدفاع عنه أمام القضاء.

أو

٦- إذا كانت معالجة البيانات ضرورية لغايات الطب الوقائي، التشخيص الطبي، المعالجات الطبية وكانت المعالجة تُنفَّذ من قبل متخصص في الصحة أو أي شخص آخر خاضع قانوناً لالتزام الحفاظ على السر المهني.

يمكن للدول المتعاقدة، لغايات المصلحة العامة الهامة، اعتماد استثناءات إضافية على أحكام الفقرة الأولى من هذه المادة مع مراعاة الضمانات الملائمة.

إن المعالجات المتعلقة بالجرائم الجزائية أو بتدابير الأمن لا يمكن تنفيذها إلا تحت رقابة السلطة العامة. ويمكن للدول المتعاقدة أن تقر أن معالجة البيانات المتعلقة بالعقوبات الإدارية أو الأحكام المدنية تتم أيضاً تحت رقابة السلطة العامة.

المادة ٨: معالجة البيانات ذات الطابع الشخصي وحرية التعبير

تعتمد الدول المتعاقدة بالنسبة لمعالجات البيانات ذات الطابع الشخصي، المنفذة لغايات الصحافة أو التعبير الأدبي أو الفني، إعفاءات من التقيد بأحكام هذا الإرشاد شرط احترام الحياة الخاصة.

الفصل الرابع: التزامات مراقب المعالجة بإعلام الشخص المعني

المادة ٩: التزامات مراقب المعالجة عند تجميع المعلومات لدى الشخص المعني

يجب على مراقب المعالجة أو ممثله أن يقدم للشخص الذي يتم تجميع المعلومات عنه لديه المعلومات التالية:

١- هوية مراقب المعالجة وممثله.

٢- غايات المعالجة.

٣- المُرسل لهم البيانات أو فئاتهم.

٤- الطابع الاختياري أو الإجباري للإجابة على الأسئلة والنتائج التي قد تترتب على عدم الإجابة.

٥- وجود حق بالإطلاع على البيانات المتعلقة به وحق بطلب تصحيحها.

٦- معلومات إضافية حول: الأساس القانوني لعملية المعالجة التي تستهدفها البيانات، المدة الزمنية لتخزين المعلومات، حق اللجوء في أي وقت للمشرف عن معالجة البيانات.

المادة ١٠: التزامات مراقب المعالجة عند تجميع المعلومات عن الشخص المعني لدى الغير

في حال لم يتم تجميع المعلومات عن الشخص المعني لديه، يجب على مراقب المعالجة أو ممثله، منذ لحظة تسجيل البيانات أو لحظة نقل البيانات للغير، أن يقدم للشخص المعني المعلومات المنوه عنها في المادة السابقة بالإضافة إلى فئات البيانات المعنية.

يعفى مراقب المعالجة من الالتزام المذكور في هذه المادة إذا كانت المعالجة لغايات إحصائية أو البحث التاريخي أو العلمي، وكان إعلام الشخص المعني مستحيلاً أو يتطلب جهوداً غير متناسبة أو إذا كانت التشريعات الوطنية تسمح بتسجيل البيانات أو بنقلها.

الفصل الخامس: حق الشخص المعني بالإطلاع على البيانات وبطلب تصحيحها

المادة ١١: حق الإطلاع والتصحيح

يحق للشخص المعني أن يستحصل من مراقب المعالجة، ضمن فواصل زمنية معقولة ودون تأخير أو تكبد مصاريف

زائدة، على التالي:
- التأكد من أن المعلومات المتعلقة به قد تمت معالجتها أم لا، والحصول على معلومات حول غايات المعالجة وفئات البيانات والمُرسل لهم البيانات أو فئاتهم.
- أن تنقل إليه في شكل مفهوم البيانات المتعلقة به موضوع المعالجة، وكذلك كل معلومة حول أصل البيانات.
- تصحيح أو محو أو منع الدخول إلى البيانات المتعلقة به، والتي تكون موضوع معالجة غير قانونية وفق هذا الإرشاد، لاسيما إذا كانت البيانات غير كاملة أو غير صحيحة.
- إبلاغ الغير الذي نقلت إليه البيانات بكل تصحيح، محو أو منع دخول منفذ وفق الفقرة السابقة إذا كان هذا الأمر غير مستحيل أو لا يتطلب جهوداً غير متناسبة.

الفصل السادس: حق الشخص المعني بالاعتراض على المعالجة

المادة ١٢: الحق بالاعتراض
يحق للشخص المعني الاعتراض على:
١- معالجة البيانات ذات الطابع الشخصي المتعلقة به وذلك لأسباب مشروعة مرجحة، ما خلا وجود نص قانوني مخالف. وفي حال الاعتراض المعلّل، لا يمكن أن تتناول المعالجة البيانات المتعلقة بالشخص المُعترض.
٢- معالجة البيانات الشخصية المتعلقة به لغايات الترويج التجاري، أو نقل هذه البيانات للغير لغايات الترويج التجاري.

المادة ١٣: القرارات الفردية الآلية
يحق للشخص المعني أن لا يخضع لأي قرار يُنتج آثاراً قانونية تجاهه، ويستند على معالجة ممكننة للبيانات بهدف تقييم بعض خصائص شخصيته، كإنتاجيته المهنية أو مصداقيته أو تصرفاته. يمكن أن يخضع الشخص المعني للقرار المنوه عنه في هذه المادة في الحالات التالية:
١- إذا كان القرار متّخذاً في إطار إبرام عقد أو تنفيذه شرط تمكينه من إبداء رأيه لحماية مصالحه المشروعة.
٢- إذا كان القرار مجازاً بموجب قانون يحدد الوسائل التي تضمن حماية المصالح المشروعة للشخص المعني.

الفصل السابع: التزامات المراقب والمعالج لجهة سرية وأمان المعالجات

المادة ١٤: سرية المعالجات
على كل شخص يعمل تحت سلطة المراقب، وكذلك المعالج، أن يمتنع عن معالجة بيانات ذات طابع شخصي إلا بأمر من مراقب المعالجة ما خلا حالة وجود نص قانوني مخالف.

المادة ١٥: أمان المعالجات
يجب على مراقب المعالجة أن يستعمل وسائل تقنية وتنظيمية ملائمة من أجل حماية البيانات ذات الطابع الشخصي من التدمير العرضي أو غير المشروع والتعديل والبث أو الوصول غير المشروع والمعالجة غير المشروعة. يجب أن تؤمن هذه الوسائل، بالنظر لواقع الحال وللكلفة، مستوى أمان مناسباً لمواجهة مخاطر المعالجات وطبيعة المعلومات.

يجب على مراقب المعالجة أن يختار معالجاً يطبق ضمانات كافية بالنسبة لوسائل الأمان التقنية والتنظيمية المتعلقة بالمعالجات.

إن تنفيذ المعالجات بواسطة المعالج يجب أن ينظم بعقد خطي يتضمن التالي:

١- أن المعالج لا يتصرف إلا بأمر من المراقب.
٢- أن الالتزامات المنصوص عليها في الفقرة الأولى من هذه المادة تقع أيضاً على عاتق المعالج.

الفصل الثامن: التصريح أمام سلطة الرقابة الرسمية المختصة والترخيص المسبق منها

المادة ١٦: يجب على مراقب المعالجة أن يتقدم مسبقاً بتصريح أمام سلطة الرقابة الرسمية قبل مباشرة أي معالجة ممكننة كلياً أو جزئياً للبيانات ذات الطابع الشخصي .
توافق الدول الأعضاء ألا تعتمد إجراءات مبسّطة للتصريح أو أن تعفي من التصريح إلا في الحالات التالية:
١- عندما لا يمكن أن تشكل المعالجات، تبعاً لطبيعة البيانات المُعالجة، أي تعدٍ على حقوق الأشخاص المعنيين أو حرياتهم.
٢- عندما يكون موضوع المعالجة، بموجب نصوص قانونية، مسك سجل مخصص لإعلام الجمهور ومفتوح لاستشارته أو لكل شخص له مصلحة مشروعة مبررة.
٣- إذا كانت المعالجة تنفذ في إطار النشاطات المشروعة لمؤسسات لا تتوخى الربح ولغايات سياسية أو دينية أو نقابية شرط أن تنحصر المعالجة بأعضاء المؤسسة أو بأشخاص يرتبطون بها بعلاقات منتظمة متعلقة بغايات المؤسسة، وشرط أن لا تنقل البيانات إلى الغير دون موافقة الأشخاص المعنيين.
٤- إذا كانت معالجات البيانات ذات الطابع الشخصي غير ممكننة.

المادة ١٧: مضمون التصريح
يجب أن يتضمن التصريح المعلومات التالية:
١- اسم مراقب المعالجة وعنوانه وكذلك اسم ممثله وعنوانه.

٢- غايات المعالجة.
٣- مدة حفظ البيانات.
٤- وصف لفئات الأشخاص المعنيين وللبيانات أو لفئات البيانات.
٥- المُرسل إليهم البيانات أو فئاتهم.
٦- نقل البيانات المقرر لبلدان أجنبية.
٧- وصف عام لوسائل الأمان المطبقة على المعالجات.

تحدّد الدول المتعاقدة آليات التصريح أمام سلطة الرقابة الرسمية المختصة عن التعديلات على المعلومات المذكورة في هذه المادة.

المادة ١٨: الترخيص المسبق

تحدد الدول المتعاقدة معالجات البيانات ذات الطابع الشخصي التي تمثل أخطاراً فريدة على حقوق الأشخاص المعنيين وحرياتهم، وتفرض بالتالي أن تخضع هذه المعالجات لدراسة مسبقة وترخيص مسبق من قبل سلطة الرقابة الرسمية. ويمكن للدول المتعاقدة أن تشترط صدور ترخيص مسبق عن السلطة الرسمية العليا لتنفيذ أنواع معينة من معالجات البيانات ذات الطابع الشخصي.

المادة ١٩: نشر المعالجات

تأخذ الدول المتعاقدة التدابير اللازمة لضمان نشر المعالجات. تمسك سلطة الرقابة الرسمية سجلاً للمعالجات، يتضمن كحد أدنى المعلومات المذكورة في المادة ١٧ من هذا الإرشاد . يمكن الإطلاع على هذا السجل من قبل كل شخص.

بالنسبة للمعالجات غير الخاضعة للتصريح أو الترخيص المسبق، يجب على مراقب المعالجة أن يقدم المعلومات المنوه عنها في المادة ١٧ من هذا الإرشاد لكل شخص.

الفصل التاسع: استثناءات وقيود على الحقوق والالتزامات

المادة ٢٠: للدول الأعضاء اتخاذ تدابير تشريعية لتقييد الحقوق والالتزامات الملحوظة في سياق هذا الإرشاد عندما يكون ذلك ضرورياً من أجل:
١- صيانة أمن الدولة والدفاع الوطني.
٢- منع واستقصاء وملاحقة الجرائم الجزائية أو المخالفات المهنية بالنسبة للمهن المنظمة بقانون.
٣- مصلحة اقتصادية مهمة للدولة.
٤- مهمة مراقبة أو تحقيق أو تنظيم للسلطة العامة.
٥- حماية الشخص المعني أو حقوق الغير وحرياته.

الباب الرابع: المراجعات القضائية، المسؤوليات والعقوبات

المادة ٢١: المراجعات القضائية

بالإضافة إلى المراجعة الإدارية المتاحة أمام سلطة الرقابة الرسمية المختصة، يكون لكل شخص حق مراجعة المحاكم المختصة في حال التعرض لأي من حقوقه المتعلقة بمعالجة البيانات ذات الطابع الشخصي.

المادة ٢٢: المسؤوليات

لكل شخص تضرر من جراء معالجة غير قانونية أو من جراء أي عمل غير منطبق على هذا الإرشاد، الحق بالحصول على التعويض من مراقب المعالجة. يمكن إعفاء مراقب المعالجة جزئياً أو كلياً من المسؤولية إذا أثبت أن الفعل المسبّب للضرر لا ينسب إليه.

المادة ٢٣: الجرائم والعقوبات

تتخذ الدول الأعضاء التدابير المناسبة لضمان تطبيق أحكام هذا الإرشاد وتحدد العقوبات الواجبة التطبيق في حال مخالفة هذه الأحكام. يمكن للدول المتعاقدة تجريم الأفعال التالية:
١- معالجة بيانات ذات طابع شخصي دون تقديم تصريح أو دون الحصول على ترخيص.
٢- معالجة بيانات ذات طابع شخصي دون التقيد بأحكام هذا الإرشاد.
٣- إفشاء بيانات ذات طابع شخصي.
٤- رفض إجابة طلب الشخص المعني بالإطلاع أو بالتصحيح.
٥- عرقلة عمل سلطة الرقابة الرسمية.

الباب الخامس: نقل البيانات ذات الطابع الشخصي إلى دول أجنبية

المادة ٢٤: المبدأ

لا يمكن نقل البيانات ذات الطابع الشخصي، موضوع المعالجة، إلى بلد أجنبي إلا إذا أمّن هذا البلد مستوى ملائماً من الحماية القانونية.
يتم تقييم مستوى الحماية في البلد الأجنبي من خلال الظروف المتعلقة بالنقل، وعلى وجه الخصوص، يتم الأخذ بعين الاعتبار طبيعة البيانات، غاية المعالجة ومدتها، بلد المنشأ وبلد الوجهة النهائية، القواعد القانونية المطبّقة، القواعد المهنية ووسائل الأمان. عند نقل المعلومات بناء لطلب المرسل إليه، تقع مسؤولية شرعية النقل على المرسل إليه والمراقب معاً.

المادة ٢٥: الاستثناء

للدول المتعاقدة أن تلحظ أنه يمكن نقل البيانات إلى دولة أجنبية لا تؤمن مستوى ملائماً من الحماية القانونية، شرط:

- أن يعطي الشخص المعني موافقته على نقل البيانات المزمع.

أو

- أن يكون النقل ضرورياً لإبرام عقد بين الشخص المعني ومراقب المعالجة، أو لتطبيق تدابير سابقة للتعاقد بناء لطلب الشخص المعني.

- أن يكون النقل ضرورياً لإبرام أو تنفيذ عقد في مصلحة الشخص المعني، بين مراقب المعالجة والغير.

أو

- أن يكون النقل ضرورياً للحفاظ على مصلحة عامة هامة أو لإثبات حق أو ممارسته أو الدفاع عنه أمام القضاء.

أو

- أن يكون النقل ضرورياً للحفاظ على مصلحة حيوية للشخص المعني.

أو

- أن يتم النقل انطلاقاً من سجل عام مخصص قانوناً لإعلام الجمهور ومفتوح لاستشارته أو لأي شخص له مصلحة مشروعة مبررة.

يمكن للدول المتعاقدة أن ترخص بنقل بيانات ذات طابع شخصي إلى بلد لا يؤمن مستوى ملائماً من الحماية القانونية، وذلك عندما يقدم مراقب المعالجة ضمانات كافية لجهة حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص. هذه الضمانات يمكن أن تنتج عن بنود تعاقدية ملائمة.

الباب السادس: قواعد التصرف

المادة ٢٦: توصي الدول المتعاقدة بوضع قواعد للتصرف تساهم في التطبيق الفعّال لقواعد هذا الإرشاد.

الباب السابع: أحكام ختامية

المادة ٢٧: يتم تسوية وضع المعالجات المنفذة قبل تاريخ نفاذ هذا الإرشاد خلال فترة ثلاث سنوات من التاريخ المذكور، على أن تصبح هذه المعالجات متوافقة مع أحكام هذا الإرشاد.

الإرشاد الخامس

الجرائم السيبرانية

٥

الورقة البحثية الخلفية لإرشاد الجرائم السيبرانية

١- هدف البحث

تتناول الورقة الشرحية الخلفية لموضوع الجرائم السيبرانية في الدول العربية، رصد وتحليل التشريعات العربية التي عالجت هذا الموضوع ومقارنتها مع الاتفاقيات الدولية المرتبطة، لتسليط الضوء على الثغرات والنقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بالجرائم السيبرانية بشكل يتناسب مع التشريعات والتنظيمات الدولية.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالجرائم السيبرانية.

تناولت أعمال البحث بشكل رئيسي الجرائم التالية:

١) **جرائم التعدي على البيانات المعلوماتية:** شملت الجرائم التي يكون موضوعها البيانات المعلوماتية أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية وجرم اعتراض بيانات معلوماتية.

٢) **جرائم التعدي على الأنظمة المعلوماتية:** وتتناول جرائم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه وجرائم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل نظام معلوماتي.

٣) **إساءة استعمال الأجهزة أو البرامج المعلوماتية:** تتناول جرائم إساءة إستعمال الأجهزة أو البرامج المعلوماتية وجرائم كل من قدّم أو أنتج أو وزّع أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أية بيانات معلوماتية معدّة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً.

٤) **الجرائم على الأموال:** تشمل جرم الاحتيال أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية وجرم أعمال التسويق والترويج غير المرغوب فيها وجرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها وجرم الإطلاع على معلومات سرية أو حساسة أو إفشائها.

٥) **جرائم الاستغلال الجنسي للقاصرين:** وهي الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أية أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية. وتشمل أيضاً إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

٦) **جرائم التعدي على الملكية الفكرية للأعمال الرقمية:** تشمل الجرائم التالية: جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلّد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

٧) **جرائم البطاقات المصرفية والنقود الإلكترونية:** تشمل أعمال تقليد بطاقة مصرفية عن قصد بصورة غير مشروعة واستعمالها عن قصد، وتزوير نقود إلكترونية بصورة غير مشروعة وعن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

٨) **الجرائم التي تمسّ المعلومات الشخصية:** تشمل الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإفشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الإطلاع عليها.

٩) **جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:** وتشمل جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية

من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

١٠) جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية: تشمل جرم تملك وإدارة مشروع مقامرة على الإنترنت، وجرم تسهيل وتشجيع مشروع مقامرة على الإنترنت، وجرم ترويج الكحول للقاصرين على الإنترنت، وجرم ترويج المواد المخدرة على الإنترنت.

١١) جرائم المعلوماتية ضد الدولة والسلامة العامة: تشمل الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية.كما وتشمل جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والإطلاع أو الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية. بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو تخبئتها، والأعمال الإرهابية التي ترتكب باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية. وجرائم التحريض على القتل باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية.

١٢) جرائم تشفير المعلومات: تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة، وأفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، بالإضافة إلى بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Convention on Cybercrime, Budapest, 23.XI.2001

- Additional Protocol to the Convention on Cybercrime - Explanatory Report.

- Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (released 7 November 2002)

- European Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

- European Council Decision of 29 May 2000 to combat child pornography on the Internet, Official Journal L 138 , 09/06/2000 P. 0001 – 0004

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime

٢) وتناولت أعمال البحث أيضاً مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم التجارة الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الاسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول أسيا الوسطى.

٣) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية والعربية الخاصة بالجرائم السيبرانية:

- Fraud in the Internet, by Computer Crime Research Center, April 11, 2005
http://www.crime-research.org/articles/Internet_fraud_0405/

- Cybercriminals Reinvent Methods of Malicious Attacks, by Trend Micro Incorporated, July 11, 2008,
http://www.crime-research.org/analytics/3451/

- Cyber-crimes - Analytical data compiled, by Vladimir Golubev, published on Computer Crime Research Center,
http://www.crime-research.org/analytics/cyber_crimes0108/

- Crime on The Net,
http://rogerdarlington.me.uk/crimeonthenet.html#Hacking

- What is Cyber-terrorism, by Serge Krasavin Ph.D. MBAv, published by Computer crime research center (CCRC)
http://www.crime-research.org/library/Cyber-terrorism.htm

- How Computer Viruses Work, by Marshall Brain
http://computer.howstuffworks.com/virus2.htm

- How Hackers Work, Microsoft,
http://technet.microsoft.com/en-us/library/cc505928.aspx

- Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, John Draper, January 2010.
http://www.terrorism.com/content/cybershock-

- Cyber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth", Dhanashree Nagre Priyanka Warade http://www.contrib.andrew.cmu.edu/~dnagre/Final_Report_dnagre_pwarade.pdf

- Tracking a Computer Hacker, by *Daniel A. Morris*, Assistant United States Attorney Computer and Telecommunications Coordinator, District of Nebraska; published on 2005. http://www.cybercrime.gov/usamay2001_2.htm

- Internet Blocking: Crimes Should Be Punished and Not Hidden, by *Joe McNamee* - EUROPEAN DIGITAL RIGHTS (EDRI), June 2010. http://www.soros.org/initiatives/information/focus/policy/articles_publications/publications/edri-blocking-100606/EDRI-blocking-100606.pdf

- Data Breaches: What the Underground World of "Carding" Reveals, by *Kimberly Kiefer Peretti*- U.S. Department of Justice-Computer Crime and Intellectual Property Section. http://www.cybercrime.gov/DataBreachesArticle.pdf

- IT security and crime prevention methods, Published by *Interpol*, http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp

- Financial and high-tech crimes, http://www.interpol.int/Public/FinancialCrime/Default.asp

- The Globalization of Crime a Transnational Organized Crime Threat Assesment, UNODC, 2010, page 203- 209 http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

- الإطار التشريعي لجرائم المعلوماتية والإنترنت، الدكتور نضال الشاعر، مؤتمر "جرائم المعلوماتية والإنترنت – نظرة على دول الشرق الأوسط- شباط ٢٠٠٦ http://www.ijma3.org/Admin/Additionals/Cybercrime/Judge%20Nidal%20El%20Chaer%20Presentation.pdf

- جرائم الحاسوب الاقتصادية، دراسة نظرية وتطبيقية، دكتور نائلة عادل محمد فريد قورة، جامعة حلوان، مصر.

- مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، تأليف د. ناصر بن محمد البقمي، سنة ٢٠٠٩.

- الجرائم المعلوماتية، ماهيتها وصورها، تأليف الدكتور محمود صالح العادلي أستاذ القانون الجنائي، ورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة surviving-hackers-phreakers-identity-thieves-internet-terrorists-and-weapons-mass

- Prosecuting Computer Crimes Manual, published February, 2007. http://www.justice.gov/criminal/cybercrime/ccmanual/index.html

- Fighting cyber terrorism, by Carol Ko, June 17, 2008, Source: Computerworld.com.my http://www.crime-research.org/news/17.06.2008/3416/

- Organized crime: from trafficking to terrorism, By Frank Shanty http://books.google.com.lb

- Intellectual Property crimes: are proceeds from counterfeited goods funding terrorism? Hearing before the committee on International relations House of Representatives, July 16, 2003, Serial No. 108–48 http://www.foreignaffairs.house.gov/archives/108/88392.pdf

- Prosecuting Intellectual Property Crimes manual, Third Edition September 2006, CCIPS Criminal Division http://www.justice.gov/criminal/cybercrime/ipmanual/index.html

- COMPUTER-RELATED OFFENCES. A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France. http://www.cybercrimelaw.net/documents/Strasbourg.pdf

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime and final Report of the European Committee on Crime Problems. http://www.oas.org/juridico/english/89-9&final%20Report.pdf

- Cyber Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker1; 1 in 5 will become a Victim2; http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01

- Internet Gambling: Overview of federal criminal law; http://books.google.com.lb/

- The Myth of Cyberterrorism: There are many ways terrorists can kill you-computers aren't one of them. Joshua Green, The Washington Quartlerly Online http://www.washingtonmonthly.com/features/2001/0211.green.html

الجرائم الإلكترونية" مسقط ٢-٤ ابريل ٢٠٠٦م.
www.ituarabic.org/coe/2006/E-Crime/.../Doc2-Text-ar.DOC

- الجرائم الإلكترونية تشكل تحديات أمام القانون.ونظام المكافحة في المملكة حماية للاقتصاد الوطني. تأليف عبدالله عبد العزيز العجلان. صحيفة الرياض.
http://www.alriyadh.com/2008/02/29/article321790.html

- التحديات القانونية في الجرائم الإلكترونية. تأليف سمية بنت عبد الرحمن بن سليمان الحمدا.
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-forensic-and-computer-crimes/1075-legal-challenges-in-cyber-crime.html

٤) وتم الاسترشاد أيضاً بالدراسات التي أعدتها منظمة الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق. ٢- وضع التشريعات السيبرانية في سلطنة عمان ، دولة الإمارات العربية المتحدة ، دولة قطر. ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٥) بالإضافة إلى ذلك تناولت أعمال البحث مراكز مكافحة الجرائم السيبرانية، وأبرزها:

- Computer Crime & Intellectual Property Section United States Department of Justice
http://www.justice.gov/criminal/cybercrime/reporting.htm

- Internet Crime Complaint Center (IC3)
http://www.ic3.gov/default.aspx

- Department of Defence-United States of America Cyber Crime Center,
http://www.dc3.mil/

- Computer Crime Task Forces – USA,
http://www.ccmostwanted.com/CP/LEccuUS.htm

- Computer Crime Task Forces – Global,
http://www.ccmostwanted.com/CP/LEccuGL.htm

- موقع مكتب مكافحة غسيل الأموال التابع لوزارة التجارة والصناعة في الكويت
http://www.mlcoo.org

٦) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى انه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بمكافحة الجرائم السيبرانية، ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شموليتها للنقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بالجرائم السيبرانية

تبين أثناء أعمال البحث أن هناك أربع دول عربية فقط عملت على إصدار تنظيم الجرائم السيبرانية ضمن تشريعات خاصة بها وهي السعودية، والإمارات العربية المتحدة والأردن والسودان. أما الأردن فقد أصدر قانوناً مؤقتاً لسنة ٢٠١٠ لمكافحة جرائم أنظمة المعلومات[١]. تتناول هذه التشريعات تحديد الأفعال الجرمية المرتكبة عبر شبكة الإنترنت والتي تعتبر جرائم معلوماتية كما تناولت العقوبات المقررة لكل منها وذلك لتحقيق الأهداف التالية: تحقيق الأمن المعلوماتي، حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، حماية المصلحة العامة، والآداب والأخلاق العامة، وحماية الاقتصاد الوطني.

وهذه التشريعات المتعلقة بالجرائم السيبرانية هي التالية:

الأردن:
قانون جرائم أنظمة المعلومات لسنة ٢٠١٠
http://www.watnnews.net/NewsDetails.aspx?NewsID=12801

الإمارات العربية المتحدة:
القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات
http://www.theuaelaw.com/vb/showthread.php?t=1022

السودان:
قانون رقم ١٤ لسنة ٢٠٠٧

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالجرائم المعلوماتية، مثال:

سوريا، التي قامت بإعداد مشروع قانون مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية السوري[٣].

وقد عمدت بعض الدول العربية مثال سلطنة عمان إلى تعديل قانونها الجزائي ليشمل أحكاماً تتعلق بجرائم الحاسوب، وأصدرت دول أخرى قرارات أو مراسيم من شأنها مكافحة بعض جرائم المعلوماتية مثال لبنان، وهناك دول أخرى قامت بتشكيل هيئات مختصة لمكافحة جرائم الحاسوب:

سلطنة عمان:
مرسوم سلطاني رقم ٢٠٠١/٢٧، تعديل بعض أحكام قانون الجزاء العماني ، إضافة المادة ٢٧٦ مكرر حول جرائم الحاسوب
http://www.oman-net.net/vb/t443.html

الكويت:
مشروع قانون لمكافحة جرائم شبكة الإنترنت وتقنية المعلومات، أعدته النيابة العامة الكويتية[٤].

لبنان:
- تعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥، حماية برامج المعلوماتية ومكافحة القرصنة.
- قرار رقم ٧٨١٨ تاريخ ٢٠٠١/٨/٥ نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال.

مصر:
قرار وزاري رقم ٣٢٧ لسنة ٢٠٠٥، إنشاء إدارة متخصصة لمكافحة جرائم الحاسبات والشبكات بوزارة الداخلية تسمى "إدارة مباحث مكافحة جرائم الحاسبات الإنترنت".

السعودية:
نظام مكافحة جرائم المعلوماتية
http://www.mcit.gov.sa/arabic/Regulations/CriminalLaws/

اليمن:
مشروع قانون لمكافحة الجرائم الإلكترونية[٥].

إلا أننا نلاحظ أن معظم التشريعات الصادرة في الدول العربية والمتعلقة بالمعاملات والتواقيع الإلكترونية والتجارة الإلكترونية وحماية المستهلك نصت على مواد تحدد الجرائم المعلوماتية التي ترتكب في معرض ممارسة المعاملات أو التجارة الإلكترونية ومواد تتضمن العقوبات المترتبة عليها، وهي:

الأردن:
القانون الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الإلكترونية.

البحرين:
مرسوم قانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية.

سوريا:
قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الالكتروني وخدمات الشبكة.

سلطنة عمان:
مرسوم سلطاني رقم ٢٠٠٨/٦٩ بإصدار قانون المعاملات الإلكترونية.

فلسطين:
مشروع قانون المبادلات والتجارة الإلكترونية.

مصر: قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الالكتروني.

الكويت:
مشروع قانون المعاملات الإلكترونية.

السعودية:
نظام التعاملات الإلكترونية.

اليمن:
قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

من ناحية أخرى، نفيد ضمن هذا المجال أن جامعة الدول العربية قد قامت بتبني قانون الإمارات العربية المتحدة الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وهذا القانون تناول تحديد جرائم المعلوماتية وتحديد العقوبات عند ارتكاب هذه الجرائم، من حبس وفرض غرامات وإبعاد الأجنبي المخالف.

ب - شمولية التشريعات الوطنية الخاصة

كما ذكرنا أعلاه، نجد أن السعودية والإمارات العربية المتحدة والأردن والسودان فقط، قد أصدرتا تشريعات خاصة بمكافحة جرائم تقنية المعلومات في منطقة الإسكوا، حيث اكتفت الدول العربية الأخرى بتجريم الأفعال غير المشروعة التي

ترتكب أثناء القيام بالمعاملات والتجارة الإلكترونية وفرض العقوبات المترتبة عليها فقط. لذا نجد أن هذه العقوبات غير شاملة لجميع الجرائم المعلوماتية. وعلى سبيل المثال، إنّ جرائم تشفير المعلومات وجرائم الاستغلال الجنسي للقاصرين عبر الإنترنت أو جرائم ترويج المخدرات عبر الانترنت بقيت غير منظمة ضمن مواد قانونية خاصة وبالتالي لا يجرم مرتكبوها ولا يعاقبون في حال تم ارتكابها عملاً بالمبدأ الساري "لا عقوبة بدون نص".

أما التشريعات الخاصة بمكافحة جرائم المعلوماتية الصادرة عن السعودية والإمارات العربية المتحدة، فهي تتناول مواد عقابية حول الدخول غير المشروع إلى المواقع الإلكترونية والأنظمة المعلوماتية المملوكة من الغير، وانتهاك المعتقدات الدينية أو الحياة الخاصة، والدخول غير المشروع واللعب بالبيانات الشخصية، والتنصت أو التقاط أو اعتراض الرسائل الإلكترونية، والتهديد والابتزاز عبر الوسائط الإلكترونية، وجرائم البطاقات المصرفية والتحاويل والنقود الإلكترونية. وتناولت أيضاً الجرائم الماسة بالنظام العام والآداب العامة، وجرائم الاتجار بالجنس البشري وجرائم الإرهاب وجرائم غسل الأموال والمخدرات، بالإضافة إلى أنها شملت أيضاً الجرائم الماسة بالملكية الفكرية عبر شبكة الإنترنت.

وقد تصل العقوبات المترتبة على جرائم المعلوماتية إلى حد السجن لفترة خمس سنوات بالإضافة إلى فرض الغرامات وإبعاد الأجنبي عن البلد الذي ارتكبت فيه الجريمة.

وقد شمل قانون الجزاء العماني، بعد تعديله وإضافة المادة ٢٧٦ (مكرر) عليه، تحديد الجرائم التي تعتبر جرائم معلوماتية، فكان أن شملت المواد القانونية المذكورة أعلاه معظم جرائم المعلوماتية، إلا أنها لم تتطرق إلى جرائم التشفير وجرائم الاستغلال الجنسي للقاصرين عبر الانترنت، وجرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية، وجرائم المعلوماتية ضد الدولة والسلامة العامة. وقد نصّت هذه المادة على الآتي: "يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين....كل من تعمد استخدام الحاسوب في ارتكاب احد الأفعال التالية: ١- الالتقاط غير المشروع للمعلومات أو البيانات، ٢- الدخول غير المشروع على أنظمة الحاسوب، ٣- التجسس والتنصت على البيانات والمعلومات، ٤- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بإسرارهم، ٥- تزوير بيانات أو وثائق مبرمجة أياً كان شكلها، ٦- إتلاف وتغيير ومحو البيانات والمعلومات، ٧- جمع المعلومات والبيانات وإعادة استخدامها، ٨- تسريب المعلومات والبيانات، ٩- التعدي على برامج الحاسوب سواء بالتعديل أو الاصطناع، ١٠- نشر واستخدام برامج الحاسوب بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية".

ونصت المادة ٢٧٦ (مكرر ٣) على انه " يعاقب بالسجن مدة لا تزيد على ٥ سنوات وبغرامة لا تتجاوز ألف ريال كل من: ١- قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب، ٢- استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك، ٣- قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك". كما جاء في المادة ٢٧٦ (مكرر ٤) على انه " يعاقب بالسجن مدة لا تزيد على ٣ سنوات وبغرامة لا تتجاوز خمسمائة ريال كل من: ١- استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له، ٢- استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك، ٣- استعمل بطاقة الغير بدون علمه".

أما تعميم مصرف لبنان القاضي بحماية برامج المعلوماتية ومكافحة القرصنة فينص على "أن الحماية القانونية لبرامج الحاسوب مهما كانت لغاتها، بما في ذلك الأعمال التحضيرية، تخضع للتشريعات المتعلقة بحماية الملكية الفكرية في لبنان، لاسيما قانون الملكية الأدبية والفنية رقم ١٩٩٩/٧٥." بالإضافة إلى **نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال** القاضي بتجريم غسيل الأموال عبر التحاويل الإلكترونية.

إلا أننا نجد أن المشرع العربي قد حدد بعض الجرائم المعلوماتية وفرض على مرتكبيها العقوبات في تشريعات متفرقة كالتشريعات الخاصة بالمعاملات والتجارة الإلكترونية، والاتصالات وحقوق المؤلف والملكية الفكرية، وقانون العقوبات. فقد ورد مثلاً، في المرسوم بقانون رقم (٥) لسنة ١٩٩٩م بشأن حقوق الملكية الفكرية في الكويت، تحديد المخالفات المرتبطة مباشرة ببرامج الحاسوب والتي يمكن أن تنطبق على كل من برامج الحاسوب وقواعد البيانات، وأي إنتاج مرتبط بتقنية المعلومات. ونص التشريع ذاته على أن يعاقب بالحبس مدة لا تزيد على سنة واحدة وبغرامة لا تزيد عل خمسمائة دينار أو بإحدى هاتين العقوبتين: ١- كل من كشف أو سهّل كشف برامج الحاسوب قبل نشرها، ٢- كل من ساعد في إزالة حماية تنظيم أو تقييد إطلاع الجمهور على المصنف أو الأداء أو البث أو التسجيل. كذلك الأمر بالنسبة إلى سلطنة عمان حيث جرّم المشرع العماني من القانون رقم ٦٥ لسنة ٢٠٠٨ بشأن حماية حق المؤلف والحقوق المجاورة في المادة ٥٢ بيع وتداول البرامج الحاسوبية دون إذن صاحبها سواء تم ذلك بالطرق التقليدية أو بالطرق المستحدثة كاستخدام شبكة الإنترنت وفرض

عقوبة السجن سنتين كحدٍ أقصى فضلاً عن غرامة مالية لا تزيد عن عشرة آلاف ريال.

هوامش

١ – راجع لائحة تشريعات الدول الأجنبية – ملحق رقم ٣.

٢– راجع القانون المؤقت لمكافحة جرائم أنظمة المعلومات
http://www.watnnews.net/NewsDetails.aspx?NewsID=12801

٣– راجع مشروع قانون مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية السوري المنشور على الموقع الالكتروني:
http://www.dp-news.com/pages/detail.aspx?l=1&articleId=58379

٤– راجع مشروع قانون لمكافحة جرائم شبكة الإنترنت وتقنية المعلومات:
http://www.kwtfuture.com/vb/t8495.html

٥– راجع مشروع قانون لمكافحة الجرائم الإلكترونية
http://sh22y.com/vb/t10623.html

مقدمة إرشاد الجرائم السيبرانية

أسهم التطور التقني المتلاحق في أجهزة وأنظمة وشبكات الحاسوب[1] والإمكانية المتاحة لأي فرد في أن يمتلك ويستعمل جهاز حاسوب أو هاتف محمول في المنزل أو في المقهى أو أي مكان عام إلى تغيير كبير في ارتكاب الفعل الإجرامي[2] وفي ابتداع أساليب جديدة لارتكاب الجرائم السيبرانية وتبعاً لذلك تطور المفهوم الجرمي[3]، حيث لم يعد المجرم بحاجة إلى أدوات إجرامية وأساليب غير تقليدية، بل يكفي أن يكون الشخص ملماً باستعمال الحاسوب وأنظمته لكي يقوم بارتكاب جريمة من جرائم الفضاء السيبراني، سواء كانت الوسائل المعلوماتية أداة الجريمة أو كانت ضحية الفعل الجرمي. ومثال ذلك التعدي على حقوق المؤلف عبر تحميل أغاني أو أفلام مجاناً عن شبكة الإنترنت أو مشاهدة وإرسال أفلام إباحية تشمل الأطفال أو من هم دون السن القانونية بواسطة البريد الالكتروني الخ.. أو وضع برنامج خبيث[4] يمكن من خلاله خرق شبكة حواسب أو تدمير نظام حمائي أو اختراق جهاز آخر.

يعتمد المبدأ العام في القانون الجزائي في مختلف التشريعات والأنظمة القانونية على عدم التوسع في تطبيق و تفسير القواعد الجزائية وذلك لأن هذه القواعد تنص على عقوبات وتدابير إكراهية تنال من حرية الشخص أو ماله أو حقه بالتمتع بحقوقه. لهذا السبب لا يسوغ التوسع في تفسير هذه القواعد عبر القياس أو التحليل الخاص بالقاضي إذ من شأن ذلك الخروج عن مبدأ: لا عقوبة ولا جريمة بدون نص، وبسبب عدم جواز تشويه الإرادة الفعلية للمشترع عند وضعه نص القانون الجزائي إذ من خلال التوسع في التفسير قد تجرم أفعال لم يقصد المشترع، المعبّر عن إرادة المجتمع، تجريمها أو لا تعتبر أفعال أخرى جريمة تستوجب العقوبة المنصوص عنها في نص القانون الذي جرى تفسيره ليطابق جريمة الحاسوب أو الفضاء السيبراني. إلا انه مع ذلك ثمة أنظمة قانونية تستخدم في صياغتها لوصف الفعل الجرمي عبارات قد تفتح المجال لتوسّع نسبي في التفسير، ومن قبيل ذلك استعمال عبارة آلي في نص من قانون العقوبات باللغة العربية مما يسمح بان تشمل الأدوات المعلوماتية كونها تعتبر من الأدوات الآلية أيضاً.

ومن جهة أخرى، يقوم قانون الجزاء أو العقوبات على ركيزتين أساسيتين هما التجريم (وصف فعل على أنه جرم) والعقاب، إذ أن إعطاء وصف جرمي لفعل ما وفرض عقوبات عليه يخضع عادةً لاعتبارات ثقافية واجتماعية وضرورات اقتصادية خاصة بالدولة. فما يعتبر جرماً يمس الآداب العامة في الوطن العربي قد يعتبر تعبيراً عن الرأي في أوروبا، طبعاً مع الأخذ بعين الاعتبار أن العولمة أوجبت على المشترع اعتماد تعاريف ووصف لبعض الجرائم متلائمة مع القوانين العالمية الأمر الذي يجعل المشرع العربي ملزماً باعتماد الوصف الذي أعطاه المشرع الدولي لهذه الجرائم. فقد تتجه إرادة الناس في بعض المجتمعات إلى تشديد العقوبة على الجرائم التي تتناول مقدسات دينية أو أعمالاً لها علاقة بالعمليات المصرفية، بينما لا نرى مثل هذا التوجه في مجتمعات أخرى.

تنقسم جريمة الحاسوب أو جريمة الفضاء السيبراني[5] إلى نوعين أساسيين: النوع الأول هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة، كجرائم الاختلاس وانتحال الصفة والأفعال الإباحية. وهي جرائم عادية والحاسوب هو مجرد الوسيلة التي سمحت بارتكابها. والنوع الثاني هو الذي يكون فيه جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعاً للجريمة، أي أن الفعل الجرمي ارتكب على هذا الجهاز، مثل اختراق نظام أمان أو إرسال برنامج خبيث أو التعدي على اسم موقع على الإنترنت مما يشكل جرماً يطال حقاً من حقوق الملكية الفكرية.

لقد أصبحت البرامج والأدوات المعلوماتية تُستخدم كوسائل فعّالة لارتكاب الجرائم العادية، فهذه الجرائم لم يتغير مفهومها أو عناصرها الجرمية، كالاحتيال أو الاختلاس أو السرقة أو التخريب أو القدح أو التهديد. إنما أصبحت طرق تنفيذها تجري بوسائل معلوماتية بدل الوسائل التقليدية الشائعة، كأن يتم التهديد عبر رسالة بريد إلكتروني أو يتم الاختلاس عبر التلاعب في النظام المعلوماتي الذي يخزّن تفاصيل عمليات حسابات الزبائن. وقد يكون الضرر وحجم الجريمة عند استخدام وسائل معلوماتية أكبر بكثير من الحالات المعروفة سابقاً. كما يمكن أن تكون الوسائل المعلوماتية، كالبرامج والبيانات المعلوماتية، هي موضوع الجرائم ذاتها، كالتعدي على الأنظمة والبيانات المعلوماتية أو تعديل ومحو هذه البيانات أو اعتراضها. وهذه الطائفة من الجرائم هي جرائم استجدّت بظهور المعلوماتية[6]، ولم تكن معروفة قبل ذلك. وقد أسهم نمو التجارة الإلكترونية والتعاملات الإلكترونية وشيوعها بين أوساط العامة في ازدياد حالات حصول هذه الطائفة الجديدة من الجرائم[7]. وقد وجدت المحاكم صعوبة في تكييف النصوص القانونية العامة الواردة في قانون العقوبات لتجريم الأفعال التي موضوعها أدوات

المعلوماتية. فالنص الجزائي يُفسّر على سبيل الحصر، عملاً بقاعدة "لا جريمة ولا عقوبة بدون نص". وكان لا بد بالتالي من إقرار قوانين جديدة تجرّم الأفعال الواقعة على الأنظمة والبيانات المعلوماتية باعتبارها جرائم حديثة[٨]، وكذلك توسّع نطاق المفاهيم الراسخة للجرائم التقليدية لتشمل حالات استخدام المعلوماتية كوسيلة لتنفيذ الجرائم.

وبفعل الشبكات المعلوماتية وتخطيها للحدود الجغرافية، كشبكة الإنترنت التي لا تخضع لسيادة أي دولة وبالتالي لسيادة أي قانون صادر عن مشترع وطني معيّن، تجاوزت الجرائم المعلوماتية النطاق الوطني، فظهرت مثلاً العصابات التي تتلاعب بالبطاقات المصرفية على الصعيد الدولي وتنقل نشاطها من دولة إلى أخرى حتى لا تنكشف، وظهر المحتالون على شبكة الإنترنت ينتحلون شخصيات معينة عبر سرقة عناصر التعريف العائدة لأشخاص آخرين، وذلك للاستيلاء على الأموال بصورة غير مشروعة.

يتفاقم يوماً بعد يوم وضع جريمة الفضاء السيبراني، حيث بالإضافة إلى الجرائم التي ترتكب فردياً، أصبحت الجريمة السيبرانية منظمة[٩] إلى درجة أنها باتت تعتبر أحد أساليب الحرب الجديدة[١٠] وإحدى وسائل الهجوم الإرهابي[١١] مما دفع وزارة الدفاع الأميركية إلى إصدار بيان اعتبرت فيه أن على الحكومة الأميركية أن تتخذ الإجراءات الكفيلة برد أي اعتداء على أنظمة الحاسوب في إطار اي حرب أو نزاع مستقبلي.

لذلك، وبناءً على الوضع التشريعي القائم، كان من اللازم إيجاد حلول للثغرات في التشريعات السيبرانية لملاحقة الجريمة السيبرانية المتخطية للحدود الوطنية بغية تفعيل مكافحتها، ولتأمين انسجام التشريعات الوطنية معها حتى لا يفلت المجرم من العقاب بعد ارتكاب فعله وينتقل إلى بلد آخر. وبغية اتباع سياسة جنائية مشتركة، وتعزيز التعاون بين الدول، حاولت الجهات الدولية وضع تشريعات نموذجية في هذا المجال. ونذكر خصوصاً اتفاقية بودابست المتعلقة بالجريمة الإلكترونية تاريخ ٢٠٠١/١١/٢٣ والصادرة عن مجلس أوروبا، والتي تشكل نموذجاً جدياً يمكن الاسترشاد به عند إعداد التشريعات الوطنية في هذا المجال. وقد تم الاسترشاد باتفاقية بودابست المتعلقة بالجريمة الإلكترونية وبالقانون الفرنسي رقم ٢٠٠٤/٥٧٥ الصادر بتاريخ ٢٠٠٤/٦/٢١ وبقوانين وطنية مختلفة وبالأعمال الفقهية، في إعداد نصوص الإرشاد الحالي الموجه إلى الدول العربية حول جرائم المعلوماتية والفضاء السيبراني.

لقد تم تقسيم القانون الاسترشادي المُقترح على ثلاثة عشر باباً، تتناول مختلف الجرائم المعلوماتية والعقوبات العائدة لها. وهذه الأبواب هي:

الباب الأول: جرائم التعدي على البيانات المعلوماتية.
الباب الثاني: جرائم التعدي على الأنظمة المعلوماتية.
الباب الثالث: إساءة استعمال الأجهزة أو البرامج المعلوماتية.
الباب الرابع: الجرائم على الأموال.
الباب الخامس: جرائم الاستغلال الجنسي للقاصرين.
الباب السادس: جرائم التعدي على الملكية الفكرية للأعمال الرقمية.
الباب السابع: جرائم البطاقات المصرفية والنقود الإلكترونية.
الباب الثامن: الجرائم التي تمسّ المعلومات الشخصية.
الباب التاسع: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية.
الباب العاشر: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية.
الباب الحادي عشر: جرائم المعلوماتية ضد الدولة والسلامة العامة.
الباب الثاني عشر: جرائم تشفير المعلومات.
الباب الثالث عشر: العقوبات.

شروحات حول الإرشاد المتعلق بالجرائم السيبرانية

يتضمن **الباب الأول** المعنون "جرائم التعدي على البيانات المعلوماتية" الجرائم التي يكون موضوعها البيانات المعلوماتية[١٢] أي التي تقع على بيانات معلوماتية. وهي جرم التعرض للبيانات المعلوماتية وجرم اعتراض بيانات معلوماتية. تُعاقب المادة ١ كل من أقدم قصداً بصورة غير مشروعة على تعديل أو إلغاء أو محو أو إفساد أو تدمير البيانات الرقمية. يجوز اشتراط أن الفعل المذكور يجب أن يؤدي إلى إلحاق ضرر لتحقق الجرم . إن الفعل يجب أن يكون قصدياً لتمييزه عن أي فعل عرضي أي عن حصول تعديل البيانات المعلوماتية أو محوها عرضاً. كما أن الفعل يشمل كل أنواع التعرض والتغيير في البيانات المعلوماتية، سواء تم كلياً أم جزئياً. إن التجريم لا يرتبط بوقوع أضرار جسيمة بحق المجني عليه، لكن يمكن إضافة هذا الشرط على شروط التجريم. كما تُعاقب المادة ٢ كل من أقدم قصداً بصورة غير مشروعة على اعتراض بيانات معلوماتية بوسائل تقنية وذلك عند نقلها غير المُتاح للجمهور من أو إلى أو داخل نظام معلوماتي. ويجوز اشتراط أن يتم الفعل بنية جرمية أو بنية الربط مع أنظمة معلوماتية أخرى. إن اعتراض بيانات معلوماتية يعني التقاطها بوسائل تقنية معلوماتية وليس مادية، سواء تم استعمالها فيما بعد أم لا. فمثلاً إن الاستيلاء على الحاسوب الذي خزّنت عليه البيانات المعلوماتية لا يدخل ضمن نطاق هذا الجرم. كما يفترض هذا الفعل أن تكون البيانات المعلوماتية غير مفتوحة لاطلاع الجمهور، أي أن نقلها عبر الشبكات المعلوماتية أو الأنظمة المعلوماتية هو محمي ولا يمكن الدخول إلى هذه البيانات إلا من قبل الأشخاص المفوضين.

يشتمل **الباب الثاني** المعنون "جرائم التعدي على الأنظمة المعلوماتية[١٣]" على جرم الولوج غير المشروع إلى نظام معلوماتي، أو المكوث فيه، وجرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية، وجرم إعاقة عمل نظام معلوماتي[١٤]. تُعاقب المادة ٣ كل من أقدم قصداً على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه. ويجوز اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحماية الجارية على النظام المعلوماتي وبنية الحصول على بيانات رقمية، أو بنيّة أخرى جرمية أو بنيّة جرمية تتعلق بالربط مع أنظمة معلوماتية أخرى. إن مفهوم الولوج إلى نظام معلوماتي يعني الدخول إلى النظام واختراقه[١٥] والوصول إلى ما يحتويه وإمكانية الاطلاع على هذا المحتوى. يُشترط أن يكون الولوج غير مشروع أي أنه قد تم من قبل شخص غير مخول بالولوج، أو من قبلَ شخص مخول ولكن خلافاً للصلاحيات الممنوحة له أو خارج الأوقات المُتاحة له. كما يعني المكوث غير المشروع في نظام معلوماتي، أن الشخص بعد دخوله المشروع إلى النظام قد بقي فيه بعد انتهاء الوقت المخصص له. ويعتبر الفعل جرمياً ولو كان النظام المعلوماتي غير محمي، أو لم يكن القصد الاطلاع على محتوى النظام المعلوماتي من بيانات معلوماتية، إلا أنه يمكن إضافة شرط كون النظام محمياً من ضمن عناصر الجرم أو أن قصد الدخول هو الاطلاع على بيانات معلوماتية. تضيف المادة ٤ كشرط للتجريم قيام الفاعل بتعديل البيانات الرقمية أو البرامج أو إلغائها أو محوها أو إفسادها أو تدميرها أو المساس بعمل النظام المعلوماتي وذلك بعد دخوله غير المشروع إلى النظام المعلوماتي. وبطبيعة الحال، تكون العقوبة المقررة في هذه الحالة للجريمة أشد لكون الضرر هو فعلي وجسيم. في نهاية هذا الباب، تُعاقب المادة ٥ كل من أقدم بنية الغش، وبأي وسيلة، على إعاقة عمل نظام معلوماتي أو على إفساده. إن إعاقة عمل نظام معلوماتي أو إفساده تعني تعطيل وظائف النظام كلياً أو جزئياً، كعدم تمكنه من إتمام عملياته بشكل كلي أو بشكل جزئي أو التأخر في إتمام هذه العمليات أو إتمام العمليات مع الحصول على نتائج خاطئة. ويمكن تصور الحالات الجرمية التالية: تلقيم فيروس لتخريب النظام المعلوماتي[١٦]، وإغراق النظام المعلوماتي بالأوامر أكثر من طاقته، محو البيانات المعلوماتية. تفترض المادة نيّة الغش لدى الفاعل، وبالتالي تُستبعد الحالات العرضية التي تحصل بطريق الخطأ غير المقصود.

يعالج **الباب الثالث** المعنون "إساءة استعمال الأجهزة[١٧] أو البرامج المعلوماتية" جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية. فالمادة ٦ تطال كل من قدّم أو أنتج أو وزّع أو استورد أو صدر أو روّج أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلوماتية معّدة أو كلمات سر أو تراميز دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً. تشترط هذه المادة وجود نية جرمية خاصة لدى الفاعل[١٨]، أي وجود نية لديه بالاستعمال لاقتراف أي من الجرائم المعيّنة سابقاً (جرائم الولوج أو التعدي على الأنظمة المعلوماتية والبيانات المعلوماتية.)، وليس فقط قيامه بالإنتاج أو الحيازة أو التوزيع، وذلك لو لم يحصل الاستعمال لاحقاً إذ يكفي وجود النية مسبقاً. وتخرج بالتالي عن نطاق تطبيق هذه المادة حالات استخدام الأدوات المعدّة لاختراق الأنظمة المعلوماتية والتعدي على البيانات المعلوماتية لاختبار سلامة هذه الأنظمة أو لإجراء الأبحاث، ففي هذه الحالة تكون الأهداف مشروعة.

يتضمن **الباب الرابع** المعنون "جرائم التعدي على الأموال والمعاملات" جرم الاحتيال[١٩] أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية[٢٠] وجرم أعمال التسويق والترويج غير المرغوب فيها[٢١] وجرم الاستيلاء على أدوات التعريف والهوية[٢٢] المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها وجرم الاطلاع على معلومات سرية أو حساسة أو إفشائها. تحدد المادة ٧ جرم الاحتيال أو الغش بوسيلة معلوماتية، فهو فعل من أقدم عن قصد بصورة غير مشروعة على إلحاق ضرر مالي بالغير عن طريق: إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية أو بكل شكل من أشكال التعدي على عمل نظام معلوماتي، وذلك بنيّة الغش للحصول دون حق على منفعة مادية لنفسه أو للغير. فهذا النص لا يخرج عن المفهوم التقليدي لجرم الاحتيال المعروف، لكنه يحدد الوسائل الاحتيالية المستخدمة للاستيلاء على أموال الغير أو للحصول على المنفعة غير المشروعة بالتعرض للبيانات المعلوماتية أو الأنظمة المعلوماتية. أي أن البيانات المعلوماتية والأنظمة المعلوماتية تكون هي الوسائل المستخدمة لارتكاب الجرم ولا تكون موضوع الجرم. تعرّف المادة ٨ جرم التزوير المعلوماتي، فهو فعل كل من أقدم عن قصد وبصورة غير مشروعة على إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، نتج عنها بيانات غير صحيحة بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه. فموضوع التزوير هنا هو البيانات المعلوماتية وليس المخطوطات الورقية، إنما القصد يبقى ذاته وهو التحوير المتعمد للحقائق لاستعمالها في نطاق القانون. فمفهوم التزوير التقليدي يبقى هو نفسه إنما ينصب هنا على البيانات المعلوماتية. ولا يتطلب تحقق الجرم كون البيانات المعلوماتية تفهم مباشرةً من قبل الإنسان ويكفي بالتالي إمكانية فك رموزها واستعراضها بشكل مفهوم للإنسان عبر الاستعانة بأجهزة حواسب. وجرم التزوير المعلوماتي ينطبق على فعل كل من أقدم عن قصد على استعمال البيانات المعلوماتية غير الصحيحة المذكورة في الفقرة الأولى. تُعاقب المادة ٩ على اختلاس الأموال أو سرقتها باستعمال وسيلة معلوماتية. ويُشترط في هذه الحالة أن تُستعمل الوسيلة المعلوماتية لاختلاس المال أو سرقته، لا لغرض آخر. ويبقى تعريف جرم السرقة والاختلاس منطبقاً على ذلك المعروف في قانون العقوبات العام. تعرّف المادة ١٠ جرم أعمال التسويق والترويج غير المرغوب بها[٢٣] بأنه فعل كل من أقدم على إرسال رسائل ترويج أو تسويق غير مرغوب بها دون تمكين المُرسل إليهم من إيقاف ورود هذه الرسائل، في حال رغبوا بذلك، ومع عدم تحمل أي نفقات إضافية. فقد أصبح إرسال رسائل الترويج للمنتجات والخدمات من قبل التجار للمستهلكين وللمتعاملين شائعاً جداً إلى درجة أصبح مرهقاً لهؤلاء المتعاملين وللأنظمة المعلوماتية بذاتها، ويقتضي بالتالي إتاحة المجال أمام كل متعامل لإيقاف إرسال هذه الرسائل له، وذلك تحت طائلة تجريم الفعل[٢٤]. تُعرّف المادة ١١ فعل الاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر، والمستخدمة في نظام معلوماتي، والاستخدام غير المشروع لها[٢٥]. فقد أضحت هذه الأفعال من النشاطات الجرمية التي تُمارس على نطاق واسع على شبكة الإنترنت بانتحال هوية أو صفة شخص آخر توسلاً للاحتيال أو لسرقة الأموال. ففي التعامل عن قرب، يستطيع الشخص التعرف على الشخص الآخر من خلال ملامحه وصوته وشكله. أما في التعامل عن بعد، فالتعريف عن الشخص يتم من خلال أدوات تعريف تقنية وبرامج معلوماتية قد تكون عرضة للتلاعب، مما يحتّم توفير الحمأي القانونية الرادعة لمثل هذه التصرّفات. في نهأي هذا الباب، تعالج المادة ١٢ فعل الاطلاع بوسائل معلوماتية عن قصد ودون سبب مشروع على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. ويجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة. فالسرية على الشبكات والأنظمة المعلوماتية، حتى المحميّة منها تقنياً، هي دوماً عرضة للانتهاك من قبل مرتكبين يملكون مؤهلات تقنية متقدمة. ويجب بالتالي تجريم هذه الأفعال لردع هؤلاء المنتهكين. وإن تطبيق هذه المادة يرتبط بطبيعة المعلومات، السرية أو الحساسة، كما يرتبط بوسيلة الإفشاء أو الاطلاع التي يجب أن تكون معلوماتية.

يتناول **الباب الخامس** المعنون "جرائم الاستغلال الجنسي للقاصرين" الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية[٢٦]. وتعطي المادة ١٣ تعريفاً للمواد الإباحية[٢٧]، بمفهوم هذا القانون، معتبرةً أنها الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أي أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية، والتي تُظهر للعيان: قاصراً يقوم بفعل جنسي صريح، شخصاً يبدو كقاصر يقوم بفعل جنسي صريح، صوراً واقعية أو مصطنعة بالمحاكاة تظهر قاصراً يقوم بفعل جنسي صريح. هذا التعريف هو واسع يشمل كل الأشكال الممكن تصورها لاستغلال القاصرين جنسياً، بحيث تمنع تفلت المنتهكين من العقوبة. ويحتمل هذا التعريف قيام قاصر فعلياً بالمشاركة في أعمال إباحية، كما يحتمل قيام الراشد الذي له مظهر القاصر بها، أو حتى الصور المصنّعة بالمحاكاة دون اشتراك فعلي لإنسان ما فيها[٢٨]. كما تعرّف المادة ١٣ القاصر بأنه كل من لم يتم الثامنة عشرة من عمره[٢٩]. ويجوز لدولة عضو أن

تخفضّ السن إلى حدود أدنى، لا تقل عن السادسة عشرة. تجرّم المادة ١٤ فعل إنتاج مواد إباحية لقاصرين عن قصد وبصورة غير مشروعة بهدف بثها بواسطة نظام معلوماتي. فالإنتاج لوحده دون قصد البث غير معاقب عليه، ولا يدخل ضمن نطاق هذه المادة، باعتبار أن ضرر المواد الإباحية لا يتحقق إلا ببثها على نطاق واسع. تتناول المادة ١٥ جرم عرض أو توفير أو تقديم بواسطة نظام معلوماتي عن قصد وبصورة غير مشروعة. ويكفي في هذه الحالة قيام المرتكب بعرض المواد الإباحية ولو لم يقم هو نفسه بإنتاجها. تجرّم المادة ١٦ فعل توزيع أو بث أو نقل مواد إباحية قصداً بصورة غير مشروعة لقاصرين بواسطة نظام معلوماتي. فالغأي من هذه المادة المساهمة في منع وضع المواد الإباحية قيد اطلاع الجمهور، الأمر الذي يؤدي إلى انتهاك الآداب العامة وخدش الشعور العام للمواطنين. وتختلف هذه المادة عن المادة التي تسبقها بأن نطاق الأفعال المذكورة فيها أوسع بحيث تطال الجمهور أو فئات كبيرة منه، بخلاف المادة الأولى التي يمكن أن تطال أفعالها شخصاً واحداً فقط. هذا الأمر يحتم أن تكون عقوبة هذه المادة أشد من عقوبة المادة السابقة. تتعلق المادة ١٧ بجرم التزود أو تزويد الغير قصداً بمواد إباحية لقاصرين بواسطة نظام معلوماتي. هذه المادة تطبق على الأفعال الفردية، حيث يقوم شخص بالاستحصال عبر نظام معلوماتي على مواد إباحية لنفسه أو لغيره، ولا يتعدى ذلك إلى الجمهور. إن عقوبة هذا الجرم يجب أن تكون متناسبة مع الضرر المحدود الناتج عنها. تتطرق المادة ١٨ إلى جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي قصداً أو بصورة غير مشروعة. إن قيام شخص بحيازة هذه المواد الإباحية عن قصد يدل عن اتجاه منحرف لديه، ويبرر معاقبته. ولكن لا تدخل الحيازة العرضية أو المؤقتة غير المقصودة، كأن يقوم شخص بسحب صور عن الإنترنت، ثم يكتشف لاحقاً أنها مواد إباحية لقاصرين بعد الاطلاع عليها، ويقوم بالتالي بمحوها عن حاسوبه الشخصي. تجرّم المادة ١٩ فعل تحريض أو تشجيع القاصرين على القيام بأنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية وذلك سواء مجاناً أو لقاء عوض. كأن يستدرج الجاني أحد القاصرين عبر منتديات الحوار على الإنترنت أو عبر مخاطبته برسائل بريدية إلكترونية، ويقنعه بتنفيذ أعمال جنسية واعداً إياه بمكافأة أو غيرها. هذا الفعل يدل على وجود تفكير خلقي متدنٍ ومتمادٍ جرمياً لدى الفاعل، ويعمل على إفساد المجتمع، مما يحتم تشديد عقوبته. تتناول المادة ٢٠ جرم التحرش الجنسي بالقاصرين على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى، وذلك من أجل إشباع الرغبة الجنسية أو من أجل إقناعهم بالقيام بأنشطة جنسية سواء مجاناً أو بعوض. تختلف هذه المادة عن سابقتها في أن الفعل الجنسي الذي يجري إقناع القاصر بتنفيذه يتم في الحالة الأولى مع الغير إلا أنه في الحالة الثانية يتم مع الجاني.

يتضمن **الباب السادس** المعنون "جرائم التعدي على الملكية الفكرية للأعمال الرقمية[٣٠]" الجرائم التالية: جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات[٣١]، وجرم بيع أو عرض عمل مقلّد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة. ومن المتعارف عليه أن الأعمال الرقمية هي محمية بموجب حق المؤلف على الأعمال الفكرية إذا كانت تلبي شروط الابتكار. تجرّم المادة ٢١ فعل التعدي الحاصل على حق المؤلف بِنِسبَة العمل إلى الفاعل عبر وضع اسمه عليه، فتعاقب بالتالي كل من أقدم بقصد الغش على وضع اسم مختلس على عمل أدبي رقمي أو كلّف الغير بذلك. تتناول المادة ٢٢ جرم تقليد إمضاء المؤلف أو ختمه بقصد الغش. وفي ذلك أيضاً حمأي لحق المؤلف بِنِسبَة العمل إليه عبر تمكينه من وضع إمضائه أو ختمه على عمله، مما يثبت أبوته لهذا العمل. تتعلق المادة ٢٣ بجرم تقليد عمل أدبي وفني رقمي أو قرصنة البرمجيات، فهي تحدّد أعمال التقليد الواقعة على العمل الرقمي وكذلك قرصنة البرمجيات. ويشمل التقليد نسخ أو إعادة إنتاج أو طبع أو تصوير العمل الرقمي أو نقله إلى الغير وذلك دون حق. تجرم المادة ٢٤ الاعتداء على الحقوق المادية لصاحب حق المؤلف، فهي تعاقب كل من أقدم على بيع أو عرض للبيع أو وضع بالتداول أو قدّم قصداً عملاً أدبياً فنيا رقمياً مقلداً. تتوسع المادة ٢٥ في الحمأي القانونية الجزائية حتى لا يفلت أي فعل اعتداء على العمل الرقمي من العقاب، وتعاقب كل فعل اعتداء قصداً على أي حق من حقوق المؤلف أو الحقوق المجاورة المتعلقة بالأعمال الرقمية[٣٢].

يتناول **الباب السابع** المعنون "جرائم البطاقات المصرفية والنقود الإلكترونية"[٣٣] الأفعال الجرمية الواقعة على البطاقات المصرفية[٣٤] والنقود الإلكترونية. فالمادة ٢٦ تجرّم فعل تقليد بطاقة مصرفية عن قصد بصورة غير مشروعة. ويعني التقليد صنع أو إنتاج بطاقة مصرفية مزيفة تستعمل للوصول إلى حسابات الغير بصورة غير مشروعة. وتتعلق المادة ٢٧ بجرم استعمال بطاقة مصرفية مقلّدة عن قصد مع العلم بحقيقة البطاقة. فالضرر الحقيقي اللاحق بمصالح الآخرين بالاستيلاء على أموالهم يتحقق فعلياً باستعمال البطاقة المصرفية المزيفة، ولذلك جاءت هذه المادة لتوفر الحمأي القانونية المطلوبة في هذا المجال. ولا يهم طريقة حصول الجاني على البطاقة المصرفية المزيفة، سواء

صنعها بنفسه أو اشتراها أو استولى عليها أو استعارها. كما لا تأثير لنتيجة الاستعمال أي أن الجرم يعتبر واقعاً سواء أدى استعمال البطاقة المزيفة إلى الاستيلاء على أموال أو لا لسبب لا يعود للجاني، كأن يقوم المجرم بمحاولة سحب أموال عبر البطاقة فيتبيّن أن الحساب المجرى منه السحب فارغ. كما حددت المادة ٢٧ في فقرتها الثانية حالات تجريم استعمال أرقام البطاقات المصرفية المسروقة أو الاستيلاء عليها عن قصد. تجرّم المادة ٢٨ الطرف الآخر الذي يُشارك في الجرم ولو بصورة غير مباشرة عبر قبول الإيفاء ببطاقة مصرفية مقلّدة مع علمه بحقيقتها. فمن شأن التغاضي عن تجريم هذا الفعل تشجيع الجاني على التمادي في استعمال البطاقات المصرفية المزورة، ولو تنبه الآخرون إلى وجوب التدقيق في حقيقة البطاقات المصرفية وامتنعوا عن قبول الإيفاء بواسطة بطاقات مقلدة لساهم هذا الأمر في انحصار جرائم تزييف البطاقات واستعمالها. في نهاية هذا الباب، تجرّم المادة ٢٩ كل من أقدم عن قصد بصورة غير مشروعة على تزوير نقود إلكترونية، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

يتضمن **الباب الثامن** المعنون "الجرائم التي تمسّ المعلومات الشخصية" الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي. تجرّم المادة ٣٠ معالجة المعلومات ذات الطابع الشخصي عن قصد وبدون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، إذ إن معالجة المعلومات ذات الطابع الشخصي تخضع لقواعد خاصة لناحية ضرورة الحصول على ترخيص من المراجع الرسمية المختصة أو تقديم تصريح لها حول المعالجة وخصائصها، ولاسيما إذا كانت المعالجة تهدد الحياة الخاصة أو الحريات الشخصية. كما تتضمن هذه القواعد أيضاً قواعد تتعلق بجمع المعلومات وموجب الإعلام وأصول شكلية إجرائية وقواعد تضمن حق الشخص المعني بالاطلاع على المعلومات المُعالجة الخاصة به وطلب إجراء التصحيح اللازم بشأنها. وهذه القواعد هي آمرة ويقتضي فرض احترامها عبر تجريم أي مخالفة لأحكامها لردع المخالفين. ويقتضي بالتالي، وفقاً للمادة ٣١، تجريم معالجة المعلومات ذات الطابع الشخصي التي تتم دون احترام القواعد القانونية المقررة لذلك وفق القانون. كما يجب على المسؤول عن المعالجة المحافظة على سرية معلومات جمعها وهو بصدد معالجتها، حفاظاً على خصوصية الأفراد وحياتهم الخاصة. لذلك تجرّم المادة ٣٢ كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات الطابع الشخصي لأشخاص لا يحق لهم الاطلاع عليها. وقد أشرنا إلى حق الشخص المعني بالاطلاع وطلب التصحيح بخصوص المعلومات المُعالجة المتعلقة به، ولا بد من ضمان تقيد المسؤول عن المعالجة بموجباته لهذه الجهة، عبر فرض عقوبات رادعة على أي مخالفة. وتجرّم المادة ٣٣ لذلك عدم الاستجابة في مهلة قصيرة لطلب الشخص المعني بالاطلاع على المعلومات ذات طابع شخصي المتعلقة به أو بتصحيحها.

يتناول **الباب التاسع** المعنون "جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية"[٣٥] الجرائم التالية: جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية[٣٦]، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية. تجرّم المادة ٣٤ فعل كل من أقدم قصداً على نشر وتوزيع معلومات تثير النعرات العنصرية وتهدف إلى التمييز العنصري بحق أشخاص معينين، وذلك بواسطة شبكة الإنترنت أو غيرها من الوسائل المعلوماتية. وتشترط المادة ٣٤ أن تكون وسيلة النشر أو وسيلة إيصال المعلومات إلى الغير وسيلة معلوماتية، وبالتالي تُستبعد الوسائل الورقية التقليدية من نطاق تطبيق هذه المادة كما باقي المواد اللاحقة. تجرّم المادة ٣٥ جرم تهديد أشخاص أو تحقيرهم أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى. ففعل التحقير والتهديد هو ذاته المعرّف في نطاق قانون العقوبات العام، ولكن وسيلة تحقق الفعل قد اختلفت في هذه الحالة، فهي وسيلة معلوماتية. كما تحدّد المادة ٣٦ فعل توزيع معلومات عن قصد بوسيلة معلوماتية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية. ويقتضي تشديد العقوبات المطبّقة على جرائم هذا الباب بالنظر لخطورتها وطبيعتها وذهنية الفاعل المتطرفة. وأخيراً، وفي هذا الباب ذاته، تعتبر المادة ٣٧ أفعال المساعدة أو التحريض عن قصد بوسيلة معلوماتية على ارتكاب جرائم ضد الإنسانية بمثابة جرم. فيمكن أن يتم التحريض عبر إرسال رسائل بريد إلكتروني أو عبر منتديات الحوار.

يتضمن **الباب العاشر** المعنون "جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية"[٣٧] الجرائم التالية[٣٨]: جرم تملك وإدارة مشروع مقامرة على الإنترنت، وجرم تسهيل وتشجيع مشروع مقامرة على الإنترنت، وجرم ترويج الكحول للقاصرين على الإنترنت، وجرم ترويج المواد المخدرة على الإنترنت. تجرّم المادة ٣٨ فعل كل من تملك أو أدار مشروع مقامرة أو عرض ألعاب مقامرة على شبكة الإنترنت أو بأي وسيلة معلوماتية

أخرى. في بعض الدول، تكون ألعاب المقامرة مشروعة في حال الترخيص، ويقتضي بالتالي مراعاة هذا الأمر. يُفترض بألعاب المقامرة وفق هذه المادة أن تكون مُتاحة على شبكة الإنترنت أو بوسيلة معلوماتية، وتُستبعد بالتالي ألعاب المقامرة التقليدية. وتتضمن هذه المادة ثلاثة أفعال جرمية: تملك مشروع مقامرة، إدارة مشروع وإن كان عائداً لشخص آخر، عرض ألعاب مقامرة ولو بصورة عرضية وفردية وخارج إطار مشروع مستمر. تُجرّم المادة ٣٩ فعل تسهيل وتشجيع إنشاء أو إدارة أو ترويج مشروع مقامرة على شبكة الإنترنت أو بوسيلة معلوماتية. يمكن أن تكون أفعال التسهيل أو التشجيع بجميع الطرق المتاحة، كالوعد بجلب زبائن أو المساهمة في تصميم موقع على شبكة الإنترنت. ولكن مشروع المقامرة يجب أن يكون مُتاحاً للجمهور بواسطة وسيلة معلوماتية. تتطرق المادة ٤٠ إلى جرم ترويج الكحول للقاصرين على الإنترنت، فيعد جرماً فعل ترويج الكحول مع استهداف القاصرين على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. فمن شروط هذا الجرم الخاصة: ترويج الكحول من خلال وسيلة معلوماتية كشبكة الإنترنت، واستهداف القاصرين بشكل مباشر أي التوجه إليهم بشكل خاص أو التوجه إلى كل الفئات العمرية دون تخصيص ودون استثناء القاصرين وتنبيههم. تجرّم المادة ٤١ فعل ترويج أو بيع أو عرض طرق إنتاج المواد المخدرة على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. إن ماهية المواد المخدرة هي معروفة ومحددة وفق القوانين الوطنية. إنما جديد هذه المادة هو الوسيلة التي يتم الترويج بها ألا وهي وسيلة معلوماتية أو شبكة الإنترنت.

يتناول **الباب الحادي عشر** المعنون "جرائم المعلوماتية ضد الدولة والسلامة العامة" الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني. وهذه الجرائم على قدر من الأهمية لتأثيرها على الدولة وانتظام عملها وبالتالي على المواطنين كافة، مما يقتضي معه تشديد العقوبات المقررة لهذه الجرائم. فالمادة ٤٢ تجرّم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال أي وسيلة معلوماتية أو إنتاج أو توزيع أو حيازة برامج معدة لهذا الاستعمال. فالأعمال الحكومية وأعمال السلطة العامة تتعلق بإدارة الدولة وممارسة أجهزتها لمهامها وفق السلطات الممنوحة لها بموجب القوانين المرعية الإجراء. تجرّم المادة ٤٣ فعل كل من امتنع عن قصد أو أبلغ عن قصد بشكل خاطئ عن جرائم المعلوماتية. فجريمة الإبلاغ لا تتعلق بجميع الجرائم بل فقط بنوع خاص منها هو جرائم المعلوماتية. وهذه الجريمة هي جريمة قصدية، أي يجب أن يكون الجاني قد علم بحصول الجريمة المعلوماتية، وتمنع عن الإبلاغ عنها أو أبلغ عنها بشكل خاطئ ومضلّل لتجهيل الفاعل أو لاتهام آخرين أو لإخفاء الأدلة. تجرّم المادة ٤٤ فعل من أقدم على الاطلاع أو على الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. إن حمأي المعلومات السرية العائدة للدولة يجب أن تكون فعّالة، فتسريبها يمكن أن يمسّ بانتظام الدولة وكيانها وأمنها وسلامتها. وتشترط هذه المادة استعمال وسيلة معلوماتية للوصول إلى المعلومات السرية وليس أي وسيلة أخرى. في نهأي هذا الباب، تجرّم المادة ٤٥ فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو تخبئتها أو التعديل فيها أو محوها. لقد أصبحت المعلوماتية تستخدم كوسيلة مساعدة لارتكاب أي جريمة، وقد تكون موضوع الجريمة نفسها. لذلك، فضبط الجرائم المعلوماتية وكذلك الجرائم العادية وإثباتها يتطلب جمع أدلة معلوماتية عليها وخصوصاً الحفاظ عليها من العبث والإتلاف والتخبئة أو التعديل فيها أو محوها لتفادي الإدانة[٣٩]. تجرّم المادة ٤٦ فعل بث أو إذاعة أو نشر بيانات أو معلومات تهدد الأمن والسلامة العامة في الدولة أو أي دولة أخرى، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى. فقد أصبحت الشبكات والوسائل المعلوماتية تستعمل كطرق فعّالة لنشر المعلومات بالنظر لقدرتها على تخطي الحواجز والأبعاد الجغرافية والوصول إلى كل مكتب وبيت، وإن جسامة الضرر الناجم عنها يفوق بأشواط ذلك العائد لأي وسيلة أخرى عادية، كالرسائل أو الخطابات الورقية أو الخطب العلنية. تجرّم المادة ٤٧ فعل كل من ارتكب أعمالاً إرهابية أو ساهم فيها أو حرّض عليها باستعمال شبكة الإنترنت[٤٠] أو أي وسيلة معلوماتية أخرى. فالأعمال الإرهابية[٤١] لا تقتصر على التفجيرات أو أعمال القتل الجماعي أو تعطيل مصالح الدولة بل أصبحت تطال الأنظمة المعلوماتية التي تتحكم بمختلف قطاعات الخدمات الحديثة المقدمة للمواطنين، كقطاع النقل الجوي أو المصارف أو الاتصالات. فتعطيل النظام المعلوماتي المعتمد لتنظيم سير الطائرات قد يؤدي إلى سقوطها. وإن تخريب هذه القطاعات من خلال اختراق الأنظمة المعلوماتية يشكّل بطبيعة الحال يشكل عملاً إرهابياً كونه يطال المصالح العليا للدولة والسلامة العامة. أخيراً، يعدّ جرماً وفق المادة ٤٨ فعل كل من أقدم على تحريض شخص آخر على القتل باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى. فقد يتم ذلك من خلال توجيه رسائل بريد إلكتروني إلى القاتل أو صور أو أفلام مركبة تستفزّه وتحرضه على القتل.

يتطرق **الباب الثاني عشر** المعنون "جرائم تشفير المعلومات" إلى الأفعال الجرمية الناشئة عن التشفير[٤٢]. إن التشفير هو كل عمل يرمي إلى تحويل معلومات أو إشارات

واضحة، عبر اتفاقات سرية، إلى معلومات أو إشارات غامضة للغير، أو إلى إجراء العملية المعاكسة عبر وسائل مادية أو معلوماتية مخصّصة لهذا الغرض. ويستخدم التشفير لأغراض السرية عند نقل المعلومات أو تخزينها. فالمعلومات المشفرة تكون غير قابلة للفهم من قبل الغير إلا بعد فك التشفير. كذلك يُستخدم التشفير لتوثيق المعلومات وللمصادقة عليها ولوظيفة التوقيع الإلكتروني. ويكون بالتالي للتشفير وجهان للاستخدامات: استخدامات مدنية واستخدامات عسكرية. لذلك تحرص جميع الدول على فرض مراقبة قانونية على التشفير لمنع إساءة استعماله. وتقرن هذه المراقبة بعقوبات جزائية رادعة. تجرّم المادة ٤٩ فعل تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة. فأعمال التسويق أو التوزيع أو الاستيراد أو التصدير تجري على نطاق واسع، وفي معظم الأحيان من قبل تجار أو من قبل مؤسسات متخصصة. ويفترض أن تخضع للترخيص أو لموجب تقديم تصريح للمراجع المختصة في الدولة للتمكن من إخضاعها للرقابة مخافة تحول استخدام وسائل التشفير لارتكاب الجرائم أو لإخفاء معالمها أو لأعمال عسكرية عدوانية كالتجسس. تجرّم المادة ٥٠ فعل تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل الجهات الرسمية المختصة في الدولة. فهذا الفعل قد يتم لمرة واحدة فقط ومن قبل شخص غير متخصص أيضاً، إلا أن خطورته تنبع من استخدام التشفير لتأمين السرية، وقد يكون ذلك لأعمال غير شرعية كالتجسس أو التواصل بين الجماعات الإرهابية أو الإجرامية. تجرّم المادة ٥١ فعل كل من أقدم على بيع أو تسويق أو تأجير وسائل تشفير ممنوعة. فقد تحظّر المراجع الرسمية المختصة في الدولة بعض وسائل التشفير لاعتبارات متنوعة: عدم إمكانية مراقبة استخداماتها، عدم تعاون المصنّعين مع أجهزة الدولة، عدم موثوقية هذه الوسائل وإمكانية اختراقها. ولا بد من فرض عقوبات جزائية رادعة لضمان فعالية الحظر المطبّق.

يتناول **الباب الثالث عشر**[٤٣] العقوبات العائدة للجرائم المعددة في هذا الإرشاد. وتنص المادة ٥٢ على أن كل من يقترف أياً من الجرائم المحددة في هذا الإرشاد يتعرض لعقوبة السجن لفترة تحددها الدولة المعنية والغرامة أو بإحدى هاتين العقوبتين. ويُترك للدولة المعنية أمر تقدير مدة عقوبة السجن وقيمة الغرامة بحديها الأدنى والأعلى. أما المادة ٥٣ فتتعلق بمصادرة الأجهزة التي استخدمت في الجريمة. وتتعلق المادة ٥٤ بحالات تخفيف العقوبة أو تشديدها مثلاً في حال التكرار.

أما **الباب الرابع عشر**، فيتناول إنشاء هيئة وطنية قومية لمكافحة الجرائم المعلوماتية. فقد نصت المادة ٥٥ على أن تحرص الدول الأعضاء على إنشاء وحدة متخصصة في الأجهزة الأمنية التابعة للقضاء والموكلة بالتحقيقات القضائية، وتتولى أعمال التحقيق في الجرائم المعلوماتية ورصدها تحت إشراف القضاء. وتتألف هذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات. كما نصت المادة ٥٦ على أن تحرص الدول الأعضاء على التعاون فيما بينها في مجال التحقيقات القضائية المتعلقة بالجرائم المعلوماتية.

هوامش

١ – Internet وIntranet والشبكات الخاصة ببعض الأجهزة التابعة لمؤسسة أو منظومة واحدة مثل الشبكة التي تربط بين أجهزة حاسوب ضمن إدارة رسمية أو وزارة.

٢– *Actus rea*، تعبير لاتيني يعني الفعل الجرمي.

٣– *Means rea* ، تعبير لاتيني يعني الفكر الإجرامي أي نية ارتكاب عمل غير قانوني بمعرفة وقصد المرتكب. النص اللاتيني هو *actus non facit reum nisi mens sit rea* وترجمتها للعربية هي: لا يشكل الفعل جرماً ما لم يكن فاعله يقصد إحداث الجرم.

4- Virus/Malware. Crime on the Net,
http://rogerdarlington.me.uk/crimeonthenet.html#Hacking

Viruses, in the broadest sense, come in three forms:
- *Virus*: This is a code that attaches itself to a program in a computer and then reproduces itself. It can erase files or lock up a system.
- *Worm*: This is similar to a virus but does not attach itself to files or programs in a computer. This leaves it free to spread through a network on its own.

- *Trojan horse*: This is a program that performs malicious actions while pretending to do something else. It is similar to a virus but does not try to reproduce itself.

٥ – أمثلة على جرائم الانترنت:
http://www.lawoflibya.com/forum/showthread.php?t=3624
تشير مجلة لوس انجيلوس تايمز في عددها الصادر في ٢٢ مارس عام ٢٠٠٢ إلى أن خسارة الشركات الإمريكية وحدها من جراء الممارسات التي تتعرض لها و التي تندرج تحت بند الجريمة الإلكترونية تقدّر بحوالي ٠١ مليار دولار سنويا× و للتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة ٢٦٪ من تلك الجرائم تحدث من خارج المؤسسة و عن طريق شبكة الانترنت بينما تنتج النسبة الباقية (٨٣ ٪) من تلك الخسائر عن ممارسات تحدث من داخل المؤسسات ذاتها.

مثال آخر حديث قد لا يتوقع أحد كم الخسائر الناجمة عنه وهو تلك الأعطال و الخسائر في البرامج والتطبيقات والملفات ونظم العمل الآلية وسرعة وكفاءة شبكات الاتصال والذي ينجم عن التعرض للفيروسات والديدان مثل ذلك الهجوم الأخير والذي تعرضت له الحواسيب المتصلة بشبكة الانترنت في اغلب دول العالم من خلال فيروس يدعى (WS32.SOBIG) والذي أصاب تلك الأجهزة من خلال رسائل البريد الالكتروني بصورة ذكية للغاية حيث كان ذلك الفيروس يتخفي في الوثيقة الملحقة بالبريد الالكتروني (Attachment File) في صورة ملف ذي اسم براق و عند محاولة فتح ذلك الملف فان الفيروس ينشط ويصيب جهاز الحاسب و يبدأ في إرسال المئات من رسائل البريد الالكتروني من ذلك الجهاز المصاب مستخدما كل أسماء حسابات البريد الالكتروني المخزنة عليه. الأمر الذي أدى إلى إصابة عدد هائل من الحواسب الشخصية للأفراد والشركات وملء خوادم البريد الالكتروني بتلك الرسائل. مثال على ذلك إصابة خوادم البريد الالكتروني لشركة أميركا أون لاين بما يقارب ال ٠٢ مليون رسالة ملوثة وأدى ذلك أيضا إلى بطء شبكات وخطوط الاتصال بصورة كبيرة و أحيانا بالشلل التام مما أدى إلى تعطّل الكثير من الأعمال و تلف العديد من الملفات الهامة على تلك الحواسب. وقد قدرت الخسائر الناجمة عن ذلك الفيروس بما يقارب ال ٠٥ مليون دولار أمريكي في داخل الولايات المتحدة الامريكية وحدها.

6- Current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center along with its description, http://www.ic3.gov/crimeschemes.aspx

Auction Fraud, Counterfeit Cashier's Check, Credit Card Fraud, Debt Elimination, Parcel Courier Email Scheme, Employment/ Business Opportunities, Escrow Services Fraud, Identity Theft, Internet Extortion, Investment Fraud, Lotteries, Nigerian Letter or "419", Phishing/Spoofing, Ponzi/Pyramid, Reshipping, Spam, Third Party Receiver of Funds.

7- Cyber Crime Statistics from the 2006 Internet Crime Report, http://www.computer-forensics-recruiter.com/home/cyber_crime_statistics.html

- In 2006, the Internet Crime Complaint Center received and processed over 200,000 complaints.
- More than 86,000 of these complaints were processed and referred to various local, state, and federal law enforcement agencies.
- Most of these were consumers and persons filing as private persons.
- Total alleged dollar losses were more than $194 million.
- Email and websites were the two primary mechanisms for fraud.
- Although the total number of complaints decreased by approximately 7,000 complaints from 2005, the total dollar losses increased by $15 million.
- The top frauds reported were auction fraud, non-delivery of items, check fraud, and credit card fraud.
- Top contact mechanisms for perpetrators to victims were email (74%), web page (36%), and phone (18%) (there was some overlap).

The Internet Crime Complaint Center is a clearinghouse for online economic crime complaints. It is maintained by the National White Collar Crime Center and the Federal Bureau of Investigations. To review the results of the study, visit the National White Collar Crime Center's site.

Cyber Crime Statistics from the 12th Annual Computer Crime and Security Survey:

- Between 2006 and 2007 there was a net increase in IT budget spent on security.
- Significantly, however, the percentage of IT budget spent on security awareness training was very low, with 71% of respondents saying less than 5% of the security budget was spent on awareness training, 22% saying less than 1% was spent on such training.
- 71% of respondents said their company has no external insurance to cover computer security incident losses.
- 90% of respondents said their company experienced a computer security incident in the past 12 months.
- 64% of losses were due to the actions of insiders at the company.

The top 3 types of attack, ranked by dollar losses, were:

- financial fraud ($21.1 million)
- viruses/worms/trojans ($8.4 million)
- system penetration by outsiders ($6.8 million)

The complete results of this study, as well as past studies, which are conducted annually by the Computer Security Institute, can be found at the CSI website www.gocsi.com . Interestingly, these statistics are compiled from voluntary responses of computer security

professionals. Thus, there is certainly an inference that the damages due to computer security incidents are much higher than those cited here, as companies without responding security professionals undoubtedly were the victim of computer security incidents.

Cyber Crime Statistics from the Online Victimization of Youth, Five Years Later study:

- Increasing numbers of children are being exposed to unwanted sexual materials online.
- Reports of online sexual solicitations of youth decreased while reports of aggressive sexual solicitation of youth did not (perhaps indicating that some prevention and education measures may be working, while the most serious offenders may not be deterred).
- Online child solicitation offenses are rarely reported to any authority.
- Incidents of online harassment and bullying increased.

This is an empirical study based on approximately 1500 surveys conducted with online youth in 2005 that were compared to the results of a similar study in 2001. The study was conducted by the National Center for Missing and Exploited Children, the Crimes Against Children Research Center, and the Office for Juvenile Justice and Delinquency Prevention at the United States Department of Justice. The complete results of the study can be found here http://www.missingkids.com.

8- Types of Cybercrime, : http://www.brighthub.com/internet/security-privacy/articles/3435.aspx

Assault by Threat – threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.
Child Pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
Cyber Contraband – transferring illegal items through the internet (such as encryption technology) that is banned in some locations.
Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.
Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology.
Cyber theft – using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy. Examples include:

- Advertising or soliciting prostitution through the internet. It is against the law to access prostitution through the internet (including in the state of Nevada in the United States) because the process of accessing the internet crosses state and sometimes national borders. This is a violation of the federal Digital Millennium Copyright Act http://www.copyright.gov/legislation/dcma.pdf.

- Drug Sales. Both illegal and prescription drug sales through the internet are illegal except as a customer through a state licensed pharmacy based in the United States http://www.fda.gov.

- Computer-based fraud. Fraud is different from theft because the victim voluntarily and knowingly gives the money or property to the criminal but would not have if the criminal did not misrepresent themselves or their offering. Fraud is a lie. If someone leads you on or allows you to believe something that is false to benefit them, they are lying and this is fraud. You become a victim when you voluntarily surrender monies or property based on their misrepresentation or lie. Losing money from computer crime can be especially devastating because often it is very difficult to get the money back. Examples are: scams and altering data to get a benefit, such as removing arrest records from the police station server, changing grades on the school computer system or deleting speeding tickets from driving records.

- Online Gambling. Gambling over the internet is a violation of American law because the gambling service providers require electronic payment for gambling through the use of credit cards, debit cards, electronic fund transfers which is illegal with the Unlawful Internet Gambling Enforcement Act http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4411eh.txt.pdf.

- Cyber tresspass – someone accesses a computer's or network's resources without the authorization or permission of the owner but does not alter, disturb, misuse, or damage the data or system. This is hacking for the purpose of entering an electronic network without permission. Examples might include:

- Using a wireless internet connection at a hotel at which you are staying and accessing the hotel's private files without disturbing them because they are available.

- Reading email, files, or noting which programs are installed on a third-party's computer system without permission just for fun, because you can. This is sometimes called Snooping.

- Cyber vandalism - Damaging or destroying data rather than stealing or misusing them (as with cyber theft) is called cyber vandalism. This can include a situation where network services are disrupted or stopped. This deprives the computer/network owners and authorized users (website visitors, employees) of the network itself and the data or information contained on the network. Examples:

- Entering a network without permission and altering, destroying, or deleting data or files.

- Deliberately entering malicious code (viruses, Trojans) into a computer network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network.

- Attacking the server of the computer network (DDoS attack) so the server does not perform properly or prevents legitimate website visitors from accessing the network resources with the proper permissions.

9- Organized Crime.

10- Study of Russia-Georgia Cyber Conflict Brings Warnings To U.S. Businesses, Citizens, By Tim Wilson, Aug 18, 2009, available: http://www.darkreading.com/security/cybercrime/showArticle.jhtml;jsessionid=XNYFLA2S30SIPQE1GHPSKHWATMY32JVN?articleID=219400367.

11- Definition of Cyber terrorism, http://eziearticles.com/?An-Orthodox-Report-On-Organized-Cyber-Crime&id=5236455.
Many definitions exist for cyber terrorism like the various definitions of terrorism. A security expert named Dorothy Denning describes cyber terrorism as: politically induced hacking operations projected to cause massive loss like the severe economic breakdown or loss of life. Others denote cyber terrorism as a massive substantial attack that tears down computerized infrastructures like the telecommunications, electric power grid or the Internet without even touching a keyboard.

12 - Crime on the Net, http://rogerdarlington.me.uk/crimeonthenet.html#Hacking
Hacking can take several forms:

- Accessing - entering a network which is intended to be private
- Defacing – changing the content of another person's Web site
- Hijacking – redirecting elsewhere anyone trying to access a particular Web site
- Bombing – overwhelming a site with countless messages to slow down or even crash the server
- Denial of service – running a program which sends thousands of requests to a site simultaneously, frequently from more than one source, so that the relevant server slows down considerably or preferably (from the point of view of the hacker) crashes.

13- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193_en.htm
The main types of criminal offences covered by this Framework Decision are attacks against information systems such as piracy, viruses and denial of service attacks. This new criminal activity, which knows no borders, can be prevented and combated by:
- enhancing the security of information infrastructures
- giving law enforcement authorities the means to act.

To this end, the present Framework Decision proposes the approximation of criminal law systems and the enhancement of cooperation between judicial authorities concerning:

- illegal access to information systems;
- illegal system interference;
- illegal data interference.

In all cases, the criminal act must be intentional. Instigating, aiding, abetting and attempting to commit any of the above offences will also be liable to punishment.

14- See The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) took effect on January 1, 2004, http://www.spamlaws.com/federal/can-spam.shtml.

Fighting Back Against Email Spammers, Internet Hackers, and other Web Thieves, http://www.infohq.com/Computer/Spam/fight-internet-hackers-email-spammers.htm.

A hacker is an individual that attempts to take control over someone else's computer by using viruses, worms, and other types of Internet attacks. One of their favorite "tricks", is to use hacked computers to bring down a large web site by overloading the targeted site with millions of transmissions in a "denial of service" (DOS) attack.

While hackers were glorified in the early days of the Internet as people standing up for their rights against big corporations and the Government, hacking is now the hobby of criminals and thieves. Hackers prey on all citizens of the Internet and they are extremely dangerous to individuals, corporations, and governments.

How does a hacker find your computer?

Most hack attempts against personal computers result from viruses and worms running from an infected PC. It is not very difficult for the creator of the hacking program to predetermine the Internet addresses that his program will attack.
There are also amateur hackers, that use software programs, to randomly check for online computers to attack

What makes Spamming or Hacking Illegal?

The U.S. Congress outlawed certain types of spam with the CAN-SPAM Act of 2003. The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. However a "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

The Federal Trade Commission (FTC), the nation's consumer protection agency, is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

However, 38 states have also passed anti-spam laws that have various penalties for illegal spammers and hackers. If you don't live in a state with an anti-spam law, you are still protected from fraudulent schemes, illegal pornography, and other illegal acts by various state and federal laws.

In addition, if a spammer or hacker causes harm to a Government computer they are subject to the penalties of USC Title 18, Part I, Chapter 47, Sec. 1030. - Fraud and related activity in connection with computers.

15- http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.
The term “hacking” is used to describe the unlawful access of a computer system. It is one of the oldest computer-related crimes, and in recent years has become a mass phenomenon. By targeting computer systems that host large databases, offenders can obtain identity-related data on a large scale, and this is an increasingly popular approach. In the largest case detected in the past in the USA, the thieves obtained more than 40,000,000 credit card records.

16- Prosecuting Computer crimes, February 2007- Computer Fraud and Abuse Act, Effective September 26, 2008, 18 U.S.C. § 1030 was amended by the Identity theft Enforcement and Restitution Act of 2008, http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.html.

17- F. Damaging a Computer or Information: 18 U.S.C. § 103(a)(5), http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.html#E.2.
Criminals can cause harm to computers in a wide variety of ways. For example, an intruder who gains unauthorized access to a computer can send commands that delete files or shut the computer down. Alternatively, intruders can initiate a "denial of service attack" that floods the victim computer with useless information and prevents legitimate users from accessing it. In a similar way, a virus or worm can use up all of the available communications bandwidth on a corporate network, making it unavailable to employees. In addition, when a virus or worm penetrates a computer's security, it can delete files, crash the computer, install malicious software, or do other things that impair the computer's integrity. Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts.

Section 1030(a)(5) criminalizes a variety of actions that cause computer systems to fail to operate as their owners would like them to operate. Damaging a computer can have far-reaching effects. For example, a business may not be able to operate if its computer system stops functioning or it may lose sales if it cannot retrieve the data in a database containing customer information. Similarly, if a computer that operates the phone system used by police and fire fighters stops functioning, people could be injured or die as a result of not receiving emergency services. Such damage to a computer can occur following a successful intrusion, but it may also occur in ways that do not involve the unauthorized access of a computer system.

Title 18, United State Code, Section 1030(a)(5) provides:

Whoever
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subsection (A), caused (or, in the case of an attempted offense, would, if completed, have caused) (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security
shall be punished as provided in subsection (c) of this section.

18- Crime on the Net, http://rogerdarlington.me.uk/crimeonthenet.html#Hacking.
One of the most common types of fraud on the Internet is designed to trick users of certain sites - notably banks and building societies - into disclosing their passwords or other confidential information needed to access their accounts. A common means of doing this is to e-mail customers advising that it is necessary to check or confirm their password by clicking onto a realistic but fake website and then inputting the confidential information. It is then possible for money to be fraudulently transferred from the individual's account.

In the Autumn of 2003, this type of fraud was perpetrated against UK customers of Barclays, Nat West, Lloyds TSB, Citibank, Halifax and Nationwide. In fact, no bank of financial institution would ever ask a customer to disclose confidential information in this way.

19- Credit Card Theft, http://www.ehow.com/list_7448512_cyber-identity-theft-methods.html.
Purchasing items on the Internet with your credit card can lead to having your card used by thieves to make purchases. When shopping online, stick with websites you know and trust. When making a purchase, always look at the address bar to make sure there is an "s" after the http. This indicates a secure transfer of your information. Use antivirus software that has firewall protection and prevents browser hijacking to reinforce your security.

20- Fighting Back Against Email Spammers, Internet Hackers, and other Web Thieves, http://www.infohq.com/Computer/Spam/fight-internet-hackers-email-spammers.htm.
Spam in a general sense is any email you don't want to receive. There are many types of email that you may not want e.g. advertisements, newsletters, or questionnaires, however these emails are not what the computer community refers to as spam. What the computer community is most concerned with is illegal email spam.

The definition of illegal email spam is -- attempts to deceive by falsification of seller identity or email address, and use of other trickery (defrauding), in the hope of gaining monetary advantage (stealing) from the email recipient and other parties.
The Federal Trade Commission's definition of spam, "Not all UCE is fraudulent, but fraud operators - often among the first to exploit any technological innovation - have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. In fact, UCE has become the fraud artist's calling card on the Internet. Much of the spam in the Commission's database contains false information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes." From Prepared Statement Of The Federal Trade Commission On "Unsolicited Commercial email", November 3, 1999.

How does a spammer get your email address?
There are many ways a spammer can obtain your email address.

a. You can disclose it yourself by posting your email address on auctions, bulletin boards, advertising, or email locators.
b. Businesses might sell your email address or other personal information to a spammer.
c. Spammers can use software programs to collect email addresses from web sites or they can use random number generators to send spam out randomly.

21- Cyber Identity Theft Methods, http://www.ehow.com/list_7448512_cyber-identity-theft-methods.html.
One of the most frequent cyber crimes on the Internet is identity theft. Having your identity stolen cannot only lead to huge financial loss, it can be damaging to your reputation and leave you feeling violated as well. According to Javelin Strategies, "Incidences of the

crime increased by 11 percent from 2008 to 2009, altering the lives of 11 million Americans."
Identity theft is a form of theft in which the targets are bank accounts, credit cards, debit cards, social security numbers and information that is linked to a person's identity.

22- How spam works, http://computer.howstuffworks.com/internet/basics/spam.htm.
Spam is a huge problem for anyone who gets e-mail. According to Business Week magazine:
In a single day in May [2003], No. 1 Internet service provider AOL Time Warner (AOL) blocked 2 billion spam messages -- 88 per subscriber -- from hitting its customers' e-mail accounts. Microsoft (MSFT), which operates No. 2 Internet service provider MSN plus e-mail service Hotmail, says it blocks an average of 2.4 billion spams per day. According to research firm Radicati Group in Palo Alto, Calif., spam is expected to account for 45% of the 10.9 trillion messages sent around the world in 2003.

23- The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) took effect on January 1, 2004, http://www.spamlaws.com/federal/can-spam.shtml.

24- The globalization of crime a transnational organized crime threat assessment, UNODC, 2010, page 203- 209 (fig 161, 162, 163, 164, http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

25- European Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal L 013 , 20/01/2004 P. 0044 – 0048, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML.
Child pornography: pornographic material that visually depicts or represents a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child, or a real person appearing to be a child involved or engaged in such conduct, or realistic images of a non-existent child involved or engaged in such conduct.

European Council Decision of 29 May 2000 to combat child pornography on the Internet, Official Journal L 138 , 09/06/2000 P. 0001 – 0004, http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0375:EN:HTML.

26- The following is deemed to be punishable conduct that constitutes an offence related to child pornography, whether undertaken by means of a computer system or not:

- production of child pornography;
- distribution, dissemination or transmission of child pornography;
- supplying or making available child pornography;
- acquisition and possession of child pornography.

Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm..

27- Child Pornography Domains Reported To The Internet Watch Foundation (UK), FIG. 165, 166, 167, 168, 169 http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

28- Child: anyone below the age of 18 years.
Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_trafficking_in_human_beings/l33138_en.htm.

29- Combating Online Infringement and Counterfeits Act, a bill introduced by Senator Patrick Leahy (D-VT), The Senate of the United States on September 20, 2010, http://www.wired.com/images_blogs/threatlevel/2010/09/CombatingOnlineInfringementAndCounterfeitsAct1.pdf.

30- The two forms of IP most frequently involved in cyber crime are copyrighted material and trade secrets. Piracy is a term used to describe IP theft—piracy of software, piracy of music, etc. Theft of IP affects the entire U.S. economy. Billions of dollars are lost every year to IP pirates. For example, thieves sell pirated computer software for games or programs to millions of Internet users. The company that actually produced the real product loses these sales and royalties rightfully due to the original creator. http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html.

31- Mississipi code of 1972- SEC. 97-45-9. Offense against intellectual property; penalties, http://www.mscode.com/free/statutes/97/045/0009.htm.
An offense against intellectual property is the intentional:
(a) Destruction, insertion or modification, without consent, of intellectual property; or
(b) Disclosure, use, copying, taking or accessing, without consent, of intellectual property.
Whoever commits an offense against intellectual property shall be punished, upon conviction, by a fine of not more than One

Thousand Dollars ($1,000.00), or by imprisonment for not more than six (6) months, or by both such fine and imprisonment. However, when the damage or loss amounts to a value of One Hundred Dollars ($100.00) or more, the offender may be punished, upon conviction, by a fine of not more than Ten Thousand Dollars ($10,000.00) or by imprisonment for not more than five (5) years, or by both such fine and imprisonment.
The provisions of this section shall not apply to the disclosure, use, copying, taking, or accessing by proper means as defined in this chapter.
Sources: Laws, 1985, ch. 319, Sec. 5, eff from and after July 1, 1985.

32- Internet Fraud: Tips to avoid Internet fraud, http://www.fbi.gov/scams-safety/fraud/internet_fraud/internet_fraud.

33- Financial and high-tech crimes, http://www.interpol.int/Public/FinancialCrime/Default.asp.
Payment card fraud is a generic term used to describe a range of offences involving theft and fraudulent use of payment card account data. Frequent types of payment card fraud include:

Application fraud – a type of ID theft crime in which payment cards are obtained through a fraudulent application process using stolen or counterfeit documents.
Account takeover – another type of ID theft crime, this usually involves deception of a financial institution, re-issue of a payment card and its redirection to a different address.
Lost / stolen card – as the name suggests, this type of fraud involves misuse of actual cards that are either lost or stolen from the genuine cardholder.

Counterfeit card – fraud undertaken using plastic cards that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash.

Card not present (CNP) – fraud committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed by Internet, mail order or telephone. CNP fraud is currently the fastest growing payment card related type of fraud in many areas of the world.

34- Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

35- Australian Human Rights Commission: Cyber racism is a term used for racism on the internet. It includes racist websites, images, blogs, videos and comments on web forums.
Racist material on the internet that is offensive, harassing or threatening may also be a criminal offence under Commonwealth as well as State and Territory law. This will depend upon the nature of material published. http://www.hreoc.gov.au/racial_discrimination/publications/cyberracism_factsheet.html.

36- Federal law prohibits individuals from betting on sports or gambling contests using a "wire communication facility," which includes the Internet. Yet the Internet allows immediate and anonymous communication that makes it difficult to trace gambling activity. Internet sites can be altered or removed in a matter of minutes. For these reasons organized crime operates Internet gambling sites.
Operators alter gambling software to be in their favor so the customer always loses. Unlike real casinos that are highly regulated, Internet gambling is unregulated and dangerous. Individuals gambling on the Internet risk providing credit card numbers and money to criminal gambling operators. Further, minors can gamble on the sites since the Internet is unaware of the age of its users. All a minor needs is access to a credit card number. Internet gambling also lures compulsive gamblers who may suffer devastating financial losses.

37- Internet Gambling: Overview of federal criminal law, http://books.google.com.lb/.

38- Evidence tampering: Tampering with evidence is the knowing and intentional physical manipulation, altering or destruction or falsification of evidence relevant to a criminal case or investigation. It is important to note that tampering is not the accidental destruction or modification of evidence, it is only if the individual had reason to believe the material or item was part of an investigation.
http://www.criminaldefenselawyer.com/crime-penalties/federal/Tampering-with-evidence.htm.

39- Computer Crime Research Center: What is a Cyber Crime? "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."
http://www.crime-research.org/library/Cyber-terrorism.htm.

40- Cyber Terrorism Vulnerabilities and Policy Issues “Facts Behind The Myth” by Dhanashree Nagre Priyanka Warade, http://www.contrib.andrew.cmu.edu/~dnagre/Final_Report_dnagre_pwarade.pdf

Cyberterrorism can be defined in different ways viz. it can be politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage; or

It can be unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, or

It can be a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard.

Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all three methods described above (physical attack, EA, and cyber attack) might contribute to, or be labeled as "cyber terrorism."

41- Illinois Statute, January 1, 2009 (720 Illinois Compiled Statutes § 16D-5.5.), http://cyb3rcrim3.blogspot.com/2008/10/unlawful-use-of-encryption.html

A person shall not knowingly use or attempt to use encryption, directly or indirectly, to:
(a) commit, facilitate, further, or promote any criminal offense;
(b) aid, assist, or encourage another person to commit any criminal offense;
(c) conceal evidence of the commission of any criminal offense; or
(d) conceal or protect the identity of a person who has committed any criminal offense.

Telecommunications carriers and information service providers are not liable under this Section, except for willful and wanton misconduct, for providing encryption services used by others in violation of this Section.
A person who violates this Section is guilty of a Class A misdemeanor, unless the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law. If the encryption was used or attempted to be used to commit an offense for which a greater penalty is provided by law, the person shall be punished as prescribed by law for that offense.
A person who violates this Section commits a criminal offense that is separate and distinct from any other criminal offense and may be prosecuted and convicted under this Section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this Section.

٤٢- يمكن للدول التي تستعين بهذا الإرشاد الاستعاضة عن الباب الثالث عشر عبر الإحالة إلى قانون الجزاء أو العقوبات بالنسبة لارتكاب الجرائم المعلوماتية وذلك بإضافة مادة تنص على أنه تطبق على الجرائم المحددة بهذا الإرشاد (القانون)، العقوبات المشار إليها في المواد من . . . إلى قانون الجزاء.

٤٣- في الدول العربية قد يكون من الأجدى عدم حصر تطبيق المواد بالقاصرين فقط، ذلك أن الإباحية والمواد الجنسية تعتبر محرمة وممنوعة قانوناً، إلا أن اعتماد نص المواد والباب الخامس على عبارة القاصرين كان بسبب ذكرها في النصوص القانونية المسترشد بها مثل معاهدة بودابست ٢٠٠١ ولسهولة العودة إلى المرجع.

نص إرشاد الجرائم السيبرانية

تحرص الدول الأعضاء على تجريم الأفعال التالية:

الباب الأول: جرائم التعدي على البيانات المعلوماتية

المادة ١: جرم التعرض للبيانات المعلوماتية

كل من أقدم قصداً بصورة غير مشروعة على تعديل أو إلغاء أو محو أو إفساد أو تدمير البيانات المعلوماتية. يجوز الاشتراط أن يتسبّب الفعل المذكور بأضرار جسيمة لاعتباره جرماً.

المادة ٢: جرم اعتراض بيانات معلوماتية

كل من أقدم قصداً بصورة غير مشروعة على اعتراض بيانات معلوماتية بوسائل تقنية وذلك عند نقلها غير المُتاح للجمهور من النظام المعلوماتي أو إلى داخله. ويجوز اشتراط أن يتم الفعل بنية جرمية أو بنية الربط مع أنظمة معلوماتية أخرى.

الباب الثاني: جرائم التعدي على الأنظمة المعلوماتية

المادة ٣: جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه

كل من أقدم قصداً على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه. ويجوز اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحمأي الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة أخرى جرمية أو في ما يتعلق بالربط مع أنظمة معلوماتية أخرى.

المادة ٤: جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية

كل من أقدم على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه مع قيامه بتعديل البيانات الرقمية أو البرامج أو إلغائها أو محوها أو إفسادها أو تدميرها أو المساس بعمل النظام المعلوماتي. ويجوز أيضاً اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحمأي الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة أخرى جرمية أو بنية الربط مع أنظمة معلوماتية أخرى.

المادة ٥: جرم إعاقة عمل نظام معلوماتي

كل من أقدم بنيّة الغش، وبأي وسيلة، على إعاقة عمل نظام معلوماتي أو على إفساده.

الباب الثالث: إساءة استعمال الأجهزة أو البرامج المعلوماتية

المادة ٦: جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية

كل من قدّم أو أنتج أو وزّع أو استورد أو صدر أو روّج أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلوماتية معدّة أو كلمات سر أو تراميز دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في الإرشاد الحاضر.

الباب الرابع: جرائم التعدي على الأموال والمعاملات

المادة ٧: جرم الاحتيال أو الغش بوسيلة معلوماتية

كل من أقدم عن قصد و بنيّة الغش وبصورة غير مشروعة على إلحاق ضرر مالي بالغير عن طريق:

إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية.

أي شكل من أشكال التعدي على عمل نظام معلوماتي.

وذلك للحصول دون وجه حق على منفعة مادية لنفسه أو للغير.

المادة ٨: جرم التزوير المعلوماتي

كل من أقدم عن قصد، وبصورة غير مشروعة، على إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، نتج عنها بيانات غير صحيحة، بقصد استخدامها، أو التعويل عليها في أغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر أو لا.

كل من أقدم عن قصد على استعمال البيانات المعلوماتية غير الصحيحة المذكورة في الفقرة الأولى.

المادة ٩: جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية
كل من أقدم على سرقة أموال أو على اختلاسها باستعمال وسيلة معلوماتية.

المادة ١٠: جرم أعمال التسويق والترويج غير المرغوب بها
كل من أقدم على إرسال رسائل ترويج أو تسويق غير مرغوب بها إلى الغير دون تمكين المُرسل إليهم من إيقاف ورود هذه الرسائل، في حال رغبوا بذلك، بدون أن يتحملوا أي نفقات إضافية.

المادة ١١: جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها
كل من أقدم على الاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر، والمستخدمة في نظام معلوماتي، وكذلك من أقدم عن قصد وبصورة غير مشروعة ومع علمه بالأمر على استخدام أدوات التعريف والهوية العائدة لشخص آخر في نظام معلوماتي.

المادة ١٢: جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها
كل من أقدم عن قصد ودون سبب مشروع على الاطلاع بوسائل معلوماتية على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. يجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة.

الباب الخامس: جرائم الاستغلال الجنسي للقاصرين[٤٣]

المادة ١٣: تعاريف
تشمل المواد الإباحية الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أي أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية:

- قاصر يقوم بفعل جنسي صريح.
- شخص يبدو كقاصر يقوم بفعل جنسي صريح.
- صور واقعية أو مصطنعة بالمحاكاة تظهر قاصراً يقوم بفعل جنسي صريح.

القاصر هو كل من لم يتم الثامنة عشرة من عمره. ويجوز لدولة عضو أن تخفض السن إلى حدود أدنى، لا تقل عن السادسة عشرة.

المادة ١٤: جرم إنتاج مواد إباحية لقاصرين بقصد بثها بواسطة نظام معلوماتي
كل من أنتج قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بقصد توزيعها أو بثها عبر نظام معلوماتي.

المادة ١٥: جرم عرض مواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من عرض أو وفر أو قدّم قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.

المادة ١٦: جرم توزيع أو بث أو نقل مواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من وزّع أو بثّ أو نقل قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.

المادة ١٧: جرم التزود أو تزويد الغير بمواد إباحية لقاصرين بواسطة نظام معلوماتي
كل من حصل قصداً، وبصورة غير مشروعة، على مواد إباحية لقاصرين عبر نظام معلوماتي لصالحه أو لصالح الغير.

المادة ١٨: جرم حيازة مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي
كل من حاز قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين على وسيطة إلكترونية أو نظام معلوماتي.

المادة ١٩: جرم تحريض القاصرين على أنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية
كل من شجّع أو حرّض قاصراً على القيام بأنشطة جنسية غير مشروعة سواء مجاناً أو بعوض أو ساهم في إعداده لهذا الأمر، وذلك بأي وسيلة معلوماتية.

المادة ٢٠: جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية
كل من أقدم على التحرش جنسياً بقاصر على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى، من أجل إشباع الرغبة الجنسية أو من أجل إقناع القاصر بالقيام بأنشطة جنسية سواء مجاناً أو بعوض.

الباب السادس: جرائم التعدي على الملكية الفكرية للأعمال الرقمية

المادة ٢١: جرم وضع اسم مختلس على عمل
كل من أقدم بقصد الغش على وضع اسم مختلس على عمل أدبي رقمي أو كلّف الغير بذلك.

المادة ٢٢: جرم تقليد إمضاء المؤلف أو ختمه
كل من قلّد بقصد الغش إمضاء المؤلف أو ختمه أو إشارته.

المادة ٢٣: جرم تقليد عمل رقمي أو قرصنة البرمجيات
كل من أقدم قصداً على تقليد عمل أدبي فني رقمي أو على قرصنة البرمجيات. ويعتبر نسخ البرمجيات من قبيل أفعال التقليد.

المادة ٢٤: جرم بيع أو عرض عمل مقلّد أو وضعه في التداول
كل من أقدم على بيع أو عرض للبيع أو وضع بالتداول أو قدّم قصداً عملاً أدبياً فنياً رقمياً مقلداً.

المادة ٢٥: جرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة
كل من أقدم قصداً على الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة المتعلقة بالأعمال الرقمية.

الباب السابع: جرائم البطاقات المصرفية والنقود الإلكترونية

المادة ٢٦: جرم تقليد بطاقة مصرفية
كل من أقدم قصداً بصورة غير مشروعة على تقليد بطاقة مصرفية.

المادة ٢٧: جرم استعمال بطاقة مصرفية مقلّدة
كل من أقدم قصداً، مع علمه بالأمر، على استعمال بطاقة مصرفية مقلّدة سواء حصل بنتيجة هذا الاستعمال على أموال أو لم يحصل لسبب لا يعود إليه. في حال استعمال عن قصد أرقام بطاقات مصرفية مسروقة أو الاستيلاء عليها تطبق أحكام المادة ١١.

المادة ٢٨: جرم قبول الإيفاء ببطاقة مصرفية مقلّدة
كل من قبِلَ إيفاءه مبلغاً من المال بواسطة بطاقة مصرفية مقلّدة مع علمه بحقيقتها.

المادة ٢٩: جرم تزوير النقود الإلكترونية
كل من أقدم عن قصد بصورة غير مشروعة على تزوير نقود إلكترونية.

الباب الثامن: الجرائم التي تمسّ المعلومات الشخصية

المادة ٣٠: جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص
كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص مسبق يتيح له القيام بمثل هذه المعالجة من المراجع الرسمية.

المادة ٣١: جرم معالجة معلومات ذات طابع شخصي دون احترام القواعد القانونية
كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون التقيد بالقواعد القانونية المقررة لمعالجة المعلومات ذات الطابع الشخصي.

المادة ٣٢: جرم إفشاء معلومات ذات طابع شخصي
كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات طابع شخصي، لأشخاص لا يحق لهم الاطلاع عليها.

المادة ٣٣: جرم عدم الاستجابة لطلب الشخص المعني بالاطلاع أو التصحيح
كل من يرفض بدون وجه حق الاستجابة في مهلة قصيرة إلى طلب الشخص المعني بالاطلاع على المعلومات ذات الطابع الشخصي الخاصة به أو بتصحيحها.

الباب التاسع: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية

المادة ٣٤: جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية
كل من أقدم قصداً على نشر وتوزيع معلومات تثير النعرات العنصرية وتهدف إلى التمييز العنصري بحق أشخاص معينين، وذلك بواسطة شبكة الإنترنت أو غيرها من الوسائل المعلوماتية.

المادة ٣٥: جرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية

كل من أقدم على تهديد شخص أو تحقيره أو التعدي عليه بسبب انتمائه العرقي أو المذهبي أو لونه، وذلك بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى.

المادة ٣٦: جرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية

كل من أقدم قصداً على توزيع أو نشر معلومات بواسطة شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.

المادة ٣٧: المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية

كل من ساعد قصداً أو حرّض بواسطة شبكة الإنترنت أو أي وسيلة معلوماتية أخرى شخصاً آخر على ارتكاب جرائم ضد الإنسانية.

الباب العاشر: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية

المادة ٣٨: جرم تملك وإدارة مشروع مقامرة على الإنترنت

كل من تملك أو أدار مشروع مقامرة أو عرض ألعاب مقامرة على شبكة الإنترنت أو بأي وسيلة معلوماتية أخرى.

المادة ٣٩: جرم تسهيل وتشجيع مشروع مقامرة على الإنترنت

كل من سهّل أو شجّع أو روّج لإنشاء مشروع مقامرة على شبكة الإنترنت أو باستعمال وسيلة معلوماتية أخرى.

المادة ٤٠: جرم ترويج الكحول للقاصرين على الإنترنت

كل من أقدم على ترويج الكحول مستهدفاً القاصرين على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤١: جرم ترويج المواد المخدرة على الإنترنت

كل من أقدم بصورة غير مشروعة على ترويج أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة على شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

الباب الحادي عشر: جرائم المعلوماتية ضد الدولة والسلامة العامة

المادة ٤٢: جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية

كل من أقدم على تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال أي وسيلة معلوماتية، وكل من أنتج أو وزع أو حاز برامج معدة لهذا الاستعمال.

المادة ٤٣: جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية

كل من امتنع عن قصد في الإبلاغ أو أبلغ عن قصد بشكل خاطئ عن جرائم المعلوماتية.

المادة ٤٤: جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة

كل من أقدم على الاطلاع أو على الحصول أو الاطلاع على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤٥: جرم العبث بالأدلة القضائية المعلوماتية

كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو تخبئتها أو التعديل فيها أو محوها.

المادة ٤٦: جرم بث بيانات تهدد الأمن والسلامة العامة بوسيلة معلوماتية

كل من أقدم على بث أو إذاعة أو نشر بيانات أو معلومات تهدد الأمن أو السلامة العامة في الدولة أو أي دولة أخرى، وذلك من خلال شبكة الإنترنت أو باستعمال أي وسيلة معلوماتية أخرى.

المادة ٤٧: جرم الإرهاب بوسيلة معلوماتية

كل من ارتكب أعمالاً إرهابية أو ساهم فيها أو حرّض عليها باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى.

المادة ٤٨: جرم التحريض على القتل بوسيلة معلوماتية

كل من أقدم على تحريض شخص آخر على القتل باستعمال شبكة الإنترنت أو أي وسيلة معلوماتية أخرى.

الباب الثاني عشر: جرائم تشفير المعلومات

المادة ٤٩: جرم عدم حيازة ترخيص أو تصريح عن تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير
كل من أقدم على توزيع أو تسويق أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة.

المادة ٥٠: جرم تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص
كل من أقدم على توفير وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل الجهات الرسمية المختصة في الدولة.

المادة ٥١: جرم بيع أو تأجير وسائل تشفير ممنوعة
كل من أقدم على بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

الباب الثالث عشر: العقوبات

المادة ٥٢: يُعاقب كل من يرتكب إحدى الجرائم المحددة في هذا الإرشاد بعقوبة السجن وبالغرامة أو بإحدى هاتين العقوبتين. يُترك للدولة المعنية تحديد مدة عقوبة السجن وقيمة الغرامة بحدّيها الأدنى والأعلى.

المادة ٥٣: تُصادر الأجهزة الإلكترونية وخلافها التي استعملت في ارتكاب الجرم.

المادة ٥٤: تُشدد العقوبة في حال التكرار وفقاً للقواعد العامة المنصوص عليها في قوانين الجزاء. ويتم إبعاد الأجنبي لارتكابه إحدى هذه الجرائم.

الباب الرابع عشر: هيئة متخصصة لمكافحة الجريمة المعلوماتية

المادة ٥٥: تحرص الدول العربية على إنشاء وحدة متخصصة في الجرائم المعلوماتية في الأجهزة الأمنية المولجة بالتحقيقات القضائية تحت إشراف القضاء، كالضابطة العدلية. تتولى هذه الوحدة أعمال التحقيق في الجرائم المعلوماتية ورصدها تحت إشراف القضاء. ويتألف الجهاز البشري لهذه الوحدة من عناصر فنية متخصصة ذات كفاءة في مجال المعلوماتية والاتصالات.

المادة ٥٦: التعاون الدولي
على الدول العربية احترام المعاهدات والاتفاقيات الدولية ذات الطابع الجماعي أو الثنائي المتعلقة بمكافحة الجرائم بشكل عام مع مراعاة طبيعة الجرائم السيبرانية، وذلك لجهة تسهيل وتسريع الإجراءات الخاصة بجمع الأدلة وضبطها وتبادل المعلومات حول الجرائم المذكورة وملاحقة مرتكبيها؛ كما وتحرص الدول العربية على التعاون فيما بينها في مجال التحقيقات القضائية في الجرائم المعلوماتية، وأعمال رصدها ومكافحته.

الإرشاد السادس

حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني

٦

الورقة البحثية الخلفية لإرشاد حماية حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني في الدول العربية، رصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية، تسلط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار قرارات أو تنظيمات خاصة تتعلق بحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

٢- موضوع وأقسام البحث

ينص مشروع إعداد «إرشادات الإسكوا للتشريعات السيبرانية» على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على «توجيهات الاتحاد الأوروبي» في هذا المجال لأجل صياغة الإرشاد الخاص بحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) الحماية القانونية لبرامج الحاسوب: تتناول الأحكام القانونية التي تنظم الحماية القانونية للبرامج المعلوماتية، لجهة السند القانوني للحماية والمستفيدون من الحماية وحقوق صاحب حق المؤلف ونطاق الحماية والاستثناءات على الحماية والتدابير لفرض الحماية.

٢) الحماية القانونية لقواعد البيانات: تتضمن القواعد القانونية التي تنظم الحماية القانونية لقواعد البيانات، وهي ترتكز إلى مؤسستين قانونيتين: الحماية بموجب حق المؤلف في حال توفر الابتكار، الحماية بموجب الحق الخاص بالاستثمار.

٣) الحماية القانونية للمنتجات شبه الموصلة: الأحكام القانونية التي تنظّم هذه الحماية لجهة شروط الحماية وصاحب الحق المحمي وحقوقه، ولجهة التسجيل لتكريس الحق ومدة الحماية، بالإضافة إلى الحقوق الحصرية التي تعود لصاحب الحق على طوبوغرافيا المنتج شبه الموصل وما تزوده من حقوق أخرى ضمن هذا المجال.

٤) الحماية القانونية للأعمال الرقمية الأخرى: تتناول المبدأ القانوني المُعتمد لحماية الأعمال الرقمية الأخرى التي لم تُوضع لها أحكام خاصة مثل البرامج وقواعد البيانات والمنتجات شبه الموصلة.

٥) الحماية القانونية لأسماء المواقع: تتناول القواعد القانونية التي تطبق على أسماء المواقع لجهة المرجع الصالح لمنح أسماء المواقع ومسؤوليته والشروط الإدارية والمالية المطلوبة لذلك وإجراءات التسجيل ومحاذيره وإلغاء، إثم الموقع وفصل النِزاعات المتعلقة بأسماء المواقع.

وتناولت أعمال البحث أيضاً أنواع البرمجيات وكيفية صناعتها ومنهجياتها بالإضافة إلى أنواع قواعد البيانات ومكوناتها، والحماية القانونية المتوفرة لكل منها فشملت الأعمال التالية:

- **الأنواع الرئيسية لبرامج الحاسوب**[1] ، وأهمها أنظمة التشغيل (System software/Operating system)، ولغة البرمجيات أو الأنظمة المعدة للصناعة (Programming software/programming languages)، بالإضافة إلى الأنظمة التطبيقية (Application software)؛

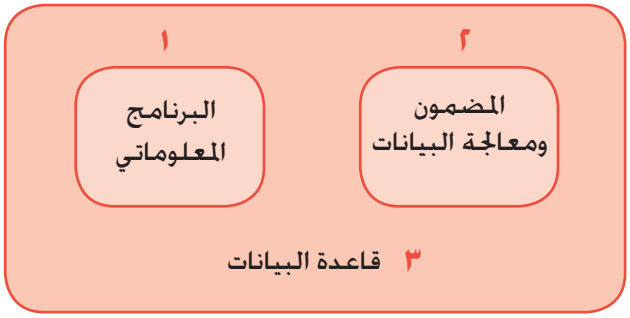
- **الحماية القانونية:** من المفيد الإشارة إلى أن الاتحاد الأوروبي يميز بين نوعين من الحماية القانونية لبرمجيات الحاسوب حيث يقسمها إلى: النوع المحمي بموجب قوانين حماية حق المؤلف والنوع المحمي بموجب قانون براءات الاختراع، وهذا النوع الأخير يتعلق بالبرمجيات التي لديها مفعول تقني أو صناعي أي التي تؤدي دوراً تقنيا أو صناعياً.

- **كيفية صناعة البرامج ومراحل بناء النظام البرمجي:** بناء النظام البرمجي ليس مجرد كتابة شفرة، وإنما هو عملية إنتاجية لها عدة مراحل أساسية وضرورية للحصول على المنتج: ١- كتابة وثيقة الشروط الخارجية والداخلية:

٢- التحليل، وهو عملية تجميع المعلومات بدقة، وتحديد المتطلبات والمهام التي سيقوم بها البرنامج، وتوصف هذه المهام بدقة تامة، كما تدرس الجدوى المرجوة من البرنامج؛ ٣- التصميم، أي تقسيم البرمجية إلى كتل وتعريف العلاقات بين هذه الكتل ثم وضع الخوارزميات الملائمة لكل كتلة؛ ٤- الترميز أي تحويل الخوارزميات إلى إحدى اللغات البرمجية، وتحويلها إلى لغة الآلة التي يتعامل بها جهاز الحاسوب فقط؛ ٥- الاختبار والتكاملية، وهي عملية تجميع الكتل مع بعضها واختبار النظام للتأكد من موافقته لجدول الشروط والمواصفات، وخاصة إذا كانت الكتل قد كتبت من قبل عدة أعضاء في الفريق؛ ٦- التوثيق وهو مرحلة هامة من مراحل بناء النظام البرمجي حيث يتم توثيق البناء الداخلي للبرنامج، وذلك بغرض الصيانة والتطوير. وهناك أكثر من طريقة للتوثيق: -توثيق المبرمج وهو ممكن أن يجري بإضافة تعليقات داخل الشفرة البرمجية، -توثيق المحلل بكتابة مستندات شرح لدورة البرنامج المستندية وخلافه،- توثيق مختبر النظام وفيها يتم تسجيل نقاط الخلل في البرنامج. ٧- الصيانة والتطوير وهي المرحلة الأطول في حياة النظام البرمجي لبقاء النظام قادراً على مواكبة التطورات والمعدات الحديثة. إن جزءاً من هذه المرحلة يكون في تصحيح الأخطاء، والجزء الآخر يكون في التطوير وإضافة تقنيات جديدة.

- **أنواع قواعد البيانات:** تأخذ قواعد المعلومات أشكالاً متنوعة: كالموسوعات العامة والمتخصصة المتكونة من نصوص وأصوات ورسوم بيانية وصور ثابتة ومتحركة، والصحف الإلكتروني وغيرها.

- **مكونات قواعد البيانات:** تتألف قواعد البيانات من ثلاثة عناصر رئيسية: العنصر الأول هو المكون من البرنامج الذي كان في أساس بناء قاعدة البيانات؛ العنصر الثاني هو مضمون ومعالجة البيانات المخزنة في قاعدة البيانات؛ والعنصر الثالث هو قاعدة البيانات المكونة من العنصر الأول والعنصر الثاني مجموعين. وبالتالي يمكن اعتبار كل مكوّن جزءاً مستقلاً، والعناصر الثلاثة مجتمعة جزءاً واحداً، وهو ما يعرف بقاعدة البيانات.



- **حماية قواعد البيانات:** منح الإرشاد الأوروبي حماية مزدوجة لقواعد البيانات، فمنح أولاً الحماية للبرنامج المعلوماتي المكونة منه قاعدة البيانات، و/أو اختيار وتنسيق المواد والمعلومات المجمعة أذا كان في هذا الاختيار أو التنسيق ابتكاراً يقتضي الحماية الكلاسيكية المنصوص عليها في قوانين حماية الملكية الفكرية، ومنح ثانياً مضمون قاعدة البيانات الحماية بموجب الحق الخاص «sui generis» حيث تشمل هذه الحماية عنصر الاستثمار الذي يتطلب توظيفات مالية و/أو مجهود العنصر البشري، بالإضافة إلى الوقت والطاقة.

وأبرز ما تناوله البحث الأعمال التالية:

١) الوثائق الرسمية الأساسية الصادرة عن المجلس الأوروبي المتعلقة بهذا المجال ومنها:

- Directive 2009/24/EC of the European Parliament and of the council of 23 April 2009 on the legal protection of computer programs

- Directive 2001/29/EC of the European Parliament and of the council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society

- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

- Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products

- Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property

- Council Decision 96/644/EC of 11 November 1996 on the extension of the legal protection of topographies of semiconductor products to persons from the Isle of Man [Official Journal L 293 of 16.11.1996]

- Council Decision 94/824/EC of 22 December 1994 on the extension of the legal protection of topographies of semiconductor products to persons from a Member of the World Trade Organization [Official Journal L 349 of 31.12.1994]

- Council Decision 94/700/EC of 24 October 1994 on the extension of the legal protection of topographies of

- Protection of Computer Software - A Synopsis of Intellectual Property Rights
http://www.gillhams.com/articles/174.cfm

- An Empirical Analysis of Patent Litigation in the Semiconductor Industry, By Bronwyn H. Hall, and Rosemarie Ham Ziedonis , January 2007
http://www.econ.berkeley.edu/~bhhall/papers/HallZiedonis07_PatentLitigation_AEA.pdf

- The Anticybersquatting Consumer Protection Act—An Offensive Weapon for Trademark Holders, by W. Chad Shear
http://www.jltp.uiuc.edu/recdevs/shear.pdf

- 2009 Update: International Legal Protection for Software Chart, by International Legal Protection for software
http://www.softwareprotection.com/chart.htm#EAPC

- Database protection in the USA, by Arnoud Engelfriet
http://www.iusmentis.com/databases/us/

- Legal theories of database protection: United States, Prof. Laura Gasaway's Cyberspace Law course at the UNC School of Law for Spring, 2006
http://www.unc.edu/courses/2006spring/law/357c/001/projects/dougf/node3.html

- Ultra Rapid semiconductor protection fuses, westcode catalogue, March 2005
http://www.westcode.com/fuses.pdf

- Chip Protection in Europe, by Dr. Thomas Hoeren,
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf

- Protecting High Value Domains, SSAC Public Meeting ICANN Cairo 2008,
http://cai.icann.org/files/meetings/cairo2008/piscitello-high-value-domains-03nov08.pdf

- Intellectual property the internet and Electronic Commerce, Legal protection of Domain
Names, by Mr. George Dimitrov, 2001
http://www.wipo.int/edocs/mdocs/ip-conf-g/en/wipo_ectk_sof_01/wipo_ectk_sof_01_1_6.doc

- Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions, ICANN, 12 July 2005
http://www.icann.org/en/announcements/hijacking-report-12jul05.pdf

- How To Protect Yourself Against Domain Name Hijackers
http://securityskeptic.typepad.com/the-security-skeptic/how-to-protect-yourself-against-domain-name-hijackers-.html

semiconductor products to persons from Canada [Official Journal L 284 of 01.11.1994]

- Council Decision 93/520/EEC of 27 September 1993 amending Decision 93/16/EEC on the extension of the legal protection of topographies of semiconductor products to persons from the United States of America and certain territories [Official Journal L 246 of 02.10.1993]

- Council Decision 93/16/EEC of 21 December 1992 on the extension of the legal protection of topographies of semiconductor products to persons from the United States of America and certain territories [Official Journal L 11 of 19.01.1993].

٢) وتناولت أعمال البحث أيضاً مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم الاتصالات الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، الفنلندية، السويسرية، والبريطانية، بالإضافة إلى بعض التشريعات الخاصة من دول أسيا الوسطى.

٣) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية والعربية الخاصة بالاتصالات الإلكترونية وحرية التعبير وخصوصية البيانات:

- Intellectual Property Rights on the Internet, by Stuart P. Meyer
http://www.fenwick.com/docstore/publications/ip/ip_rights_on_the_internet.pdf

- Examination Guidelines for Computer-Related Inventions, Patent and Trademark Office United States Department of Commerce
http://www.uspto.gov/web/offices/pac/dapp/pdf/ciig.pdf

- Patents for Computer Implemented Inventions and Business Methods, May 2006 Donald M. Cameron, R. Scott MacKendrick and Yuri Chumak Ogilvy Renault LLP, Toronto
http://www.jurisdiction.com/itpatents.pdf

- Study on Intellectual Property Rights, the Internet, and Copyright, by Alan Story
http://www.iprcommission.org/papers/pdfs/study_papers/sp5_story_study.pdf

- Intellectual Property Rights Violations: Federal Civil Remedies and Criminal Penalties Related to Copyrights, Trademarks, and Patents, Updated October 31, 2008, by Brian T. Yeh Legislative Attorney, American Law Division
http://www.fas.org/sgp/crs/misc/RL34109.pdf

- EU protection for domain names, 22 September 2008, http://www.neurope.eu/articles/89831.php#

- The Law and Economics of Reverse Engineering, Written by Pamela Samuelson and Suzanne Scotchmer, 30 April 2002, available: http://www.yalelawjournal.org/the-yale-law-journal/content-pages/the-law-and-economics-of-reverse-engineering/

- محاضرات الدكتور وسيم حرب – الدراسات العليا في القانون، كلية الحقوق-الجامعة اللبنانية، ١٩٩٥- ٢٠٠٥، مكتب المحاماة والاستشارات القانونية والتحكيم.

- ورقة عمل تشريعي نموذجي لحماية الملكية الفكرية، د. مها بخيت، رئيسة وحدة الملكية الفكرية، مكتب الأمين العام لجامعة الدول العربية
http://www.carjj.org

- اللائحة التنفيذية المعدلة لنظام براءات الاختراع لدول مجلس التعاون الخليجي، مكتب براءة الاختراعات بدول مجلس التعاون الخليجي
http://www.mawhopon.net/Tips-for-innovators/1708-html

- حماية الملكية الفكرية في البيئة الرقمية من خلال منظور الأساتذة الجامعيين: أساتذة جامعة منتوري نموذجاً
http://www.journal.cybrarians.info/

- حماية برامج الكمبيوتر وقواعد البيانات، تأليف طوني عيسى، ١٩٩٩
http://www.lipa-lb.org/myFiles/itemsFiles/computer%20program.pdf

٤) وقد تم الاسترشاد أيضاً بالدراسات التي أعدتها منظمة الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق، ٢- وضع التشريعات السيبرانية في سلطنة عمان، دولة الإمارات العربية المتحدة، دولة قطر، ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٥) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا الخاصة بحماية حقوق الملكية وبراءات الاختراع، والقوانين العربية الاسترشادية الخاصة بحماية حقوق المؤلف والحقوق المجاورة بالإضافة إلى ورقة العمل التشريعي النموذجي لحماية الملكية الفكرية.

٦) هذا بالإضافة إلى المعاهدات والاتفاقات الدولية الخاصة بحماية حقوق الملكية الفكرية في ما يتخطى النطاق الوطني، ومنها ما هو سابق للتطور الرقمي ومنها ما هو لاحق، مثل: اتفاقية باريس لحماية الملكية الصناعية (١٨٨٣)؛ اتفاقية برن لحماية المصنفات الأدبية والفنية (١٨٨٦)؛ معاهدة الوايبو للملكية الفكرية؛ اتفاقية تريبس (منظمة التجارة العالمية).

والاتفاقية العربية الخاصة بحماية حقوق المؤلف والمنشورة على الموقع الخاص:
http://e-lawyerassistance.com/LegislationsPDF/InternationalConventions/ArabConventionForTheProtectionOfIntellectualPropertyAr.pdf

تجدر الإشارة من ناحية أخرى إلى انه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم الملكية الفكرية في المجال المعلوماتي والسيبراني، ومقارنتها مع التشريعات الأجنبية لمعرفة مدى شموليتها للنقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني:

تبين أثناء أعمال البحث أن معظم الدول العربية عملت على إصدار تشريعات خاصة لتنظيم الملكية الفكرية وهي التالية:

١- الأردن:
- قانون حماية حق المؤلف والحقوق المجاورة رقم ٢٢/ ١٩٩٢
- قانون براءات الاختراع رقم ٣٢ لسنة ١٩٩٩
http://www.mit.gov.jo/

٢- الإمارات العربية المتحدة:
- قانون حقوق المؤلف والحقوق المجاورة رقم ٧ لسنة ٢٠٠٢
http://portal.unesco.org/culture/fr/files/39522124937588873/uae_copyright_2002_ar.pdf/uae_copyright_2002_ar.pdf

- قانون براءات الاختراع والنماذج الصناعية الإماراتية رقم ٤٤ لسنة ١٩٩٢
http://www.arabruleoflaw.org/compendium/Files/UAEpdf.39

٣- البحرين:
- قانون رقم (٢٢) لسنة ٢٠٠٦ بشأن حماية حقوق المؤلف والحقوق المجاورة
http://www.gcc-legal.org/mojportalpublic/BrowseLawOption.aspx?LawID=3740&country=6
- قانون رقم (١) لسنة ٢٠٠٤ بشأن براءات الاختراع ونماذج المنفعة
http://www.legalaffairs.gov.bh/viewhtm.aspx?ID=K0104

٤- سوريا:
- قانون حماية حق المؤلف رقم ١٢ الصادر عام ٢٠٠١
http://www.arabpip.org/arablaws_syr_authr.htm
- قانون براءة الاختراع

٥- العراق:
- قانون حماية حق المؤلف رقم (٣) لسنة ١٩٧١
- قانون براءة الاختراع والنماذج الصناعية رقم (٦٥) لسنة ١٩٧٠
http://www.iraq-ild.org/

٦- السعودية:
- قانون حماية حق المؤلف لسنة ٢٠٠٣
- قانون براءات الاختراع السعودي رقم – م/٣٨ التاريخ – ١٤٠٩/٦/١٠ هـ
http://ashrfmshrf.wordpress.com

٧- سلطنة عمان:
- قانون حماية حقوق المؤلف والحقوق المجاورة رقم ٣٧ لسنة ٢٠٠٠
- مرسوم سلطاني رقم ٢٠٠٠/٨٢ بإصدار قانون براءات الاختراع
http://portal.unesco.org/culture/en/files/39500124929722183Om_copyright_2000_ar.pdf/Om_copyright_2000_ar.pdf

٨- فلسطين:
http://www.pogar.org/publications/other/laws/media/telecomm-pal-05-a.pdf

٩- قطر:
- قانون رقم ٧ لسنة ٢٠٠٢ بشأن حماية حق المؤلف والحقوق المجاورة
http://e-lawyerassistance.com/LegislationsPDF/qatar/CopyrightLawAr.pdf

١٠- الكويت:
مرسوم بقانون رقم٥ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية
http://www.gcc-legal.org/mojportalpublic/BrowseLawOption.aspx?country=1&LawID=2996

١١- لبنان:
- قانون حماية الملكية الفكرية والفنية رقم ١٩٩٩/٧٥
- قانون براءات الاختراع رقم ٢٤٠ لسنة ٢٠٠٠
- تعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥ حول حماية برامج المعلوماتية ومكافحة القرصنة
http://www.economy.gov.lb/

١٢- مصر:
- قانون رقم ٨٢ لسنة ٢٠٠٢ ولائحته التنفيذية والخاص بحماية حقوق الملكية الفكرية
www.aproarab.org/Down/Egypt/59.doc

١٣- اليمن:
- قانون حماية الملكية الفكرية رقم ١٩ لسنة ١٩٩٤
http://www.legalaffairs.gov.ye

ب- شمولية التشريعات الوطنية الخاصة

لا بد من الإشارة إلى أن بعض التطورات الملحوظة في بعض التشريعات العربية الحديثة من ناحية المعاملات والتجارة الإلكترونية لم تنسحب إلى تنظيم كامل لحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني إلا بشكل بسيط جداً اقتصر على تعديل القوانين الموجودة المتعلقة بحماية حقوق المؤلف والحقوق المجاورة، حيث عملت على إدخال برامج الحاسوب وقواعد البيانات من ضمن لائحة المصنفات المحمية بموجب قانون حماية حقوق المؤلف.

وهنا لا بد من الإشارة إلى أن جميع الدول العربية نظمت حماية البرامج المعلوماتية وقواعد البيانات ضمن القوانين الخاصة بحماية حقوق المؤلف والحقوق المجاورة، ونذكر منها على سبيل المثال:

- **الإمارات العربية المتحدة:** قامت دولة الإمارات العربية المتحدة بتوفير الحماية القانونية لبرامج الحاسوب وقواعد البيانات وذلك ضمن قانون حقوق المؤلف والحقوق المجاورة

رقم ٧ لسنة ٢٠٠٢ وحددتها في المادة ٢ المتعلقة بنطاق الحماية، حيث نصت على «٢- برامج الحاسب وتطبيقاتها ، وقواعد البيانات ، وما يماثلها من مصنفات تحدد بقرار من الوزير»، الحقوق الأدبية للمؤلف المتعلقة ببرامج الحاسوب وقواعد البيانات وذلك في المواد (٨، ١٢، ٢٢). كما وفرضت عقوبات على « تحميل أو تخزين الحاسب بأية نسخة من برامج الحاسب أو تطبيقاته أو قواعد البيانات دون ترخيص من المؤلف أو صاحب الحق أو خلفهما» في المادة ٣٨.

- **البحرين:** نظمت البحرين الحماية القانونية لقواعد المعلومات وبرامج الحاسوب ضمن قانونها رقم (٢٢) لسنة ٢٠٠٦ بشأن حماية حقوق المؤلف والحقوق المجاورة، حيث نصت المواد (٢،٣،٦،٧،٨،٩،١٠) على الحماية القانونية لقواعد البيانات، والمواد (٢،٦، ١٩، ٢٠، ٢١، ٢٦) على حماية برامج الحاسوب. كما وقد أفردت البحرين ضمن قانونها رقم ١٣ لسنة ٢٠٠٦ الخاص بتعديل بعض أحكام المرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ بشان المعاملات الإلكترونية، مادة خاصة (م ١) بحماية أسماء النطاق.

- **سوريا:** عملت سوريا أيضاً على تنظيم قواعد البيانات وبرامج الحاسوب ضمن قانونها رقم ١٢ لعام ٢٠٠١ المتعلق بحماية حقوق المؤلف، فقد نصت المواد (٣، ٩، ١٠) على الحماية القانونية لقواعد البيانات، والمواد (٣،٥،٦،٨،١٠،٢١،٤١) على حماية برامج الحاسوب.

- **سلطنة عمان:** نظمت سلطنة عمان حماية البرامج المعلوماتية وقواعد البيانات ضمن قانونها الخاص بحماية حقوق المؤلف والحقوق المجاورة رقم ٣٧ لسنة ٢٠٠٠، فنصت المادة ٣ على الحماية القانونية لقواعد البيانات، والماد ٢ على حماية برامج الحاسوب.

- **قطر:** كذلك الأمر بالنسبة لقطر، التي نظمت موضوع الحماية القانونية لقواعد البيانات في المواد (٣) وحماية برامج الحاسوب في المادة ٢ من قانون رقم (٧) لسنة ٢٠٠٢ بشأن حماية حق المؤلف والحقوق المجاورة.

- **مصر:** تناولت مصر الحماية القانونية لقواعد البيانات ونظمتها في المواد (١٣٨،١٤٠) وبرامج الحاسوب في المواد القانونية (١٣٨،١٤٠،١٤٧) من قانون حماية الملكية الفكرية المصري رقم ٨٢ لسنة ٢٠٠٢.

إن هذا الأمر ينطبق على الدول العربية الأخرى (الكويت، لبنان، والأردن) التي قامت بتعديل قوانينها الخاصة لتوفير الحماية القانونية لقواعد البيانات والبرامج المعلوماتية، باستثناء العراق حيث لم نجد أي نص من شأنه حماية قواعد البيانات أو برامج الحاسوب. وقد تبين لنا أن فلسطين هي بصدد إعداد مشروع قانون جديد لحماية حقوق المؤلف والحقوق المجاورة.

وقد نجد بعض القوانين الخاصة بحماية برامج الحاسوب والمنتجات شبه الموصلة. فقد أفرد لبنان مثلا نصاً خاصاً لحماية برامج المعلوماتية وهو التعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥ الخاص بحماية برامج المعلوماتية ومكافحة القرصنة. كما أفرد لبنان ضمن قانون براءة الاختراع رقم ٢٤٠ لسنة ٢٠٠٠ باباً ثالثاً خاصاً بتنظيم المنتجات شبه الموصلة، ينظم إيداع هذه المنتجات والحقوق الناشئة عن الإيداع وكيفية انتقالها وسقوطها.

كما قد ورد صراحةً في بعض قوانين الدول العربية الحديثة المتعلقة ببراءات الاختراع، أن برامج الحاسوب لا تعتبر من قبيل الاختراعات التي تحمى بموجب قانون براءات الاختراع، ونذكر منها على سبيل المثال: سلطنة عمان، التي اعتبرت ضمن مرسومها السلطاني رقم ٢٠٠٠/٨٢ الخاص بإصدار قانون براءات الاختراع أن برامج الحاسوب لا تعد من قبيل الاختراعات وبالتالي فهي لا تخضع للحماية التي يؤمنها هذا القانون، حيث نصت المادة (٤): «لا يعد من قبيل الاختراعات في مجال تطبيق أحكام هذا القانون ما يلي:

أ - النظريات العلمية والطرق الرياضية وبرامج الحاسوب، وممارسة الأنشطة الذهنية المحضة وممارسة لعبة من الألعاب.

وسوريا، التي حددت في المادة ٢ من قانون براءات الاختراع، أنه لا تمنح براءة الاختراع للتصاميم وقواعد المناهج المتعلقة بميدان البرامج المعلوماتية.

نتيجة لما تقدم، يمكننا استخلاص النقاط التالية:

١- إن تشعب المجالات المتعلقة بحماية حقوق الملكية الفكرية في المجال الرقمي أدى إلى تبسيط لنطاق الحماية بتطبيق نفس الحماية القانونية للمصنفات الأدبية والفنية من خارج المجال الرقمي على المجال الرقمي: قواعد البيانات، وبرامج الحاسوب.

مثال على ذلك: (١) المادة ٢ من القانون رقم ٩٩/٧٥، لبنان: الأعمال المشمولة بالحماية: برامج الحاسوب مهما كانت غاياتها بما في ذلك الأعمال التحضيرية: (٢) قانون رقم ٨٢

عام، ٢٠٠٢ جمهورية مصر العربية، المواد ١٤٠،١٤٧، ١٥٧، ١٥٨.

٢- لا نجد في القوانين العربية قواعد قانونية متخصصة تتعلق بالحماية القانونية في المجال الرقمي مثل منع الولوج إلى قواعد البيانات ومنع فك التشفير بطرق غير قانونية، أو تحديد أساليب نقل المصنفات ونسخها بين النظراء على الخط peer-to-peer. يترك هذا الأمر عادةً لتقدير المحاكم على الرغم من صعوبة الإثبات وصعوبة التجريم لعدم توافر نصوص صريحة وأدلة يمكن الركون إليها. ويُعتمد مبدأ القياس في كل حال.

٣- غياب أو عدم اكتمال التشريعات المتخصصة في مجال حماية مواقع الإنترنت ذات الترميز الوطني ccTLD.

٤- نقص الخبرة في مجال الإثبات والتخصص من قبل خبراء المحاكم وسلطات التحقيق العدلية.

٥- غياب التشريع المتخصص حول حماية العلامات التجارية في المجال الرقمي، مثل: منع استعمال العلامات التجارية خاصة الغير كأسماء مواقع الإنترنت، وعدم استعمال العلامات في الإعلانات، ومنع الإعلانات الأوتوماتيكية.

٦-عدم وجود قواعد قانونية ناظمة لتسجيل أسماء المواقع ذات الترميز الوطني. مثل لبنان: لا يوجد نص حول إلزامية تسجيل اسم الموقع كعلامة تجارية في الفئة ٣٥ من التصنيف الدولي.

هوامش

1- Types of software, available:
http://www.computing.net/answers/windows-xp/types-of-software/175673.html
Practical computer systems divide software systems into three major classes: system software, programming software and application software, although the distinction is arbitrary, and often blurred.

- System software: helps run the computer hardware and computer system. It includes: device drivers, operating systems, servers, utilities, windowing systems.
The purpose of systems software is to unburden the applications programmer from the details of the particular computer complex being used, including such accessory devices as communications, printers, readers, displays, keyboards, etc. And also to partition the computer's resources such as memory and processor time in a safe and stable manner.

- Programming software: Programming software usually provides tools to assist a programmer in writing computer programs, and software using different programming languages in a more convenient way. The tools include: compilers, debuggers, interpreters, linkers, text editors.
An Integrated development environment (IDE) is a single application that attempts to manage all these functions.

- Application software: Application software allows end users to accomplish one or more specific (not directly computer development related) tasks. Typical applications include: industrial automation, business software, computer games, telecommunications, (ie the internet and everything that flows on it) databases, educational software, medical software, Application software exists for and has impacted a wide variety of topics.

٢- راجع لائحة تشريعات الدول الأجنبية – ملحق رقم ٣.

مقدمة إرشاد الملكية الفكرية في المجال المعلوماتي والسيبراني

أدى التطور التقني الحديث المتمثل بالاستعانة بالحواسيب وما يمكن أن تخزنه من بيانات ومراجع والوظائف التي يمكن أن تقوم بها هذه الحواسيب، إلى ظهور إنتاج بشري فكري من نوع جديد. فمؤلف العمل الرقمي سواء أكان هذا العمل برنامجاً للحاسوب أو قاعدة بيانات أو تصميماً هندسياً جديداً، لم يعد نتيجة عمل فرد واحد ولم يعد بالإمكان نسبة هذا العمل إليه بمجرد توقيعه له. فالتعقيد المتمثل بعدد المبتكرين العاملين على برنامج واحد مثلاً ودور كل منهم والجديد الذي أتاه كل منهم في العمل، ألزم المشترع بضرورة حماية الأعمال الرقمية من التعدي. ولذا كان لا بد من أن تنزل الأعمال الرقمية منزلة الأعمال الذهنية الجديدة والمبتكرة لأجل حمايتها بواسطة قوانين حماية الملكية الفكرية.

إلا أن مجرد حماية الأعمال الرقمية من برامج وقواعد بيانات وخلافه بموجب قوانين حماية الملكية الفكرية على اعتبارها أعمالاً ذهنية لا يكفي بدون مراجعة تلك التشريعات والحرص على ملاءمتها لتشمل تلك الأعمال.

من هنا قامت الدول الغربية في بادئ الأمر بوضع تشريعات جديدة للملكية الفكرية الخاصة بالأعمال الرقمية وأعادت النظر تعديلاً وإضافةً ببعض القوانين الأخرى.

إلا أن المشكلة القانونية الأبرز في هذا السياق كانت متمثّلة بالتعديات العابرة للحدود على الأعمال الرقمية. من هنا فقد كان لا بد من توسيع نطاق تطبيق المعاهدات الدولية الخاصة بحماية الملكية الفكرية لتشمل الأعمال الرقمية[1].

لقد أدى تطور تقنيات البرمجيات وتنامي شبكة الإنترنت وإدخال المعلوماتية إلى جميع النشاطات البشرية إلى تعاظم الإنتاج من البرامج وقواعد البيانات والأعمال الرقمية الأخرى والمنتجات شبه الموصلة[2]. ومن المعروف أن الوظائف المؤداة من قبل المنتجات شبه الموصلة تتعلق بشكل أساسي بطوبوغرافيا هذه المنتجات. وقد ساهمت المعلوماتية والتكنولوجيا المُرتكزة على المنتجات شبه الموصلة بشكل مباشر في دفع الاقتصاد في الدول كافة، ومن بينها الدول العربية، حتى ظهر ما يُعرف بالاقتصاد الرقمي. لذلك، عملت مختلف الدول منذ البداية على تشجيع هذا الاقتصاد الرقمي وصناعة البرمجيات والمنتجات شبه الموصلة وعلى إيجاد سبل لحمايتها[3].

إن هذا الإنتاج الرقمي، غالباً ما يتطلب نشاطاً ذهنياً مميزاً فردياً ولمحة شخصية من قبل المنتج أو المُبتكر، أو غالباً ما يستلزم توظيف ضخمة على صعيد رؤوس الأموال أو الموارد المالية والبشرية والتقنية المُستعملة. في مقابل ازدياد حجم الإنتاج الرقمي، تضاعفت أيضاً أعمال التعدي على هذا الإنتاج والنسخ غير المشروع عنه، تبعاً للإمكانات التقنية التي توفرها المعلوماتية، كسهولة النسخ (دون كلفة تقريباً وبوقت قصير جداً)، وسهولة التحميل من الإنترنت، وإمكانية حفظ كمية هائلة من المعلومات على دعامة إلكترونية تُحمل في الجيب، واتساع الفضاء السيبراني أو الإنترنت وانتفاء المركزية والمرجعية القانونية فيه وضعف الرقابة عليه.

إن أعمال التعدي الحاصلة على حقوق أصحاب البرامج وقواعد البيانات والأعمال الرقمية لا يحفز بطبيعة الحال ازدهار هذا القطاع وتشجيع الاستثمار فيه. ويقتضي بالتالي فرض حماية قانونية فعّالة، تشكل رادعاً للمنتهكين وحافزاً للمؤلفين ولأصحاب الحقوق لتطوير منتجاتهم ومبتكراتهم. كما يجب أن تكون هذه الحماية منسقّة بين الدول بالنظر لتجاوز الانتهاكات الحدود الوطنية، ولاسيما على شبكة الإنترنت، مما يفرض أن تكون التشريعات الوطنية متجانسة أو على الأقل مُستندة إلى المبادئ القانونية ذاتها. وهذه الحماية القانونية قد تستند إلى حماية حق المؤلف المعروفة في قوانين الملكية الأدبية والفنية، إذا توفر شرط الحماية ألا وهو الابتكار، كما قد تستند إلى مؤسسات قانونية أخرى، وهي خاصة بالقطاع الرقمي والمعلوماتي كالحماية بموجب الحق الخاص[4] الذي جاء به الإرشاد الأوروبي رقم ١٩٩٦/٩ تاريخ ١٩٩٦/٣/١١ المتعلق بالحماية القانونية لقواعد البيانات. بطبيعة الحال، قد تطبق الأحكام القانونية المتعلقة بالملكية الأدبية والفنية في مجال حماية البرامج المعلوماتية وقواعد البيانات التي تستوفي شرط الابتكار[5]، إلا أنه بالنظر للخصائص التقنية للبرامج المعلوماتية ولقواعد البيانات والأعمال الرقمية، فإن الإرشاد الحالي يأتي بأحكام قانونية إضافية وخاصة لتطبق في هذا المجال.

يأتي هذا الإرشاد حول حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني ليشكل إطاراً قانونياً متكاملاً في هذا المجال. وقد تم الاسترشاد بالإرشاد الأوروبي رقم ٢٠٠٩/٢٤ تاريخ ٢٠٠٩/٤/٢٣ المتعلق بالحماية القانونية لبرامج الحاسوب أو للبرامج المعلوماتية، وبالإرشاد الأوروبي رقم

٢٠٠١/٢٩ تاريخ ٢٠٠١/٥/٢٢ المتعلق بتنسيق بعض جوانب حق المؤلف والحقوق المجاورة في مجتمع المعلومات، لاسيما لناحية التدابير التقنية لحماية الأعمال، وكذلك بالإرشاد الأوروبي رقم ١٩٩٦/٩ تاريخ ١٩٩٦/٣/١١ المتعلق بالحماية القانونية لقواعد البيانات، وبالقوانين الوطنية في هذا المجال، وذلك لتحضير أحكام الإرشاد الحالي الذي يتوجه إلى الدول العربية في موضوع حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

كما وتم الاسترشاد أيضاً بالاتفاقيات والمعاهدات الدولية المتعلقة بهذا الموضوع وأهمها اتفاقية برن لحماية الملكية الأدبية والفنية المعدلة في ٢٨ سبتمبر ١٩٧٩، ومعاهدة الوايبو بشأن حق المؤلف، المعتمدة في جنيف بتاريخ ٢٠ ديسمبر١٩٩٦، واتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس) لسنة ١٩٩٤ ، بالإضافة إلى معاهدة IPIC (المتعلقة بحماية المنتجات شبه الموصلة و Integrated circuits).

لقد تم تقسيم القانون الاسترشادي المُقترح على سبعة أبواب تتناول مختلف جوانب حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: الحماية القانونية لبرامج الحاسوب (البرامج المعلوماتية).
الباب الثالث: الحماية القانونية لقواعد البيانات.
الباب الرابع: الحماية القانونية للمنتجات شبه الموصلة.
الباب الخامس: الحماية القانونية للأعمال الرقمية الأخرى.
الباب السادس: الحماية القانونية لأسماء المواقع.
الباب السابع: أحكام مشتركة.

شروحات حول الإرشاد المتعلق بحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني

يتضمن **الباب الأول** المعنون « أحكام عامة» تعاريف لبعض المصطلحات التقنية والمفاهيم المُستعملة في نص الإرشاد. وتضع المادة ١ من الإرشاد تعاريف للمنتج شبه الموصل الذي هو الشكل النهائي أو الوسيط لكل منتج يكون مؤلفاً من جوهر يتضمن طبقة من مواد شبه موصلة، ومكوّناً من طبقة أو عدة طبقات أخرى من مواد موصلة وعازلة أو شبه موصلة، وتكون الطبقات مرتبة وفقاً لخريطة ذات أبعاد ثلاثية معينة، ويكون المنتج معدّاً للقيام حصرياً أو بصورة غير حصرية بوظيفة إلكترونية. وتعرف المادة ١ طوبوغرافيا المنتج شبه الموصل، بأنها سلسلة صور مربوطة ببعضها، أياً كانت المادة المُثبّتة أو المُرمّزة بواسطتها، وهي تمثّل الخريطة الثلاثية الأبعاد للطبقات التي تشكّل منتجاً شبه موصل، حيث تمثّل كل صورة الرسم أو جزءاً من الرسم العائد لسطح أو لإحدى طبقات المنتج شبه الموصل في أية مرحلة من مراحل صنعها. أخيراً، يعني الاستثمار التجاري للمنتجات شبه الموصلة البيع أو التأجير أو أية وسيلة للتوزيع التجاري أو أي عرض مقدّم للغايات المذكورة.

وتعرّف المادة ١ من الإرشاد الاستثمار التجاري، بأنه البيع أو التأجير أو أية وسيلة للتوزيع التجاري أو أي عرض مقدّم للغايات المذكورة. كما وتعرف المادة ١ أيضاً اسم الموقع، بأنه ما يعبّر بحروف الأبجدية وبالأرقام عن العنوان الرقمي المعين لموقع إلكتروني على شبكة الإنترنت. فلكل موقع على الإنترنت عنوان رقمي يعبّر عنه لسهولة الاستعمال والحفظ بعبارة معينة مكّونة من كلمة أو أكثر مدمجة مع بعضها، مثلاً اسم الموقع لوزارة العدل اللبنانية هو «Justice.gov.lb». أما رمز النطاق على المستوى الوطني[٦] ، (مثلاً lb.) فهو يعرّف أسماء مواقع الإنترنت التي تختص ببلد معين، وهو يتواجد في القسم الأخير من اسم الموقع وفق نظام العنونة لشبكة الإنترنت. وهو يكون عادةً مختصراً لاسم البلد مثل حالة لبنان Lebanon تصبح lb.

يتضمن **الباب الثاني** المعنون «الحماية القانونية لبرامج الحاسوب (البرامج المعلوماتية)» الأحكام القانونية التي تنظم الحماية القانونية للبرامج المعلوماتية[٧]، لجهة السند القانوني للحماية والمستفيدين منها وحقوق صاحب حق المؤلف ونطاق الحماية والاستثناءات عليها والتدابير المتخذة لفرضها[٨].

تحدد المادة ٢ من هذا الإرشاد السند القانوني لحماية البرامج المعلوماتية الذي يرتكز على الحماية بموجب حق المؤلف بالمعنى المنصوص عليه في اتفاقية برن لحماية الأعمال الأدبية والفنية[٩]. وقد تتخذ البرامج المعلوماتية المعنية أي شكل، حتى قد تكون مُدمجة ضمن التجهيزات لتشغيلها. كما تمتد الحماية إلى أعمال التصميم التحضيرية التي تُعتبر من ملحقات البرنامج المعلوماتي، شرط أن تتيح لاحقاً تنفيذ البرنامج. وتضع المادة ٢ الشروط القانونية المطلوبة لمنح الحماية، ألا وهي توفر الابتكار[١٠] في البرنامج المعلوماتي والتعبير عنه في شكل ما، لا أن يبقى مجرد أفكار لم تنفذ. فالأفكار والمبادئ التي هي في أساس المنطق المُتبع والخوارزميات[١١] والبرمجيات لا تكون محمية بذاتها وفق هذا الباب. ويعرّف الاجتهاد الفرنسي البرنامج المُبتكر بأنه البرنامج الذي يحمل علامة الإضافة الذهنية لمؤلفه، والذي يتجلى بجهد شخصي يتعدى وضع قيد التنفيذ منطقاً آلياً ومُلزماً من الناحية التقنية[١٢]. إن الجهد الشخصي للمؤلف قد يظهر من خلال جوانب عدة في تصميم البرنامج أو تنفيذه، كهيكلية البرنامج أو الخيارات المتخذة أو طريقة المقاربة العامة والتحديد في وظائف البرنامج وتكوينه.

تحدد المادة ٣ صفات الشخص صاحب حق المؤلف على البرنامج المعلوماتي، أو بمعنى آخر من يُعتبر صاحب حق المؤلف على البرنامج المعلوماتي، لاسيما في حالة الأعمال الجماعية والأعمال المشتركة والأعمال المنفذة من قبل مُستخدِم. بالمبدأ، إن مؤلف البرنامج المعلوماتي هو كل شخص طبيعي أو مجموعة من الأشخاص الطبيعيين ابتكروا البرنامج، كما يمكن أن يكون هذا الشخص شخصاً معنوياً إذا كانت تسمح بذلك التشريعات الوطنية لدولة عضو. وفي حالة الأعمال الجماعية، فإن الشخص المُعتبر بموجب التشريعات المذكورة كمُبتكر للعمل يكون هو أيضاً المؤلف. وقد لا تعترف التشريعات الوطنية بمبدأ الأعمال الجماعية، لذلك وُضعت الفقرة المتعلقة بالأعمال الجماعية على سبيل الافتراض. وفي حالة الأعمال المشتركة، أي عندما يتم ابتكار برنامج معلوماتي بالاشتراك من قبل عدة أشخاص طبيعيين، فإن الحقوق الحصرية للمؤلف تعود بالاشتراك لهؤلاء الأشخاص. وتعالج الفقرة الأخيرة من المادة ٣ حالة الابتكار الذي تم من قبل مُستخدِم بمعرض ممارسته لوظيفته أو وفق تعليمات صاحب العمل، ففي هذه الحالة يكون صاحب العمل هو المخوّل ممارسة الحقوق المادية المتعلقة بالبرنامج المعلوماتي، باستثناء حالة وجود بنود تعاقدية مخالفة. وتكون المادة ٣ قد غطّت جميع الحالات التي تبين من هو صاحب حق المؤلف أو من هم أصحاب حق المؤلف.

تتطرق المادة ٤ من هذا الإرشاد لنطاق الحماية القانونية بموجب حق المؤلف لجهة الأشخاص المستفيدين منها، وتحيل

في هذا الصدد إلى أحكام التشريعات الوطنية. فالحماية تُعطى لكل شخص طبيعي أو معنوي يستفيد من أحكام التشريعات الوطنية في نطاق حقوق المؤلف المطبّقة على الأعمال الأدبية.

تتعرض المادة ٥ من الإرشاد إلى حقوق صاحب حق المؤلف لبرنامج معلوماتي لجهة ماهية هذه الحقوق وامتدادها والأعمال موضوع هذه الحقوق. وتتسم هذه الحقوق بالطابع الحصري الذي يخول صاحبها وحده حق ممارستها والقيام بالأعمال المتعلقة بها وكذلك السلطة اللازمة لإباحة هذه الأعمال. بطبيعة الحال، تشمل حقوق المؤلف حقوقاً معنوية وحقوقاً مادية. والحقوق المعنوية للمؤلف هي تلك المتعارف عليها في نطاق الملكية الأدبية والفنية. وتتضمن هذه الحقوق المعنوية[١٣]: حق نِسبة العمل إلى المؤلف، وحق المؤلف بإشهار العمل، وحق المؤلف بسحب العمل حتى بعد التعاقد على استثماره مع الغير (هذا الحق مُلغى في حالة البرامج المعلوماتية)، وحق المؤلف بمنع أي تحوير أو تعديل أو تغيير في العمل ضمن شروط معيّنة (وهذا الحق ضيّق جداً في حالة البرامج المعلوماتية). أما الحقوق المادية والتي تتعلق باستثمار أو باستغلال البرنامج المعلوماتي، فقد فصّلتها المادة ٥ من هذا الإرشاد مع مراعاة المادتين ٦ و٧ منه. وفي المبدأ تتضمن الحقوق الحصرية لصاحب حق المؤلف حق فعل أو الترخيص بالتالي: نسخ وإعادة إنتاج العمل بشكل دائم أو مؤقت للبرنامج المعلوماتي جزئياً أو كلياً بأية وسيلة كانت وبأي شكل كان. وترجمة البرنامج المعلوماتي وتكييفه وإعادة ترتيبه وكل تحويل له وإعادة إنتاج البرنامج الناتج عن ذلك مع حفظ حقوق الشخص الذي تولى تحويل البرنامج المعلوماتي. وكل شكل من التوزيع والنقل بما فيه التأجير للجمهور للنسخة الأصلية للبرنامج المعلوماتي أو لنسخه. ويعني تأجير برنامج معلوماتي وضع هذا البرنامج أو نسخة منه بالتصرّف من أجل استعماله لمدة محددة ولغايات تجارية.

تحدد المادتان ٦ و٧ من الإرشاد الأعمال المُستثناة من الحماية القانونية الممنوحة لصاحب حق المؤلف، والتي يستطيع كل شخص القيام بها دونما حاجة لترخيص من الأول. إلا أن هذا الترخيص يصبح ضرورياً بالنسبة للمادة ٦ في حالة وجود اشتراطات خاصة في العقود. وهاتان المادتان توضحان بالتالي الحقوق الممنوحة للمُستخدم المخوّل استعمال البرنامج المعلوماتي[١٤]. وفق المادة ٦، لا تُطلب موافقة صاحب حق المؤلف على نسخ البرنامج أو إعادة إنتاجه أو على تكييفه وترجمته وتحويله وترتيبه، وذلك عندما تكون هذه الأعمال ضرورية من أجل تمكين المستخدم الشرعي من استعمال البرنامج المعلوماتي بطريقة ملائمة للغرض الذي وضع من أجله، ومن ضمنها تصحيح الأخطاء. وهذا الأمر بديهي، فقد تتضرر النسخة الأصلية للبرنامج بفعل فيروس ما، ويضطر صاحبها إلى نسخها مجدداً على حاسوبه الشخصي. كما يجب أحياناً إجراء تكييف ولو بسيط على البرنامج ليعمل على مواصفات معيّنة لحاسب المستخدم أو مع برامج أخرى. بالتالي، يعود للشخص الذي له الحق باستخدامه، صنع نسخة لحفظ هذا البرنامج طالما أنها ضرورية لاستخدامه. كما يعود للشخص المخوّل استخدام نسخة من البرنامج المعلوماتي، دون ترخيص من صاحب حق المؤلف، مراقبة طريقة عمل البرنامج أو دراستها أو فحصها، من أجل تحديد الأفكار والمبادئ التي تشكل أساس أي عنصر في البرنامج، وذلك عندما يقوم هذا الشخص بكل عملية تحميل أو عرض أو تنفيذ أو نقل أو تخزين للبرنامج.

ووفق المادة ٧ من الإرشاد، لا تُشترط موافقة صاحب حق المؤلف، عندما تكون إعادة إنتاج البرمجيات (حل شيفرة البرنامج المعلوماتي) أو ترجمة شكل هذه البرمجيات، ضرورية من أجل الحصول على المعلومات اللازمة لتشغيل البرنامج المعلوماتي مع برامج معلوماتية أخرى، وبشرط التقيد بالشروط التالية: قيام المُرخص له باستخدام البرنامج بهذه الأعمال، إتاحة المعلومات اللازمة للتشغيل مع برامج أخرى بشكل سهل وسريع، حصر هذه الأعمال بالأجزاء من البرنامج المعلوماتي اللازمة للتشغيل. هذا الحق للمستخدم هو بديهي، إذ إن أي برنامج معلوماتي لا يعمل بالمبدأ وحده بل مع برامج أخرى وتجهيزات ومستخدمين آخرين وبالتواصل معهم. وإن فعالية الأنظمة والبرامج المعلوماتية تنتج عن إمكانية الربط بينها وتبادل المعلومات بينها والتوفير على المستخدم إعادة إدخال البيانات بل تزويده مباشرةً بالنتائج النهائية. وحتى يكون ذلك ممكناً يجب أحياناً الحصول على البرمجيات الأساسية للبرامج لتحقيق الربط والتشغيل. على أن هذه المعلومات المحصلة لغاية التشغيل تبقى فقط لهذه الغاية، بحيث يُمنع استعمالها لغايات أخرى أو إعطاؤها للغير خارج إطار التشغيل مع برامج أخرى أو لإنتاج برنامج معلوماتي مشابه وتسويقه. وأخيراً، لا يمكن تفسير هذه المادة بشكل يسمح بتطبيقها بطريقة تلحق ضرراً غير مبرّر بالمصالح المشروعة لصاحب حق المؤلف أو تتعرّض للاستخدام الطبيعي للبرنامج المعلوماتي، وذلك منعاً لأي استغلال من قبل البعض لهذه المادة وتوسله تطبيقها خلافاً للعلة التي بررتها. ويتبين، وفق ما تقدم، من المادتين ٦ و٧ من الإرشاد، أن الحقوق الأساسية العائدة للمُستخدم على برنامج معلوماتي هي التالية: حق تكييف البرنامج لغاية الاستعمال وتصحيح الأخطاء، صنع نسخة للحفظ، تحليل

البرنامج واختباره، حل شيفرة البرنامج للتشغيل مع برامج أخرى. ضماناً لفعالية الأحكام الواردة في هذا الباب، فرضت المادة ٨ من الإرشاد اتخاذ تدابير لحماية البرامج المعلوماتية. وقد تكون هذه التدابير عقابية عبر فرض عقوبة جزائية أو احترازية لمنع تفاقم الضرر، وذلك عن طريق الضبط والمنع والحجز. والأفعال المجرّمة أو المحظورة تتجلى بالتالي: الوضع بالتداول مع العلم بذلك لنسخة غير مشروعة لبرنامج معلوماتي، والحيازة لغايات تجارية مع العلم بذلك لنسخة غير مشروعة لبرنامج معلوماتي، وثبوت القيام بأفعال هندسة عكسية[١٥] تكون غايتها خلق برنامج معلوماتي منافس ومطابق للبرنامج المعلوماتي المحمي. ويكفي الاعتقاد بتوفر أسباب لعدم مشروعية نسخة البرنامج المعلوماتي لدى الشخص لاعتباره سيء النية، ولتطبيق تدابير الحماية بحقه.

تتعرض المادة ٩ من الإرشاد لعلاقة الباب الثاني منه ببعض القوانين الأخرى ولمدى تأثيره عليها. وتنص المادة ٩ بالتالي على أن الأحكام القانونية المنصوص عليها في هذا الباب لا تؤثر على الأحكام القانونية الأخرى، لاسيما تلك المتعلقة ببراءات الاختراع والعلامات التجارية والمنافسة غير المشروعة وسرية الأعمال وحماية المنتجات شبه الموصلة وقانون العقود. كما تؤكد المادة ٩ من الإرشاد على الطابع الإلزامي لبعض أحكامه، بحيث لا يمكن للفرقاء الاتفاق على عكسها، ولا يمكن للطرف القوي أن يفرض خلافها على الطرف الأضعف في العقد. فكل بند تعاقدي مخالف لأحكام المادة ٧ أو للاستثناءات المنصوص عليها في المادة ٦ (المقطع الثاني والثالث فقط) يكون باطلاً.

يتناول **الباب الثالث** المعنون «الحماية القانونية لقواعد البيانات[١٦]» القواعد القانونية التي تنظم الحماية القانونية لقواعد البيانات، وهي ترتكز إلى مؤسستين قانونيتين[١٧]: الحماية بموجب حق المؤلف في حال توفر الابتكار، والحماية بموجب الحق الخاص للاستثمار[١٨]. ويتضمن الباب الثاني عدة فصول: الفصل الأول (نطاق تطبيق أحكام هذا الباب)، الفصل الثاني (الحماية القانونية لقواعد البيانات بموجب حق المؤلف)، الفصل الثالث (الحماية القانونية بموجب الحق الخاص)، الفصل الرابع (أحكام ختامية).

يتعرّض الفصل الأول من هذا الباب في المادة العاشرة لنطاق تطبيق أحكام الباب الثاني. فهذا الباب الأخير يطبق على قواعد البيانات أياً كان شكلها، ومنها قواعد البيانات غير الإلكترونية، ولكنه لا يطبق على البرامج المعلوماتية. والفرق واضح من الجهة التقنية بين البرامج المعلوماتية وقواعد البيانات. فقواعد البيانات هي مجموعة أعمال أو بيانات أو عناصر أخرى مستقلة منظّمة بطريقة منهجية ومكن للوصول إليها بوسائل إلكترونية أو بأية وسيلة. وبالتالي، فإن قاعدة المعلومات قد تكون مجموعة أعمال أدبية أو فنية أو موسيقية أو نصيّة أو صوتية أو مجموعة صور أو أرقام أو وقائع أو بيانات أو غيرها. فقواعد البيانات هي الوعاء الذي يسمح بحفظ كميات هائلة من المعلومات وإدارتها لجهة الإضافة والتعديل والمحو والاسترجاع، أما البرامج المعلوماتية فلا تحفظ المعلومات، بل تتولى معالجتها فقط وأداء وظائف معيّنة مبرمجة من قبل الفنيين. لذلك أيضاً، فإن الحماية القانونية المنصوص عليها في هذا الباب لا تطبق على البرامج المعلوماتية المُستخدمة في صنع أو طريقة عمل قواعد البيانات الممكن الوصول إليها بوسائل إلكترونية. فقد تُستعمل برامج مع قواعد البيانات لمعالجة البيانات المحفوظة، ويقتضي بالتالي عدم الخلط بينها وبين قواعد البيانات ذاتها.

يتناول الفصل الثاني من هذا الباب بالتفصيل الحماية القانونية لقواعد البيانات بموجب حق المؤلف[١٩]. وتبين المادة ١١ من الإرشاد الشرط القانوني لاستفادة أية قاعدة بيانات من هذه الوسيلة القانونية في الحماية، وهذا الشرط هو الابتكار في قاعدة البيانات لدى اختيار المواد (أي مضمونها) أو تنظيمها أو ترتيبها، ولا يُطلب توفر أية شروط إضافية أخرى، بل يكفي توفر شرط واحد هو شرط الابتكار. ويقتضي التفريق بين قاعدة البيانات، وهي الهيكلية أو القالب أو الخزان الذي توضع فيه المعلومات وبين هذه المعلومات ذاتها أو ما يُعرف بمحتوى قاعدة البيانات. فقد تشتمل قاعدة البيانات على صور أو ألحان أو برامج هي محمية بذاتها بموجب حق المؤلف كونها ابتكارات ذهنية، وذلك بمعزل عن الحماية القانونية لقاعدة البيانات التي تخزّنها. في هذه الحالة، يجب الحصول بطبيعة الحال على ترخيص من قبل صاحب حق المؤلف على العمل المُدخل في القاعدة قبل إدخاله. بالتالي، فإن الحماية القانونية لقواعد البيانات بموجب حق المؤلف لا تشمل محتوى قواعد البيانات ولا تتعرض للحقوق على هذا المحتوى، بل إن الحماية القانونية لقاعدة البيانات تنصب على هيكليتها، وعلى العناصر اللازمة لتشغيلها أو لاستعمالها كالمكنز وأنظمة التوثيق. وهذا الأمر منطقي وفق ما تقدم بيانه.

تتولى المادة ١٢ من الإرشاد تحديد من هو صاحب حق المؤلف على قاعدة البيانات المحمية، وبالتالي من هو الشخص الذي يستفيد من الحماية القانونية والحقوق والامتيازات التي يعطيها له القانون. فمؤلف قاعدة البيانات هو الشخص

الطبيعي أو مجموعة الأشخاص الطبيعيين الذين أنشأوا قاعدة البيانات. ويمكن أن يكون أيضاً شخصاً معنوياً إذا كانت تجيز ذلك التشريعات الوطنية لأي دولة عضو. كذلك عندما تعترف التشريعات الوطنية لأي دولة عضو بالأعمال الجماعية، فإن الحقوق المادية عليها تعود للشخص المُعتبر صاحب الحق بموجب هذه التشريعات. ففي المبدأ في التشريعات الوطنية، يُعتبر الشخص الطبيعي أو المعنوي الذي أخذ المبادرة بابتكار العمل والإشراف على تنفيذه هو صاحب حق المؤلف. أما في حالة الأعمال المشتركة، حيث قد يستحيل تحديد نصيب أي من المشتركين في ابتكار العمل، كما قد يمكن أيضاً تحديد هذا النصيب، فتعود الحقوق الحصرية للمؤلف بالاشتراك وتُترك مسألة قاعدة البيانات المُبتكرة من قبل مُستخدم أثناء قيامه بعمله أو بناءً لتوجيهات صاحب العمل، لتقدير كل دولة عضو. ولا شيء يمنع من النص في التشريعات الوطنية على أن الحقوق المادية على قاعدة البيانات المُبتكرة تعود لصاحب العمل باستثناء حالة وجود بنود تعاقدية مخالفة. وتجدر الإشارة إلى أن الحقوق المعنوية للشخص الطبيعي تكون لمؤلف قاعدة البيانات وفق اتفاقية برن لحماية الأعمال الأدبية والفنية، وتبقى الحقوق المعنوية خارج إطار تطبيق الباب الثاني من هذا الإرشاد[٢٠].

تعرض المادة ١٣ من الإرشاد الحقوق الحصرية لصاحب حق المؤلف على قاعدة البيانات التي تستفيد من الحماية، فهذه الحقوق الحصرية هي ذاتها المنصوص عليها في المادة ٥ من هذا الإرشاد. صحيح أن هذه المادة تتعلق بالبرامج المعلوماتية، إلا أن المؤسسة القانونية التي تحمي هي ذاتها، فتكون الحقوق الحصرية هي ذاتها.

تذكر المادة ١٣ من الإرشاد الاستثناءات على حقوق صاحب حق المؤلف على قاعدة البيانات التي تستفيد من الحماية. فالمستخدم الشرعي لقاعدة بيانات أو لنسخ عنها يستطيع القيام بجميع الأعمال المنصوص عليها في المادة الرابعة من الإرشاد، والتي تكون ضرورية للوصول إلى محتوى قاعدة البيانات ولو استخدامها بشكل عادي من قبله، وذلك دون ترخيص من قبل مؤلف قاعدة المعلومات. وهذا الأمر منطقي، فطالما أنه مُرخص له باستعمال قاعدة البيانات، فلا بد من السماح له بالأعمال التي تؤمن هذا الاستعمال ولو كانت من ضمن سلطات صاحب حق المؤلف، شرط عدم إساءة استعمال هذه الأعمال لغايات أخرى غير الاستعمال بصيغته الحصرية، كقيامه مثلاً بنسخ قاعدة البيانات بقصد التقليد وبيع النسخ المقلدة. كما يمكن للدول الأعضاء وضع قيود على الحقوق الحصرية لصاحب حق المؤلف المنصوص عليها في المادة الرابعة من الإرشاد في الحالات التالية: في حالة النسخ وإعادة الإنتاج لغايات خاصة لقاعدة بيانات غير إلكترونية، وفي حالة الاستخدام حصرياً لغايات التوضيح في التعليم أو لغايات البحث العلمي مع موجب تحديد المصدر وفي الحدود المبرّرة بالهدف غير التجاري المُتوخى، وفي حالة الاستخدام لغايات الأمن العام أو لغايات متعلقة بإجراءات إدارية وقضائية، وفي حالات أخرى منصوص عليها تقليدياً في التشريعات الوطنية. وهذه الاستثناءات ليست جديدة في مجال الحماية القانونية بموجب حق المؤلف، فإن تشريعات الملكية الفكرية قد لحظت مثل هذه الاستثناءات بالنسبة للأعمال الفكرية التقليدية كالكتب والألحان. إلا أنه في مطلق الأحوال، لا يمكن تطبيق هذه الاستثناءات بطريقة تلحق ضرراً غير مبرّر بالمصالح المشروعة لصاحب الحق أو تتعرّض للاستخدام الطبيعي لقاعدة البيانات، وذلك وفقاً لأحكام اتفاقية برن لحماية الأعمال الأدبية والفنية.

ينظم الفصل الثالث من هذا الباب الحماية القانونية لقواعد البيانات بموجب الحق الخاص[٢١] . وتحدد المادة ١٥ من الإرشاد شروط الحماية القانونية لقاعدة البيانات بموجب الحق الخاص. ففي حال لم يتوفر شرط الابتكار في قاعدة البيانات، فلا يمكن حمايتها بموجب حق المؤلف، إنما يمكن حمايتها بموجب الحق الخاص إذا كان إنشاء قاعدة البيانات يستلزم استثماراً مهماً من الناحية النوعية أو الكمية في الأموال والتجهيزات والموارد البشرية (الوسائل المادية والجهد والوقت.). وإن الحق الخاص يحمي الاستثمار الحاصل في تجميع معلومات محتوى قاعدة البيانات والتحقق منها وتقديمها. ويستفيد من الحماية بموجب الحق الخاص صانع قاعدة البيانات، فالحماية هي للاستثمار كما قلنا. ومنتج أو صانع قاعدة البيانات هو الشخص الذي يبادر إلى إنشائها ويتولى مسؤولية الإنتاج متحملاً مخاطر الاستثمار، ويخرج عن هذا المفهوم المقاول من الباطن. وبالتالي يمكن لصاحب الحق الخاص منع أي شخص آخر من استخراج وإعادة استعمال محتوى قاعدة البيانات، سواء كان ذلك يهدف ذلك لصنع منتج آخر منافس بشكل طُفيلي أو حتى للاستعمال العادي المُلحق للضرر. ويُعرّف الاستخراج بأنه النقل الدائم أو المؤقت لكامل محتوى قاعدة البيانات أو لجزء مهم منها على دعامة أخرى بأية وسيلة كانت أو تحت أي شكل كان. أما إعادة الاستعمال فهي كل شكل من أشكال الوضع بتصرف الجمهور لكامل محتوى قاعدة البيانات أو لجزء مهم منها، وذلك من خلال توزيع نسخ عنها أو بالتأجير أو بالنقل على الخط أو تحت أشكال أخرى. إن الحق باستخراج محتوى قاعدة البيانات أو بإعادة استعماله هو حق مادي يتعلق باستثمار قاعدة البيانات، ولذلك يمكن نقله أو التنازل عنه أو إعطاؤه للغير بموجب عقد إجازة مُبرم من قبل صاحب الحق الخاص. وهنا أيضاً يقتضي التفريق بين

قاعدة البيانات ومحتواها من الأعمال التي قد تكون محمية بذاتها كالمقالات الأدبية والألحان وغيرها. كما يقتضي الإشارة إلى أن الحماية بموجب الحق الخاص لقاعدة البيانات لا تنفي الحماية بموجب حق المؤلف لهذه القاعدة في حال توفر شرط الابتكار. فقد تكون قاعدة البيانات مبتكرة وفي ذات الوقت تطلب صناعتها استثمارات ضخمة، ويعود لصاحبها التذرع بوسيلة الحماية الأنجع التي يرتئيها. أخيراً يؤكد المقطع الأخير من المادة ١٥ على حماية حقوق صاحب الحق الخاص منعاً لأي تعسف أو سوء استعمال من قبل المستخدم لحقوقه. ففي المبدأ، إن الاستخراج أو إعادة الاستعمال لأجزاء غير مهمة من قاعدة البيانات هو مسموح وفق المادة ١٥. إلا أن الاستخراج أو إعادة الاستعمال المتكررة والمنهجية لأجزاء غير مهمة من محتوى قاعدة البيانات، والتي تفترض أعمالاً منافية للاستعمال العادي لقاعدة البيانات أو التي تسبب ضرراً غير مبرّر للمصالح المشروعة لصانع قاعدة البيانات، يكون غير مسموح. وهذه القاعدة الأخيرة هي تطبيق لمبدأ عدم التعسف في استعمال الحق أو تخوير الغايات.

تحدّد المادة ١٦ من الإرشاد حقوق مُستخدم قاعدة البيانات وموجباته. فلمُستخدم قاعدة البيانات الموضوعة بتصرف الجمهور، والمُرخص له، أن يستخرج أو يعيد استعمال أجزاء غير مهمة من محتوى القاعدة. ويُنظر إلى أهمية الأجزاء المُستخرجة أو المُعاد استعمالها ليس من ناحية حجمها فقط بل من ناحية خطورتها أيضاً. إلا أن على المستخدم أن يلتزم بحدود هذا الحق، وأن لا يتعسف باستعمال حقه. فهو لا يستطيع القيام بأعمال تتعارض مع الاستثمار العادي لقاعدة البيانات أو تضر بطريقة غير مبرّرة بالمصالح المشروعة لصانع قاعدة البيانات، أو تضر بصاحب حق المؤلف أو صاحب الحقوق المجاورة القائمة على أعمال محتوى قاعدة البيانات.

تتعرض المادة ١٧ من الإرشاد إلى الاستثناءات على حقوق صاحب الحق الخاص على قاعدة البيانات. وهذه الاستثناءات تتعلق بحقوق المستخدم المُرخص له باستعمال قاعدة البيانات. فلهذا المستخدم استخراج أو إعادة استعمال جزء مهم من محتوى قاعدة البيانات الموضوعة بتصرف الجمهور دون ترخيص من صانع قاعدة البيانات في الحالات التالية: في حالة الاستخراج لغايات خاصة لمحتوى قاعدة بيانات غير إلكترونية، وفي حالة الاستخراج لغايات التوضيح في التعليم أو لغايات البحث العلمي شرط ذكر المصدر وفي الحدود المبرّرة للهدف غير التجاري المتوخّى، وفي حالة الاستخراج أو إعادة الاستعمال لغايات الأمن العام أو لغايات متعلقة بإجراءات إدارية أو قضائية. وهذه الاستثناءات على حقوق صاحب الحق الخاص هي مشابهة لتلك المذكورة سابقاً والجارية على حق المؤلف على قاعدة بيانات.

تحدّد المادة ١٨ من الإرشاد مدة الحماية[٢٢] بموجب الحق الخاص الجارية على قاعدة بيانات. فالحق الخاص ينتج مفاعليه منذ انتهاء صنع قاعدة البيانات، وينقضي بعد مرور خمس عشرة سنة تُحسب ابتداء من الأول من كانون الثاني الذي يلي تاريخ الانتهاء من الصنع، أو ابتداء من الأول من كانون الثاني الذي يلي تاريخ وضعها بتصرف الجمهور بأية طريقة كانت. على أن مدة هذه الحماية تتجدد بكل تعديل مهم على قاعدة البيانات تطلّب أيضاً استثمارات مهمة جديدة، فسبب الحماية هو واحد، وهو وجود استثمار، فكلما تجدّد الاستثمار، تجددت الحماية. وبالتالي، فإن كلّ تعديل مهم، مقيّم من الناحية النوعية أو الكمية، لمحتوى قاعد البيانات، لاسيما كل تعديل مهم ناتج عن تراكم الإضافات أو الإلغاءات أو التغييرات المستمرة، والتي توحي بوجود استثمار مهم جديد مقيّم من الناحية النوعية والكمية، يسمح بتجديد الحماية لقاعدة البيانات لمدة خمس عشرة سنة جديدة تُحسب ابتداءً من الأول من كانون الثاني الذي يلي تاريخ انتهاء تحديث قاعدة البيانات.

يتناول الفصل الرابع من هذا الباب أحكاماً ختامية، منها ما يتعلق بالأفعال الواجب تجرمها، ومنها ما يتعلق بإلزامية مواد هذه الباب. فالمادة ١٩ من الإرشاد تحرص على معاقبة الأفعال التي تنتهك الحقوق المنصوص عليها في هذا الباب[٢٣]، إذ إن أية حماية قانونية لن تكون فعالة إلا بوجود عقوبات رادعة تطبق على المخالفين. كما تشير المادة ٢٠ من الإرشاد إلى مواد هذا الباب التي تتمتع بطابع آمر وإلزامي، بحيث لا يجوز الاتفاق على مخالفتها من قبل الفرقاء، وكل اتفاق مخالف لها يكون باطلاً. وتعتبر المادة ٢٠ البنود التعاقدية المخالفة لأحكام الفقرة الأولى من المادة ١٤ ولأحكام المادة ١٦ من هذا الإرشاد باطلة.

يتضمن **الباب الرابع** المعنون «الحماية القانونية للمنتجات شبه الموصلة» الأحكام القانونية التي تنظّم هذه الحماية لجهة شروط الحماية وصاحب الحق المحمي وحقوقه ولجهة التسجيل لتكريس الحق ومدة الحماية[٢٤]. إن المنتجات شبه الموصلة تدخل في تكوين مختلف الأجهزة الإلكترونية، بحيث أصبحت شائعة الاستعمال إلى درجة كبيرة. إن تصميم المنتجات شبه الموصلة قد أصبح على درجة عالية من التعقيد تبعاً لتشعب الوظائف التي تؤديها، ويتطلب هذا التصميم جهداً وكفاءة كبيرين واستثماراً في الوقت والإمكانات، وهذه الأمور تبرّر بطبيعة الحال توفير حماية

قانونية لهذه المنتجات. ويرتكز كل منتج شبه موصل إلى طوبوغرافيا معينة. فالمنتج شبه الموصل يُصنّع وفق تصميم وخريطة معينة يُعبّر عنهما من خلال طوبوغرافيا. بشكل مبسط، الطوبوغرافيا هي الخريطة للمُنتَج، والمُنتَج هو السلعة النهائية.

تشترط المادة ٢١ من الإرشاد لحماية طوبوغرافيا المنتَج شبه الموصل صرف مُبتكرها لجهد فكري وذهني[٢٥] بالإضافة إلى كونها غير شائعة سابقاً. إلا أنه إذا تكونت الطوبوغرافيا من عدة عناصر أو أجزاء كانت شائعة ومعروفة، فإنها تستفيد أيضاً من الحماية إذا كان تجميع عناصرها كمكوّن واحد استلزم جهداً فكرياً وذهنياً وإذا كان المكون بمجمله وطريقة التجميع غير شائعين.

تحدّد المادة ٢٢ من الإرشاد صاحب الحق بالحماية القانونية للمنتج شبه الموصل[٢٦]. فالحق بالحماية يُعطى لمبتكري طوبوغرافيا المنتجات شبه الموصلة، مع مراعاة أحكام هذه المادة. ويمكن لكل دولة عضو أن تعطي الحق بالحماية لصاحب العمل بالنسبة للطوبوغرافيا المُبتكرة من قبل موظف مدفوع الأجر باستثناء حالة وجود بنود مخالفة في عقد العمل، وكذلك للطرف في العقد الذي طلب الطوبوغرافيا بالنسبة للطوبوغرافيا المُبتكرة بموجب عقد غير عقد عمل باستثناء حالة وجود بنود مخالفة في العقد. في بعض الأحيان، قد لا يظهر بشكل واضح صاحب الحق بالحماية، ويُفترض قانوناً في هذه الحالة، وفق المادة ٢٢، أن المستفيد من الحماية هو الشخص الذي يقوم بأول استثمار تجاري للطوبوغرافيا غير المستثمرة أبداً سابقاً، أو الشخص الذي تلقى من آخر مخوّل التصرف بالطوبوغرافيا الترخيص الحصري للقيام بالاستثمار التجاري للطوبوغرافيا[٢٧]. وفي النهاية، تمتد الحماية إلى خلفاء الأشخاص المذكورين أعلاه.

تنظم المادة ٢٣ من الإرشاد مسألة تسجيل طوبوغرافيا المنتَج شبه الموصل ومفاعيل التسجيل، وتبقى هذا التسجيل اختيارياً[٢٨] وفق ما ترتأيه كل دولة عضو[٢٩]. فتسجيل طوبوغرافيا المنتَج شبه الموصل لا يكون إلزامياً إلا إذا تم النص على ذلك بموجب التشريعات الوطنية، بحيث لا تستفيد بالتالي الطوبوغرافيا من الحماية إلا إذا تم تسجيلها لدى هيئة رسمية. وهذا التسجيل يجب أن يتم في خلال سنتين تليان أول استثمار تجاري لها. ويجب أن تكون هذه الهيئة رسمية وليس خاصة، كونها تشكل نوعاً من مرجع للتوثيق، يجب أن يحظى بمصداقية عالية وأن يخضع لرقابة مستمرة من الدولة. كما يمكن، بالإضافة إلى التسجيل، فرض إيداع المواد التي تمثّل الطوبوغرافيا أو تجميعاً معيناً لها لدى الهيئة الرسمية، وكذلك التصريح عن تاريخ أول استثمار تجاري للطوبوغرافيا، عندما يكون هذا الاستثمار سابقاً لتاريخ إيداع طلب التسجيل. وهذان التسجيل والإيداع هما إجراء شكلي ولكن جوهري لحفظ الحق عليها . وكذلك لإعلام الغير بصاحب الحق عليها. ويجب احترام مبدأ سرية الأعمال في معاملة الإيداع، بحيث لا يجوز للجمهور الإطلاع على مواد الطوبوغرافيا في هذه الحالة، باستثناء حالة إطلاع الغير بناءً لأمر قضائي أو لأمر سلطة مختصة في حالات المنازعات. في حال اشتراط تسجيل الطوبوغرافيا، من البديهي لتحديد صاحب الحق فرض تسجيل كل انتقال للحقوق الجارية على الطوبوغرافيا المحميّة. ونكون أمام سجل لمجموع الطوبوغرافيا والوقوعات الجارية عليها يحول دون التنازع على الحقوق عليها ويوضّح للمتعاملين من هو صاحب الحق على الطوبوغرافيا ومن هو المعتدي. كما يمكن في حالة التسجيل، ولتغطية أعباء الهيئة الرسمية المكلفة بذلك، فرض دفع رسم لدى إتمام تسجيل أو إيداع طوبوغرافيا المنتج شبه الموصل. أخيراً، ما خلا معاملة التسجيل والإيداع، لا تستلزم الحماية القانونية لطوبوغرافيا المنتج شبه الموصل إتمام أي شكليات أو إجراءات أخرى. على أن التسجيل قد يكون غير محق أو يتعرض لحقوق الغير، ويقتضي بالتالي إتاحة المجال لهذا الغير للطعن بالتسجيل بالطرق الإدارية والقضائية عند الضرورة.

تحدّد المادة ٢٤ من الإرشاد ماهية الحقوق الحصرية[٣٠] العائدة لصاحب الحق على طوبوغرافيا المنتج شبه الموصل، وهذه الحقوق الحصرية تتضمن الحق بترخيص أو بمنع الأعمال التالية: نسخ وإعادة إنتاج الطوبوغرافيا المحمية، والاستثمار التجاري أو الاستيراد لهذه الغاية لطوبوغرافيا أو لمنتج شبه موصل مُصنّع بواسطة هذه الطوبوغرافيا. وهذه الحقوق الحصرية مشابهة في المبدأ للحقوق الحصرية الجارية على قواعد البيانات والبرامج المعلوماتية. وكذلك الأمر، تورد المادة ٢٤ استثناءات على الحقوق الحصرية على الطوبوغرافيا، وهذه الاستثناءات تُعطى وفق خيار كل دولة عضو، أي يجب النص عليها في التشريعات الوطنية. وتشمل هذه الاستثناءات نسخ أو إعادة إنتاج طوبوغرافيا بصفة خاصة لغايات غير تجارية، والنسخ أو إعادة الإنتاج لغايات التحليل أو التقييم أو تعليم المفاهيم والآليات والأنظمة والتقنيات المُدخلة في الطوبوغرافيا أو للطوبوغرافيا ذاتها[٣١]. كما تكون جائزة الأعمال اللاحقة على وضع الطوبوغرافيا أو المنتجَ شبه الموصل في السوق من قبل الشخص المُرخص له بتسويقها، ولا تكون هذه الأعمال تتعرض للحقوق الحصرية لصاحب الحق. أخيراً، تستند الفقرة الأخيرة من المادة ٢٤ إلى حسن نية الغير أو سوء نيته. فالشخص

الذي يكتسب منتَجاً شبه موصل دون معرفة أن المنتَج هو محمي أو دون توفر إفتراض منطقي لمعرفته، لا يمكن منعه من الاستثمار التجاري للمنتج. فهذا الشخص حسن النية واستثماره التجاري للمنتَج مشروع. أما بالنسبة للأعمال المُرتكبة بعد معرفة الشخص أو بعد توفر إفتراض منطقي لمعرفته بأن المنتج شبه الموصل يستفيد من الحماية، فإن المحكمة تستطيع الحكم، بناءً لطلب صاحب الحق، ووفقاً لأحكام القانون الوطني المطبّق، بدفع التعويضات الملائمة. ففي الحالة الأخيرة، يكون الغير سيء النية ويقتضي إلزامه بالتعويض عن الضرر اللاحق بصاحب الحق. وتجدر الإشارة أن الغير قد يُعتبر غير محق، ولو كان لا يعلم بحقيقة المنتَج شبه الموصل، إذا كان عدم المعرفة غير مبرّر كأن يكون الغير مهملاً أو أن الطوبوغرافيا مسجّلة وفق الأصول.

تحدد المادة ٢٥ من الإرشاد المدة القانونية للحقوق الحصرية لصاحب الحق على الطوبوغرافيا. فالحقوق الحصرية على طوبرغرافيا المنتج شبه الموصل تنشأ ابتداءً من تاريخ الاستثمار التجاري الأول للطوبوغرافيا أو تاريخ إيداع طلب التسجيل بشكل نظامي أو عند تثبيت الطوبوغرافيا أو ترميزها للمرة الأولى. ويراعى في ذلك حالة ما إذا ما كانت الطوبوغرافيا تخضع للتسجيل لدى هيئة عامة أم لا لتحديد تاريخ بدء سريان الحقوق الحصرية. عندما تنشأ الحقوق الحصرية على طوبوغرافيا المنتجات شبه الموصلة بموجب التسجيل أو الاستثمار التجاري، يحق للشخص الذي له الحق بالحماية القانونية أن يقدم وسائل طعن بالنسبة للفترة السابقة لنشوء الحقوق الحصرية، على أن يثبت أن الغير قد نسخ أو استثمر تجارياً أو استورد لهذه الغايات طوبوغرافيا، وذلك بشكل احتيالي. إن الحقوق الحصرية تنقضي بعد مرور فترة عشر سنوات تبتدئ من نهاية السنة التي تم خلالها إيداع طلب التسجيل بشكل نظامي أو من نهاية السنة التي تم خلالها الاستثمار التجاري للطوبوغرافيا للمرة الأولى في أي مكان في العالم. عندما لا يتم الاستثمار التجاري للطوبوغرافيا في أي مكان من العالم في خلال خمس عشرة سنة ابتداءً من التاريخ الذي يتم فيه تثبيتها أو ترميزها للمرة الأولى، فإن كل الحقوق الحصرية على الطوبوغرافيا تنقضي. وفي الدول التي يكون فيها التسجيل شرطاً لنشوء الحقوق الحصرية أو لاستمرارها، فإن أية حقوق حصرية جديدة لا يمكن أن تنشأ إلا إذا تم إيداع طلب بالتسجيل بشكل نظامي ضمن المهلة المذكورة آنفاً. ختاماً، يمكن القول أن المادة ٢٥ قد بيّنت حالات وتواريخ نشوء وانقضاء الحقوق الحصرية على طوبوغرافيا المنتجات شبه الموصلة.

تحصر المادة ٢٦ من الإرشاد الحماية القانونية الممنوحة وفق هذا الباب لطوبوغرافيا المنتَج شبه الموصل فقط، وتستثني من الحماية كل مفهوم وآلية ونظام وتقنية ومعلومة مثبتة مُدخلة كلها في الطوبوغرافيا، وقد تكون هذه الأمور المعدّدة محمية بموجب وسيلة قانونية أخرى كحق المؤلف وغيره[٣١].

يتناول **الباب الخامس** المعنون «الحماية القانونية للأعمال الرقمية الأخرى» المبدأ القانوني المُعتمد لحماية الأعمال الرقمية الأخرى التي لم تُوضع لها أحكام خاصة مثل البرامج وقواعد البيانات والمنتجات شبه الموصلة. فالأعمال الرقمية الأخرى يفترض تكييفها وإعطاؤها الوصف القانوني الملائم لها لإيجاد المؤسسة القانونية التي يمكن واستخدامها لتأمين حمايتها، فقد يمكن حمايتها بموجب حق المؤلف إذا كانت تلبي شرط الابتكار أو بموجب نظام العلامات التجارية أو بموجب الحق الخاص إذا تضمنت قاعدة بيانات. وتنص المادة ٢٧ من الإرشاد في هذا الصدد على أن الأحكام القانونية الواردة في هذا الإرشاد أو في القوانين الوطنية، المتعلقة بالحماية بموجب حق المؤلف والحقوق المجاورة أو بموجب الحق الخاص أو بموجب العلامات التجارية، تطبق أيضاً على سبيل القياس على الأعمال الرقمية الإلكترونية أو على مكونات منها، وفق الوصف القانوني الممكن إعطاؤه لها أو لكل مكون منها وشرط أن تستوفي الشروط القانونية المطلوبة للحماية. وتعطي المادة ٢٧ عدة أمثلة على الأعمال الرقمية الإلكترونية، فهي تشمل فهارس المواقع الإلكترونية وصفحات المواقع الإلكترونية ومحركات البحث ووصلات النصوص الفائقة والأنظمة التطبيقية المختلفة والرسوم والصور الإلكترونية وألعاب الفيديو والوسائط المتعددة.

يتضمن **الباب السادس** المعنون «الحماية القانونية لأسماء المواقع»[٣٣] القواعد القانونية التي تطبق على أسماء المواقع لجهة المرجع الصالح لمنح أسماء المواقع ومسؤوليته والشروط الإدارية والمالية المطلوبة لذلك وإجراءات التسجيل ومحاذيره وإلغاء اسم الموقع وفصل النِزاعات المتعلقة بأسماء المواقع[٣٤].

تنشىء المادة ٢٨ من الإرشاد هيئة رسمية متخصصة بالترخيص لشركة أو مؤسسة خاصة تتولى منح أسماء المواقع ضمن النطاق الوطني وفق شروط إدارية ومالية تقنية معينة. ومن المتعارف عليه قيام المؤسسات الخاصة وليس الجهات الرسمية بمنح أسماء المواقع ضمن النطاق الوطني ولكن تحت رقابة السلطات الرسمية. ولكن بالنظر للطابع الدولي للإنترنت ولتجاوزه الجغرافيا الوطنية، وطالما أن أي مؤسسة ضمن النطاق الوطني لا تستطيع منح أسماء مواقع إلا بالتعاون مع المراجع الدولية المختصة التي تنسّق نظام تسمية المواقع على الإنترنت على المستوى الدولي.

الإرشاد السادس- حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني

وهي حالياً هيئة قانونية أميركية لا تبغي الربح معروفة بـ Internet Corporation for Assigned Names and Numbers (ICANN) فإن المادة ٢٨ تضع شرطاً على كل مؤسسة تتقدم لطلب ترخيص بالاستحصال مسبقاً على موافقة هذه المراجع الدولية.

تحدد المادة ٢٩ من الإرشاد الشروط المالية والإدارية والتقنية لمنح أسماء المواقع ضمن النطاق الوطني. فهذه الشروط تتولى وضعها الهيئة الرسمية المتخصصة المُنشأة بموجب المادة ٢٨، ويجب أن تكون هذه الشروط منسجمة مع شروط المراجع الدولية المختصة بتسجيل مواقع الإنترنت، وإلا قد لا تقبل هذه المراجع عمليات التسجيل. والمبدأ الأساسي في هذه الشروط هو الموضوعية في التعاطي مع الجميع وضرورة احترام المساواة بين طالبي أسماء المواقع وعدم وجود أي تمييز في عمليات منح أسماء المواقع. وتكون هذه الشروط علنية ويحاط العامة علماً بها عن طريق نشرها على شبكة الإنترنت. في المبدأ، إن شروط تسجيل أسماء مواقع الإنترنت هي تعاقدية أساساً توخياً للمرونة ولعدم تجميدها بقانون صعب التعديل والتطوير. ويُراعى هذا الأمر عبر الإحالة إلى شروط توضع من قبل الهيئة الرسمية.

تُعالج المادة ٣٠ من الإرشاد إجراءات تسجيل اسم الموقع وإدارته، وهذه تكون أيضاً بوسائل إلكترونية للتيسير على المتعاملين. وفي جميع الأحوال، يجب أن لا يؤدي التسجيل إلى المساس بحقوق الغير عن طريق استعمال اسم للموقع قد يتعارض مع حقوق ملكية سابقة صناعية أو أدبية أو غيرها. ولذلك يتم تسجيل اسم الموقع مع احترام حقوق الغير، ولاسيما حقوق الملكية الصناعية والملكية الأدبية والفنية والأسماء التجارية والعائلية والعلامات التجارية. فالمبدأ المعمول به في منح أسماء المواقع وهو «من يصل أولاً يخدم أولاً» قد أنتج في بعض الأحيان مخالفات، إذ تفاجأت مؤسسات كثيرة بقيام شخص آخر بتسجيل علامتها التجارية كاسم موقع له دون مبرر مقبول. وهذه الظاهرة تعرف بـ «القرصنة السيبرانية» Cybersquatting.[٣٥]

تتناول المادة ٣١ من الإرشاد مسؤولية الشركة أو المؤسسة المُرخص لها بمنح أسماء المواقع. فهذه الشركة أو المؤسسة لا تكتسب أي حق على أسماء المواقع المستعملة، كما أنها لا تكون مسؤولة عن التعابير والكلمات التي يتم انتقاؤها لأسماء المواقع، بل تقع مسؤولية ذلك على طالب التسجيل في حال التعرض لحقوق الغير. ولكن يتوجب على الشركة أو المؤسسة المُرخص لها بمنح أسماء المواقع أن تتحقق من تلبية طالب التسجيل لاسم موقع معين للشروط الإدارية والمالية والتقنية المفروضة قانوناً، وإلا فإنها تكون مسؤولة عن الإخلال بذلك.

تبين المادة ٣٢ من الإرشاد حالات إلغاء اسم الموقع وصلاحية الشركة أو المؤسسة المُرخص لها بمنح أسماء المواقع في هذا الإطار، إذ يعود للشركة أو المؤسسة المُرخص لها أن تُلغي اسم الموقع في حال تبين لها عدم توفر الشروط الإدارية والمالية والتقنية في طالب التسجيل، أو عدم صحة المعلومات المُقدّمة منه أو عدم كفايتها، أو في حال مخالفة تسمية اسم الموقع للنظام العام أو الآداب العامة، وأخيراً في حال عدم قيام طالب التسجيل بدفع الرسوم القانونية المتوجبة. وإن صلاحية الشركة أو المؤسسة في إلغاء اسم الموقع تبدو محصورة في الحالات المذكورة، إلا أن هذه الحالات تستوعب جميع المخالفات المهمة التي قد تشوب عملية تسجيل اسم الموقع والتي قد تسبب ضرراً للغير أو للمصلحة العامة.

تولي المادة ٣٣ من الإرشاد النِزاعات المتعلقة بأسماء المواقع أهمية خاصة، فمن المتوقع أن تثار النِزاعات حول تسميات أسماء الموقع ومدى تعرضها لأسماء تعود حقوقها للغير كالعلامات التجارية والأسماء التجارية وغيرها. لذلك، تؤكد المادة ٣٣ على صلاحية المحاكم للبت بالنِزاعات المتعلقة بأسماء المواقع. ولتسريع عملية الفصل بهذه النِزاعات، واعتماد التخصص وتخطي مشكلة الصلاحية الإقليمية للنزاعات، من الممكن إيلاء صلاحية الفصل بها لمركز تحكيمي متخصص[٣٦]. ويمكن للمحاكم أو للهيئات التحكيمية أن تلجأ عند الفصل في نِزاعات تسميات أسماء المواقع إلى الأحكام القانونية التقليدية المتعلقة بالعلامات التجارية والأسماء التجارية والمنافسة غير المشروعة والتعسف في استعمال الحق والخطأ وحسن النية وغيرها[٣٧].

يتطرق **الباب السابع** المعنون «أحكام مشتركة» في المادة ٣٤ إلى الوسائل التقنية المعتمدة لحماية البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية من أي نسخ غير مشروع أو انتهاك أو تقليد. يجوز لأصحاب الحقوق على البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية حمايتها من أي اعتداء بتدابير تقنية ملائمة. يمكن أن تشمل هذه التدابير وضع رمز سري للاستخدام الشرعي أو اعتماد وسائل للتشفير أو استعمال آلية لمراقبة النسخ أو ضرورة التسجيل من قبل المستخدم لتفعيل البرنامج. ولكي تكون هذه الحماية التقنية فعالة، وباعتبار أن المعتدين سيلجأون إلى وسائل تقنية مضادة لتعطيل وسائل الحماية التقنية المُستعملة، تُجرّم المادة ٣٥ فعل كل شخص يصنع أو يستورد أو يبيع أو يوزع أو يؤجر أو يضع بالتداول أو يحوز لغايات تجارية

كل جهاز أو وسيلة يكون هدفها الوحيد أو الأساسي تسهيل الإلغاء غير المشروع أو تعطيل الآليات التقنية الموضوعة لحماية البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية المحمية بموجب هذا الإرشاد. كما تشير المادة ٣٤ إلى إجراءات التحقيق والضبط الممكن اللجوء إليها في إطار التحقيقات الإدارية أو القضائية، إذ يمكن ضبط كل نسخة غير مشروعة لبرنامج معلوماتي أو لقاعدة بيانات أو لعمل رقمي والوسائل التقنية المستعملة لتعطيل الآليات التقنية لحماية البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية. كما وتشير المادة ٣٥ إلى نظام للعقوبات يجب أن تعتمده الدول الأعضاء ليطبق على مخالفة أحكام هذا الإرشاد. ويجب أن تكون هذه العقوبات فعالة ورادعة ومتناسبة مع حجم ومدى المخالفة. وذلك كما ينص عليه «الباب السادس: جرائم التعدي على الملكية الفكرية للأعمال الرقمية» من الإرشاد الخاص بالجرائم السيبرانية.

هوامش

١ – تم توسيع نطاق اتفاقية برن لحماية المصنفات الفنية والأدبية عام ١٩٩٦ بواسطة اتفاقية حق المؤلف Copyright Treaty التي أضافت الأعمال الرقمية إلى مجموع الأعمال المحمية بموجب اتفاقية برن.

http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html

2- Semiconductors: Any of various solid crystalline substances, such as germanium or silicon, having electrical conductivity greater than insulators but less than good conductors, and used especially as a base material for computer chips and other electronic devices.

3- See Internet Law - Violation of Intellectual Property Rights on the Internet: for Digital risks, Digital Solutions, available:
http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1711
Internet has made intellectual property (IP) rights more vulnerable to violations by every sector of society; business, students, and, of course, the committed copyright infringer. Thus, those directly affected by copyright violations have resorted to alternative methods to manage intellectual property rights. Those alternative methods are digital technology programs designed to control internet access and use of copyrighted material. There is a range of companies currently offering a variety of digital programs for IP management, this is not news. The extraordinary is the creativity found in some of these digital programs. For instance, Digimarc, an American provider of IP management solutions, created a program called «Digital Watermark.» This program is the digital equivalent of traditional chemical watermarks.
Digital Watermark allows copyright owners to track distribution, access and payment of its material. Bits of information are embedded in data codes that are imperceptible during normal use but readable by computers and software. Digital watermarks may be used in audio, video, images, printed documents, music and any digital or analog format. The watermarks are made very difficult to remove, and if removed, there would be a distortion of the IP material.
The greatness of digital solutions to protect IP rights is that they are also covered by most countries IP′ legislation. The United States copyright law (17 USC), §120 prohibits circumvention of copyright protection systems. §1201(a) specifically says: «no person shall circumvent a technological measure that effectively controls access to a work protected under this title.» 17 USC §1201(b) even condemns the import, offer to the public, supply of and traffic in technology, services, parts or components thereof, and products designed, market or used to circumvent copyright protection systems. This means US copyright laws not only prohibit the action of violating or circumventing digital protection systems but also the act of trading on these products.

4- See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, available:
http://www.wipo.int/wipolex/en/text.jsp?file_id=126789
Chapter III- SUI Generis Right, Article 7:
«1- Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database…»

5- See Briefing Note - Protection of Computer Software - A Synopsis of Intellectual Property Rights, available:
http://www.gillhams.com/articles/174.cfm

A survey of small and medium-sized enterprises (SMEs) has demonstrated that the most common methods they employ to protect computer software are copyright, technical systems of protection, licensing and secrecy. They apparently patent less, as they find the system complicated, expensive and do not view patents as conferring any particular advantage for their software-based products. Patenting was thought to be laborious and complex and made no sense in the fast pace development environment of software development. They think that patenting is not particularly appropriate for their software products as other forms of intellectual property protection, such as informal methods - technical systems and licensing - are equally effective. The most effective technical systems of protection involved use of dongles, encryption, stenographic techniques, key diskettes, firewalls and passwords.
The survey found that 27% of the SMEs interviewed regard licensing as the most effective means of protection and 24% ranked technical systems of protection as the most important means. 21% found copyright effective, while only 8% thought that patents were of any use.

6- ccTLD: Country Code Top Level Domain Name: Country-code Top-level Domains (ccTLDs) are two-letter top-level domains especially designated for a particular country or autonomous territory to use to service their community. Available:
http://www.iana.org/domains/root/cctld/

٧- من المفيد الإشارة إلى أن هناك نوعين من الحماية القانونية لبرمجيات الحاسوب: النوع الأول المحمي بموجب قوانين حماية حق المؤلف والنوع الثاني المحمي بموجب قانون براءات الاختراع. وهذا النوع يتعلق بالبرمجيات التي لديها مفعول تقني أو صناعي أي للبرمجيات المعدة للصناعة. يراجع:
Patent Protection, available:

http://www.softwareprotection.com/patent.htm

More than half of the 170+ countries in the world that grant patents permit the patenting of software-related inventions, at least to some degree. There is a worldwide trend in favor of adopting patent protection for software-related inventions. This trend accelerated following the adoption in 1994 of the TRIPS Agreement, which mandates member countries to provide patent protection for inventions in all fields of technology, but which stops short of mandatory patent protection for software per se.
The most widely followed doctrine governing the scope of patent protection for software-related inventions is the «technical effects» doctrine that was first promulgated by the European Patent Office (EPO). This doctrine generally holds that software is patentable if the application of the software has a «technical effect.» Thus, for example, software that controls the timing of an electronic engine is patentable under this doctrine, whereas software that detects and corrects contextual homophone errors (e.g., «there» to «their») may not be patentable.
The EPO law regarding patentability of software tends to be somewhat more liberal than the individual laws of some of the EPO member countries that conduct substantive examinations of applications on the merits. Thus, one desiring to patent a software-related invention in Europe may choose to file an EPO application designating the EPO countries in which protection is sought, rather than filing separate patent applications in individual EPO countries. An EPO application, after allowance, is then granted in force within the selected countries.
For each country, the exact nature of software patentability is a complicated question. Even in countries that are liberal in granting patents on computer software, certain limitations apply. For example, in the United States and Japan, software that affects a physical process may be patentable. If the software preempts a mathematical algorithm, however, it is not patentable.
Obtaining patent protection for any invention, including software, is relatively expensive. For each country in which patent protection is sought, the cost is typically several thousands of dollars in attorney fees, patent draftsman charges, and governmental fees. Why, then, would one seek patent protection for software rather than rely upon copyright protection? First, a patent is valid against everyone in that country who makes, uses or sells the patented invention, even if the infringer invented it independently. In the United States, a provisional patent application may be filed on a software-related invention to preserve priority of invention that may then be perfected as domestic and international patent rights. Second, while copyright law protects only the expression of an idea, patent law protects the underlying idea, provided the idea is within the statutory categories of patentable subject matter and is not so fundamental that it constitutes a law of nature. Thus, for example, under U.S. patent law a mathematical algorithm is not patentable if the patent claim preempts the entire algorithm, but may be patentable if it applies the algorithm to accomplish a specific technical purpose. Finally, because many software products are mass-marketed without a signed license agreement, the strong protection provided by patent laws is increasingly important.

8- See Copyright Protection, available:
http://www.softwareprotection.com/copyright.htm
The trend is strongly toward express statutory protection for software in copyright laws around the world. Statutory protection has become increasingly important because more software is mass-marketed through traditional channels or distributed from a website without a signed license agreement (although in many instances with a «clickwrap» license agreement). In many countries, courts have held software to be within the subject matter protection of existing copyright law. Generally, copyright laws protect the form of expression of an idea, but not the idea itself. With respect to software, this typically means that the computer program, in both human-

readable and machine-executable form, and the related manuals are eligible for copyright protection, but the methods and algorithms within a program are not protected expression. Source code and object code are protected against literal copying. In addition, certain nonliteral elements of expression (including the structure, sequence, organization and «look and feel» of a program) have sometimes been afforded protection under U.S. copyright law. This trend has not clearly surfaced in foreign courts. Therefore, the current scope of protection of software under U.S. law is, at least in this respect, probably broader than under any foreign law.

9- See 2009 Update: International Legal Protection for Software Chart, by International Legal Protection for software, available: http://www.softwareprotection.com/chart.htm#EAPC.
This chart can be used to determine if subject matter protection is currently available in a particular country for either a U.S. or foreign party's software, and whether it is protected under «Copyright» or «patent» law, example:
- Oman: Computer software is protected under the «Law for the Protection of Copyright and Neighboring Rights» (Law No. 37/2000), which came into force on May 21, 2000
- Qatar: Computer software is protected under the Qatar Copyright Law, which came into force on October 3, 2002;
- Egypt: Computer software is expressly protected under the Intellectual Property Rights Code, effective June 3, 2002
- Kuwait: Computer software is expressly protected under the Decree Law No. 64/1999 Relating to Intellectual Property Rights, which became effective on February 9, 2000
- Saudi Arabia: new Saudi Arabia Copyright Law, which expressly protects computer software, became effective on March 14, 2004
- UAE: In 2002, the United Arab Emirates enacted a Copyright Law, Federal Law No. 7 of 2002. The law, which repealed the previous law, includes computer programs as a protected category of works.

10- See International Legal Protection for software, available:
http://www.softwareprotection.com/copyright.htm
A common requirement of copyright laws is that a work be original. Originality means that a work has been created independently and is the personal expression of the author. This factor must be distinguished from the concept of novelty, which usually is not required. Proof of originality is assisted in some jurisdictions by registration of a work with specified regulatory authorities. Independent development is a defense to a claim of copyright infringement or trade secret misappropriation, but not to a claim of patent infringement.

11- An algorithm is a specific set of instructions for carrying out a procedure or solving a problem, usually with the requirement that the procedure terminate at some point. Specific algorithms sometimes also go by the name method, procedure, or technique.
http://wiki.answers.com/

١٢- تمييز فرنسي، هيئة عامة، قرار تاريخ ٧ آذار ١٩٨٦، JCP، ١٩٨٦، II-٢٠٦٣١.

13- See International Legal Protection for Software, available:
http://www.softwareprotection.com/copyright.htm.
The exclusive rights of a copyright holder that are recognized and protected by most copyright laws are the rights to reproduce or copy, adapt (i.e., prepare derivative works), distribute and publicly perform the work. The precise nature of these rights, however, often differs among countries. The exclusive right to display is not generally recognized outside the United States, except to the extent that it may be covered by the moral right of disclosure.
A number of countries, and the EU Software Directive as well, also recognize «moral rights,» which may include the right to be known as the author of the work (right of paternity), the right to prevent others from distorting the work (right of integrity), the right to control publication of the work (right of disclosure) and the right to withdraw, modify or disavow a work after it has been published (right of withdrawal). Moral rights protection reflects the view that the individual, not only the work, is to be protected. The scope of these rights varies among the countries that protect moral rights of authors. The Berne Convention recognizes only the first two moral rights above. In most such jurisdictions, agreements to waive or transfer moral rights are not enforceable. In those countries where moral rights are protected, such rights may restrict the transferee of the software (such as the party who commissioned the work) from making changes to the software without the express consent of the original author.

14- See The Digital Millennium Copyright Act of 1998, available:
http://www.copyright.gov/legislation/dmca.pdf

Title III: Computer Maintenance Or Repair

Title III expands the existing exemption relating to computer programs in section 117 of the Copyright Act, which allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The exemption only permits a copy that is made automatically when a computer is activated,

and only if the computer already lawfully contains an authorized copy of the program. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.

15- See The Law and Economics of Reverse Engineering, Written by Pamela Samuelson and Suzanne Scotchmer, 30 April 2002, available:
http://www.yalelawjournal.org/the-yale-law-journal/content-pages/the-law-and-economics-of-reverse engineering/
Reverse engineering has a long history as an accepted practice. What it means, broadly speaking, is the process of extracting know-how or knowledge from a human-made artifact. Lawyers and economists have endorsed reverse engineering as an appropriate way to obtain such information, even if the intention is to make a product that will draw customers away from the maker of the reverse-engineered product. Given this acceptance, it may be surprising that reverse engineering has been under siege in the past few decades.
While some encroachments on the right to reverse-engineer have been explicit in legal rulemaking, others seem implicit in new legal rules that are altogether silent on reverse engineering, including the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the Economic Espionage Act of 1996 (EEA). TRIPS is an international treaty that, among other things, obligates member states of the World Trade Organization to protect trade secrets, yet it neither requires nor sanctions a reverse engineering privilege. The EEA created the first federal cause of action for trade secrecy misappropriation. Its lack of a reverse engineering defense has troubled some commentators because rights granted under the EEA arguably implicate certain reverse engineering activities previously thought to be lawful.

١٦- وقد تحمى أيضا قواعد وبنوك البيانات عبر المسؤولية المدنية من أي أعمال تعد أو منافسة غير مشروعة أو طفيلية. ولقبول سماع الدعوى يجب إثبات الفعل الضار والضرر والرابطة السببية بينهما. ولأجل تطبيق مبدأ المنافسة الطفيلية تفتَرض بعض القوانين وجوب أن يثبت المدعي انه قام بمجهود ترويجي واستثمار وقد قام المنافس الطفيلي بالاستفادة من هذا الترويج، إلا أن المحاكم لم تفرض وجوب إثبات هذه العناصر الثلاثة واكتفت بحصول الفعل الضار فقط لتطبيق نظرية المنافسة الطفيلية.
المنافسة الطفيلية: هي عبارة عن قيام أحد الأشخاص بالاستفادة من الشهرة والسمعة الطيبة اللتين اكتسبهما الغير بصورة مشروعة نتيجة جهده الشخصي دون أن يؤدي ذلك بالضرورة إلى أي خطر التباس يصيب الجمهور، ومثال على ذلك هو استعمال أساليب دعاية ناجحة معدة لصنف معين يعود للغير من أجل استقطاب الزبائن وتحويلهم نحو بضاعة من صنف آخر يختلف تماماً عن الأول.)راجع: المنافسة غير المشروعة والاحتكار في القانون الكويتي، إعداد محمد مبارك فضيل البصمان الرشيدي، ٢٠٠٦-٢٠٠٨).

See Protection of databases, by Daniel R Zuccherino, available:
http://www.managingip.com/Article/2677142/Magazine-Briefing/Protection-of-databases.html
Databases have acquired – in the digital era – paramount importance for commercial activities, since they gather information that can be used, for example, to design marketing programmes (databases containing information about potential clients) or reducing risks when granting credits (databases containing the credit history of a person).As the creation of these databases generally entails significant investment, creators have looked for the best way of legally protecting their investment.One basic tool for obtaining such protection is the unfair competition legal regime, which tries to avoid parasitic activities.In Argentina, based on Article 10 bis of the Paris Convention and local rules, and in the context of the mentioned unfair competition regime, it is possible to take legal steps in order to obtain protection for databases.However, the legal framework of the unfair competition regime is still incomplete, since there are isolated rules and not an organic regime of unfair competition, and court enforcement is still scarce.Another legal tool for obtaining protection is the rules that protect copyright. These, however, require originality as an excluding requirement, limiting the acknowledgment of the exclusive right to original databases.
Section 2.5 of the Bern Convention envisages protecting compilations that are literary or artistic works, while certain progress was also made with the approval of the TRIPS Agreement, which established that although the compiled data lack originality, protection can be obtained under the TRIPS system when the selection or arrangement of the data can be assimilated to an intellectual creation.
With protection contract clauses, the disadvantage is that such contract clauses are not enforceable against third parties that are not related to the license of use of the database.
In order to not leave non-original databases unprotected, certain countries have recognized a sui generis right, regardless of any originality criterion (the European Union and Mexico have acted in this way).
Under Argentine law, databases are mainly protected by copyright law 11,723. Legal authors generally claim that the protection granted by said law is limited to original databases, and since Argentine laws do not acknowledge a sui generis right, legal protection of databases could be understood as limited only to such original databases.
However, in several judgments (for example Errepar and Axesor) courts have acknowledged protection to database creators that have been damaged by the parasitic activities of competitors trying to take advantage of the creators> efforts and investment.

17- See Database protection, available:
http://www.ipr-helpdesk.org/documents/ES_Databases_0000006544_00.xml.html
There are two main bases for database protection: copyright protection (under the condition of creativity) and new *sui generis* protection (under the condition of substantial investment). Copyright protection has an international character (databases are protected in almost

all countries in the world), whereas *sui generis* protection is obtained for persons from the EU only in EU countries. Persons from outside the EU may obtain protection only under the condition of reciprocity if, in their country, such protection is introduced. For example, the USA does not provide *sui generis* protection as such. Under EU law, cumulative protection of databases is possible under copyright and the sui generis right.
Neither copyright protection nor *sui generis* protection creates a new or additional protection for each individual element of a database. Database protection provides protection for a database only as a compilation.

18- See iLaw Eurasia 2004 Emerging Legal and Policy Issues for the Information Age, 15 December 2004, available:
http://cyber.law.harvard.edu/ilaw/eurasia_2004_schedule/wednesday
Database Protection and Recent Caselaw
In November 2004, the European Court of Justice (ECJ) has handed down judgments in four cases concerning the interpretation of the EU Directive on the Legal Protection of Databases, which provides a «sui generis database right» (to be distinguished from copyright) to the maker of a database if there has been a substantial investment in either the obtaining, verification or presentation of the contents of the database. The cases relate to similar factual circumstances and concern databases of sporting information (horse racing information and football fixture lists.) Certain pieces of information from these databases were used by third parties for commercial gambling operations. In proceedings before the relevant national courts, the claimants alleged that these uses by the gambling operators were an infringement of the claimants> sui generis rights under the Directive. In each case, the national courts referred a set of questions to the ECJ.
In these cases, the ECJ, inter alia, now has clarified the definition of the term «database» as used in the Directive; determined the scope of protection (especially with regard to the «substantial investment» requirement); and, specified the infringement of the sui generis right through extraction or re-utilization.
Taken together, these several doctrinal areas – copyright, trademark, patent, database protections and so forth – present extremely important issues, especially for developing countries, related to the control of knowledge necessary to compete in the global economy.

19- See Database legal Protection, available:
http://www.bitlaw.com/copyright/database.html
Databases as Compilations: Databases are generally protected by copyright law as compilations. Under the Copyright Act, a compilation is defined as a «collection and assembling of preexisting materials or of data that are selected in such a way that the resulting work as a whole constitutes an original work of authorship.» 17. U.S.C. § 101. The preexisting materials or data may be protected by copyright, or may be unprotectable facts or ideas.
An example of a database that is protected as a compilation would be a database of selected quotations from U.S. Presidents. The individual quotations themselves may or may not be subject to copyright protection. However, the selection of the quotations involves enough original, creative expression that it is protected by copyright. Therefore, a database of quotations will be protected by copyright as a compilation even though some of the quotations are not protected.
A database of facts is also protected as a compilation, assuming the grouping contains enough original expression to merit protection. An example of a protectable grouping of facts would be a database of Internet locations for selected legal articles. Each location consists merely of factual information, namely that a particular article can be found at a particular URL location on the Internet. There is no copyright protection for each location. Therefore, while the individual locations can be copied by others, if an entire database of locations (or a substantial portion of the database) were copied, the copyright in the compilation would be infringed. The creative, original expression that is being protected is the selection of locations for the database. If the locations were divided by topic in the database, the organization of the database would also be protected.

20- See Works Unprotected by Copyright Law, available:
http://www.bitlaw.com/copyright/unprotected.html.
Some types of material are ineligible for copyright protection. Generally, these materials are either protected by some other intellectual property, or have been considered inappropriate for protection. The following unprotected works are discussed in greater detail below:
Ideas, procedures, principles, discoveries, and devices are all specifically excluded from copyright protection. As stated in the Copyright Act: «In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.» This specific exclusion helps maintain the distinction between copyright protection and patent law. Ideas and inventions are the subject matter for patents, while the expression of ideas is governed by copyright law. If copyright were extended to protect ideas, principles and devices, then it would be possible to circumvent the rigorous prerequisites of patent law and secure protection for an invention merely by describing the invention in a copyrightable work.

21- See Database protection, available:
http://www.ipr helpdesk.org/documents/ES_Databases_0000006544_00.xml.html#N20063
Sui generis protection was introduced in the EU by database directive from 1996 (directive 96/9/EC on the legal protection of databases). Under that directive, database producers obtain new *sui generis* protection. This form of protection should not affect the rights of the creators of works incorporated in the contents of a database.
Condition of sui generis protection: Protection is granted if a substantial investment is made to obtain, verify, and present database content. A substantial investment is the deployment of financial resources and/or the expenditure of time, effort, and energy to generate and present the database content. Protection applies to the whole of a database or a substantial part (measured qualitatively or quantitatively).
It should be pointed out that an investment to generate data that goes into the database is not considered an investment in creating the database itself and therefore cannot be grounds for protection. This is meant to prevent monopolization of the information itself.
Content of SUI generis right: Sui generis right consists of two rights:
- The right to extract all or a substantial part of the database and
- The right to re-use all or a substantial part of the database.

The former is similar to the right of reproduction, the latter to the right of distribution granted to a copyright holder.

22- See Database protection, available:
http://www.ipr- helpdesk.org/documents/ES_Databases_0000006544_00.xml.html#N20063.
The duration of rights of the database producer right is 15 years from the completion of the database. If a new substantial investment is made to an existing database, the creator can gain a new right to the altered (e.g. updated or supplemented) database or its substantial part.

23- IP crime Report – Annual report 2009-2010, available:
http://www.ipo.gov.uk/ipcreport09.pdf

24- See Copyright Act, Chapter9- Protection of Semiconductor Chip Products (§§ 901—914), available:
http://www.copyright.gov/title17/92chap9.html#901

25- See Chip Protection in Europe, by Dr. Thomas Hoeren, available:
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf
Topography is capable of protection if it is «the result of its creator′s own intellectual effort and is not commonplace in the semiconductor industry» (Article 2 (2)) of the EU directive (87/54/EEC). This standard of «originality» was interpreted as being the main reason for the sui generis protection system. It is said that copyright and patent law require a very high standard of originality or inventiveness. With regard to this standard, most topographies will remain unprotected under «traditional» industrial property law.

26- See Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, available:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31987L0054:EN:HTML
There is an obligation on Member States to adopt legislation to protect topographies in so far as they are the result of their creator′s own intellectual effort and are not commonplace in the semiconductor industry.
The right to protection is granted to the person who is the topography′s creator, subject to that person being a natural person who is a national of a Member State or ordinarily resident there. However, Member States may specify to whom the right is granted where a topography is created in the course of the creator′s employment or under a contract other than a contract of employment.
Under certain conditions, protection is also granted to natural persons, companies or other legal persons who first commercially exploit a topography:
- which has not previously been exploited commercially and;
- who have been exclusively authorized to commercially exploit the topography throughout the Community by the person entitled to dispose of it.

The Directive lays down the procedure for extending the right to protection to persons not covered by the Directive.

27- See Chip Protection in Europe, by Dr. Thomas Hoeren, available:
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf
The exclusive rights to exploit or import a semiconductor product are exhausted after the product has been put on the market in a member state by the person entitled to authorize its marketing or with his consent (art.5 (5)). This rule refers to the traditional «exhaustion doctrine».
In the Netherlands, the exclusive rights include any kind of exploitation of a protected topography, even if it is not commercial. Therefore, art 1 (e) forbids to exploit a topography without the consent of the right holder.

28- See Chip Protection in Europe, by Dr. Thomas Hoeren, available:
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf
According to the Directive(87/54/EEC), the EC member states have the option of requiring registration and, additionally, the deposit of materials describing or exemplifying the topography (art. 4).
The copyright approach toward chip protection was adopted by the United Kingdom, Ireland26 and Belgium. These states established an unregistered right. In the United Kingdom, the legislator was unanimous on the very nature of chip protection. Initially, 1987, it enacted the Semiconductor Products (Protection of Topography) Regulations in 1987. These regulations, which very much resembled the EC Directive, have been replaced by the Design Right [Semiconductor Topographies] Regulations 1989. These Regulations implemented a modified version of the design right It differs on various points from the SCPA and the EC Directive. The protection is extended to any design document for a semiconductor product, i. e., «any record of a design, whether in the form of a drawing, a written description, a photograph, data stored in a computer or otherwi -se» (section 263 (1)). These documents are protected against any importation or commercial dealing under the condition that they are not commonplace. The regulations do not define originality in terms of «the creator′s own intellectual effort». Furthermore, the configuration of the interfacing area of the topography and its structure in electronic form are not protected because they may fall within the exception of section 213 (3) (a) and (b).
Most EC countries have followed the second option and adopted the registration system30. Thus, the creator of topographies has to apply for registration at the national patent office or (in Spain) alternatively with the Provincial Directorates of the Ministry of Industry and Energy. In addition to the registration, material identifying or exemplifying the topography must be deposited with a public authority. Material deposited is, however, not made available to the public as it is regarded as a trade secret. The registration and deposit of topographies has to be paid for by the right holder. The fees differ from approximately $ 25 up to $ 400.
See Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31987L0054:EN:HTML
Member States may refuse or remove protection in respect of the topography of a semiconductor product where an application for registration in due form has not been filed with a public authority within two years of its being commercially exploited for the first time. They may require that material identifying or exemplifying the topography be deposited. However, they must ensure that material deposited is not made available to the public where it is a trade secret.

29- See Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31987L0054:EN:HTML
The rights granted are exclusive rights. They include the right to authorise or prohibit reproduction of a protected topography and the right to authorise or prohibit commercial exploitation or the importation for that purpose of a topography or of a semiconductor product manufactured using the topography. The exclusive right to authorise or prohibit reproduction does not apply to the reproduction for the purpose of analysing, evaluating or teaching the concepts, processes, systems or techniques embodied in the topography or the topography itself.
Where registration of the topography constitutes a condition for the coming into existence of exclusive rights, those rights will take effect on the date on which the application for registration is filed or on the date on which the topography is first commercially exploited anywhere in the world, whichever comes first. If registration is not a condition for protection, the rights will come into existence when the topography is first commercially exploited anywhere in the world or when it is first fixed or encoded.
The exclusive rights come to an end 10 years from the end of the calendar year in which the topography was first commercially exploited. Where registration is required, the 10-year period is calculated from the end of the calendar year in which the application for registration was filed or from the end of the calendar year in which the topography was first commercially exploited, whichever comes first.

31- See Chip Protection in Europe, by Dr. Thomas Hoeren, available:
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf
Reverse Engineering:
The reproduction of topography for private, non-commercial purposes and for analyzing or evaluating its concepts cannot be prohibited by the right holder. Even the development of a new topography based on such an analysis does not infringe on the exclusive reproduction right of the author if it is the result of the creator′s own intellectual effort (reverse engineering).
As Hart has already pointed out, there are some discrepancies between the reverse engineering provisions laid down in the US Semiconductor Chip Protection Act and those of the EC Directive. In the U. S., reverse engineering permits the incorporation of a first chip into another original mask work, while under the Directive; it is only permissible to create a new (original) topography on the basis of the analysis or evaluation of another topography.
In Europe, this exception has led to considerable debate. The discussion focuses on the question whether reverse engineering is allowed under «traditional» patent or copyright law. Some authors state that reverse engineering is a new principle of chip protection law. This view has, however, in legal doctrine been rejected by various authors. They try to demonstrate that reverse engineering has to be regarded a traditional rule of industrial property law. In their view, patent law has always permitted the analysis of a protected invention

and the use of the results of this analysis to produce a «new» (original) invention. Even in copyright law, a protected work may be analyzed, the results of which may be used in order to create a individual work.

32- See Chip Protection in Europe, by Dr. Thomas Hoeren, available:
http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/036.pdf
The legal situation outside the EC:
- Sweden: Sweden has been the first European country to enact special regulations for the protection of microchips. First, the Swedish Government set up a Commission which investigated the ways of protecting computer technology under copyright law. This Commission emphasized in its report (published in 1986) that semiconductor products may be efficiently protected under traditional copyright law. A sui generis protection with regard to chips was held to be unnecessary. Unfortunately, the legislature did not follow this recommendation. The Swedish Act on the Protection of the Layout-Design in Semiconductor Products entered into force on April 1, 1987. The Swedish Act protects the layout-designs in their two-dimensional forms (drawings and masks) and in their three dimensional forms (semiconductor products). Under the Act, the creator of the layout-design has the exclusive right to copy the design, to transfer it onto or into a material support, and to make the design available to the public (Sect. 1 (1)). Further, the Act contains provisions on innocent infringement and the exhaustion of rights (Sect.3).
The act lacks a provision on reverse engineering. Instead, it provides that copies may be made for teaching on, or analysis of, the design. The reproduction of single copies for private use is also allowed (Sect. 2 (1)). As the Swedish delegation at the WIPO Session stated, reverse engineering may be regarded as lawful copying for the purpose of analysis. Hence, a special provision was considered unnecessary. The Swedish legislator has opted for protection without any formalities, similar to the position under copyright law. The layout design will be protected upon its creation. Protection is available up till the end of the 10th year after the year when the layout-design was first commercially exploited (Sect. 1 (2)).
The sanctions laid down in the act are more severe than those of the EC Directive. For instance, an infringer is held to be liable for damages even if he has acquired a topography or semiconductor product in good faith. The innocent infringement doctrine has only been used to protect an infringer from surrender and destruction of his unlawful copies. Apart from these very innovative characteristics, the Swedish act contains two regrettable elements:
  - protection has only been extended to layout designs created by Swedish nationals or domiciliaries, and to layout designs first distributed in Sweden. Other foreign layout designs may only be protected under the condition of a corresponding government proclamation on the basis of material reciprocity.
  - The Swedish Copyright Act has been amended in that layout designs protected by the Semiconductor Protection Act are not copyrightable. In spite of the «originality» of the Swedish provisions, the act has been accepted by the United States as corresponding to the requirements under the SCPA. Meanwhile, Finland4 7 and Norway4 8 seem to adopt the Swedish model in their chip protection law. Thus it appears that a uniform Scandinavian way of chip protection is going to be established.
  - Switzerland: Chip protection has been regarded by the Swiss Government as a matter of competition law. Consequently, the Swiss delegate at the second WIPO Session49 stated that chip piracy constitutes an unfair act according to Article 5 (c) of the new Unfair Competition Act50. This Article prohibits the appropriation and exploitation of another's marketable product «as such by means of a technical reproduction process without adequate personal expenditure».
In the meantime, the Swiss legislature has drafted a new topography act, which has been presented to the Parliament on June 19, 198951. The draft contains all characteristic elements of the EC Directive and resembles the German Chip protection act. This hasty retreat may only be regretted.

33- Copyright law does not protect domain names. The Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization that has assumed the responsibility for domain name system management, administers the assignation of domain names through accredited registers.

34- See S.1255 – Anticyber squatting Consumer Protection Act (Introduced in Senate - IS), available:
http://thomas.loc.gov/cgi-bin/query/z?c106:S.1255.IS

35- See Model Law Guidelines- Report on Consensus points for trademark laws, by International Trademark Association, available:
http://www.inta.org/Advocacy/Documents/INTAModelLawGuidelines.doc
«*... To some extent the practice of cyber squatting has been mitigated by the establishment by ICANN (the International Corporation of Assigned Names and Numbers) of the Uniform Dispute Resolution Procedure (UDRP), which applies to the generic top-level domain names ("gTLD's"). However, sanctions against cyber squatting should also be backed by similar dispute resolution mechanisms in the country-code top-level domain names ("ccTLD's") (where not already implemented) and by appropriate national legislation, such as the Anticyberpiracy Consumer Protection Act in the United States, which was enacted on November 29, 1999 and made a part of the federal trademark laws. The dispute resolution mechanisms and legislation should make it clear that cyber squatting is indeed a form of illegal commercial activity*.»

36- UDRP: Uniform Domain Name Dispute Resolution Policy: The Uniform Domain-Name Dispute Resolution Policy (UDRP) has been adopted by ICANN-accredited registrars in all gTLDs (.aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel). Dispute proceedings arising from alleged abusive registrations of domain names (for example, cybersquatting) may be initiated by a holder of trademark rights. The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars., available:
http://www.icann.org/en/udrp/

37- See Rules for Uniform Domain Name Dispute Resolution Policy (the «Rules»), as approved by the ICANN Board of Directors on 30 October 2009, available:
http://www.icann.org/en/dndr/udrp/uniform-rules.htm

نص إرشاد حقوق الملكية الفكرية في المجال المعلوماتي والسيبراني

الباب الأول: أحكام عامة

المادة ١: تعاريف

المنتج شبه الموصل: هو الشكل النهائي أو الوسيط لكل منتج يكون:

- مؤلفاً من جوهر يتضمن طبقة من مواد شبه موصلة.
- مكوناً من طبقة أو عدة طبقات أخرى من مواد موصلة وعازلة أو شبه موصلة، وتكون الطبقات مرتبة وفقاً لخريطة ذات أبعاد ثلاثية معينة.
- معدّاً للقيام، حصرياً أو بصورة غير حصرية، بوظيفة إلكترونية.

طوبوغرافيا المنتج شبه الموصل: هي سلسلة صور مربوطة ببعضها، أياً كانت المادة المُثبّتة أو المُرمّزة بواسطتها، وهي تتمتع بالخصائص التالية:

- تمثّل الطوبوغرافيا الخريطة الثلاثية الأبعاد للطبقات التي تشكّل منتجاً شبه موصل.
- في الطوبوغرافيا، كل صورة تمثّل الرسم أو جزءاً من الرسم العائد لسطح أو لإحدى طبقات المنتج شبه الموصل في أية مرحلة من مراحل صنعها.

الاستثمار التجاري: هو البيع أو التأجير أو أية وسيلة للتوزيع التجاري أو أي عرض مقدّم للغايات المذكورة.

اسم الموقع: هو ما يعبّر بحروف الأبجدية وبالأرقام عن العنوان الرقمي المعين لموقع إلكتروني على شبكة الإنترنت.

رمز النطاق على المستوى الوطني: يعرّف أسماء مواقع الإنترنت التي تختص ببلد معين (مثلاً lb.)، وهو يتواجد في القسم الأخير من رمز اسم الموقع وفق نظام العنونة لشبكة الإنترنت.

الباب الثاني: الحماية القانونية لبرامج الحاسوب (البرامج المعلوماتية)

المادة ٢: حماية البرامج المعلوماتية بموجب حق المؤلف

وفق أحكام الإرشاد الحالي، تحمي الدول الأعضاء برامج المعلوماتية بموجب حق المؤلف كعمل أدبي بالمعنى المنصوص عليه في اتفاقية برن لحماية الأعمال الأدبية والفنية. إن مصطلح «برنامج معلوماتي»، وفق هذا الإرشاد، يتضمن مواد أعمال التصميم التحضيرية.

إن الحماية المنصوص عليها في هذا الإرشاد تطبق على كل شكل للتعبير عن برنامج معلوماتي. إن الأفكار والمبادئ التي تشكل أساس بعض عناصر برنامج معلوماتي، بما فيها تلك التي تشكل أساس عناصر التواصل والتخاطب، ليست محمية بموجب حق المؤلف وفق هذا الباب من الإرشاد.

إن البرنامج المعلوماتي يكون محمياً إذا كان مبتكراً، بمعنى أنه يكون الابتكار الذهني والفكري الخاص بمؤلفه. لا يطبق أي معيار آخر لتحديد البرامج المحمية بموجب هذا الباب من الإرشاد.

المادة ٣: صفات صاحب حق المؤلف للبرنامج المعلوماتي

إن مؤلف البرنامج المعلوماتي هو كل شخص طبيعي أو مجموعة من الأشخاص الطبيعيين ابتكروا البرنامج، أو عندما تسمح بذلك التشريعات الوطنية لدولة عضو، يكون أيضاً الشخص المعنوي المُعتبر بموجب التشريعات الوطنية صاحب حق المؤلف.

عندما تعترف التشريعات الوطنية لدول عضو بالأعمال الجماعية، فإن الشخص المُعتبر بموجب التشريعات المذكورة كمُبتكِر للعمل يكون هو أيضاً المؤلف.

عندما يتم ابتكار برنامج معلوماتي بالاشتراك من قبل عدة أشخاص طبيعيين، فإن الحقوق الحصرية للمؤلف تعود بالاشتراك لهؤلاء الأشخاص.

عندما يتم ابتكار البرنامج المعلوماتي من قبل مُستخدِم بمعرض ممارسته لوظيفته أو وفق تعليمات صاحب العمل، يكون صاحب العمل هو المخوّل ممارسة الحقوق المادية المتعلقة

بالبرنامج المعلوماتي، باستثناء حالة وجود بنود تعاقدية مخالفة.

المادة ٤: المستفيدون من الحماية القانونية بموجب حق المؤلف للبرنامج المعلوماتي

تُعطى الحماية لكل شخص طبيعي أو معنوي يستفيد من أحكام التشريعات الوطنية في نطاق حقوق المؤلف المطبّقة على الأعمال الأدبية.

المادة ٥: حقوق صاحب حق المؤلف لبرنامج معلوماتي

مع مراعاة المادتين ٦ و٧ من هذا الإرشاد، فإن الحقوق الحصرية لصاحب حق المؤلف تتضمن حق فعل أو الترخيص بما يلي:

- نسخ وإعادة إنتاج العمل بشكل دائم أو مؤقت للبرنامج المعلوماتي، جزئياً أو كلياً، بأية وسيلة كانت وبأي شكل كان. عندما تتطلب أعمال تحميل البرنامج المعلوماتي أو عرضه أو تنفيذه أو نقله أو تخزينه ضرورة نسخه أو إعادة إنتاجه، فإن هذه الأعمال تخضع للترخيص من قبل صاحب حق المؤلف.
- ترجمة البرنامج المعلوماتي وتكييفه وإعادة ترتيبه وكل تحويل له وإعادة إنتاج البرنامج الناتج عن ذلك، مع حفظ حقوق الشخص الذي تولى تحويل البرنامج المعلوماتي.
- كل شكل من أشكال التوزيع والنقل، بما فيه التأجير، للجمهور للنسخة الأصلية للبرنامج المعلوماتي أو لنسخه.

المادة ٦: استثناءات على الحماية بموجب حق المؤلف للبرنامج المعلوماتي

باستثناء حالة وجود بنود تعاقدية مخالفة، لا يخضع للترخيص من قبل صاحب حق المؤلف الأعمال المذكورة في الفقرتين (أ) و(ب) من المادة ٥ من هذا الإرشاد، عندما تكون هذه الأعمال ضرورية من أجل تمكين المستخدم الشرعي من استعمال البرنامج المعلوماتي بطريقة ملائمة للغرض الذي وضع من أجله، ومن ضمنها تصحيح الأخطاء.

إن الشخص الذي له الحق باستخدام البرنامج المعلوماتي لا يمكن منعه من صنع نسخة للحفظ عن هذا البرنامج طالما أنها ضرورية لاستخدام البرنامج.

إن الشخص المخوّل استخدام نسخة من البرنامج المعلوماتي يستطيع، دون ترخيص من صاحب حق المؤلف، مراقبة طريقة عمل البرنامج أو دراستها أو فحصها، من أجل تحديد الأفكار والمبادئ التي تشكل أساس أي عنصر في البرنامج، وذلك عندما يقوم هذا الشخص بكل عملية تحميل أو عرض أو تنفيذ أو نقل أو تخزين للبرنامج.

المادة ٧: إعادة إنتاج البرمجيات

لا يُطلب ترخيص صاحب حق المؤلف، عندما تكون إعادة إنتاج البرمجيات (حل شيفرة البرنامج المعلوماتي) أو ترجمة شكل هذه البرمجيات، بالمعنى المذكور في الفقرتين (أ) و(ب) من المادة ٥ من هذا الإرشاد، ضرورية من أجل الحصول على المعلومات اللازمة لتشغيل البرنامج المعلوماتي مع برامج معلوماتية أخرى، وبشرط التقيد بالشروط التالية:

- أن يقوم بهذه الأعمال المُرخص له باستخدام نسخة من البرنامج أو أي شخص يعمل لمصلحته.
- أن تكون المعلومات اللازمة للتشغيل مع برامج أخرى مُتاحة بشكل سهل وسريع للأشخاص المذكورين في البند (أ) أعلاه.
- أن تكون هذه الأعمال محصورة بالأجزاء من البرنامج المعلوماتي اللازمة للتشغيل.

إن المعلومات المُستحصل عليها بموجب أحكام المقطع الأول من هذه المادة تخضع للمحظورات التالية:

- لا يمكن استخدام المعلومات المنوه عنها لغايات مختلفة عن تنفيذ التشغيل مع برامج معلوماتية أخرى.
- لا يمكن إعطاء هذه المعلومات للغير، إلا إذا كان ذلك ضرورياً للتشغيل مع برامج معلوماتية أخرى.
- لا يمكن استخدام هذه المعلومات لإنتاج أو تسويق برنامج معلوماتي مشابه أو من أجل كل عمل ينتهك حق المؤلف.

وفقاً لأحكام اتفاقية برن لحماية الأعمال الأدبية والفنية، لا يمكن تفسير هذه المادة بشكل يسمح بتطبيقها بطريقة تلحق ضرراً غير مبرّر بالمصالح المشروعة لصاحب حق المؤلف أو تتعرّض للاستخدام الطبيعي للبرنامج المعلوماتي.

المادة ٨: التدابير الخاصة لحماية البرامج المعلوماتية

تتخذ الدول الأعضاء، وفقاً لتشريعاتها الوطنية، تدابير وعقوبات ملائمة بحق الأشخاص الذين يرتكبون أحد الأفعال التالية:

- كل شخص يضع بالتداول نسخة لبرنامج معلوماتي مع علمه بأنها غير مشروعة أو لديه أسباب للاعتقاد بذلك.
- كل شخص يحوز لغايات تجارية نسخة لبرنامج معلوماتي مع علمه بأنها غير مشروعة أو لديه أسباب للاعتقاد بذلك.
- كل شخص يثبت قيامه بأفعال هندسة عكسية تكون غايتها خلق برنامج معلوماتي منافس ومطابق للبرنامج المعلوماتي المحمي.

المادة ٩: العلاقة مع الأحكام القانونية الأخرى

إن الأحكام القانونية المنصوص عليها في هذا الباب لا تؤثر على الأحكام القانونية الأخرى، لاسيما تلك المتعلقة ببراءات الاختراع والعلامات التجارية والمنافسة غير المشروعة وسرية الأعمال وحماية المنتجات شبه الموصلة وقانون العقود.

كل بند تعاقدي مخالف لأحكام المادة ٧ أو للاستثناءات المنصوص عليها في المادة ٦ (المقطع الثاني والثالث فقط) يكون باطلاً.

الباب الثالث: الحماية القانونية لقواعد البيانات

الفصل الأول: نطاق التطبيق

المادة ١٠: نطاق تطبيق أحكام الباب الثاني

يهتم هذا الباب بالحماية القانونية لقواعد البيانات أياً كان شكلها، ولا يطبق على البرامج المعلوماتية.
قواعد البيانات هي مجموعة أعمال أو بيانات أو عناصر أخرى مستقلة منظّمة بطريقة منهجية ويمكن الوصول إليها بوسائل إلكترونية أو بأية وسيلة.

إن الحماية القانونية المنصوص عليها في هذا الباب لا تطبق على البرامج المعلوماتية المُستخدمة في صنع أو طريقة عمل قواعد البيانات الممكن الوصول إليها بوسائل إلكترونية.

الفصل الثاني: الحماية القانونية لقواعد البيانات بموجب حق المؤل

المادة ١١: شروط الحماية القانونية لقواعد البيانات بموجب حق المؤلف

وفقاً لهذا الإرشاد، فإن قواعد البيانات التي، من خلال اختيار أو تنظيم المواد، تشكل ابتكاراً ذهنياً أو فكرياً خاصاً بمؤلفها، تكون محمية بموجب حق المؤلف. لا يطبق أي معيار آخر لتحديد ما إذا كانت تستفيد من الحماية القانونية.

إن الحماية القانونية لقواعد البيانات بموجب حق المؤلف لا تشمل محتوى قواعد البيانات ولا تتعرض للحقوق على هذا المحتوى.

المادة ١٢: صاحب حق المؤلف على قاعدة البيانات

إن مؤلف قاعدة البيانات هو الشخص الطبيعي أو مجموعة الأشخاص الطبيعيين الذين أنشأوا قاعدة البيانات، أو عندما تجيزه التشريعات الوطنية لدولة عضو، يكون أيضاً الشخص المعنوي المُعتبر بموجب هذه التشريعات صاحب الحق.

عندما تعترف التشريعات الوطنية لدولة عضو بالأعمال الجماعية، فإن الحقوق المادية عليها تعود للشخص المُعتبر صاحب الحق.

عندما يتم إنشاء قاعدة بيانات بالاشتراك من قبل عدة أشخاص طبيعيين، فإن الحقوق الحصرية للمؤلف تعود بالاشتراك لهؤلاء الأشخاص.

المادة ١٣: الحقوق الحصرية لصاحب حق المؤلف على قاعدة البيانات

إن مؤلف قاعدة بيانات يستفيد، إذا كانت هذه القاعدة محمية بموجب حق المؤلف، من الحقوق الحصرية المنصوص عليها في المادة ٤ من هذا الإرشاد.

المادة ١٤: الاستثناءات على حقوق صاحب حق المؤلف على قاعدة البيانات

إن المستخدم الشرعي لقاعدة بيانات أو لنسخ عنها يستطيع القيام بجميع الأعمال المنصوص عليها في المادة السابقة، والتي تكون ضرورية للوصول لمحتوى قاعدة البيانات ولاستخدامها بشكل عادي من قبله، وذلك دون ترخيص من قبل مؤلف قاعدة المعلومات. في الحالة التي يكون المستخدم الشرعي مُرخصاً له باستخدام جزء من قاعدة البيانات، فإن الأحكام القانونية للمقطع الحالي تطبق فقط بالنسبة لهذا الجزء.

يمكن للدول الأعضاء وضع قيود للحقوق المنصوص عليها في المادة السابقة في الحالات التالية:

- عندما يتعلق الأمر بنسخ وإعادة إنتاج لغايات خاصة لقاعدة بيانات غير إلكترونية.

- عندما يكون الاستخدام حصرياً لغايات التوضيح في التعليم أو لغايات البحث العلمي مع موجب تحديد المصدر وفي الحدود المبرّرة بالهدف غير التجاري المُتوخى.
- عندما يكون الاستخدام لغايات الأمن العام أو لغايات متعلقة بإجراءات إدارية وقضائية.
- عندما يتعلق الأمر باستثناءات أخرى على حقوق المؤلف منصوص عليها تقليدياً في التشريعات الوطنية مع مراعاة الفقرات السابقة من هذه المادة.

وفقاً لأحكام اتفاقية برن لحماية الأعمال الأدبية والفنية، لا يمكن تفسير هذه المادة بشكل يسمح بتطبيقها بطريقة تلحق ضرراً غير مبرّر بالمصالح المشروعة لصاحب الحق أو تتعرّض للاستخدام الطبيعي لقاعدة البيانات.

الفصل الثالث: الحماية القانونية بموجب الحق الخاص

المادة ١٥: شروط الحماية القانونية لقاعدة البيانات بموجب الحق الخاص

تقر الدول الأعضاء لصانع قاعدة البيانات الحق بمنع استخراج وإعادة الاستعمال لكامل محتوى قاعدة البيانات أو لجزء منها، مقيّم بشكل نوعي وكمي، وذلك عندما يكون الحصول على هذا المحتوى أو التحقق منه أو تقديمه يتطلب استثماراً مهماً من الناحية النوعية أو الكمية في الأموال والتجهيزات والموارد البشرية.

لغاية هذا الفصل، تعتمد التعاريف التالية:

- منتج أو صانع قاعدة البيانات هو الشخص الذي يبادر إلى إنشائها ويتولى مسؤولية الإنتاج.
- الاستخراج هو النقل الدائم أو المؤقت لكامل محتوى قاعدة البيانات أو لجزء مهم منها على دعامة أخرى بأية وسيلة كانت أو تحت أي شكل كان.
- إعادة الاستعمال هي كل شكل من أشكال الوضع بتصرف الجمهور لكامل محتوى قاعدة البيانات أو لجزء مهم منها، وذلك من خلال توزيع نسخ عنها أو بالتأجير أو بالنقل على الخط أو تحت أشكال أخرى.

إن الحق المنصوص عليه في المقطع الأول من هذه المادة يمكن نقله أو التنازل عنه أو إعطاؤه بموجب عقد إجازة.

إن الحق المنصوص عليه في المقطع الأول من هذه المادة يطبق بالاستقلال عن إمكانية حماية قاعدة البيانات بموجب حق المؤلف أو بموجب حقوق أخرى. بالإضافة إلى ذلك، يطبق هذا الحق بالاستقلال عن إمكانية حماية محتوى قاعدة البيانات بموجب حق المؤلف أو بأية حقوق أخرى. إن حماية قاعدة البيانات بموجب الحق المنصوص عليه في المقطع الأول من هذه المادة لا يمس الحقوق القائمة على محتوى قاعدة البيانات.

يحظر الاستخراج أو إعادة الاستعمال المتكررة والمنهجية لأجزاء غير مهمة من محتوى قاعدة البيانات، والتي تفترض أعمالاً منافية للاستعمال العادي لقاعدة البيانات أو التي تسبب ضرراً غير مبرّر للمصالح المشروعة لصانع قاعدة البيانات.

المادة ١٦: حقوق مُستخدم قاعدة البيانات وموجباته

لا يستطيع صانع قاعدة البيانات، الموضوعة بتصرف الجمهور بأية طريقة، منع المستخدم الشرعي لهذه القاعدة من استخراج أو إعادة استعمال أجزاء غير مهمة لمحتواها، مقيّمة بشكل نوعي وكمي، ولأية غاية كانت. إذا كان مُرخّصاً للمُستخدِم الشرعي باستخراج أو إعادة استعمال جزء فقط من قاعدة البيانات، فإن أحكام المقطع الحالي تطبق بالنسبة لهذا الجزء فقط.

لا يستطيع المُستخدِم الشرعي لقاعدة البيانات، الموضوعة بتصرف الجمهور بأية طريقة كانت، القيام بأعمال تتعارض مع الاستثمار العادي لها أو تضر بطريقة غير مبرّرة بالمصالح المشروعة لصانعها.

لا يستطيع المُستخدِم الشرعي لقاعدة البيانات، الموضوعة بتصرف الجمهور بأية طريقة كانت، الإضرار بصاحب حق المؤلف أو صاحب الحقوق المجاورة القائمة على أعمال محتوى قاعدة البيانات.

المادة ١٧: الاستثناءات على حقوق صاحب الحق الخاص

للدول الأعضاء أن تقر أنه يعود للمُستخدِم الشرعي لقاعدة البيانات، الموضوعة بتصرف الجمهور بأية طريقة كانت، ودون ترخيص من صانع قاعدة البيانات، استخراج أو إعادة استعمال جزء مهم من محتوى قاعدة البيانات، وذلك في الحالات التالية:

- عندما يتعلق الأمر باستخراج لغايات خاصة لمحتوى قاعدة بيانات غير إلكترونية.

- عندما يتعلق الأمر باستخراج لغايات التوضيح في التعليم أو لغايات البحث العلمي، شرط ذكر المصدر وفي الحدود المبرّرة للهدف غير التجاري المتوخّى.
- عندما يتعلق الأمر باستخراج أو إعادة استعمال لغايات الأمن العام أو لغايات متعلقة بإجراءات إدارية أو قضائية.

المادة ١٨: مدة الحماية بموجب الحق الخاص

إن الحق الخاص ينتج آثاره منذ انتهاء صنع قاعدة البيانات، وينقضي بعد مرور خمس عشرة سنة تُحسب ابتداءً من الأول من كانون الثاني الذي يلي تاريخ الانتهاء من الصنع، أو ابتداءً من الأول من كانون الثاني الذي يلي تاريخ وضعها بتصرف الجمهور بأية طريقة كانت.

كل تعديل مهم مقيّم من الناحية النوعية أو الكمية، لمحتوى قاعد البيانات، لاسيما كل تعديل مهم ناتج عن تراكم الإضافات أو الإلغاءات أو التغييرات المستمرة التي توحي بوجود استثمار مهم جديد مقيّم من الناحية النوعية والكمية، يسمح بتجديد الحماية لقاعدة البيانات لمدة خمس عشرة سنة جديدة تُحسب ابتداءً من الأول من كانون الثاني الذي يلي تاريخ انتهاء تحديث قاعدة البيانات.

الفصل الرابع: أحكام ختامية

المادة ١٩: معاقبة الأفعال التي تنتهك الحقوق

تحرص الدول الأعضاء على إقرار عقوبات مناسبة للأفعال التي تنتهك الحقوق المنصوص عليها في هذا الباب.

المادة ٢٠: الطابع الآمر والإلزامي لبعض المواد

تعتبر البنود التعاقدية المخالفة لأحكام الفقرة الأولى من المادة ١٤ ولأحكام المادة ١٦ من هذا الإرشاد باطلة.

الباب الرابع: الحماية القانونية للمنتجات شبه الموصلة

المادة ٢١: شروط حماية المنتجات شبه الموصلة

تحمي الدول الأعضاء طوبوغرافيا المنتجات شبه الموصلة بإقرار التشريعات التي تعطي حقوقاً حصرية عليها وفقاً لهذا الباب من الإرشاد.

إن طوبوغرافيا المُنتَج شبه الموصل هي محمية طالما أنها ناتجة عن الجهد الفكري والذهني لمُبتكرها وليست شائعة في قطاع شبه الموصلات. عندما تتكون طوبوغرافيا المنتَج شبه الموصل من عناصر شائعة في قطاع شبه الموصلات، تكون محمية فقط طالما أن تجميع هذه العناصر، كمكون واحد، يلبي الشروط المنوه عنها أعلاه.

المادة ٢٢: صاحب الحق بالحماية القانونية للمنتج شبه الموصل

إن الحق بالحماية يُعطى لمبتكري طوبوغرافيا المنتجات شبه الموصلة، مع مراعاة أحكام هذه المادة.
يعود للدول الأعضاء أن:

- تقر أن الحق بالحماية يُعطى لصاحب العمل بالنسبة للطوبوغرافيا المُبتكرة من قبل موظف مدفوع الأجر، باستثناء حالة وجود بنود مخالفة في عقد العمل.
- تقر أن الحق بالحماية يُعطى للطرف في العقد الذي طلب الطوبوغرافيا بالنسبة للطوبوغرافيا المُبتكرة بموجب عقد غير عقد عمل، باستثناء حالة وجود بنود مخالفة في العقد.

عندما لا يتبين من هو المستفيد من الحماية بموجب أية أحكام قانونية أخرى، يُعطى الحق بالحماية القانونية للأشخاص الذين:

- يقومون بأول استثمار تجاري للطوبوغرافيا غير المستثمرة أبداً سابقاً.
- تلقوا من الشخص، المخوّل التصرف بالطوبوغرافيا، الترخيص الحصري للقيام بالاستثمار التجاري للطوبوغرافيا.

يُعطى الحق بالحماية لخلفاء الأشخاص المذكورين أعلاه في هذه المادة.

المادة ٢٣: تسجيل طوبوغرافيا المنتج شبه الموصل وإيداع موادها

للدول الأعضاء أن تعتمد أن طوبوغرافيا المنتج شبه الموصل لا تستفيد أو تتوقف استفادتها من الحقوق الحصرية الممنوحة وفقاً للمادة السابقة، إذا لم يتم إيداع طلب بالتسجيل بشكل نظامي لدى هيئة رسمية في خلال سنتين تلي أول استثمار تجاري لها. للدول الأعضاء أن تطلب، بالإضافة إلى التسجيل، أن يتم إيداع المواد التي تمثّل الطوبوغرافيا أو تجميعاً معيناً لها لدى هيئة رسمية، بالإضافة إلى تصريح عن تاريخ أول استثمار تجاري للطوبوغرافيا عندما يكون هذا الاستثمار سابقاً لتاريخ إيداع طلب التسجيل.

تحرص الدول الأعضاء على أن لا تُوضع المواد المُودعة وفقاً لأحكام الفقرة السابقة بتصرف الجمهور، إذا كانت هذه المواد تخضع لسرية الأعمال. لا تخول أحكام هذه المادة دون إفشاء هذه المواد بناءً لأمر قضائي أو لأمر سلطة مختصة في حالات المنازعات التي يكون موضوعها انتهاك الحقوق الحصرية القائمة على منتج شبه موصل.

يجوز للدول الأعضاء أن تُلزم بتسجيل كل انتقال للحقوق الجارية على الطوبوغرافيا المحميّة.

يجوز للدول الأعضاء أن تُوجب دفع رسم لدى إتمام تسجيل أو إيداع طوبوغرافيا المنتج شبه الموصل.

لا تستلزم الحماية القانونية لطوبوغرافيا المنتج شبه الموصل إتمام أي شكليات أو إجراءات أخرى غير تلك المذكورة آنفاً.

إن الدول الأعضاء التي تُلزم بتسجيل طوبوغرافيا المنتج شبه الموصل، تتيح طرقاً للطعن بالتسجيل لصالح الشخص الذي له الحق بالحماية وفق هذا الباب، والذي يستطيع إثبات أن الغير غير المخول قد طلب أو استحصل على تسجيل للطوبوغرافيا.

المادة ٢٤: ماهية الحقوق الحصرية على طوبوغرافيا المنتج شبه الموصل

إن الحقوق الحصرية على طوبوغرافيا المنتج شبه الموصل تتضمن الحق بترخيص أو بمنع الأعمال التالية:

- نسخ وإعادة إنتاج الطوبوغرافيا المحمية.
- الاستثمار التجاري أو الاستيراد لهذه الغاية لطوبوغرافيا أو لمنتج شبه موصل مُصنّع بواسطة هذه الطوبوغرافيا.

مع مراعاة الفقرة السابقة، يعود لدولة عضو أن ترخص بنسخ أو بإعادة إنتاج طوبوغرافيا بصفة خاصة لغايات غير تجارية.

إن الحقوق الحصرية بالنسبة لطوبوغرافيا المنتج شبه الموصل لا تطبّق على النسخ أو إعادة الإنتاج لغايات التحليل أو التقييم أو تعليم المفاهيم والآليات والأنظمة والتقنيات المُدخلة في الطوبوغرافيا أو للطوبوغرافيا ذاتها.

إن الحقوق الحصرية على طوبوغرافيا المنتج شبه الموصل لا تمتد إلى الأعمال المتعلقة بطوبوغرافيا محميّة بموجب هذا الباب، تم ابتكارها انطلاقاً من تحليل أو تقييم لطوبوغرافيا أخرى مُنجزة وفقاً للفقرة السابقة.

إن الحق الحصري بترخيص أو بمنع استثمار طوبوغرافيا المنتج شبه الموصل لا يطبق على الأعمال المُرتكبة بعد وضع الطوبوغرافيا أو المنتج شبه الموصل في السوق من قبل الشخص المخول بالترخيص لتسويقه أو بموافقته.

إن الشخص الذي يكتسب منتجاً شبه موصل دون معرفة أن المنتَج هو محمي أو دون توفر افتراض منطقي لمعرفته، لا يمكن منعه من الاستثمار التجاري للمنتج. أما بالنسبة للأعمال المُرتكبة بعد معرفة الشخص أو بعد توفر افتراض منطقي لمعرفته بأن المنتج شبه الموصل يستفيد من الحماية، فإن المحكمة تستطيع الحكم، بناءً لطلب صاحب الحق، ووفقاً لأحكام القانون الوطني المطبّق، بدفع التعويضات الملائمة.

المادة ٢٥: المدة القانونية للحقوق الحصرية

تعتمد الدول الأعضاء أن الحقوق الحصرية على طوبرغرافيا المنتج شبه الموصل تنشأ:

- بالنسبة للحالة الأولى التي يكون فيها التسجيل شرطاً للحصول على الحقوق الحصرية، في التاريخ الأول من التواريخ التالية:
  - في التاريخ الذي تم فيه الاستثمار التجاري للمرة الأولى في أي مكان في العالم.
  - في التاريخ الذي يتم فيه إيداع طلب التسجيل بشكل نظامي.
- أو في الحالة الثانية لدى الاستثمار التجاري الأول للطوبوغرافيا في أي مكان في العالم.
- أو في الحالة الثالثة عندما يتم تثبيت الطوبوغرافيا أو ترميزها للمرة الأولى.

عندما تنشأ الحقوق الحصرية على طوبوغرافيا المنتجات شبه الموصلة وفقاً للحالتين الأولى والثانية، فإن الدول الأعضاء تعتمد، بالنسبة للفترة السابقة لنشوء الحقوق الحصرية، وسائل طعن لصالح الشخص الذي له الحق بالحماية بموجب هذا الباب، والذي يستطيع أن يثبت أن الغير قد نسخ أو استثمر تجارياً أو ستورد لهذه الغايات طوبوغرافيا، وذلك بشكل احتيالي.

إن الحقوق الحصرية تنقضي بعد مرور فترة عشر سنوات تبتدئ من نهاية السنة التي تم خلالها الاستثمار التجاري للطوبوغرافيا للمرة الأولى في أي مكان في العالم، أو إذا كان التسجيل شرطاً لنشوء الحقوق الحصرية أو لاستمرارها، فتنقضي الحقوق الحصرية بعد فترة عشر سنوات ابتداءً من التاريخ الأول من التواريخ التالية:

- نهاية السنة التي تم خلالها الاستثمار التجاري للطوبوغرافيا للمرة الأولى في أي مكان في العالم.
- أو نهاية السنة التي تم خلالها إيداع طلب التسجيل بشكل نظامي.

عندما لا يتم الاستثمار التجاري للطوبوغرافيا في أي مكان من العالم في خلال خمس عشرة سنة ابتداءً من التاريخ الذي تم فيه تثبيتها أو ترميزها للمرة الأولى، فإن كل الحقوق الحصرية على الطوبوغرافيا تنقضي. وفي الدول التي يكون فيها التسجيل شرطاً لنشوء الحقوق الحصرية أو لاستمرارها، فإن أية حقوق حصرية جديدة لا يمكن أن تنشأ إلا إذا تم إيداع طلب بالتسجيل بشكل نظامي ضمن المهلة المذكورة آنفاً.

المادة ٢٦: استثناءات من الحماية

إن الحماية القانونية الممنوحة لطوبوغرافيا المنتج شبه الموصل وفق هذا الباب من الإرشاد، لا تطبق إلا على الطوبوغرافيا ذاتها، ويُستثنى من الحماية كل مفهوم وآلية ونظام وتقنية ومعلومة مثبتة مُدخلة كلها في الطوبوغرافيا.

الباب الخامس: الحماية القانونية للأعمال الرقمية الأخرى

المادة ٢٧: الحماية القانونية للأعمال الرقمية الأخرى وفق الوصف القانوني لها

إن الأحكام القانونية الواردة في هذا الإرشاد أو في القوانين الوطنية، المتعلقة بالحماية بموجب حق المؤلف والحقوق المجاورة أو بموجب الحق الخاص أو بموجب العلامات التجارية، تطبق أيضاً على سبيل القياس على الأعمال الرقمية الإلكترونية أو على مكونات منها، وفق الوصف القانوني الممكن إعطاؤه لها أو لكل مكوِّن منها وشرط أن تستوفي الشروط القانونية المطلوبة للحماية.

تشمل هذه الأعمال الرقمية الإلكترونية فهارس المواقع الإلكترونية وصفحات المواقع الإلكترونية ومحركات البحث ووصلات النصوص الفائقة والأنظمة التطبيقية المختلفة والرسوم والصور الإلكترونية وألعاب الفيديو والوسائط المتعددة.

الباب السادس: الحماية القانونية لأسماء المواقع

المادة ٢٨: الترخيص لشركة أو مؤسسة خاصة بمنح أسماء المواقع ضمن النطاق الوطني

للدول المتعاقدة أن تنشىء هيئة رسمية متخصصة في إعطاء ترخيص لشركة أو مؤسسة خاصة لتتولى منح أسماء المواقع المتعلقة بالنطاق الوطني، ضمن شروط إدارية ومالية وتقنية معينة، وشرط استحصال هذه الشركة أو المؤسسة على موافقة المراجع الدولية المختصة بتسجيل أسماء مواقع الإنترنت.

المادة ٢٩: الشروط المالية والإدارية والتقنية لمنح أسماء المواقع

تضع الهيئة المتخصصة المذكورة في المادة السابقة الشروط الإدارية والمالية والتقنية اللازمة لمنح أسماء المواقع ضمن النطاق الوطني، على أن تلبي الشروط المطلوبة من المراجع الدولية المختصة بتسجيل مواقع الإنترنت، وتُوضع هذه الشروط الإدارية والمالية والتقنية بتصرف الجمهور وتُنشر على الإنترنت.

يجب أن تكون الشروط الإدارية والمالية والتقنية موضوعية، وأن لا تتضمن أي تمييز في منح أسماء المواقع. وتسري هذه الشروط على كل شخص يتقدم بطلب للحصول على اسم موقع.

المادة ٣٠: تسجيل اسم الموقع

تتيح الدول الأعضاء إمكانية تسجيل اسم الموقع وإدارته بوسائل إلكترونية.

يتم تسجيل اسم الموقع مع احترام حقوق الغير، ولاسيما حقوق الملكية الصناعية والملكية الأدبية والفنية والأسماء التجارية والعائلية والعلامات والأسماء التجارية.

المادة ٣١: مسؤولية الشركة أو المؤسسة المُرخص لها بمنح أسماء المواقع

إن قيام الشركة أو المؤسسة المُرخص لها بمنح أسماء المواقع لا يعطيها أي حق على هذه الأسماء، وهي لا تكون مسؤولة عن التعابير والكلمات التي يتم انتقاؤها لأسماء المواقع، ولكن يتوجب عليها التحقق من تلبية طالب التسجيل لاسم موقع معين للشروط الإدارية والمالية والتقنية المفروضة قانوناً.

المادة ٣٢: إلغاء اسم الموقع

يعود للشركة أو المؤسسة المُرخص لها أن تُلغي اسم الموقع في حال تبين لها عدم توفر الشروط الإدارية والمالية والتقنية في طالب التسجيل، أو عدم صحة المعلومات المُقدّمة منه أو عدم كفايتها، أو في حال مخالفة تسمية أو الموقع للنظام العام أو الآداب العامة، وأخيراً في حال عدم قيام طالب التسجيل بدفع الرسوم القانونية المتوجبة أو الاستجابة ضمن فترة معينة لطلبات الشركة أو المؤسسة المرخصة بضرورة تزويد أو تصحيح بيانات خاصة بطالب التسجيل.

المادة ٣٣: البت بالنِزاعات المتعلقة بأسماء المواقع

تبت المحاكم في النِزاعات المتعلقة بأسماء المواقع.
بالإضافة إلى الاختصاص القضائي الوطني، يمكن للدول الأعضاء أن تعتمد مركزاً تحكيمياً دولياً أو محلياً مُتخصّصاً للفصل بهذه النِزاعات.

الباب السابع: أحكام مشتركة

المادة ٣٤: الوسائل التقنية للحماية

يجوز لأصحاب الحقوق على البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية حمايتها بتدابير تقنية ملائمة من أي اعتداء. يمكن أن تشمل هذه التدابير وضع رمز سري للاستخدام الشرعي أو اعتماد وسائل للتشفير أو استعمال آلية لمراقبة النسخ أو ضرورة التسجيل من قبل المستخدم لتفعيل البرنامج.

تحرص الدول الأعضاء على تجريم فعل كل شخص يصنع أو يستورد أو يبيع أو يوزع أو يؤجر أو يضع بالتداول أو يحوز لغايات تجارية كل جهاز أو وسيلة يكون هدفها الوحيد أو الأساسي تسهيل الإلغاء غير المشروع أو تعطيل الآليات التقنية الموضوعة لحماية البرامج المعلوماتية وقواعد البيانات والأعمال الرقمية المحمية بموجب هذا الإرشاد.

تكون كل نسخة غير مشروعة لبرنامج معلوماتي أو لقاعدة بيانات أو لعمل رقمي قابلة للحجز والضبط وفق تشريعات الدولة العضو المعنية. كما يمكن للدول المتعاقدة أن تجيز حجز وضبط المواد والوسائل المذكورة في الفقرة السابقة.

المادة ٣٥: العقوبات

تعتمد الدول الأعضاء نظاماً للعقوبات يطبق على مخالفة أحكام هذا الإرشاد، وذلك كما ينص عليه «الباب السادس: «جرائم التعدي على الملكية الفكرية للأعمال الرقمية» من الإرشاد الخاص بالجرائم السيبرانية. يجب أن تكون العقوبات فعالة ورادعة ومتناسبة مع حجم ومدى المخالفة.

الملاحق

ملحق ١
قائمة بالتقارير الدولية والإقليمية

No.	Title
1- Conventions	
1	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981. http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm
2	Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Approved by the Committee of Ministers, in Strasbourg, on 15 June 1999. http://conventions.coe.int/Treaty/EN/Treaties/Html/108-1.htm
3	Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Strasbourg,8.XI.2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/181.htm
4	Convention on Cybercrime, Budapest, 23.XI.2001. http://conventions.coe.int/treaty/en/treaties/html/185.htm
5	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003. http://conventions.coe.int/treaty/en/treaties/html/189.htm
2- European Directives	
6	Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs.
7	COUNCIL DIRECTIVE 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission. http://www.ebu.ch/CMSimages/en/leg_ref_ec_directive_copyright_satellite_cable_270993_tcm6-4289.pdf
8	European Parliament and Council Directive 95/46/EC 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 [Official Journal L 281 of 23.11.1995].
9	The Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
10	Directive 97/66/EC - concerning the processing of personal data and the protection of privacy in the telecommunications sector
11	Directive 97/7/CE du parlement Européen et du conseil, du 20 Mai 1997 concernant la protection des consommateurs en matière de contrats à distance.
12	Directive 97/55/EC of European Parliament and of 6 October 1997 amending Directive 84/450/EEC concerning misleading advertising so as to include comparative advertising.
13	Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations

14	Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions.
15	Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs.
16	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
17	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").
18	European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.
19	Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art.
20	Directive 2002/20/EC of the European Parliament and of the Council.
21	Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:EN:PDF
22	Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques.
23	Directive 2002/58/EC of the European Parliament and of 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).
24	Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
25	Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
26	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
27	Directive 2006/115/CE du Parlement européen et du Conseil du 12 décembre 2006 relative au droit de location et de prêt et à certains droits voisins du droit d'auteur dans le domaine de la propriété intellectuelle (version codifiée).
28	Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights.
29	Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:299:0025:0033:EN:PDF
30	Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs

31	Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.
32	Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
3- UN/UNCITRAL Guidelines and Model Laws	
33	Guidelines for the regulation of computerized personal data files, A/RES/45/95, adopted by the General Assembly on 14 December 1990. http://www.legislationline.org/documents/action/popup/id/6723
34	56/80 Model Law on Electronic Signatures, adopted by the United Nations Commission on International.
35	51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
36	United Nations Manual on the prevention and control of computer-related crime.
37	1996 - UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.
4- Recommendation & Decisions	
38	Council Decision 92/242/EEC of 31 March 1992 in the field of information security.
39	Recommendation No (95) 13 adopted on 11 September 1995 concerning problems of criminal procedural law connected with information technology.
40	Commission recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder.
41	Recommendation No R (85) 10 adopted on 28 June 1985 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications.
42	Recommendation No (87) 15 adopted on 17 September 1987 concerning the regulating of the use of personal data in the police sector.
43	Commission Recommendation 87/598/EEC of 8 December 1987, concerning a European code of conduct relating to electronic payments [Official Journal L 365 of 24.12.1987].
44	Recommendation No (88) 2 on piracy in the field of copyright and neighbouring rights adopted on 18 January 1988.
45	Recommendation No (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes adopted on 13 September 1989.
46	Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies.
5- Resolution	
47	Council Resolution of 21 November 1996 on new policy-priorities regarding the information society (96/C 376/01).
48	Council Resolution of 15 July 1974 on a Community policy on data processing.

6- Regulations	
49	Commission communication of 18 April 1997: A European Initiative in the sector of Electronic Commerce.
50	Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.
51	The Electronic Commerce (EC Directive) Regulations 2002.
52	Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.
7- Others	
53	The Bucharest Declaration on Combating Counterfeiting and Piracy, 12 July 2006. http://www.ccapcongress.net/archives/Regional/Files/Bucharest%20Declaration.pdf
54	European Commission Green Paper of 27 July 1995 on Copyright and Related Rights in the Information Society [COM(95) 382 final - Not published in the Official Journal].
55	Communication from the Commission of 11 April 2000 to the Council and the European Parliament "The organization and management of the internet. International and European policy issues 1998-2000" [COM(2000) 202 final - Not published in the Official Journal]
56	Communication from the Commission of 22 January 2004 on unsolicited commercial communications or 'spam' [COM(2004) 28 final - not published in the Official Journal].
57	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
58	Communication from the Commission of 31 May 2006: A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" [COM(2006) 251 final - not published in the Official Journal]

ملحق ٢
لائحة النصوص القانونية المتعلقة بالتشريعات السيبرانية للدول الأعضاء في الإسكوا

الرقم	التشريعات
	المملكة الأردنية الهاشمية
١	قانون المعاملات الإلكترونية رقم ٨٥ لسنة ٢٠٠١.
٢	قانون توظيف موارد تكنولوجيا المعلومات في المؤسسات الحكومية (قانون مؤقت رقم ٨١ لسنة٢٠٠٣).
٣	قانون الإحصاءات العامة المؤقت رقم ٨ لسنة ٢٠٠٣، الخاصة بسرية البيانات الإحصائية ومنع إفشائها (مادة ١١ و ١٢ و ١٥-١٧).
٤	مشروع قانون حماية المستهلك ٢٠٠٦.
٥	قانون حماية حق المؤلف والحقوق المجاورة رقم ٢٢ لسنة ١٩٩٢.
٦	تعديل قانون حق المؤلف رقم ٨ لسنة ٢٠٠٥ .
٧	تعديل قانون حق المؤلف رقم ٩ لسنة ٢٠٠٥ .
٨	قانون براءات الاختراع رقم ٣٢ لسنة ١٩٩٩.
٩	قانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧.
١٠	قانون مكافحة غسل الأموال رقم ٤٦ لسنة ٢٠٠٧.
	الإمارات العربية المتحدة – إمارة دبي
١١	قانون حماية البيانات الشخصية ٢٠٠٧.
١٢	قانون رقم (٢) لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية.
١٣	القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات.
١٤	قانون حقوق المؤلف والحقوق المجاورة لسنة ٢٠٠٢.
١٥	قانون الاتحادي رقم ٤٤ لسنة ١٩٩٢ في شأن تنظيم وحماية الملكية الصناعية لبراءات الاختراع والرسوم والنماذج الصناعية.
١٦	قانون بتعديل قانون العلامات التجارية لسنة ٢٠٠٢.
١٧	قانون رقم ٢٤ لسنة ٢٠٠٦ المتعلق بحماية المستهلك.
١٨	قانون رقم ٣٦ لسنة ٢٠٠٦ بتعديل بعض أحكام قانون الإثبات في المعاملات المدنية والتجارية (١٩٩٢)- م ١٧.
١٩	قانون الجمارك (١٩٩٨) – م ٤ و٢٤ و١١٨ .
٢٠	قانون منطقة دبي الحرة للتكنولوجيا و التجارة الإلكترونية و الإعلام (٢٠٠٠)– م ١و٢و٣و ٨ و٩ و١٠.
٢١	قانون هيئة وسوق الإمارات للأوراق المالية (٢٠٠٠) – م ٢٠ و ٤٥.
٢٢	قرار النظام الخاص بالتداول والمقاصة والتسويات ونقل الملكية وحفظ الأوراق المالية (٢٠٠١) - م ٦ و١٣ و٢٤.
٢٣	قانون استخدام الحاسب الآلي في الإجراءات الجزائية (٢٠٠١)- م ٣.
٢٤	قانون إنشاء وحماية شبكة الاتصالات (٢٠٠٢) – م ٢.
٢٥	قانون بتعديل قانون العلامات التجارية (٢٠٠٢) –م ١٤.
٢٦	قانون تعديل قانون منطقة دبي الحرة للتكنولوجيا (٢٠٠٣) – م ٢ و ٩ و١٠.
٢٧	مرسوم مكافحة الجرائم الإرهابية (٢٠٠٤) – م٧.
٢٨	قانون التسجيل العقاري في إمارة دبي (٢٠٠٦) – م ٢ و ٨.
	مملكة البحرين
٢٩	مرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية.
٣٠	قانون رقم ١٣ لسنة ٢٠٠٦ بتعديل بعض أحكام مرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية.
٣١	قانون الاتصالات البحريني رقم ٤٨ لسنة ٢٠٠٢.
٣٢	قرار رقم ٣ لسنة ٢٠٠١ بشأن تشكيل لجنة تنظيم التجارة الإلكترونية.
٣٣	قرار رقم ٢ لسنة ٢٠٠٦ بشأن الاشتراطات الفنية لقبول الجهات العامة للتعامل الإلكتروني.

٣٤	قرار رقم ٢٥ لسنة ٢٠٠٥ تشكيل لجنة عليا لتقنية المعلومات والاتصالات.
٣٥	مرسوم رقم ٩ لسنة ٢٠٠٢ إعادة تنظيم الجهاز المركزي للمعلومات.
٣٦	قانون رقم ٢٢ لسنة ٢٠٠٦ حماية حقوق المؤلف والحقوق المجاورة.
٣٧	قانون رقم (١) لسنة ٢٠٠٤ بشأن براءات الاختراع ونماذج المنفعة.
الجمهورية العربية السورية	
٣٨	قانون التوقيع الإلكتروني وخدمات الشبكة رقم ٤ لعام ٢٠٠٩.
٣٩	قانون حماية حق المؤلف رقم ١٢ الصادر عام ٢٠٠١.
٤٠	قانون حماية المستهلك ٢٠٠٦.
جمهورية السودان	
٤١	قانون المعاملات الإلكترونية لسنة ٢٠٠٧.
٤٢	قانون جرائم المعلوماتية لسنة ٢٠٠٧.
جمهورية العراق	
٤٣	قانون حماية المستهلك رقم ١ لسنة ٢٠١٠ (تاريخ ٢٠١٠/١/٤).
٤٤	قانون العلامات والبيانات التجارية رقم ٢١ لسنة ١٩٧٥ المعدل بموجب قانون ٢٠١٠ (المعدل لقانون العلامات التجارية والمؤشرات الجغرافية) تاريخ ٢٠١٠/١/٤.
سلطنة عُمان	
٤٥	قانون المعاملات الإلكترونية رقم ٦٩ لسنة ٢٠٠٨.
٤٦	مرسوم سلطاني رقم ٢٠٠١/٢٧ تعديل بعض أحكام قانون الجزاء العماني. إضافة المادة ٢٧٦ مكرر حول جرائم الحاسب الآلي.
٤٧	مرسوم اشتراعي رقم ٣٧ لسنة ٢٠٠٠ المتعلق بحماية حق المؤلف.
٤٨	قانون غسل الأموال لسنة ٢٠٠٤.
٤٩	مرسوم سلطاني رقم ٢٠٠٠/٨٢ بإصدار قانون براءات الاختراع.
فلسطين	
٥٠	مشروع قانون المبادلات والتجارة الإلكترونية لعام ٢٠٠٣.
٥١	قرار مجلس الوزراء رقم (٧٤) لسنة ٢٠٠٥م بشأن الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات.
٥٢	قرار مجلس الوزراء رقم (٦٥) لسنة ٢٠٠٥م بالمصادقة على اعتماد مبادرة فلسطين الإلكترونية.
٥٣	قرار مجلس الوزراء رقم (٢٦٩) لسنة ٢٠٠٥م بالمصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة.
٥٤	قرار مجلس الوزراء رقم (٣) لسنة ٢٠٠٤م بشان منع بيع وتسويق خدمات الاتصالات وتقنية المعلومات والبريد السريع.
٥٥	قرار مجلس الوزراء رقم (٣٥) لسنة ٢٠٠٤م بشأن النفاذ إلى الشبكة العالمية (الإنترنت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي.
٥٦	قرار مجلس الوزراء رقم (٣٩) لسنة ٢٠٠٤م باللائحة التنفيذية لقانون التحكيم رقم ٣ لسنة ٢٠٠٠م– م.١٩
٦٧	قانون الأوراق المالية رقم (١٢) لسنة ٢٠٠٤م – المادة ٢٦ (التوقيع الإلكتروني) .
٥٨	قانون البيانات في المواد المدنية والتجارية رقم (٤) لسنة ٢٠٠١م – المادة ١٩ (الإثبات عبر البريد الإلكتروني).
٥٩	مشروع قانون لسنة ٢٠٠٥ بشأن الهيئة الوطنية الفلسطينية لمسميات الإنترنت.
٦٠	قرار رقم (٢٠) لسنة ٢٠٠١م إنشاء الهيئة الوطنية لمسميات الإنترنت.
٦١	قانون حماية المستهلك رقم ٢١ لسنة ٢٠٠٥.
٦٢	قانون الإحصاءات العامة رقم ٤ لسنة ٢٠٠٠ بشان الحق في الوصول إلى معلومات الإحصاءات (م ٤) .
٦٣	قانون الاتصالات السلكية واللاسلكية رقم ٣ لسنة ١٩٩٦.
دولة الكويت	
٦٤	مقترح مشروع قانون التجارة الإلكترونية.
٦٥	قانون حق المؤلف الكويتي رقم ٥ لسنة ١٩٩٩.
٦٦	قانون بشان نظم المعلومات المدنية رقم ٣٢ لسنة ١٩٨٢.

الجمهورية اللبنانية	
٦٧	مشروع قانون التجارة الإلكترونية.
٦٨	تعميم رقم ٤ تاريخ ٢٠٠٦/٠٥/٢٥ حماية برامج المعلوماتية ومكافحة القرصنة لبنان.
٦٩	قرار رقم ٩٢١٧ تاريخ ٢٠٠٥/١٢/٢٣ تعديل القرار الأساسي رقم ٧٥٤٨ تاريخ ٢٠٠٠/٣/٣٠ المتعلق بالعمليات المالية والمصرفية بالوسائل الإلكترونية.
٧٠	نظام المقاصة الإلكتروني العائد لبطاقات الإيفاء أو الدفع أو الائتمان المصدرة في السوق اللبنانية والمستعملة محلياً على أجهزة الصراف الآلي (ATM).
٧١	نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال.
٧٢	الصراف الآلي وبطاقات الائتمان والوفاء.
٧٣	مرسوم رقم ١٣٠٦٨ بتاريخ ٧ آب ٢٠٠٤ المتعلق بحماية المستهلك.
٧٤	قانون حماية الملكية الفكرية والفنية رقم ١٩٩٩/٧٥.
٧٥	قانون براءات الاختراع رقم ٢٤٠ تاريخ ٢٠٠٠/٨/٧.
جمهورية مصر العربية	
٧٦	قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤
٧٧	القانون رقم ٨٢ لسنة ٢٠٠٢ ولائحته التنفيذية والخاص بحماية حقوق الملكية الفكرية.
٧٨	قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣
٧٩	قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤
٨٠	قرار وزاري رقم ٣٢٧ لسنة ٢٠٠٥ إنشاء إدارة متخصصة لمكافحة جرائم الحاسبات والشبكات بوزارة الداخلية تسمى " إدارة مباحث مكافحة جرائم الحاسبات الإنترنت".
٨١	قانون الإثبات في المواد المدنية والتجارية رقم ٢٥ لسنة ١٩٦٨.
٨٢	قانون حماية الملكية الفكرية رقم ٢٠٠٢/٨٢.
المملكة العربية السعودية	
٨٣	مرسوم ملكي رقم ١٨ نظام التعاملات الإلكترونية.
٨٤	قرار وزاري بشأن شروط مزاولة مهنة الاستشارات في مجال الاتصالات وتقنية المعلومات رقم ٦٦٦٧ تاريخ ١/ ٧ /١٤٢٦هـ.
٨٥	نظام مكافحة جرائم المعلوماتية.
٨٦	قانون حماية حق المؤلف لسنة ٢٠٠٣.
٨٧	اللائحة التنفيذية لنظام التعاملات الإلكترونية لسنة ٢٠٠٧.
٨٨	قرار مجلس الوزراء رقم (٤٠) تاريخ ٢٠٠٦/٣/٢٧م. ضوابط تطبيق التعاملات الإلكترونية الحكومية.
الجمهورية اليمنية	
٨٩	قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.
٩٠	قرار جمهوري بالقانون رقم (١٩) لسنة ١٩٩٤م بشأن الحق الفكري.
٩١	قانون مكافحة غسل الأموال تاريخ ٥ ابريل ٢٠٠٣م.
جامعة الدول العربية	
٩٢	القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة.
٩٣	قرار رقم ٤١٧ بشأن مشروع قانون عربي استرشادي لمكافحة جرائم المعلوماتية. عام ٢٠٠٣.

ملحق ٣
قائمة مختارة من التشريعات السيبرانية في الدول الأجنبية

No.	Title of law
Belgium	
1	24 Août 2005, Loi visant à transposer certaines dispositions de la directive services financiers à distance et de la directive vie privée et communications électroniques.
2	22 Mai 2005, Loi transposant en droit belge la Directive européenne 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
3	La nouvelle loi belge sur le commerce électronique.
4	28 Janvier 2004 Loi modifiant le Code de la taxe sur la valeur ajoutée (Facture électronique).
5	11 Mars 2003, Loi sur certains aspects juridiques des services de la société de l'information.
6	4 Avril 2003, Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique.
7	17 Juillet 2002, Loi relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds.
8	Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.
9	6 Décembre 2002, Arrêté´ royal organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifies.
10	9 Juillet 2001, Signature électronique et les services de certification.
France	
11	Code de la propriété intellectuelle, Version consolidée au 25 Juillet 2010.
12	Arrêté du 6 Mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.
13	Décret n° 2010-112 du 2 Février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
14	Décret n° 2009-834 du 7 Juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».
15	Arrêté du 7 Avril 2009 relatif à la communication par voie électronique devant les tribunaux de grande instance.
16	Arrêté du 25 Mai 2007 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie.
17	Loi no 2006-961 du 1er Août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.
18	Décret n° 2005-1450 du 25 Novembre 2005 relatif à la commercialisation à distance de services financiers auprès des consommateurs.

19	Loi du 21 Juin 2004 pour la confiance dans l'économie numérique .
20	Arrêté du 26 Juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation - 26 Juillet 2004.
21	Loi no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .
22	Arrêté du 14 avril 2003 relatif à la création par la direction centrale de la sécurité des systèmes d'information d'un site Internet.
23	Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
24	Règlement No 2002 – 13 relatif à la monnaie électronique et aux établissements de monnaie électronique.
25	Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
26	Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
27	Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
28	Code Pénal Articles 226-16 à 24.
Luxemburg	
29	Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité «commerce électronique».
Germany	
30	Federal data protection act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325).
Sweden	
31	Personal Data Act (1998:204); Issued 29 April 1998.
Suisse	
32	Ordonnance sur la conduite de la guerre électronique.
33	Loi Fédérale sur les services de certification dans le domaine de la signature électronique. No. 943.03.
34	Swiss Informatics Society Code of Ethics.
Romania	
35	Anti-corruption law Title III on preventing and fighting cyber-crime.
Canada	
36	The Electronic Information and Documents Act, 2000 (Saskatchewan).
37	Some computer related offences found in the 1998 Criminal Code of Canada.
38	Personal Information Protection and Electronic Documents Act , 2000.
39	Electronic Commerce Act (Newfoundland).
40	Electronic Transactions Act (Manitoba).
41	Electronic Transactions Act (Alberta).
42	Electronic Commerce Act (Yukon).
43	Electronic Commerce Act (Prince Edward Island).
44	Electronic Commerce Act (Ontario).

45	Electronic Commerce Act (Nova Scotia).
USA	
46	Computer security Act of 1987.
47	Uniform Electronic Transactions Act.
48	The Privacy Act of 1974 5 U.S.C. 552a.
49	Electronic Signatures in Global and National Commerce Act (E-SIGN), at 15 U.S.C. 7001.
50	United States code annotated title 18. crimes and criminal procedure part I —Crimes, chapter 47- Fraud and false statements, § 1029. Fraud and related activity in connection with access devices.
51	United States code annotated title 18. crimes and criminal procedure part i—Crimes chapter 47- Fraud and false statements, § 1030. Fraud and related activity in connection with computers.
52	United States code annotated title 18. crimes and criminal procedure part i—Crimes, chapter 65- Malicious mischief, § 1362. Communication lines, stations or systems.
53	United States code annotated title 18. crimes and criminal procedure part I—Crimes, chapter 119- Wire and electronic communications interception and interception of oral communications, § 2510. Definitions.
54	United States code annotated title 18. crimes and criminal procedure part i—Crimes, chapter 121- Stored wire and electronic communications and transactional records access, § 2701. Unlawful access to stored communications
55	United States code annotated title 18. crimes and criminal procedure part II- Criminal procedure, chapter 206--pen registers and trap and trace devices
56	Provisions of section 225 (“the cyber security enhancement act”) of the homeland security act of 2002, h.r. 5710 That Amend Title 18 of the United States Code.
57	Field guidance on new authorities that relate to computer crime and electronic evidence enacted in the USA patriot act of 2001.
58	The No electronic theft (NET) Act of 1977.
59	Anticybersquatting Consumer Protection Act'.
60	Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.
UK	
61	Data Protection Act 1998.
62	Computer Misuse Act 1990 (UK) Commencement 29 August 1990.
63	Electronic Communications ACT 2000.
ASEAN	
Malysia	
64	Computer Crimes Act 1997.
65	Digital Signature Regulations 1998.
Singapore	
66	Electronic Transactions Act 1998.

ملحق ٤
لائحة المراجع الفقهية

دراسات وأبحاث

١- **الإثبات الإلكتروني في القانون اللبناني:** معاناة قاض، تأليف سامي منصور ودراسة مجلة العدل سنة ٢٠٠١.

٢- **قيمة مستخرجات التقنيات العلمية الحديثة ومدى حجيتها في الإثبات**، تأليف أسامة أحمد شوقي المليجي، دراسة، مؤتمر معالجة المعلومات القانونية في القرن ٢١ وتحدياتها – تقنيات الاتصال الحديث والوصول إلى المعلومة، بيروت، ٧-٢/٩/٢٠٠١.

٣- **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**، تأليف د. ناصر بن محمد البقمي، سنة ٢٠٠٩.

٤- **التجارة الإلكترونية عبر الإنترنت**، تأليف محمد السيد عرفه، بحث مؤتمر القانون والكمبيوتر والإنترنت، ١-٣/٥/٢٠٠٠، جامعة الإمارات العربية المتحدة.

٥- **ملاحظات حول حجية الدفاتر التجارية في ظل انتشار الكمبيوتر**، تأليف ناجي عبد المؤمن، بحث مؤتمر القانون والكمبيوتر والإنترنت، ١-٣/٥/٢٠٠٠، جامعة الإمارات العربية المتحدة.

٦- **مبدأ حرية الإثبات في المواد التجارية**، الإثبات بالتلكس وغيره، تأليف ماجدة مزيحم، دراسة معهد الدروس القضائية، ١٩٩٣.

٧- **العرب وثورة المعلوماتية والاتصالات على عتبة الألفية الثالثة**، تأليف الدكتور وسيم حرب – مقالة في جريدة السفير، سنة ١٩٩٩.

٨- **المتطلبات القانونية لتطوير برامج الكمبيوتر**، الدكتور وسيم حرب، محاضرة ألقيت ضمن إطار المؤتمر العربي الاقليمي للمنظمة الدولية لحماية الملكية الفكرية، الأهمية الاقتصادية لحقوق الملكية الفكرية، بيروت، سنة ١٩٩٩.

٩- **تحديات استخدام الإنترنت وحاجات التنظيم القانوني**، الدكتور وسيم حرب، محاضرة ألقيت ضمن إطار مؤتمر لبنان عاصمة دائمة للإعلام، سنة ٢٠٠٠.

١٠- **النظام القانوني للعرض عبر الإنترنت**، الدكتور وسيم حرب، محاضرة ألقيت ضمن إطار ندوة الاتحاد الدولي لجمعية قانون المعلوماتية، باريس-فرنسا، سنة ٢٠٠٠.

١١- **الجرائم المعلوماتية، ماهيتها وصورها**، تأليف الدكتور محمود صالح العادلي أستاذ القانون الجنائي، ورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الالكترونية" مسقط ٢-٤ أبريل ٢٠٠٦م.
www.ituarabic.org/coe/2006/E-Crime/.../Doc2-Text-ar.DOC

١٢- **الجرائم الإلكترونية تشكل تحديات أمام القانون.** ونظام المكافحة في المملكة حماية للاقتصاد الوطني، تأليف عبدالله عبد العزيز العجلان، صحيفة الرياض.
http://www.alriyadh.com/2008/02/29/article321790.html

١٣- التحديات القانونية في الجرائم الالكترونية، تأليف سمية بنت عبد الرحمن بن سليمان الحمدان
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/51-forensic-and-computer-crimes/1075-legal-challenges-in-cyber-crime.html

١٤- التجارة الإلكترونية وتنمية الاقتصاد الشبكي العربي، أ.د سعيد عبد الخالق
http://www.tashreaat.com/view_studies2.asp?id=26&std_id=25

١٥- الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات - بناء مجتمع المعلومات ٢٠٠٧-٢٠١٢.
صيغت هذه الاستراتيجية لتكون إطاراً للتنمية الإقليمية لتكنولوجيا الاتصالات والمعلومات فى الدول العربية، آخذة فى الاعتبار التطورات الاقليمية والدولية ذات الصلة بمجتمع المعلومات وعلى وجه الخصوص مخرجات القمة العالمية حول مجتمع المعلومات بمرحلتيها فى جنيف ٢٠٠٣ وتونس ٢٠٠٥. كما تعد بنود هذه الوثيقة ومحاورها الأساس لوضع الاطار التنفيذى من خلال خطط العمل والمشروعات المشتركة ذات الأولوية فيما بين الدول العربية
http://isper.escwa.org.lb/isper/Default.aspx?tabid=195&&language=ar-LB

الكتـب

١- تزوير التوقيع الإلكتروني، تأليف المحامي منير محمد الجنبيهي والمحامي ممدوح محمد الجنبيهي، عضو اتحاد المحامين العرب، دار الفكر الجامعي، سنة ٢٠٠٦ .

٢- الحماية الجنائية للمستند الإلكتروني، "دراسة مقارنة"، تأليف الدكتور أشرف توفيق شمس الدين، أستاذ ورئيس قسم القانون الجنائي بكلية الحقوق بجامعة بنها، دار النهضة العربية، الطبعة الأولى، سنة ٢٠٠٦.

٣- حق الجمهور بالمعرفة، الوصول إلى المعلومات والوثائق الرسمية، منظمة لافساد.

٤- حماية برامج الكومبيوُتر، الأساليب والثغرات، دراسة في القانون المقارن، تأليف د. نعيم مغبغب، دكتور في القانون واستاذ متفرغ في الجامعة اللبنانية، الطبعة الاولى ٢٠٠٦.

٥- مخاطر المعلوماتية والإنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، تأليف د. نعيم مغبغب، دكتور في القانون، سنة ١٩٩٨.

٦- التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، تأليف د. طوني ميشال عيسى، الطبعة الأولى ٢٠٠١.

٧- البطاقة المصرفية والإنترنت، دراسة حول الوضعيتين التقنية والقانونية، تأليف حسين ابراهيم القضماني، طبعة اولى، اتحاد المصارف العربية ٢٠٠٢.

٨- مسؤولية مزودي خدمات الإنترنت التقنية، تأليف د. اودين سلوم الحايك، سنة ٢٠٠٩.

٩- الحق في الاطلاع، الواقع العربي في ضوء التجارب العالمية (عمل جماعي)، سنة ٢٠٠١.

١٠- جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، تأليف المحامي محمد أمين أحمد الشوابكة، ماجيستر القانون الجنائي المعلوماتي، سنة ٢٠٠٤.

١١- **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، (دراسة قانونية متعمقة في القانون المعلوماتي)، تأليف د. عبد الفتاح بيومي حجازي، نائب رئيس مجلس الدولة المصري والمستشار القانوني للمجلس الوطني الاتحادي بدولة الامارات العربية المتحدة، سنة ٢٠٠٦.

١٢- **جرائم الحاسوب وأبعادها الدولية**، إعداد الباحث محمود أحمد عبابنة، إشراف د. محمد معمر الرازقي، سنة ٢٠٠٥.

١٣- **الجهاز الإلكتروني لمكافحة الجريمة**، تأليف د. مصطفى محمد موسى، سنة ٢٠٠٦.

١٤- **أساليب إجرامية بالتقنية الرقمية، ماهيتها مكافحتها**، دراسة مقارنة، تأليف د. مصطفى محمد موسى، سنة ٢٠٠٥.

١٥- **جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، دراسة مقارنة تقديم أ.د فتوح الشاذلي، رئيس قسم القانون الجنائي في كلية الحقوق – جامعة الاسكندرية، و تأليف عفيفي كامل عفيفي، ماجيستر في القانون الجنائي، الطبعة الثانية ٢٠٠٧.

١٦- **التجارة الإلكترونية، في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت**، تأليف الدكتور المستشار/عبد الفتاح بيومي حجازي، نائب رئيس مجلس الدولة المصري والمستشار القانوني للمجلس الوطني الاتحادي بدولة الإمارات العربية المتحدة، الطبعة الأولى ٢٠٠٦.

١٧- **الإثبات الإلكتروني**، تأليف القاضي وسيم شفيق الحجار، مجاز في هندسة الكمبيوتر والاتصالات من الجامعة الاميركية في بيروت، سنة ٢٠٠٩

١٨- **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية**، على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١، تأليف د.هلالي عبد الله أحمد، الطبعة الأولى ٢٠٠٣.

١٩- **الحماية الجنائية للتجارة الإلكترونية عبر الانترنت**، La protection pénale du commerce éléctronique à travers l'internet، تأليف د. هدى حامد قشقوش، أستاذ القانون الجنائي كلية الحقوق – جامعة عين شمس، سنة ٢٠٠٠.

٢٠- **جرائم الحاسوب الإلكتروني في التشريع المقارن**، تأليف د. هدى حامد قشقوش، أستاذ القانون الجنائي كلية الحقوق – جامعة عين شمس، سنة ١٩٩٢ (البحث الحاصل على جائزة أفضل البحوث الممتازة لجامعة عين شمن).

٢١- **جرائم المعلوماتية والإنترنت**، (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محلياً وعربياً ودولياً، تأليف الأستاذ عبد الله عبد الكريم عبد الله، عضو مساعد في مشروع مكافحة الفساد بالأمم المتحدة، سنة ٢٠٠٧.

٢٢- **العرب وعصر المعلومات**، تأليف د. نبيل علي، نيسان ١٩٩٤ م.

ملحق ٥
مراجع فقهية أجنبية

Articles published on the Internet

1- Privacy and the Collection of Personal Information Online, by *Ann Bartow*, Visiting Assistant Professor of Law, University of Dayton School of Law. A learning manual provides information on Data Collection in Cyberspace, and protecting the privacy of Adults and Children; The European approach to protecting the privacy of personal information is investigated, with an emphasis on the European Data Privacy Protection Directive. This manual is published on the following link:
http://www.cyberspacelaw.org/bartow/index.html#adults

2- Privacy and Encryption Export Controls: A Crypto Trilogy (Bernstein, Junger & Karn), By *Keith Aoki* Associate Professor, University of Oregon School of Law, Revised on August 24, 2000. This module considers how digital electronic communications are both enabling but troublingly insecure. Such module is organized as a series of questions and answers revolving around the use of encryption to ensure privacy in one's communication. This module is composed of 76 pages, and it is published on the following link:
http://www.cyberspacelaw.org/aoki/index.html

3- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *OECD*, adopted on 23 September 1980. The guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties
http://www.oecd.org/documentprint/0,3455,en1,00-1-1-1-1815186-34255-2649-.html

4- Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989). The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations.
http://www1.umn.edu/humanrts/instree/q2grcpd.htm

5- The Guide to Data Protection, *ICO Information Commissioner's Office*. This Guide explains the purpose and effect of each principle, and gives practical examples to illustrate how the principles apply in practice. We hope that, by answering many frequently asked questions about data protection, the Guide will prove a useful source of practical advice to those who have day-to-day responsibility for data protection.
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf

6- Data Protection - Protecting People, A Data Protection Strategy for the Information Commissioner's Office, *By Information Commissioner's Office*, September 2009. This data protection strategy sets out how we approach our task of minimizing data protection risk. It is concerned with ensuring our maximum long term effectiveness in bringing about good practice. This strategy is published on the following link:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_dps_final.pdf

7- The National Strategy to Secure Cyberspace, February 2003; This strategy was developed by the *White House –Washington* in order to provides a framework for protecting against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. This strategy is composed of 60 pages, and it is published on the following link:
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

8- An Advocacy Handbook for the Non Governmental Organizations, by *Dr. Yaman AKDENIZ* director of Cyber-Rights & Cyber-Liberties organization (UK), first Published on December 2003, Updated and revised in May 2008. This advocacy handbook for the NGOs provides a policy analysis of the Cyber-Crime Convention 2001 and the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems from a human rights perspective for policy specialists, NGOs, and human rights activists within the 45 member states of the Council of Europe. This handbook is composed of 57 pages, and it is published on the following link:
http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf

9- Tracking a Computer Hacker, by *Daniel A. Morris*, Assistant United States Attorney Computer and Telecommunications Coordinator, District of Nebraska; published on 2005. A report written near the start of the Information Age warned that America's computers were at risk from hackers. This report is composed of 6 pages and it is published on the following link:
http://www.cybercrime.gov/usamay2001_2.htm

10- Internet Blocking: Crimes Should Be Punished and Not Hidden, by *Joe McNamee* Advocacy Coordinator - European Digital Rights (EDRI), June 2010. The EU is considering a proposal to introduce filters for blocking of child abuse websites. Child abuse and its portrayal on the Internet is a terrible crime that is sometimes of a severity that is scarcely believable. It must be treated seriously, with policies based on evidence and effectiveness and not on politics or gut reactions. This article is published on the following link:
http://www.soros.org/initiatives/information/focus/policy/articles_publications/publications/edri-blocking-100606/EDRI-blocking-100606.pdf

11- Data Breaches: What the Underground World of "Carding" Reveals, by *Kimberly Kiefer Peretti*- U.S. Department of Justice - Computer Crime and Intellectual Property Section. This article provides a brief background on large scale data breaches and the criminal "carding" organizations that are responsible for exploiting the stolen data. This article is composed of 33 pages, and it is published on the following link:
http://www.cybercrime.gov/DataBreachesArticle.pdf

12- Prosecuting Intellectual Property Crimes, Third Edition Published by the *Office of Legal Education Executive Office for United States Attorneys*, September 2006. This manual builds on the success of the editions published in 2001 and 1997 by giving much broader and deeper treatment to all subject areas, while also adding several new topics to address the Digital Millennium Copyright Act, patent law, and victim issue. This Manual is composed of 436, and it is published on the following link:
http://www.cybercrime.gov/ipmanual/ipma2006.pdf

13- Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations- Third Edition, September 2009 Published by Office of Legal Education, Executive Office for United States Attorneys. The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored

in computers. Electronic records such as computer network logs, email, word processing files, and image files increasingly provide the government with important (and sometimes essential) evidence in criminal cases. The purpose of this publication is to provide Federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations. This publication is composed of 299 pages, and it is published on the following link:
http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf

14- IT security and crime prevention methods, Published by *Interpol*. This document gives an introduction to what an investigator needs to know about Information Technology (IT) security measures in order to be able to carry out investigations in an IT environment and to give advice in crime prevention methods. The prevention methods in this report can be used to prevent crime in companies, but can also be used to protect private computer systems. Report publishes on the following link:
http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp

15- The UNCITRAL Legislative Guide on Secured Transactions (the "*Guide*"), Supplement on Security Rights in Intellectual Property (the "*Supplement*") was prepared by the *United Nations Commission on International Trade Law (UNCITRAL)*, July 2010). The overall objective of the Guide is to promote low-cost credit by enhancing the availability of secured credit. The *Supplement* is intended to make credit more available and at a lower cost to intellectual property owners and other intellectual property rights holders, thus enhancing the value of intellectual property rights as security for credit. This Guide is composed of 129 pages, and it is published on the following link:
http://www.uncitral.org/pdf/english/texts/security-lg/e/Final.Draft.15_July.2010.clean.pdf

16- Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, *UNITED NATIONS*, Vienna, 2009. The present publication analyses the main legal issues arising out of the use of electronic signatures and authentication methods in international transactions, provides an overview of methods used for electronic signature and authentication and their legal treatment in various jurisdictions, and considers the use of electronic signature and authentication methods in international transactions and identifies the main legal issues related to cross-border recognition of such methods. This publication is composed of 119 pages, and it is published on the following link:
http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

17- The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, by *Jeremy Warner,* 2005. The function of this paper is to examine the growth and development of legal restrictions on the retention of records—the right to oblivion—rather than the requirement of retention or preservation of records. This paper is composed of 30 pages, and it is published on the following link:
http://www.uoltj.ca/articles/vol2.1/2005.2.1.uoltj.Warner.75-104.pdf

مسرد المصطلحات

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١	اتصال/مكالمة	call	أي تواصل قائم بين وسائل هاتفية متوافرة للعموم تسمح بإجراء اتصال مباشر بين طرفين.
٢	اتصالات	communication	تبادل بيانات بين عدد محدد من الأشخاص بواسطة خدمة اتصالات إلكترونية متوافرة للعموم، وهي لا تشتمل البيانات المرسلة كجزء من خدمات بث للعموم بواسطة شبكة اتصالات إلكترونية باستثناء ما يمكن نسبته من بيانات لمشترك قابل للتحديد أو لمستخدم يتلقى البيانات.
٣	إجراءات التوثيق المحكّمة	verification procedures	الإجراءات التي تهدف الى التحقق من أن الرسالة الإلكترونية قد صدرت من شخص معين، والكشف عن أي خطأ أو تعديل في محتويات أو في نقل أو تخزين رسالة إلكترونية أو سجل إلكتروني خلال فترة زمنية محددة، ويشمل ذلك أي اجراء يستخدم مناهج حسابية أو رموزاً أو كلمات أو أرقاماً تعريفية أو تشفيراً أو اجراءات للرد أو لإقرار الاستلام وغيرها من وسائل اجراءات حماية المعلومات.
٤	أداة التوقيع الإلكتروني	e-signature tool	أي جهاز أو بيانات إلكترونية معدة بشكل ميز للعمل بطريقة مستقلة أو بالاشتراك مع اجهزة بيانات آخرى وذلك لوضع رقمي محدد لشخص معين وتشمل هذه العملية أي انظمة تنتج أو تلتقط بيانات ميزة كالرسوم أو الحروف أو الأرقام أو المفاتيح الخصوصية أو أرقام تعريف الشخصية.
٥	استعمال عادل (لحقوق الملكية الفكرية)	fair use	هو مبدأ في قانون حماية حقوق الملكية الفكرية يسمح باستخدام محدود من المواد المحفوظة في إطار حقوق التأليف والنشر دون اشتراط إذن من أصحاب الحقوق، مثل استخدامها للحصول على المنح الدراسية أو المراجعة. وهو ما يُعرف ببعض القوانين كاستثناء من الحماية.
٦	اسم نطاق	domain name	المنتج الذي تعطيه شركات تعيين وتسجيل أسماء النطاقات لعملائها. غالباً ما تُدعى هذه الأسماء أسماء النطاقات المُسجلة وهنا يكون IP وعدة نطاقات تدل عليه وتسمى نطاقات فرعية.
٧	الإرهاب السيبراني	cyberterrorism	يقصد به استخدام أجهزة الحاسوب و/أو الإنترنت لإحداث ضرر أو تخريب بهدف ترويج أفكار دينية أو سياسية أو عرقية. يستهدف عادةً الحكومات والمؤسسات الرسمية
٨	الاعتماد الاختياري	voluntary Accreditation	هو كل ترخيص يحدد الحقوق والموجبات الخاصة بتقديم خدمات المصادقة الإلكترونية، يُعطى، بناءً على طلب مزود خدمات المصادقة الإلكترونية المعني، من قبل هيئة عامة أو خاصة مكلفة بوضع هذه الحقوق والموجبات وبمراقبة احترامها.
٩	الباب الخلفي	back door	يعني وسيلة غير مدونة للولوج عن بعد إلى حاسوب عبر تخطي أنظمة المصادقة أو الحماية.
١٠	التقاط	interception	مشاهدة البيانات أو الحصول عليها بدون مسوغ نظامي صحيح.
١١	السند الإلكتروني	e-record	هو القيد أو العقد أو المراسلة التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٢	العمل المحمي	copyrighted work	هو حسب مفهوم قوانين الملكية الفكرية كل عمل ذهني أدبي أو فني مثل الكتب والمسرحيات والموسيقى والأفلام والرسم والنحت والخرائط والأعمال السمعية وبرامج الحاسوب وقواعد البيانات تتمتع بالحماية وفقاً لقانون حماية الملكية الفكرية والاتفاقيات الدولية.
١٣	إلكتروني (ة)	electronic	تقنية استعمال وسائل كهربائية أو مغناطيسية أو كهرومغناطيسية أو بصرية أو ضوئية أو بأيومترية أو فوتونية أو أي شكل من وسائل التقنية المشابهة في تبادل المعلومات و/ أو تخزينها
١٤	المعلومات المتعلقة بحركة البيانات	data traffic	يقصد بها أي معلومات تتعلق بعملية نقل للبيانات أو اتصال عبر شبكة إلكترونية، ينتجها النظام المعلوماتي المرتبط بالشبكة الإلكترونية، وتحدد هذه المعلومات مصدر الاتصال أو مُرسل البيانات والمُرسل إليه أو المُتلقي وخريطة طريق إرسال المعلومات ووقت الإرسال وتاريخه وحجم البيانات المُرسلة ومدة الإرسال وغيرها من المعلومات التقنية.
١٥	إثبات الهوية	identity check record	أي مستند إلكتروني أو خلافه يتم تقديمه لمزود خدمة التصديق ويثبت هوية المشترك أو الموقِّع.
١٦	اختراق	hacking	يعني استعمال البرمجة أو المعرفة الرقمية بهدف خرق أو تخطي أنظمة الحماية في الشبكات وأجهزة الحاسوب للولوج إليها والعبث فيها.
١٧	اغتصاب علامة تجارية بواسطة اسم موقع	cybersquatting	التعدي على اسم موقع على الإنترنت أو على علامة تجارية أو اسم تجاري عبر تسجيلها كاسم موقع على الإنترنت. ويشمل نوع typosquatting وهو تغيير بسيط في طريقة الكتابة الصحيحة من شأنها أيقاع المستخدمين باللبس مثل: كتابة gooqle بدلا من google .
١٨	انتهاك حقوق الملكية الفكرية	copyright infringement	يعني الاستعمال غير المرخص للمواد المحمية بموجب قانون حقوق النسخ بشكل يعارض أحد حقوق المؤلف الخاصة، مثل إعادة طباعة أو نسخ أعمال محمية بقانون حقوق النسخ.
١٩	أمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية	e-payment order, e-transfer order	هو الأمر الذي ينظم كلياً أو جزئياً بوسيلة إلكترونية، ويفوض بموجبه العميل مصرفاً أو مؤسسة مالية، بإجراء دفع إلكتروني أو تحويل إلكتروني للأموال النقدية أو إتمام قيد دائن أو مدين على حسابه.
٢٠	آلية آمنة لإنشاء توقيع إلكتروني	secure tool to create an e-signature	هي آلية لإنشاء توقيع إلكتروني وتجري بوسائل تقنية وبإجراءات ملائمة، وتلبي المتطلبات التالية مجتمعةً، أن البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن عملياً مصادفتها إلا مرة واحدة وأن سريتها هي مؤمنة بصورة معقولة، وأن هناك ضمانة كافية أن البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن أيجادها بالاستنتاج وأن يكون التوقيع محمياً من أي تزوير أو تقليد بوسائل تقنية متاحة فعلياً، وأن البيانات المستخدمة لإنشاء توقيع إلكتروني هي محمية بطريقة موثوقة من قبل الموقّع الشرعي من أي إستخدام من قبل الغير، وأن الآلية الآمنة للتوقيع الإلكتروني لا تعدل البيانات الموقّعة، ولا تمنع أن تعرض هذه البيانات على الموقّع قبل التوقيع.
٢١	آلية لإنشاء توقيع إلكتروني	creating an e-signature tool	هي برنامج معلوماتي أو تجهيزات معلوماتية معدة لتضع موضع التطبيق البيانات اللازمة لإنشاء توقيع إلكتروني.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٢٢	آلية للتحقق من توقيع إلكتروني	verification of e-signature tool	هي برنامج أو تجهيزات معلوماتية معدة من أجل وضع موضع التطبيق بيانات التحقق من التوقيع الإلكتروني.
٢٣	بث	transmission	هو نقل العمل إلى الجمهور عن طريق الإرسال اللاسلكي بما في ذلك الإرسال عن طريق الأقمار الصناعية أو على الخط online
٢٥	براءة إختراع	patent	تعني صكاً تصدره الدولة للمخترع الذى يستوفي اختراعه الشروط اللازمة لمنح براءة اختراع صحيحة يمكنه بموجبها أن يتمسك بالحماية التي يضفيها القانون على الاختراع. وتشمل الحماية التي يقررها القانون لصاحب البراءة الحق في أن يستأثر وحده باستعمال الاختراع واستغلاله إقتصادياً. وبالتالي تمكينه من جني أرباح من وراء هذا الاستغلال في مقابل ما قدمه من كشف سر الاختراع للمجتمع. وتعتبر براءة الاختراع صالحة لمدة ٢٠ عاماً.
٢٦	براءة إختراع تحت البحث	patent pending	تعني تحذير يتم وضعه على منتجات معينة بطلب تسجيلها كبراءة إختراع إلا أنه لم يتم منحها البراءة بتاريخه. وتهدف إلى تحذير الجمهور من مغبة تقليدها أو استعمالها بدون ترخيص.
٢٧	برنامج التجسس	spyware	هو عبارة عن برنامج حاسوبي من شأنه أن يجمع بيانات عن عأداة تصفح الإنترنت لمشترك معين وهو يرسل هذه البيانات للغير بدون علم و موافقة المشترك.
٢٨	برنامج الحاسوب	computer software	هو مجموعة من الأوامر معبر عنها بكلمات أو برموز أو بأي شكل آخر، عندما تدخل في مادة يمكن للحاسوب ان يقرأها، أن تجعله يؤدي أو ينفذ مهمة ما أو يعطي نتيجة ما.
٢٩	برنامج الخصوصية الجيدة	pretty good privacy	يعني برنامج تشفير يستخدم ١٢٨ بت، وهو يستخدم لتشفير البريد الإلكتروني.
٣٠	بروتوكول الإنترنيت	internet protocol	يعبر عنه اختصاراً: أي بي (IP)، وهو بروتوكول يعمل على الطبقة الثانية (طبقة وصلة البيانات (Internet Layer) من نموذج OSI، يحدد كيفية تقسيم المعلومة الواحدة إلى أجزاء أصغر تسمى رزماً (packet)، إن لزم الأمر، ثم يقوم الطرف المرسل بإرسال الرزمة إلى جهاز آخر على الشبكة يستخدم نفس الميثاق (البروتوكول)، ثم يقوم هذا الجهاز الثاني بدوره بإرسال الرزم إلى جهاز آخر بنفس الطريقة، وتكرر هذه العملية إلى أن تصل الرزم إلى الطرف المرسل إليه.
٣١	بريد غير مرغوب به	spam	هو فعل إعلان أو إرسال رسائل بريد إلكتروني غير مطلوبة وغير ملتمسة، بما في ذلك مواد إعلانية وترويجية، لعدد كبير من المستخدمين الذين لا يرغبون أو لا يريدون استقبال مثل هذه الرسائل أو المحتوى
٣٢	بطاقة الدفع أو السحب المصرفية	debit or credit card	هي بطاقة صادرة عن مصرف أو عن مؤسسة مالية، وهي تتيح لصاحبها سحب الأموال وتحويلها أو سحبها فقط.
٣٣	بيانات	data	معلومات تتم معالجتها بواسطة جهاز يعمل آلياً بناءً على أوامر أعطيت له لهذه الغأية، ومحفوظة بشكل يتيح معالجتها بواسطة هذا الجهاز.
٣٤	بيانات شخصية	personal data	أي بيانات تتعلق بشخص معروف أو قابل للتعريف مباشرة أو غير مباشرة لا سيما عبر رقم تعريف أو غير ذلك من الميزات الشخصية، الجسدية ، العقلية، الاقتصادية الثقافية أو الهوية الاجتماعية أو عبر البيانات المحفوظة لدى «المراقب».

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٣٥	بيانات شخصية حساسة	sensitive personal data	هي بيانات شخصية تتعلق بشكل مباشر أو غير مباشر بمعلومات عن الشخص من ناحية العرق، الآراء السياسية، المعتقدات الدينية أو ما شابه، صحته أو حالته الجسدية أو العقلية، وحياته الجنسية، وسجله العدلي.
٣٦	بيانات الموقع	location data	هي أي معلومات معالجة في شبكة اتصالات إلكترونية تشير إلى موقع جهاز المستخدم الخاص بخدمة اتصالات إلكترونية متوافرة للعموم.
٣٧	بيانات لازمة لإنشاء توقيع إلكتروني	prerequisite data to create an e-signature	هي بيانات فريدة، مثل رموز أو مفاتيح تشفير خاصة، يستخدمها الموقّع لإنشاء توقيع إلكتروني.
٣٨	بيانات لازمة للتحقق من التوقيع الإلكتروني	prerequisite data to check an e-signature	هي بيانات، مثل رموز أو مفاتيح تشفير عامة، تستخدم للتحقق من توقيع إلكتروني.
٣٩	تاجر الى مستهلك	business to consumer B2C	تاجر إلى مستهلك وهي أي تعامل تجاري إلكتروني يكون احد أطرافه تاجراً والآخر مستهلكاً.
٤٠	تاجرالى تاجر	business to business B2B	يعني أي تعامل تجاري إلكتروني يكون طرفاه تجّار.
٤١	تبادل البيانات الإلكترونية	electronic data exchange	نقل المعلومات إلكترونياً من شخص الى آخر باستخدام نظم معالجة المعلومات
٤٢	تجارة إلكترونية	electronic commerce	أي معاملة تتم بين طرفين أو أكثر عبر الإنترنت أو عبر استعمال المراسلة الإلكترونية وتشمل بيع، شراء، تأجير، ترخيص، عرض، تسليم منتجات أو خدمات أو معلومات مقابل مردود مادي.
٤٣	تحويل إلكتروني للأموال	e-payment	أنظمة حاسوب تُستعمل لإجراء معاملات مالية إلكترونية مثل تحويل الأموال من حساب إلى آخر في مؤسسة مالية واحدة أو عبر عدة مؤسسات
٤٥	الانتحال أو انتحال الصفة	spoofing or phishing	التخفي هو عمل احتيالي من مرسلي الرسائل الدعائية، وهو رسالة دعائية تدعي أنها من مكان له صلة بالمال مثل المصارف أو البورصة أو الشركات المالية. وهذه الرسالة غالباً ما تكون مشابهة بالشكل والصيغة للرسالة الأصلية التي يرسلها المصرف لكي لا يتم كشفها، تتضمّن هذه الرسالة وصلة تأخذك إلى موقع على الإنترنت تبدو وكأنها نظامية تماماً، ولكن في الحقيقة ليست كذلك لأن هذه المواقع الشريرة صممت ببراعة لكي تخدع المستخدمين، حتى الأكثر حذراً منهم، وغالباً ما تظهر هذه المواقع الملفقة العناية الفائقة وخاصة بأدق التفاصيل، وهي تنسخ الخط والشكل والرسومات بشكل كامل من الموقع الحقيقي لكي يتم تجنّب الشك من قبل المستخدم البسيط.
٤٦	تزوير معلوماتي	computer-related forgery	فعل كل من أقدم عن قصد وبصورة غير مشروعة على إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، نتج عنها بيانات غير صحيحة، بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر أو لا.
٤٧	تشفير	encryption	يقصد به عملية ترتيب أحرف وأرقام بشكل متتال لأجل تحويل بيانات إلى نص غير مفهوم سوى لمن لديه إمكانية فك التشفير.
٤٨	توقيع إلكتروني	electronic signature	مجموعة بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وهي تستخدم كوسيلة لتأكيد الموثوقية.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٤٩	توقيع إلكتروني متقدم	advanced electronic signature	هو توقيع إلكتروني يلبي المتطلبات التالية مجتمعةً: أن يكون مرتبطاً فقط بالموقّع، أن يسمح بتحديد الموقّع، أن يُنشأ بوسائل تكون تحت رقابة الموقّع الحصرية وأن تكون هذه الوسائل مرتبطة بالبيانات المُوقّعة بشكل أن كل تعديل لاحق في البيانات الموقعة يكون قابلاً للاكتشاف.
٥٠	توقيع إلكتروني مصدق	certified electronic signature	توقيع إلكتروني مصدق بشهادة تصديق إلكتروني.
٥١	حاسوب	computer	الحاسوب هو أي جهاز إلكتروني ثابت أو منقول يحتوي على نظام معالجة البيانات، أو تخزينها أو ارسالها أو استقبالها أو تصفحها ويتعامل معها بواسطة برامج وانظمة معلوماتية.
٥٢	جرائم الإستغلال الجنسي للقاصرين	sexual abuse of minors	تشمل المواد الإباحية: الرسوم أو الصور أو الكتابات أو الأفلام أو الإشارات أو أية أعمال إباحية يشارك فيها قاصرون أو تتعلق باستغلال القاصرين في المواد الإباحية، والتي تُظهر «للعين» أو «للنظر»: - قاصر يقوم بفعل جنسي صريح، - شخص يبدو كقاصر يقوم بفعل جنسي صريح، - صور واقعية أو مصطنعة بالمحاكاة تظهر قاصراً يقوم بفعل جنسي صريح.
٥٣	جرم الاحتيال أو الغش بوسيلة معلوماتية	digital fraud or cyber fraud	يقصد به كل من أقدم عن قصد و بنيّة الغش وبصورة غير مشروعة على إلحاق ضرر مالي بالغير عن طريق إدخال أو تبديل أو محو أو تدمير بيانات معلوماتية، بكل شكل من أشكال التعدي على عمل نظام معلوماتي، وذلك للحصول دون وجه حق على منفعة مادية لنفسه أو للغير.
٥٤	جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية	cyber embezzelment	يقصد به كل من أقدم على سرقة أموال أو على اختلاسها باستعمال وسيلة معلوماتية.
٥٥	جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية	failing to report or bad reporting of a cyber crime	يقصد به كل من أخفق أو إمتنع عن قصد في الإبلاغ أو أبلغ عن قصد بشكل خاطئ عن جرائم المعلوماتية.
٥٦	جرم الإرهاب بوسيلة معلوماتية	cyber terrorism	يقصد به كل من ارتكب أعمالاً إرهابية أو ساهم فيها أو حرّض عليها باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية آخرى.
٥٧	جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشروع لها	identity theft	يقصد به كل من أقدم على الاستيلاء على أدوات التعريف والهوية العائدة لشخص آخر، والمستخدمة في نظام معلوماتي، وكذلك من أقدم عن قصد وبصورة غير مشروعة ومع علمه بالأمر على استخدام أدوات التعريف والهوية العائدة لشخص آخر في نظام معلوماتي.
٥٨	جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها	viewing and/or disseminating secret or sensitive data	يقصد به كل من أقدم عن قصد ودون سبب مشروع على الاطلاع بوسائل معلوماتية على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. يجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة.
٥٩	جرم الإعتداء على أي حق من حقوق المؤلف أو الحقوق المجأورة	offences related to infringements of copyright and related rights	يقصد به كل من أقدم قصداً على الإعتداء على أي حق من حقوق المؤلف أو الحقوق المجأورة المتعلقة بالأعمال الرقمية.
٦٠	جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية	cyber sexual harrassment against minors	يقصد به كل من أقدم على التحرش جنسياً بقاصر على شبكة الإنترنت أو بأية وسيلة معلوماتية آخرى، من أجل إشباع الرغبة الجنسية أو من أجل إقناع القاصر بالقيام بأنشطة جنسية سواء مجاناً أو بعوض.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٦١	جرم التحريض على القتل بوسيلة معلوماتية	inciting to commit murder in a digital way	يقصد به كل من أقدم على تحريض شخص آخر على القتل باستعمال شبكة الإنترنت أو أية وسيلة معلوماتية آخرى.
٦٢	جرم التزود أو تزويد الغير بمواد إباحية لقاصرين بواسطة نظام معلوماتي	procuring child pornography through a computer system for oneself or for another person	يقصد به كل من حصل قصداً، وبصورة غير مشروعة، على مواد إباحية لقاصرين عبر نظام معلوماتي لصالحه أو لصالح الغير.
٦٣	جرم التعرض للبيانات المعلوماتية	data interference	يقصد به فعل كل من أقدم قصداً وبصورة غير مشروعة على تعديل أو إلغاء أو محو أو إفساد أو تدمير البيانات الرقمية. يجوز الاشتراط أن يتسبّب الفعل المذكور بأضرار جسيمة.
٦٤	جرم التنصت أو التقاط أو اعتراض الرسائل	messages or communication	يقصد به كل من يتنصت عن طريق شبكة المعلومات أو أجهزة الحاسوب أو يلتقطها أو يعترضها، دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة.
٦٥	جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة	obtaining secret governmental data in a digital way	يقصد به كل من أقدم على الاطلاع أو على الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أية وسيلة معلوماتية آخرى.
٦٦	جرم العبث بالأدلة القضائية المعلوماتية	cyber tampering with judicial evidence	يقصد به كل من أقدم على العبث بأدلة قضائية معلوماتية أو على إتلافها أو تخبئتها أو التعديل فيها أو محوها.
٦٧	جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه	illegal access	يقصد به كل من أقدم قصداً على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه. ويجوز اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحماية الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة آخرى جرمية أو في ما يتعلق بالربط مع أنظمة معلوماتية آخرى.
٦٨	جرم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه مع التعرض للبيانات المعلوماتية	illegal access to a computer system or staying there with data interference	يقصد به كل من أقدم على الولوج غير المشروع إلى نظام معلوماتي أو جزء منه أو المكوث غير المشروع فيه مع قيامه بتعديل البيانات الرقمية أو البرامج أو إلغائها أو محوها أو إفسادها أو تدميرها أو المساس بعمل النظام المعلوماتي. ويجوز أيضاً اشتراط أن يتم الفعل عن طريق مخالفة تدابير الحماية الجارية على النظام المعلوماتي وبنيّة الحصول على بيانات رقمية أو بنيّة آخرى جرمية أو بنية الربط مع أنظمة معلوماتية آخرى.
٦٩	جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية	misuse of computers and software	يقصد به كل من قدّم أو أنتج أو وزّع أو حاز بغرض الإستخدام جهازاً أو برنامجاً معلوماتياً أو أية بيانات معلوماتية معّدة أو كلمات سر أو شيفرات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في الإرشاد الحاضر.
٧٠	جرم استعمال بطاقة مصرفية مقلّدة	use of forged credit card	يقصد به كل من أقدم قصداً، مع علمه بالأمر، على استعمال بطاقة مصرفية مقلّدة سواء حصل بنتيجة هذا الاستعمال على أموال أو لم يحصل لسبب لا يعود إليه.
٧١	جرم إعاقة عمل نظام معلوماتي	system hindering	يقصد به كل من أقدم بنيّة الغش، وبأية وسيلة، على إعاقة عمل نظام معلوماتي أو على إفساده.
٧٢	جرم اعتراض بيانات معلوماتية	digital data interception	يقصد به كل من أقدم قصداً وبصورة غير مشروعة على إعتراض بيانات معلوماتية بوسائل تقنية وذلك عند نقلها غير المُتاح للجمهور من أو إلى أو داخل نظام معلوماتي. ويجوز اشتراط أن يتم الفعل بنية جرمية أو بنية الربط مع أنظمة معلوماتية آخرى.
٧٣	جرم إفشاء معلومات ذات طابع شخصي	dissemination of personal data	يقصد به كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات طابع شخصي، لأشخاص لا يحق لهم الاطلاع عليها.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٧٤	جرم إنتاج مواد إباحية لقاصرين بقصد بثها بواسطة نظام معلوماتي	producing child pornography for the purpose of its distribution through a computer system	يقصد به كل من أنتج قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بقصد توزيعها أو بثها عبر نظام معلوماتي.
٧٥	جرم أعمال التسويق والترويج غير المرغوب بها	unsolicited marketing and promoting offense	يقصد به كل من أقدم على إرسال رسائل ترويج أو تسويق غير مرغوب بها إلى الغير دون تمكين المُرسل إليهم من أيقاف ورود هذه الرسائل، في حال رغبوا بذلك، بدون ان يتحملوا أية نفقات إضافية.
٧٦	جرم بث بيانات تهدد الأمن والسلامة العامة بوسيلة معلوماتية	digitally transmitting information that threatens public safety or national security	يقصد به كل من أقدم على بث أو إذاعة أو نشر بيانات أو معلومات تهدد الأمن أوالسلامة العامة في الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال أية وسيلة معلوماتية آخرى.
٧٧	جرم بيع أو تأجير وسائل تشفير ممنوعة	encryption tools selling or leasing prohibited	يقصد به كل من أقدم على بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.
٧٨	جرم بيع أو عرض عمل مقلّد أو وضعه في التداول	selling or offering counterfeit work	يقصد به كل من أقدم على بيع أو عرض للبيع أو وضع بالتداول أو قدّم قصداً عملاً رقمياً مقلداً.
٧٩	جرم تحريض القاصرين على أنشطة جنسية غير مشروعة أو إعدادهم لذلك بوسيلة معلوماتية	inciting minors to...	يقصد به كل من شجّع أو حرّض قاصراً على القيام بأنشطة جنسية غير مشروعة سواء مجاناً أو بعوض أو ساهم في إعداده لهذا الأمر، وذلك بأي وسيلة معلوماتية.
٨٠	جرم ترويج الكحول للقاصرين على الإنترنت	providing alcohol to minors online	يقصد به كل من أقدم على ترويج الكحول مستهدفاً القاصرين على شبكة الإنترنت أو باستعمال أية وسيلة معلوماتية آخرى.
٨١	جرم ترويج المواد المخدرة على الإنترنت	drug dealing online	يقصد به كل من أقدم على ترويج المواد المخدرة على شبكة الإنترنت أو باستعمال أية وسيلة معلوماتية آخرى.
٨٢	جرم تزوير النقود الإلكترونية	cyber money forgery	يقصد به كل من أقدم عن قصد وبصورة غير مشروعة على تزوير نقود إلكترونية.
٨٣	جرم تسهيل وتشجيع المقامرة على الإنترنت	facilitating and encouraging online gambling	يقصد به كل من سهّل أو شجّع أو روّج لإنشاء مشروع مقامرة على شبكة الإنترنت أو باستعمال وسيلة معلوماتية آخرى.
٨٤	جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية	cyber interference in government's activities	يقصد به كل من أقدم على تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال أية وسيلة معلوماتية.
٨٥	جرم تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص	providing encryption tools that secure privacy without a license	يقصد به كل من أقدم على توفير وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة.
٨٦	جرم تقليد إمضاء المؤلف أو ختمه	forging author's signature or seal	يقصد به كل من قلّد بقصد الغش إمضاء المؤلف أو ختمه أو إشارته.
٨٧	جرم تقليد بطاقة مصرفية	credit card counterfeiting	يقصد به كل من أقدم قصداً وبصورة غير مشروعة على تقليد بطاقة مصرفية.
٨٨	جرم تقليد عمل رقمي أو قرصنة البرمجيات	piracy of a digital work or software	يقصد به كل من أقدم قصداً على تقليد عمل رقمي أو على قرصنة البرمجيات، ويعتبر نسخ البرمجيات من قبيل أفعال التقليد.
٨٩	جرم تملك وإدارة مشروع مقامرة على الإنترنت	owning and operating a gamblig business online	يقصد به كل من تملك أو أدار مشروع مقامرة أو عرض ألعاب مقامرة على شبكة الإنترنت أو بأية وسيلة معلوماتية آخرى.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
٩٠	جرم تهديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية	cyber threatening or attacking ,persons because of their race color or religious views	يقصد به كل من أقدم على تهديد شخص أو تحقيره أو التعدي عليه بسبب إنتمائه العرقي أو المذهبي أو لونه، وذلك بواسطة شبكة الإنترنت أو بأية وسيلة معلوماتية آخرى.
٩١	جرم توزيع أو بث أو نقل مواد إباحية لقاصرين بواسطة نظام معلوماتي	distributing or transmitting child pornography through a computer system	يقصد به كل من وزّع أو بثّ أو نقل قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.
٩٢	جرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير	disseminating data that is likely to deny, alter or justify crimes against humanity	يقصد به كل من أقدم قصداً على توزيع أو نشر معلومات بواسطة شبكة الإنترنت أو بأية وسيلة إلكترونية آخرى من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.
٩٣	جرم حيازة مواد إباحية لقاصرين على وسيلة تخزين إلكترونية أو نظام معلوماتي	possessing child pornography in a computer system or on a computer-data storage medium	يقصد به كل من حاز قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين على وسيلة تخزين إلكترونية أو نظام معلوماتي.
٩٤	جرم عدم الاستجابة لطلب الشخص المعني بالاطلاع أو التصحيح	failing to respond to the request of the subject concerned in correction or view	يقصد به كل من يرفض بدون وجه حق الاستجابة في مهلة قصيرة إلى طلب الشخص المعني بالاطلاع على المعلومات ذات الطابع الشخصي الخاصة به أو بتصحيحها.
٩٥	جرم عدم حيازة ترخيص أو تصريح لتسويق أو توزيع أو تصدير أو استيراد وسائل تشفير	Lacking or failing to obtain a license to market, distribute import or export encryption tools	يقصد به كل من أقدم على توزيع أو تسويق أو تصدير أو استيراد وسائل تشفير دون حيازة ترخيص أو تصريح من قبل المراجع الرسمية المختصة في الدولة.
٩٦	جرم عرض مواد إباحية لقاصرين بواسطة نظام معلوماتي	offering or making available child pornography through a computer system	يقصد به كل من عرض أو وفّر أو قدّم قصداً، وبصورة غير مشروعة، مواد إباحية لقاصرين بواسطة نظام معلوماتي.
٩٧	جرم قبول الدفع ببطاقة مصرفية مقلّدة	accepting payment through a counterfeit credit card	يقصد به كل من قبِلَ أيفاءه مبلغاً من المال بواسطة بطاقة مصرفية مقلّدة مع علمه بحقيقتها.
٩٨	جرم معالجة معلومات ذات طابع شخصي دون احترام القواعد القانونية	illegal personal data processing	يقصد به كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون التقيد بالقواعد القانونية المقررة لمعالجة المعلومات ذات الطابع الشخصي.
٩٩	جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص	personal data processing without a license	يقصد به كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص مسبق يتيح له القيام بمثل هذه المعالجة من المراجع الرسمية.
١٠٠	جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية	cyber dissemination and publication of racist news	يقصد به كل من أقدم قصداً على نشر وتوزيع معلومات تثير النعرات العنصرية وتهدف إلى التمييز العنصري بحق أشخاص معينين، وذلك بواسطة شبكة الإنترنت أو غيرها من الوسائل المعلوماتية.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٠١	جرم وضع إسم مختلس على عمل	copyright infringement	يقصد به كل من أقدم بقصد الغش على وضع إسم مختلس على عمل رقمي أو كلّف الغير بذلك.
١٠٢	جريمة سيبرانية	cyber crime	يقصد بها أي فعل جرمي أو عمل غير مشروع يستعمل أياً من أدوات وخدمات شبكة الإنترنت مثل غرف المحادثة، المواقع الإلكترونية، الرسائل الإلكترونية الخ.. لإرتكاب أعمال غش أو احتيال تطال مالاً معيناً أو تتعرض لشخص ما معنوياً أو مادياً أو تخرب أجهزة أو شبكات أو برامج حاسوب. يدخل ضمنها إرسال الفيروسات وإرسال البريد غير المرغوب به والإباحية لدى الأطفال، تغطية الدعارة على الخط.
١٠٣	جدار حماية	firewall	يعني نظاماً أمنياً لتنظيم حركة المرور عند نقاط الاتصال بين إنترنت وإنترانت (أو بين أي شبكتين في الحالة العامة)، يسمح لحزم البيانات بالعبور بين الشبكتين، أو يمنعها، اعتماداً على مجموعة من القواعد يحددها مدير شبكة إنترانت (مثل اسم المستخدم وكلمة السر، أو عنوان IP، أو رقم هاتف المتصل في حالة السماح بالدخول عبر اتصالات dial-in). ويوجد العديد من حلول الحواجز النارية، فبعضها عبارة عن برمجيات فقط تعمل على أي مزوّد، والبعض الآخر حلول متكاملة، تتألف من برمجيات تعمل على أجهزة مخصصة، ومزودة بمودمات وبطاقات شبكة.
١٠٤	حاسوب مخدم	computer server	حاسوب أو برنامج حاسوب يقوم بتقديم خدمات معينة لعملاء يستعملون برامج على حواسيب آخرى مثلweb server خادم صفحات الويب.
١٠٥	حصان طروادة	trojan horse	هو برنامج حاسوب يقوم بإخفاء نفسه بشكل برنامج مفيد لكنه يعرض الخصوصية والحماية مما يسمح للغير بالولوج إلى جهاز الحاسوب المصاب بعد إضعاف الحماية.
١٠٦	حقوق النسخ والتأليف	copyright	مجموعة من الحقوق الحصرية (exclusive rights) التي تنظم استعمال النصوص أو أي تعبير عملي (فني، أدبي، أكاديمي) عن فكرة أو معلومة ما. أي انه «حقوق نسخ واستخدام» عمل إبداعي جديد. تشكل هذه الحقوق نوعاً من الحماية للمبدع ليتقاضى أجرا عن إبداعه لفترة محددة تختلف من بلد إلى آخر.
١٠٧	حقوق حصرية	exclusive rights	حق النسخ، حق الإشتقاق، حق التمثيل أوالإداء، حق العرض، حق النشر أو التوزيع هي الحقوق الأساسية التي يتمتع بها صاحب حق المؤلف بالنسبة لمؤلفه وهي حقوق مصانة قانونياً.
١٠٨	حقوق مجأورة	neighbouring rights	هي الحقوق التي يتمتع بها الفنانون المؤدون ومنتجو التسجيلات السمعية ومؤسسات ومحطات وشركات وهيئات البث التلفزيوني والإذاعي ودور النشر.
١٠٩	حماية المستهلك	consumer protection	قواعد قانونية تعنى بحماية المستهلك من أي إساءة قد يتعرض لها أثناء قيامه بتعامل تجاري مع محترف.
١١٠	حماية وفقاً للحق الخاص	sui generis	هي نوع من أنواع الحماية القانونية الخاصة لقواعد البيانات وبعض الأعمال التي تتمتع بحسب طبيعتها بميزة تجعل حمايةها عبر القوانين العادية للملكية الفكرية غير كاملة مما يوجب حمايةها بموجب نص خاص يراعي طبيعتها.
١١١	خادم صفحات الويب	web server	برنامج حاسوب يقوم بخدمة صفحات الويب.
١١٢	خدمة إلكترونية	electronic service	هي كل خدمة، عادةً لقاء مقابل، مقدّمة عن بعد بواسطة وسائل معلوماتية لمعالجة وتخزين البيانات، وذلك بناءً على طلب فردي من المتعامل.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١١٣	خدمة القيمة المضافة	value added service	كل خدمة تتطلب معالجة حركة البيانات أو بيانات الموقع بما يتعدى حركة البيانات اللازمة لأجل إرسال المراسلة أو فوترتها.
١١٤	خطابات أو اتصالات تجارية	commercial communication	كل شكل اتصال مخصص لترويج، بشكل مباشر أو غير مباشر، الأموال أو الخدمات أو صورة شركة أو مؤسسة أو شخص يمارس نشاطاً تجارياً أو صناعياً أو حرفياً أو يمارس مهنة منظمة بقانون.
١١٥	خوارزمية التشفير	cryptographic algorithm	يقصد بها النمط المتبع الذي يتم بواسطته تحويل نص مقروء إلى نص غير مقروء من العامة بدون استعمال خوارزمية فك التشفير.
١١٦	دخول غير مشروع	illegal access	دخول شخص بطريقة غير معتمدة الى الحاسوب، أو إلى موقع إلكتروني أو نظام معلوماتي أو شبكة حواسيب غير مصرح لذلك الشخص بالدخول اليها.
١١٧	منصة إلكترونية	electronic platform	كل وسيلة مادية تستخدم لتخزين وتدأول المعلومات والبيانات الإلكترونية.
١١٨	دفع إلكتروني	e-payment	كل نظام أو برنامج يمكن من القيام بعمليات الدفع بالاستعمال الكلي أو الجزئي للوسيلة الإلكترونية.
١١٩	دفع مقابل النقرة	pay-per-click	طريقة إعلانية على الخط حيث يتم الدفع عن كل مرة يقوم فيها مستهلك بالنقر للدخول إلى موقع أو وصلة إلكترونية.
١٢٠	دودة	worm	الدودة هي عبارة عن شيفرة خاص بالحاسوب صمم لينتشر ذاتياً بدون واسطة برنامج آخر وهو ينسخ نفسه ويقوم بألإضرار بجهاز حاسوب أو شبكة حواسيب ويبطىء عمله.
١٢١	رسالة إلكترونية قنبلة	email bomb	تعني إغراق عنوان بريد إلكتروني بعدد كبير جداً من الرسائل الإلكترونية بهدف شل عمل نظام الشبكة حيث يكون المتلقي متصلاً.
١٢٢	رسالة إلكترونية أو بريد إلكتروني	data message or email	المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها كلياً أو جزئياً بوسائل إلكترونية أو بوسائل مشابهة بما في ذلك تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي أو أي وسيلة تقنية لنقل معلومات.
١٢٣	رمز نطاق على المستوى الوطني	ccTLD	هو رمز النطاق على المستوى الوطني الذي يعرّف بنطاق الدولة مثل .com.us أو .co.uk.
١٢٤	سند إلكتروني	electronic record	القيد أو العقد أو المراسلة أو المعلومات التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم.
١٢٥	سلطة مراقبة معالجة البيانات	data processing supervising authority	وهي السلطة أو الهيئة المعيّنة من قبل الحكومة لمراقبة معالجة البيانات وصحة استعمالها.
١٢٦	«سنيفر»	sniffer	السنيفر هو ببساطة برنامج صغير يمكنه جلب أي بيانات في الشبكة والاستفادة منها سواء للاختراق أو للمراقبة.
١٢٧	شخص ثالث، الغير	third party	هو كل من يرد ذكره في القانون ولا يكون مراقب البيانات أو معالج البيانات (أو أحد موظفيه) أو متلقي البيانات أو الشخص موضوع البيانات.
١٢٨	شخص موضوع البيانات (صاحب البيانات)	data subject	هو الشخص الطبيعي الذي هو موضوع البيانات/صاحب البيانات.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٢٩	شهادة مصادقة إلكترونية	digital certificate	هي شهادة إلكترونية تربط ما بين بيانات التحقق من التوقيع الإلكتروني وشخص معين وتؤكد هوية هذا الشخص التوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية.
١٣٠	شهادة مصادقة إلكترونية مؤهلة	qualified certificate	هي شهادة إلكترونية تشتمل على إشارة إلى أنها شهادة موصوفة، تحدد مزود خدمات المصادقة الإلكترونية والبلد الذي يقيم فيه، اسم الموقّع، إمكانية صفة خاصة للموقّع عند الإقتضاء في ضوء كيفية استخدام شهادة المصادقة، وبيانات التحقق من التوقيع الإلكتروني التي تقابل بيانات إنشاء التوقيع الإلكتروني الموضوعة تحت رقابة الموقّع، تحديد بدأية مدة صلاحية الشهادة وإنتهائها، ورقم الشهادة والتوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية الذي أصدر الشهادة، وحدود إستخدام الشهادة، والقيمة القصوى للمعاملات التي يمكن استخدام الشهادة فيها، وينبغي أن تكون الشهادة صادرة من قبل مزود خدمات مصادقة إلكترونية يلبي شروطاً معينة.
١٣١	شيك إلكتروني	electronic cheque	هو الشيك الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً.
١٣٢	صفحة الوب أو موقع الوب أو موقع الإنترنت	web page, website	هو موقع (أو صفحة على الإنترنت) متكوّن من مجموعة صفحات وب وصور وفيديو أو أي مضمون رقمي آخر يتم الولوج إليه وفقاً لمحدد مصدر موحد URL وهي عامةً مؤلفة من اسم الموقع والمعرّف الرقمي لجهاز الحاسوب IP address.
١٣٣	صك إلكتروني	electronic bond	يقصد به ورقة مالية أو تجارية قابلة للتداول إلكترونياً.
١٣٤	طرف معوّل	relying party	هو كل شخص يجوز أن يتصرف استناداً إلى شهادة مصادقة إلكترونية أو إلى توقيع إلكتروني.
١٣٥	طوبوغرافيا المنتجات شبه الموصلة	topography	طوبوغرافيا تعني سلسلة صور مربوطة ببعضها، أياً كانت المادة المُنبّتة أو المُرمّزة بواسطتها، وهي تتمتع بالخصائص التالية: أ. تمثّل الطوبوغرافيا الخريطة الثلاثية الأبعاد للطبقات التي تشكّل منتجاً شبه موصل. ب. في الطوبوغرافيا، كل صورة تمثّل الرسم أو جزءاً من الرسم العائد لسطح أو لإحدى طبقات المنتج شبه الموصل في أية مرحلة من مراحل صنعها.
١٣٦	عقد إلكتروني	electronic contract	هو عقد نظّم بوسيلة إلكترونية.
١٣٧	عقد عن بعد (التعاقد عن بعد)	distance contact	هو أي عقد يتعلق بمنتجات أو خدمات بين تاجر ومستهلك بواسطة خطة أو خدمة بيع عن بعد منظمة من قبل التاجر بهدف التعاقد وهذه الخطة تستعمل بشكل حصري أسلوباً أو عدة أساليب وسائل اتصال عن بعد بما في ذلك وقت إتمام التعاقد.
١٣٨	عنوان الفوترة	billing address	وهو العنوان حيث يستلم المستهلك كشف حساب بطاقة إئتمانه. ويُستعمل للتأكد من أن مستعمل البطاقة هو مالكها الحقيقي.
١٣٩	غش بطاقات الإئتمان	credit card fraud	الاستعمال غير المرخص به وغير القانوني لبطاقة إئتمان لا تعود للمستعمل بالضرورة، لأجل شراء منتجات أو خدمات أو لإضافة كلفة على بطاقة عن خدمات أو بضائع لم يتم شراؤها بالفعل.
١٤٠	تزييف	pharming	تعني السعي والبحث للحصول على معلومات سرية عن طريق التخفي.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٤١	فك التشفير	decryption	يقصد به عملية إعادة تحويل بيانات مشفرة إلى وسيلة مقروءة عن طريق استعمال برنامج أو طريقة لفك التشفير.
١٤٢	فيروس	virus	فيروس هو برنامج حاسوب أو شيفرة خفية في برنامج آخر ينتقل من جهاز إلى آخر ويصيب الجهاز خلال التجوال ويقوم بتخريب البرمجيات أو الأجهزة.
١٤٣	قاصر	minor	القاصر هو كل من لم يتم الثامنة عشرة من عمره. ويجوز لدولة عضو أن تخفضّ السن إلى حدود أدنى، لا تقل عن السادسة عشرة.
١٤٤	قاعدة البيانات	database	هي مجموعة من عناصر البيانات المنطقية المرتبطة مع بعضها البعض بعلاقة رياضية، وتتكون قاعدة البيانات من جدول واحد أو أكثر من جدول. ويتكون الجدول من سجل (Record) أو أكثر من سجل ويتكون السجل من حقل (Field) أو أكثر من حقل. تُخزَّن في جهاز الحاسوب عَلى نحو منظّم، حيث يقوم برنامج الحاسوب المسمّى محرك قاعدة البيانات (Database Engine) بتسهيل التعامل معها والبحث ضمن هذه البيانات، وتمكين المستخدم من الإضافة والتعديل عليه.
١٤٥	قنبلة ذكية أو منطقية	logic bomb	هي عبارة عن شيفرة ضمن برنامج معلوماتي متمثّل بفيروس يتم تفعيله عند القيام بعمل معين من قبل من يستعمل الجهاز المصاب به.
١٤٦	كتابة إلكترونية	e-writing	كل حروف أو أرقام أو رموز أو أي علامات آخرى تثبت على دعامة إلكترونية أو ضوئية أو أي وسيلة آخرى مشابهة وتعطي دلالة قابلة للإدراك.
١٤٧	كره الأجانب على الخط	internet xenophobia	يقصد به أي من أفعال ترويج أو دس التعابير والرسوم العنصرية المعادية للأجانب التي تتم ياستعمال شبكة الإنترنت.
١٤٨	شيفرة خبيث	malicious code	الشيفرة الخبيثة يعني أي شيفرة تضاف، تعدل، تغير، أو تزال من برنامج لأجل إحداث ضرر أو تحوير طريقة عمل البرنامج أو النظام. الأمثلة هي الفيروسات وأحصنة طروادة والدودة.
١٤٩	مُرسل إليه	adressee	هو الشخص الطبيعي أو المعنوي أو الهيئة الذين يكونون مخولين تلقي بيانات. والمرسل إليه يختلف عن الشخص المعني بالمعالجة وعن المسؤول عن المعالجة وعن المعالج الثانوني وعن تابعي الأخيرين. ولا تعتبر بمثابة مُرسل إليه السلطات المخولة قانوناً طلب بيانات من المسؤول عن المعالجة.
١٥٠	متلقي البيانات	recipient	هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذين يتلقون البيانات أو الذين يستحصلون على إذن بالاطلاع عليها.
١٥١	مجتمع المعلومات	information society	هو مجتمع حيث صناعة وتوزيع وعرض واستعمال وإدخال وتبادل والتحكم بالمعلومات يعتبر نشاطاً إقتصادياً وسياسياً وثقافياً.
١٥٢	محترف	professional	هو الشخص الطبيعي أو الشركة أو المؤسسة الذين يحترفون نشاطاً معيناً كبيع السلع أو توزيعها أو تأجيرها أو تقديم الخدمات.
١٥٣	مراسلة إلكترونية	electronic communication	مراسلة بأي شكل مخصصة لترويج، بشكل مباشر أو غير مباشر، لمنتجات أو خدمات أي شخص يمارس نشاطاً تجارياً أو صناعياً أو حرفياً أو يمارس مهنة حرة. باستثناء المراسلة التي: أ- تحتوي فقط على معلومات تسمح بالوصول لهذا الشخص كالمكان الجغرافي ورقم الهاتف وعنوان الموقع على الإنترنت أو البريد الإلكتروني؛ أو ب- تتعلق بمنتجات أو خدمات هذا الشخص إنما تمت بالاستقلال عنه.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٥٤	مراقب البيانات	data controller	هو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذين يقومون منفردين أو بالإشتراك مع آخرين بتحديد كيفية وغاية معالجة البيانات.
١٥٥	مزوِّد خدمة الإنترنت	internet service provider	هو كل هيئة أو شخص طبيعي أو معنوي يقدم خدمة النفاذ إلى الإنترنت
١٥٦	مزود خدمات مصادقة إلكترونية	certification services provider	هو كل هيئة أو شخص طبيعي أو معنوي يسلّم شهادة إلكترونية أو يقدم خدمات إلكترونية آخرى مرتبطة بالتواقيع الإلكترونية.
١٥٧	مزود خدمة	service provider	منظمة (عامة أو خاصة) تؤمن خدمات اتصالات أو حفظ أو معالجة أو الثلاثة معاً. مثل شركات الهاتف ومزودي خدمات الإنترنت ومزودي خدمات البرمجيات ومزودي خدمات الحفظ.
١٥٨	مزود خدمة الاتصال	communication service provider	يقصد به أي منظمة أو هيئة تقوم بتقديم خدمة اتصال إلكترونية سواء شملت الصوت فقط كالهاتف أو البيانات أو الإترنت، أو الثلاثة معاً، وتتضمن هذه الخدمة تمكين المشترك من نقل البيانات عبر الاتصال.
١٥٩	مساعدة أو تحريض بوسيلة إلكترونية على إرتكاب جرائم ضد الإنسانية	inciting or assisting in committing crimes against humanity online	يقصد به كل من ساعد قصداً أو حرّض بواسطة شبكة الإنترنت أو أية وسيلة إلكترونية آخرى شخصاً آخر على إرتكاب جرائم ضد الإنسانية.
١٦٠	مستضيف البيانات	data host	هيئة، أو منظمة تتولى تخزين المعلومات العائدة للغير لديها، ولحساب هذا الغير، مقابل بدل مادي أو مجاناً، كما تتولى وضع هذه المعلومات بتصرف الجمهور من خلال إستخدام شبكات اتصال.
١٦١	مستهلك	consumer	أي شخص طبيعي يتصرف لغايات غير متعلقة بتجارته، عمله أو مهنته.
١٦٢	مشغل وسيلة الاتصال عن بعد	operator of a means of communication	هو أي جهة خاصة أو حكومية تكون وظيفتها جعل وسائل الاتصال عن بعد مؤمنة للتجار.
١٦٣	مصنف جماعي	collective work	المصنف الذي يساهم فيه عدة اشخاص طبيعيين، بمبادرة شخص طبيعي أو معنوي وتحت إشرافه بحيث يصعب فصل عمل كل مساهم وتمييزه على حدة، ويتم نشر هذا المصنف باسم الشخص الطبيعي أو المعنوي.
١٦٤	مصنف مشترك	co-work	المصنف الذي يساهم في آخراجه مؤلفان اثنان أو اكثر ويمكن فصل عمل كل منهما وتمييزه على حدة.
١٦٥	مضايقة أو ملاحقة السيبرانية	cyber stalking	استعمال أجهزة الحاسوب والإنترنت لمضايقة أفراد وملاحقتهم بشكل يزعجهم أو يعتبر تدخلاً في خصوصياتهم.
١٦٦	معالج البيانات	data proccessor	يقصد به المسؤول عن المعالجة وهو الشخص الطبيعي أو المعنوي أو السلطة العامة أو الهيئة أو خلافه الذي يقوم منفرداً أو بالإشتراك مع آخرين بمعالجة البيانات لصالح المراقب.
١٦٧	معالج ثانوي	secondary data processor	الشخص الطبيعي، أو المعنوي أو الهيئة، الذي يعالج بيانات ذات طابع شخصي لمصلحة المسؤول عن المعالجة.
١٦٨	معالجة البيانات الشخصية	proccessing of personal data	عملية أو مجموعة عمليات منفذة على البيانات الشخصية بوسيلة آلية أو غيرها مثل الجمع والتسجيل، التنظيم والتحديث والتعديل والإسترجاع والمعاينة والحفظ والكشف بواسطة النقل والضبط والإفشاء أو بشكل عام العرض علانية والدمج والمحو ومنع الوصول أو الإلغاء.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٦٩	معاملات	transactions	إجراء، أو مجموعة من الإجراءات . يتم بين طرفين أو اكثر لانشاء التزامات على طرف واحد أو التزامات تبادلية بين اكثر من طرف ويتعلق بعمل تجاري أو التزام مدني أو بعلاقة مع أي دائرة حكومية .
١٧٠	معاملات إلكترونية	electronic transactions	المعاملات التي تنفذ بوسائل إلكترونية.
١٧١	معاملات إلكترونية مؤتمتة	automated e-transactions	معاملات يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بواسطة وسائل أو سجلات إلكترونية، حيث تكون سجلات احد أو كلا الطرفين غير خاضعة لمتابعة أو مراجعة من شخص طبيعي ، كما في السياق العادي لإنشاء وتنفيذ العقود والمعاملات .
١٧٢	عنوان بروتوكول الإنترنت	IP address	هو عنوان بروتوكول الإنترنت لأي جهاز (حاسوب، هاتف محمول، آلة طابعة، موجه Router...إلخ) مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت، سواء أكانت شبكة محلية أو شبكة الإنترنت. يقابل عنوان بروتوكول الإنترنت مثلاً في شبكات الهاتف رقم الهاتف.
١٧٣	معلومات إلكترونية	electronic information	البيانات والنصوص والكتابات والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك التي يتم حفظها، تخزينها، إرسالها، تعديلها، إسترجاعها أو معأينتها بطيقة إلكترونية.
١٧٤	المفتاح الخاص والعام	public and private key	يقصد بالمفتاح الخاص والعام، الخوارزمية التي تطبق على النص بحيث تغير من شكل البيانات، وهي بشكل عام عبارة عن معادلة رياضية معقدة جداً. يستخدم المفتاح العام للتشفير ويستخدم المفتاح الخاص لفك التشفير.
١٧٥	مكان العمل	place of business	أي مكان يعود لشخص ما بشكل دائم حيث يقوم هذا الشخص بنشاط تجاري عبر تأمين المنتجات والخدمات من مكان محدد لفترة محدودة.
١٧٦	ملف بيانات ذات طابع شخصي	personal data file	مجموعة بيانات شخصية منظمة بشكل يمكن الوصول إليها بناءً على معأيير معينة سواء متعلقة بالشخص أو بأي إشارة للشخص وتكون جاهزة للقراءة حتى ولو لم تكن معالجة بواسطة جهاز يعمل بأوامر أعطيت له لهذه الغاية.
١٧٧	ملف بيانات مؤتمة	automated Files	ملف يتضمن بيانات تتم معالجتها بشكل آلي.
١٧٨	مستخدم	user	أي شخص يقوم باستخدام خدمة اتصال إلكترونية لأهداف خاصة أو لأجل العمل بدون ان يكون بالضرورة مشتركاً بالخدمة.
١٧٩	منافسة طفيلية	parasitic competition	تعني قيام أحد الأشخاص بالاستفادة من الشهرة والسمعة الطيبة اللتين اكتسبهما الغير بصورة مشروعة، نتيجة جهده الشخصي دون أن يؤدي ذلك بالضرورة إلى أي خطر التباس يصيب الجمهور، ومثال على ذلك استعمال أساليب دعأية ناجحة معدة لصنف معين يعود للغير من أجل استقطاب الزبائن وتحويلهم نحو بضاعة من صنف آخر تختلف تماماً عن الأول.
١٨٠	منتج شبه الموصل	semiconductor	المنتج شبه الموصل يعني الشكل النهائي أو الوسيط لكل منتج يكون مؤلفاً من جوهر يتضمن طبقة من مواد شبه موصلة، ومكوّن من طبقة أو عدة طبقات آخرى من مواد موصلة وعازلة أو شبه موصلة، وتكون الطبقات مرتبة وفقاً لخريطة ذات أبعاد ثلاثية معينة، ويكون المنتج معداً للقيام حصرياً أو بصورة غير حصرية بوظيفة إلكترونية، وقد أصبحت المنتجات شبه الموصلة تدخل في تكوين مختلف الأجهزة الإلكترونية، بحيث أصبحت شائعة الاستعمال لدرجة كبيرة.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٨١	منتج توقيع إلكتروني	electronic-signature product	هو كل منتج تجهيزات أو برامج أو عنصر خاص من هذا المنتج، معدّة للاستخدام من قبل مزود خدمات مصادقة إلكترونية من أجل تقديم خدمات التواقيع الإلكترونية، أو معدّة للاستخدام من أجل إنشاء التواقيع الإلكترونية أو التحقق منها.
١٨٢	منشئ السجل	originator	الشخص الطبيعي أو المعنوي الذي يقوم مباشرة، أو يتم القيام بالنيابة عنه، بإنشاء و/أو إرسال السجل أو الرسالة الإلكترونية، ولا يعتبر مُنشِئاً الشخص أو الجهة العاملة كمزود خدمات في ما يتعلق بإنتاج أو معالجة أو إرسال أو حفظ تلك الرسالة الإلكترونية وغير ذلك من الخدمات المتعلقة بها.
١٨٣	بيانات تخضع لموافقة	data subject's consent	كل نوع من أنواع التعبير الطوعي والواضح والمحدد الذي يبديه الشخص موضوع البيانات بعد تلقيه المعلومات والذي يسمح بموجبه بمعالجة بياناته الشخصية.
١٨٤	موقّع	signatory	هو كل شخص يحوز آلية لإنشاء توقيع ويتصرف إما لحسابه الخاص أو لحساب شخص طبيعي أو معنوي يمثّله.
١٨٥	ند للند	p2p (peer to peer)	النظير للنظير أو مأيعرف باللغة الإنجليزية (Peer-to-Peer) وهو عملية تبادل الملفات والبيانات بين جهازين (حاسوب) شخصيين على شبكة الإنترنت. يستخدم هذا البروتوكول بكثرة في برامج مشاركة الملفات وتقاسمها.
١٨٦	نظام تشفير الملفات	encrypting file system (EFS)	عبارة عن تقنية تستخدم لتشفير و فك تشفير الملفات والمجلدات تحت نظام الملفات NTFS باستخدام مفتاح عام Public Key ومفتاح خاصPrivate Key .
١٨٧	نظام حفظ البيانات الشخصية	personal data filing system	مجموعة بيانات شخصية منظمة بشكل يمكن الوصول إليها بناءً على معايير معينة سواء متعلقة بالشخص أو بأي إشارة للشخص وتكون جاهزة للقراءة حتى ولو لم تكن معالجة بواسطة جهاز يعمل بأوامر أعطيت له لهذه الغأية.
١٨٨	نظام رسائل معلوماتي آلي	automated e-messaging system	هو برنامج أو وسيلة إلكترونية تُستخدم لاستهلال إجراء ما أو للإستجابة كلياً أو جزئياً للرسائل الإلكترونية أو لعمليات تنفيذها، وذلك دون مراجعة أو تدخل من شخص طبيعي في كل مرة يستهل النظام إجراء ما أو يطلق استجابة ما.
١٨٩	نظام معالجة البيانات	data processing system	أي نظام إلكتروني يستخدم لإنشاء رسائل البيانات أو إرسالها أو تسليمها أو معالجتها أو تخزينها على أي وجه آخر.
١٩٠	نظام معلوماتي	information system	نظام معلوماتي أو أي وسيلة إلكترونية آخرى تستعمل من اجل تنفيذ إجراء أو الاستجابة لإجراء بقصد إنشاء أو إرسال أو تسلم رسالة معلومات دون تدخل شخصي.
١٩١	نظام معلوماتي مؤتمت	automated message system	نظام معلوماتي مؤتمت أو أي وسيلة إلكترونية آخرى تستعمل من اجل تنفيذ اجراء أو الاستجابة لاجراء بقصد انشاء أو ارسال أو تسلم رسالة معلومات دون تدخل شخصي.
١٩٢	نقل البيانات	data transfer	يقصد بها نقل وتبادل البيانات إلكترونياً بين طرفين أو اكثر.
١٩٣	نقل المعلومات للجمهور بوسيلة إلكترونية	electronic data transfer to the public	يقصد به كل وضع بتصرف الجمهور أو فئات منه، بواسطة وسائل اتصالات إلكترونية، لإشارات أو كتابات أو صور أو أصوات أو رسائل من أية طبيعة كانت، والتي ليس لها طابع المراسلات الخاصة.
١٩٤	نقل المعلومات للجمهور على الخط	online data transfer to the public	يقصد به كل نقل، بناء لطلب فردي، لبيانات أو لمعلومات رقمية ليس لها طابع المراسلات الفردية، بواسطة وسائل اتصالات إلكترونية، تسمح بتبادل المعلومات بين المُرسل والمُستقبل.

	المصطلح باللغة العربية	المصطلح باللغة الإنكليزية	الشرح باللغة العربية
١٩٥	نقود إلكترونية	e-money	تتكون من وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية لمدة محددة، وتصدر مقابل نقد تتم مبادلته فوراً، بنفس القيمة ونفس العملة وتتيح للغير دون المصدر إتمام عمليات دفع.
١٩٦	وسائل الاتصال عن بعد	means of distance communication	أي وسائل يمكن استعمالها للتعاقد بين المستهلك والتاجر دون تواجدهما في مكان واحد.
١٩٧	وسائل اتصال إلكترونية	electronic communication means	أي وسائل اتصال تستعمل الأساليب الرقمية والإلكترونية لوصل مستعمل بشبكة أجهزة أو بالإنترنت أو بمشترك آخر.
١٩٨	وسائل تشفير المعلومات	encryption methods	يقصد بها التجهيزات أو البرامج المعدّة من أجل تحويل البيانات، عبر إتفاقات سرية، أو من أجل تحقيق العملية المعاكسة. تهدف وسائل التشفير إلى ضمان سرية المعلومات المخزّنة أو المُرسلة أو تأمين سلامتها أو موثوقيتها.
١٩٩	وسيط	intermediary	هو الشخص الذي يقوم، نيابة عن شخص آخر، بإرسال أو إستلام أو تخزين رسالة إلكترونية أو بتقديم خدمات آخرى فيما يتعلق بهذه الرسالة.
٢٠٠	وسيط إلكتروني	electronic intermediary	يقصد به برنامج الحاسوب أو أي وسيلة إلكترونية أخرى تستعمل من أجل تنفيذ اجراء بقصد إنشاء أو إرسال أو تسلم رسالة معلومات دون تدخل شخصي.
٢٠١	وسيط إلكتروني مؤتمت	automated electronic intermediary	برنامج أو نظام إلكتروني لحاسوب يمكن ان يتصرف أو يستجيب لتصرف بشكل مستقل، كلياً أو جزئياً، دون اشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له.
٢٠٢	وسيلة الدفع الإلكتروني	e-payment method	أي وسيلة تمكن صاحبها من القيام بعمليات الدفع المباشر كلياً أو جزئياً عن بعد عبر الشبكات، وتشمل الشيك الإلكتروني، وصورة الشيك، وبطاقات الدفع وغيرها من الوسائل.
٢٠٣	وصلة إلكترونية	link	عنوان موقع إلكتروني موجود على موقع آخر يمكن نقره، ويمكن نقره من الولوج مباشرة إلى الموقع بدون الحاجة لكتابة العنوان.
٢٠٤	هيئة الإنترنت للأسماء والأرقام المخصصة (الأيكان)	internet corporation for assigned names and numbers (ICANN)	هي منظمة غير ربحية تم تأسيسها دولياً لتتولى مسؤولية توزيع مجالات العناوين في بروتوكول الإنترنت وتخصيص معرّفات البروتوكول وإدارة نظام سجلات المواقع العامة عالية المستوى (gTLD) وسجلات المواقع عالية المستوى لرمز الدولة (ccTLD)، كما أنها تضطلع بمسؤولية وظائف إدارة نظام الخوادم المركزية.