جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي ومنظومات المعلومات الإلكترونية

د.عطية عبد السلام الفيتوري
محاضر بكلية القانون – جامعة عمر المختار

مقدمة:

الدخول غير المشروع يشكل تجريماً غير مسبوق في تشريعات أغلب دول العالم، فالتشريعات الجنائية والمدنية ذهبت على تجريم الدخول إلى مسكن بدون رضاء صاحبه أو الدخول إلى عقار للاستيلاء على حيازته ضد إرادة صاحبه، أما ما نحن بصدده فهو تجريم معنوي وليس مادى، فالفاعل لا يقوم بالدخول إلى النظام بالكسر أو التلف أو الحريق أو استعمال مفاتيح مصطنعة، بل يتم ذلك من على بُعد باستعمال العديد من البرامج الالكترونية "برامج الهاكر" بفعل الدخول غير المشروع إلى الأجهزة والمنظومات الالكترونية بطريقة عمدية أو غير عمدية إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها. [1]

وأهتمت الدول الأوربية بتجريم الدخول غير المشروع لأنه يشكل تهديداً للأنظمة المعلوماتية [2] ، ونصت تشريعاتها على تجريم فعل الدخول إلى الأنظمة المعلوماتية كدولة السويد التي أسمته قانون البيانات السويدي سنة (1973) والذى أشتمل على جرائم الدخول غير المشروع على البيانات، والدنمارك سنة (1985) والتي نصت في قانونها الجنائي على جرائم الحاسب الآلي بفعل الدخول غير المشروع سواء بالتزوير أو بالتلاعب غير المشروع أو الاتلاف أو التغيير، ودولة فرنسا والتي أهتمت اهتماما ملحوظاً في النص على تجريم فعل الدخول غير المشروع منذ سنة (1988) وبريطانيا منذ سنة (1981) وهولندا والمجر وبولندا.

---

[1] للمزيد حول مفاهيم عامة لجريمة الدخول غير المشروع راجع:-

- جريمة الدخول غير المشروع في تشريعات الجرائم الالكترونية العربية – دراسة مقارنة – المجلة القانونية والقضائية – العدد الأول، السنة العاشرة – يوليو – 2016 – مبحث منشور في مجلة الوطن على الموقع-www.al watan.com – 2017.5.2.

[2] القرارات التي تم أتخاذها في أوربا حول هذه الجريمة ومن أمثلتها:-

Such as the European parlian ent and council directive 98/84 on the legal protection of services based on, and consisting of, conditional access, the European parliament and council directive 2001/29 on the harmonization of certain aspects of copyright and related rights in the information society the proposal for a council framework decision on attacks against information system con (2002) 173 final.

وأنظر أيضاً:-

Rico calleja, conditional access piracy, computer and telecommunications law review, 2003-9-8 p.239-240.

أما الولايات المتحدة الأمريكية فقد شرعت قانوناً خاصاً لأنظمة الحاسب الآلي فمنذ سنة (1985) نصت على تجريم الاستخدام غير المشروع عن بعد. إن انتشار مثل هذه الجرائم في الآونة الأخيرة وبشكل سريع دعى التشريعات الجنائية إلى النص على تجريمها سواء بإضافتها إلى تشريعاتها القائمة أو بسن تشريعات جديدة أو تعديلها، وذلك نظراً لخطورتها على الدول بصفة عامة لا سيما الشركات والقطاعات الاقتصادية الكبرى وكذلك خطورتها على أنظمة الدولة بصفة عامة، كون التشريعات التقليدية لم تنص عليها، مما سبب فراغاً تشريعياً واضحاً مما أصبح يشكل عبء على كاهل الدول بعد انتشار الجرائم الالكترونية بصفة عامة، خاصة مع استخدام شبكة المعلومات.

أهمية البحث:-

تقع أهمية البحث كونه يبحث في أهم وأخطر الجرائم في الآونة الأخيرة والمتعلقة بالجرائم الالكترونية، الأمر الذى يتطلب تناول بحثه بشكل تفصيلي والوقوف على أهم الأفعال التي تقع به جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية مع بيان التشريعات التي تناولت هذه الجريمة بنص خاص، مع دراسة التشريعات القائمة وهل هي كافية لسد مثل هذه الجرائم من عدمه، والتي خلت تشريعاتنا في ليبيا من مثل هذه الجرائم الالكترونية. ونظراً لأهمية وخطورة مثل هذه الجرائم ففي تاريخ 2017.5.12 تعرض العالم لهجوم الكرتوني كبير نتج عنه تعرض العديد من الأجهزة والمنظومات للدخول غير المشروع لأكثر من 100 دولة بطريقة متعمدة، فقد ذكرت وزارة الداخلية البريطانية أنه وقع عطل بالنظام الصحي في بريطانيا، فقد تأثرت (45) منشأة صحية في بريطانيا واسكتلندا لبرامج خبيثة استخدمت في الهجوم الإلكتروني والذى يمنع المستخدمين من الدخول إلى ملفات على حواسيبهم.[3] وتأثرت روسيا بهذا الهجوم حيث تأثر حوالى ألف جهاز كمبيوتر بذلك، ونظراً لأهمية الجريمة ذكر مركز الجريمة الالكترونية في شرطة الاتحاد الأوربي (يوروبول) أنه يعمل عن كثب مع محققين في الدول وفى شركات أمنية خاصة للتغلب على التهديد ومساعدة ضحاياه وقال في بيان "أن مسئول ذلك الهجوم الحديث غير مسبوق ويتطلب تحقيقاً دولياً معقداً للتعرف على مرتكبيه"، فيتطلب الأمر دراسة هذه الجريمة من جميع جوانبها سواء فعل الدخول المجرد أو المرتبط بغرض ما والوصول إلى حماية جنائية فعالة للحد من هذه الجرائم، وكذلك حتى يتمكن مشرعنا في ليبيا في النص على مثل هذه الجريمة نظراً لخطورتها. [4]

---

[3] موقع الحرية https://www.alhurra.com

بتاريخ 13 مايو 2017

وتسبب الهجوم عن اختراق الكترونى نجم عنه تحويل حالات الطوارئ والغاء جميع العمليات الجراحية غير العاجلة وكذلك عدم قدرة المستشفيات على استخدام هواتفها وأجهزة الحاسوب.

[4] د. أسامة عبدالله جايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، 1988، ص 86 وما بعدها.

إشكالية البحث:- تقع إشكالية البحث كونه يبحث في جريمة حديثة نصت أغلب التشريعات عليها أما بشكل منفصل أو بالتعديل والإضافة لتشريعات قائمة كما أن البحث في جريمة الدخول غير المشروع يتطلب تحديد الأفعال المادية التي تقوم عليها الجريمة بشكل دقيق خاصةً إذا علمنا بأن الأفعال التي تقوم عليها مثل هذه الجرائم قابلة للزيادة نظراً لاستحداث العديد من الأنظمة المعلوماتية وشبكات الانترنت وكيفية الدخول والالغاء والحذف والتعديل. إن جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي ومنظومات المعلومات الالكترونية يتطلب الوقوف على كل ما هو جديد ومطوّر في عالم المعلومات الالكترونية لتحديد الأفعال المادية المجرمة والتي تقع بها هذه الجريمة وتحديد صورها، إلا أن الخوض في مثل هذه الجرائم والبحث فيها يسهل النص عليها في التشريعات الجنائية سواء بنص خاص أو بالتعديل والاضافة في التشريعات الجنائية القائمة.

خطة البحث:- عليه سنقسم هذا البحث إلى مبحثين نتناول في الأول ماهية جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي ومنظومات المعلومات الإلكترونية وركنها المادي أما الثاني سنخصصه للركن المعنوي لجريمة دخول غير المشروع ووسائل مكافحتها.

المبحث الأول: ماهية جريمة الدخول غير المشروع وركنها المادي:

المطلب الأول: ماهية جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي:

لعبت التجارة الالكترونية وأنظمة الدول المتعددة دوراً هائلاً جداً في تطور الاقتصاد العالمي وسياسات الدول بصفة عامة والاقتصاد الوطني بصفة خاصة والتوسع في أنظمة الدول الإلكترونية، فلا يمكن انكار مثلاً أن التجارة الالكترونية عملت وبشكل كبير جداً على سرعة انتقال المعاملات ورؤوس الأموال، وألغت ما كان يعوقها قديماً من الحواجز الجغرافية التي كانت تحد كثيراً من حركتها وكذلك قلة المعلومات التي كانت تعتبر في الماضي الحاجز الأكبر في اجتياز اقتصاد العديد من الدول في العبور للعالمية، إلا أنه ومن جهة أخرى فإن هذا التقدم الكبير في الجانب المعلوماتي والإلكتروني أصبح من السهل الدخول إليه وعبوره لتنفيذ عديد الجرائم كالتهديد والاتلاف والأضرار باقتصاد الدول وكلك الأفراد أو التعديل أو الالغاء، فالمجتمع الأوربي شعر بخطورة مثل هذه الجرائم [5] إذ من المعروف أن أكثر

---

[5] أنظر للطرق القانونية الجديدة لدى:-

See for sone new forensic techniques, (peter sommer) evidence in internet paedophilio cases, computer and telecommunications law review, 2002, (8,7) 176-184.

وأنظر أيضاً اعتراف المنظمات الدولية بمثل هذه الجرائم الجديدة والتي ترتكب عبر الحدود الوطنية، وضرورة تناغم الحلول والحماية القانونية لها:- تاريخ الزيارة 2016.7.4 See in general www.oecd.org(منظمة التعاون الاقتصادي والتنمية)والاتحاد الأوربي: See http://europea.eu.int/indexen.htm
تاريخ الزيارة: 2016.7.4والانتربول ومجموعة الثماني الكبرى:

الجرائم الالكترونية التي يتم ارتكابها يكون الهدف الأساسي لها هو الحصول على المعلومات الالكترونية أو إتلافها أو تعديلها أو إلغاءها وهو نفس الشعور الذى كان يعكر صفو الولايات المتحدة الأمريكية في كثير من سياستها.

مثال ذلك: ما أعلنته شبكة أخبار (CNN) تحت عنوان طالب يسطو على المعهد الذى يدرس به، جاء فيه عام 1989 أن سلطات ولاية تكساس تحقق مع طالب يدعى (فيليب أوستين) قد سطا إلكترونياً على المعهد الذى يدرس به حيث أستخدم كمبيوتر في اقتحام والدخول في أنظمة أجهزة المعهد، حيث قام بسرقة بيانات خاصة بالضمان الاجتماعي وكذلك بيانات شخصية ومعلومات خاصة عن حوالى (55) ألف طالب وعضو هيئة تدريس بالمعهد، وقد قرر الطالب أنه لم تكن لديه أي نوايا إجرامية، وإنه لم يكن يخطط لاستخدام تلك البيانات في أي أنشطة إجرامية. [6]وللتعريف بهذه الجريمة يتعين الوقوف على التشريعات القانونية لعديد الدول لمعرفة مفهوم هذه الجريمة وطبيعتها القانونية. [7]

ففي سنة 1985 طبقت دولة كندا قوانين متخصصة في مجال التعامل مع جرائم الانترنت في قانونها الجنائي إذ عدلته في نفس السنة ليشمل قوانين خاصة لجرائم الحاسب الآلي والانترنت خاصةً جرائم الدخول غير المشروع على المعلومات الالكترونية، وقامت دولة الدنمارك في نفس العام بتعديل قانونها ليشمل قانون العقوبات فيها جرائم الحاسب الآلي وبالتحديد جرائم الدخول غير المشروع إلى الحاسب الآلي وفى ألمانيا تم تعديل القوانين الخاصة بها وأصبح للقاضي الجنائي الحق في إصدار أوامره بمراقبة

---

[6] كما أظهرت دراسات اجريت من قبل منظمة:-

(The computer srcurity institute)

سنة 1999 أن خسائر حوالى 163 شركة أمريكية من جرائم الحاسب الآلي والانترنت قد بلغت أكثر من 123 مليون دولار وزاد ذلك في عام 2000 بسبب جرائم الدخول غير المشروع والسرقة والغش والنصب المعلومات، أنظر التفصيل: منير محمد الجنبيهى، ممدوح محمد الجنبيهى، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص 18، أنظر أيضاً www.CNN.com، أنظر أيضاً Joseph. M. Oliven baum. Rethinking Federal Computer crime legislation, S.H.L.Rev, 1997, Vol, 27, P. 586.

[7] د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية -2003 2004 ص 329، وراجع أيضاً قضية الطالب Morris في نفس السنة في جامعة كورنل والذى تمكن من الدخول على 6200 جهاز حاسب بشكل متعمد، د. مدحت رمضان، مرجع سبق ذكره، ص 41، وقد ركزت توصيات التقرير الختامي للاجتماع التحضيري لغرب أسيا في بيروت 2004 على تعزيز التعاون وتبادل الخبرات بين الحكومات والقطاع الخاص لإنشاء آلية لمكافحة الجرائم المتعلقة بالكمبيوتر أنظر في ذلك:

See the final report of the west Asia preparatory meeting, April 2004, Beirut, A/CONF203/RPM4/L.2.

اتصالات الحاسب الآلي وتسجيلها والتعامل معها، ومنذ يناير 1978 أراد المشرع الفرنسي مواجهة الأجرام المعلوماتي ففي سنة 1988 أراد المشرع الفرنسي حماية أنظمة المعلومات، وتم الاتفاق فيما بعد بمجلس الشيوخ على أن ينص على الجرائم المعلوماتية في قانون العقوبات الجديد وأن صور التجريم بها تمتد لتشمل البيانات الأسمية وحماية أنظمة المعلومات وتخصص الكتاب الثالث من قانون العقوبات الجديد للجنايات والجنح التي تقع على الأموال وخصص الباب الثاني منه للجرائم الأخرى على الأموال، وخصص الفصل الثالث من هذا الباب لجرائم الاعتداء على أنظمة معالجة البيانات، فنص عليها في مواده 323-1 إلى 323-7 فنصت المادة 323-3 على معاقبة المتهم بالحبس لمدة ثلاثة سنوات وغرامة 300.000 ألف فرنك فرنسي على عملية إدخال بيانات بطريقة غير مشروعة فى نظام معالجة البيانات أو إلغاء أو تعديل البيانات التى يهتدى عليها النظام بطريقة غير مشروعة.

وبالتالي فإن المشرع الفرنسي أقام ثلاثة أنواع من الجرائم وهى الدخول العمدى غير المشروع على نظام لمعالجة البيانات، وإعاقة تشغيل النظام، وإدخال أو إلغاء بيانات في برنامج معالجة البيانات، وينصرف معنى مصطلح الدخول في إطار المعلوماتية ليشمل كافة الأفعال التي تسمى بالولوج في نظام معلوماتي ويتحقق الدخول غير المشروع إلى جهاز الكمبيوتر بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الكمبيوتر دون رضاء المسئول عن هذا النظام أو المعلومات التي يحتوى عليها، أو بمعنى أخر إساءة نظام الكمبيوتر عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله لاستخدامها في غرض ما. [8]، وفعل الدخول غير المشروع يعنى كذلك توجيه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرقة أو المساس بالسلامة أو المحتوى والتكاملية أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها.

ففي الولايات المتحدة الأمريكية صدر القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله سنة 1984 وعُدّل في أعوام 1986 – 1994 و 1996 وورد في الفصل (1030) منه نصوص خاصة تجرم الاعتداء على الكمبيوتر، ويعاقب في هذا الفصل على الأفعال التي من شأنها الدخول عمداً على جهاز كمبيوتر بدون تصريح أو يحصل متجاوزاً التصريح الممنوح له بأية وسيلة كانت على معلومات حددت حكومة الولايات المتحدة الأمريكية أنه لا يجوز الكشف عنها لأمور تتعلق بالدفاع الوطني أو العلاقات الخارجية أو أي بيانات سرية كتلك المتعلقة بالأمور المحددة بالفقرة (ى) من الفصل الثاني من

---

[8] د. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الطبعة الأولى، الدار الجامعية، 2007، ص 84 وأنظر أيضاً، الدخول غير المشروع على أنظمة المعلومات بحث منشور على الانترنت http://irbd.hooxs.com/t16012-topic 2016.5.4 ود. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة جامعة طنطا، 2001، ص 510.

قانون الطاقة النووية الصادر سنة 1954 [9] وأعتبر المشرع الأمريكي جريمة الدخول غير المشروع لقوانين 1984 و 1986 و 1996 نقطة البداية لأية جريمة معلوماتية أخرى. وقد عّرف المشرع السعودي تجريم الدخول إلى النظام في القانون الصادر سنة 2007 الخاص بمكافحة الجرائم المعلوماتية والتعاملات الالكترونية في مادته الأولى بقوله " الدخول غير المشروع دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع الكترونى أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"، ونصت المادة الثالثة فقرة 2 من نفس القانون على الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، والمادة الخامسة فقرة 1 نصت على أن الدخول غير المشروع قد يكون لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها، فالدخول غير المشروع قد يكون إلى موقع إلكترونى 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 [10] وذلك دائماً للأضرار بها. [11]ونص المشرع الأوربي على جريمة الدخول غير المشروع لموقع إلكترونى أو نظام معلوماتي وفق التشريع الأوربي وتحديداً وفق النصوص الواردة فى قانون جرائم أنظمة المعلومات لعام 2010، إذ نص على أن أساس هذه الجريمة هو الاستيلاء على المعلومات أو إتلافها عبر تقنية الفيروسات وغيرها من وسائل التدمير المعلوماتي من الاختراق المباشر للشبكات وأنظمة المعلومات والاتلاف والاضافة والتدمير والتعديل للبيانات والمعلومات، وإلى غيرها من الدول فقد تم تجريم الدخول غير المصرح به إلى نظام الحاسب الآلى وإن اختلفت فيما بينها من حيث الشروط المتطلبة لإعمال نصوصها، فالدخول غير المشروع وإن كان يتم بوسيلة منطقية وحيدة قوامها البحث والوصول إلى المعلومات باستخدام وسائل إلكترونية إلا أنه ينبغى تحديد مواصفات هذه الوسيلة والتى قد تتخذ شكل القيام بعملية دخول غير مشروع أو اعتراض

---

[9] أنظر فى ذلك بالتفصيل د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2012، ص 41 وما بعدها.

[10] The Recommendation No R(89)9 on computer – Related crine, Op.eit .. p.49-51.

[11] مثال ذلك الحالة التى تمكن فيها أحد الأشخاص من الدخول إلى نظام الحاسب الآلى الخاص بأحد المعامل الخاصة بتصنيع وتجبة الأسلحة النووية بكاليفورنيا بالولايات المتحدة الأمريكية، وقد تحمل المعمل خسائر مادية قدرت بحوالى مائة ألف دولار أمريكى وهى تكلفة الابحاث التى أجريت لمحاولة وقف هذا الدخول غير المصرح به،أنظر:
The law commission working paper No. 110 on computer misuse, C.L.S.R., may-June 1989-1990.

نظام الحاسب أو البقاء غير المشروع داخل النظام بعد عملية الدخول، كما ينبغى تحديد المحل الذى ينصب عليه فعل الدخول والذى قد يكون معلومة أو نظاماً للحاسب الآلى أو شبكة معلومات.[12] وأخيراً لم ينص مشرعنا الليبي على مثل هذه الجرائم فى جميع تشريعاته، رغم التطور الملحوظ فى مجال المنظومات الالكترونية على جميع التخصصات.

وأخيراً حسب رأينا فإن تعريف جريمة الدخول غير المشروع طبقاً لعديد القوانين تعنى " قيام شخص عمداً وبصفة غير مشروعة بالدخول على نظام معالجة البيانات سواء بالتعديل أو الالغاء أو إعاقة تشغيل النظام لا سيما إذا كان ذلك فى المعاملات الإدارية والإقتصادية والتجارية سواء للدولة أو على مستوى الأفراد".

أما عن تحديد الهدف الذى يعقب عملية الدخول فقد وجد خلافاً أظهرته النصوص القانونية المختلفة التى تناولت هذه الجريمة، وقد أسفر ذلك التساؤل حول مدى ملاءمة تدخل المشرع الجنائى للعقاب على الدخول المجرد إلى نظام الحاسب، فيرى المشرع الإنجليزى فى قانون 1990 أنه لا يمكن عقاب كل من يقرع على باب الحاسب الآلى، وإنما يجب أن يحاط التجريم بشروط محددة، أما المشرع الفرنسى فيذهب إلى أن هذه الجريمة تقوم بمجرد فعل الدخول بغض النظر عن النتيجة التى تعقب هذا الدخول، أما المشرع الأمريكى فذهب إلى أن جريمة الدخول غير المشروع هى الجريمة المعلوماتية الأساسية أماما يعقب بعدها من أفعال فهى لا تشكل سوى ظروف مشددة [13] إذاً فطبيعة هذه الجريمة هى شكلية تقع بمجرد أتيان النشاط وهو الدخول فى النظام سواء بطريقة مشروعة أو غير مشروعة، مقصودة أو غير مقصودة، ومع ذلك قد يترتب على جريمة الدخول إلى النظام أو البقاء فيه أضرارا بالمعطيات سواء بمحوها أو بتعديلها أو أفسادها ولكن هذا الضرر أو النتيجة التى تتحقق لا تغير من طبيعة الجريمة بأعتبارها جريمة شكلية، وإن كان هذا الضرر يمكن أن يشدد العقاب على الجانى وبالتالى تقع الجريمة ولو لم تكن لدى الجانى النية فى تحقيق نتيجة ما [14]، أما عن الشروع فى هذه الجريمة فهو يقع بمحاولة الدخول إلى النظام بطريقة غير مشروعة وذلك بمجرد (عمل الهاكر) الذى يحاول تخمين كلمة المرور.[15]

---

[12] أنظر فى ذلك د. نائلة عادل محمد فريد، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية، 2003، 2004، ص 330.

[13] المرجع السابق ص 330.

[14] د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، مرجع سبق ذكره، ص 150.

[15] فهو ما نص عليه المشرع السعودى فى مادته العاشرة فى القانون السابق ذكره بقوله (يعاقب كل من شرع فى القيام بأى من الجرائم المنصوص عليها فى هذا النظام كما لا يتجاوز نصف الحد الأعلى للعقوبه المقررة، وقررت المادة 7-323 من القانون الفرنسى على معاقبة الشروع فى ارتكاب هذه الجريمة بأفعالها المتعددة بالمواد 323-1 / 323-3 بذات العقوبات المقررة للجريمة التامة.

المطلب الثاني : الركن المادي لجريمة الدخول:

عملت اللجنة الأوربية بشأن مشاكل الجريمة ولجنة الخبراء في مجال جرائم الكمبيوتر على إعداد مشروع اتفاقية تتعلق بجرائم الكمبيوتر، وعليه أعلن المجلس الأوربي مشروع هذه الاتفاقية في 27 أبريل 2000. [16]ومن الأفعال التي اعتبرها هذا المشروع – و التي تشكل الركن المادي لهذه الجريمة – الالتقاط العمدى بأي وسيلة تقنية لأى نقل لبيانات كمبيوتر أو داخل نظام الكمبيوتر، أو أي إرسال كهرومغناطيسي من نظام للكمبيوتر يحمل هذه المعلومات (المادة 3 من المشروع) وكذلك الاتلاف والحذف والتعديل والالغاء والمسح العمدى لأى من البيانات ومن الجرائم الملحقة بجرائم الكمبيوتر تزييف برامج الكمبيوتر سواء بالإدخال أو التعديل أو التبديل أو المسح العمدى للبيانات لاستخدامها من الناحية القانونية كما لو كانت أصلية، ولا يشترط أن يكون في الامكان قراءة هذه البيانات أو أن تكون واضحة [17] وكذلك من الأفعال المادية لهذه الجريمة التسبب العمدى في فقد ملكية أي شخص آخر سواء بالإدخال أو التعديل أو الالغاء أو المسح لبيانات تخص الكمبيوتر وكذلك التدخل في عمل الكمبيوتر بقصد الحصول على أي فوائد اقتصادية لنفسه أو للغير، وللتوضيح أكثر حول فعل الركن المادي الذى تقع به هذه الجريمة يتعين النظر في التشريعات المقارنة للوقوف على مثل هذه الأفعال ومنها المشرع الأمريكي في تشريعاته المنصوص عليها سابقاً والذى عاقب على هذه الجريمة بمجرد الدخول عمداً على جهاز كمبيوتر بدون تصريح أو أن يحصل متجاوزاً التصريح الممنوح له بأي وسيلة كانت على معلومات حددت حكومة الولايات المتحدة الأمريكية أنه لا يجوز الكشف عنها، كما عاقب المشرع الأمريكي على من يدخل على جهاز للكمبيوتر يستخدم في التجارة أو الاتصال بين الولايات ويقوم عمداً بنقل لبرنامج أو معلومة أو كود لكمبيوتر أو نظام للكمبيوتر وعاقب أيضاً على منع الغير من استعمال الكمبيوتر أو النظام أو البيانات وكذلك العاقب على أي نقل لبرامج أو معلومات دون موافقة المسئولين على الكمبيوتر، أو أن هذا النقل أدى إلى خسائر لشخص أو أكثر تبلغ ألف دولار (1000) أو أكثر خلال فترة سنة أو تعديل أو إفساد كلى أو جزئي لكشف طبى أو علاج أو رعاية صحية[18]، وعاقب أيضاً على الغش في استعمال كلمات المرور بما يسمح بالدخول على نظام كمبيوتر دون تصريح إذا كان من شأن ذلك الأضرار بالتجارة.

---

(16) http://www.cybcrcrinc.gov/cocdraft.htm

(17) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، مرجع سبق ذكره، ص 39 .

(18) أنظر:

Olivenbaun (Joseph n.), Rethinking Federal computer crine legislation S.H.L.Rev., 1997, Vol. 27.P.586.

وتناول المشرع الفرنسى مجموعة من الأفعال التى تنطوى على تجريمه الدخول غير المشروع وذلك فى المواد 323-1 إلى 323-7 وعاقب على الدخول بطريق الغش أو التدليس على نظام للمعلومات أو تعديل البيانات الموجودة بالنظام أو تعديل تشغيل النظام وكذلك إعاقة أو التسبب فى تحريف أو تعديل تشغيل نظام معالجة البيانات، وأيضاً عملية أدخال بيانات بطريقة غير مشروعة فى نظام معالجة البيانات أو إلغاء أو تعديل البيانات التى يحتوى عليها النظام بطريقة غير مشروعة، وخرج المشرع الفرنسى على القواعد العامة حيث عاقب على الأعمال التحضيرية وذلك فى حالة المساهمة فى جماعة أو الاتفاق بين مجموعة من الأشخاص للتحضير بعمل أو أعمال مادية لارتكاب جريمة أو أكثر أو ارتكاب جريمة أو أكثر من الجرائم السابقة، وبرر ذلك رغبة المشرع الفرنسى فى تقرير نوع من الحماية الوقائية لنظم المعلومات من مخاطر الاعداد لمثل هذه الجرائم [19]، فالمشرع الفرنسى قام بتجريم الدخول العمدى غير المشروع على نظام لمعاجة البيانات وكذلك اعاقة تشغيل نظام البيانات وإدخال أو إلغاء بيانات فى برنامج معالجة البيانات، وقد توسع المشرع الفرنسى فى تحديد هذه الأفعال التى يتوافر بها الركن المادى لهذه الجريمة وسمح بتجريم استعمال أى وسيلة تقنية للدخول على نظام لمعالجة البيانات كالدخول عن طريق كلمة السر الحقيقية إذا لم يكن للجانى حق استخدامها، بأستخدام برنامج أو شفرة خاصة [20] ويستوى فى جميع الأحوال أن يكون الدخول مشروع أو غير مشروع أومباشرة أو غير مباشرة، وبأعتبار جريمة الدخول من الجرائم الوقتية فيستوى أن تقع من الخبراء أو الأفراد العاديين وتقع حتى لمجرد الفضول وحب الاستطلاع، [21]وتقع الجريمة تامة لمجرد الدخول غير المشروع ولو لم يتحقق ضرر أو تلاعب فى البيانات، أما البقاء داخل النظام فيفترضوا أختلاس وقت النظام ويتخذ صورة الجريمة المستمرة. [22]

---

[19] د. على عبد القادر القهوجى، الحماية الجنائية للبيانات المعالجة إلكترونياً بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الفترة من 1-3 مايو 2000، مجموعة أعمال المؤتمر جامعة الامارات العربية المتحدة – مشار إليه د. مدحت عبد الحليم رمضان، مرجع سبق ذكره، ص 47-48 .

[20] Alaw Bensouss An. Internet, Aspects Juridiques. Hernes, 1996, 1997, P. 108.

[21] Henri Aeterman, La Fraude Lnforma tlque, GP. 1988 Doct P.530.

فالدخول إلى المعلومات وأنظمة الحاسبات الآلية قد يتم بطريقة مباشرة عن طريق الحاسب الآلى الذى يحتوى على المعلومات والنظام وقد يكون غير مباشر عندما يدخل الفاعل إلى هذه المعلومات والأنظمة بواسطة نظام أخر يتصل بالأول بواسطة شبكة للأتصالات ويتم ذلك عن طريق اعتراض النظام الأول أو يتصل بالنوع الأول وهو الدخول المباشر عمليات الدخول غير المشروع التى تتم عن طريق العاملين بالمؤسسات (المجنى عليه) ويتصل بالنوع الثانى عمليات الدخول التى تم من الخارجين على هذه المؤسسات. د. نائلة عادل محمد، مرجع سبق ذكره، ص 332.

[22] د. جميل عبد الباقى الصغير، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن أستخدام الحاسب الآلى، 1992، دار النهضة العربية، ص 152 وما بعدها.

عليه فالتشريعات المقارنة نصت على الأفعال التى يقع بها الركن المادى لهذه الجريمة وهو الدخول غير المشروع، وإضافة بعض التشريعات منها صورة البقاء غير المصرح به وهى الدخول إلى نظام معين لمدة معينة ولكنه يستمر بعد المدة المصرح له به، ويأخذ صورة الموظف الذى يعمل لدى جهات معنية والتى من حقه أستخدام أجهزة كمبيوتر تلك الجهات فى ساعات محددة، ولكنه يسىء أستخدامها فى غير تلك الأوقات، وبالتالى فإن الدخول غير المشروع يأخذ صوراً عديدة ومختلفة الغرض منها الاطلاع على البيانات أو نقلها أو تعديلها أو إلغاءها وتقع كذلك بمجرد فتح الكمبيوتر او الدخول عن بعد بالنظام حتى ولو كانت هذه الملفات محمية بكلمة مرور ولم يتمكن من فتحها، ومن جهة أخرى لا يعتبر دخولاً غير مشروع إذا توافررضاء صاحب النظام كأن يكون هناك اتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة، ولا يعتبر دخولاً غير مشروع الجهة العامة التى لها الحق فى مراقبة أجهزة الكمبيوتر المتواجدة لدى الأفراد ما دام أن النظام يسمح لتلك الجهات بممارسة الحق فى المراقبة، وخاصة فى الحالات التى يسمح لها النظام لمكافحة جرائم الأداب والأرهاب والأمن الوطنى، ومن التشريعات العربية فى مكافحة هذه الجريمة ما قام بهالمشرع السعودى وفق نظام مكافحة جرائم المعلوماتية 2007 الذى نص فى مادته الثالثة فقرة 3 " على عقوبة السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بأحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الأتية:- 1- ..... 2- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

3. الدخول غير المشروع إلى موقع الكترونى، أو الدخول إلى موقع إلكترونى لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.

ونص فى المادة الرابعة فقرة 2 على أنه يعاقب بالسجن .... كل شخص يرتكب أياً من الجرائم المعلوماتية الأتية: 1.... ، 2- الدخول – دون مسوغ نظامى صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أو أوراق مالية للحصول على بيانات أو معلومات أو أموال أو نتيجة من خدمات، ونص فى مادته الخامسة على عقوبة السجن لكل شخص يرتكب أياً من الجرائم المعلوماتية الأتية:- " 1- الدخول غير المشروع لالغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها.

2- إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج والبيانات الموجودة وحذفها ...." ، ونص أيضاً فى مادته السابقة فقرة 2 على عقوبة السجن لمدة عشر سنوات وغرامة لكل شخص يرتكب الدخول غير المشروع إلى موقع الكترونى أو نظام معلوماتى مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلى للحصول على بيانات تمس الأمن الداخلى أو الخارجى أو الاقتصاد الوطنى، فالمشرع السعودى حدد وبشكل دقيق الصور التى تقع بها هذه الجرائم وعاقب أيضاً

على كل من حرض غيره أو ساعده أو أتفق معه على ارتكاب مثل هذه الجرائم (المادة الثامنة) ونص أيضاً على العقاب على من شرع فى القيام بإى من هذه الجرائم المنصوص عليها فى هذه النظام.

أما المشرع الانجليزى فقد أطلق قانون إعادة أستخدام الكمبيوتر فى أغسطس 1990 ووضع ثلاثة بنود فيه وهو البند الأول: الدخول المحظور على مواد الكمبيوتر وهذا النص حدد صور السلوك الأجرامى الذى تقوم به جريمة الدخول وهى إذا قام بفعل يؤثر على أى وظيفة بالنسبة لتأمين إدخال بيانات برنامج أو بيانات موجودة فى الكمبيوتر أو تعمد الدخول المحظور للكمبيوتر وإذا علم الشخص أنه حينما يقوم بهذه العملية أنه يرتكب جريمة، يُعد الشخص هذا مذنباً، أما الصورة الأخرى وهى أن تتجه نية الشخص الذى يرتكب جريمة تحت هذا البند إلى الاعتداء على أى برنامج أو بيانات محددة أو بيانات محددة النوع أو موجودة فى أى كمبيوتر محدد، أما البند الثانى فنص على الاشتراك فى جريمة الدخول المحظور والتسهيل فى استعمالها.

أما المشرع الاماراتى فنص لى القانون رقم 2 لسنة 2006 على جريمة اختراق المواقع والأنظمة الالكترونية وينتج عن ذلك إلغاء أو حذف أو تدمير معلومات أو ترتب عليها نتيجة متعلقة بانتهاك معلومات شخصية، أو فى حال القيام بالفعل أثناء أو بسبب العمل أو التسهيل للغير بالقيام بالفعل.

ونص القانون رقم 26 لسنة 2007 السورى المتعلق بالأحوال المدنية على الصور التى تقع بها هذه الجريمة فى مادته السابعة وهى التلاعب بالسجلات أو ضياعها أو تلفها، ونظم جريمة الدخول غير المصرح فى نظام السجل المدنى، وميز بين حالتين الأولى إذا كان الفاعل غير موظف فى وزارة الداخلية فإن الجريمة تقع بمجرد الدخول غير المصرح به إذا تبين أن القصد هو تعديل البيانات حذفاً أو إضافة أو تعديلاً أو تعديل البيانات، أما الثانية وهى إذا كان الفاعل موظفاً فى وزارة الداخلية شريطة أن يكون مخولاً بالدخول فى معلومات السجل المدنى، وعاقب المشرع السورى على الشروع بهذه الجرائم فى مادته 73 من القانون المشار إليه بعقوبة الفعل التام، [23] ونص قانون رقم 63 لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات الكويتى على صور السلوك الاجرامى التى يقع الركن المادى لهذه الجريمة فنص فى المادة الثانية من القانون على الدخول غير المشرع إلى جهاز حاسب آلى أو نظام معلوماتى وذلك إذا ترتب عليه إلغاء أو حذف أو تدمير أو تغيير اتلاف أى معلومات، وشدد العقوبة إذا كانت البيانات أو المعلومات شخصية [24]، ونص فى المادة الثالثة على صورة الدخول غير المشروع بقصد

---

[23] وصدرت العديد من القوانين فى هذا الاطار من المشرع السورى ومنها قانون حماية حقوق المؤلف رقم 12 لسنة 2001 وقانون التوقيع الالكترونى وخدمات الشبكة السورى رقم 4 لسنة 2009 وقانون الاعلام السورى رقم 26 الصادر بتاريخ 14-2-2011.

[24] وزارة الداخلية – دولة الكويت 30.5.2016

http://www.noi.gov.kw/portal/varabic/ecccd/aspx.

الحصول على بيانات أو معلومات وشدد العقوبة فى حالة ترتب على ذلك إلغاء تلك البيانات أو إتلافها أو تدميرها، [25] عليه يمكن النظر إلى التشريعات المختلفة التى جرمت الدخول غير المشروع إلى نظام الحاسب الآلى (الكمبيوتر) من عدة أوجه وذلك للوقوف أكثر على معرفة الركن المادى لهذه الجريمة من خلال ما هو محل الدخول وما هو فعل الدخول؟ أما عن محل الدخول فيتعين أستعراض السياسات التشريعية المختلفة فى تحديد المحل الذى يتخذه الركن المادى فى جريمة الدخول غير المشروع من خلال:

– الاتجاه الذى يجمع بين المعلومات وأنظمة الحاسبات وشبكة المعلومات (الاتجاه الموسع) وذلك لتشمل شبكة المعلومات ويشمل التجريم علميات الاعتراض غير المشروعة للاتصالات التى تتم من خلال الدخول إلى هذه الشبكات ويعد القانون الفرنسى مثالاً على هذا الاتجاه، ولقد أجمع الفقه الفرنسى من واقع الأعمال التحضيرية للقانون السابق ذكره على أن نظام المعالجة الآلية للمعلومات فى تطبيق المادة 321-1 ينصرف إلى المعلومات والنظام الذى يحتوى عليها وكذلك إلى شبكات المعلومات، ويؤدى هذا التوسع فى تعريف هذه النظم إلى نتيجة مؤداها أن التقاط الاشارات الناجمة عن تبادل المعلومات عبر شبكات المعلومات يعد دخولاً غير مشروع إلى نظام المعالجة الآلية الذى يحتوى على هذه المعلومات [26] وهذا ما ذهبت إليه الولايات المتحدة الأمريكية فى قانونها الفيدرالى فى المادة (1030).

ووفقاً لهذا التوسع فإن المحل الذى تنصب عليه جريمة الدخول غير المشروع يتسع ليشمل المعلومات وأنظمة الحاسبات الآلية وكذلك شبكة المعلومات [27] وتتميز تشريعات أخرى بكونها أكثر صراحةً فى الإشارة إلى شبكات المعلومات كمحل ينصب عليه النشاط الاجرامى فى جريمة الدخول كما فى قانون العقوبات اليونانى والنرويجى والفنلندى والدنماركى والكويتى والسعودى. [28]

– الاتجاه الذى يستبعد شبكات المعلومات من نطاق التجريم، ويعد القانون الانجليزى من أبرز الامثلة على هذا الاتجاه وفق قانونه الصادر سنة 1990 الذى عاقب على الدخول غير المشروع إلى البرامج والمعلومات التى يحتوى عليها أى حاسب آلى وقد تضمنت المادة 17 من القانون بعض التعريفات التى تساعد على تفسير نصوصه، إلا أنها لم تتضمن تعريفاً للحاسب الآلى أو البرامج أو المعلومات محل جريمة

---

[25] ونص المشرع الكويتى على عديد القوانين فى جانب حماية الأنظمة الالكترونية والمعلوماتية وهى القانون رقم 20 لسنة 2014 فى شأن المعاملات الالكترونية والقانون رقم 37 لسنة 2017 بإنشاء هيئة تنظيم الاتصالات

[26] Repport de Jacques Thydraud, Journal official de la République Francaise, documentation sénat, 1987-1988. 1''section, No3, P.51.

[27] وإن كان المشرع الأمريكى وضع ضوابط فيما يتعلق بالمعلومات والأنظمة التى يتم الدخول إليها أنظر فى ذلك:
Olivenbaun (joseph n.), Rethinking Federal Computer Crine Leglislation, S.H.L. Rev., 1997, Vol. 27, P. 586.

[28] د. نائلة عادل محمد فريد، مرجع سبق ذكره، ص 342.

الدخول ولم تتضمن المادة الأولى أية أشارة إلى شبكات المعلومات بل أقتصرت على البرامج والمعلومات التى يحتوى عليها الحاسب الآلى، ويترتب على ذلك استبعاد المعلومات التى يتم نقلها، وتطبيقاً لذلك وفى إطار التجارة الالكترونية قيام أحد العاملين السابقين بأحد المتاجر فى إنجلترا بزيارة زميله السابق فى العمل أثناء قيامه بشراء بعض المستلزمات من المتجر الذى كان يعمل به، وأثناء انشغال زميله قام المتهم بإدخال بعض التعليمات إلى نظام الحاسب الآلى يتم بمقتضاها خصم نسبة 70% من قيمة البضائع التى كان يريد شراءها، قُدم المتهم للمحاكمة بتهمة الدخول غير المشروع إلى نظام الكمبيوتر تطبيقاً للمادة الأولى من قانون إساءة أستخدام الحاسبات الآلية لعام 1990، إلا أن محكمة أول درجة برأت المتهم من التهمة المنسوبة إليه وجاء فى حكمها " أن العبارات الواردة بالمادة الأولى سالفة الذكر تتطلب أن يتم الدخول إلى الحاسب الآلى عن طريق حاسب آلى آخر حيث أن هذه المادة تتطلب الدخول غير المشروع إلى المعلومات والبرامج التى يحتوى عليها أى حاسب آلى وليس الحاسب الآلى الذى يستخدمه المتهم والا جاء نص المادة متضمناً تجريم الدخول إلى المعلومات والبرامج التى يحتوى عليها هذا الحاسب الآلى أو أى حاسب ألى آخر" إلا أن محكمة الاستئناف ألغت الحكم المتقدم، وجاء فى حيثيات حكمها أنه لا يجب تحميل عبارات النص أكثر مما تحتمل، حيث أن النص لم يحدد نطاق تطبيقه بضرورة أن يكون الدخول إلى الحاسب الآلى بواسطة حاسب آلى آخر، وإنما تقوم الجريمة بوجود حاسب آلى واحد هو المحل الذى ينصب عليه فعل الدخول". [29]

– أما تجريم الدخول غير المشروع إلى أنظمة الحاسبات الآلية عبر شبكة المعلومات، وهذا ما نص عليه التعديل الذى أدخله قانون العقوبات السويسرى سنة 1995 فى المادة 143 وذلك بمعاقبة على الدخول غير المشروع إلى أنظمة الحاسبات الألية بواسطة جهاز لنقل المعلومات، فالنص المتقدم لا يعالج سوى حالات الدخول التى تم عن طريق أشخاص خارج المؤسسات التى تحتوى على الأنظمة بواسطة شبكات الاتصالات العامة، وكذلك المادة 76 من قانون العقوبات الاسترالى الصادر سنة 1989 حيث تم تجريم الدخول غير المشروع إلى أنظمة الحاسبات الآلية التى لا تتبع الكومنولث بشرط أن يكون الدخول إليها قد تم بواسطة شبكات الاتصالات العامة.

– أما تجريم الدخول غير المشروع إلى أنظمة الحاسبات الآلية وشبكات المعلومات وتجريم اعتراض عملية نقل المعلومات بنصوص منفصلة تجرم كلا منهما على حده، وهذا ما ذهب إليه القانون البرتغالى رقم 109 لسنة 1991 الخاص بجرائم المعلوماتية.

– وتجريم الدخول غير المشروع إلى المعلومات التى يتم معالجتها آلياً ومنها القانون السويدى فى مادته 21 الصادر سنة 1973 والمعدل بالقانون رقم 1986 و 1990 فكل معلومة يتم تسجلها على أى

---

[29]) د. نائلة عادل محمد فريد، مرجع سبق ذكره، ص 337.

وسيط لتخزين المعلومات كالشرائط الممغنطة على سبيل المثال، والتى تشكل جزءاً من الحاسب الآلى ولا يمكن الوصول إليها إلا من خلال نظم المعالجة الآلية للمعلومات تعد محلاً يمكن أن ينصب عليه فعل الدخول غير المشروع [30].

وأخيراً تجريم الدخول إلى أحد الأجزاء التى يتكون منها نظام المعالجة الآلية للمعلومات، كالقانون الفنلندى الذى يُجرم صراحةً الدخول إلى أى جزء من الأجزاء التى يتكون منها نظام المعالجة الآلية للمعلومات، أما عن فعل الدخول فهو الذى ينطوى على نشاط ذهنى يقوم به الفاعل وليس نشاطاً مادياً محضاً، والأسئلة المطروحة حول فعل الدخول كثيرة ومتفرعة فهل يمكن تجريم الدخول بمجرد قراءة المعلومات على الشاشة دون أى نشاط سابق من الفاعل؟ وهل يكفى مجرد الدخول إلى نظام الحاسب لقيام الجريمة؟ وهل تقوم الجريمة بالبقاء غير المشروع داخل النظام؟ وهل يستوى الدخول إلى النظام واعتراضه لقيام الجريمة؟ وهل يشترط للعقاب على الدخول أن يتم اختراقاً للاجراءات الامنية التى تحمى النظام، أى هل يجب أن يتمتع النظام بهذه الحماية لتجريم الدخول إليه؟ سوف نحاول بأختصار الاجابة عن هذه الأسئلة من واقع التشريعات المختلفة، لا شك أن تحديد الشخص المسئول عن نظام الحاسب الآلى يسمح بتحديد الأشخاص الذين ينطبق عليهم وصف الدخول غير المشروع،ذلك أن الذى يملك حق الدخول إلى نظام الحاسب هو المسئول عنه أو من يحصل منه على ترخيص بهذا الدخول، أما ما عدا ذلك فهو غير مصرح له، وبناء على ذلك فهناك أشخاص داخل المؤسسة المسئولة عن النظام ينطبق عليهم بصفة عامة صفة الدخول غير المشروع، وكذلك أشخاص خارج المؤسسة المسئولة عن النظام، وهؤلاء يدخلون إلى نظام الحاسب أما مباشرة أو عن طريق أعتراض هذا النظام (غير مباشر) كما سبق أن بيناه، وللوقوف على ذلك نعرض تطبيقات قضائية لتوضيح ذلك، تعرض القضاء الانجليزى لحالة الدخول المشروع إلى نظام الحاسب الآلى لغرض غير مشروع وتتلخص وقائع القضية فى قيام شرطين بالدخول إلى نظام الحاسب الآلى الخاص بالإدارة التابعين لها للحصول على بعض المعلومات لأغراض لا تتعلق بعملها، وقُدما للمحاكمة بتهمة الدخول غير المشروع تطبيقاً للمادة الأولى من القانون الانجليزى وقد أدانت محكمة أول درجة المتهمين بتهمة الدخول، إلا أنهم طعنوا فى الحكم وألغت محكمة الاستئناف حكم محكمة أول درجة، وذهبت إلى أن المتهمين يملكان الحق فى الدخول إلى نظام الحاسب الآلى وأن أستخدام هذا الحق فى عرض غير مشروع لا ينفى أن الدخول مشروع. [31]

---

[30] أنظر:

Jareborg (Nils), Computer Crines and Other Against information technology in Sweden, (R.P.L., 1993, Vol. 64, pp. 587-588)

[31] مشار إليها د. نائلة عادل محمد، مرجع سبق ذكره، ص 343، وأنظر أيضاً :

والقضية الثانية تتعلق بطلب تقدمت به حكومة الولايات المتحدة الأمريكية إلى المملكة المتحدة لتسليم أحدى العاملات بشركة أمريكان إكسبريس لقيامها بالدخول إلى نظام الحاسب الآلى الخاص بالشركة للحصول على بعض البيانات الخاصة ببعض العملاء لأسباب تتعلق بالعمل، وقد ذهبت محكمة الاستئناف الانجليزية إلى أن الفعل الذى قامت به المتهمة لا يشكل جريمة وفقاً للقانون الانجليزى، حيث يشترط لانطباق المادة الأولى من قانون إساءة أستخدام الحاسبات الآلية الانجليزى السابق الإشارة إليه أن يكون الدخول غير مشروع وهو ما لم يتحقق فى هذه الحالة، وقد أنتقد الحكمان الاستئنافيان السابقان بشدة نظراً لتضييق نطاق تطبيق قانون إساءة أستخدام الحاسبات الآلية الانجليزى [32]، هذا من حيث الأشخاص أما عن مدى ضرورة وجود نشاط يسبق الدخول إلى نظام الحاسب الآلى، فقد تبيانت مواقف التشريعات منها، فقد اتجهت بعض التشريعات إلى استبعاد ما يسمى بالدخول الذهنى المحض كالقانون الانجليزى فمجرد قراءة المعطيات على الشاشة لا يكفى لتحقق الركن المادى للجريمة، كما استلزمت تشريعات أخرى أستخدام وسائل محددة لقيام الجريمة وهو ما يعنى ضرورة القيام بنشاط ما ومن هذه التشريعات قانون العقوبات الهولندى فهو يستلزم لقيام الجريمة أن يتم الدخول عن طريق مخالفة القواعد الأمنية أو استعمال وسائل تقنية أو استخدام شفرة غير صحيحة وكذلك قانون العقوبات السويسرى الذى يشترط جهاز لنقل المعلومات وكذلك وقانون العقوبات الكندى والفنلندى وعلى عكس من ذلك لم تتضمن تشريعات أخرى أية اشارة إلى طلب نشاط ما سابق عن فعل الدخول أو أى وسائل محددة كالقانون الفرنسى والبرتغالى والأمريكى وبعض التشريعات العربية السابق ذكرها، وأتجهت تشريعات أخرى إلى تجريم الدخول إلى المعطيات التى يحتوى عليها نظام الحاسب الآلى من معلومات وبرامج دون أن تشير إلى النظام ذاته كمحل للجريمة، وسيتخلص من هذا الاتجاه أنه يمكن العقاب على مجرد قراءة معلومات سرية على شاشة الحاسب الآلى دون أن يتطلب ذلك قيام الفاعل بالدخول إلى النظام لاحضار المعلومات كقانون العقوبات السويدى والدنماركى واليونانى.

أما عن الدخول المجرد إلى نظام الحاسب الآلى، فيرى البعض أنه ليس من الضرورى أن ينجح الفاعل فى الدخول إلى أى من المعلومات أو البرامج كى يتم النشاط الإجرامى فى هذه الجريمة، بل يكفى مجرد الدخول إلى نظام الحاسب الآلى وذلك أنه ولئن كانت العلة من تجريم الدخول غير المشروع هى حماية

---

[32] أنظر:

- R.V.Bow street magistate and Allison (AP), ex parte US government (1999) 3 WLR 620.

- Bainbridge (David), Introduction to computer law, Op. Cit., P. 312; Walden (Lan), Op. Cit., P. 286.

المعلومات من الوصول إليها والتلاعب بها، إلا أن هذه الجريمة هى من الجرائم التى تمثل عدواناً محتملاً على الحق وليست من الجرائم التى تتمثل فى تحقيق العدوان على الحق الذى يحميه القانون، وتأخذ أغلب النصوص القانونية التى تناولت جريمة الدخول غير المشروع إلى نظام الحاسب بهذا الرأى، وهو العقاب على فعل الدخول بمجرد أن يبدأ الفاعل بتشغيل الحاسب الآلى [33]، إلا أن هناك تشريعات أخرى تتطلب أن يتم الوصول إلى المعلومات التى يتضمنها النظام لقيام الجريمة ففى الولايات المتحدة الأمريكية تعاقب على فعل الدخول للحصول على معلومات محددة وكذلك فى التشريع الإسترالي.

وهذا ما يجعلنا ندخل فى تحديد الطبيعة القانونية لفعل الدخول وهل هو جريمة مادية أم جريمة شكلية بمعنى آخر هل يجب أن يكون هذا الدخول منتجاً لأثره أى أن يؤدى إلى تحقيق نتيجة إجرامية محددة وهى الوصول إلى المعلومات كما بينا سابقاً أم أن الجريمة تتم بمجرد الدخول، ويبدو أن الأفضل فى ذلك هو ما ذهب إليه قانون إساءة أستخدام الحاسبات الآلية فى إنجلترا سواء فيما يتعلق بتحديد أن فعل الدخول لا يتم إلا من خلال سلوك إيجابى يتمثل فى أى فعل من شأنه أن يتسبب فى أن يقوم الحاسب الآلى بأية وظيفة كانت أو فيما يتعلق بتحديد أن الدخول إنما يكون للحصول على المعلومات، فيجب أن يصل الفاعل إلى المعلومات المخزونة داخل الحاسب الآلى، فالحكمة من تجريم الدخول غير المشروع هى حماية المعلومات بمعناها الواسع، أما حماية النظام ذاته والحفاظ على حق المسئول عن النظام فى السيطرة عليه فيمكن تحقيقه بالعقاب على الشروع فى جريمة الدخول غير المشروع،[34] حيث يمكن فى هذه الحالة تجريم النشاط المتمثل فى تشغيل الحاسب إلى الدخول إلى النظام والمعلومات والبرامج التى يعتدى عليها دون أن يتمكن الفاعل من الوصول إلى هذه المعلومات لأسباب خارجه عن إرادته كما ذهبت إلى ذلك تشريعات عديدة كاالولايات المتحدة الأمريكية والبرتغال وفنلندا والسويد، بل أن الأخيرتين تعاقبا على الأعمال التحضيرية التى تسبق هذه الجريمة، أما عن البقاء غير المشروع داخل نظام الحاسب الآلى وهو المتمثل فى أن يجد الشخص نفسه داخل نظام لحاسب آلى غير مسموح له بالدخول إليه (الخطأ) أى يجد نفسه بسبب الخطأ – كاستخدام شفرة خاطئة مثلاً – داخل نظام آخر، وفى هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه للخطأ الذى وقع فيه وقد يستمر فى البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مسموح له بالدخول إليه، ومما لا شك فيه

---

[33] حيث يتم إرسال إشارة كهربائية نحو وحدة المعالجة المركزية – هى الوحدة المسئولة عن كل العمليات التى يجريها الحاسب الآلى والمسئوله عن تنفيذ البرامج الموضوعة لها بدقة – والتى تقوم بدورها بإرسال البرنامج المسئول عن تشغيل ذاكرة القراءة، د. نائلة عادل محمد، مرجع سبق ذكره ص 355 وهذا ما تتطلبه النصوص القانونية فى كل من فرنسا واليونان والبرتغال وفنلندا وهولندا.

[34] للمزيد حول الشروع فى الجرائم المعلوماتية راجع: خالد بن مرزوق بن سراج، الجوانب الإجرائية فى الشروع فى الجرائم المعلوماتية، دراسة مقارنة، مركز الدراسات العربية، القاهرة، 2014، ص 43 وما بعدها.

أن اتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مسموح له بالبقاء فيه لا يختلف فى جوهره عن الدخول غير المشروع فالنتيجة الاجرامية فى الحالتين واحدة وهى الوصول إلى نظام غير مسموح بالدخول إليه، فذهب المشرع الفرنسى على تجريمه البقاء غير المشروع داخل نظام الحاسب الآلى وتطبيقاً لذلك ذهبت محكمة استئناف باريس فى حكم لها صادر فى 5 أبريل 1994 إلى أن القانون يجرم البقاء غير المشروع داخل نظام الحاسب الآلى سواء كان الدخول قد تم عن طريق الخطأ أو تم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة عدم المشروعية، كما لو فقد الفاعل حقه فى البقاء نتيجة لخطأ من جانبه، ويذهب البعض إلى أن الاختلاف بين جريمة الدخول غير المشروع وجريمة البقاء داخل هذا النظام بعد دخوله عن طريق الخطأ يكمن فى أن الأولى جريمة إيجابية من ناحية ووقتية من ناحية أخرى، فى حين أن الثانية جريمة سلبية من ناحية ومستمرة من ناحية أخرى، لذا لا يمكن الجمع بينهما فى نص قانونى واحد نظراً لاختلاف الطبيعة القانونية لكل منهما، فكون البقاء داخل الحاسب الآلى جريمة مستمرة نظراً لاستمرار الاعتداء على المصلحة التى يحميها القانون كلما أستمر البقاء غير المشروع داخل نظام الكمبيوتر، كما أن الدخول غير المشروع يعد جريمة وقتية سواء كان الدخول غير المشروع مجرماً بمجرد الدخول أو بالدخول إلى المعلومات التى يحتوى عليها جهاز الحاسب، إلا أننا إذا كنا نتفق أن الدخول غير المشروع هو سلوك إيجابى فإننا لا نرى فى أن البقاء غير المشروع سلوك سلبى، فليس الامتناع عن الخروج من النظام الذى تم الدخول إليه هو مناط التجريم، بل البقاء داخل هذا النظام بعد الدخول إليه عن غير قصد مع العلم بأن هذا البقاء غير مسموح له به، وهو ما يشكل سلوكاً إيجابياً. [35]

ومع هذا كله يمكن حسب رأينا القول بأن جريمة الدخول غير المشروع هى جريمة متتابعة الأفعال حيث تقوم بأفعال متعددة يجمع بينها وحدة الحق المعتدى عليه ووحدة الغرض الاجرامى المستهدف بها، والذى يتطلب أيضاً لاشارة صراحة إلى جريمة البقاء غير المشروع داخل النظام صراحة سواء كانت جريمة الدخول تتم بمجرد الدخول إلى النظام أو تتم بالوصول إلى المعلومات والبرامج لما يشكله فعل البقاء من تهديد للمعلومات والنظام، [36]أما عن الأعتراض غير المشروع لنظام الحاسب الآلى يعد جريمة كونه يؤدى

---

[35] د. نائلة عادل محمد، مرجع سبق ذكره، ص 361 وأنظر أيضاً د. محمود نجيب حسنى شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازى، 1989 فقرة 309، ص 282 وأنظر أيضاً: د. محمد عبد اللطيف عبد العال، الجرائم المادية وطبيعة المسئولية الناشئة عنها، دار النهضة العربية، 1997، ص 74 وما بعدها.

[36] للأستزادة أنظر د. جميل عبد الباقى الصغير، مرجع سبق ذكره، ص 150، أنظر أيضاً:

Alain Bensousan. Internet, Aspects Juridiques, Hermes. 1996-1997- P. 108.

إلى نتيجة واحدة مع فعل الدخول وهى الوصول إلى معطيات غير مسموح للفاعل الوصول إليها، ويمكن تشبيه اعتراض نظام الحاسب الألى بالتنصت على محادثة تليفونية على سبيل المثال فالاعتراض هو التقاط الموجات الكهربائية وجمع المعلومات عن بعد، وتطبيقاً لذلك قضت محكمة الجنح المستأنفة فى فرنسا بإدانة أحد مندوبى شركة فرنسا للاتصالات والذى كان مكلفاً بالرقابة والاشراف على سنترال تليفونى بتهمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعلومات، [37] وكذلك لا يشترط للعقاب على مجرد الدخول إلى النظام أو البقاء فيه بطريق غير مشروع أن يكون النظام الذى تم الدخول إليه أو البقاء فيه محمياً بأجهزة أمان لأن ذلك يؤدى إلى قصر نطاق الحماية الجنائية على الأنظمة المحمية فقط، دون الأنظمة المفتوحة للجمهور مثل الدليل الالكترونى.[38]

المبحث الثانى: الركن المعنوى لجريمة الدخول ووسائل مكافحتها:-

المطلب الأول: الركن المعنوى لجريمة الدخول وصورها:

أولاً : الركن المعنوى:

جريمة الدخول إلى النظام بطريق غير مشروع أو البقاء فيه جريمة عمدية، والقصد العام كاف لقيامها، وهذا يتطلب علم الجانى بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير أو أن يدخل فيه دون أن يكون له الحق فى ذلك، وأن تنجه إرادته إلى أرتكاب هذه الجريمة، ويستدل على توافر سوء النيه لدى الجانى إذا كان دخوله إلى النظام نتيجة اختراقه واعتراضه لجهاز الأمن الذى يحمى هذا النظام، أو إذا كان الدخول إلى النظام أو البقاء فيه يقتصر على من يحمل بطاقة معينة أو شفره من قبل صاحب النظام فقام الجانى بسرقة البطاقة أو قام بتزويرها أو توصل إلى كلمة السر أو الشفرة بطريق غير مشروع ودخل بها إلى النظام، ويتطلب العلم والإرادة معرفة موضوع الحق المعتدى عليه فيتعين توافر علم الجانى أن فعله ينصب على نظام الحاسب الآلى مما يتضمنه من معلومات وبرامج بأعتباره محل الحق الذى يحميه المشرع، فإذا أعتقد الفاعل بناء على أسباب معقولة أنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلى دون أن يتجه علمه إلى أنه يقوم بالدخول إلى نظام الحاسب بما يحتوى عليه من معلومات وبيانات فإن قصد الدخول لا يتوافر لديه ولا يسأل جنائياً لانتفاء القصد الجنائى لديه، أما إذا دخل بطريق الخطأ ولكنه ظل موجوداً داخله مع علمه بذلك فإنه يقع تحت طائلة

---

[37] CA. Aix-en province, 13e ch, 23 Octobre 1996, J.C.P éd. E mai 1998. Droit de l'informatique, chron No 26, P. 848, note VIV ANT (nichel) et LE Stang (christian), G.P.20-22 Juillet 1997, P. 34.

أنظر أيضاً: د. جميل عبد الباقى الصغير، الانترنت والقانون الجنائى، دار النهضة العربية، القاهرة، 2001، ص 61 .

[38] د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، دار الجامعة الجديدة، الإسكندرية، 2001، ص 151.

القانون[39]، ويتوافر القصد الجنائى ولو لم يتوقع الجانى أى أثار عن فعله، كونه دخل إلى نظام غير مشروع له بالدخول إليه ولا يشترط أن يتوقع الضرر الذى سوف يلحق النظام أو صاحبه من جراء هذا الدخول [40] وقد نصت المادة 17 من قانون إساءة أستخدام الحاسبات الآلية فى المملكة المتحدة على أن التحقق من توافر النية الإجرامية فى جريمة الدخول غير المشروع إلى نظام الحاسب الآلى لا ينبغى أن يرتبط بنوعية المعلومات أو البرامج أو الأنظمة محل الجريمة، فالفاعل يسأل عن جريمته ولو لم يكن دخوله مصحوباً بتحديد المعلومات أو البرامج التى تم الدخول إليها [41]، وقد تطلبت بعض التشريعات الخاصة بجريمة الدخول غير المشروع قصداً خاصاً إلى جانب القصد العام، مما يترتب عليه تشديد العقوبة، ففى الدنمارك تشدد العقوبة متى أرتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، وفى أستراليا يوجد نص خاص يشدد العقوبة على من أرتكب فعل الدخول بنية الأضرار بالغير وفى النرويج تشدد العقوبة على نحو ملحوظ متى أرتكب فعل الدخول غير المشروع بنية حصول الفاعل له أو للغير على ربح غير مشروع أو الحاق الضرر بالغير نتيجة للاطلاع على المعلومات التى يعتدى عليها النظام، [42] أما القانون البرتغالى فتطلب قصداً خاصاً لجريمة الدخول غير المشروع، فالمادة السابقة من القانون البرتغالى للجرائم المعلوماتية لسنة 1991 يعاقب كل من يقوم على نحو غير مشروع بالدخول إلى أنظمة أو شبكات المعلومات بنية الحصول له أو للغير على ربح أو فائدة غير مشروعة، وتطلب المشرع السعودى فى قانونه الصادر سنة 2007 والسابق الإشارة إليه، توافر قصداً خاصاً سواء فى مادته الثالثة والخامسة والسابعة، وهو قصد الجانى من الدخول غير المشروع لغرض التهديد أو الابتزاز أو بغرض الحصول على بيانات تمس أمن الدولة أو تمس الاقتصاد الوطنى، وقد تضمن قانون إساءة أستخدام الحاسبات الآلية الإنجليزى لسنة 1990 فى مادته الثانية نصاً يجرم الدخول غير المشروع متى توافر لدى الفاعل قصداً خاصاً يتمثل فى نية أرتكاب جريمة أخرى لاحقه على هذا الدخول كالسرقة أو التهديد أو النصب. [43]

ثانياً:صور جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلى ومنظومات المعلومات الالكترونية:لقد أصبحت المعلومة السلعة الرئيسية فى العالم كله أى أن الدول لن تقاس بجيوشها أو قواتها أو ثرواتها بل أصبح المقياس الأول لقوة الدول هو مقدار ما تنتجه فى حقل صناعة المعلومات

---

[39] د. محمد محمد شتا، مرجع سبق ذكره، ص 152 .

[40] د. نائلة عادل محمد، مرجع سبق ذكره، ص 381.

[41] للمزيد حول موضوع القصد الجنائى فى الجرائم المعلوماتية راجع: مروان بن مرزوق الروقى، القصد الجنائى فى الجرائم المعلوماتية، دراسة تأصيلية مقارنة،مركز الدراسات العربية، القاهرة،2013، ص 36.

[42] المرجع السابق، ص 72 وما بعدها.

[43] د. نائلة عادل محمد فريد، مرجع سبق ذكره، ص 332.

وأستخدامها والتعامل معها وخاصة فى مجال التجارة، فالمعلومة قوة، وهذا الانفجار المعلوماتى الذى نشهده الآن فى مجال التجارة الالكترونية هو ثمرة المزاوجة بين تكنولوجيا الاتصالات وتكنولوجيا الحاسب الآلى والذى أدى إلى ميلاد علم جديد هو علم اتصالات المعلومات وأستخدامته [44]،

عليه فإننا سنتطرق إلى صور جريمة الدخول غير المشروع والتى تشكل فى حد ذاتها جرائم معاقب عليها وهى:-

1- الدخول غير المشروع بقصد معرفة معلومات سرية تتعلق بأحدى الشركات التجارية وغيرها:

وقد نصت على هذه أغلب التشريعات فمجرد الدخول تقع الجريمة ويسمى بالدخول المجرد وقد أخذت به تشريعات فرنسا وأمريكا بشرط أن يتعلق فعل الدخول بأنظمة محددة وعلى سبيل المثال أنظمة الحاسبات الآلية للشركات التجارية الكبرى. [45]

2- الدخول غير المشروع لغرض تعديل والتلاعب فى المعلومات والبرامج:

ويرى الفقه الجنائى أن نسبة هذا النوع من الجرائم تقدر بحوالى 15% من مجموعة حالات الجرائم المعلوماتية، وتأخذ الصورة الغالبة لهذه البرامج قيام المجرم المعلوماتى بتعديل البرنامج أولاً والتلاعب فيه ثانياً، وذلك لتحقيق أكبر قدر ممكن من الاستفادة المادية [46] ويكون التعديل دائماً لاختلاس النقود، وتكثر تلك الجرائم فى مجال التجارة والحسابات البنكية، أما التلاعب فيكون عادة بزرع برنامج فرعى غير مسموح به فى البرنامج الأصلى ويسمح له بالدخول غير المشروع فى العناصر الضرورية لأى نظام معلوماتى، ويمكن دفن هذا البرنامج الصغير فى مكونات البرنامج الخاص بالمنشأة أو الشركة، ولصغره ولدقته لا يحدث أكتشافه إلا بالصدفة. [47]

---

[44] للتوسع حول ذلك أنظر: وليد عاكم، التحقيق فى جرائم الحاسوب، بحث منشور على الانترنت:
http://www.wasmia.com/jazy/crineog.pdf

[45] راجع د. مدحت رمضان عبد الحليم، مرجع سبق ذكره، ص 39. ، د. نائلة عادل محمد فريد، مرجع سبق ذكره، ص 339 .

[46] بحث منشور على الانترنت بتاريخ 25-5-2016 http://www.jle.gov.sy/index.php/
أنظر أيضاً بالتفصيل: د. هدى حامد قشقوش، الاتلاف العمدى لبرامج وبيانات الحاسب الألكترونى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون الفترة 1-3- مايو 2000 مجموعة أعمال المؤتمر، جامعة الامارات العربية المتحدة.

[47] هناك التلاعب فى المعلومات ويعد هذا النمط من الاجرام المعلوماتى من أكثر صور الجريمة المعلوماتية شيوعاً فى أوربا أنظر فى ذلك د. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعى، الإسكندرية، 2006 ص 83 وما بعدها وهناك التلاعب المباشر والتلاعب غير المباشر أما الأول فيتم عن طريق أدخال معلومات بمعرفة المسؤول عن القسم المعلوماتى والذى غالباً ما تسند إليه وظيفة المحاسبة والمعاملات المالية أما الثانى فيتم عن طريق أستخدام أحد وسائط التخزين أو بوساطة التلاعب عن بعد بأستخدام وسائل معينة ومعرفة أرقام الشفرات الخاصة بالحسابات، كالتلاعب فى الشرائط الممغنطة والتلاعب فى البيانات عن بعد. ومن أمثلة الصورة الأولى قيام أحد الموظفين بأحدى فروع الشركة الفرنسية (LsoverstGobain) بإرسال شريط ممغنط احتوى على 139 إذن دفع، وعند معالجته بالبنك فى القسم المعلوماتى تم رفض نسخة لعيب فى طول الشريط والقى القبض على المتهم الذى لو نجحت محاولته لحقق مبالغ طائلة، المرجع السابق ص 180 .

3- الدخول غير المشروع بقصد الاضرار بتجارة الآخرين أو للحصول على أرباح غير مشروعة.

ويستوى أن يؤدى نشاط الجانى إلى توقف النشاط لأنظمة الشركات الكبرى بصورة دائمة أو مؤقتة، أو أن يستخدم الجانى فى ارتكاب الجريمة أى وسيلة من شأنها الاضرار بتجارة الأخرين أو الحصول على أرباح غير مشروعة كالاعتداد المادى على النظام المعلوماتى أو نشر فيورس به حيث أنه يستوى لدى المشرع الوسيلة المستخدمة.

4- الدخول غير المشروع لغرض ارتكاب والتسهيل لجرائم أخرى: ولعل أبرز الأمثلة على هذه الصورة هو القانون الإنجليزى الذى جّرم الدخول غير المشروع إلى نظام الحاسب الآلى وذلك بنية أرتكاب أو تسهيل أرتكاب جريمة أخرى، وشدد المشرع الانجليزى العقوبة فى هذه الحالة إلى السجن لمدة خمس سنوات أو بغرامة يقدرها القاضى أو كليهما معاً، إلا أنه يتطلب الأمر الاشارة إلى تجريم الدخول غير المشروع صراحةً سواء تم بمجرد الدخول إلى النظام أو بالدخول إلى ما يحتوى عليه هذا النظام من معلومات وذلك لغرض أرتكاب أى جريمة أخرى.

5- الدخول غير المشروع بقصد التهديد والابتزاز: وقد أشار ذلك صراحة القانون السعودى الصادر سنة 2007 فى مادته الثالثة وذلك لغرض تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً فالعقاب هنا هو الدخول بقصد التهديد والابتزاز.

6- الدخول غير المشروع لغرض العبث بالمواقع الالكترونية:

سواء تم ذلك بتغيير تصميم المواقع أو إتلافه أو تعديله فالمعروف دائماً أن هناك أسماً للموقع، فمن يقوم بالدخول فى عنوان الموقع حتى يحول دون أستخدامه بشكل أو بآخر تنطبق عليه هذه الصورة مادام أن نيته من وراء الدخول غير المشروع هو الوصول إلى تحقيق تلك الغاية.[48]

المطلب الثانى: العقوبات المقررة لجريمة الدخول غير المشروع ووسائل مكافحتها:

أولاً: العقوبات:

يتطلب بيان هذه العقوبات النظر فى التشريعات التى حرمت الدخول غير المشروع بصوره المتعددة، وأول هذه التشريعات التشريع الفرنسى الذى نص فى مادته 323-1 على العقاب على الدخول بطريق الغش أو التدليس على نظام للمعلومات أو إبقاء الاتصال بطريقة غير مشروعة به بالحبس لمدة سنة وبغرامة مائة ألف فرنك فرنسى إذا ترتب على نشاط الجانى إلغاء أو تعديل البيانات الموجودة بالنظام أو تعديل

[48] للمزيد حول ذلك أنظر: هدى قشقوش، الاتلاف العمدى لبرامج وبيانات الحاسب الآلى، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات فى الفترة 1-3 مايو 2000.

تشغيل النظام، وتعاقب المادة الثانية بالحبس لمدة ثلاثة سنوات وغرامة 300.000 ألف فرنك فرنسى على إعاقة أو التسبب فى تحريف تشغيل نظام معالجة البيانات، وتعاقب المادة الثالثة بالحبس لمدة ثلاثة سنوات وغرامة 300.000 ألف فرنك فرنسى على عملية إدخال بيانات بطريقة غير مشروعة فى نظام معالجة البيانات أو إلغاء أو تعديل البيانات التى يحتوى عليها النظام بطريقة غير مشروعة، ونصت المادة 323-5 على بعض العقوبات التكميلية للعقوبات الأصلية المقررة للجرائم السابقة وهى:-

- الحرمان لمدة لا تتجاوز 5 سنوات من الحقوق المدنية وتلك المتعلقة بالأسرة وفقاً لأحكام المادة -26 131 من قانون العقوبات الفرنسى، - الحرمان لمدة لا تتجاوز 5 سنوات من شغل الوظائف العامة أو نشاط مهنى أو أجتماعى، - مصادر الشىء أو الأشياء التى أستخدمت فى أرتكاب الجريمة أو اعدت للأستعمال فى ارتكابها أو حصلت عنها، - الإغلاق لمدة لا تزيد على 5 سنوات للأماكن أو المشروعات التى أستخدمت فى أرتكاب الجريمة، - الأبعاد لمدة لا تجاوز 5 سنوات عن الاسواق العامة وهى العقوبة التى تحمى المستهلك من مثل هؤلاء الجناة وردعهم عن العودة لمثل هذه الجرائم، - المنع من إصدار شيكات لمدة لا تجاوز 5 سنوات، - الاعلان ونشر الحكم، وقد نص المشرع الفرنسى على مساءلة الأشخاص المعنوية عن جميع الجرائم السابقة طبقاً لنص المادة 323-6 فى ضوء الأحكام العامة لمساءلة الأشخاص المعنوية المنصوص عليها فى المادة 121-2 من قانون العقوبات الفرنسى.

أما المشرع الأمريكى فنص على عقوبات مشددة لجرائم الدخول غير المشروع وحدد عقوبات أخرى للشروع فيها وهذا ما تناوله الفصل 1030 من نصوص خاصة تُجرم الاعتداء على الكمبيوتر والمتعلقة بأنشطة متصلة بالكمبيوتر من رقم 1 إلى 6 .

أما المشرع الإنجليزى فنص فى قانونه الصادر سنة 1990 على عقوبة السجن لمدة لا تتجاوز ستة أشهر أو لغرامة لا تتجاوز ألف جنيه استرلينى أو لكليهما معاً (المادة الأولى) ونص القانون على عقوبات أخرى فى حالة الدخول غير المشروع بقصد التسهيل والتحريض على الجرائم بين الجنح والجنايات التى لا تتجاوز 5 سنوات وبغرامة يقدرها القاضى أو لكليهما معاً ونص أيضاً على عقوبة السجن لمدة تتجاوز 6 أشهر وغرامة فى حالة تبديل أو تحويل مواد الكمبيوتر.

وكانت دولة السويد هى الأولى فى إصدار التشريع الذى جرّم الدخول غير المشروع إلى نظام الحاسب الآلى سنة 1973 والمعدّل بالقانون 1986-1990 ونصت على عقوبات وشددت فى بعض صورها، وذهبت على أثرها تشريعات أخرى كاليونانى والبرتغالى والفنلندى والهولندى والنرويجى والدنماركى، والألمانى والذى أشترط للعقاب أن يحصل الفاعل على معلومات نتيجة هذا الدخول، فالمشرع الألمانى يعاقب على ما يحصل عليه الفاعل من معلومات، وأن تكون هذه المعلومات مشمولة بحماية نظم أمنية، كما أنه فى ظل هذه العقوبات تنص بعض التشريعات على تشديد العقوبة فى حالة توافر الظروف المشددة لبعض الجرائم، كفعل اختراق نظام الأمن الخاصة بنظام الحاسب الآلى يجعل فعل الدخول إليه

أكثر خطورة، فوجود هذه الأنظمة قرينة على أهمية المعلومات التى يحتوى عليها نظام الحاسب الآلى الذى تم الدخول إليه وهو ما يقتضى تشديد العقوبة، فالظروف المشددة قد تتعلق بماديات الجريمة أو بركنها المعنوى، فالمادية تتعلق بالجريمة وكيفية ارتكابها وما أكتنفها من ملابسات، كظرف الليل والمحل المسكون والكسر فى جريمة السرقة، أما الظروف الشخصية (المعنوية) وهى تعنى ازدياد خطورة الأثم كظرف الخدمة فى جريمة السرقة [49]، ونص المشرع الاماراتى فى قانونه رقم 2 لسنة 2006 على عقوبة الحبس أو الغرامة فى حالة أختراق المواقع والأنظمة الإلكترونية وشدد العقوبة فى حالة ما ترتب عليه من إلغاء أو حذف أو تدمير معلومات بالأنظمة، ونص القانون السعودى الصادر سنة 2007 والخاص بمكافحة جرائم المعلوماتية فى مادته الثالثة بعقوبة السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين، كل شخص قام بالدخول غير المشروع إلى موقع إلكترونى أو الدخول إلى موقع الكترونى لتغيير تصاميم المواقع أو اتلافه أو تعديله أو شغل عنوانه، ونصت المادة الخامسة من نفس القانون على عقوبة السجن لمدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص قام بالدخول غير المشروع لالغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها، ونص أيضاً فى مادته السابقة على عقوبة السجن لمدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب الدخول غير المشروع إلى موقع الكترونى أو نظام معلوماتى مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلى للحصول على بيانات تمس الأمن الداخلى أو الخارجى للدولة أو إقتصادها الوطنى، ونصت المادة التاسعة على عقوبة المساهمة الجنائية، فى هذه الجرائم بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ونصت المادة العاشرة على عقوبة الشروع فى هذه الجرائم بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة، أما المادة الحادية عشر فنصت على جواز الاعفاء من جميع هذه العقوبات لكل من يبادر من الجناة بإبلاغ السلطات المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، ونص القانون رقم 26 لسنة 2007 المتعلق بالأحوال المدنية السورى فى مادته 73/د على عقوبة الاشغال الشاقة من ثلاث إلى خمس سنوات لكل شخص غير موظف فى وزارة الدخلية قام بالدخول لغرض تعديل البيانات حذفاً أو إضافة أو تعديلاً، أما إذا كان موظفاً فى وزارة الداخلية فتكون العقوبة الحبس من شهر إلى ستة أشهر وبغرامة مالية من عشرة ألاف إلى خمسة ألف ليرة سورية، أما إذا كان قصد الموظف من الادخال هو التزوير فتكون العقوبة الأشغال الشابقة من ستة سنوات إلى عشرة مع العقاب على الشروع فى الجرائم السابقة بعقوبة الفعل التام، كما أوصى المجلس الأوربى فى توصيته

[49] د. محمود نجيب حسنى، شرح قانون العقوبات، القسم العام، مرجع سبق ذكره.

الخاصة بجرائم الحاسب الآلى بتجريم الدخول غير المشروع واقترحت اللجنة فى تقريرها نصاً خاصاً لهذه الجريمة بمقتضاة يتم تجريم الدخول غير المشروع عن طريق أختراق نظم الأمن الخاصة بهذا النظام.

ثانياً: آليات حماية أجهزة الحاسب الآلى ومنظومات المعلومات الإلكترونية.

لحماية أجهزة الحاسبات والمنظومات المعلوماتية من جريمة الدخول غير المشروع يتطلب الأمر عدة أساليب تتمثل فى الأتى:-

1- يتطلب الأمر تجريم كل دخول غير مشروع إلى أنظمة التجارة الالكترونية سواء الدخول المجرد المتعلق بأنظمة محددة أو بأنظمة محددة لها عدة أنواع من المعلومات.

2- أسلوب التجريم لفعل الدخول المتعلق بغرض اتلاف المعلومات أو البرامج المخزونة كما فعل التشريع الفيدرالى فى الولايات المتحدة الأمريكية.

3- أسلوب التجريم لفعل الدخول المتعلق بأختراق نظم الحاسبات الآلية الكبيرة والصغيرة لغرض الحصول على المعلومات أو اختراق أنظمة المعلومات الالكترونية.

4- اسلوب التجريم لفعل الدخول لمواقع التجارة الالكترونية ثم تشديد العقوبة فى بعض الحالات وخاصة إذا كان الغرض هو ارتكاب جرائم أخرى كالغش والنصب والسرقة والاتلاف لهذه المواقع .

5- أسلوب التجريم لفعل الدخول غير المشروع للأنظمة المتعلقة بالاستهلاك اليومى للتجارة الالكترونية خاصةً إذا كان الغرض تغيير الاسعار وأستبدال المعروضات أو بيان عكس المعروض سواء فى النوع أو الكمية أو الجودة أو كيفية الوصول.

وإذا أردنا وضع هذه الأساليب بشكل أكثر ضمانة فلابد من بيان خطورة جريمة الدخول غير المشروع إلى الكمبيوتر بصفة عامة، فهو أساس الجرائم المعلوماتية الأخرى، على أن يكون مفهوم الدخول هو الوصول إلى المعلومات، كما يتطلب الأمر ضرورة العقاب على الفعل (فعل الدخول) بوصف الشروع متى تحققت أركانه لغرض حماية أنظمة الحاسب الآلى، مع تشديد العقاب فى حالة الدخول عن طريق أختراق نظم الأمن الخاصة مثلاً بالشركات التجارية، وكذلك إذا نتج عن الدخول اتلاف المعلومات سواء كان هذا الاتلاف كلياً أو جزئياً وأخيراً إذا ترتب على فعل الدخول ضرر يلحق بصاحب المعلومات وخاصة المستهلك الالكترونى الذى يتم الدخول عليه لتغيير المعلومات المطلوبة وكذلك الضرر الواقع على مواقع التجارة الالكترونية مثلاً، فالأمر يتطلب مواجهة الاعتداءات المتكررة على المعلومات والأنظمة الالكترونية التى لا تكفى النصوص التقليدية لقانون العقوبات من مواجهتها، فعديد التشريعات تدخلت لحماية المعلومات والأنظمة الالكترونية من الأفعال الاجرامية كالقانون الفرنسى والأمريكى والسويدى والفنلندى والبرتغالى والدنماركى والانجليزى والاماراتى والسعودى والكويتى والسورى والهدف هو حماية المعلومات الاكترونية لا سيما حماية التجارة والإقتصاد العام والخاص والدول بصفة عامة، فالتكنولوجيا ليست قاصرة على فرع قانونى بعينه، فأليات الحماية تتطلب تجربة الأفعال السابقة وكذلك تجريم

أستخدام كلمات السر الخاصة بالغير للدخول إلى مواقع التجارة الالكترونية وتجريم تعطيل أو إفساد نظام التشغيل كذلك تجريم نسخ أو تصدير أو أستيراد أى بضائع مشبوهة أو ضارة للمستهلك الالكترونى مع تجريم التلاعب فى البضائع أو تعديلها أوبيان عكس حقيقتها فى حالة عرضها الكترونياً، لابد من وضع ألية محددة لتعريف فعل الدخول على الأنظمة والمعلومات، وتحديد الأدوار وطبيعة الأعمال والمسئولية الجنائية المترتبة عليها مع تحديد الطبيعة القانونية للأنشطة التجارية المعروضة على شبكة الانترنت، وتحديد القوانين التى تخضع لها، مع إلزام متعهدى الوصول بأن يتحققوا من هوية مستخدمى الشبكة وخاصة التجارية بين العملاء وأصحاب العمل والذين يتولون توصيلهم بالحاسبات الخاصة وهذه أهم آلية ضامنة لحماية المستهلك الإلكترونى مثلاً، فالصعوبات التى تلاقيها المحاكمات فى إطار شبكة المعلومات قد تؤدى فى الواقع ببعض الهيئات القضائية إلى مجاملة القاء المسئولية الجنائية على بعض المتدخلين فى الشبكة وخصوصاً متعهدى التوصيل مثلاً، فالأمر يتطلب رصد جرائم الادخال عن طريق مجموعات متخصصة فى أمن المعلومات وهو ما ذكره مسؤول شركة أفاست لأمن المعلوماتية على مدونته " لقد رصدنا أكثر من 75 ألف هجوم فى 99 بلداً" وذلك فى منتصف عام 2017، كما قالت شركة "فودسبوينت سيكيوريتى لابس المتخصصة فى أمن المعلوماتية أنها رصدت " حملة كبيرة من الرسائل الالكترونية المعادية" بالفيروس المعلوماتى الخبيث، وأوصت جميع شركات الأمن المعلوماتى بتحديث برامج أمن المعلومات وبرامج مكافحة الفيروسات الإلكترونية وهذه من أهم آليات الحماية وعدم الدخول فى برامج ابتزاز الأموال من قبل القراصنة، كل ذلك لسد ثغرات النظام الإلكترونى. (50)

خاتمة البحث وتوصياته:

الدخول غير المشروع داخل أنظمة الحاسب الآلى سواء بطريق مباشر أو غير مباشر لا يختلف من حيث وجوب التجريم، فالنتيجة الاجرامية واحدة تتمثل فى الوصول إلى نظام غير مصرح بالدخول إليه فالمصلحة التى يحميها القانون هى حماية أنظمة الحاسبات الآلية وما تحتويه من معطيات واحدة فى الحالتين، وقد أتجهت عديد التشريعات على تجريم الدخول غير المشروع إلى أنظمة الحاسب الآلى وأنظمة المعلومات وأنها من الأنشطة الإجرامية الأكثر أنتشاراً بين جرائم الحاسب الآلى والانترنت، وتختلف الوسائل التى يمكن اللجوء إليها من أجل الدخول غير المشروع إلى تلك الأنظمة، إلا أنها جميعها تفترض قدراً من المعرفة بتكنولوجيا الحاسبات الآلية وإن كانت تتراوح فى مداها، وقد حرص مجلس أوربا على التصدى للأستخدام غير المشروع للحاسبات وأنظمة المعلومات وتجلى ذلك فى اتفاقية بودابست الموقعة فى 23 نوفمبر 2001 المتعلقة بالإجرام الكونى بمعنى الاجرام المعلوماتى أو الجرائم المعلوماتية ويكفى الادخال بأدخال البيانات على شبكة معينة من خلال عنوان المرسل إليه حتى تصبح متوافرة لأى

(50) راجع فى ذلك http//www.youn7.comstory

شخص يريد الدخول إليها، [51]كما أن الاستخدام العام للبريد الالكترونى ووصول الجمهور لمواقع الويب عبر الانترنت من أمثلة هذا التطور الذى قلب أوضاع مجتمعنا، وكان لكثرة مثل هذه الجرائم سهولة الوصول إلى المعلومات فى النظم المعلوماتية مع الامكانيات اللا محدودة لتبادلها وإرسالها بصرف النظر على المسافات الجغرافية أدى إلى نمو هائل فى حجم المعلومات المتاحة والتى يمكن الحصول عليها، وقد خلت التشريعات الجنائية وغيرها فى ليبيا من النص على مثل هذه الجرائم أو حتى الإشارة إليها الأمر الذى يصعب معه تحديد مفهوم هذه الجريمة وبيان أركانها فى التشريع الليبى.

التوصيات:

1- ضرورة مواكبة القانون الجنائى للتطورات التكنولوجية التى تقدم فرصاً واسعة لاساءة أستخدام إمكانيات الفضاء المعلوماتى وأن يعمل على ردع هذه الأفعال الاجرامية، مع تطبيق العقوبات المقررة فى تكنولوجيا المعلومات.

2- الرقابة الصارمة على الحاسبات الآلية وأنظمة المعلومات، للحد من مثل هذه الجرائم نظراً لاتساع دائرة مستخدمى الانترنت فلم تعد مقتصرة فقط على الباحثين فقط بل تضم أجيالاً مختلفة وثقافات متفاوتة.

3- كما أن أساليب الاستخدام تنوعت وتعددت أشكالها فالأمر يتطلب النص على تجريم هذه الجريمة بشكل مستقل فى تشريعات الدول نظراً لاتساع مجالاتها ومستخدميها، مع النص على عقوبات رادعة للتخفيف من اتساع مثل هذه الجرائم.

4- مع الأخذ فى الاعتبار أن الحماية الجنائية التى يوفرها القانون الجنائى لم تتأكل بفعل التطورات التكنولوجية ورغم أن القوانين الجنائية على ما هى عليه الأن، وقد نجحت فى بعض الحالات فى ملاحقة جرائم الكترونية، سيؤدى أدخال بعض التعديلات الرئيسية على تلك القوانين إلى حسم بعض الموضوعات التى يثار حولها الجدل ومن ثم تسهل ملاحقة الجرائم الالكترونية ومحاكمة مرتكبيها.

5- ضرورة مواكبة مشرعنا فى ليبيا للتطورات التكنولوجية والنص على مثل هذه الجرائم وتحديد مفهومها وأركانها والعقوبات المقررة لها، مع تحديد آلية حماية الأنظمة الالكترونية وضمان فاعليتها.

---

[51] د. علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002، ص 26، أنظر أيضاً د.عادل أبو هشيمة محمود، عقود خدمات المعلومات الإليكترونية فى القانون الدولى الخاص، دار النهضة العربية، القاهرة، 2005، ص 23، وما بعدها، أنظر أيضاً: http://www.cybercrime.gov/coepress.htm

قائمة بأهم المراجع

(1) د. أسامة عبدالله جايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، 1988، ص 86 وما بعدها.

(2) منير محمد الجنبيهى، ممدوح محمد الجنبيهى، جرائم الأنترنت والحاسب الآلى ووسائل مكافحتها، دار الفكر الجامعى، الإسكندرية، 2006.

(3) نائلة عادل محمد فريد، جرائم الحاسب الآلى الإقتصادية، دراسة نظرية تطبيقية، دار النهضة العربية 2003-2004.

(4) د. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الطبعة الأولى، الدار الجامعية، 2007.

(5) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2012.

(6) د. على عبد القادر القهوجى، الحماية الجنائية للبيانات المعالجة إلكترونياً بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الفترة من 1-3 مايو 2000

(7) د. جميل عبد الباقى الصغير، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن أستخدام الحاسب الآلى، 1992.

(8) خالد بن مرزوق بن سراج، الجوانب الإجرائية فى الشروع فى الجرائم المعلوماتية، دراسة مقارنة، مركز الدراسات العربية، القاهرة، 2014.

(9) د. محمود نجيب حسنى شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازى، 1989.

(10) د. محمد عبد اللطيف عبد العال، الجرائم المادية وطبيعة المسئولية الناشئة عنها، دار النهضة العربية، 1997.

(11) د. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، دار الجامعة الجديدة، الإسكندرية، 2001.

(12) د. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعى، الإسكندرية، 2006.

(13) هدى قشقوش، الاتلاف العمدى لبرامج وبيانات الحاسب الآلى، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الامارات فى الفترة 1-3 مايو 2000.

أهم المراجع باللغة الإنجليزية الفرنسية

1. Rico calleja, conditional access piracy, computer and telecommunications law review, 2003
2. Olivenbaun (Joseph n.), Rethinking Federal computer crine legislation S.H.L.Rev., 1997,
3. Jareborg (Nils), Computer Crines and Other Against information technology in Sweden, (R.P.L., 1993
4. 'David' Bainbridge, Introduction to Computer Law, OP.Cit., P312, Walden "Lan" Op.
5. R.V.Bow street magistate and Allison (AP), ex parte US government (1999)
6. Alain Bensousan. Internet, Aspects Juridiques, Hermes. 1996-1997

أهم المواقع الإلكترونية

www.al-watan.com

https://www.alhurra.com

http://europea.eu.int/indexen.htm

www.CNN.com

http://irbd.hooxs.com/t16012-topic

http://www.cybcrcrinc.gov/cocdraft.htm

http://www.noi.gov.kw/portal/varabic/ecccd/aspx.

http://www.wasmia.com/jazy/crineog.pdf

http://www.jle.gov.sy/index.php/

http//www.youn7.comstory