المقصود بجرائم تقنية المعلومات: يقصد بجرائم تقنية المعلومات كل فعل غير مشروع يرد على الكمبيوتر أو يتم باستعماله. كما يعرفها البعض بأنها كل نشاط إجرامي يؤدي فيه النظام دوراً لإتمامه أو يقع على النظام نفسه. صور الجرائم تقنية المعلومات: من النصوص الخاصة التي تورد تحريما لحماية تقنية المعلومات تلك التي تعاقب على الدخول في النظام بدون وجه حق، وتجريم الإخلال بسير النظام، وتحريم إتلاف البيانات أو العبث بها، التنصت أي انتهاك سرية البيانات المبرمجة والتبادلات والمراسلات الإلكترونية. صور الدخول غير المشروع في النظام السعودي الصورة الأولى ـ الدخول غير المشروع بقصد التهديد أو الابتزاز. الصورة الثانية ـ الدخول بقصد العبث بالبيانات المبرمجة. الصورة الثالثة الدخول غير المشروع للحصول على بيانات تمس الأمن القومي أو الصورة الرابعة ـ الدخول غير المشروع بقصد العبث بالموقع. تجريم الدخول إلى النظام بشكل غير مشروع نعالج في هذا المطلب التعريف بالدخول غير المشروع وأهمية تحريمه الفرع الأول) وتحريم مجرد الدخول غير المشروع وصوره الفرع الثاني). التعريف بالدخول غير المشروع وأهمية تجريمه عرف نظام مكافحة جرائم المعلوماتية في المملكة الدخول غير المشروع في المادة الأولى منه بقوله "الدخول غير المشروع دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها". (المادة الأولى، فالدخول إذن هو فعل المخترق الهاكر" الذي يستعمل عادة برامج تمكنهم من الدخول إلى أنظمة غير الخاصة من على بعد. غير أن الدخول يشمل كل استعمال للحاسب الآلي دون رضاء صاحب الحق فيه، أيا كانت صورة ذلك الاستعمال، ويلاحظ أن تجريم الدخول في النظام يشكل تجريماً غير مسبوق حيث هو تحريم معنوي. فالفاعل لا يقوم بالدخول إلى النظام بالكسر أو باستعمال مفاتيح مصطنعة، و لم يشترط النظام السعودي أن يكون النظام محميا بكلمة السر، معاقب عليه حتى ولو لم يهتم صاحبه بوضع كلمة المرور عليه لكي يحميه من تطفل الآخرين. وعلى الرغم من أن النظام المشار إليه قد جرم الدخول غير المشروع في نظام حاسب آلي أو موقع إلكتروني أو شبكة، فإنه لم يجرم مجرد الدخول، غاية معينة، أي استلزم توافر نية معينة وهو ما نسميه بالقصد الخاص. ضرورة حماية المعلومات داخل الكمبيوتر بشكل أكبر عن المعلومات الورقية أصبح من الضروري تحقيق حماية جزائية أوسع وأكبر للمعلومات المبرمجة من الحماية المقررة للمعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات لأهميته في آن واحد. فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية. هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام. كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد. كل هذه الاعتبارات دعت منظمي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها، النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية. ويرجع السبب في تلك الحماية الخاصة إلى أن من يدخل نظام الكمبيوتر غالبا ما يكون قد أخل بحرمة المكان دون أن يقوم بدخول مادي في هذا المكان في حالات كثيرة. يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير، الأمر الذي لا يتوافر في حالة الملفات الورقية التقليدية. طبيعة الجريمة الدخول جريمة نشاط تقع جريمة الدخول غير المصرح به بمجرد إتيان النشاط المؤثم، وهو هنا الدخول في النظام بعد الدخول فيه بطريقة عرضية وغير مقصودة. وللتعرف على طبيعة جريمة الدخول غير المشروع إلى نظامي الكمبيوتر يقتضي التعرف على موقف التشريعات المقارنة المجرمة لهذه الصورة الإجرامية. يمكن القول من خلال الاطلاع على التشريعات المقارنة أنها تباينت فيما بينها، ويمكن التمييز بين اتجاهين أشارت إليها بوضوح المادة الثانية من اتفاقية بودابست ٢٠٠١ بشأن مكافحة جرائم الفضاء المعلوماتي وعنوانها جريمة النفاذ أو الولوج أو الدخول غير المشروع " سوف يتبنى كل طرف تدابير تشريعية وغيرها من التدابير حيثما كان ذلك لازماً لاعتبار الدخول إلى كل جزء من نظام. الحاسب دون وجه حق جريمة مؤثمة طبقاً لقانون الداخلي إذا ما ارتكبت عمداً، فالأصل أن جريمة الدخول إلى النظام جريمة نشاط وليست جريمة ضرر في غالبية الأنظمة المقارنة مادام أنه لا يلزم لوقوعها تحقق ضرر من نوع معين، ومؤدى ما سبق أن الجريمة تقع عند الدخول إلى النظام، أما محاولة الدخول إلى النظام بطريق غير مشروع وهو عمل الهاكر" الذي يحاول تخمين كلمة المرور وقد لا ينجح، تجريم مجرد الدخول غير المشروع وصوره ـ تحريم مجرد الدخول في التشريعات المقارنة: تعاقب غالبية التشريعات المقارنة الحديثة على الدخول في نظام الحاسوب. غير أن موقف التشريعات الحديثة تتباين في تحريم الدخول غير المصرح به من هذه التشريعات ما يقيد تحريم الدخول بقيد يتعلق بالركن المعنوي، القومي أو الاقتصاد الوطني للعقاب على هذا الدخول أو قصد التهديد أو الابتزاز. يوضح هذا التجريم ضرورة استحداث نصوص خاصة لحماية المعلومات داخل الحاسوب فقد استشعر المشرع في دول عديدة الحاجة إلى إدخال تشريعات جديدة تحمي المعلومات داخل نظام الحاسوب نظرا لقصور القواعد التقليدية في قانون

العقوبات عن حماية هذا النظام. من هذه النصوص ما يجرم مجرد التداخل في نظام الحاسوب، ومنها ما يجرم إتلاف المعلومات المبرمجة، ومنها ما يجرم تغيير هذه المعلومات. وسوف نقوم بعرض سياسة النظام السعودي لمكافحة جرائم تقنية المعلومات.
صور الدخول غير المشروع في النظام السعودي: من صور الدخول غير المشروع المعاقب عليها وفقا للنظام في المملكة هي: الصورة الأولى الدخول غير المشروع بقصد التهديد أو الابتزاز: تعاقب المادة الثالثة من النظام على هذه الصورة من صور الدخول غير المشروع بقولها: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا. وبالتالي فإن النظام السعودي لا يعاقب في هذا النص على التهديد أو الابتزاز، ولكن الدخول بقصد التهديد أو الابتزاز، بمعنى أنه لا يشترط أن يكون المتهم قد قام بالتهديد أو الابتزاز بالفعل. وقد عرفت المادة الأولى من النظام السعودي المقصود بالموقع بنصها على أنه مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد". في ذلك تنص المادة الثالثة على أنه يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: . ٣- الدخول غير المشروع إلى موقع إلكتروني، لتغيير تصاميم هذا الموقع أو إتلافه، أو تعديله، أو شغل عنوانه". وبالمثل فإن التجريم يتوافر ويحق توقيع عقوبة كاملة على الفاعل حتى ولو لم يتمكن من العبث بالموقع، مادام أن نيته من وراء الدخول غير المشروع هو الوصول إلى تحقيق تلك الغاية. أركان جريمة الدخول غير المشروع تتمثل أركان جريمة الدخول غير المشروع في النظام من ركنين؛ ركن مادي وركن معنوي. وسوف نتناول بالتفصيل هذين الركنيين في فرعين متتاليين؛ الركن المادي في جريمة الدخول غير المشروع يتمثل الركن المادي في جريمة الدخول بدون وجه حق في القيام بصورة واحدة من النشاط وهي الدخول غير المشروع، فلم يختر النظام السعودي صورة أخرى تعرفها التشريعات المقارنة وهي صورة البقاء غير المصرح به، وهي جريمة من يكون من حقه أن يدخل إلى نظام معين لمدة معينة، ولكنه يستمر بعد المدة المصرح له به، وهو ما يحدث من بعض الموظفين الذين يعملون في جهات معينة ومن حقهم أن يستخدموا أجهزة حاسوب تلك الجهات في فترات معينة، ولكنهم يسيئون استخدامها في غير تلك الأوقات. ويقصد بالدخول الاتصال بجهاز حاسب آلي خاص بشخص الغير بدون موافقته. ويتخذ الدخول صورا مختلفة فمنها أن يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات. ما يقوم به صاحب الجهاز أو ينتقل بين أجزاء الجهاز ليطلع على ما يحتويه أقسام هذا الجهاز من غير أن الدخول لا يلزم فيه أن يقوم الفاعل بالاطلاع على ملفات صاحب الجهاز أو على ما يقوم به من أعمال، من الدخول عن بعد بالنظام، حتى ولو كانت الملفات محمية بكلمة المرور ولم يتمكن من فتحها. وقد استعمل نظام مكافحة جرائم المعلوماتية تعبير "الدخول غير المشروع" ويقصد به الدخول بدون وجه حق. وبالتالي فإنه لا يعد دخولا غير مشروع إذا توافر رضاء صاحب النظام كأن يكون هناك اتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة وبالتالي فالجهازان متصلان بالشبكة ذاتها مما يفيد توافر الرضاء الضمني بدخول العاملين على الجهاز الخادم للشبكة إلى الأجهزة المنتمية إلى ذات الشبكة من التطبيقات على ذلك شبكة جامعة حائل حيث تهيمن على أجهزة العاملين بها الموجودة في مكاتب كليات الجامعة وإداراتها ومراكزها المختلفة. ولما كانت تلك الأجهزة تنتمي إلى العمل أي أنها من أدوات العمل، فإنه ليس لأصاحبها الحق في الحياة الخاصة أي أن من حق العاملين على الجهاز الخادم المهيمن على تلك الشبكة والمتواجد في إدارة الجامعة أن يدخل إلى تلك الأجهزة وأن يطلع على الملفات الموجودة بها. كما لا يعد من قبيل الدخول غير المشروع أن يتم ذلك من جهة عامة لها الحق في مراقبة أجهزة الحاسب الآلي المتواجدة لدى الأفراد مادام أن النظام يسمح لتلك الجهات بممارسة الحق في المراقبة، المخلة بالآداب أو جرائم الماسة بأمن الدولة. ويتصور الشروع في الدخول غير المشروع، وقد عاقب عليه نظام مكافحة جرائم المعلوماتية في المملكة بنص المادة العاشرة التي تعاقب على الشروع في الجرائم المنصوص عليها في هذا النظام ومنها جريمة الدخول بدون وجه حق. والحقيقة أنه يمكن تصور الشروع في الدخول إذا حاول الجاني استعمال أكثر من كلمة مرور مثلا، ولكنه فشل في الوصول إلى الكلمة الصحيحة. الركن المعنوي في جريمة التداخل غير المشروع تنتمي هذه الجريمة إلى الجرائم العمدية وبالتالي فإنه يلزم توافر القصد الجنائي من علم وإرادة وبالتالي لو حدث الدخول بطريق الخطأ فإن الجريمة لا تقوم. ولم يكتف النظام السعودي بتطلب القصد الجنائي العام من علم وإرادة، بل استلزم توافر القصد الجنائي الخاص الذي يتمثل في ضرورة توافر نية من نوع خاص وهو قصد الجاني من الدخول غير المشروع أن يكون بغرض التهديد أو الابتزاز أو بغرض الحصول على بيانات تمس أمن الدولة من جهة الداخل أو الخارج أو تمس الاقتصاد الوطني أو يكون غرضه أن يعبث بالنظام أو بالبيانات التي يحتويها أو يكون غرضه تغيير تصاميم موقع إلكتروني، أو إتلافه، أو تعديله، أو

شغل عنوانه. ومؤدى ما سبق أن الدخول بدون وجه حق في حد ذاته لا يعتبره النظام في المملكة جريمة معاقبا عليها. فليس مجرد استعمال برامج للتداخل (هاكر) يجعل الفعل معاقبا عليه. ومع ذلك فإن النظام السعودي يعاقب على التجسس على النظام، فمن يتداخل في جهاز غيره ويطلع فقط على ما يقوم به دون أن يكون لديه قصد خاص معين من القصود سابقة الذكر قصد التهديد أو الابتزاز، قصد العبث بالنظام أو البيانات الموجودة فيه أو قصد الإتلاف، قصد الحصول على بيانات تمس أمن الدولة أو الاقتصاد الوطني لا يرتكب جريمة التداخل، ولكنه يرتكب جريمة التنصت (مادة ٣-١ من نظام مكافحة جرائم المعلوماتية). الأساس النظامي لتجريم العبث بالنظام أو بالبيانات أورد النظام السعودي لسنة ١٤٢٨ هـ (٢٠٠٧) م. ) جريمة العبث بالنظام في شكل إيقاف عمله، أو تعطيله، أو تدميره، أو مسح البرامج وكذلك تشمل الجريمة العبث بالبيانات وذلك في شكل إتلافها أو تعديلها أو تسريبها، وذلك بنصه في المادة الخامسة بنصه: "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين، شخص يرتكب أيا من الجرائم المعلوماتية الآتية: ـ إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير أو مسح البرامج، الموجودة أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها . إعاقة الوصول إلى الخدمة، أو تشويشها أو تعطيلها، بأي وسيلة كانت. المقصود بالعبث بالنظام أو البيانات: يقصد بالعبث بالبيانات المبرمجة إدخال بيانات غير مصرح بها في النظام أو تعديل بيانات موجودة أو إلغاء هذه البيانات. فتنص المادة ٣٢٣ـ٣ـ من قانون العقوبات الفرنسي عل عقاب كل من أدخل بسوء نية بيانات في نظام معالجة البيانات او قام بسوء نية بإلغاء أو تعديل هذه البيانات بالحبس مدة لا تزيد على ثلاث سنوات حبس والغرامة التي لا تزيد على ٣٠٠ ألف فرنك. يبين مما سبق أن تلك الجريمة تقوم على ركنين ركن مادي، وركن معنوي. يتكون الركن المادي من نشاط، ونتيجة، وعلاقة سببية، ضرر وليست مجرد جريمة خطر كجريمة الدخول. والعبرة ليس بطريقة معينة اتبعها الجاني، وسيلة يحقق بها غاية معينة، إدخال بيانات غير مصرح بها. وبناء عليه فإن الركن المادي في هذه الجريمة يقوم على تعديل المحتوى المادي للبيانات وقد حددها النظام ضمن عدد معين من الأضرار منها يغزو بها spam أن يتوصل الجاني إلى إيقاف الشبكة المعلوماتية عن العمل من أمثلة ذلك أن يقوم الفاعل بإرسال إعلانات تجارية موقع الشركة بحيث لا يتمكن من استقبال طلبات الزبائن. تريد أن تضر بسير العمل في الشركة صاحبة تلك الأجهزة. ومن التطبيقات القضائية على جريمة إدخال بيانات غير مصرح بها ما قامت به المتهمة التي كانت تعمل في إحدى الشركات، وذلك قبل تركها العمل في تلك الشركة من إدخال بيانات غير صحيحة تتعلق بمعدل احتساب الضريبة على القيم المنقولة. وقد أدى ذلك إلى إرباك العمل بما كانت تزمع الشركة القيام به من أعمال المحاسبة داخل الشركة. كما يمكن أن يقع النشاط المعاقب عليه بأن يستعمل الجاني فيروسات وهي برامج الغرض منها تدمير أو مسح المعلومات، بيد أن الجريمة لا تقع بمجرد زرع الفيروس، ولكن بتحقيق نتيجة مادية معينة وهي التدمير أو المسح للمعلومات أو اضطراب في سير النظام بحيث لا يعمل على الوجه المعتاد الصحيح، إلى إتلاف النظام أو مسح المعلومات. ومن صور النشاط المعاقب عليه أن يقوم الفاعل بإعاقة النظام من التطبيقات على ذلك أن أحد المتهمين كان يعمل مستخدما في إحدى الشركات وقد استغنت عنه تلك الشركة ولما كان عالما بكلمة المرور لشبكتها قام بالدخول إليه وتغيير تلك الكلمة ولما كان العاملون فيها لا يعرفون كلمة المرور الجديدة، وتكبدت الشبكة خسائر فادحة من جراء ذلك ومن جراء تغيير الشبكة بعد ذلك. ولكن ماذا لو قام المتهم بالدخول بوجه حق لأنه من الذين لهم حق الدخول كما لو كان مستخدما في إحدى الشركات وقام بإضافة بيانات إلى ما يوجد فيه من بيانات؟ نرى أنه يمكن أن تدخل تلك الصورة في المادة الخامسة) تحت كلمة "تعديل" الواردة فيها. ونظرا لخطورة برامج الاختراق فإنه كان من المناسب أن يعاقب النظام في المملكة عن حيازة أو استعمال تلك البرامج أو الاتجار فيها أو في كلمات المرور التي تقوم بعض العصابات بنشر إعلانات عنها مفادها أنه يمكنهم أن يخترقوا أي نظام نظير دفع مبلغ معين ويعلمون الناس على ذلك. وتختلف جريمة العبث بالنظام أو بالبيانات عن جريمة الدخول بقصد العبث بالنظام أو بالبيانات في الركن المادي في كلتا الجريمتين؛ ففي الجريمة الأولى لا تقع الجريمة إلا بتحقق نتيجة معينة وهو الضرر المتمثل في العبث بالنظام بينما تقع الجريمة الثانية بمجرد التداخل إذا كان قصد المتداخل هو العبث بالنظام أو بالبيانات ولو لم يتمكن من تحقيق غايته في إلحاق الضرر بهذا النظام أو بتلك البيانات. وواضح من اتجاه النظام السعودي أنه يتمشى مع الاتجاه الحديث في ضرورة إيجاد نص خاص للعقاب على إتلاف البيانات وعدم ترك الأمر للقواعد العامة التي يختلف فيها الرأي حول ما إذا كان التجريم الخاص بالإتلاف الموجود في كثير من التشريعات يسري على البيانات مثلها في ذلك مثل غيرها من المنقولات أي هل البيانات والبرامج هي من قبيل المنقولات التي يحميها تحريم إتلاف المنقولات؟ وقد أحسن المنظم السعودي إذن بإيراده نص خاص للعقاب على إتلاف وحذف البيانات وقد أحسن المنظم السعودي صنعا أيضاً عندما

أدخل هذا النوع من التجريم لكي يحمي البيانات المبرمجة. فهذه البيانات قد تم برمجتها في الكمبيوتر حتى تحل محل البيانات المكتوبة في الملفات الورقية في شكلها التقليدي. ومن المعروف أن هذه الملفات تصلح أن تكون محررات مادام أنه يمكن التمسك بها في ترتيب آثار قانونية. عندئذ يعتبر العبث بها مشكلا الجريمة التزوير في أوراق عرفية أو في أوراق رسمية، بحسب ما إذا تعلق الأمر بمحررات رسمية أو بمحررات عرفية. بيد أنه يلاحظ أن بعض الأوراق الموجودة بالملفات الورقية لا تشكل محررات لأنها لا تصح للاحتجاج بها، وإنما أعدت للاستعمال الداخلي. في هذه الحالة لا يكون التعديل فيها مشكلاً لجريمة التزوير في المحررات. عندئذ لا يبقى سوى جريمة الإتلاف إذا وصل هذا التعديل إلى درجة إتلاف المستند. وهنا تظهر أهمية جريمة العبث بالبيانات المبرمجة. فهي تحقق للبيانات داخل الكمبيوتر حماية أكثر من تلك التي توفرها القواعد العامة في تزوير المحررات للمحررات الورقية. القيمة ولو لم تكن من شأنها أن ترتب آثار قانونية وندرس في هذا المبحث الأساس القانوني لتجريم التنصت على النظام في مطلب أول) وأركان تلك الجريمة في مطلب ثان). الأساس النظامي لتجريم التنصت على النظام يعاقب النظام السعودي في شأن مكافحة جرائم المعلوماتية على التجسس على النظام بنصه يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ أركان جريمة التنصت على النظام جريمة التنصت على النظام لها ركنان؛ ركن مادي وركن معنوي على ما سيلي توضيحه؛ الركن المادي لجريمة التنصت على النظام جريمة التنصت على النظام جريمة نشاط وليست جريمة نتيجة، مما هو منصوص عليه في المادة الثالثة من نظام مكافحة جرائم المعلوماتية وهو التنصت أو الالتقاط أو الاعتراض. وعلى الرغم من أن النظام سابق الذكر لم يعرف المقصود بالتجسس، إلا أنه عرف الالتقاط بأنه "مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح" (المادة الأولى ـ ١٠). طريقة أخرى ودون مسوغ قانوني. ويلاحظ أن الصياغة بهذا الشكل لا تغطي إلا التجسس على النظام في أثناء تشغيله، ولا تسري في حالة التجسس على النظام الذي لا يعمل وذلك عن طريق الدخول إليه وتشغيله والاطلاع على محتويات الملفات التي بداخله. ولكن يبقى أن التداخل في حد ذاته يعاقب عليه النظام السعودي، الأمن القومي أو الاقتصاد الوطني أو نية العبث بالبيانات المبرمجة. وتمتد هذه الجريمة لتشمل انتهاك سرية المراسلات الإلكترونية. وهنا يتعين أن نبين الحدود الفاصلة بين المراسلات الخاصة والمراسلات العامة على شبكة الإنترنت. فهناك الايميل وهناك الماسنجر وهي أماكن خاصة، وذلك على عكس المواقع التي يسمح للغير بالدخول إليها، الدخول في مقابل سداد رسم معين أو اشتراك معين. وهنا نؤكد على ضعف الطابع الخاص للمراسلات بطريق البريد الإلكتروني، وضرورة إقامة التماثل بين المراسلات الإلكترونية (الإيميل) والمراسلات البريدية. كما يجب إقامة التماثل بين المحادثات الفورية بطريق الماسنجر والمحادثات الهاتفية في ضرورة حمايتها بعقاب من يتنصت عليها، الأمر الذي فعله النظام السعودي الجديد. وقد أفرد النظام السعودي نصا خاصا للتجسس على بيانات البنوك بعقابه في المادة الرابعة على "الوصول ـ دون مسوغ نظامي صحيح إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال، أو ما تتيحه من خدمات". وتعاقب المادة الرابعة على ذلك بعقوبة السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين. الركن المعنوي لجريمة التنصت من الواضح أن جريمة التنصت جريمة عمدية فيها ينصرف القصد الجنائي للجاني إلى القيام بالتنصت على نظام أو جهاز الغير لمشاهدة البيانات التي بداخل جهازه أو التقاط ما يرسله جهازه من رسائل. وعلى الرغم من عدم النص صراحة على أن الجريمة عمدية، فإن طبيعة النشاط يقتضي ذلك، حيث إن المشاهدة أو الالتقاط الذي يحدث بطريقة عرضية دون قصد لا يكفي لتوافر صفة التنصت. ويكفي في القصد الجنائي العام من توافر العلم والإرادة؛ إرادة النشاط حيث إن الجريمة من جرائم الخطر، فلا يلزم توافر القصد الجنائي الخاص أي لا يلزم أن تنصرف نية الجاني إلى تحقيق مأرب معين من وراء التنصت؛ إنشاء موقع إرهابي على شبكة الإنترنت نتناول بالشرح في هذا المبحث الأساس النظامي لجريمة إنشاء موقع إرهابي على شبكة الإنترنت المطلب الأول وأركان تلك الجريمة المطلب الثاني). أولا ـ الأساس النظامي لجريمة إنشاء موقع على شبكة الإنترنت تصمن النظام لمكافحة جرائم المعلوماتية في المملكة جريمة جديدة وهي إنشاء موقع إرهابي على الإنترنت وذلك بنصه في المادة السابعة على أنه "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ ١ ـ 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 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، ثانيا ـ

أركان الجريمة: يتكون الركن المادي في تلك الجريمة من نشاط من اثنين؛ إما أن الجاني يقوم بإنشاء موقع إرهابي يدعو فيه إلى أفكار إرهابية أو يسهل الاتصال بالإرهابيين أو ينشر فيه كيفية تصنيع متفجرات أو أدوات تستخدم في الأعمال الإرهابية، وإما أنه يقوم بالدخول إلى أجهزة تحتوي على معلومات تمس أمن الدولة الداخلي أو الخارجي أو اقتصادها. الجنائي، فإذا حدث ذلك الدخول بطريق الخطأ فإنه لا يكون معاقبا عليه. الاستيلاء بطريق الاحتيال على أموال الغير يعاقب النظام السعودي على جريمة الاستيلاء على أموال الغير وذلك باستعمال الكمبيوتر، وقد اشترطت المادة الرابعة من النظام للعقاب على هذه الجريمة ركنا ماديا وركنا معنويا؛ الركن المادي في جريمة الاستيلاء على أموال الغير يتمثل الركن المادي في هذه الجريمة في الاستيلاء الفعلي على أموال الغير، إذن فهذه الجريمة من نوع الجرائم ذات النتيجة المادية وهي وقوع الضرر. فتنص على ذلك المادة الرابعة بقولها الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند. ". ولا يشترط أن يستولي الجاني لنفسه على المال،" ويشترط أن يكون المال منقولا بصريح نص المادة الرابعة من النظام، فلا تقع الجريمة بالاستيلاء على العقار، ولكنها تقع بالاستيلاء على سندات ملكية هذا العقار. غير أنه لا يشترط أن يكون هذا المال مبالغ نقدية، حق على سند بدون وجه حق. وقد اشترطت المادة السابقة استعمال وسيلة معينة في هذا الاستيلاء وهو أن يقع هذا الاستيلاء عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة. وهذه هي أساليب الاحتيال في جريمة النصب. وبناء عليه فإن النظام السعودي يعاقب على الاستيلاء على أموال الغير بطريق الاحتيال (النصب) في مجال جرائم المعلوماتية.