الفصل الثالث عشر :
القوانين الدولية لمكافحة جرائم الإنترنت

إن الجريمة على شبكة الإنترنت تتسم بالدولية لأنها تتخطى حدود كل الدول، بسبب الطبيعة العالمية لانتشار خدمات الإنترنت على نطاق العالم أجمع، فقد انتشرت الجريمة على الإنترنت بدرجة كبيرة، ومازالت السلطات في بلدان كثيرة، مثل: الولايات المتحدة الأمريكية، وبريطانيا، وكوريا، والبرازيل، وغيرها، تتلقى بلاغات عديدة يومياً حول حدوث مثل هذه الجرائم. ولذلك، فإن التعامل معها يختلف من دولة إلى أخرى حسب التشريعات والقوانين السائدة في كل منها، فبعض الدول لديها القوانين التي تتعامل بها مع هذا النوع من الجرائم الجديدة، بينما هناك دول أخرى ليس لها مثل هذه التشريعات والأنظمة القانونية التي تواجهها بها.

وبناء على ذلك، فقد بدأت العديد من الدول خاصة التي لم تبحث أنظمة عقوباتها في مشكلة الجريمة على الإنترنت، في وضع قوانين عقوبات لمحاربة هذا النوع الذي لم يكن معروفا من الجرائم، الذي سيكون مصدر تهديد خطير للشركات والأفراد والمؤسسات من نواحٍ عدة؛ نفسية، واجتماعية، ومادية، وسيكون له تأثير شديد الخطورة على مستقبل شبكة الإنترنت وصناعة تقنية المعلومات بصورة عامة.

ولتجنب اتساع الجريمة وانتشارها على الإنترنت، وخاصة التي يقوم بها المتخصصون والمحترفون في هذا المجال أو الحد منها، فهناك إجماع من قبل مقدمي خدمة الإنترنت ومستخدميها والمعنيين بأمرها من أفراد ودول ومنظمات، على أن الخطوة الأولى لضبط استخدام الإنترنت، والحد من الجريمة فيها، هو وضع تشريع عام لأمن المعلومات فيها، ووجود شرطة مدربة، وقضاة مختصين، وضباط معنيين بتطبيق القانون توكل إليهم مسؤولية منع وقوع الجرائم وحدوث أعمال

مشينة في الشبكة، طالما أن القوانين الجنائية التقليدية لم تعد ملائمة لمعالجة هذا النوع من الجريمة، بسبب صعوبة إثبات عناصر الجريمة من خلالها.

وستقاس فعالية القوانين المشرعة للقضاء على الجريمة في الإنترنت، بمدى النجاح الذي تحققه في مقاضاة المجرمين أو مرتكبي الجرائم والمخالفات، والقضاء على هذه الجريمة الخطيرة المنتشرة في كل المجالات، وسد الثغرات والنقص الذي تعاني منه القوانين والتشريعات الحالية لدى معظم بلدان العالم، حتى المتقدمة منها، في هذا المجال التي تعاني من خطر الجريمة بصورة أكبر من غيرها.

ولقد قامت العديد من الدول بإعادة صياغة التشريعات والقوانين التقليدية، لتشمل الاحتيال عن طريق الحاسب الآلي. وكانت أولى هذه الدول السويد حيث كان قانون البيانات السويدي الصادر في أبريل ١٩٧٣، أول تشريع يعالج مشكلة الاحتيال عن طريق الحاسب. وتلتها في هذا المجال الولايات المتحدة الأمريكية التي أصدرت في الفترة من ١٩٧٦ – ١٩٨٥، قوانين مكافحة جرائم الحاسب التي تشمل كل ما يتعلق بأمور الحاسب من احتيال، وسرقة برامج وخدمات ومعلومات، أو إتلافها والهجوم على المعدات والدخول غير المشروع. ثم جاءت بعد ذلك بريطانيا بقانون مكافحة التزوير والتزييف لعام ١٩٨١م. وتلا ذلك تعديل القانون الجنائي الكندي في عام ١٩٨٥، ليشمل معاقبة المخالفين وتدمير الأجهزة والدخول غير المشروع، واستخدام بطاقات الائتمان، وجميع أنواع البطاقات المستخدمة للبنوك والخدمات الأخرى. وجاء بعد ذلك القانون الدانمركي لعام ١٩٨٥، وهو أول قانون جنائي عن الحاسب الآلي.

١٣-١ الوضع الحالي

لقد أدى انتشار استخدام الإنترنت على نطاق عالمي إلى صعوبة وضع قواعد وقوانين تحكم استخدامها من قبل الناشرين والمستقبلين. وفي الوقت ذاته لم تستطع القوانين المحلية في كل بلد السيطرة على الناشرين خارج حدودها الجغرافية. فمن أهم خواص الإنترنت أنها لا تتبع لجهة محددة تقع عليها مسؤولية تنظيمها أو التحكم في طريقة عملها أو إصدار التشريعات الخاصة بها. ولذلك لا توجد قوانين محددة متفق عليها ملزمة لجميع مستخدمي الإنترنت. ونتيجة لهذا الفراغ التشريعي وعدم الإجماع الدولي على موقف مجمع عليه لجأت كل دولة أو جهة مرتبطة بالإنترنت إلى وضع القوانين والسياسات الخاصة بها.

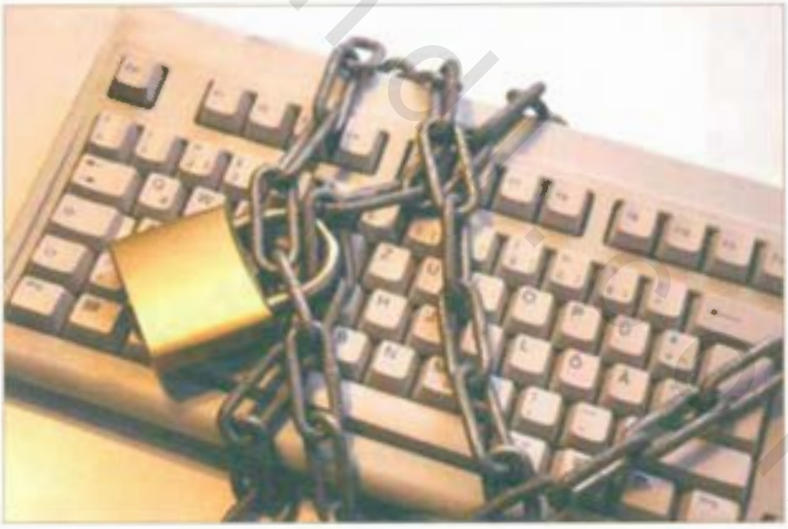
والذي شجع أكثر على ذلك حداثة تقنية الإنترنت وطبيعتها العالمية، فهي تتكون من حاسبات وشبكات منتشرة في مختلف أنحاء العالم. ولذلك، فإن المستخدم يستطيع من أي مكان في العالم الدخول إلى أي معلومات في حاسب آخر أو شبكة حاسبات أخرى مرتبطة بالإنترنت في أي مكان من العالم. وهذا يعني بالطبع وجود حرية كاملة وغير مقيدة في تداول المعلومات على الإنترنت مع تنوع مصادرها وأشكالها ومحتواها. وهو يعني أيضاً إمكانية الحصول على معلومات من موقع تتعارض الأعراف والقيم الاجتماعية السائدة فيه مع قوانين معظم، أو كل دول العالم، مثل: تخصيص مواقع لنشر الرذيلة، والعنف والتمييز العرقي، أو الديني، والإباحية، ولعب القمار، وتجارة المخدرات، والدعاية السياسية، بل أيضا ظهور مواقع تشجع على الانتحار، وجرائم القتل والاغتصاب مقابل أجر يتم الاتفاق عليه، من خلال تلك المواقع التي تديرها عصابات دولية محترفة، تعرض خدماتها لتصفية الخصوم، أو إذلالهم وأهانتهم عن طريق اغتصاب زوجاتهم وبناتهم.

ومن هنا يتساءل كثيرون عن مصير القانون على الإنترنت؟ وهل ستشهد الشبكة محاولات جادة من بعض الحكومات أو الدول جميعها لفرض قوانين وتشريعات محددة على نطاق

دولي؟ وهل ذلك ممكن مع اختلاف قوانين الدول وأعرافها؟

إن الآراء متباينة في هذا الشأن، ولم يطرح أي طرف أجنده محددة لذلك. فبعضهم يرى أن الحاجة أصبحت ملحة لوجود مثل هذا القانون الذي يؤمل أن يتم من خلاله حماية المستخدمين من الأخطار العديدة التي تنطوي عليها شبكة الإنترنت، وعالمها الافتراضي الذي لا يعرف الحدود أو القيود.

ولكن هل تحتاج الإنترنت فعلاً إلى قانون لتنظيمها والتحكم في أنشطتها؟ وهل هذا القانون لا يتناقض مع حرية التعبير لو افترضنا أنه معمول بها في شتى أنحاء العالم؟ إن النقاش في هذا الموضوع ساخنٌ جداً في أجهزة الإعلام، فالناس يتناولون جوانبه المختلفة بحماس شديد، فهناك من يرون تعارضه مع حرية التعبير، وهناك من يعتقدون بأن أنواعاً معينة من الاتصالات يجب عدم السماح بها على الإنترنت، بينما يرى آخرون أنها يشملها التعديل الأول لقانون الاتصالات الأمريكي.



وكذلك يعتقد بعض المختصين أن المراقبة المباشرة على الشبكة ليست هي الأداة التي تقضي على الممارسات الخاطئة أو الجريمة على الشبكة. لأن الشبكة مجرد وسط للاتصالات يتميز

بالسرعة وانخفاض التكلفة، ولذلك لا ينبغي معاقبتها على ما ينشر فيها من مادة غير مقبولة، أو ما ينتشر فيها من جرائم. والقائلون بهذا قد يكونون محقين في ذلك، فالعقاب يجب أن يطال من يقومون بالنشر والترويج ومن يرتكبون الجرائم، ولكن كيف؟ وبأي قانون وأية آلية؟ وهل يصلح القانون الأمريكي، أو الألماني، أو الهولندي، أو الصيني لمعالجة هذه المشاكل؟

ولنأخذ مثلاً لاختلاف القوانين على مستوى العالم وتباينها فيما يتعلق بالإنترنت. فالولايات المتحدة مثلاً تمنع وضع الصور والأفلام الإباحية لمن تقل أعمارهم عن السنّ القانوني، ولكن كثيرين يشاهدونها في مواقع أخرى في العالم، إسبانية كانت، أم روسية أم نرويجية.

وهناك قوانين كثيرة في بلدان عديدة تحظر ممارسة القمار، أو الأعمال غير الأخلاقية، أو ترويج الجريمة، ولكن للأسف هذه القوانين لم يكن لها تأثير كبير وبقيت محصورة ضمن الحدود الجغرافية للبلدان التي فرضتها.

ففي ألمانيا قامت شركة الهاتف الألمانية بقطع الخدمة الهاتفية عن مقدم خدمة أمريكي، بسبب بثه مادة دعائية للنازية في وقت تنشر فيه هذه المواد من قبل دول أخرى وتعد قانونية جداً. وكذلك أوقفت ألمانيا أحد أكبر مقدمي خدمة الإنترنت العالميين، وهو (كوميو سيرف) إلى أن قام بإزالة مئتي مجموعة إخبارية، ولم تكتفِ بذلك بل قامت بملاحقة المدير المحلي للشركة قضائياً بتهمة علمه بمرور المعلومات الممنوعة.

وفي خطوة أكبر من ذلك دعا البرلمان الأوربي إلى تحرك عالمي لضبط تبادل المواد الإباحية والعنصرية على الإنترنت، ودعا إلى تكوين (شرطة للإنترنت)، ووضع اتفاقيات دولية لمحاكمة من يسيئون استخدام الإنترنت، مركّزاً على ضرورة الاتفاق على معايير لتحديد المواد والاستخدامات غير المرغوب فيها على الشبكة.

وفي ماليزيا، حدد القانون أقل عمر لمستخدم الإنترنت بخمسة وعشرين عاماً. وفي الصين يتطلب استخدام الإنترنت تصريحاً من الشرطة. وفي دولة الإمارات العربية المتحدة

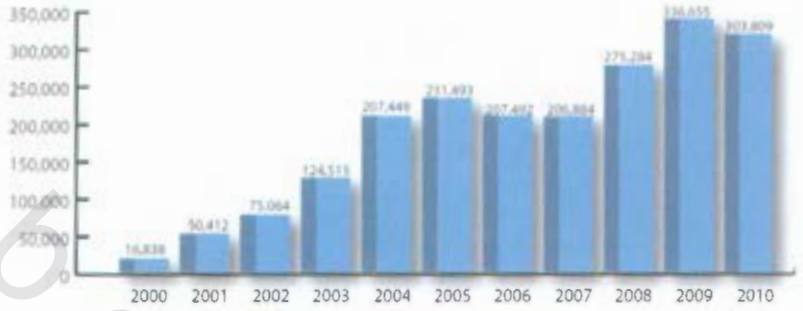
شكلت لجنة من الشرطة، ووزارة الإعلام، ومؤسسة الإمارات للاتصالات، وجامعة الإمارات، لوضع إستراتيجية قومية لاستخدام شبكة الإنترنت عندما اعترف مقدم الخدمة الرئيس بصعوبة التحكم بالشبكة.

وفي دبي طالبت الشركة المقدمة لخدمة الإنترنت علناً برقابة أفضل على الإنترنت. أما في سنغافورة فالإنترنت تصنف على أساس أنها وسيلة بث إعلامية، ومن ثم تخضع للرقابة الإعلامية عند نشر معلومات سياسية أو دينية.

ومع وجود كل هذه الاختلافات، فهناك إجماع عام على ضرورة حماية الأطفال، والحيلولة دون دخولهم إلى المواقع الإباحية، والحد من الجريمة على الشبكة أياً كان نوعها، وخاصة في الدول الإسلامية.

وعلى الرغم من عدم وجود تسجيل دقيق لجرائم الحاسب على نطاق العالم، فتشير التقارير المتداولة والمعلومات المتوفرة إلى أن جرائم الحاسب في تزايد مستمر.

فكما جاء في تقرير مركز شكاوى الإنترنت لعام ٢٠٠٨، أنه في الفترة من ١ يناير ٢٠٠٨ -- ٣١ ديسمبر ٢٠٠٨ ، كان هناك (٢٧٥٢٨٤) من الشكاوى التي وردت إلى (IC٣). الذي يشكل زيادة (٣٣,١ ٪) بالمقارنة مع عام ٢٠٠٧، الذي ظهرت به شكاوى عددها (٢٠٦٨٨٤). ومع تتبع هذه البيانات التي بدأت في عام ٢٠٠٠، وسجلت شكاوى عددها (١٦٨٣٨). ومنذ ذلك الحين، تضاعفت الشكاوى في كل عام وصولاً إلى عام ٢٠٠٤ ، عندما بلغت الشكاوى (٢٠٧٤٤٩). ومن عام ٢٠٠٤ حتى عام ٢٠٠٧، ظلت حول نفس النسبة . وفي عام ٢٠٠٨، كان هناك تصاعد من جديد إلى ما يقرب من (٧٥٠٠٠) شكوى التي شكلت ما مجموعه (٢٧٥٢٨٤). وقفزت في عام ٢٠٠٩م، إلى (٣٣٦،٦٥٥) غير أنها تراجعت في العام ٢٠١٠م إلى (٣٠٣،٨٠٩) شكاوى. ويوضح الرسم البياني الآتي في الشكل



شكل١٣-١: يوضح الزيادة المطّردة في عدد بلاغات جرائم الإنترنت وشكاواها

وتعد الزيادة في عدد جرائم الحاسب نتيجة طبيعية لاستخدام الحاسب في المجتمع الأمريكي على نطاق واسع وفي جميع المجالات. واختراع الحاسب مثلُه كغيره من الاختراعات، فتح الأبواب أمام مجرمين لسرقته، أو لاستخدامه في تسهيل القيام بجرائم أخرى. فالحاسب قد يكون أداة للهجوم عندما يستخدمه أحد الأشخاص ليسهل عليه ارتكاب بعض الجرائم التقليدية كالغش، باستخدام أحد البرامج لسرقة الأموال من حسابات المودعين مباشرة. أو خزن السجلات المتعلقة بتجارة المخدرات بدلاً عن الاعتماد على نظام الدفاتر القديمة.

وعلى الرغم من أن أجهزة الحاسب قد تكون في بعض الأحيان ثانوية في ارتكاب الجريمة، فهي مهمة جداً بالنسبة للجهات المعنية بتطبيق القانون لأنها تحوي أدلة على الجريمة.

ولقد أثارت الطرق المختلفة التي يستخدم بها المجرمون الحاسب نقاشاً فلسفياً بين المعنيين، بتطبيق القانون في الولايات المتحدة الأمريكية. فبعضهم يحاول إقناع الآخرين بأن جرائم الحاسب هي مجرد جرائم تقليدية يتم ارتكابها، بمعدات جديدة ذات تقنية عالية. ولكن آخرين يصرون على خلاف ذلك رافضين مساواة جرائم الحاسب بالجرائم التقليدية، انطلاقاً من أن مقاومتها تتطلب وجود أساليب مبتكرة لتطبيق القانون وإصدار قوانين جديدة خصيصا لمواجهة

سوء استغلال التقنيات الحديثة.

ففي عام ١٩٨٤، تبنى الكونغرس وجهة النظر الأخيرة، وسنَّ تشريعاً منفصلاً لمواجهة الجريمة في المجالات الإلكترونية. وبما أن بعض جرائم الحاسب وجدت أصلاً في التقنيات الحديثة، فيجب مقاومتها بقانون خاص. فمثلاً التخريب الواسع الذي يحدث بسبب إطلاق الفيروسات في شبكات الحاسب العالمية لا يمكن القضاء عليه أو الحد منه بطريقة فعالة من خلال الاعتماد على قانون عام لتشريعات مكافحة الجريمة. فهل كان من الممكن أن يحاكم مثل من حوكموا بسبب إطلاق الفيروسات، كروبرت موريس المسؤول عن إطلاق دودة موريس وتعطيل حوالي (٦٠٠٠) حاسب آلي على نطاق العالم، أو الهاكر الأعظم كيفن ميتنك، أو غيره من مرتكبي الجريمة على الإنترنت ما لم يكن الكونغرس قد أصدر قانون مكافحة الغش وسوء استخدام الحاسب؟

ولإعطاء صورة واضحة عن نوعية التشريعات والقوانين الخاصة بالإنترنت، وحجم الخطر الذي تواجهه، سنناقش هذا الموضوع على ضوء ما يجري في الولايات المتحدة الأمريكية بوصفها المؤسس لشبكة الإنترنت، وأكثر بلدان العالم استخداماً لتقنية المعلومات وأجهزة الحاسب وتعرضاً لجرائم هذه التقنية.

وإن جرائم الحاسب، سواء وصفت بأنها جرائم قديمة أو جديدة كلياً، فهي تتسبب في حدوث مشاكل لا حصر لها للجهات المعنية بتطبيق القانون، واحتواء الخطر على الصالح العام في الولايات المتحدة. وأصعب ما قد تواجهه الجهات المشرعة هو وضع التشريعات المتعلقة بنقل التقنية من شيء مادي إلى بيئة غير ملموسة كبيئة الإنترنت، وإلى صيغ إلكترونية غير محسوسة. فهل يمكن أن تخضع الجرائم التي ترتكب بواسطة أجهزة الحاسب على الشبكة للضوابط أو القوانين العادية المعمول بها؟

إن جرائم السرقة والأذى كانت في السابق لها حدود مادية، فاللص يمكنه في ليلة واحدة اقتحام عدة منازل، ولكنه لا يستطيع أن يأخذ إلا أشياء محدودة. ولكن في عصر المعلومات

والأجهزة والشبكات المرتبطة بالإنترنت لم تعد الحدود المادية لها وجود. فقد أصبح بإمكان المجرم الاستيلاء على المعلومات المخزونة، من أي جهاز حاسب مرتبط بشبكة يمكن الوصول إليها عن طريق الاتصال بالهاتف في أي مكان في العالم. ومن ثم، فإن كمية المعلومات المسروقة أو مقدار الضرر الذي يحدثه المهاجم بواسطة شيفرة برمجية ذكية لا يحد منه إلا سرعة الشبكة، ونوعية معدات الحاسب الخاصة بالمجرم. وبالطبع فإن هذه الجرائم والسرقات يمكن أن تحدث داخل أي بلد وعبر حدوده.

وفي واقع الأمر، إن الانتقال الواضح إلى بيئة غير مادية وبلا حدود، كشبكة الإنترنت، وزيادة تعرض المعلومات إلى خطر السرقة وتحويلها إلى صيغ إلكترونية، يجعل من الصعوبة بمكان مواجهة هذا الواقع اعتماداً على قوانين قديمة أعدت أساساً لحماية الممتلكات المادية فقط. والأمثلة على ذلك كثيرة، فالتشريع الخاص بنقل الممتلكات المسروقة بين الولايات الأمريكية، مثلاً:)البند رقم ٢٣١٤ من المادة ١٨ USA)، يتحدث عن البضائع والأدوات والتجارة، ومن ثم فهو كما وصفته عدة محاكم في ولايات مختلفة لا ينطبق على الممتلكات غير المادية. وبالطريقة ذاتها، فإن قانوناً مثل قانون الابتزاز الأمريكي مثلاً، والمعروف منذ فترة طويلة يجعل العنف المادي الذي يهدد الممتلكات غير قانوني. فالتهديد بتفجير قنبلة في مبنى مثلاً يقع تحت طائلة هذا القانون، ولكن التهديد بحذف ملف لم يكن أصلاً وارداً في تصور واضعي القانون.

ولمواجهة مشكلة جرائم الحاسب المتنامية في الولايات المتحدة ومختلف أنحاء العالم، فقد اتفقت آراء معظم الذين تناولوا هذه المسألة بالدراسة على منهجين للمواجهة. الأول: يقوم على مراجعة جميع القوانين المتعلقة بهذا الموضوع في الولايات المتحدة للتعرف على كل تشريع، يمكن أن يتأثر فعلياً باستخدام التقنيات الحديثة للحاسوب، وأنظمة المعلومات وتعديله بالصورة المناسبة. والثاني: هو تركيز التعديلات الأساسية على قانون مكافحة الخداع، وسوء استخدام الحاسب الناجم عن استخدام التقنيات الحديثة.

ولقد أقر المشرعون في الولايات المتحدة المنهج الثاني للمواجهة، وهو تركيز التعديلات

الأساسية على قانون مكافحة الخداع وسوء استخدام الحاسب لأسباب عديدة، منها: أن الولايات المتحدة قد استمرت تواجه المسائل الجوهرية لأمن المعلومات على المستويين المحلي والدولي بتشريع واحد يتعلق بالمحافظة على سرية المعلومات والأنظمة وسلامتها وتوفرها، لأن هذه الموضوعات (السرية، والسلامة، والتوفر) تُعدُ القاعدة الأساسية للتعاون والنمو الاقتصادي لأية منظمة، والموجّهَات الرئيسة لأمن المعلومات، حسب ما هو وارد في (مسودة المبادئ) الخاصة بتوفر المعلومات السرية واستخدامها (رقم ٤٣٦٢ بتاريخ ٢٠ يناير ١٩٩٥). ولذلك فإن الولايات المتحدة الأمريكية تكون من خلال تكييف قانون مكافحة أعمال الخداع وسوء استخدام الحاسب مع موجهات أمن أنظمة الحاسب، قد بدأت بإعادة التفكير في كيفية مواجهة جرائم تقنية المعلومات، وفي الوقت ذاته حماية السرية والمحافظة على سلامة المعلومات وأنظمتها وضمان توفرها.

إن تبني هذا الخيار من قبل الولايات المتحدة سيؤدي إلى تشجيع دول أخرى على اتباع أطر عمل مماثلة، ومن ثم إيجاد طريقة أكثر شمولاً واتساعاً لمواجهة خطر جرائم الحاسب والشبكات على البنية التحتية العالمية الحالية للمعلومات. وبذلك تكون الولايات المتحدة قد وفرت نقطة مرجعية واحدة للمحققين والمدعيين العامين والمشرعين، وهي المادة (٣٠) من قانون مكافحة الخداع وسوء استخدام الحاسب، ليستندوا عليها في تحديد ما إذا كان سوء استخدام معين للتقنية الجديدة يشمله، أو لا يشمله، قانون الجريمة الاتحادي.

وبما أن قانون الجريمة يتطلب إعادة نظر كلما دخلت تقنيات جديدة مجال الاستخدام، فإن عملية الموالفة الدقيقة للمادة (٣٠) من القانون قد تكون ملائمة جداً، بحيث لا يصبح من الضروري البحث المستمر في مدونة القوانين الأمريكية بكاملها.

إن هذا القانون سيوفر فهماً أفضل لحدود جريمة الحاسب والشبكات وأبعادها، ويتيح إمكانية الحصول على إحصائيات أكثر موثوقية فيما يتعلق بسوء استخدام الحاسب.

ويمكن أن تتم محاكمة جرائم الحاسب بموجب هذا القانون، وتحت تشريعات مكافحة

الجريمة المسمى (A Host Criminal Statute) ومن المحتمل جداً أن ينجح هذا الوضع في الحد من الجريمة إذا اعتمدت الولايات ا لمتحدة طريقة المزج بين القوانين، وقامت بتعديل الشروط المختلفة للمادة (١٨) لتشمل جرائم الحاسب الجديدة لأن وجود تفسيرات وتطبيقات مختلفة للقانون سيؤدي إلى تفاقم مشكلة موجودة أصلاً.

١٣-٢ مشكلة تأخر المحاكمات في جرائم الإنترنت

إن عقد المحاكم لمحاكمة المتهمين في جرائم الإنترنت يتأخر كثيراً بسبب تعقد نوعية القضايا، وقلة عدد الذين يتمتعون بخبرة في هذا المجال من القضاة وممثلي الاتهام، والأمثلة على ذلك كثيرة. فلقد استغرق الأمر أربع سنوات وخمسة أشهر لينتقل الهاكر المشهور (كيفن ميتنك) من مرحلة الاعتقال بتهمة الاحتيال، إلى مرحلة قضاء العقوبة. وقد تم ذلك دون محاكمة كافية. فهذا الهاكر الذي حُكم عليه بموجب هذه التهمة في اليوم الثامن من شهر آب/ أغسطس من عام ١٩٩٩بعقوبة سجن مدتها ستة وأربعون شهراً، والذي أطلق سراحه في بداية عام ٢٠٠٠، ليس هو الوحيد الذي عانى من هذه المسألة. فالهاكر كيفن بولسن، هو الآخر قد اعتقل في عام ١٩٩١، وظل محتجزاً في السجن لمدة تزيد عن العام ونصف العام، قبل أن توجه إليه وزارة العدل الأمريكية تهمة التجسس، التي رفضتها المحكمة مؤخراً. ولكنه في آخر الأمر أمضى خمس سنوات وشهرين دون محاكمة. وفي صفقة مع هيئة الاتهام اعترف بتهمة واحدة هي إجراء محادثة لاسلكية للفوز بسيارة بورش.

وقد كان التأخير الطويل في هاتين الحادثتين الشهيرتين بالرغم من عدم ارتباطهما ببعضهما يعزى جزئياً إلى وجود كميات هائلة من الأدلة المعقدة. وقد أثبتت دراسة حديثة أن عالم الجريمة ذات التقنية العالية يكون في كثير من الأحيان معقداً جداً إلى درجة يصعب على ممثلي الادعاء التعامل معه بصورة مناسبة، وهي حقيقة كانت نتيجتها القيام بعمليات تفتيش واعتقال وتعطيل غير لازم للمحاكمات.

وقد ذكر ديفيد بانيسار أحد العاملين في مركز (خصوصية المعلومات الإلكترونية) أنه: «لا يوجد كثير من المحامين الذين يتولون الدفاع في جرائم الحاسب، ولا المدعون العامون، أو ممثلو النيابة، الذين يتمتعون بالخبرة الواسعة في هذا المجال». ويقول أيضاً: «إنه في بعض الأحيان يكون الشخص الوحيد المؤهل لمناقشة هذه المسائل التقنية هو المتهم نفسه، والذي لن يصدقه أحد على كل حال».

١٣-٣ كثرة الاعتقال وقلة المحاكمات

وجد ديفيد بانيسار من خلال المعلومات التي حصل عليها من وزارة العدل الأمريكية بموجب حرية المعلومات، أن (٤١٩) قضية من قضايا الاحتيال بالحاسب قد أحيلت إلى المدعين العامين الاتحاديين بسبب نقص الأدلة. وهو وضع يدل على وجود مشكلة حقيقية فيما يتعلق بتطبيق القانون في هذا المجال.

وتدل الإحصائيات على أن معدل الاتهام قد ظل ثابتا منذ عام ١٩٩٣، على الرغم من

تضاعف عدد القضايا ثلاث مرات. ففي كل عام يتم استبعاد ما بين ٦٤٪ - ٧٨٪ من قضايا الاحتيال بالحاسب، أو إرسالها إلى الولايات للمقاضاة.

وهذا يعني أن الشرطة تحصل على ضمانات بحث للتحري في الجرائم المزعومة، والقيام بالاعتقالات اللازمة في قضايا أضعف من أن تتم المقاضاة فيها على المستوى الاتحادي. وقد ذكر بانيسار أنه: «كما يوجد العديد من الجرائم الأخرى، فهناك عدد كبير من المخالفات الفنية للقانون التي يجب إيقافها بطرق أخرى». ولكن ينبغي أخذ الأمر بالحجم المعقول، وعدم المبالغة فيه، وهو يعطي مثالاً على ذلك قائلاً: «إذا كان كل شخص يتجاوز السرعة القصوى المحددة في الساعة بميل واحد يتم توقيفه، فإن البلد لا محالة ستتحول إلى دولة بوليسية». وهو يدعو إلى إيجاد الحلول اللازمة لهذه المشكلة القانونية والتقنية في الوقت ذاته.

١٣-٤ حلول مقترحة

أول هذه الحلول لهذه المشكلة هو تثقيف الشرطة وممثلي الادعاء في المسائل التقنية الخاصة بهذا المجال، وهو أمر يتطلب في أحسن الأحوال كثيراً من الجهد والمثابرة. ومع ذلك فإن إدارة الرئيس كلينتون التي أصدرت سلسلة من الأوامر الإدارية، وقدمت كثيراً من الاقتراحات حول الجريمة على الإنترنت، اتهمها البعض بأنها تحاول تقليص الخصوصية على الشبكة حتى يتسنى لها تنفيذ قوانين يصعب حتى تطبيقها في العديد من الحالات. ففي السادس من شهر آب/ أغسطس من عام ١٩٩٩، وقّع الرئيس كلينتون أمراً تنفيذياً بتكوين مجموعة عمل بمستوى استشاري لتقرر ما إذا كانت القوانين الحالية كافية للبت في قضايا جرائم الإنترنت. وقد كلفت المجموعة أيضاً بالبحث في التقنيات والأساليب والسلطات القانونية الجديدة التي يمكن أن تساعد الشرطة في محاربة الجريمة على الشبكة. وقد قوبل الجزء الأخير من هذا الأمر التنفيذي

الذي أصدره الرئيس الأمريكي بسيل من الانتقادات، بدعوى أنه ذريعة مغلفة لعودة صكوك التنفيذ، وفتح باب خلفي لفرض تنفيذ القانون، للحصول على مفاتيح حل شيفرة ما يسمى ببرامج التشفير القوية.

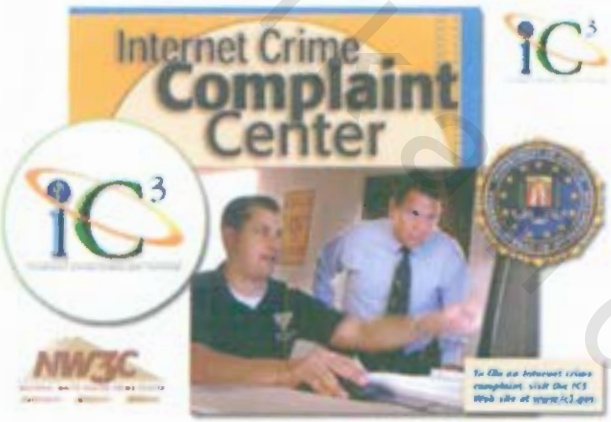
ومع ذلك فإن مسؤولاً إدارياً على صلة لصيقة بمجموعة العمل صرح بأن التشفير لن يدخل ضمن التحريات التي تقوم بها المجموعة، وأن الأمر يتعلق فقط باستخدام القوانين والأدوات الحالية بطرق جديدة. وهو يركز على الاعتماد على التنظيم الذاتي أكثر من إعطاء سلطات إضافية للشرطة.

وبالإضافة إلى محاولات إدارة الرئيس كلينتون إصدار قوانين تنفيذية جديدة، فإن وزارة العدل ومكتب التحقيقات الاتحادي (FBI) ووزارة الدفاع ووكالة الأمن الوطني تسعى جميعها إلى طلب زيادة في ميزانياتهم لمحاربة جرائم الإنترنت، ومواجهة حرب المعلومات، على الرغم من حقيقة أن أقل من ربع القضايا التي وصلت إلى السلطات الاتحادية قد تم إصدار أحكام فيها في نهاية الأمر، وهو ما تزعم الانتقادات الموجهة إلى ما تقوم به إدارة الرئيس كلينتون في هذا المجال بالإضافة إلى ما تسعى إليه هذه الوزارات والإدارات من انهماك في إنشاء إمبراطورية باستخدام تهديد مبطن باللجوء إلى إعداد برامج جديدة وبسط نفوذ إداراتها. وكان نائب وزير الدفاع جون هامري الذي وصف الهجوم الذي تعرض له مقر وزارة الدفاع الأمريكية في شهر فبراير من عام ١٩٩٨، بأنه أعنف هجوم قضائي واجهه المقر حتى الآن، قد استطاع إقناع الكونغرس بتخصيص مزيد من الأموال لمحاربة إرهاب الشبكة. وقد تم ذلك حتى بعد اكتشاف أن الهجمات قد قام بها ثلاثة مراهقين أحدهما إسرائيلي عمره ١٨ سنة، والآخران مراهقان من كاليفورنيا يستخدمان ثغرة معروفة على نطاق واسع في نظام تشغيل الحاسب. وهو شبيه بالوضع الذي يحدث الآن بخصوص فرض تنفيذ القوانين دون استخدام الإجراءات الوقائية الصحيحة، والخبرات المناسبة في مجال الحاسب. ولذلك فإن المسؤولين يستطيعون من خلال

استخدام المزيد من الأموال القيام بمزيد من الاعتقالات في مجال الجريمة المرتبطة بالإنترنت وأجهزة الحاسب.

ومع ذلك فإن العدد الفعلي للمحاكمات والإدانات حسب بيانات ديفيد بانيسار ستظل كما هي.

١٣- ٥ مركز الشكاوى الخاصة بجرائم الإنترنت (IC3)



إن مركز الشكاوى الخاصة بجرائم الإنترنت (IC3) هو كناية عن نظام تبليغ وإحالة شكاوى الناس في الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت. ويقدم المركز استمارة للشكاوى مرسلة على الإنترنت، ويقوم المركز بواسطة فريق من الموظفين والمحللين، بخدمة الجمهور ووكالات فرض تطبيق القوانين الأميركية والدولية التي تحقق في جرائم الإنترنت.

وقد نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة ١٩٩٨م، بإدراك أن الجريمة بدأت تدخل الإنترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الإنترنت.

ولم يكن هناك آنذاك أي مكان يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الإنترنت والنشاطات الإجرامية الأخرى التي تُبلّغ عنها عادةً الشرطة المحلية، ومكتب التحقيقات الفدرالي، والوكالات الأخرى التي تطبق القوانين الفدرالية، وهيئة التجارة الفدرالية (FTC)، والمكتب الأميركي للتفتيش البريدي (USPIS)، وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الأميركية، وغيرها من الوكالات.

وقد تم تأسيس أول مكتب للمركز سنة ١٩٩٩ بولاية وست فرجينيا، وسمّي مركز شكاوى الاحتيال على الإنترنت. ومثّل المكتب شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح متعاقدة مع وزارة العدل الأميركية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون، بهدف اكتشاف جرائم الإنترنت أو الجرائم الاقتصادية ومعالجة أمرها.

وفي العام ٢٠٠٢، وبغية توضيح نطاق جرائم الإنترنت التي يجري تحليلها، بدءاً من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الإنترنت، وأعيدت تسمية المركز فأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الإنترنت، ودعا مكتب التحقيقات الفدرالي وكالات فدرالية أخرى، مثل: مكتب التفتيش البريدي، وهيئة التجارة الفدرالية، والشرطة السرية، وغيرها، للمساعدة في تزويد المركز بالموظفين، وللإسهام في العمل ضد جرائم الإنترنت.

وقد أصبح هناك اليوم في مركز الشكاوى القائم بولاية وست فرجينيا، ستة موظفين فدراليين وما يقرب من أربعين محللاً من القطاع الأكاديمي، وقطاع صناعة الكمبيوتر، وخدمات الإنترنت، يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في الشكاوى، وإعداد ملفها، وإحالتها إلى وكالات تطبيق القانون الفدرالية والمحلية والتابعة للولايات، وإلى أجهزة تطبيق القانون الدولية، أو الوكالات التنظيمية، وفرق العمل التي تشارك

فيها عدة وكالات، للقيام بالتحقيق فيها.

ويمكن للناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم على الإنترنت (gov.http://www.ic٣). ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه؛ إضافة إلى اسم، وعنوان، ورقم هاتف، والعنوان الإلكتروني- إذا كانت متوفرة- للشخص، أو المنظمة، المشتبه بقيامه بنشاط إجرامي؛ علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب اعتقاده بوقوعها؛ بالإضافة إلى أي معلومات أخرى تدعم الشكوى.

وكما جاء في موقع الحكومة الأمريكي www.america.gov/ar أن مركز الشكاوى الخاصة بجرائم الإنترنت، يعمل أيضاً مع منظمات دولية، مثل: هيئة الجرائم الاقتصادية والمالية (EFCC) في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال، والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال ٤١٩، مما كانت له عواقب سلبية شديدة على ذلك البلد.

وتجمع جريمة احتيال ٤١٩، التي أطلق عليها اسمها لخرقها الفقرة ٤١٩ من مدونة القوانين الجنائية النيجيرية، ما بين جرم انتحال الشخصية وتشكيلة متنوعة من مؤامرات قبض الأموال مسبقاً لمشاريع وهمية. فالضحية المحتملة تتلقى رسالة، أو رسالة إلكترونية، أو فاكس، من أشخاص يدعون أنهم موظفون حكوميون نيجيريون أو أجانب، يطلبون فيها المساعدة في إيداع مبالغ طائلة من المال في حسابات في مصارف خارجية، عارضين حصة من الأموال مقابل ذلك. ويعتمد المخطط على إقناع الضحية الراغبة في التعاون بإرسال مبلغ من المال إلى كاتب الرسالة على دفعات لأسباب متنوعة.

وقد أدى خطر هذه الجرائم في نيجيريا إلى تأسيس لجنة الجرائم الاقتصادية والمالية هناك. وخلال السنة الماضية، قام مركز الشكاوى الخاصة بجرائم الإنترنت بعدة عمليات جديدة صودرت فيها بضائع، وتم إلقاء القبض على أشخاص في أفريقيا الغربية، نتيجة لهذا التحالف بين

المركز ولجنة الجرائم الاقتصادية والمالية، ونتيجة لتحالفات أخرى.

ويعمل مركز الشكاوى عن كثب أيضاً مع المنظمة الكندية المسماة؛)الإبلاغ عن الجرائم الاقتصادية على خط الإنترنت) (RECOL) . ويدير هذه المنظمة المركز القومي للجرائم المكتبية في كندا، وتدعمها شرطة الخيالة الملكية الكندية، ووكالات أخرى. وتنطوي منظمة الإبلاغ عن جرائم الإنترنت على شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفدرالية والإقليمية من جهة، وبين المسؤولين عن وضع أنظمة العمل وتطبيقها، والمنظمات التجارية الخاصة التي لها مصلحة تحقيقية مشروعة في تلقي شكاوى الجرائم الاقتصادية، من جهة أخرى.

وهناك مجموعة متنامية من الوكالات الدولية المنخرطة في محاربة جرائم الإنترنت. ويعمل مركز الشكاوى الخاصة بجرائم الإنترنت مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها أستراليا والمملكة المتحدة. كما يحضر ممثلو مركز الشكاوى أيضاً اجتماعات دورية للمجموعة الفرعية حول جرائم التقانة المتقدمة التابعة لمجموعة الثماني (كندا، وفرنسا، وألمانيا، وإيطاليا، واليابان، وروسيا، والمملكة المتحدة، والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية على محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها.

ويشكل مشروعا مركز الشكاوى الخاصة بجرائم الإنترنت (IC3)، ووحدة مبادرات جرائم الإنترنت ودمج مواردها (CIRFU)، فريق عمل متطور ومتقدم باستمرار. وفي أثناء هذا التقدم، يراجع موظفو ومحللو مركز الشكاوى ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادر التي تزودهم بمعلومات استخباراتية، ليصبحوا أكثر فطنة بخصوص جرائم الإنترنت، ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية.

١٣-٦ المركز الوطني الإرشادي لأمن المعلومات

يعمل المركز الوطني الإرشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات، على رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات ويقوم بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية. ومن ضمن أهداف المركز أيضاً؛ رفع مستوى الثقة في التعاملات الإلكترونية، فضلاً عن تقديم المشورة والنصح للأفراد وللمؤسسات في ما يتعلق بأمن المعلومات.

شكل ١٣-٢ المركز الوطني الإرشادي لأمن المعلومات

١٣-٧ مركز التميز لأمن المعلومات

قامت وزارة التعليم العالي بإنشاء وتمويل مركز التميز لأمن المعلومات بجامعة الملك سعود، بهدف جمع أفضل الباحثين و المتميزين في أمن المعلومات لنقل الخبرة وتوجيه الأبحاث في هذا المجال، لتقييم وحل المشاكل الوطنية في أمن المعلومات. ويهدف المركز إلى الاستثمار في الخبرات الوطنية من خلال التعاون الدولي والداخلي مع الجامعات ومراكز الأبحاث و الشركات لحل المشاكل المختصة بأمن المعلومات ونقل الخبرات وتقديم برامج تعليمية وتثقيفة متميزة ومبدعة تشجع على التخصص في أمن المعلومات وتحذر من المخاطر الأمنية. انظر شكل ١٣-٣ مركز التميز لأمن المعلومات.

شكل ١٣-٣ مركز التميز لأمن المعلومات

١٣-٨ كرسي سمو الأمير مقرن لتقنيات لأمن المعلومات

مع التواصل والعولمة المعلوماتية المتصاعدة عبر الإنترنت، باتت قضية (أمن المعلومات) أولوية رئيسة لحماية الأمن الوطني والعالمي في هذا العصر.ومن هذا المنطلق جاءت مُبادرة صاحب السمو الملكي الأمير مقرن بن عبد العزيز، بتمويل كرسي بحثي في مجال (تقنيات أمن المعلومات) في جامعة الملك سعود. ويطمح الكرسي إلى أن تكون نشاطاته متفاعلة مع مُتطلبات تقنيات أمن المعلومات على المستوى الوطني من جهة، ومع التطور العلمي الذي يشهده العالم في مجالاتها من جهة أخرى ويهدف إلى تحقيق إنجازات في البحث العلمي، وتطوير منتجات تقنية تختص بأمن المعلومات، إضافة إلى تقديم الاستشارات المتخصصة بواسطة عدد من الخبراء المحليين والدوليين.

شكل ١٣-٤ كرسي الأمير مقرن لتقنيات لأمن المعلومات.

١٣-٩ نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية

أثبتت الإحصائيات تصدر المملكة العربية السعودية المركز الأول على مستوى دول الخليج العربي في التعرض للجرائم الإلكترونية وذلك وفقاً لما ذكرته شركة (ترينـد مايكرو) إلى وجود أكثر من (٧٠٠) ألف حالة انهيار نظامي خلال تسعة شهور فقط في السعودية بنسبة ٦٤٪.

مما أدى إلى اهتزاز الثقة بالتعامل الإلكتروني عبر الإنترنت مما يحتم وجود قانون مكافح لمثل هذه الجرائم. وعليه فإن مجلس الوزراء السعودي أقر في جلسته يوم الاثنين ٧ ربيع الأول ١٤٢٨هـ، برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز – حفظه الله – نظام مكافحة جرائم المعلوماتية، بتحديد الجرائم والعقوبات المقررة لها للحد من نشوءها. وتتجاوز مجموع العقوبات المالية الواردة في النظام مبلغ (١١) مليون ريال، موزعة بالتفاوت المبني على فداحة الجرم الالكتروني المرتكب.

١٣-٧-١ أبرز مواد نظام مكافحة الجرائم الإلكترونية :

المادة الثالثة:

في هذه المادة يعاقب الشخص بالسجن لمدة سنة وبغرامة خمسمائة ألف ريال إذا ارتكب أحد الجرائم الآتية: كالتنصت والدخول غير المشروع من أجل الابتزاز والتخريب والمساس بالحياة الخاصة، وقد نصت هذه المادة على الآتي:

« يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمس مئة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظام صحيح أو التقاطه أو اعتراضه.

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.

٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة»

المادة الرابعة:

في هذه المادة يعاقب الشخص بالسجن لمدة ثلاث سنوات وبغرامة مليوني ريال إذا ارتكب أحد الجرائم الآتية: كالاستيلاء على مال منقول أو على سند والوصول دون مسوغ إلى بيانات بنكية أو ائتمانية، وقد نصت هذه المادة بالآتي:

« يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

٢-الوصول دون مسوغ نظام صحيح . إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات»

المادة الخامسة:

في هذه المادة يعاقب الشخص بالسجن لمدة أربع سنوات وبغرامة ثلاثة ملايين ريال إذا ارتكب أحد الجرائم الآتية: كالدخول غير المشروع لإلغاء أو إتلاف بيانات خاصة، وإيقاف الشبكة المعلوماتية عن العمل وإعاقة الوصول إلى الخدمة، وقد نصت هذه المادة بالآتي:

«يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

١-الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها أو إتلافها أو تغييرها، أو إعادة نشرها.

٢-إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدميرها، أو مسح البرامج أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

٣-إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت».

المادة السادسة:

في هذه المادة يعاقب الشخص بالسجن لمدة خمس سنوات وبغرامة ثلاثة ملايين ريال إذا ارتكب أحد الجرائم الآتية:إنتاج ما فيه المساس بالنظام العام أو القيم الدينية وإنشاء مواقع للاتجار في الجنس البشري أو المخدرات، وقد نصت هذه المادة بالآتي:

«يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله،أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.

٢-إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس لبشري، أو تسهيل التعامل به.

٣-إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة، و نشرها، أو ترويجها.

٤-إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار لمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها، أو تسهيل التعامل به».

المادة السابعة:

في هذه المادة يعاقب الشخص بالسجن لمدة عشر سنوات وبغرامة خمس ملايين ريال إذا ارتكب أحد الجرائم الآتية: كإنشاء موقع لمنظمات إرهابية أو الدخول غير المشروع لغرض الحصول على معلومات أمنية، وقد نصت هذه المادة بالآتي:

«يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

١-إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات أو أي من أعضائها، أو ترويج أفكارها أو تمويلها. أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

٢-الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني».