الإختلافات التشريعية في تجريم الدخول غير المصرح به إلى أنظمة المعلومات

عباوي نجاة
أستاذة مساعدة أ
كلية الحقوق والعلوم السياسية
جامعة بشار

ملخص

عرفت أنظمة المعلومات ولا تزال تشهد تطورات هائلة ومتوالية جعلت منها ضرورة لا مناص من الإعتماد عليها في المساعي المبذولة لتحقيق تقدم يمس كافة المجالات.

رافق تطور أنظمة الحاسبات والإتصالات تزايد الجرائم المرتكبة ضدها أو عبرها بطرق تزداد تنوعا وتطورا كل يوم، ذلك ما دفع غالبية دول العالم إلى الإسراع في سن تشريعات في محاولة للتصدي لجرائم المعلوماتية .

يسبق معظم الأفعال المرتكبة ضد أنظمة المعالجة الآلية للمعطيات أو عبرها دخولا غير مصرح به للنظام إذ تعد هذه الجريمة بوابة ارتكاب غيرها من الاعتداءات.

يحاول هذا البحث تحديد المقصود بالدخول غير المصرح به مع الوقوف على التباين التشريعي في عناصر تجريم هذا الفعل.

ABSTRACT

Information systems have known a tremendous development in the last few years which made it a necessity for the progress of all the fields.

The development in this domain came in parallel with augmentation in the assaults on information systems as well as through it.

Such assault urged many coutries to make legislations concerning cybercrimes.

Unauthorized access to automatic data processing systems comes ahead of other crimes for it perceed other forms of assaults.

This paper tries to define unauthorized access , as it spots the light on how the different legislations deal with such crimes.

مقدمـــة

تتعرض أنظمة المعلومات وبصفة خاصة تلك التي تعمل من خلال شبكات معلوماتية واسعة النطاق إلى العديد من الإختراقات، غير أنه لا يمكن ارتكاب جرائم المعلوماتية إلا بالتعامل مع نظام المعالجة الآلية للمعطيات، وتتخذ هذه المرحلة صورة الدخول إلى نظام المعلوماتية للوصول إلى البيانات والبرامج باعتباره مرحلة ضرورية لكل جريمة تدخل في عداد هذه الجرائم.

وقد عكفت التشريعات على تعديل قوانينها الجزائية أو استحداث نصوص خاصة من أجل مواكبة التطورات التقنية المتواصلة والتي يزداد الإعتماد على مفرزاتها سعيا لحماية مصالح الأفراد وحقوقهم ومحاولة لكبح جماح إجرام فاقت أضراره كل التوقعات.

فهل هناك توافق بين مختلف التشريعات التي تصدت لإجرام المعلوماتية؟ أم أن الإختلاف هو ميزتها؟

تنبع أهمية هذه الإشكالية من انتماء جرائم المعلوماتية للجرائم العابرة للحدود والتي تتطلب مكافحتها قدرا من التعاون والتوافق التشريعي في مختلف أركانها وعناصرها على مستوى إقليمي و دولي.

تهدف هذه الورقة إلى تحديد ماهية الدخول غير المصرح به و بيان أركان الجريمة من خلال الوقوف على أهم الإختلافات التشريعية في كل تلك العناصر محاولين مقارنة ما جاء به التشريع الجزائري مع غيره من التشريعات المقارنة.

المطلب الأول: ماهية الدخول غير المصرح به.

لا بد من تحديد المقصود بجريمة الدخول غير المصرح به وبيان محلها وما يصحب ذلك من إشكالات قبل الخوض في ركنيها المادي والمعنوي.

تحقق الدخول غير المصرح به إلى نظام المعلوماتية بالوصول إلى المعلومات والبيانات داخل النظام دون رضا المسؤول عن هذا النظام، وهو بقول آخر إساءة استخدام النظام عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات بداخله لاستعمالها في غرض ما.[1]

تم تجريم الدخول غير المصرح به إلى أنظمة المعلوماتية في العديد من الدول، وإن اختلفت فيما بينها من حيث الشروط المتطلبة لتطبيق نصوصه.[2]

عزفت العديد من التشريعات عن وضع تعريف لهذا الدخول كالتشريعين الجزائري والفرنسي وقد أحسن المشرع السعودي بإدراج تعريف له عندما حدد معاني الألفاظ الواردة بقانون جرائم المعلوماتية،[3] وإن كان التعريف الذي أورده قاصرا عن الإحاطة بكل صور الدخول غير المشروع .

ترتكب الجريمة بأحد الطريقين أولهما ألا يكون هناك تصريح بالدخول بتاتا لدى من يقوم بالدخول وهي إحدى صور جريمة الدخول غير المصرح به والتي لا تثير إشكالا، وثانيهما أن يوجد تصريح بالدخول لكن المصرح له يقوم بتجاوز الحدود التي رسمت له في هذا التصريح ويحدث هذا التجاوز في حالتين:

- **الحالة الأولى: تجاوز المجال المحدد في التصريح.**

في هذه الحالة يملك الشخص الذي يدخل النظام تصريحا بالدخول، لكن هذا التصريح ليس عاما أي أنه غير شامل لكامل النظام وإنما يقتصر على بعض المجالات دون أخرى، بحيث يكون الدخول إلى المجالات المصرح بها مشروعا ويكون غير مشروع في غيرها.

وغالبا ما يتم هذا النوع من الدخول من قبل العاملين بالمؤسسة، والذين يملكون عادة تصريحات جزئية تشمل مناطق محددة بحسب الوظيفة التي يؤديها كل عامل، لذلك تعتبر عدة تشريعات توافر صفة العامل ظرفا مشددا.

والتجاوز المقصود هنا هو التجاوز في المكان لا في الزمان، أي تجاوز الفاعل للمناطق والمجال المكاني المصرح به إلى غيره من المجالات غير المصرح له بدخولها، ذلك أن المسموح به هو الإطلاع على معلومات أو بيانات محددة، وفيما عدا ذلك فإن الأصل العام ينطبق هنا ألا وهو سرية المعلومات وعدم جواز الإطلاع عليها.[4]

إذا كان تجاوز التصريح بالدخول يقع كثيرا من العاملين في المؤسسات الضحية، فإنه قد يقع من غير العاملين أيضا ويرى الفقه أن ما يحكم تجاوز الفاعل للتصريح المقدم له هو ما يسمى بالعرف المعلوماتي، إذ هناك معايير تحكم استخدام الأنظمة تقضي بأن مصممي البرامج يقومون بتصميمها لتأدية عدة مهام، ومزودي خدمات شبكة المعلومات يسمحون بوجود هذه البرامج فيجيزون للمستخدمين القيام بهذه المهام، ويصرحون

ضمنا للمستخدمين بذلك، لكنهم لا يصرحون في المقابل باستغلال الضعف في البرامج لإنجاز وظائف غير تلك التي منح من أجلها التصريح بالدخول إذ يكون هنا الدخول غير مشروع، وهذه الحالة يسميها الفقه والقضاء الأمريكي باختبار تأدية الوظيفة،[5] وقد تعرض لها القضاء الأمريكي في واحدة من أهم قضايا جرائم المعلوماتية وهي قضية (MORRIS) أو ما تعرف بقضية دودة الأنترنت (internet worm case).[6]

- **الحالة الثانية: تجاوز الغرض الممنوح من أجله الترخيص.**

إختلف الفقه و القضاء في إضفاء وصف الدخول غير المصرح به على الدخول المصرح به إذا استخدم لغرض آخر غير الغرض الذي منح من أجله التصريح.

هناك من يرى بأن الدخول هنا يكون مشروعاً و بالتالي لا تقوم الجريمة، وهو موقف القضاء الإنجليزي الذي تعرض لهذه الحالة في حكمين انتهى في كل منهما إلى أن الدخول في هذه الحالة يعد مصرحاً به، ورفض تطبيق المادة الأولى من قانون إساءة استخدام الحاسبات الآلية التي تتعلق بالدخول غير المصرح به إلى نظام المعلوماتية.[7]

وقد تعرض الحكمان الإستئنافيان السابقان لإنتقاد شديد لما يؤديان إليه من تضييق في نطاق تطبيق قانون إساءة استخدام الحاسبات الآلية، وبحكم تنافيهما و المفهوم الصحيح للتصريح بالدخول إلى أنظمة المعلوماتية، لأن الحق في الدخول إلى نظام المعلوماتية أوفي تنظيم هذا الدخول لابد أن يكون مقيداً بالغرض الذي أعطيت من أجله هذه السلطة، فمتى تعارض هذا الغرض الذي تم من أجله الدخول مع الغرض الأصلي أصبح الدخول غير مصرح به.[8]

تبنى القضاء الأمريكي رأيا مخالفا إذ رأى أن الدخول غير المصرح به يتحقق في حالة استخدام العامل لنظام المعلوماتية لأسباب تتعارض مع مصلحة رب العمل، أما في حالة ما إذا كان العامل لا يعمل لمصلحة رب العمل فيذهب هذا الرأي إلى أن الباعث هنا هو الذي يحدد ما إذا كان الدخول مصرحاً به أو غير مصرح به، و تسمى هذه الحالات في الفقه الأمريكي بحالات سوء إدارة العاملين (Employees Misconduct case) .

من أهم القضايا التي تعرض لها القضاء الأمريكي في هذا الشأن قضية (Shergard)، وهناك قضية واحدة أسست على السلوك و ليس على الباعث و هي قضية (Briggs), فهي لا تمثل القاعدة في القضاء الأمريكي.[9]

إن نص المادة 394 مكرر من قانون العقوبات الجزائري صريح في تجريم الدخول غير المصرح به إلى أنظمة المعلوماتية، إذ ينص على أن الدخول عن طريق الغش يشكل جريمة في ذاته، و ليس في ما يحصل بعد هذا الدخول من إلتزام بحدود التصريح أو تجاوزه. فصفة الغش إذا تنصرف إلى عملية الدخول و ليس إلى حدود التصريح بهذا الدخول،حيث أن مبادئ التفسير في القانون الجزائي لا تسمح بالتوسع أو القياس.

إذن لا يمكن تطبيق نص هذه المادة على الدخول المصرح به المتجاوز لحدود التصريح أو للغرض الذي منح من أجله هذا التصريح، لكن خطورة هذه الأفعال ومساسها بأنظمة المعلوماتية تكمن في سهولة ارتكابها، الأمر الذي يستدعي تجريمها درءً للأضرار التي يمكن أن تنجم عنها.

جرمت غالبية التشريعات كالتشريعين الجزائري والسعودي وكذا التشريع الفرنسي الدخول غير المصرح به دون تفصيل أنواعه، إلا أن رفع اللبس ومنع التوسع في النصوص الجزائية يقتضي أن يتم النص على حالة الدخول المصرح به والمتجاوز لحدود التصريح أو الغرض الذي منح من أجله الترخيص، وهو ما دعا إليه القانون الإتحادي لدول الخليج العربية حيث تنص المادة الثالثة منه على أن:" يعاقب كل من دخل عمدا وبدون وجه حق إلى موقع أو نظام المعلومات الإلكتروني أو تجاوز الدخول المصرح به.." .

المطلب الثاني: الركن المادي.

هناك اختلافات تشريعية حول تجريم الدخول غير المصرح تتعلق بتحديد محل الجريمة و السلوك المجرم فيها و الإعتداد بالنتيجة المترتبة عليها.

أولا: محل الجريمة.

تختلف التشريعات في تحديد محل جريمة الدخول غير المصرح به كما تختلف التسميات التي تطلق على هذا المحل وإن كان لا يخرج عن عناصر ثلاث و هي المعلومات في ذاتها، والثانية هي الحاسبات الآلية التي ترتبط فيما بينها من خلال شبكات الإتصال والثالثة هي شبكات المعلومات.

اتجه القانون الإنجليزي إلى استبعاد شبكات الإتصال من نطاق التجريم فالمادة الأولى من قانون إساءة استخدام الحاسبات الآلية الصادر عام 1990 تعاقب على الدخول غير المصرح به إلى البرامج والمعلومات التي يحتوي عليها أي حاسب آلي،[10] وقد تضمنت المادة 17 من هذا القانون بعض التعريفات التي تساعد على تفسير نصوصه إلا أنها لم تتضمن تعريفا للحاسب الآلي أو البرامج أو المعلومات محل جريمة الدخول غير المصرح به، ويترتب على ذلك استبعاد المعلومات التي يتم نقلها عبر شبكات المعلومات كما أن النص لا يتسع للشبكات إجمالا.

هناك إتجاه آخر يمثله القانون السويدي الذي يعاقب على الدخول غير المشروع إلى أنظمة الحاسبات الآلية بواسطة جهاز لنقل المعلومات، فالنص على هذه الجريمة لا يعالج سوى حالات الدخول غير المصرح بها التي تتم عن طريق أشخاص خارج المؤسسات التي تحتوي على الأنظمة بواسطة شبكات الإتصالات، أما الحالات التي تنطوي على دخول مباشر إلى النظام، والتي يقوم بها غالبا العاملون في المؤسسات التي تحتوي على هذه الأنظمة فلا يشملها النص ما لم يكن الدخول إلى النظام قد تم من خلال شبكة داخلية تابعة للمؤسسة،[11] والموقف ذاته نجده في قانون العقوبات الأسترالي حيث تم تجريم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية غير التابعة للدولة، بشرط أن يكون الدخول إليها قد تم بواسطة شبكات الإتصالات العامة.[12]

إتجاه ثالث يجعل محل الجريمة من الإتساع بحيث يشمل كل جزء من أجزاء أنظمة المعلومات أويشير إليها بلفظ أنظمة المعلومات منظورا إليها بالمعنى الواسع لتشمل إلى جانب أنظمة الحاسبات شبكات المعلومات والمعلومات المعالجة عبرها، يعد القانون الفرنسي مثالا على هذا الإتجاه، فالمادة 1/321 من قانون العقوبات تجرم فعلي الدخول أو البقاء غير المشروعين داخل نظم المعالجة الآلية للمعلومات بالمعنى الواسع للكلمة،[13] وتجرم هذه المادة الدخول إلى كل النظام أو إلى أي جزء منه كشرط لقيام الجريمة،ولا تقوم الجريمة بالدخول إلى أي عنصر يحتوي على معلومات متى كان بمعزل عن نظام المعالجة الآلية للمعلومات.

وقد أجمع الفقه الفرنسي -من واقع الأعمال التحضيرية للقانون- على أن نظام المعالجة الآلية للمعلومات في تطبيق المادة 1/321 ينصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات.[14]

في الولايات المتحدة الأمريكية تجرم المادة 1030 (أ) (3)[15] الدخول المجرد إلى الحاسبات،[16] وتشمل الحاسبات الآلية وفقا لهذا القانون كل جهاز إلكتروني أو كهربائي أو جهاز سريع لمعالجة المعلومات يقوم بإجراء عمليات منطقية وحسابية، كما تشمل أيضا كل وسيلة آلية لتخزين المعلومات وكذلك كل وسائل الإتصالات التي تعمل بالإتصال مع أي من هذه الأجهزة.[17]

وأخيرا لابد من الإشارة إلى أن المشرع الجزائري قد جرم الدخول إلى نظام المعالجة الآلية للمعطيات دون تفصيل، وهو بذلك يشمل الدخول إلى كافة عناصر النظام مجتمعة من أنظمة حاسبات وأنظمة إتصالات

وقد جاءت صياغة المادة 394 مكرر من قانون العقوبات الجزائري مماثلة لنص المادة 1/321 من قانون العقوبات الفرنسي بأن جرمت الدخول إلى نظام المعالجة الآلية للمعطيات بصفة عامة.[18]

اعتبر المشرع الجزائري أنظمة المعالجة الآلية للمعطيات محلا لجريمة الدخول غير المصرح به دون تعريف محدد لها في قانون العقوبات، و بالرجوع إلى قانون القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال نجد أنه استخدم مصطلح المنظومة المعلوماتية وعرفها بأنها نظام منفصل أو أنظمة متصلة ببعضها تقوم بمعالجة آلية للبيانات تنفيذا لبرنامج معين، ويمكن الإستناد إلى هذا التعريف لأن الجريمة تطال في الغالب كل ما تشمله أنظمة المعلومات.[19]

وإن كان المشرع السعودي قد جعل محل الجريمة مفصلا بأن عرف في المادة الأولى من نظام مكافحة الجريمة المعلوماتية النظام المعلوماتي بأنه:" مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية"، ثم عرف الشبكة المعلوماتية والحاسب الآلي وبرامجه و الموقع الإلكتروني وإن كانت كلها تدخل ضمن النظام المعلوماتي الذي يجمع أنظمة الحاسبات والإتصالات إلا أن هذا التفصيل قد يحول دون تضييق التفسير وإفلات المجرمين.[20]

ثانيا: السلوك الإجرامي

إن كان الدخول غير المصرح به يقوم بإتيان أفعال قوامها البحث والوصول إلى المعلومات باستخدام طرق آلية وتقنية، فإن المشرع الفرنسي لم يحدد وسيلة الدخول إلى النظام وكذلك فعل المشرع الجزائري، وعليه يجوز أن ترتكب الجريمة بأية وسيلة كانت.

تختلف الوسائل التي من الممكن اللجوء إليها لتحقيق الدخول غير المصرح به وتفترض جميعها قدرا من المعرفة بتقنيتي الحاسبات و الإتصالات وإن كانت تتراوح في مداها، ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل النظام أو فتح برنامج تشغيله، وأحيانا أخرى يتطلب الحصول على شفرات خاصة كما يمكن الدخول إلى النظام من خلال برنامج يتم دمجه في أحد البرامج الأصلية للنظام المستهدف حيث يعمل على تسجيل شفرات المستخدمين الشرعيين.[21]

أثار تحديد الهدف الذي يعقب عملية الدخول خلافا أظهرته النصوص القانونية المختلفة التي تناولت الجريمة.

حدا المشرع الجزائري حدو المشرع الفرنسي في تجريمه لمجرد الدخول غير المصرح به في المادة 394 مكرر[22] أيا كانت النتيجة التي تعقبه، وكان موفقا في اتجاهه كونه أحاط نظام المعالجة الآلية بضمانات فعالة تحميه من الإختراق.

وقد نصت على ذلك أيضا المادة 3 من وثيقة الرياض للنظام الإسترشادي الموحد لمكافحة جرائم تقنية المعلومات لدول الخليج العربية،[23] أما عن نظام مكافحة جرائم المعلوماتية السعودي فقد ذهب في مادته الثالثة إلى ما ذهب إليه المشرع الإنجليزي بتجريم الدخول غير المصرح به فقط في الحالات التي يكون الغرض منه إرتكاب إعتداء آخر،[24] فلا يجرم الدخول غير المشروع إلا إذا ارتكب من أجل حذف البيانات أو تدميرها أو تغييرها أو نشرها أو للحصول على معلومات الأمر الذي يجعل الفعل خارج نطاق التجريم في الحالات التي يتم الدخول و لا تحدث تلك النتائج لصعوبة اثبات سبب دخول الجاني.

لا تخفى الأهمية التي يحظى بها تجريم الدخول المجرد بغض النظر عما يعقبه من نتائج وذلك لما تنطوي عليه هذه الجريمة من خطورة في حد ذاتها كما أنها تعد مفتاحا لباقي الإعتداءات، وهو ما انتهجته غالبية التشريعات.

ثالثا: النتيجة الإجرامية.

باستثناء بعض التشريعات التي تربط قيام جريمة الدخول غير المشروع بحدوث نتيجة معينة فإن معظم التشريعات التي جرمت الدخول غير المصرح به اعتبرته من جرائم السلوك ولم تشترط حدوث نتيجة ما لإكتمال الركن المادي، في حين جعلت من الجرائم التي قد ترتكب بعد هذا الدخول ظروفا تجعل العقوبة أكثر تشديدا وهو ما فعله المشرع الجزائري وكذا الفرنسي حيث جرما الدخول المحض إلى أنظمة المعلومات ثم أوردا صورا لتشديد عقوبة الفعل حصراها في حذف أو تغيير المعطيات أو تخريب النظام أما التعامل في معطيات متحصلة من هذه الجرائم كتوفيرها ونشرها فاعتبراها جرائم مستقلة وهو الإتجاه الأنسب لحصر مختلف أنواع السلوك الإجرامي المصاحب لفعل الدخول المجرم.

المطلب الثالث: الركن المعنوي.

جريمة الدخول غير المصرح به من الجرائم العمدية التي يقوم ركنها المعنوي على ضرورة توافر القصد الجنائي، وتنسحب على هذا الركن تلك الإختلافات المتعلقة بالسلوك الإجرامي بحكم ارتباطه الشديد بعناصر الركن المادي.

أولا: القصد الجنائي العام.

يقوم هذا القصد على توافر عنصري العلم والإرادة بمعنى علم الجاني بأن دخوله إلى النظام غير مشروع وأن فعله ينصب على نظام للمعلومات إضافة إلى اتجاه إرادته السليمة إلى إتيانه ولا يثير ذلك أية إشكالات إذ تبقى جريمة الدخول غير المصرح به قائمة سواء كانت مقصودة في ذاتها أو ارتكبت باعتبارها وسيلة لتحقيق جرائم أخرى.

ثانيا: القصد الجنائي الخاص.

لا بد أن يتجه قصد الجاني إلى ارتكاب فعل الدخول إلى نظام المعلوماتية ويعتبر ذلك كافيا لاكتمال الركن المعنوي بالنسبة للتشريعات التي تجرم الدخول المحض كالتشريعين الجزائري والفرنسي، أما عن التشريعات التي لا تجرم الفعل إلا إذا اقترن بنية ارتكاب

فعل آخر كالتدمير أو الحصول على المعلومات فلا بد من توافر هذا القصد الخاص ويعرقل هذا الإقتران الذي اشترطته بعض التشريعات متابعة الجناة الذين يكون دخولهم غير المشروع من باب الهواية أو استعراض الملكات وإثبات القدرات.[25]

خاتمـــة

تعتبر الجهود التي بذلتها الدول في سن تشريعات بغرض التصدي لإجرام المعلوماتية الذي تفوق خسائره بكثير ما يمكن أن ينجم عن تفشي غيره من الإجرام خطوة مهمة رغم ما يعتريها من نقائص قد تكون محلا للتعديل ورغم ما يميزها من اختلافات هي مدعوة لتلافيها سعيا لتسهيل متابعة المجرمين لا سيما وأنها من الجرائم العابرة للحدود.

تنبع أهمية التصدي لجريمة الدخول غير المصرح به من كونها الفعل الذي يقود إلى اقتراف باقي أنواع الإعتداءات والمدخل الرئيسي إليها، إذ في تجريمه الحد مما يعقبه من أشكال للإجرام المعلوماتي.

وقد خلصنا من خلال هذه الورقة إلى ما يلي:

- صعوبة التعاون الدولي بسبب إختلاف النصوص التشريعية المجرمة لفعل الدخول غير المصرح به، وأهمية توحيد النصوص.
- تثمين جهود مختلف الجهات العاملة على وضع قوانين استرشادية وضرورة العمل بها.
- أهمية إعادة النظر في القوانين السارية وتعديلها بما يكفل عدم تنصل الجناة من عقوباتها.
- أهمية تفصيل الشروط المتعلقة بالسلوك المجرم كإدراج تجريم الدخول المتجاوز لحدود التصريح.
- ضرورة تجريم الدخول المحض الذي لا تعقبه أية نتيجة ولا يقترن به قصد خاص لاقتراف جريمة أخرى لانطواءه على الخطورة في حد ذاته بالنسبة لكافة التشريعات تسهيلا للتعاون الدولي في التصدي له.
- ضرورة تشديد العقوبة في الحالات التي تعقب الدخول غير المصرح به جرائم أخرى.
- توسيع محل الجريمة ليشمل كافة أنواع الدخول غير المصرح به إما باستعمال مصطلحات شاملة تتسع لما قد يستجد أو بتفصيل ما يمكن اعتباره محلا.

- الحاجة إلى تجريم إعتراض أنظمة المعلومات بنصوص خاصة تجنبا للتفسير الموسع للنصوص ومنعا للتنصل من الجريمة.

المراجع

1. أنظر مزيدا من التعريفات الفقهية لدى بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية للمعطيات، منشورات الحلبي الحقوقية، الطبعة الأولى2012، ص178 .
2. أنظر المادة 394 مكرر من قانون العقوبات الجزائري،المادة 1/323 من قانون العقوبات الفرنسي، المادة الأولى من القانون الانجليزي الخاص بإساءة استخدام الحاسبات الآلية لعام 1990، المادة 1030 (أ) من القانون الفيدرالي لإساءة استخدام الحسابات الآلية في الولايات المتحدة الأمريكية، المادة 1/342 من قانون العقوبات الكندي.
3. الدخول غير المشروع هو دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها" المادة 7/1من نظام مكافحة جرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7 هـ، و المصادق عليه بموجب المرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ.
4. يشير بعض الفقه إلى حالة السماح بالدخول إلى جزء محدد من النظام دون غيره عند استخدام البطاقات البنكية الممغنطة فحامل هذه البطاقة ليس له الحق في الدخول سوى إلى أحد الأجزاء التي تتكون منها الذاكرة التي يطلق عليها ذاكرة مستخدم البطاقة، نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية بيروت، لبنان، الطبعة الأولى، 2005، ص 338.
5. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية مصر، 2006، ص 151.
6. تتلخص وقائع القضية في قيام طالب أمريكي يدعى(robert morris) باطلاق برنامج خبيث (verus) يتاريخ 1988/08/02 عبر الانترنت عرف باسم دودة مورس أدى إلى إصابة ما يفوق 6 آلاف جهاز يرتبط معها حوالي 60000 نظام معلوماتي وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي 100 مليون دولار فضلا عن الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة وقد حكم على مورس بالسجن 3 سنوات إضافة إلى الغرامة المقدرة ب 10 آلاف دولار رغم دفعه بأنه لم يقصد تعطيل تلك الأنظمة وإحداث الضرر.

أنظر في هذا الشأن منير محمد الجنبيهي وممدوح محمد الجنبيهي،أمن المعلومات الإلكترونية، دار الفكر الجامعي الاسكندرية 2005.

7. تتلخص وقائع القضية الأولى (DPP V - Bingell) في قيام شرطيين بالدخول إلى النظام المعلوماتي الخاص بالإدارة التابعين لها للحصول على بعض المعلومات لأغراض لا تتعلق بعملهما. وقدما للمحاكمة بتهمة الدخول غير المصرح به إلى النظام المعلوماتي، تطبيقاً للمادة الأولى من قانون إساءة استخدام الحاسبات الآلية لعام (1991). و قد أدانت محكمة أول درجة المتهمين بتهمة الدخول غير المصرح به إلى النظام المعلوماتي وقد ألغت محكمة الاستئناف الحكم محكمة وذهبت إلى أن المتهمين يملكان الحق في الدخول إلى النظام المعلوماتي، وأن استخدام هذا الحق في غرض غير مشروع لا ينفي أن الدخول مصرح به. وقد ذهبت المحكمة أيضاً إلى أن الفقرة الخامسة من المادة 17 من القانون سالف الذكر و التي تحدد أن الدخول غير مصرح به إذا كان الشخص الذي قام بالدخول لا يملك سلطة على النظام و لا على تنظيم الدخول إليه ، ولم يحصل على تصريح ممن له هذه السلطة،لا تنطبق على المتهمين حيث أنهما بحكم عملهما لهما الحق في السيطرة على النظام و الدخول إليه.

– أما القضية الثانية (RV-Bow Magistrate and allison) فتتعلق بطلب تقدمت به حكومة الولايات المتحدة الأمريكية إلى المملكة المتحدة لتسليم إحدى العاملات بشركة أمريكان أكسبرس، لقيامها بالدخول إلى النظام المعلوماتي الخاص بالشركة للحصول على بعض البيانات الخاصة ببعض العملاء لأسباب لا تتعلق بالعمل.

و قد ذهبت محكمة الاستئناف الإنجليزي إلى أن الفعل الذي قامت به المتهمة لا يشكل جريمة وفقاً للقانون الإنجليزي، حيث أنه يشترط لانطباق المادة الأولى من قانون إساءة استخدام الحاسبات الآلية أن يكون الدخول غير مصرح به و هو ما لم يتحقق في هذه الحالة. حيث أن لهذه الموظفة الحق في الدخول إلى النظام المعلوماتي الخاص بالشركة لأسباب تتعلق بعملها، حتى لو استغلت هذا الدخول متجاوزة حدوده.

8. نائلة عادل محمد فريد قورة، المرجع السابق، ص 340 .

9. تدور وقائع هذه القضية في قيام المدعى عليه بإغراء العديد من موظفي المدعي، بمن فيهم موظفاً يدعى (Eric Leland) الذي كان على علم بكيفية الدخول إلى خطط العمل السرية للمدعي وأسراره التجارية. وقبل ترك هذا الموظف للشركة قام بإرسال العديد من هذه الأسرار التي تخص المدعي و المعلومات المملوكة له إلى المدعى عليه عبر شبكة المعلومات. تمت محاكمة هذا الموظف على أساس أنه قد تعمد الدخول إلى نظام المدعي انتهاكا لتشريع الدخول غير المصرح به الفيدرالي، وقد تبنت المحكمة وجهة النظر التي تقضي بأن التصريح الممنوح للعاملين ينتهي– وبدون علم المدير– إذا نال مصالح مضادة، أو إذا كان الفاعل مذنباً

بشكل أو بأخر بإخلال خطير لولاءه للمؤسسة، أنظر: محمد خليفة، المرجع السابق، ص 153 .

10. تنص المادة الأولى من قانون إساءة استخدام الحساب الآلي الصادر عام 1990 على ما يأتي:
« AP oron is guilty ofan offence if :
(one) he course a computer to perform any function with the intent to recure accento any program or data held in any computer.
(tow) the acen he intends to recure unauthorired; and
(three) he now at the time when he causes the computer to perform the function that this is the care.

11. نائلة عادل محمد فريد قورة، المرجع السابق ص 327.

12. المادة 76 (د) من قانون العقوبات الاسترالي الصادر عام 1989 تعاقب كل من يقوم بمساعدة وسيلة اتصالها تديرها أو تقدمها الدولة بالدخول عمدا أو بدون تصريح إلى معطيات معلوماتية تم تخزينها داخل الحاسب الآلي.

13. تنص المادة 321/1 من قانون العقوبات الفرنسي على ما يلي:
« le fait d'accéder ou de maintenir, frauduleusement, dans tout ou partie d'un système de troitement automatisé de donnée est puni d'un an d'emprison-nement et de 100.000 F d'amende. L'orsqu'il en est résulté soit la supréssion ou la modification de données peins est de deux ans d'emprisonnement et de 100.000 F d'amende ».

14. نائلة عادل محمد فريد قورة، المرجع السابق، ص 323.

15. united states code, title 18,part 1, chapter 47,subsection 1030, published at: https://www.law.cornell.edu/uscode/text/18/1030 .

16. جاء في المادة (1030) أنه يعاقب كل من يتصل عن علم وبصورة غير مرخصة أو اتصل بصورة مرخصة واستغل هذا للحصول على معلومات سرية تابعة للحكومة الأمريكية تتعلق بالأمن القومي بهدف الإضرار بالولايات المتحدة الأمريكية،أوالحصول على معلومات تتبع مؤسسات مالية بعقوبات تصل إلى الحبس مدة لا تزيد عن عشرين عاما، أنظر في ذلك:
محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع عمان الأردن، 2004، ص 86.

17. يماثل ما ورد بقانون الولايات المتحدة الأمريكية ما تضمنه كل من القانون الاسترالي والسويدي والهولندي والبرتغالي والكندي.

18. تنص المادة 394 مكرر من القانون 15/04 قبل تعديله على ما يلي:
"يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.
تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.
وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج."
19. المادة 2/ ب من القانون رقم 09-04 مؤرخ في 2009/06/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما.
20. أنظر المادة 1 و3/3 و 2/4 و 2/7 من نظام مكافحة جرائم المعلوماتية السعودي السابق ذكره.
21. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي،الإسكندرية، الطبعة الأولى، 2006، ص 356.
22. الأمر 66-156 المؤرخ في 1966/6/8 المتضمن قانون العقوبات الجزائري المعدل والمتمم، منشور على الموقع الإلكتروني للجريدة الرسمية على الرابط : http://www.joradp.dz/TRV/APenal.pdf.
23. وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات الصادر عن دول مجلس التعاون الخليجي المعتمدة في 2012/12/25 بالبحرين، منشورة على موقع المجلس على الرابط: file:///C:/Users/user/Downloads/1373542617%20(1).pdf .
24. COMPUTER MISUSE ACT 1990, published on THE OFFICIAL HOME OF UK LEGISLATION at http://www.legislation.gov.uk/ukpga/1990/18/contents
25. أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي، مجلة دراسات المعلومات، العدد 14، ماي 2012،ص 18.