



جامعة دمشق
كلية الحقوق
قسم القانون الجزائي

جريمة الدخول إلى منظومة معلوماتية

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون الجزائي

إعداد الطالب

أحمد قاسم

إشراف الدكتور

حسام الدين ساريج

المدرس في قسم القانون الجزائي

٢٠١٥\٢٠١٤

الشكر والتقدير

الحمد لله رب العالمين والصلاة والسلام على جميع الأنبياء والمرسلين وبعد

.....

لا يسعني بعد أن وفقني الله على إتمام هذه الرسالة المتواضعة إلا أن أتقدم بخالص شكري وتقديري إلى كل من ساعدني في إنجاز هذا العمل وكان سبباً في إتمامه، فجزاهم الله عني خير جزاء.

وأخص بالشكر أستاذي الدكتور حسام الدين ساريج الذي كان له فضل الإشراف على هذه الرسالة، وحسن المتابعة، والرعاية.

كما أتقدم بخالص شكري واحترامي إلى السادة أعضاء لجنة المناقشة الذين تفضلوا مشكورين بقبول الاشتراك بمناقشة هذه الرسالة وإبداء الملاحظات القيمة التي لها الأثر الكبير في إثراء الرسالة وتقويمها.

كما أتقدم بالشكر والتقدير إلى أعضاء الهيئة التدريسية في كلية الحقوق عامة، وقسم القانون الجزائي خاصة لما بذلوه من جهد وعطاء.

كما أتقدم بالشكر والامتنان إلى من مدّ لي يد العون والمساعدة في إنجاز هذا العمل.

الإهداء

إلى أمي

إلى أبي

إلى أختي

إلى أصدقائي

أهدي هذا العمل المتواضع.....

مقدمة

الجريمة ظاهرة قديمة قدم البشرية، تتغير وتتغير تبعاً لتغير الزمان والمكان، والدوافع والعوامل والظروف المؤدية إليها، فهناك جرائم ماسة بالأشخاص كالقتل والإيذاء والقدح والذم وغيرها، وجرائم ماسة بالأموال كالسرقة والاحتياز، وجرائم ترتكب ضد أمن الدولة كالخيانة والتجسس.

كما أنّ التغيرات التي يتعرض لها العالم في الوقت الراهن، وما واكبتها من تطورات خطيرة سببتها النزاعات المادية وحب التملك وتراجع القيم الأخلاقية، أدت إلى ظهور أنماط مستحدثة من الإجرام كان لها بالغ الأثر على المجتمعات جميعها وفي المجالات جميعها.

وإنّ التطورات التي واكبت العصر الصناعي، وما تبعه من تطورات في مجال تكنولوجيا المعلومات وتقنية الاتصالات، ساهمت في ظهور المعلومات كقيمة جديدة في الاقتصاد العالمي، وأصبحت مورداً لا يقل أهمية عن الموارد الأخرى، وأضحت المعلومات السمة الأساسية للمجتمعات الحديثة في جوانبها كافة الاقتصادية والاجتماعية والسياسية والثقافية، وهو ما دفع بعض الفقهاء إلى تسمية العصر الذي نعيش فيه بعصر المعلومات^(١).

وإنّ هذه التغيرات المتلاحقة التي طرأت على المجتمعات أدت إلى ظهور أنماط مستحدثة من السلوك الإجرامي، نتيجة إساءة استغلال وسائل التكنولوجيا الحديثة لتحقيق أغراض غير مشروعة، ولقد تعددت التسميات التي أطلقت على هذه الظاهرة الإجرامية الناشئة في بيئة المعلومات، فسميت: إساءة استخدام الحاسب، احتيال الحاسب، جرائم الحاسب، الجرائم المرتبطة بالحاسب، جرائم التقنية العالية، الجرائم

(١) بيل جيتس، المعلوماتية بعد الانترنت، ترجمة عبد السلام رضوان، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ١٩٩٨، ص ٣٥.

الالكترونية، جرائم الهاكرز أو الاختراقات، جرائم الانترنت، جرائم نظم المعلومات، الجرائم المعلوماتية، و Cyber Crime^(١).

وقد نتج عن هذه الظاهرة الإجرامية الحديثة الناشئة في بيئة المعلومات آثاراً اقتصادية هائلة، وتكبد الاقتصاد العالمي خسائر جسيمة فاقت الخسائر التي تترتب على جرائم الأموال مجتمعة^(٢)، كما تميّز هذا النوع الجديد من الإجرام بأنه عابر للحدود، حيث أنّ تطور تقنيات الاتصالات الحديثة سهلت عمليات نقل المعلومات وإتاحتها على نطاق واسع مما جعل العالم يبدو كقرية كونية صغيرة^(٣)، وأضحت الجرائم المعلوماتية تتم في فضاء الكتروني هو عبارة عن شبكة اتصالات لا متناهية وغير مجسدة أو مرئية، ومتاحة لأي شخص حول العالم، وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، وله وجود حقيقي وواقعي، لكنه غير محدد بمكان، كما أنّ ارتباط هذا النوع من الإجرام بالبيئة المعلوماتية جعل أمر الكشف عنه أو تتبع مصدره أو التنبؤ بوقوعه أو بشخص فاعله أمراً بالغ الصعوبة، وهذه الأخطار المتزايدة عن هذا النوع الجديد من الإجرام جعلت دول العالم قاطبة تسعى للتصدي له.

وإنّ هذه الخصائص التي اتسم بها الإجرام المعلوماتي شكلت تحدياً أمام النظام القانوني القائم، ولا سيما قانون العقوبات الذي يحكمه مبدأ شرعية الجرائم العقوبات والتفسير الضيق للنصوص القانونية، وهذا ما دفع كثير من الدول إلى سن تشريعات لمواجهة هذا النوع الجديد من الإجرام، وكان في مقدمتها السويد، وتلتها الولايات المتحدة الأمريكية، ثم المملكة المتحدة وكندا وفرنسا ومعظم الدول الأوروبية الأخرى، وفي هذا الإطار أصدر المشرع السوري قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بالمرسوم التشريعي رقم ١٧ لعام ٢٠١٢.

(١) د. أيمن فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٧، ص ٧٥.

(٢) المرجع ذاته، ص ٩٩.

(٣) بيل جيتس، المرجع السابق، ص ٣٥٨.

وجريمة الدخول التي نحن بصدد دراستها تعد من أبرز مظاهر الإجرام المعلوماتي، حيث أن معظم الاعتداءات المعلوماتية تتطلب لبدءاً الدخول إلى النظام، وعرفت إعلامياً في السنوات الأخيرة باسم "القرصنة"، وهي تعني الوصول إلى المعلومات من قبل أشخاص غير مصرح لهم بالوصول إليها أو من قبل موظفين لا يملكون صلاحية ذلك^(١)، أو بعبارة أخرى هي إساءة استخدام الحاسبات الآلية من قبل أشخاص غير مصرح لهم باستخدامها أو الوصول إليها لتحقيق أغراض غير مشروعة، أو لإشباع الرغبة في التحدي، أو حب الظهور والاستطلاع، أو لكشف أوجه القصور في أنظمة الحماية الفنية^(٢).

وتتجلى خطورة الدخول في أنه الوسيلة التي يتم من خلالها التسلل إلى الأنظمة، والتي تتيح للفاعل الوصول إلى المعلومات المخزنة أو تعديلها أو إتلافها، أو استخدام موارد النظام لتحقيق أغراض غير مشروعة، أو عرقلة عمل النظام وتخفيض إنتاجيته، أو حرمان المستخدمين الشرعيين من الخدمات التي يقدمها النظام.

وتزداد خطورة هذه الأنشطة في الحالة التي تتعلق فيها المعلومات التي تم الوصول إليها ببعض المصالح الحيوية، كالمعلومات التي تتعلق بالأمن القومي أو الأنشطة الاقتصادية لبعض القطاعات، أو إذا ترتب على الدخول انقطاع الخدمات عن

(1) Scot Law Com. No 106, Report on Computer Crime.Cm.174 1987, para.2.7, Retrieved 6\June\2014 from: http://www.scotlawcom.gov.uk/download_file/view/391

(2) Council of Eroup, Computer Related Crime: Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, Strasbourg 1990, p. 50, Retrieved 2\Apr\2014 from: http://www.oas.org/juridico/english/cyber_links_coe.htm

أحد القطاعات التي تشكل فيها وقت المعالجة أمراً هاماً وحيوياً كموائى تنظيم حركة النقل الجوي أو أسواق تداول الأسهم^(١).

وتعدُّ الحماية الفنية للأنظمة من أهم الوسائل التي يتم من خلالها التصدي لحالات الاختراق، إلا أنَّ الوقائع قد أثبتت أن هذه القواعد مهما بلغت من درجة التطور والتعقيد فإنَّها لم تمنع من وقوع الاعتداءات في حالات كثيرة، ويكفي للتدليل على ذلك ذكر أنَّ وكالة الطيران والفضاء الأمريكية "ناسا" تخصص سنوياً أكثر من ٥٨ مليون دولار لأمن تكنولوجيا المعلومات، وعلى الرغم من ذلك فقد تعرضت أنظمتها في عامي ٢٠١٠ و ٢٠١١ لـ ٥٤٠٨ حالة اعتداء، أدت إلى إعاقة عمل العديد من أجهزتها الحاسوبية وإرباك كبير في أعمالها وسرقة معلومات حساسة تجاوزت قيمتها ٧ مليون دولار^(٢).

وعلى الرغم من الأخطار التي تترتب على عمليات الدخول فقد ثار جدل واسع في الفقه بين مؤيد ومعارض للتدخل القانوني في تجريم الدخول، فذهب اتجاه إلى ضرورة المواجهة القانونية لأفعال الدخول غير المصرح به، وذلك لقصور قواعد الحماية الفنية عن منع الاعتداءات على المعلومات، ولتخفيض التكاليف المرتفعة التي يتكبدها أصحاب الأنظمة في محاولة منع الاختراقات، ولحماية الاستثمارات في مجال المعلوماتية، ذلك أن الرغبة في الاستثمار تتخفض إذا ما تمت إعاقة هذه الأنظمة بشكل كبير من خلال الاعتداءات المتكررة وتمَّ الشعور بانعدام الأمن بين مشغليها،

⁽¹⁾ Global Information Assurance Certification Paper, Retrieved 28\Mar\2014 from: <http://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264>

⁽²⁾ Martin. Paul, NASA Cybersecurity: An Examination of the Agency's Information Security, p. 1, Retrieved 10\Mar\2015 from: http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

ولتشكل رادعاً تجاه الأشخاص الذين يدخلون إلى الأنظمة لتحقيق أغراض غير مشروعة.

وذهب اتجاه آخر إلى عدم ضرورة المواجهة القانونية لحالات الدخول، ذلك لأنه في حالات الدخول المجرد التي تتم دون نية لارتكاب اعتداءات لاحقة لا تعدو كونها مجرد استعراض لملكات ذهنية أو فنية للفاعل، أو محاولة منه للكشف عن نقاط الضعف في الإجراءات الفنية التي تحمي المعلومات وهو ما لا يمكن عده جريمة، كما أنّ حالات الدخول التي لا تترافق مع ارتكاب اعتداءات لاحقة لا يمكن الكشف عنها، كما أنّها حتى لو تم اكتشافها فإنه لا يمكن تتبع مصدرها أو معرفة مرتكبها، وتبعاً لذلك فإنّ تجريم الدخول سيكون أمراً عبثياً لا فائدة تُرجى منه، إلا أنّ هذه الحجج لم تشكل عائقاً يحول دون ضرورة تجريم الدخول غير المشروع، وذلك لأنّ الدخول أياً كان الدافع إليه لا يغير من حقيقته أنّه يشكل تعدياً على المعلومات وقد تمّ دون حق، كما أنّ النية لارتكاب اعتداءات خطيرة قد تتولد في المرحلة اللاحقة للدخول، فضلاً عن ذلك فقد بينت الوقائع أنّه قد تمّ الكشف عن العديد من عمليات الدخول في عدة حالات، وتمّ الاستعانة في عدة مرات في سبيل ذلك بأنظمة الاتصالات العامة وبالإجراءات التقنية التي تمّ اتخاذها داخل الأنظمة التي تمّ الدخول إليها⁽¹⁾.

وبعيداً عن هذا الجدل الفقهي فقد اتجهت عدة تشريعات إلى تجريم الدخول غير المصرح به، وكان في مقدمتها القانون السويدي، كما جرم المشرع السوري في المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الدخول غير المشروع إلى منظومة معلوماتية.

(1) Law Com. No.186, Computer Misuse. Cm.819 1989, paras.2.14,2.17,2.18,2.19,2.24, Retrieved 6June\2014 from: <http://www.bailii.org/ew/other/EWLC/1989/186.pdf>

- ١ - إشكالية البحث:

جوهر الدخول هو الوصول إلى المعلومات، وهو يعد مرحلة ضرورية لارتكاب الجرائم المعلوماتية التي تتطلب ابتداءً الوصول إلى النظام، كما أنه من ناحية أخرى قد يقصد في ذاته بحيث لا يكون الغرض من الدخول ارتكاب اعتداءات لاحقة، وهذا ما أثار الخلاف حول الكيفية التي يتم فيها تجريم الدخول إلى النظام: فهل يتم تجريمه بوصفه الجريمة المعلوماتية الأساسية والتي تعد مقدمة لارتكاب جرائم أخرى؟ أو يتم تجريمه بوصفه حالة خطرة تهدد المعلومات؟ أو بقصر التجريم على بعض الحالات التي تكشف عن ازدياد الخطورة على المعلومات؟

وهنا برزت إشكالية البحث وتمحورت في: دراسة الدخول على ضوء القانون المقارن، وتحديد الإطار القانوني للجريمة، والذي يكفل نظاماً حمائياً أمثل لمواجهة أفعال الدخول غير المصرح بها، وأثارت هذه الإشكالية العديد من التساؤلات أهمها: حول ماهية المحل الذي ينصب عليه النشاط الإجرامي، ونوع الحق المحمي، ومفهوم نشاط الدخول وطبيعته ونطاقه، والأثر الذي يترتب عليه، ومفهوم الصفة غير المشروعة التي يسبغ بها، وصورة الإرادة الجرمية، تساؤلات عديدة ومتنوعة نثيرها جريمة الدخول يتعين علينا بحثها ووضع الإجابات الواضحة ما أمكن ذلك.

- ٢ - أهمية البحث:

إنَّ اهتمامنا بهذا الموضوع يرجع إلى عدة أسباب علمية وعملية:

الأسباب العملية: تقشي ظاهرة الإجرام المعلوماتي على المستوى الدولي والداخلي، وما يترتب عليه من أضرار جسيمة تؤثر على مجالات الحياة كافة، وظهور فئة من المجرمين امتنعت الإجرام المعلوماتي، وكذلك إلى الأهمية المتزايدة لمواجهة ظاهرة الإجرام المعلوماتي، ومساسها بعصب الحياة الحديثة والمتمثل بالمعلومات.

أما بالنسبة للأسباب العلمية: ترجع إلى قلة الدراسات المتخصصة على المستوى الوطني.

٣ - أهداف البحث:

بناءً على ما تقدم فقد حاولنا من خلال هذه الدراسة إلى الوقوف على المشكلات التي تثيرها جريمة الدخول، واستخلاص النموذج القانوني لهذه الجريمة، بما يقدم نظاماً حمائياً أمثل لمواجهة الاعتداءات المعلوماتية.

٤ - صعوبات البحث:

واجهت هذه الدراسة العديد من الصعوبات كان أبرزها الصبغة الفنية للموضوع، فارتباط الجريمة محل الدراسة بتقنية المعلومات يتطلب الفهم الكامل لهذه التقنيات الحديثة، وهذا ما تطلب جهداً فنياً بالإضافة إلى الجهد القانوني، كما أنّ صعوبة الحصول على المراجع القانونية العربية التي تعالج الإجرام المعلوماتي، وحادثة هذه الظاهرة، وانعدام التطبيقات القضائية في المحاكم العربية، صعوبات أخرى اعترضت البحث وبالتالي كان لزاماً علينا اللجوء إلى القانون والفقه والقضاء المقارن في النظم القانونية للدول المتقدمة في مواجهة الإجرام المعلوماتي، للوقوف على ما تم التوصل إليه بخصوص ذلك.

٥ - منهجية البحث:

استخدمنا في بحثنا هذا المنهج التحليلي، بغية تحليل عناصر جريمة الدخول ومناقشة الإشكاليات التي تثيرها وإيجاد الحلول المناسبة لها، ومن ناحية أخرى لم نغفل عن الاستعانة بالمنهج المقارن في كثير من الحالات للمقارنة بين اتجاهات الدول السباقة في تجريم الدخول، وذلك للاستفادة وسد الثغرات التي اعترت تشريعنا الوطني من أجل تحكم أفضل في التجريم.

- ٦ - خطة البحث:

بناءً على ما تقدم فإنّه يمكن تقسيم موضوع الدراسة إلى فصلين، واستدعى هذا التقسيم ضرورة منطقية ومنهجية، تتمثل الأولى في أنّ تحديد محل الجريمة تسبق تحديد أركانها، أمّا الضرورة المنهجية تتمثل في السعي لتحقيق نوع من التوازن بين الفصلين.

وعلى هذا الأساس خصصنا الفصل الأول للتحديث موضوع جريمة الدخول، وقسمناه إلى مبحثين، تناولنا في المبحث الأول المحل المادي الذي يتحقق فيه نشاط الدخول، وتناولنا في المبحث الثاني فلسفة التجريم.

أمّا في الفصل الثاني فخصصناه لركني الجريمة، ولم نستطع في تحليلنا لهذه الأركان الخروج عما جرى العمل عليه من تقسيم الجريمة إلى ركن مادي وآخر معنوي، وتبعاً لذلك فقد قسمنا هذا الفصل إلى مبحثين، تناولنا في المبحث الأول الركن المادي لجريمة الدخول، وفي المبحث الثاني الركن المعنوي.

ثم أنهينا هذا البحث في النهاية بخاتمة تتضمن مجموعة من النتائج والاقتراحات التي توصلنا إليها.

وعليه سوف نقوم بدراسة موضوع جريمة الدخول من خلال:

الفصل الأول: موضوع الدخول.

الفصل الثاني: ركني الدخول.

الفصل الأول: موضوع الدخول

إنَّ موضوع جريمة الدخول ينطوي على شقين: أحدهما مادي ويتمثل بالمحل المادي الذي يتحقق فيه نشاط الدخول، والآخر قانوني ويتمثل بالحق أو المصلحة المراد حمايتها من خلال تجريم الدخول غير المشروع.

وتبعاً لذلك فإنَّ دراسة موضوع جريمة الدخول يتطلب بيان المحل المادي الذي يتحقق فيه نشاط الدخول، وتحديد المصلحة المراد حمايتها من خلال جريمة الدخول، وسنقوم بذلك من خلال المبحثين التاليين:

المبحث الأول: محل الدخول.

المبحث الثاني: المصلحة المحمية.

المبحث الأول: محل الدخول

محل جريمة الدخول هو الموضوع المادي الذي يتحقق فيه نشاط الدخول، ويتمثل في جريمة الدخول بالمعلومات الالكترونية، ولا يتاح للمعلومات هذا الوصف ما لم تكن جزءاً من نظام معلوماتي يتولى مهمة معالجة المعلومات، وتتباين التشريعات في تحديد المعلومات التي تشكل المحل المادي لجريمة الدخول، ويعود ذلك لاختلافها في تحديد نطاق هذه الجريمة.

وتبعاً لذلك سنتناول محل الدخول من خلال بيان الاتجاهات التشريعية في تحديد محل الدخول في المطلب الأول، ثم نتعرض لدراسة كل من المعلومات في المطلب الثاني، ونظام المعلومات في المطلب الثالث.

المطلب الأول: الاتجاهات التشريعية في تحديد محل الدخول

لم تنتهج التشريعات في سياق تحديدها لمحل الحماية الجزائية في جريمة الدخول نهجاً واحداً، وإنما يمكن تمييز اتجاهين في ذلك: أحدهما يوسع من نطاق محل الحماية ليشمل كلاً من المعلومات والأنظمة المعلوماتية التي تحتفظها وشبكات الاتصالات التي تربط بينها، وآخر يضيق من نطاق هذا المحل ليقصر على المعلومات والأنظمة التي تحتفظها دون أن يشمل شبكات الاتصالات، وسنتناول كلاً من هذين الاتجاهين فيما يلي:

أولاً: الاتجاه الموسع لمحل الدخول

من التشريعات التي أخذت بهذا الاتجاه القانون الأمريكي على المستوى الفيدرالي، والذي يجرم أفعال الدخول إلى كل من أنظمة الحاسبات الآلية والمعلومات التي تحتويها، وتشمل الحاسبات الآلية وفق هذا القانون كل جهاز إلكتروني أو مغناطيسي أو ضوئي أو كيميائي كهربائي أو جهاز لمعالجة المعلومات يقوم بعمليات منطقية وحسابية وكل وسيلة آلية لتخزين المعلومات وكل وسيلة للاتصالات تعمل

مباشرة أو جنباً إلى جنب مع هذا الجهاز، ووفقاً لهذا التحديد فإن الحاسبات الآلية تشمل كلاً من المعلومات وأنظمة الحاسبات الآلية وشبكات الاتصالات، إلا أن القانون الأمريكي خفف من هذا التوسع في محل الحماية من خلال وضع ضوابط محددة سواء فيما يتعلق بالمعلومات أو الأنظمة المعلوماتية، فقد تطلب أن تكون المعلومات المراد الحصول عليها تتعلق بالقضايا الإستراتيجية للدولة أو أمور الائتمان المالي، وبأن تتبع الأنظمة التي يتم الدخول إليها للحكومة الفيدرالية أو أن تكون متعلقة بأعمالها^(١).

ومن قبيل هذا الاتجاه أيضاً القانون الفرنسي الذي يجرم أفعال الدخول إلى نظم المعالجة الآلية للبيانات^(٢)، وعلى الرغم من أن هذا القانون لم يتضمن تعريفاً للنظام، إلا أن المناقشات السابقة لصدوره أحالت ذلك إلى التعريف الوارد في القانون المتعلق بالمعلوماتية وحماية الحريات ١٩٧٨ والذي يعرف المعالجة الآلية بأنها مجموعة العمليات التي تتم بأي وسيلة كانت وتتعلق بجمع وتسجيل وتجميع و تنظيم وتغيير واسترجاع وتخزين ونشر واستخدام المعلومات^(٣)، وعلى ذلك فإن محل الحماية يشمل كلاً من المعلومات والنظام الذي يحتويها والشبكة التي تربط بين عدة أنظمة.

وبعد القانون اليوناني من هذا الاتجاه أيضاً، فهو يجرم الدخول إلى البيانات المخزنة في الحاسب الآلي أو في الذاكرة الخارجية له أو التي تنتقل عن طريق شبكات الاتصالات السلكية أو اللاسلكية^(٤)، ومن التشريعات التي أخذت بهذا الاتجاه أيضاً القانون الإيطالي الذي يجرم الدخول إلى نظام الحاسب الآلي أو شبكات الاتصالات السلكية واللاسلكية^(٥)، والقانون النرويجي الذي يجرم الدخول إلى البيانات والبرامج التي

(١) المادة ١٠٣٠ و ١٠٣١ ح من القانون الفيدرالي الأمريكي لإساءة استخدام الحاسبات الآلية.

(٢) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

(3) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Chapitre Ier: Principes et définitions, Article 2, Retrieved 10\Mar\2014 from:
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

(٤) المادة ٢٣٧٠ من قانون العقوبات اليوناني.

(٥) المادة ٦١٥ من قانون العقوبات الإيطالي.

يتم تخزينها أو نقلها بالوسائل التقنية الالكترونية أو غيرها^(١)، والقانون الفنلندي الذي يجرم الدخول إلى نظام الحاسب الآلي حيث تتم معالجة البيانات أو تخزينها أو نقلها بواسطة الطرق الفنية الالكترونية^(٢)، وكذلك الحال في القانون البرتغالي الذي يجرم الدخول إلى نظام المعلومات وشبكة الاتصالات^(٣)، والقانون الألماني الذي يجرم الدخول إلى البيانات التي يتم تخزينها أو إرسالها إلكترونياً و مغناطيسياً أو في أي من الأشكال الغير مرئية مباشرة^(٤).

ثانياً: الاتجاه المضيق لمحل الدخول

يعد القانون الانكليزي أحد أبرز الأمثلة على هذا الاتجاه، فهو يجرم الدخول إلى البرامج والمعلومات التي يحتويها الحاسب الآلي^(٥)، وكذلك فإن القانون الهولندي يجرم الدخول إلى النظام الآلي لتخزين أو معالجة البيانات^(٦)، ومن التشريعات التي أخذت بهذا الاتجاه أيضاً القانون السويدي الذي يجرم الدخول إلى تسجيل لمعالجة البيانات الآلية^(٧)، والقانون السويسري الذي يجرم الدخول إلى نظام معالجة البيانات^(٨)، والقانون البلجيكي الذي يجرم الدخول إلى نظام الحاسب الآلي^(٩)، كما أن القانون السوري يجرم الدخول إلى المنظومة المعلوماتية أو الجهاز الحاسوبي أو الموقع الالكتروني^(١٠).

(١) المادة ١٤٥ من قانون العقوبات النرويجي.

(٢) القسم ٨ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(٣) المادة ٧ من القانون الجزائي لحماية المعلومات البرتغالي.

(٤) المادة ٢٠٢ أ من قانون العقوبات الألماني.

يمكن الاطلاع على هذه القوانين على الموقع الالكتروني:

& <http://www.legislationonline.org/documents/section/criminal-codes>

<http://www.cybercrimelaw.net/Cybercrimelaws.html>

(٥) المادة الأولى من قانون إساءة استخدام الحاسبات الانكليزي.

(٦) المادة ١٣٨ أ من قانون العقوبات الهولندي.

(٧) القسم ٩ من الفصل ٤ من قانون العقوبات السويدي.

(٨) المادة ١٤٣ من قانون العقوبات السويسري.

(٩) لمادة ٥٥٠ ب من قانون العقوبات البلجيكي.

(١٠) المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

ويبرز الاختلاف بين الاتجاهين في أنَّ الأول يعد شبكة الاتصالات التي تربط بين الأنظمة محلاً صالحاً لجريمة الدخول فيما لا يعد الاتجاه الثاني ذلك، ومن شأن هذا الاختلاف أن يؤدي إلى اعتبار أفعال اعتراض المعلومات المتداولة على الشبكة إحدى صور جريمة الدخول غير المصرح به وفق الرأي الأول فيما لا يعد الاتجاه الثاني هذا السلوك كذلك، ولذلك فإنَّ بعض التشريعات التي لا تعد الشبكة المعلوماتية من بين صور محل جريمة الدخول تلجأ إلى تجريم أفعال اعتراض المعلومات من خلال نصوص خاصة كما هو الحال في القانون السوري، والذي يجرم في المادة ١٨ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية أفعال الاعتراض والالتقاط غير المشروع للمعلومات المتداولة على منظومة معلوماتية أو الشبكة أو التنصت عليها^(١).

وعلى أي حال فإنه يمكن التمييز بين ثلاثة صور لمحل جريمة الدخول: الأولى هي النظام المعلوماتي، والثانية هي البرامج والمعلومات التي يخترنها النظام المعلوماتي، والثالثة هي شبكة الاتصالات المرتبطة بالنظام المعلوماتي.

(١) المادة ١٨ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

المطلب الثاني: المعلومات

أدى تطور الحاسبات الآلية كنتاج للتطور العلمي والتقدم التقني إلى تدخل أنظمة المعالجة الآلية في شتى مجالات الحياة، نظراً لما تتمتع به هذه الحاسبات من قدرة على تجميع أكبر قدر من المعلومات وتخزينها واسترجاعها ، وهذا ما أدى إلى ظهور المعلومات قيمة جديدة إلى جانب القيم الأخرى، والتي اكتسبت شيئاً فشيئاً طابعاً مالياً بعد أن كانت أحد مظاهر الحريات العامة، وأضحت المعلومات موضوعاً لجرائم جديدة ومنها جريمة الدخول.

هذا وقد استخدمت كلمة المعلومات استخداماً متبايناً بتباين المجالات حتى كادت تفقد وزنها الدلالي ما لم تكن مرتبطة بموضوعات اجتماعية وعلمية أو غيرها، وعلى الرغم من كثرة الاستخدام فلا نجد للمعلومات معنى متفقاً بشأنه، وإنما أصبحت التعريفات مجرد تعبير عن وجهة نظر أصحابها، وتكون مقبولة في بعض المجالات ومرفوضة في أخرى، وتم تقدير تعريفات المعلومات بما يزيد عن ٤٠٠ تعريف تعكس آراء مختلف المجالات^(١)، وسنحاول توضيح مجموعة من التعريفات فما يلي للوصول إلى المعنى الذي يتفق مع طبيعة جريمة الدخول.

أولاً: التعريف اللغوي للمعلومات

المعلومات من حيث مدلولها اللغوي مشتقة من المصدر علم، ولهذه المشتقات العديد من المعاني منها ما يتصل بالعلم أي إدراك طبيعة الأمور، والمعرفة أي القدرة على التمييز والتعليم والتعيين والإرشاد والتوعية والإبداع والشهرة والتمييز والتيسير....إلى آخر ذلك من المعاني المتصلة بوظائف العقل^(٢)، ومصطلح (information) هو المقابل الانكليزي للمعلومات، وهي كلمة انكليزية مشتقة من اللاتينية (information) والتي كانت تعني في الأصل الاتصال أو التلقي، ويوجد

(١) د. حشمت قاسم، مدخل لدراسة المكتبات وعلم المعلومات، مكتبة غريب، بدون مكان وسنة نشر، ص ١٤.

(٢) د. أحمد علي، مفهوم المعلومات في إدارة المعرفة، مجلة جامعة دمشق، المجلد الأول، العدد الأول، ٢٠١٢، ص ٤٧٨.

لها في اللغة العربية معنيين متقابلين متميزين وهما: الإعلام كعملية أو نشاط والمعلومات التي يتم الإعلام بها^(١)، وهناك مصطلح آخر للمعلومة مشتق من التصور (informatum) والذي يعني الرسم أو التخطيط، وهذين المعنيين وجهان لحقيقة واحدة، إذ أن الأول يوضح الجانب الحركي للمعلومة و الثاني يوضح الجانب الوصفي لها^(٢)، ويعرف المنجد المعلومة بأنها كل ما يعرفه الإنسان عن قضية أو حادث، أما معجم اللغة العربية المعاصرة فعرفها بأنها أخبار وتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور واتخاذ القرارات^(٣).

ثانياً: المعلومات اصطلاحاً

المصطلح ما اصطلح عليه القوم، وتتمثل التعريفات الاصطلاحية في ما ورد في المعاجم والموسوعات المتخصصة، ومن التعريفات الاصطلاحية للمعلومات التعريف الذي ورد في المعجم الموسوعي في الكمبيوتر والإلكترونيك بأنها معطيات تم تسجيلها أو تصنيفها وتنظيمها وتفسيرها ووصفها في إطار معين لإظهار معانيها^(٤)، كما عرفها قاموس البنهاوي الموسوعي بأنها الحقائق الموصلة أو رسالة تستخدم لتمثيل حقيقة أو مفهوم استخدام وحدة وسط بيانات ومعناه أو هي عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة^(٥)، أما المعجم الموسوعي لمصطلحات المكتبات والمعلومات فعرفها بأنها البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد لأغراض اتخاذ القرارات ، أي البيانات التي أصبح لها قيمة بعد تحليلها أو

(١) د. حشمت قاسم، المرجع السابق، ص ١٢.

(٢) رصاع فتحية، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة ماجستير، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، ٢٠١١-٢٠١٢، ص ٢٦، استخرج بتاريخ ٢٠ كانون الثاني \ ٢٠١٤ من الموقع الإلكتروني: http://scholar.najah.edu/sites/default/files/all-thesis/legal_protection_of_computer_programs.pdf

(٣) د. أحمد مختار محمد، معجم اللغة العربية المعاصرة، المجلد الثاني، عالم الكتب، القاهرة، ٢٠٠٨، ص ١٤٢٩.

(٤) أندريه لوغارف، المعجم الموسوعي في الكمبيوتر والإلكترونيك، ترجمة د. عبد الحسن الحسيني، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، الطبعة الثانية، ١٩٨٨، ص ٣٧٢.

(٥) د. شعبان خليفة، قاموس البنهاوي الموسوعي في مصطلحات المكتبات والمعلومات، دار العربي للنشر والتوزيع، القاهرة، ١٩٩٠، ص ٨.

تفسيرها أو تجميعها في شكل ذي معنى وإلى يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل، وعرفها أيضا بأنها المقومات الجوهرية في أي نظام للتحكم^(١).

ثالثاً: المعلومات فقهاً

عرف أحد الفقهاء المعلومات بأنها المعرفة المتحصلة بشأن حقيقة أو ظرف معين^(٢)، وعرفها آخر بأنها التعبير الأول وصياغة مصممة لجعل الرسالة مقابلة للنقل أو الإبلاغ^(٣)، وانتقد جانب من الفقه هذا التعريف لاشتراطه وصول الرسالة إلى المتلقي، ولذلك فقد تم اقتراح تجاهل هذا الشرط وذلك من خلال اعتبار المعلومات شيء، ويكون ذلك عندما يكون لها وجود في العالم الخارجي من خلال الدعامة المادية التي تجسدها كالإشارات والحروف^(٤)، وانتقد البعض هذا الاتجاه لأنه يؤدي إلى تلاشي المفهوم الحسي للمعلومة والتركيز على النموذج الذي لا يشكل هدفاً عندما يتعلق الأمر بالمعلومات، ولأنه يتجاهل ضرورة وجود وسيلة للاتصال، ولذلك فقد تم تعريفها بأنها عمل من أعمال الاتصال للحقائق والأفكار^(٥)، أو هي فعل التواصل الذي يبلغ المعرفة^(٦).

(١) أحمد محمد الشامي وسيد حسب الله، المعجم الموسوعي لمصطلحات المكتبات والمعلومات، دار المريخ، الرياض، ١٤٠٨-١٩٨٨، ص ١.

(2) Losee. Robert, 1988, A Discipline Independent Definition of Information, J. of the American Society for Information Science, U. of North Carolina-Chapel Hill, P. 3, Retrieved 22\Jun\2014 from: <http://www.ils.unc.edu/~losee/book5.pdf>

(3) Vivant. Michel, La privatisation de l'information par la propriété intellectuelle, Revue internationale de droit économique, 2006, 20 4, p. 363, 22\Jun\2014 en publié surle site: http://www.cairn.info/resume.php?ID_ARTICLE=RIDE_204_0361

(4) Ibid, p. 363

(5) Ibid, p. 400

(6) Geiger. Christophe, La privatisation de l'information par la propriété intellectuelle, Revue internationale de droit économique, 2006, 20 4, p. 400,

ويرى بعض الفقهاء أنَّ المعلومات ليست مقصورة على الكائنات الحية والجانب الأساسي لها ليس بناء العقل البشري وإنَّما هي تشكل ظاهرة كونية، ولذلك تم تعريفها بأنَّها إحدى الخصائص الأساسية للكون^(١)، وهي بذلك شأنها شأن الطاقة يمكن النظر إليها بشكل تجريدي بغض النظر عن شكلها، فهي ليست بالمدرجات الحسية وليست بالمحتوى المحدد للرسالة، وإنَّما هي حامل العلاقات المتبادلة والتفاعل بين المدرجات والمحتويات^(٢).

وقام بعض الفقهاء بتعريف المعلومة من خلال علاقتها مع البيانات، فالمعلومات تتكون من عنصرين: مادي يتمثل بالوسيط أو الكيان الذي يحوي أو تتجسد فيه المعلومة، ومعنوي يتمثل في الدلالة أو الفحوى أو المعنى، ويشكل العنصر الأساسي للمعلومة. أما البيانات ففي صورتها الالكترونية تتجسد بكيان مادي يتمثل بالنبضات الالكترونية أو الإشارات الالكترونية الممغنطة، وفي هذه الصورة تكون البيانات شيء له وجود في العالم الخارجي، أما في صورتها التقليدية فليس لها وجود مستقل، وإنَّما تكون تابعة للكيان المادي الموجودة فيه وبالتالي فهي تعد شيء معنوي^(٣).

وتتمثل علاقة البيانات بالمعلومات في أنَّ الأولى هي المادة الخام التي تستق منها الثانية^(٤)، وهذه العلاقة ذات طبيعة دورية، فالبيانات يتم تجميعها ومعالجتها للحصول على المعلومات، والتي تستخدم بدورها في اتخاذ القرارات، والتي تؤدي بدورها إلى تنفيذ مجموعة من الإجراءات، والتي تحتاج إلى مجموعة إضافية من البيانات تتم

Retrieved 22Jun\2014 en publié sur le site: <http://www.cairn.info/revue-internationale-de-droit-economique-2006-4-page-389.htm>

^(١) Stonier. Tom، 1990، Information and the Internal Structure of the Universe, an exploration into information physics، new york، springer - verlag، p. 92، 26Jun\2014 from: <http://www.burlgrey.com/xtra/infola/infolap006.htm>

^(٢) د. حشمت قاسم، المرجع السابق، ص ١٦.

^(٣) د. أيمن فكري، المرجع السابق، ص ٤٠.

^(٤) د. محمد السعيد خشبة، المعالجة الالكترونية للمعلومات، بدون دار نشر، ١٩٩١، ص ٨.

معالجتها للحصول على معلومات إضافية لاتخاذ قرار آخر يؤدي بدوره إلى تنفيذ مجموعة من الإجراءات^(١).

ومن خلال ما سبق يتبين أنَّ البيانات هي مجموعة الحقائق والأفكار والمشاهدات وتكون عادة على هيئة أرقام أو حروف أو أشكال بيانية تصف أو تمثل شيئاً أو فكرة أو موضوعاً، أما المعلومات فهي البيانات التي تم ترتيبها ومعالجتها لتخرج بشكل جديد أكثر فائدة واستخداماً^(٢).

رابعاً: المعلومات تشريعاً

عرفت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية البيانات بأنها كل عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية المعالجة الآلية بما في ذلك برنامج مناسب لجعل منظومة الكمبيوتر تؤدي وظائفها^(٣)، ويلاحظ أنَّ هذه الاتفاقية تنظر للبيانات بأنها تلك التي تأخذ شكلاً إلكترونياً أو أي شكل آخر يسمح بمعالجتها مباشرة، ولذلك تمَّ استخدام مصطلح البيانات المعلوماتية في هذه الاتفاقية^(٤)، ويعد هذا التعريف مشابهاً لما أخذت به غالبية تشريعات الولايات في الولايات المتحدة الأمريكية والتي تعرف البيانات بأنها كل تمثيل للمعلومات والمعارف والحقائق والمفاهيم وبرمجيات وبرامج الكمبيوتر^(٥).

(١) المرجع ذاته، ص ٩.

(٢) د. يحيى مصطفى حلمي ومحمد السعيد خشبة، الكمبيوتر ونظم المعلومات، مكتبة عين شمس، القاهرة، ١٩٩٠، ص ١٢.

(٣) Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, article 1, Retrieved 22Jun\2014 from: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

(٤) Council of Europe, Explanatory Report for Convention on Cybercrime, para.25, Retrieved 22Jun\2014 from: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

(٥) المادة ٣/٨١٥ من قانون ولاية فلوريدا، المادة ٥٠٢ من قانون ولاية كاليفورنيا، المادة ٥٠١/١٥٦ من قانون ولاية نيويورك.

يمكن الاطلاع على هذه القوانين على الموقع الإلكتروني: <http://law.justia.com>

وعرف قانون الأونيسترال النموذجي للتجارة الالكترونية البيانات بأنها المعلومات التي يتم إنتاجها أو إرسالها أو تخزينها بوسائل الكترونية أو بصرية أو بوسائل مماثلة^(١)، وهذا ما أخذت به غالبية التشريعات العربية، فعرفها المشرع السوري بأنها العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابلاً للإدراك مرتبطاً بسياق محدد^(٢)، أما المشرع السعودي فعرفها بأنها المعلومات أو الأوامر أو الرسائل أو الأصوات أو الصور التي تعد أو التي سبق إعدادها لاستخدامها في الحاسب الآلي كالأرقام والحروف وغيرها^(٣)، وعرفها المشرع الإماراتي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات بوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها^(٤).

ويلاحظ مما سبق أنَّ معظم التشريعات لم تميز بين البيانات والمعلومات، وإنما استخدمت كل منهما للدلالة على الآخر، ولذلك فقد أخذت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية في ١٩٩٢ الخاصة بأمن نظم المعلومات بمبدأ التمييز بين البيانات والمعلومات، فعرفت البيانات بأنها مجموعة الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلاً محدداً يجعلها قابلة للتبادل والتفسير وللمعالجة بواسطة الأفراد أو بوسائل الكترونية، أما المعلومات فهي المعنى المستخلص من البيانات^(٥).

وينبغي عدم التمييز بين البيانات والمعلومات، وذلك لأنَّ ما يعنينا بالمقام الأول هو حماية المعلومات، وبما أنَّ المعلومات هي المعنى المستخلص من البيانات

(١) قانون الأونيسترال النموذجي بشأن التجارة الالكترونية مع دليل التشريع ١٩٩٦، منشورات الأمم المتحدة، نيويورك، ٢٠٠٠، استخرج في ٢٢ كانون الثاني\٢٠١٤ من الموقع الالكتروني:

http://www.uncitral.org/pdf/arabic/texts/electcom/ml-ecomm-a_ebook.pdf

(٢) المادة ١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

(٣) المادة ١ من نظام مكافحة جرائم المعلوماتية السعودي.

(٤) المادة ١ من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

يمكن الاطلاع على هذه القوانين على الموقع الالكتروني: <http://www.eastlaws.com>

(٥) OECD Guidelines for the Security of Information Systems 26 November 1992, Retrieved 20\Feb\2014 from:

<http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformation systems1992.htm>

فالحماية يجب أن تشملهما معاً، والمعلومة قد لا تكون مفهومة لدى متلقيها وهذا ما يجعلها خارج دائرة الحماية طبقاً لهذه التفرقة على الرغم من أن المساس بها على قدر كبير من الخطورة^(١)، ولذلك فإنّ التفرقة من وجهة النظر القانونية ليست سوى مسألة فلسفية أكثر منها ذات مردود قانوني، حيث أنّ الحماية ستمتد لتشمل ما يدخل في إطار النص القانوني دون اعتبار للتسميات، فالعبرة في الحقائق والمعاني لا بالألفاظ والمباني^(٢).

(١) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية تطبيقية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٤، ص ٩٨.

(٢) د. أيمن فكري، المرجع السابق، ص ٤٥.

المطلب الثالث: نظام المعلومات

إنّ نظام المعلومات هو الصورة الأخرى للمحل المادي في جريمة الدخول، ومصطلح نظام المعلومات هو مصطلح حديث يشير إلى الحالة التي نشأت عن الانتقال من مرحلة المعالجة البشرية للمعلومات إلى مرحلة المعالجة الالكترونية، وحتى يتم إسباغ وصف النظام المعلوماتي على أي من منتجات الحياة المعاصرة من وسائل التكنولوجيا ينبغي أن يتوافر عدة عناصر، وتبعاً لذلك فإن دراسة نظام المعلومات تتطلب بيان مفهوم نظام المعلومات أولاً، ومكوناته ثانياً .

أولاً: مفهوم نظام المعلومات

إنّ كلمة نظام أو منظومة ويقابلها في الانكليزية (system) إحدى الكلمات التي استتفزها كثرة الاستعمال حتى كادت تفقد وزنها الدلالي ما لم تكن مرتبطة بأحد المجالات أو السياقات، فلدينا النظام المعلوماتي واللغوي والاقتصادي والثقافي وما إلى ذلك....، وتستعمل هذه الكلمة بمعنى الخطة والأداة والعملية أو مجموعة الإجراءات والأدوات والنسق، وتدل على مجموعة التدابير والموارد والعمليات والإجراءات التي ترمي إلى تحقيق هدف معين^(١)، ويمكن تعريف النظام بأنه مجموعة من العناصر المترابطة مع بعضها بعلاقة تبادل، فهو عبارة عن كينونة تتركب من عنصرين أو أكثر، وكل عنصر من عناصرها متصل مع الآخر بطريقة مباشرة أو غير مباشرة^(٢)، هذا هو النظام بشكل عام إلا أنه ما يهمنا هو النظم المعلوماتية.

ومفهوم الأنظمة المعلوماتية أقدم من الحاسبات الالكترونية وغيرها من التقنيات الأخرى، فهي مجموعة من الموارد والتدابير والقنوات وعمليات والإجراءات التي تحكم تدفق المعلومات في وسط معين، وتشمل أنشطة إنتاج وبث وتجميع وتخزين واسترجاع المعلومات والاستفادة منها وما يترتب على ذلك من آثار التي قد تؤدي إلى إنتاج المزيد من المعلومات، ويتراوح الوسط الخاص بالنظام بين الفرد والمجتمع، وهذا يعني أنّ لكل

(١) د. حشمت قاسم، المرجع السابق، ص ٩٤.

(٢) د. محمد السعيد خشبة، نظم المعلومات المفاهيم والتكنولوجيا، دون دار ومكان نشر، ١٩٨٧، ص

فرد ولكل تجمع بشري أياً كانت طبيعته وأهدافه ونشاطه وحدوده منظومة خاصة به، ولكل مؤسسة ولكل تحصيل علمي ولكل مجال من المجالات الأخرى منظومة خاصة به، فالأنظمة المعلوماتية ليست مفهوماً حديثاً، وإنما هي احد الظواهر الأساسية المرتبطة بالإنسان منذ بدأ يستطلع العالم حوله ويحاول التعامل مع بيئته على اختلاف عناصرها^(١).

هذا بالنسبة لمفهوم الأنظمة المعلوماتية، أما مصطلح النظم المعلوماتية فهو مصطلح حديث نشأ في بداية السبعينات من القرن العشرين بهدف وصف الحالة التي نشأت عن اندماج تقنية نظم المعلومات مع تقنية الاتصالات عن بعد وهندسة التحكم، وهذا ما أدى إلى اختراع تقنيات متطورة ساعدت في أساليب معالجة البيانات بمختلف أنواعها وأشكالها، وأصبحت أحد أهم العوامل المؤثرة في تحديد ملامح عصرنا في شتى نواحي الحياة المعاصرة^(٢).

ويعرف النظام المعلوماتي في الاتفاقية الأوربية لمكافحة الجريمة المعلوماتية بأنه جهاز أو مجموعة من الأجهزة المتصلة أو المتعلقة ببعضها البعض ويقوم واحد منها أو أكثر تبعا لبرنامج بعمل معالجة آلية للبيانات^(٣)، وتوضح المذكرة التفسيرية لهذه الاتفاقية بأن النظام المعلوماتي هو جهاز يتكون من معدات وبرامج قائمة للمعالجة الآلية للبيانات، ويمكن أن تشتمل على طرق سهلة للإدخال واستخراج وتخزين البيانات، ويمكن أن تكون منفردة أو متصلة مع أجهزة مماثلة أخرى داخل الشبكة، وتوضح المذكرة بأن عبارة آلية تعني بدون تدخل بشري، أما عبارة معالجة البيانات فتعني مجموعة العمليات التي تطبق على البيانات ويتم تسجيلها عن طريق تنفيذ برامج للمعلوماتية^(٤).

(١) د. حشمت قاسم، المرجع السابق، ص ٩٥.

(٢) د. أيمن فكري، المرجع السابق، ص ٧١.

(٣) Council of Europe, Convention on Cybercrime, Budapest, article 1

(٤) Council of Europe, Explanatory Report for Convention on Cybercrime, para.23

أمّا قانون الأونيسترال النموذجي فعرف النظام المعلوماتي بأنّه النظام الذي يستخدم لإنتاج رسائل البيانات أو إرسالها وتلقيها أو تخزينها أو لأي إجراء آخر، ويوضح الدليل التشريعي لهذا القانون بأنّ القصد من هذا التعريف أن يشمل النظام كافة الوسائل التقنية المستخدمة لإرسال المعلومات وتلقيها وتخزينها، وعلى ذلك فقد يشير نظام المعلومات إلى شبكة الاتصالات وفي حالة أخرى إلى أجهزة البريد الإلكتروني أو حتى إلى ناسخ حرفي^(١).

وعرفته منظمة التعاون الاقتصادي والتنمية بأنّه الحاسبات الآلية ووسائل ومرافق الاتصالات وشبكات الحاسوب والاتصالات والبيانات والمعلومات التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحاسبات بما في ذلك البرامج والمواصفات وجميع القواعد اللازمة لتشغيل هذه الأنظمة والمحافظة عليها^(٢).

وعرف المشرع السوري المنظومة المعلوماتية بأنّها مجموعة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها، كما أنّه يعرف الأجهزة الحاسوبية بأنّها الأجهزة التي تستخدم التقانات الإلكترونية أو الكهربائية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها، ويعرف البرمجيات الحاسوبية بأنها سلسلة من التعليمات المرمزة التي يمكن تنفيذها على جهاز حاسوبي بغية تمكينه من أداء الوظائف والتطبيقات المطلوبة، كما يعد القانون السوري الموقع الإلكتروني أحد الصور الخاصة لنظام المعلومات، ويعرفه بأنّه منظومة معلوماتية لها اسم أو عنوان يعرفها وتتضمن معلومات أو خدمات يمكن الوصول إليها عن طريق الشبكة وخاصة الانترنت^(٣)، كما يعرف القانون الإماراتي النظام بأنّه مجموعة برامج وأدوات لمعالجة

(١) قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع ١٩٩٦.

(٢) OECD Guidelines for the Security of Information Systems 26 November 1992

(٣) المادة ١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

وإدارة البيانات أو المعلومات أو الرسائل الالكترونية وغير ذلك^(١)، والسعودي بأنه مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية^(٢).

أما القانون الفرنسي فلم يتضمن تعريفاً للأنظمة المعلوماتية إلا أن مجلس الشيوخ الفرنسي عرفها بأنها كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي يتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال أو الإخراج وأجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة البيانات^(٣).

وكذلك الحال بالنسبة للقانون الانكليزي فلم يتضمن تعريفاً للنظام، كما أن اللجنة القانونية في مجلس النواب لم تحاول ذلك لأنه في رأيها أن صياغة تعريف ليكون جامعاً مانعاً سيكون مهمة معقدة جداً، ومن المحتمل أن ينتج جدل واسع، وبالتالي إرباك القضاة الذين ستكون مهمتهم تطبيق أحكام القانون في القضايا التي تنتظر أمامهم^(٤).

كما أنه لم تتضمن تشريعات الولايات المتحدة الأمريكية تعريفاً للأنظمة المعلوماتية إلا أنها استعاضت عن ذلك بتعريف الحاسب وشبكة الحاسب وبرمجيات الحاسب وخدمات الحاسب ونظام الحاسب، فالحاسب هو الجهاز الأوتوماتيكي الذي يقوم بإجراء معالجة للبيانات تلقائياً، وشبكة الحاسب هي النظام الذي يوفر الاتصالات بين واحد أو أكثر من أنظمة الحاسب ووحدات الإدخال والإخراج بما في ذلك على سبيل المثال لا الحصر محطات العرض والطابعات التي ترتبط بها مرافق الاتصالات السلكية واللاسلكية، وبرمجيات الحاسب هي مجموعة البيانات أو التعليمات والتي عند

(١) المادة ١ من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

(٢) المادة ١ من نظام مكافحة جرائم المعلوماتية السعودي.

(٣) د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، ١٩٩٢، ص ٣٧.

(٤) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.26.

تنفيذها أو تعديلها تسبب أداء الكمبيوتر أو نظامه أو شبكة الاتصالات لوظائف محددة، وخدمات الحاسب تشمل وقت الكمبيوتر ووظائف معالجة البيانات وتخزينها أو الاستخدامات الأخرى لشبكة الحاسب ونظام أو جهاز الحاسب أو غيرها، ونظام الحاسب هو جهاز أو مجموعة من الأجهزة يحتوي إحداها أو أكثر على برامج الحاسب والتعليمات الالكترونية والبيانات المدخلة ونواتجها والتي تؤدي وظائف متنوعة^(١).

ومما سبق نرى أنّ التعريفات التي قدمتها التشريعات في تعريف نظام المعلومات تمت صياغتها من حيث البناء (القانون السوري) أو الوظيفة (القانون الإماراتي)، إلا أنّه أي تعريف سيقدم في هذا المجال من شأنه أن ينطوي على مخاطر عدم مسايرته للتقدم التكنولوجي المستمر^(٢)، ولذلك فنحن نرى عدم التدخل التشريعي في صياغة تعريف للنظام المعلوماتي أو على الأقل أن تقدم صياغة تتيح انضمام المفاهيم المستحدثة للنظام مستقبلاً، وذلك من خلال تضمن هذه التعريفات عبارات تفيد هذا المعنى.

ثانياً: مكونات النظام المعلوماتي

حتى يمكن إسباغ وصف النظام المعلوماتي على أي من منتجات الحياة المعاصرة من وسائل تكنولوجيا المعلومات يجب أن يتوافر فيها عدة عناصر يمكن تقسيمها إلى فئتين: المكونات المادية، المكونات المنطقية.

١ - المكونات المادية:

تشير المكونات المادية (hard ware) إلى جميع أقسام النظام المعلوماتي وأدواتها العلمية والمادية وتتكون من وحدات الإدخال والإخراج ووحدات المعالجة المركزية^(٣).

(١) الفصل ٨١٥ من قانون ولاية فلوريدا.

(٢) Scot Law Corm. No 106, Report on Computer Crime.Cm.174 1987, para.4.17

(٣) أندريه لوغارف، المرجع السابق، ص ٣٣٣.

أ - وحدات الإدخال:

تعرف وحدات الإدخال (input units) بأنها عبارة عن أجهزة مرتبطة بوحدة المعالجة المركزية وتستخدم لإدخال البيانات والأوامر إليها^(١) ومن أشهر هذه الوحدات:

- لوحة المفاتيح (keyboard): وتعتبر من إحدى أشهر وسائل الإدخال في مجال الإدخال المعلوماتي، وتتكون من مجموعة من المفاتيح يمكن تقسيمها إلى مجموعات رئيسية تحتوي كل منها على عدد من المفاتيح تقوم كل منها بوظائف معينة^(٢)، وتستخدم بشكل عام لإدخال البيانات والأوامر إلى النظام^(٣).

- الفأرة (mouse): وهي عبارة عن أداة تحرك على سطح مستو تدل الحاسب على الموقع المطلوب^(٤)، وتعد من أهم الأجهزة التي أحدثت ثورة في استخدام الحاسب ويمكن هذا الجهاز المستخدم من إدخال الأوامر إلى النظام^(٥).

- الماسح الضوئي (scanner): وهو جهاز لتحويل الصورة إلى بيانات رقمية يمكن معالجتها بالحاسب^(٦).

- لوحة تحكم باللمس (touch control penal): وهي لوحة تحكم تشغل المفاتيح باللمس تسمح للمستخدم أن يقوم بإدخال البيانات عن طريق لمس الشاشة^(٧).

- القلم الضوئي (light pen) : وهو أداة ضوئية على هيئة قلم تستخدم للإشارة إلى البيانات والأشكال المعروضة على شاشة النهاية الطرفية التي يراد تعديلها^(٨).

(١) د. ياسر يوسف عبد المعطي، مقدمة في الحاسب الآلي وتطبيقاته، شركة المكتبات الكويتية، ١٩٩٤، ص ٤٣.

(٢) المرجع ذاته، ص ٤٥.

(٣) معجم الحاسبات، الطبعة الثانية الموسعة، مجمع اللغة العربية، مصر، ١٩٩٥، ص ١٠٩.

(٤) معجم الحاسبات، المرجع السابق، ص ١٢٣.

(٥) د. ياسر يوسف عبد المعطي، المرجع السابق، ص ٤٩.

(٦) معجم الحاسبات، المرجع السابق، ص ١٥٧.

(٧) المرجع ذاته، ص ١٨٠.

- قارئة البطاقات (card reader): وهي جهاز لتحويل المعلومات المشفرة إلى الشفرة الداخلية للحاسب^(٢).

- ب - وحدات الإخراج:

تعرف وحدات الإخراج (output units) بأنها عبارة عن أجهزة تستخدم لإخراج المعلومات في صورتها بعد المعالجة^(٣) ومن أشهر هذه الوحدات:

- الشاشة (screen): وهي عبارة عن سطح أنبوبة أشعة كاثودية تعرض عليها البيانات المدخلة أو المعلومات التي نتجت عن عمليات المعالجة، ويطلق هذا المصطلح على أي لوحة عرض^(٤).

- الطابعة (printer): هي جهاز يستخدم بتمثيل المخرجات المعلوماتية على الورق، وتختلف الطابعات في التكنولوجيا المستخدمة وسرعة التشغيل والتطبيق المستهدف وخصائص المخرجات الورقية، وأكثر الطابعات انتشاراً هي طابعات الأسطر^(٥).

- مايكرو فيلم (com): هي إحدى الأشكال المختلفة من تكنولوجيا المخرجات تستخدم لتسجيل كمية كبيرة من المعلومات على المصغرات الفيلمية بدلاً من تسجيلها على الورق^(٦)، وتتميز هذه التكنولوجيا بأنها غير مكلفة وسهلة، إلا إنها تعد أوساطاً غير مريحة للتعامل معها على عكس المخرجات الورقية^(٧).

(١) المرجع ذاته، ص ١١٣.

(٢) المرجع ذاته، ص ٣٤.

(٣) د. ياسر يوسف عبد المعطي، المرجع السابق، ص ٥٤.

(٤) معجم الحاسبات، المرجع السابق، ص ١٥٨.

(٥) د. محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقاتها، دار الشروق، دون مكان نشر، ١٩٨٩، ص ٨٦.

(٦) المرجع ذاته، ص ٨٨.

(٧) د. عماد الصباغ، نظم المعلومات ماهيتها ومكوناتها، مكتبة دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٠، ص ٦٦.

- القرص المرن (floppy disk): وهو عبارة عن قرص صغير يستخدم لتخزين المخرجات المعلوماتية وسعته التخزينية صغيرة جداً^(١).

القرص الصلب (hard dick): وهو يقوم بنفس وظيفة القرص المرن إلا أن سعته التخزينية أكبر بكثير^(٢)، ويعد من أكثر أوعية اختزان المعلومات استخداماً ويتميز بسرعته العالية في تخزين واسترجاع المعلومات والذي يتم بطريقة مباشرة^(٣).

ج - وحدة المعالجة المركزية:

تعد وحدة المعالجة المركزية (cup) من أكثر أجهزة الحاسب أهمية لاحتوائها على جميع الإمكانيات الضرورية اللازمة لإنجاز مهام معالجة وتداول المعلومات والرقابة على جميع الأجزاء الأخرى وتنسيق العمل بينها ولذلك تعد بمثابة القلب في الآلة^(٤)، وتتكون هذه الوحدة من ثلاثة أجزاء هي: ^(٥)

- ١ - وحدة التخزين الرئيسية (main storage unit) وتسمى أحياناً الذاكرة الرئيسية (main memory) ^(٦) وهي الوحدة الرئيسية لتخزين وتداول البيانات التي يتم إدخالها إلى الأنظمة المعلوماتية لتتم معالجتها^(٧) وتنقسم هذه الذاكرة إلى نوعين:

- أ - ذاكرة القراءة والكتابة (ram): وهي عبارة عن مساحة عمل فارغة يتم من خلالها إدخال البيانات والبرامج المختلفة إلى النظام لمدة مؤقتة حتى يمكن معالجتها ولذلك فهي يجب أن تكون قابلة للمسح والكتابة من جديد وتغير ما عليها من بيانات باستبدال البيانات التي لا حاجة للمعالج بها ببيانات أخرى جديدة أو بمجرد

(١) معجم الحاسبات، المرجع السابق، ص ٨٤.

(٢) المرجع ذاته، ص ٩٤.

(٣) د. ياسر يوسف عبد المعطي، المرجع السابق، ص ٦٠.

(٤) د. محمد السعيد خشبة، المرجع السابق، ص ٩٦.

(٥) د. عماد الصباغ، المرجع السابق، ص ٥١.

(٦) د. محمد السعيد خشبة، المرجع السابق، ص ٩٨.

(٧) د. ياسر يوسف عبد المعطي، المرجع السابق، ص ٤١.

إطفاء الجهاز أو انقطاع التيار الكهربائي^(١) ولذلك تسمى الذاكرة المؤقتة أو الذاكرة المتطايرة^(٢).

- ب - ذاكرة القراءة فقط (rom): وهي عبارة عن شريحة تخزن عليها برامج هامة بالنسبة للحاسب وتعبر عن خطوات ثابتة ومعيّنة يقوم بها الحاسب من تلقاء نفسه في وقت معين يتناسب مع الغرض المعد لأجله هذا البرنامج، وهذه الذاكرة توضع من قبل الشركة المصنعة للحاسب ولا يمكن للمستخدم أن يعدل عليها^(٣).

- ٢ - وحدة الرقابة والتحكم (control penal): تعتبر هذه الوحدة بمثابة الجهاز العصبي المركزي للأنظمة^(٤)، وتختص بالتحكم في عمليات المعالجة من ناحية التوقيت المناسب والترتيب المناسب فهي تعمل على تنظيم عمليات المعالجة وفقاً للبرنامج المستخدم وذلك لضمان نجاح عملية المعالجة بكفاءة وسرعة^(٥).

- ٣ - وحدة الحساب والمنطق (arithmetic and Logic Unit): هي مجموعة الدوائر الالكترونية التي تختص بإجراء العمليات الحسابية والمنطقية على البيانات الواردة لها من وحدة التخزين طبقاً للتعليمات الصادرة لها من التحكم^(٦).

د - شبكة الاتصالات:

بالإضافة إلى العناصر السابقة التي يجب توافرها في كيان معين حتى يوصف بأنه نظام معلوماتي فإن هناك عنصراً إضافياً له أهمية كبرى في النظم المعلوماتية ألا وهو الاتصالات الالكترونية التي تتم من خلال الشبكات المعلوماتية^(٧)، فمع التطور

(١) د. عبد الغفور عبد الفتاح قاري، معجم مصطلحات الكمبيوتر، مطبوعات مكتبة الملك فهد السلسلة الثالثة، الرياض، ٢٠٠١م، ص ٢٤٨.

(٢) معجم الحاسبات، المرجع السابق، ص ١٤٢.

(٣) د. ياسر يوسف عبد المعطي، المرجع السابق، ص ٤١.

(٤) د. محمد محمد الهادي، المرجع السابق، ص ٧٤.

(٥) د. يحيى مصطفى حلمي، أساسيات نظم المعلومات، مكتبة عين شمس، القاهرة، ١٩٩٨، ص ١٢٤.

(٦) المرجع ذاته، ص ١٢٤.

(٧) د. أيمن فكري، المرجع السابق، ص ٦٥.

والتقدم التكنولوجي أصبحت النظم المعلوماتية تحتوي على منظومات معلوماتية مكونة من العديد من الأجزاء المترابطة فيما بينها من خلال وسائل الاتصال والتي تتيح للمستخدمين نشر المعلومات ونقلها وإتاحتها والتعامل معها على نطاق واسع، وبهذا فقد أصبحت شبكات الاتصالات أحد الأجزاء الرئيسية من النظام ولم تعد مجرد جهازاً ملحقا به.

وتعرف الاتصالات بأنها إرسال المعلومات بأي شكل (صوت، صورة، بيانات، نصوص) إلى مكان آخر باستخدام الوسائل الالكترونية أو الضوئية، أما شبكة الاتصالات فتعرف بأنها أي ترتيب يتوفر فيه إرسال رسالة عبر قناة هي عبارة عن وسيط من نوع^(١)، وتتكون هذه الشبكات من عدة عناصر هي: المحطات الطرفية التي من خلالها يستطيع المستخدم الاستفادة من الخدمات التي توفرها الشبكة، ومعالجات الاتصالات التي يسند إليها عملية إرسال واستقبال البيانات من المحطات الطرفية والحاسب، وقنوات وأوساط الاتصالات التي يتم من خلالها إرسال واستلام البيانات، والحواسيب التي تقوم بوظيفة معالجة البيانات، وبرمجيات السيطرة التي تتألف من برامج موضوعة في الحواسيب وتقوم بإدارة وظائف الشبكة^(٢)، ويمكن التمييز بين ثلاثة أنواع لشبكات الاتصال: الشبكات المحلية (local area networks): وهي شبكة اتصالات تغطي مساحة صغيرة لا تتجاوز بضعة كيلومترات وتستخدم في نطاق المؤسسة أو المؤسسات أو الجامعة، وشبكات المناطق (metropolitan area network): وهي تغطي منطقة جغرافية واسعة نسبياً تصل إلى حدود المدينة والشركات أو المؤسسات الواسعة، والشبكات الكبيرة (wide area networks): وهي تغطي مساحات شاسعة ويستخدم في ذلك الأقمار الصناعية أو شبكات الهاتف أو

(١) د. عماد الصباغ، المرجع السابق، ص ٩١.

(٢) المرجع ذاته، ص ٩٢.

الكابلات البحرية، وأشهر هذه الشبكات الانترنت (internet) والتي تغطي العالم بأجمعه وتتصل مع عدة شبكات أخرى^(١).

- ٢ - المكونات المنطقية:

تشير المكونات المنطقية (soft ware) إلى جميع المكونات غير المادية التي يتكون منها النظام، وتشمل البيانات والمعلومات والبرامج^(٢).

- أ - البيانات:

كلمة بيانات (data) هي جمع بيان (datum)، وتستخدم بصورة شائعة في اللغة العربية لتمثيل الجمع والمفرد بأن واحد^(٣)، وهي تمثل مجموعة الحقائق أو الأفكار أو المشاهدات أو الملاحظات أو القياسات، وهي تصف فكرة أو موضوعاً أو هدفاً أو حقائق أخرى^(٤)، وتأخذ بصورة عامة صيغاً مختلفة تشمل البيانات الرقمية والنصوص والصوت والصور^(٥)، ويمكن تعريف البيانات بأنها تعبير عن الأحداث موضوع الاهتمام التي يتم إدخالها إلى النظام بغرض الحصول على المعلومات^(٦)، وفي تعريف آخر هي المادة الخام التي تشتق منها المعلومات^(٧).

- ب - المعلومات:

تعد المعلومات ثمرة عمليات تنظيم وترتيب أو جدولة أو تحويل البيانات إلى مجموعات مختارة بطريقة معينة، وتعرف بأنها البيانات التي تمت معالجتها بشكل

(١) د. حسن طاهر داود، الحاسب وأمن المعومات، معهد الإدارة العامة، المملكة العربية السعودية، الرياض، ١٤٢١هـ، ص ٢٩١.

(٢) معجم الحاسبات، المرجع السابق، ص ١٦٤.

(٣) د. عماد الصباغ، المرجع السابق، ص ١٩.

(٤) د. محمد السعيد خشبة، المعالجة الالكترونية للمعلومات، دون دار ومكان نشر، ١٩٩١، ص ٨.

(٥) د. عماد الصباغ، المرجع السابق، ص ١٩.

(٦) د. قاسم عبد الرزاق، نظام المعلومات المحاسبة الحاسوبية، مكتبة الثقافة للنشر والتوزيع، عمان، ١٩٩٨، ص ١٢.

(٧) د. محمد السعيد خشبة، المرجع السابق، ص ٨.

ملائم لتعطي معنى كامل للمستخدم تمكنه من استخدامها في العمليات الجارية أو المستقبلية^(١)، وفي تعريف آخر هي مجموعة البيانات التي يتم تحويلها إلى صورة ذات معنى وقابلة للاستخدام من قبل المستفيد الأخير^(٢).

- ج - البرامج:

إنّ البيانات تشكل المادة الأولية التي تخضع لمجموعة العمليات التحويلية التي من شأنها تحويلها إلى معلومات مفيدة، وتعرف هذه العملية باسم معالجة البيانات^(٣)، وتتم هذه العملية من خلال استخدام البرامج التي تشكل العنصر الثالث من المكونات المنطقية للنظام المعلوماتي، ويمكن النظر إلى هذا المكون على اعتباره يشكل روح النظام، فهو يقوم بتشغيله، وهو مجرد أفكار مجردة يستوعبها العقل ولا يمكن لمسها باليد، ويتكون من مجموعة التعليمات التي تدخل الحاسب^(٤)، والبرامج في حقيقتها إحدى الصور الخاصة للمعلومات، فهي بيانات تمت معالجتها وأصبحت رموزاً وإشارات لا يمكن للإنسان العلم فيها إلا من خلال الآلة^(٥)، ويعرف البرنامج بأنّه مجموعة من التعليمات في لغة معينة تحدد المراحل المعتمدة في حل مسألة ما^(٦)، وفي تعريف آخر هو مجموعة التعليمات التي يعبر عنها بأي لغة أو رمز بأي شكل من الأشكال بحيث يمكن توجيهها بطريقة مباشرة أو غير مباشرة إلى الحاسب الآلي للوصول إلى نتيجة أو غاية معينة^(٧).

وتنقسم البرامج من حيث الأداء: إلى برامج تشغيلية (operating programs) وبرامج تطبيقية (application programs)، ولا يوجد اختلاف بينها من حيث مراحل

(١) د. قاسم عبد الرزاق، المرجع السابق، ص ١٣.

(٢) د. عماد الصباغ، المرجع السابق، ص ١٩.

(٣) د. محمد السعيد خشبة، المرجع السابق، ص ٨.

(٤) د. يحيى مصطفى حلمي ومحمد السعيد خشبة، المرجع السابق، ص ١٦.

(٥) د. أيمن فكري، المرجع السابق، ص ٤٧.

(٦) أندريه لو غارف، المرجع السابق، ص ٥٤٨.

عبد الرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي، رسالة ماجستير، جامعة (٧) النجاح الوطنية، نابلس، ٢٠٠٨، ص ١٣، استخرج بتاريخ ٢٠ كانون الثاني \ ٢٠١٤ من الموقع الإلكتروني: <http://dspace.univ-tlemcen.dz/bitstream/112/2818/3/rassa3.pdf>

التأليف والإعداد والتنفيذ، وإنّما الاختلاف يبرز في أداء كل منها^(١)، فالبرامج التشغيلية تقوم بتشغيل وإدارة الأجهزة المختلفة التي تتكون منها النظام وتنسيق العمل فيما بينها ومراقبة أدائها ومراقبة عمليات الإدخال والإخراج والتخزين المختلفة^(٢)، أما البرامج التطبيقية فتقوم بأداء مهام فردية معينة^(٣)، وهي تنقسم إلى برامج التطبيقات التجارية ومن أمثلتها تطبيقات البنوك و الأجور ومراقبة المخزون وبرامج التطبيقات العلمية ومن أمثلتها التطبيقات الإحصائية والرياضية والهندسية^(٤).

ومما سبق نرى أنّ وصف النظام المعلوماتي يمكن إسباغه على أي كيان يتوافر فيه مجموعة من المكونات المادية والمنطقية التي سبق ذكرها، وهو في ذلك لا يقتصر على جهاز أو آلة معينة وإنما ينطبق على أي من منتجات العصر والتي تتوافر فيها العناصر السابقة، وإنّ هذا التحديد لنظام المعلومات يثير التساؤل على أي من أجزائه تقع جريمة الدخول ؟

إنّ جوهر جريمة الدخول وفق ما حددته النصوص القانونية هو الوصول إلى المعلومات، ويقصد بالمعلومات هنا المفهوم الواسع الذي ينطوي عليه هذا المصطلح، أي جميع المكونات المنطقية للنظام والتي تشمل كلاً من البيانات والمعلومات والبرامج، ذلك لأنّه كما بيّنّا سابقاً لا جدوى من التمييز بين البيانات والمعلومات، كما أنّ البرامج تعدّ إحدى الصور الخاصة للمعلومات.

أما فيما سواها من المكونات المادية للنظام، فإنّها لا تعد محلاً صالحاً لهذه الجريمة وذلك للتعارض بين الطابع المنطقي للدخول والطبيعة المادية لهذه المكونات، والتي تعد محلاً صالحاً للحماية من خلال القواعد التقليدية في القانون والتي تحمي

(١) د. مصطفى محمد عرجاوي، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤، ص ٣٦٨.

(٢) د. يحيى مصطفى حلمي، المرجع السابق، ص ١٣٠.

(٣) د. محمد محمد الهادي، المرجع السابق، ص ١٢٥.

(٤) د. يحيى مصطفى حلمي، المرجع السابق، ص ١٢٧.

الأموال المادية، إلا أنه وعلى الرغم من ذلك فإن الطابع المنطقي للدخول يتطلب أن تكون المكونات المنطقية محمولة على العتاد المادي للنظام من دون أن يعد محلاً لهذه الجريمة.

وإنّ هذا التحديد لمحل الحماية من شأنه أن يثير تساؤلاً آخر حول إذا ما كانت هذه الجريمة تقع في الحالة التي يتم فيها الدخول إلى أحد الأجزاء المنطقية التي يتكون منها النظام، كما في الحالة التي يكون فيها الدخول مشروعاً إلى بعض أجزاء النظام دون الأجزاء الأخرى ؟

تتجه معظم التشريعات إلى تجريم هذا الدخول من خلال عدم الاكتفاء بتجريم الدخول إلى النظام وإنّما من خلال تجريم الدخول إلى أي من أجزائه أيضاً، كما هو الحال في الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية والتي تساوي بين الدخول إلى كامل النظام أو إلى أحد أجزائه^(١)، كما أنّ المشرع الفرنسي يجرم الدخول إلى كل أو جزء من نظام المعالجة الآلية للبيانات^(٢)، ويجرم القانون الهولندي أيضاً الدخول إلى النظام الآلي للتخزين أو معالجة البيانات أو إلى أي جزء من هذا النظام^(٣)، وكذلك فإنّ القانون الانكليزي يجرم الدخول إلى أي من المعلومات أو البرامج التي يحتويها النظام^(٤)، ويجرم المشرع السوري الدخول إلى أي من أجزاء النظام، وهو أمر يمكن الاستدلال عليه من خلال تجريمه الدخول الذي يتم من دون صلاحية، أي بتجاوز التصريح الممنوح للفاعل، وذلك لأنّ تجاوز التصريح يكون في أحد أشكاله الدخول إلى أحد أجزاء النظام الغير مصرح بها من قبل المسؤول^(٥).

وإنّ فكرة نظام المعلومات تنثير تساؤلاً آخر حول إمكانية وقوع جريمة الدخول على الأجزاء التي تتفصل عن هذا النظام ؟

(١) المادة الثانية من الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية.

(٢) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

(٣) المادة ١٣٨ من قانون العقوبات الهولندي.

(٤) المادة الأولى من قانون إساءة استخدام الحاسبات الآلية.

(٥) المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

تختلف التشريعات في تجريم ذلك، ففي القانون الانكليزي لا يبدو هذا التجريم ممكناً لاشتراطه أن يتم الدخول إلى المعلومات أو البرامج عن طريق نشاط يتسبب بقيام الحاسب الآلي بأداء وظيفة ما^(١)، إلا أنه وفي تشريعات أخرى يجرم هذا الدخول، كما هو الحال في القانون الفنلندي الذي يجرم الدخول إلى الأجزاء التي تتفصل عن النظام^(٢)، والقانون اليوناني الذي يجرم الدخول إلى ذاكرة خارجية^(٣)، ويجرم أيضاً القانون الأمريكي الدخول إلى كل وسيط لتخزين المعلومات أو إلى أي معلومة تمت معالجتها آلياً وإلى الأجهزة التي تربطها بالحاسب الآلي وإلى البرامج التي تقوم بتشغيلها^(٤)، كما أنه يمكن التوصل إلى هذا التجريم في القانون الفرنسي، وهذا أمر يمكن الاستدلال عليه من خلال تعريف مجلس الشيوخ لنظام المعالجة الآلية بأنه مجموعة من الأجزاء بينها روابط تؤدي إلى نتيجة محددة إلا أنه لم يشترط دوام هذا الربط وبالتالي فإنَّ الدخول إلى أي من أجهزة التخزين التي انفصلت عن النظام المعلوماتي يحقق جريمة الدخول، وكذلك الأمر في القانون السوري الذي يعرف الجهاز الحاسوبي بأنه الجهاز الذي يستخدم التقنيات الحديثة في جمع وحفظ المعلومات إلا أنه لم يشترط ذلك أن يتم في إطار متصل مع النظام^(٥).

ومما سبق نرى أنَّ المحل المادي الذي يتحقق فيه النشاط الإجرامي هو المعلومات التي يتكون منها النظام المعلوماتي بمفهومها الواسع، سواء أكانت في إطار متصل أو منفصل عن نظام المعلومات، حيث لا نرى مناساً للتمييز بين المعلومات المخزنة على الوحدات المتصلة مع نظام المعلومات والوحدات التي تتفصل عنه.

(١) المادة الأولى من قانون إساءة استخدام الحاسبات الآلية الانكليزي.

(٢) القسم ٨ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(٣) المادة ٢٣٧٠ من قانون العقوبات اليوناني.

(٤) المادة ١٠٣٠ ح من القانون الفيدرالي لإساءة استخدام الحاسبات الآلية.

(٥) المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

المبحث الثاني: المصلحة المحمية

إنَّ الهدف من القانون الجزائي هو حماية المصالح المعتمدة قانوناً، بحيث يشكل الاعتداء عليها خروجاً على أحكام القانون يستلزم العقاب الجزائي على المخالفين لزجرهم وردعهم، فحماية المصالح هو مناط التجريم والعقاب، وقد تباينت التشريعات في تحديد المصالح المعتمدة في الجريمة المعلوماتية وهذا كان من شأنه أن يؤثر على الحق المراد حمايته في جريمة الدخول.

وتبعاً لذلك سنتناول في هذا المبحث المصلحة المحمية في الجريمة المعلوماتية في المطلب الأول، ثم نبين المصلحة المراد حمايتها في جريمة الدخول في المطلب الثاني.

المطلب الأول: المصلحة المحمية في الجريمة المعلوماتية

تباينت الاتجاهات التشريعية للدول المختلفة في تحديد الأساس الذي يركز عليه التدخل التشريعي لحماية المعلومات، ويمكن أن نميز في هذا الصدد بين ثلاثة اتجاهات: الأول يركز على حماية حق الملكية، والثاني يركز على حماية المعلومات، بينما الثالث هو اتجاه مختلط يجمع بين كلا الاتجاهين السابقين.

أولاً: الاتجاه الأول

يهتم هذا الاتجاه بحماية حق الملكية، ولذلك فإنّه ينظر إلى المعلومات باعتبارها من قبيل الأشياء التي ترد عليها الملكية، والغرض من تجريم التعدي على المعلومات في هذه الحالة هو حماية الملكية الخاصة، وذلك من جراء حصول الفاعل على ربح مادي أو تعرض المالك للضرر عن طريق النشاط الإجرامي، ولذلك فإنَّ الجريمة المعلوماتية في هذه الاتجاه شأنها شأن الجرائم التقليدية^(١).

(١) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٠٩.

وتعد بعض قوانين الولايات في الولايات المتحدة الأمريكية نموذجاً لهذا الاتجاه، ولذلك فهي تتبنى تعريفاً واسعاً للملكية باعتبارها تتطوي على أي شيء له قيمة^(١)، وتذهب هذه التشريعات إلى أن الغرض من تجريم التعدي على المعلومات هو توسيع الحماية الممنوحة للأفراد والشركات والوكالات الحكومية من العبث والتدخل والضرر والوصول إلى أي من المعلومات التي تحتويها الحواسيب التابعة للجهات المذكورة^(٢)، ولذلك فهي تواجه أفعال التعدي على المعلومات في إطار المواد التي تحمي الملكية، ولهذا نجد قانون ولاية نيويورك ينص في المادة ١٥٦ من الجزء المتعلق بالسرقة على جرائم التعدي والعبث بالحاسوب، كما يجرم قانون ولاية كاليفورنيا في المادة ٥٠٢ من الفصل المتعلق بالسرقة أفعال الدخول والاستخدام غير المصرح به للحاسب الآلي وإعاقة الوصول إلى الخدمة والإتلاف المعلوماتي ونشر الفيروسات، وهذا يتمثل مع ما ذهب إليه قانون ولاية فلوريدا في الفصل ٨١٥ والذي يتعلق بالجرائم المتصلة بالكمبيوتر، كما تأخذ هذه التشريعات في الحسبان عند تحديد جسامة الجريمة أو مقدار العقوبة قيمة الأضرار التي لحقت بالمالك أو قيمة الفائدة التي تحصل عليها الفاعل، فعلى سبيل المثال يعاقب قانون ولاية كاليفورنيا على مجرد الدخول إلى نظام الحاسب الآلي بالغرامة حتى ١٠٠٠ دولار، وتصبح العقوبة الغرامة حتى ٥٠٠٠ دولار أو السجن لمدة ستة أشهر أو كلاهما إذا سبب أضراراً لا تتعدى قيمتها ٥٠٠٠ دولار، أما إذا تجاوزت قيمة الأضرار هذا الحد فيعاقب بالغرامة حتى ١٠٠٠٠ دولار أو السجن لمدة ستة أشهر أو سنتين أو ثلاث سنوات أو كلاهما، كما أن قانون ولاية نيويورك يعد الشخص الذي يرتكب جريمة العبث من الدرجة الرابعة مذنباً بجنحة من الدرجة الأولى،

(١) يعرف قانون ولاية فلوريدا الملكية في الفصل ٨١٢ بأنها أي شيء ذات قيمة وتشمل الممتلكات العقارية والشخصية الملموسة وغير الملموسة إضافة إلى الخدمات، و يعد في الفصل ٨١٥ كلاً من الصكوك المالية والمعلومات بما في ذلك البيانات المعالجة إلكترونياً وبرامج الكمبيوتر والبرامج المقروءة آلياً أو أي من الأشكال القابلة لقراءة الإنسان وأي منتجات أخرى ملموسة أخرى أو غير ملموسة ذات قيمة من قبيل هذه الممتلكات، وهذا يتمثل مع تعريف قانون ولاية نيويورك والذي عرف الملكية في المادة ١٥٥ بأنها أي أموال أو ممتلكات شخصية أو عقارية أو بيانات وبرامج الكمبيوتر أو الأشياء محل دعوى قضائية أو الدليل على دين أو عقد أو أي شيء له قيمة بما في ذلك الغاز والبخار والماء والكهرباء والتي يتم توفيرها مقابل رسوم أو تعويضات محددة.

(٢) المادة ٥٠٢ من قانون ولاية كاليفورنيا.

وبعده مذبناً بجناية من الدرجة الخامسة إذا ألحق ضرراً تزيد قيمته عن ١٠٠٠ دولار، وبجناية من الدرجة الرابعة إذا سبب ضرراً تتجاوز قيمته ٣٠٠٠ دولار وبجناية من الدرجة الثالثة إذا سبب ضرراً تتجاوز قيمته ٥٠٠٠ دولار^(١).

كما قد تأثر المشرع الفرنسي بهذا الاتجاه في قانون العقوبات الحديث، ولذلك فقد اتجه تحت عنوان جرائم أخرى ترتكب ضد الملكية إلى تجريم الاعتداءات التي ترتكب في مواجهة نظام المعالجة الآلية في المادة ١١٣٢٣ وما يليها، ونص في هذه المواد على جرائم الدخول والبقاء في نظام المعالجة الآلية للبيانات وإعاقة أو إفساد نظام التشغيل والإتلاف المعلوماتي^(٢)، وبهذا فإن المشرع الفرنسي يكون قد عامل المعلومات معاملة الأشياء التي يرد عليها حق الملكية لورودها ضمن الجرائم التي ترتكب ضد الملكية^(٣).

ثانياً: الاتجاه الثاني

يهتم هذا الاتجاه بالمعلومات ذاتها باعتبارها من الأشياء التي تقدم منفعة، ولذلك فهو ينظر إلى المعلومات باعتبارها تشكل قيمة في ذاتها ولها خصائصها الذاتية التي تميزها عن غيرها من القيم، ولذلك فالهدف في هذه الحالة هو حماية المعلومات في ذاتها سواء تعلقت بالحياة الخاصة أو كانت لها قيمة اقتصادية أو تعلقت بمصالح الدولة أو غير ذلك من المعلومات التي يخشى المساس بها، ولذلك فإن التشريعات التي تأخذ بهذا الاتجاه تفرد نصوص خاصة لحمايتها^(٤).

وقد تأثر المشرع الأمريكي على المستوى الفيدرالي بهذا الاتجاه، ولهذا فهو ينص على تجريم موسع لجريمة الدخول، فيجرم في المادة ١٠٣٠ من قانون إساءة استخدام الحاسبات الآلية كلاً من أفعال الدخول إلى نظام الحاسب الآلي الذي يعمل لأجل أو بالنيابة عن حكومة الولايات المتحدة الأمريكية إذا كان من شأن هذا السلوك

(١) المادة ٥٠٢ من قانون ولاية كاليفورنيا.

(٢) المادة ٣٢٣ من قانون العقوبات الفرنسي.

(٣) د. أيمن فكري، المرجع السابق، ص ٥٠٥.

(٤) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٠٩.

أن يؤثر على استخدام الحاسب، ويجرم أيضاً أفعال الدخول إلى المعلومات التي يحتويها نظام الحاسب الآلي والتي تم تحديدها من قبل حكومة الولايات المتحدة الأمريكية بموجب أمر تنفيذي أو لوائح تطلب الحماية ضد الاطلاع غير المصرح به لأسباب تتعلق بالدفاع الوطني أو العلاقات الخارجية أو أية بيانات سرية المحددة بموجب الفقرة ذ من المادة ١١ من قانون الطاقة الذرية لعام ١٩٥٤ إذا ما كانت نية الفاعل استخدام هذه المعلومات ضد الولايات المتحدة الأمريكية أو أية دولة أجنبية، وأفعال الدخول إلى المعلومات الواردة في سجلات المؤسسات المالية أو التي تمنح بطاقات مالية أو المعلومات التي تتعلق بالمستهلكين أو المعلومات التي يحتويها نظام الحاسب الآلي الذي يعمل لمصلحة الولايات المتحدة الأمريكية أو التي يحتويها نظام الحاسب المزود بحماية فنية، وكذلك فهو يجرم الدخول إلى نظام الحاسب الآلي الذي يتم بقصد الاحتيال إذا تم الحصول على أي شيء له قيمة أو تم التسبب بالضرر أو الخسارة أو تم استخدام خدمات من الحاسب الآلي تتجاوز قيمتها ٥٠٠٠ دولار خلال سنة واحدة^(١).

كما قد نصت المذكرة الإيضاحية للاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية على أنَّ الغرض من جرائم التعدي على المعلومات هو حماية سرية وسلامة وتوافر الأنظمة المعلوماتية^(٢)، كما خلصت اللجنة القانونية في البرلمان الانكليزي إلى أنَّ قانون إساءة استخدام الحاسب الآلي قد بُني أساساً على الحاجة إلى حماية سلامة وأمن الأنظمة المعلوماتية^(٣)، إلا أنَّ التطبيق العملي لهذا المفهوم من شأنه إسباغ بعض الحماية الجزائية على المعلومات الأخرى التي تحتفظها هذه الأنظمة^(٤)، وقد خلصت هذه اللجنة إلى هذا الرأي للتوفيق بين ضرورة حماية المعلومات وعدم

(١) المادة ١٠٣٠ من القانون الأمريكي الفيدرالي لإساءة استخدام الحاسبات الآلية.

(2) Council of Europe, Explanatory Report for Convention on Cybercrime, para.43

(3) Law Com. No.186, Computer Misuse. Cm.819 1989, para.1.37

(4) Law Com. No.186, Computer Misuse. Cm.819 1989, para.2.13

صلاحيتها للحماية وفق نصوص قانون الأضرار الجزائية ١٩٧١^(١)، ولتلافي الانتقادات التي وجهت إلى جريمة الدخول غير المصرح بشأن التمييز الذي أفرزته بين المعلومات التي يحتويها نظام الحاسب وسواها من المعلومات التي تحتويها الأجزاء الالكترونية الأخرى كبطاقات الدفع، ولاعتبارها تشكل في أحد أوجهها - تعدياً على الخصوصية والتي لم يتم إسباغ الحماية الجزائية عليها إلا في نطاق ضيق في القانون الانكليزي^(٢).

ثالثاً: الاتجاه المختلط

بالإضافة إلى الاتجاهين السابقين فإنّ هناك موقفاً تشريعياً يجمع بينهما، ويتوقف ذلك بطبيعة الحال على شكل السلوك الذي يرى المشرع أنّه يهدد المصالح في المجتمع، فهو يقوم في بعض النصوص بحماية الملكية في حين تقوم نصوص أخرى بحماية المعلومات في ذاتها^(٣)، ومن قبيل ذلك اتجاه المشرع السوري في قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، حيث استند إلى حماية الملكية من خلال تجريم أفعال شغل اسم موقع الكتروني وإعاقة الوصول إلى الخدمة وإرسال البريد الواعل والاحتيال عن طريق الشبكة والاستعمال غير المشروع لبطاقات الدفع، كما اهتم بحماية المعلومات من خلال تجريم أفعال الدخول غير المشروع إلى منظومة معلوماتية واعتراض المعلومات وتصميم البرمجيات الخبيثة واستخدامها^(٤).

(1) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.61

(2) Macewan. Niel, 2008, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future', Criminal Law Review, University of Salford, Manchester, pp. 955-967, Retrieved 20\June\2014 from: <http://www.bailii.org/ew/other/EWLC/1989/186.pdf>

(3) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣١٠.

(4) الفصل الثالث من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، المواد من ١٥ وحتى ٢٢.

المطلب الثاني: المصلحة المحمية في جريمة الدخول

إنَّ جريمة الدخول تقع على سرية المعلومات، الأمر الذي يتطلب أن تتخذ المعلومات شكلاً يسبغ عليها السرية المراد حمايتها ، وتبعاً لذلك سنتناول المصلحة المحمية في جريمة الدخول من خلال دراسة سرية المعلومات أولاً، ثم نبين معيار السرية ثانياً.

أولاً: سرية المعلومات

كما أسلفنا سابقاً أن التشريعات في سياق حمايتها للمعلومات أخذت بأحد اتجاهين: الاتجاه الذي ينظر إلى المعلومات باعتبارها من قبيل الأشياء التي يرد عليها حق الملكية وبالتالي فإن جريمة الدخول في هذه الحالة تشكل تعدياً على هذا الحق، والاتجاه الذي ينظر إلى المعلومات باعتبارها من الأموال التي تنطوي على منفعة ولذلك فهو يهتم بحماية المعلومات في ذاتها، وبالنسبة للتشريعات التي أخذت بهذا الاتجاه فنجد فيها موقفين تشريعيين: أحدهما ينظر إلى جريمة الدخول باعتبارها تشكل انتهاكاً لسلامة المعلومات (النموذج الانكليزي)، والآخر ينظر إليها باعتبارها تشكل تعدياً على سرية المعلومات (النموذج الأمريكي)، إلا أنَّ التطبيق العملي للنموذج الانكليزي لم يسفر إلا على تطبيق جريمة الدخول على حالات محدودة، وهي الحالات التي ينطوي فيها الدخول على التعدي على السلامة التشغيلية للنظام محل الحماية، أما الحالات التي ينطوي فيها الدخول على مجرد انتهاك سرية المعلومات فإنَّها تعد من حالات المراقبة غير المصرح بها^(١)، وجريمة الدخول في حقيقتها تشكل تعدياً على المعلومات بمعنى انتهاك الخصوصية وسرية المعلومات، كما أنَّها تشكل تعدياً بمعنى الانتهاك والقرصنة سلامة المعلومات وهو موقف الاتفاقية الأوربية لمكافحة الجريمة المعلوماتية^(٢)، وإنَّ التطبيق العملي للنموذج الأمريكي من شأنه أن يسبغ هذه الحماية على المعلومات، وذلك لأنَّ السرية المراد حمايتها في هذا النموذج هي السرية ذات

(1) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.25

(2) Council of Europe, Explanatory Report for Convention on Cybercrime, para.44

الطابع الموضوعي والتي تقوم على إرادة المسؤول، وبمعنى آخر أنّ السرية التي يعتد بها تجاه الفاعل تكون في الحالات التي يقوم فيها بالدخول دون إذن من المسؤول، وبهذا المفهوم للسرية فإنّ جريمة الدخول تشكل أيضاً انتهاكاً للسلطات التي يخولها حق الملكية للمالك، ولهذا فإنّه يمكن القول بأنّ المصلحة الأساسية المراد حمايتها في جريمة الدول هي السرية بما تمثله من قيمة للمالك وفق الاتجاه الأول، وهي السرية باعتبارها أحد الخصائص الأساسية للمعلومات في الاتجاه الثاني.

وعلى الرغم من ذلك فإنّ الاتجاه الأول منتقد في الفقه وذلك لاعتباره المعلومات من قبيل الأشياء التي يرد عليها حق الملكية^(١)، في حين أنّ المعلومات ليست ذات طبيعة واحدة، فالمعلومات منها المالية والتجارية والاقتصادية ومنها الشخصية ومنها التي تتعلق بمصالح الدولة وغيرها، ولكل من هذه المعلومات طبيعتها المميزة وخصائصها التي تتفرد بها عن غيرها، وإنّ اعتبار المعلومات كلها ذات طبيعة واحدة يخالف المفاهيم المستقرة في القانون^(٢)، ذلك وإن سلمنا بأنّ حق الملكية يمكن أن يتعلق بالمعلومات التي تمثل قيمة محددة في الذمة المالية كالنقود الالكترونية فإنه لا يمكن التسليم بذلك بالنسبة للمعلومات التي تتعلق بالشخصية ولا تدخل بالذمة المالية^(٣)، ويتلافى الاتجاه الثاني والذي يهتم بحماية المعلومات هذا النقد من خلال اعتباره أنّ للمعلومات قيمتها الذاتية متى ارتبطت بشخص أو كيان محدد، ولذلك فهو يحمي السرية باعتبارها أحد الخصائص الأساسية للمعلومات.

ثانياً: معيار سرية المعلومات

كما أسلفنا سابقاً أنّ جريمة الدخول تستهدف حماية سرية المعلومات، وبالتالي فإنّ المعلومة التي يحظر الوصول إليها يجب أن تنسم بالسرية، وتكون للمعلومة هذه الخاصية من خلال وجودها داخل النظم المعلوماتية، وأن تكون هذا النظم مغلقة، وغير

(١) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٠٩.

(٢) د. أيمن فكري، المرجع السابق، ص ٥١٩.

(٣) د. صبري حمد خاطر، لتأسيس لنظام قانوني للمعلومات، المجلة الدولية للملكية الفكرية، جامعة البحرين، المجلد الأول، العدد الأول، ٢٠١٣، ص ٨٦.

متاحة للجمهور، ولا يتم الدخول إليها إلا بتوافر شروط يحددها مسؤولو النظم، كالانتساب إلى هيئة معينة أو دفع اشتراك محدد أو الحصول على تصريح بالدخول، فمناطق سرية المعلومات هي وجودها في النظام المعلوماتي وعدم إتاحة الاطلاع عليها إلا لفئة محددة من الأشخاص وفق معيار يضعه المسؤول، وهذا ما يثير التساؤل عن مدى ضرورة وجود حماية فنية للنظم ؟

- ١ - قواعد الحماية الفنية:

يقصد بقواعد الحماية الفنية القواعد التي يراد منها حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تكفل تأمين المنشأة والأفراد والعاملين فيها وأجهزة الحاسبات المستخدمة ووسائل المعلومات، وذلك من خلال إتباع إجراءات ووسائل حماية عديدة تضمن أمن المعلومات، وتبدأ هذه القواعد بما يطلق عليه قواعد الأمن المادي، والتي تتمثل في حماية مركز الحاسب من الأخطار المادية التي يتعرض لها كالحريق أو انقطاع الإمداد بالطاقة الكهربائية أو التخريب أو الاقتحام أو السرقة^(١).

والى جانب هذه القواعد يوجد قواعد أخرى أكثر تعقيداً، ومنها وضع عوائق تحول دون التقاط الموجات الكهربائية الصادرة عن الأجهزة الالكترونية والتي يتم من خلالها معرفة محتوى المعلومات التي يتم نقلها، ويمكن أن يتم ذلك من خلال حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن ذلك أيضاً توزيع العمليات التي يقوم بها نظام الحاسب الآلي إلى نظام احتياطي عند الضرورة على أن يظل موقع هذا المركز سرياً ويخضع للحماية^(٢)، ومن تدابير الحماية استخدام نظام التعريف بشخص المستخدم ووثوقية الاستخدام ومشروعيته التي تهدف إلى ضمان استخدام النظام والشبكة من قبل الشخص المخول له بالاستخدام، وتضم استخدام كلمة السر بأنواعها، أو البطاقات الذكية المستخدمة للتعريف عن المستخدم، أو استخدام الوسائل البيولوجية التي تعتمد سمات الشخص المستخدم المتصلة ببنائه البيولوجي كبصمة

(١) د. حسن طاهر داود، المرجع السابق، ص ٣٦.
(٢) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٥٢.

الإصبع أو شبكية العين أو استخدام المفاتيح المشفرة والتي يمكن أن تشمل ما يعرف بالآقفال الالكترونية التي تحدد مناطق النفاذ^(١).

- ٢ - موقف الفقه من الحماية الفنية:

ينقسم الفقه القانوني في مطلب وجود حماية فنية للمعلومات محل الحماية إلى اتجاهين: أحدهما يحصر الحماية القانونية بالمعلومات التي تتمتع بحماية فنية، وآخر يوسع من نطاق هذه الحماية لتشمل جميع المعلومات دون اشتراط الحماية الفنية.

- أ - الاتجاه الأول:

يستند أنصار الاتجاه الأول في اشتراطهم للقواعد الفنية إلى قواعد المنطق والعدالة التي تقتضي عدم حماية النظم التي لا تحميها القواعد الأمنية، حيث أنه من غير المقبول المساواة بين تلك الأنظمة المحمية وتلك التي تركها المسؤولون عنها عرضة للأخطار بإهمال إجراءات الحماية اللازمة^(٢)، ويقيس أنصار هذا الاتجاه جريمة الدخول غير المصرح به على جريمة انتهاك حرمة عقار، إذ أن هذه الجريمة لا تقع بمجرد الدخول إلى العقار وإنما يجب أن يكون الدخول مصحوباً باستعمال وسائل تكون قرينة على عدم رضا صاحب العقار^(٣)، ويستند أنصار هذا الاتجاه في تدعيم موقفهم إلى عدة أسباب ترجح وجود حماية فنية، ويتمثل السبب الأول في أن النظم المعلوماتية أصبحت تتميز بالانفتاح على الخارج من خلال الشبكات المعلوماتية والتي أتاح الوصول للمعلومات بشكل سهل ويسير بالنسبة للجميع مما يستوجب وجود حماية فنية من شأنها تقييد الوصول إلى المعلومات^(٤)، والسبب الثاني يتمثل في أن غياب الحماية

(١) أمن المعلومات/ <http://ar.wikipedia.org/wiki/>

(٢) بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، دون سنة نشر، ص ٢٦٧.

(٣) Council of Eroup, Computer Related Crime: Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, Strasbourg 1990, p. 52, Retrieved 2\Apr\2014 from: http://www.oas.org/juridico/english/cyber_links_coe.htm

(٤) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٥٣.

الفنية يؤدي إلى خلق شبهة لدى الفاعل في محل الجريمة وهذا ما يؤدي إلى انتفائها، إذ أنَّ القواعد القانونية تفترض أن يكون محل الجريمة محدداً وواضحاً لا لبس فيه بالنسبة للفاعل^(١)، أما السبب الثالث فيتعلق في أنَّ وصف فعل الدخول بأنه غير مشروع يتعلق بماديات الأمر الذي يجعل من فعل الدخول فعلاً محايداً لأنه لا يدل بحد ذاته على عدم المشروعية، ومن ثم كان من اللازم تحديده من خلال تطلب اختراق إجراءات الحماية الفنية^(٢)، ويضيف أنصار هذا الاتجاه أن الحماية الفنية للأنظمة تتيح التحقق من قيام الركن المادي للجريمة حيث أنَّ اختراق هذه الأنظمة يترك آثاراً يجعل من السهل التحقق من وقوع الجريمة، كما أنَّها تعد الوسيلة الأساسية من التحقق من قيام القصد الجرمي لدى الفاعل^(٣)، وعن مستوى الحماية التي تتطلب في نظام المعلومات فإن هذا الاتجاه لا يتطلب سوى الحد الأدنى من الحماية والتي تتحقق من خلال الإجراءات المادية أو بمجرد حماية النظام من خلال كلمة مرور^(٤).

- ب - الاتجاه الثاني:

يذهب أنصار الاتجاه الثاني إلى عدم اشتراط الحماية الفنية للمعلومات قياساً على جريمة السرقة، إذ أنَّ تمتع المال المسروق بالحماية من عدمه لا يؤثر على قيام الجريمة، فهي تقع بصرف النظر عن مقدار الصعوبة التي واجهت الجاني أثناء تنفيذها^(٥)، ويستند أنصار هذا الاتجاه في تدعيم موقفهم إلى عدة أسباب، يتمثل السبب الأول في أن تطلب مثل هذا الاشتراط من شأنه تضيق نطاق الجريمة إلى أقصى الحدود ويتجاهل الثغرات التي قد يقع فيها المبرمجون في الحالة التي يستغل فيها

(١) د. أيمن فكري، المرجع السابق، ص ٢٣٤.

(٢) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٥٤.

(٣) د. علي عبد القادر القهوجي، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤، ص ٥٩٥.

(٤) Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, p.52

(٥) Scot Law Com. No 106, Report on Computer Crime.Cm.174 1987, para.4.15

الفاعل هذه الثغرات للاعتداء على النظم^(١)، والسبب الثاني مستمد من مبدأ الشرعية القانونية الذي لا يتيح الخروج عن النصوص القانونية والتي جاءت بمعظمها مطلقة ولم تشترط وجود هذه الحماية^(٢)، والسبب الثالث يستند إلى مبادئ الإنصاف والعدالة والتي تقتضي حماية النظم المعلوماتية دون اشتراط الحماية الفنية التي يتطلب توفيرها تكاليفاً كبيرة قد يفتقر إليها مسؤولو النظم ولهذا فإن إخراج هذه النظم من نطاق الحماية فيها مجافاة للعدالة ولا سيما أن النظم غير المحمية أكثر عرضة للاعتداء من تلك المحمية، والسبب الرابع يستند إلى أن تطلب هذه الحماية من شأنها أن تتجاهل الحالات التي يتم فيها الدخول دون المرور بالإجراءات الأمنية وصعوبات تحديد ما إذا كان الدخول تم من خلال اختراق القواعد الأمنية^(٣)، ويضيف أنصار هذا الاتجاه أن مسائل الإثبات يجب أن لا تمتد إلى القواعد الموضوعية للجريمة حيث أن أثرها يجب أن يظل قاصراً على القواعد الإجرائية^(٤).

- ٣ - الاتجاهات التشريعية من تطلب الحماية الفنية:

تباينت التشريعات في تطلبها للحماية الفنية، حيث ذهبت بعض التشريعات إلى عدم اشتراط وجود قواعد فنية تحمي المعلومات ومن قبيل هذه التشريعات القانون الفرنسي^(٥) والبلجيكي^(٦) والانكليزي^(٧) والأمريكي^(٨) والكندي^(٩) والسويدي^(١٠)

(١) محمد خليفة، المرجع السابق، ص ١٣٦.

(٢) آمال قارة، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، ٢٠٠١-٢٠٠٢، ص ٣٥، استخرج في ٢٠ كانون الثاني ٢٠١٤ من الموقع الإلكتروني:

http://djelfa.info/csrct/wp-content/uploads/2014/03/pdf.الجريمة_المعلوماتية.pdf

(٣) Scot Law Com. No 106, Report on Computer Crime.Cm.174 1987, para.4.15

(٤) بلال أمين زين الدين، المرجع السابق، ص ٢٨٠.

(٥) المادة ٣٢٣ من قانون العقوبات الفرنسي.

(٦) المادة ٥٥٠ من قانون العقوبات البلجيكي.

(٧) المادة ١ من قانون إساءة استخدام الحاسبات الآلية الانكليزي.

(٨) المادة ١٠٣٠ من القانون الفيدرالي لإساءة استخدام الحاسبات الآلية.

(٩) المادة ٣٤٢ من قانون العقوبات الكندي.

(١٠) القسم ٩ من الفصل ٤ من قانون العقوبات السويدي.

والدانماركي^(١) والسوري^(٢)، وقد ذهبت بعضاً من هذه التشريعات إلى تجريم الأفعال التي تساعد على اختراق قواعد الحماية الفنية كما في القانون الأمريكي الذي جرم أفعال الاتجار بكلمات المرور والمعلومات المشابهة التي تساعد على الوصول إلى الحاسب الآلي^(٣)، وكذلك الأمر في القانون الكندي الذي جرم أفعال الاستخدام أو المتاجرة بكلمات المرور أو السماح بالحصول عليها^(٤).

والى جانب هذه التشريعات فإن هناك تشريعات أخرى تشترط الحماية الفنية للمعلومات ومن قبيل هذه التشريعات القانون الألماني^(٥) والسويسري^(٦) والفنلندي^(٧) والاطالي^(٨) والهولندي^(٩) والنرويجي^(١٠)، وقد تطلبت بعضاً من هذه التشريعات أن يتم الدخول من خلال اختراق قواعد الحماية كما هو الحال في القانون السويسري الذي يشترط أن يتم الدخول من خلال اختراق القواعد الأمنية التي تحمي الأجهزة الالكترونية في مواجهة كل دخول يتم من قبل الفاعل^(١١)، كما يتطلب القانون الفنلندي أن يتم الدخول من خلال استخدام كلمة المرور أو باختراق قواعد الحماية الأخرى^(١٢)، كما يتعين في القانون الهولندي أن يتم الدخول من خلال اختراق الأنظمة الأمنية^(١٣)،

وكذلك الحال في القانون النرويجي الذي يتطلب أن يتم الدخول عن طريق اختراق القواعد التي تحمي المعلومات^(١٤)، ومن هذه التشريعات من يجرم الأفعال التي

(١) المادة ٢٦٤ من قانون العقوبات الدانماركي.

(٢) المادة ١٦ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

(٣) المادة ١٠٣٠ من القانون الفيدرالي لإساءة استخدام الحاسبات الآلية.

(٤) المادة ٣٤٢ من قانون العقوبات الكندي.

(٥) المادة ٢٠٢\أ من قانون العقوبات الألماني.

(٦) المادة ١٤٣ من قانون العقوبات السويسري.

(٧) القسم ٤ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(٨) المادة ٦١٥ من قانون العقوبات الايطالي.

(٩) المادة ١٣٨\أ من قانون العقوبات الهولندي.

(١٠) المادة ١٤٥ من قانون العقوبات النرويجي.

(١١) المادة ١٤٣ من قانون العقوبات السويسري.

(١٢) القسم ٤ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(١٣) المادة ١٣٨\أ من قانون العقوبات الهولندي.

(١٤) المادة ١٤٥ من قانون العقوبات النرويجي.

تساعد على اختراق قواعد الحماية كما هو الحال في القانون الايطالي الذي يجرم أفعال النشر والحياسة غير المشروعة للشيفرات الخاصة بالدخول إلى الحاسب الآلي^(١).

والى جانب هذه التشريعات فإن القانون اليوناني نص على الحماية الفنية للمعلومات على سبيل الاسترشاد فهو يعاقب على الدخول إلى المعلومات التي يحتويها النظام وخاصة الدخول الذي يتم من خلال انتهاك الحظر أو التدابير الأمنية المفروضة من قبل المسؤول^(٢)، كما أن المشرع البرتغالي ينظر إلى القواعد الأمنية باعتبارها ظرفاً مشدداً للعقوبة فهو يجرم الدخول إلى نظام الحاسب ويشدد العقوبة في الحالات التي يكون فيها هذا النظام محمياً^(٣).

وينبغي -في رأينا- عدم تطلب الحماية الفنية للمعلومات كشرط لإسباغ الحماية الجزائية عليها، وإنما يمكن النظر إلى هذه الحماية كأحدى القرائن على توافر القصد الجرمي، ذلك أنه من السهل التحقق من اتجاه إرادة الفاعل إلى التعدي على المعلومات متى كان ذلك نتيجة لمخالفة القواعد الفنية لما يتطلبه ذلك من بحث عن وسيلة لاختراق الجدار الأمني، ويمكن النظر إلى الحماية الفنية أيضاً كأحدى الظروف المشددة للجريمة، حيث أن هذه الحماية تجعل من فعل التعدي أكثر خطورة لأنها دليل على أهمية المحتوى الذي أراد المسؤول حمايته من خلال الاستعانة بالقواعد الفنية.

(١) المادة ٦١٥ من قانون العقوبات الايطالي

(٢) المادة ٢١٣٧٠ من قانون العقوبات اليوناني.

(٣) المادة ٧ من الفصل ١ من القانون الجزائي لحماية المعلومات البرتغالي.

خلاصة الفصل الأول

- ١ - إنّ المحل المادي الذي ينصب عليه نشاط الدخول هو المعلومات الالكترونية التي يتكون منها نظام المعلومات.
- ٢ - إنّ وصف نظام المعلومات يسبغ على أي كيان يتوافر فيه مجموعة مكونات مادية ومنطقية محددة.
- ٣ - تمثل المعلومات مجموعة من الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلاً محدداً يجعلها قابلة للتبادل والتفسير والمعالجة بواسطة الأفراد أو بوسائل الكترونية، وهي تشمل كل المكونات المنطقية لنظام المعلومات.
- ٤ - إنّ التدخل التشريعي في مواجهة الاعتداءات على المعلومات يمكن أن يبنى على أساس حماية حق الملكية، أو حماية المعلومات ذاتها.
- ٥ - إنّ المصلحة المحمية في جريمة الدخول هي سرية المعلومات.
- ٦ - تتصف المعلومات بالسرية من خلال وجودها في إطار نظام معلوماتي، وكان هذا النظام مغلق، وغير متاح للجمهور، ولا يتم الدخول إليه إلاّ بتصريح من المسؤول.
- ٧ - إنّ الحماية التقنية للمعلومات ليست شرطاً لإسباغ الحماية القانونية على المعلومات من خلال جريمة الدخول.

الفصل الثاني: ركني الدخول

إنَّ الدخول أصبح يشكل جريمة مستقلة ومتميزة عن غيرها من الجرائم الأخرى، وقد استجابت معظم الدول إلى ما جاءت به توصية المجلس الأوروبي بشأن تجريم الدخول غير المصرح به إلى المعلومات، وتعد الاتفاقية الأوروبية بشأن مكافحة الجريمة المعلوماتية النموذج الذي احتذت بها معظم التشريعات في هذا الشأن، وتعد سوريا من البلدان التي تضمنت تشريعاتها نصوصاً قانونية تجرم الدخول غير المصرح به، وقد سبقتها في ذلك عدداً من الدول وفي مقدمتها البلدان الأوروبية والولايات المتحدة الأمريكية، هذا وقد أصبحت الدراسة التحليلية لنشاط الدخول يقتضي وصفاً قانونياً خاصاً مستقلاً عن غيره من الأوصاف الأخرى، ولهذا يتعين علينا دراسة أركان جريمة الدخول بقصد التعرف على خصوصيتها من جهة، وإبراز الاختلافات بينها وبين غيرها من الجرائم من جهة أخرى.

وفي تحليلنا لجريمة الدخول كحقيقة قانونية لن نستطيع الخروج عما جرى العمل عليه من عرض للركن المادي والمعنوي للجريمة، ولكل منهما عناصره وخصوصيته، فبينما يتمثل الركن المادي بالوجه الخارجي للسلوك وهو أول ما يعير الانتباه إليه، فإن الركن المعنوي يتمثل بالوجه الباطني النفساني للسلوك وهو لا يتعدى انتماء السلوك إلى نفسية صاحبه، وتبعاً لذلك فسنتناول هذا الفصل في بحثين: نتحدث في المبحث الأول منه عن الركن المادي للجريمة، فيما نتحدث في المبحث الثاني عن الركن المعنوي لجريمة الدخول.

المبحث الأول: الركن المادي.

المبحث الثاني: الركن المعنوي.

المبحث الأول: الركن المادي

إنَّ جريمة الدخول كغيرها من الجرائم لا تقوم دون سلوك مادي ينبعث من نفسية صاحبه ويتخذ صورة أفعال خارجية يمكن استظهارها والتعرف عليه باستخدام الحواس^(١)، وللركن المادي أهمية واضحة في الجريمة إذ بغير ماديات ملموسة لا ينال المجتمع اضطراباً ولا يصيب الحقوق الجديرة بالحماية عدواناً، كما أنَّ قيام الجريمة على ركن مادي يجعل إقامة الدليل عليها أمراً ميسوراً^(٢)، ويكمن جوهر الركن المادي في جريمة الدخول بأفعال الوصول إلى المعلومات، وهذا ما يتطلب نشاطاً إجرامياً من جهة الفاعل يتم من خلاله هذا الوصول وأثراً يترتب على هذا النشاط وهو الوصول ذاته، وتبعاً لذلك فسنتناول هذا المبحث من خلال مطلبين: نتناول في الأول فعل الدخول، بينما نتناول في الثاني الوصول إلى المعلومات.

المطلب الأول: فعل الدخول

فعل الدخول هو النشاط الذي يتحقق من خلاله مخالفة القاعدة القانونية، وتتخذ فيه الإرادة الجرمية مظهرها المادي^(٣)، وهو يعد أهم عناصر الركن المادي لأنه يمثل المظهر المادي للإرادة الجرمية، فمن المعلوم أن المشرع لا يتدخل بالتجريم والعقاب ما لم تبرز الإرادة الجرمية إلى حيز الوجود في شكل مادي محسوس^(٤)، وجريمة الدخول كغيرها من الجرائم تتطلب نشاطاً جرمياً ينشأ عنه الوصول غير المصرح به إلى المعلومات، وإنَّ دراسة النشاط الجرمي لجريمة الدخول يتطلب توضيح مفهوم الدخول ونطاقه والوسيلة التي يتحقق من خلالها والصفة غير المشروعة التي يسبغ بها.

(١) د. رمسيس بهنام، المرجع السابق، ص ٤٨٧.

(٢) د. محمود نجيب حسني، المرجع السابق، ص ٢٦٧.

(٣) المرجع ذاته، ص ٢٧١.

(٤) د. محمد الفاضل، الجرائم الواقعة على الأشخاص، مطابع فتي العرب، الطبعة الثالثة، دمشق،

١٩٦٥/١٣٨٤م، ص ١٢١.

أولاً: مفهوم الدخول

يمكن تعريف الدخول بأنه جميع الأفعال التي من شأنها أن تؤدي إلى الولوج أو النفاذ إلى النظام المعلوماتي^(١)، وعلى الرغم من أن مصطلح الدخول يمكن أن يثير عدداً من الاحتمالات إلا أن أغلب التشريعات ومنها القانون السوري لا تتضمن تعريفاً للدخول، فهي تستخدم هذا المصطلح مجرداً دون إعطاء معنى له، وهذا ما يفتح المجال أمام المحاكم لتوضيح المراد بهذا المصطلح، ولعل من أفضل التفسيرات لمعنى الدخول ذاك التفسير التي قدمته محكمة كنساس العليا أثناء نظرها في قضية الولاية ضد (Allen) ، وتطور وقائع القضية حول قيام المتهم باستخدام حاسبه للدخول إلى النظام الخاص بشركة الهاتف الجنوبية الغربية التي تتحكم بمقاسم الاتصالات بعيدة المدى ليتلاعب ببياناته، بحيث تمكن من إجراء الاتصالات بعيدة المدى مجاناً، وتوصل المحققون إلى أن المتهم عندما اتصل بالنظام طالبه بإدخال بيانات المرور والتي ربما استطاع التوصل إليها عن طريق تخمين كلمة المرور بدقة، وقام فيما بعد بإزالة الدليل على نشاطه بإلغاء السجلات.

وقد اتهمت النيابة العامة الفاعل بارتكابه جريمة الدخول استناداً إلى التعريف التشريعي الواسع لعبارة access والذي ينص على أن الدخول يعني الاقتراب، الإرشاد، التواصل مع، تخزين البيانات في، استرجاع البيانات من..... أو أي استخدام لموارد الحاسب الآلي، إلا أن محكمة الموضوع رفضت الاستناد إلى هذا التعريف، وأوضحت بأنه كان من الاتساع بحيث لو أخذ على محمل الجد لحتم القول بعدم دستورية التشريع لغموضه، وانتهت المحكمة إلى أن المعنى الكامل والعادي يجب أن يطبق بدلاً من الترجمة المشوهة، ولذلك فقد استندت إلى تعريف قاموس Webster الذي يعرف الدخول كحرية أو قدرة على الحصول أو الاستفادة منه، وهذا مماثل للبناء الذي أعدته محكمة الموضوع للوصول إلى عدم وجود دليل يفيد بأن المتهم قد تمكن من الدخول إلى النظام المعلوماتي، فحتى مرحلة ما قبل وضع المتهم اسم المستخدم وكلمة المرور

(١) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩، ص ٢٤٢.

لا يمكن القول بأن لديه القدرة على الحصول أو الاستفادة من أي شيء، وعليه لا يمكن القول بأنه تمكن من الدخول إلى النظام^(١).

ويظهر أن المحكمة اعتمدت في تفسيرها لمعنى الدخول على نهج الواقع الافتراضي، حيث أن بيانات الدخول الصحيحة تسمح للمستخدم بالدخول إلى النظام والقدرة على الاستفادة من المحتوى، بينما البيانات الخاطئة تمنع المستخدم من هذا الدخول، وبغياب الدليل بأن المتهم قد دخل عبر تخمين كلمة المرور للوصول إلى المحتوى، فإنه يؤدي إلى القول بعدم دخوله إلى النظام^(٢).

وقدمت محكمة واشنطن العليا تفسيراً آخر في قضية الولاية ضد (Riley) والتي تشبه وقائع القضية السابقة، حيث تمكن المتهم من الاتصال بالنظام المعلوماتي الخاص بشركة الاتصالات الشمالية الغربية وتخمين كلمات السر العشوائية دون أن يعرف إذا ما كان قد توصل إلى كلمة سر صحيحة تخوله إجراء مكالمات هاتفية بعيدة المدى مجاناً، وقال المتهم إن سلوكه لا يعد دخولاً إلى النظام استناداً إلى تعريف ولاية واشنطن للدخول، والذي يتطابق مع تعريف ولاية كنساس والتي برأت Allen في قضية مماثلة، ومع ذلك فقد أدانت محكمة واشنطن المتهم اعتماداً على التعريف القانوني، واعتمدت المحكمة في قرارها على أن محاولات المتهم المتكررة لاكتشاف كلمة المرور المكونة من ٦ أرقام عن طريق إدخال أرقام بالتتابع تشكل أو تقترب من تشكل الاستفادة من محتوى النظام، حيث أنه بتبديل الأرقام في كل محاولة كان يقترب من النجاح في الوصول إلى محتوى النظام وبالتالي فإن سلوكه يعد دخولاً^(٣).

(1) State v. Allen, 1996, Retrieved 8\Aug\2014 from: <http://files.grimmelman.net/cases/Allen.pdf>

(2) Kerr. Orin, 2003, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 New York University Law Review 1596, p. 1627, Retrieved 10\Jun\2014 from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740##

(3) State v. Riley, 1993, Retrieved 8\Aug\2014 from: <http://law.justia.com/cases/washington/supreme-court/1993/59245-4-1.html>

وان إدانة Riley وتبرئة Allen يعود إلى أن الادعاء قد تمكن من إثبات أن Riley خمن كلمات المرور في حين أنه لم يتمكن سوى من إثبات مجرد مطالبة Allen بتسجيل الدخول، أو قد يعود إلى الاختلاف بين المحكمتين في تفسير معنى الدخول، فبينما تنتظر محكمة كنساس إلى الدخول من منظور العالم الافتراضي وتعرفه بأنه الاقتراب من الحصول على المحتوى، فإن محكمة واشنطن تنتظر إليه من زاوية الواقع المادي وتعرفه بأنه إرسال رسالة إلى النظام^(١).

ومما سبق يتبين أن الدخول المراد تجريمه وفق جريمة الدخول غير المصرح به هو الدخول ذو الطبيعة المعنوية، والذي يتماثل في طبيعته مع الدخول في ذاكرة إنسان أو قدرته على التفكير^(٢)، ووفق هذا التصور فإن الدخول يجب ألا يفهم وفق المنظور المادي، وذلك لاختلاف المعايير التي تحكم الواقع المادي عن تلك التي تحكم العالم الافتراضي، فما يمكن عده دخولاً وفق المفهوم الأول لا يمكن عده كذلك وفق المفهوم الثاني، فالحاسبات الآلية من وجهة النظر المادية تعرف بأنها الأجهزة التي تقوم بعملية الاتصال بإرسال واستقبال المعلومات، أما من وجهة نظر العالم الافتراضي فتعرف بأنها البرامج التي تتولى عملية معالجة البيانات وتحولها إلى معلومات^(٣).

ولتوضيح الاختلاف بين المفهومين نتخيل أن مستخدماً يحاول الدخول إلى حاسب آلي محمي بكلمة مرور، فيرسل طلباً إلى الحاسب الآلي يسأله إرسال الصفحة التي تطالبه بإدخال بيانات الدخول، فيزعن الحاسب الآلي لذلك كما لو أنه أشبه بالسير إلى باب مغلق ولكن حتى الآن لم يتم استخدام المفتاح، فوفق المنظور المادي يعد هذا الطلب دخولاً حيث أن الفاعل أرسل أمراً إلى الحاسب وتلقى الاستجابة المطلوبة، وبالمثل فإنه يمكن النظر إلى إرسال البريد الإلكتروني، حيث أن المستخدم لن يفهم أنه دخل إلى مزود خدمة الانترنت، فالمستخدم أرسل اتصالاً إلى مزود الخدمة والتي تقوم

(1) Kerr. Orin, opcit, p. 1627

(2) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، ٢٠٠٧، ص ١٤٢.

(3) Kerr. Orin, op.cit, p. 1620

خدماته على استقبال الاتصال والاستمرار في الإجراء، فهذا السلوك يعد دخولاً من وجهة نظر العالم المادي للنظام المعلوماتي إلا أنه لا يعد كذلك من وجهة نظر العالم الافتراضي، إذ أنَّ الفاعل لم تتاح له بسلوكه هذا أيّاً من قابلية استخدام النظام أو الاستفادة من محتواه^(١).

ولقد تبنى التقرير التفسيري للاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية رأياً يتفق مع الطبيعة المعنوية لفعل الدخول، فأشار إلى أنَّ المقصود بفعل الدخول هو التسلل على السلامة أو إلى أي من أجزاء النظام المعلوماتي من دون أن يشتمل على الإرسال العادي للرسائل الالكترونية أو البطاقات في النظام^(٢).

وقد استندت اللجنة القانونية في البرلمان الانكليزي في تعريف الدخول على تعريف قاموس أكسفورد والذي يعرف الدخول بأنه الوصول إلى المعلومات المخزنة في الحاسب الآلي أو نظام الحاسب الآلي أو النظام ذاته، مع استبعادها للحالات التي تنطوي على مجرد الوصول المادي إلى الحاسب الآلي أو الوصول إلى المعلومات المطبوعة، وفي سبيل استبعاد هذه الحالات فهي تحدد فعل الدخول بأنه الدخول الذي يسبب أداء الحاسب لأي وظيفة، وعلى الرغم من تسليم اللجنة بأن هذا التحديد من شأنه أن يمتد إلى الحالات التي يقوم فيها الفاعل بمجرد تشغيل الحاسب، إلا أنها تعمل على النية الجرمية لدى الفاعل لاستبعاد الحالات التي لا تنطوي على مخاطر حقيقية على الحاسب من نطاق التجريم^(٣).

وبذلك ننتهي إلى أنَّ الدخول المراد تجريمه هو الدخول المنطقي أو المعلوماتي والذي يتم من خلال إجراء اتصال مع النظام بإحدى الوسائل الفنية، ولهذا الدخول طبيعته المعنوية والذي يختلف في مفهومه عما هو متصور في العالم المادي، وهذا التحديد للدخول هو الذي يتفق مع الطبيعة المعنوية للمكونات المنطقية، كما أنه

(1) Ibid, p. 1621

(2) Council of Europe, Explanatory Report for Convention on Cybercrime, para.46

(3) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.26

يتمشى مع موجبات تجريم الدخول والتي تأتي في مقدمتها حماية المعلومات من الوصول غير المصرح إليها.

ثانياً: وسيلة الدخول

تختلف الوسائل التي يمكن اللجوء إليها للدخول إلى نظام المعلومات، ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الحاسب الذي يحتوي النظام أو فتح البرنامج الذي يقوم بتشغيله أو استخدام حاسب مفتوح، وقد يتطلب الدخول الحصول على شيفرات الدخول باستخدام أجهزة خاصة لفك الشيفرات، أو قد يتم الدخول من خلال التحايل على بروتوكول الانترنت عن طريق انتحال عنوان مسجل لأحد الأنظمة للوصول إلى النظام المستهدف، كما يمكن أن يتم الدخول من خلال وسائل أخرى للدخول إلى نظام المعلومات تعتمد على ضعف الأجهزة الأنظمة ذاتها أو على بعض الأخطاء الناجمة عن عمليات البرمجة^(١).

والقاعدة العامة في القانون أنه لا عبء للوسيلة التي يتم من خلالها النشاط الجرمي، وتبعاً لذلك فإن كل نشاط يتوسل به الفاعل الولوج إلى المعلومات يصلح لتكوين النشاط الجرمي في جريمة الدخول، إلا أن بعض التشريعات قد شذت عن هذه القاعدة بتطلبها أن يتم الدخول من خلال وسيلة معينة، كما هو الحال في القانون الاسترالي الذي يشترط أن يتم الدخول إلى نظام الحاسب الآلي الذي لا يتبع رابطة دول الكومنولث عبر شبكة الاتصالات العامة^(٢)، كما يتطلب القانون الفنلندي أن يتم الدخول باستخدام شيفرة دخول غير مصرح باستخدامها أو عن طريق اختراق القواعد الأمنية التي تحمي النظام^(٣)، ويستلزم القانون الهولندي بأن يتم الدخول من خلال اختراق القواعد الفنية أو باستخدام أجهزة خاصة أو شيفرة غير صحيحة^(٤)، وتضيق هذه التشريعات من نطاق جريمة الدخول من خلال اشتراط هذه الوسائل لأنها ترى أن

(١) د. خالد ممدوح ابراهيم، المرجع السابق، ص ٢٤٦.

(٢) المادة ١٤٧١ من قانون الجريمة الالكترونية الاسترالي.

(٣) القسم ٤ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(٤) المادة ١٣٨ من قانون العقوبات الهولندي.

الدخول العادي لا ينتج عنه مخاطر بالضرورة وإنّما قد يعد أحد أهم الوسائل في كشف نقاط الضعف في أمن المعلومات^(١).

وإذا كان الأمر كذلك في بعض التشريعات فإنّ معظمها لا تتطلب وسيلة معينة للدخول، إلا أنّها وبالتأكيد تتطلب أن يتم الدخول من خلال نشاط ما يتم من خلاله الوصول إلى المعلومات، ويبدو هذا الاشتراط واضحاً في بعض التشريعات، كما هو الحال في القانون الانكليزي حيث تتطلب المادة الأولى من قانون إساءة استخدام الحاسبات أن يتم الدخول إلى المعلومات والبرامج عن طريق نشاط ما يتسبب بقيام الحاسب بوظيفة معينة، إلا أنّه وفي تشريعات أخرى لا تتطلب هذا الاشتراط صراحة وإنّما هو أمر يمكن الوصول إليه من خلال القواعد العامة والتي تتطلب أن يقوم الفاعل بنشاط معين يمكن من خلاله إسناد الجريمة له.

ومهما كان الأمر فإنّه حتى في التشريعات التي لا تتطلب وسيلة محددة للدخول فإن الشكل الالكتروني للمعلومة محل الحماية والطابع المنطقي للنشاط الإجرامي من شأنهما أن يحدان من الوسائل التي يتم فيها الدخول، فالشكل الالكتروني للمعلومة يستبعد من نطاق الدخول الحالات التي يتم فيها الوصول إلى المخرجات المادية للمعلومات كالمستندات المطبوعة، كما يستبعد الطابع المنطقي للدخول حالات الدخول الذهني المحض كقيام الفاعل بقراءة معلومات ظهرت على شاشة الحاسب دون أن يكون قد قام بإحضارها بنفسه.

وينبغي - في رأينا - عدم اشتراط تحقق الدخول من خلال وسيلة محددة وهو أمر تفرضه الحماية الكاملة للمعلومات، إلا أنّه ومن جهة ثانية يمكن النظر إلى وسيلة الدخول باعتبارها مؤثر على ازدياد الخطورة الإجرامية تستلزم تشديد العقوبة تبعاً لذلك^(٢).

(1) Council of Europe, Explanatory Report for Convention on Cybercrime, para.49

(2) انظر الصفحة: - ٥١ -

ثالثاً: نطاق الدخول

يتمثل النشاط الإجرامي في جريمة الدخول بجميع الأفعال التي من شأنها أن تؤدي إلى الوصول إلى المعلومات، وفعل الدخول بهذا المفهوم يتداخل مع غيره من الأفعال الأخرى مثل البقاء في نظام المعلومات واعتراض المعلومات المرسلة عبر الشبكة والاستعمال غير المصرح به للنظام المعلوماتي.

- ١ - الدخول والبقاء في النظام:

إنَّ المقصود بالبقاء هو التواجد داخل النظام المعلوماتي ضد إرادة من له الحق في السيطرة عليها^(١)، ويرى بعض الفقهاء أنَّ البقاء بهذا المفهوم لا يختلف عن الدخول، وذلك مرده إلى اعتبارهم جريمة الدخول جريمة مستمرة، ففي نظرهم أنَّ النشاط الإجرامي في جريمة الدخول يمتد حتى تسجيل الفاعل خروجه من النظام، ووفقاً لهذا الرأي فإنَّ الأفعال المادية المكونة لنشاط الدخول تعتبر مستمرة فهي من ناحية تشكل واقعة الدخول، ومن ناحية أخرى تشكل واقعة البقاء في النظام، ولذلك فإنَّ جريمة الدخول تتحقق في أي وقت تتوافر فيه النية الإجرامية وحتى تسجيل الفاعل خروجه من النظام، ولذلك يخلص أصحاب هذا الرأي إلى أنَّ البقاء هو أحد صور الدخول غير المصرح به^(٢).

إلا أنَّ هناك رأياً آخر يعترض على ذلك بالقول بأنَّ وصف جريمة الدخول على أنَّها جريمة مستمرة مرده إلى الخلط بين النشاط الإجرامي لهذه الجريمة وأثارها^(٣)، فالركن المادي في جريمة الدخول ينتهي بمجرد وصول الفاعل إلى المعلومات، أما الحالة التي تعقب هذه الوصول فلا تعد من بين عناصر النموذج القانوني لجريمة الدخول، وإنَّما تعد مستقلة عنه وتتحقق باستمرار الفاعل في تواجده في النظام، وبذلك

(١) د. علي عبد القادر قهوجي، المرجع السابق، ص ٦٠١.

(٢) د. أيمن فكري، المرجع السابق، ص ٢٠٣.

(٣) المرجع ذاته، ص ٢٠٤.

يخلص هذا الرأي إلى القول بأن الاختلاف بين نشاط الدخول والبقاء يكمن في أن الأول نشاط آني في حين أن الثاني نشاط مستمر^(١).

ونظراً لهذا الاختلاف بين الدخول والبقاء فقد اتجهت بعض التشريعات إلى تجريم البقاء بنصوص خاصة، كما هو الحال في القانون الفرنسي الذي يجرم كلاً من الدخول والبقاء في نظام المعالجة الآلية للبيانات^(٢)، كما أن القانون البلجيكي يجرم كلاً من الدخول والاحتفاظ بالدخول إلى النظام الحاسب الآلي^(٣)، ويجرم أيضاً القانون الإيطالي كلاً من الدخول والبقاء في نظام الحاسب الآلي أو شبكات الاتصالات ضد إرادة المسؤول الضمنية أو الصريحة^(٤).

- ٢ - الدخول واعتراض المعلومات:

يعرف الاعتراض بأنه التصنت أو نقل البيانات التي تتم داخل جهاز الحاسب، أو التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة، أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات أو التي تتم عبر الأجهزة اللاسلكية، وذلك عبر أي من الوسائل الفنية^(٥)، وتعد أكثر الطرق استعمالاً في الاعتراض هي وضع وسائل سلكية تتصل بالنظام المعلوماتي أو عن طريق النقاط الرسائل عن بعد بوسائل حديثة^(٦)، وهو في هذا يعد أحد أشكال التجسس وهو مشابه لقراءة وثيقة خاصة بالاستعانة بمنظار أو الاستماع لمحادثة خاصة ممن خلال وضع جهاز تنصت خفي^(٧).

(١) بلال أمين زين الدين، المرجع السابق، ص ٢٧٣.

(٢) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

(٣) المادة ٥٥٠ ب من قانون العقوبات البلجيكي.

(٤) المادة ٦١٥ من قانون العقوبات الإيطالي.

(٥) بلال أمين زين الدين، المرجع السابق، ص ٣٠٦.

(٦) د. خالد ممدوح إبراهيم، المرجع السابق، ص ٢٤٩.

(٧) Scot Law Com. No 106, Report on Computer Crime.Cm.174 1987, para.2.10

والاعتراض يتفق مع الدخول في أنّ كلاهما يؤديان إلى الوصول إلى معلومات غير مصرح للفاعل الوصول إليها، إلا أنّه في حالة الاعتراض لا يكون للفاعل القدرة على التحكم بوظائف الحاسب، وعلى وجه الخصوص لا يمكنه تحديد المعلومات التي يحصل عليها، وإنّما يقتصر دوره على النقاط المعلومات التي يتم إرسالها من قبل شخص آخر وذلك على نقيض الدخول حيث يكون للفاعل القدرة على استدعاء البيانات والبرامج والتعامل معها^(١)، ولذلك في حالة الاعتراض لا بد وأن يكون قد تم تشغيل الحاسب الآلي الذي يحتوي المعلومات من قبل شخص آخر^(٢)، أما في حالة الدخول فلا يشترط ذلك، وإنّما قد يتم الدخول من خلال تشغيل هذا الحاسب^(٣)، ولذلك يمكن القول بأنّ الوصول إلى المعلومات قد تتم بطريقة مباشرة كما هو الحال في الدخول أو قد يتم بطريقة غير مباشرة كما هو الحال في الاعتراض^(٤).

وإنّ هذا الاختلاف بين الدخول والاعتراض هو الذي دفع المجلس الأوروبي إلى التوصية بإفراد نص خاص لتجريم الاعتراض الذي يتم بدون حق بواسطة الوسائل الفنية من أو في أو داخل نظام الحاسب أو شبكة الاتصالات^(٥)، كما جرمت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية أفعال الاعتراض، وسارت بعض التشريعات على هذا النهج كما هو الحال في القانون الفرنسي الذي يواجه أفعال الاعتراض من خلال التجريم الموسع لجريمة الدخول^(٦)، وكذلك هو الحال في القانون السوري الذي يجرم في المادة ١٨ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية يجرم

(1) Scot Law Com. No 106, Report on Computer Crime.Cm.174 1987, para.2.10

(2) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٥١.

(3) د. خالد ممدوح إبراهيم، المرجع السابق، ص ٢٥١.

(4) Council of Europe, Explanatory Report for Convention on Cybercrime, para.53

(5) Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, p. 54

(6) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

أفعال الاعتراض أو التتصت على المعلومات المتداولة على المنظومة المعلوماتية أو الشبكة^(١).

- ٣ - الدخول واستعمال النظام:

يعرف الاستعمال غير المصرح به بأنه كل استعمال غير مصرح به لوظيفة يؤديها الحاسب الآلي خلال فترة زمنية معينة^(٢)، والاستعمال بهذا المفهوم يتم من خلال كل استخدام للحاسب الآلي ونظامه للاستفادة من الخدمات التي يقدمها دون أن يكون هذا الاستخدام مشروعاً، وبهذا فهو يختلف عن الدخول غير المصرح به الذي يتم من خلال الوصول إلى المعلومات بغض النظر عن استعمالها، وهناك من يرى أنه يمكن التصدي للاستعمال غير المصرح به من خلال النصوص الخاصة بجريمة الدخول^(٣) باعتبار أن كل استعمال غير مشروع للنظام يشكل دخولاً غير مصرحاً به^(٤)، ونحن نتفق مع هذا الرأي، ونرى أن كون الدخول مصرحاً به لا يعني استبعاد إمكانية حصول استعمال للنظام كما هو الحال في استعمال الحاسب من قبل مستخدم غير أمين، ولهذا فإن أفعال الاستخدام غير المصرح بها يجب أن تتم مواجهتها من خلال نصوص خاصة.

وتبعاً لما تقدم فقد دعا المجلس الأوروبي في توصيته المتعلقة بالجرائم المتصلة بالحاسوب إلى تجريم الاستعمال غير المصرح به لخدمات الحاسب الآلي^(٥)، هذا وقد اختلفت التشريعات في ضرورة تجريم الاستعمال غير المصرح به، فعلى سبيل المثال لم يتضمن كلاً من القانون الفرنسي والانكليزي نصوصاً تجرم الاستعمال غير المصرح به لخدمات الحاسب الآلي، وقد استندت اللجنة القانونية المكلفة بوضع قانون إساءة

(١) المادة ١٨ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

(٢) د. نائلة عادل محمد فريد قوره، المرجع السابق، ص ٣٧٧.

(٣) محمد خليفة، المرجع السابق، ص ١٠٧.

(٤) د. خالد ممدوح إبراهيم، المرجع السابق، ص ٢٥٠.

(٥) Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, p.66

استخدام الحاسبات الآلية الانكليزي في ذلك إلى أنه ليس هناك ما يبرر التمييز بين الحاسب الآلي والمعدات الأخرى التي لم يتضمن القانون الجزائي تجريماً لاستعمالها^(١).

والى جانب هذه التشريعات فقد واجهت تشريعات أخرى أفعال الاستعمال من خلال جريمة الدخول، كما هو الحال في القانون الأمريكي الذي نص في المادة ١١٠٣٠ على تجريم الدخول غير المصرح به إذا ترتب على ذلك استعمال للمعلومات التي تم الدخول إليها، كما نصت المادة ٤١١٠٣٠ على تجريم الدخول إلى حاسب آلي وتم الحصول على خدمات تتجاوز ٥٠٠٠ دولار خلال سنة واحدة، كما شدد المشرع السوري في الفقرة ب من المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية عقوبة الدخول إذا تم استعمال البيانات أو المعلومات أو التصاميم التي يخترنها نظام المعلومات، وبالإضافة إلى ذلك فقد جرمت بعض التشريعات الاستعمال غير المصرح به في إطار منفصل عن جريمة الدخول، كما هو الحال في قانون العقوبات الكندي والذي جرم في المادة ١١٣٤٢ أفعال الحصول دون وجه حق وعن طريق الاحتيال بشكل مباشر أو غير مباشر على خدمات من الحاسب الآلي.

ومن خلال ما سبق يتبين أن للدخول نطاقه الخاص ومجاله الذي لا يتداخل به مع غيره من الأفعال، فالدخول يمكن تحديده بأنه التسلل الذي يتم إلى المعلومات، وهو يختلف عن الاعتراض الذي يتم من خلال النقاط الإشارات الكهربائية المتداولة، وإذا كان لكل من هذين الفعلين مجاله الخاص فإنهما قد يتكاملان في سبيل إنجاح المخطط الإجرامي للفاعل، كما في حالة اعتراض الفاعل للاتصالات في سبيل خلق ثغرة في الشبكة المعلوماتية تمكنه من الدخول إلى النظام.

كما يتميز الدخول عن البقاء الذي يتم من خلال امتناع الفاعل عن الخروج من النظام المعلوماتي، فلكل من هذين الفعلين نطاقه المحدد الذي لا يتداخل فيه مع

⁽¹⁾ Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.38

الآخر، فإذا انتفى فعل الدخول فقد يتحقق فعل البقاء، وإذا تحقق الدخول غير المصرح به فليس للبقاء محل إذ أنه في هذه الحالة يعد أثراً من آثار فعل الدخول وليس فعلاً إجرامياً قائماً بذاته.

كما يختلف الدخول عن الاستعمال، ففي حين يقع الدخول بمجرد وصول الفاعل إلى النظام فإنّ الاستعمال يتطلب استخداماً لهذا النظام، كما لا يرتبط أيّاً منهما بالآخر ارتباطاً وجودياً، ففي حين يتصور وقوع الدخول بمعزل عن الاستخدام فإنّ الاستخدام أيضاً لا يتطلب دخولاً.

رابعاً: الصفة غير المشروعة للدخول

إنّ فعل الدخول لا يشكل بحد ذاته فعلاً غير مشروع وإنما يستمد هذه الصفة من كونه غير مصرح به، أو بعبارة أخرى أن يكون دون وجه حق، وهو يتشابه في ذلك مع فعل الدخول إلى عقار، إلا أنّ مفهوم الإذن في حالة التعدي على الممتلكات العقارية يبدو واضحاً، حيث أنّ معظم الناس لديهم القدرة على فهم القواعد الاجتماعية التي تحكم ما إذا كان الشخص له الإذن في أن يكون موجوداً على ممتلكات الغير، إلا أنّ مفهوم الإذن في حالة الدخول المعلوماتي يبدو مفتقراً إلى هذا الوضوح، حيث أنّه يثير عدة تساؤلات حول الشخص الذي يملك الصلاحية في منح الإذن، والحالات التي يمكن فيها وصف الفاعل بأنه لم يكن مصرح له بالدخول.

- ١ - مسؤول التصريح:

كما قدمنا بأنّ الدخول غير المشروع هو الدخول غير المصرح به، ولذلك فقد كان تحديد المسؤول عن إعطاء هذا التصريح أمراً في بالغ الأهمية، إذ أنّ عدم مشروعية الدخول تتوقف على إرادته لأنه يملك حق التصرف والسيطرة على النظام، وقد عرفت المادة الثانية الاتفاقية الأوروبية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعلومات ذات الطابع الشخصي المسؤول بأنّه كل شخص طبيعي أو اعتباري أو كل سلطة عامة أو وكالة أو هيئة أخرى لها سلطة التصرف في النظام

وتحديد مضمونه ومحتواه وكيفية تنظيمه والغرض منه^(١)، كما عرفه الإرشاد الصادر عن البرلمان والمجلس الأوروبي بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات في المادة الثانية بأنه كل شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى يكون لها أو بالاشتراك مع غيرها سلطة على الحاسب الآلي^(٢).

وإذا كان في الأصل أن لا يكون للنظام سوى مسؤول واحد إلا أنه من الناحية النظرية يمكن تصور تعدد المسؤولين عن النظام والذين يتشاركون السلطات المختلفة على النظام أو يتقاسمونها، إلا أنه من الناحية العملية تكون السلطات المختلفة للمسؤولين متداخلة فيما بينها بحيث يصعب الفصل بينها بحيث يكون لكل منها مسؤول خاص.

كما تثار حالة تعدد المسؤولين عن النظام في الأنظمة المشتركة أو الأنظمة الناجمة عن أكثر من نظام، فبتعدد هذه الأنظمة يتعدد المسؤولون عنها ويصبح من الصعب تحديد الشخص المسؤول عن النظام الجديد، ويتم عادة في هذه الحالة تحديد الشخص المسؤول عن النظام الجديد، أما في الحالة التي لا يتم فيها تحديد المسؤول فإنه سيعيد كل مسؤول عن هذه الأنظمة المتعددة مسؤولاً عن النظام الجديد بالإضافة إلى كونه مسؤولاً عن نظامه الخاص^(٣).

(1) Convention for The protection of individuals with regard to automatic processing of personal data, Strasbourg, 28.I.1981, chapter ,article 2, Retrieved 20\Aug\2014 from:

<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

(2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 pp: 0031 – 0050, Retrieved 22\Aug\2014 from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

(3) نائلة عادل محمد فريد قورة، المرجع السابق، ص : ٣٣٦.

ومما لا شك فيه أن تحديد المسؤول له أهميته الخاصة في جريمة الدخول غير المصرح به، حيث أنّ الأشخاص المصرح لهم بالدخول هم مسؤولي الأنظمة والأشخاص الذين يصرح لهم بالدخول من قبل هؤلاء المسؤولين.

- ٢ - حالات عدم التصريح:

كما أسلفنا سابقاً أن مجرد الدخول لا يشكل فعلاً غير مشروع وإنّما يستمد هذه الصفة من كونه غير مصرح به، وقد نص المشرع السوري في المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على أنّ الدخول غير المشروع هو الدخول بغير حق أو بغير صلاحية أو تصريح، وعلى الرغم من أنّ المشرع السوري لم يبين ما هو المقصود بهذه الحالات، إلا أنّه يمكن القول أن المقصود بذلك هو الدخول الذي يتم بدون سلطة دون حق، أو بدون إذن من صاحب السلطة (دون تصريح)، أو بتجاوز الإذن الممنوح من صاحب السلطة (دون صلاحية)، وهذا يتماثل مع ما ذهبت إليه معظم التشريعات الأوروبية والأمريكية.

ويميز بعض الفقهاء بين حالات عدم المشروعية بين الدخول الذي يتم من قبل أشخاص من داخل النظام (الموظفين ومستخدمي النظام)، والدخول الذي يتم من قبل أشخاص من خارج النظام (القراصنة)، حيث أنّ الفئة الأولى لا يكون دخولهم غير مشروع إلا بتجاوز حدود التصريح الممنوح لهم، بينما الفئة الثانية يكون دخولهم يكون غير مشروع لأنه يفترق إلى تصريح من المسؤول^(١)، وتبدو أهمية هذا التمييز بين الفئتين في حالة التشريعات التي لا تجرم سوى الدخول غير المصرح به دون الدخول الذي يتم بتجاوز التصريح كما هو الحال في القانون الانكليزي، فالدخول الذي يفترق

⁽¹⁾ Jarrett H. Marshall & Michael W. Bailie, 'Prosecuting Computer Crimes: Crimes Computer Crime and Intellectual Property Section Criminal Division, Office of Legal. Education Executive Office for United States Attorneys, p. 4, Retrieved 26\Aug\2014 from: <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf>

إلى صفة المشروعية هو الدخول الذي يتم من قبل أشخاص ليسوا بذات صلة بالنظام محل الاعتداء.

كما يميز آخرون بين الدخول الذي يتم من قبل أشخاص من داخل المؤسسة التي ينتمي إليها النظام والدخول الذي يتم من قبل أشخاص خارج المؤسسة^(١)، وتبدو أهمية هذا التقسيم في الحالة التي يعد فيها الدخول من قبل العاملين في المؤسسة ظرفاً مشدداً للعقوبة، إلا أنه لا يعد تحديد ما إذا كان الشخص يتبع إحدى المؤسسات أمراً يسيراً في جميع الحالات، فهذه المسألة تثير إشكالية في حالة الأنظمة المشتركة، فهل يمكن اعتبار الشخص الذي يتبع إحدى المؤسسات التي ينتمي إليها أحد الأنظمة المشتركة يتبع أيضاً المؤسسات الأخرى التي ينتمي إليها أحد هذه الأنظمة؟

في رأينا لا يمكن ذلك، وإنما يمكن اعتبار أنّ النظام الجديد ينتمي إلى جميع المؤسسات التي تنتمي إليها أحد هذه الأنظمة، وبالتالي فإنّ مفعول الظرف المشدد ينطبق على جميع الأشخاص الذين يتبعون أيّاً من هذه المؤسسات عند قيامهم بالدخول غير المصرح به إلى النظام الجديد.

ولهذا فإنّه يمكن التمييز بين فئتين من الأشخاص داخل المؤسسة: أشخاص يخولهم مركزهم داخل المؤسسة إمكانية استغلاله في الدخول إلى النظام، وآخرون لا يخولهم مركزهم داخل المؤسسة ذلك، ومما لا شك فيه أنّ مفعول الظرف المشدد ينطبق على الفئة الأولى دون الثانية، ذلك أنّ العبرة من تشديد العقوبة هي خيانة الثقة الممنوحة للعامل، وهذا ما لا يمكن القول به إلا في حالة استغلاله للسلطات الممنوحة له.

ويشدد المشرع السوري العقوبة في المادة ٣٠ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على كل من يستغل عمله الوظيفي لارتكاب جريمة الدخول من دون أن يشترط أن يكون النظام المعتدى عليه منتبهاً إلى المؤسسة

(١) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٣٦.

التي ينتمي إليها العامل^(١)، فالمشرع السوري يرى أنه لا فائدة من التقسيم الذي يميز بين النظام الذي ينتمي إلى المؤسسة التي يتبع إليها الفاعل والنظام الذي لا ينتمي إليها باعتبار أنه في جميع حالات الاعتداء سيكون العامل قد خان الثقة الممنوحة له.

ومما سبق نرى أن الصفة غير المشروعة لفعل الدخول تتحقق في حالة الدخول الذي لا يستند إلى تصريح من قبل المسؤول، كما تتحقق في الحالة التي يتم فيها تجاوز حدود التصريح .

أ - حالة عدم وجود تصريح:

في هذه الحالة يكون دخول الفاعل غير مشروعاً لافتقاره إلى الإذن من المسؤول، وعادة ما يكون الفاعل ينتمي إلى فئة الأشخاص الذين لا تربطهم أي صلة بالنظام المعتدى عليه، وحالة عدم وجود تصريح لا تثير أي إشكالية، ذلك أنه من السهل تحديد ما إذا كان الفاعل قد حصل على تصريح بالدخول من قبل المسؤول أو لم يحصل على ذلك.

وهناك من يرى أن عدم التصريح بالدخول لا ينصرف إلى الحالات التي يكون فيها هذا التصريح مشروطاً بدفع ثمن محدد إذا لم يقيم الفاعل بتسديد الثمن المحدد، بحجة أن الحكمة من تجريم الدخول هو حماية المعلومات من وصول أشخاص ليس لهم الحق في ذلك وهو ما لا يتحقق في حالة الدخول دون أداء الثمن المحدد، لأن هذا الشرط هو مجرد شرط تنظيمي للدخول إلى النظام والذي يعد في هذه الحالة مصرحاً به بمجرد أداء الثمن المحدد، ولذلك فإن المعلومات التي يحتويها النظام تفتقر إلى السرية التي تعد المصلحة المحمية في جريمة الدخول^(٢).

إلا أن هناك رأياً آخر يذهب إلى خلاف ذلك، ويرى أن عدم التصريح بالدخول ينصرف إلى هذه الحالة أيضاً، ذلك أن السرية المراد حمايتها تتوافر في هذا

(١) المادة ٣٠ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

(٢) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٣٤.

النظام، إذ أنه لا يوجد نظام يتمتع بسرية مطلقة تجاه الجميع، وإنما يظل لفئة من الأشخاص يحددها المسؤول حق الاطلاع عليه، وفي هذه الحالة فإنَّ المسؤول يصرح بالدخول للأشخاص الذين يؤدون الثمن المحدد، أما الأشخاص الذين لا يؤدون هذا الثمن فإنَّ النظام يظل متمتعاً بالسرية تجاههم وبالتالي فإنَّ دخولهم يعد غير مصرح به^(١).

وعلى ذلك فإنه يبدو أنَّ الخلاف في تحديد ما إذا كان الدخول دون سداد الثمن يعد دخولاً غير مصرح به مرده إلى الطابع الموضوعي للإذن وإلى إمكانية تفويض الإذن، إلا أنه يمكن قياس الطابع الموضوعي للإذن على ذلك الذي يمنح لمنتسبي جهة معينة، كما أنَّ تفويض الإذن مرده إلى إرادة المسؤول والذي يملك بطبيعة الحال حظر ذلك.

ولهذه الأسباب ولأنَّ النصوص التي جرمت الدخول جاءت عامة ومطلقة يمكن القول بأنَّ الدخول دون أداء الثمن الذي يحدده المسؤول يعد دخولاً غير مصرح به، وبأنَّ المصلحة المراد حمايتها من ذلك هي السرية بما تتمثله من قيمة اقتصادية للمسؤول، وقد ذهب القضاء الأمريكي في بعض أحكامه إلى تأييد هذا الرأي، كما هو الحال في قضيتي (Allen) و (Riley) حيث قام كلا المتهمين بالدخول إلى مواقع شركة الاتصالات للقيام بإجراء اتصالات مجانية دون أداء الثمن المحدد، وذلك من خلال تخمين كلمات السر التي تحمي الموقع.

- ب - حالات تجاوز التصريح:

قد يستمد فعل الدخول عدم مشروعيته من تجاوز الفاعل لحدود الإذن الممنوح له، ويفترض في هذه الحالة أن يكون الفاعل من الأشخاص المطلعين على النظام والذين يملكون تصريحاً بالدخول إليه كالموظفين، وإذا كان من اليسير تقرير ما إذا سلوك الفاعل يفتقر إلى التصريح فإنَّ الأمر يبدو أكثر صعوبة في حالة تجاوز

(١) محمد خليفة، المرجع السابق، ص ١٤٨.

التصريح، وأياً كان الأمر فإنه يمكن القول بأنَّ الفاعل يتجاوز حدود التصريح الممنوح له إذا تجاوز في دخوله المجال الزمني أو المكاني للتصريح، أو إذا استخدم التصريح في تحقيق أغراض تختلف عن تلك التي منح التصريح من أجلها.

- ١ - تجاوز مجال التصريح:

في هذه الحالة يفترض أن يكون التصريح بالدخول مقيداً من حيث الزمان بتحديد وقت محدد يسمح فيه للفاعل بالدخول إلى النظام، أو المكان بأن يكون التصريح محدد من حيث المعلومات التي يمكن الوصول إليها، وفيما يتعلق بالتجاوز الزمني للتصريح فهناك من يرى أنَّ هذا التجاوز لا يعد غير مصرح به وذلك لانتفاء علة التجريم، ويستند أنصار هذا الرأي إلى أنَّه طالما كان دخول الفاعل قد تم بإرادة المسؤول فذلك يعني موافقته على الاطلاع على المعلومات، ولذلك فإنه لا يمكن الاحتجاج عليه بالسرية والتي تشكل المصلحة المراد حمايتها في جريمة الدخول^(١).

ونحن لا نتفق مع ذلك، ونرى أنَّ هذا الدخول يشكل دخولاً غير مصرحاً به، ذلك لأنَّ السرية المراد حمايتها هي السرية المفترضة والتي تتوقف على إرادة المسؤول، وطالما أنه لا يمكن الاحتجاج بالسرية تجاه الأشخاص المصرح لهم بالدخول، فإنه يمكن الاحتجاج بهذه السرية تجاه الأشخاص الذين لم يصرح لهم بذلك، ولذلك فإنَّ الدخول خارج المدة التي حددها المسؤول يعد دخولاً غير مصرحاً به وليس تجاوزاً للتصريح، ذلك لأنَّ العبرة في وجود التصريح من عدمه هي لحظة دخول الفاعل.

أما في الحالة الثانية والتي تتعلق بالتجاوز المكاني لحدود التصريح فإنَّ الفاعل يعد غير مصرحاً له، ذلك أن التصريح بالدخول إلى أحد أجزاء النظام لا يلغي انطباق الأصل على باقي أجزائه، وهو سرية المحتوى وعدم جواز الاطلاع عليه، هذا وإن كان من اليسير تقرير إذا ما كان الفاعل قد تجاوز التصريح في الحالة التي يلجأ فيها المسؤول إلى تحديد النطاق المكاني للتصريح صراحة، فإنَّ الأمر يكون أكثر صعوبة

(١) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٣٨.

في الحالة التي يلجأ المسؤول إلى ذلك ضمناً، وقد أثبتت هذه الحالة أمام القضاء الأمريكي في قضية (Morries)، وتتلخص وقائع هذه القضية في قيام موريس وهو طالب دراسات عليا في جامعة كورنيل بتصميم برنامج فيروسي عرف فيما بعد برنامج الدودة، لاستغلال نقاط الضعف في أمن الانترنت، وذلك لتوضيح أربع ثغرات في أمن الكمبيوتر وهي: خطأ في برنامج البريد الالكتروني، وخطأ في وظيفة الاستعلام عن المستخدمين المعروفة بوظيفة الإصبع الخفي، وعيب في تصميم أجهزة الكمبيوتر والتي تتيح باستخدام الامتيازات على أحد أجهزة الكمبيوتر الحصول على امتيازات على أخرى، وسهولة وبساطة تخمين كلمات المرور. وفي سبيل ذلك أطلق موريس فيروسه على إحدى حواسب معهد ماساتشوستس، إلا أنه ما لبث أن انتشر بسرعة خارج نطاق السيطرة وأصبح يكرر نفسه في كثير من الأحيان بحيث أغلق في نهاية المطاف أجزاء كبيرة من شبكة الانترنت في وقت مبكر، وبناءً على ذلك فقد اتهم الادعاء موريس بانتهاك المادة ٥١٨/١٠٣٠ التي تحظر الوصول إلى كمبيوتر، وقد أدانته محكمة الموضوع بموجب المادة المذكورة.

إلا أنه وأمام محكمة الاستئناف دفع المتهم بأن وصوله لم يكن دون إذن، لأنه كان له حقوق الوصول إلى العديد من الأجهزة المصابة، واستند في حجته إلى تقرير مجلس الشيوخ، والذي يميز فيه بين الدخول غير المصرح به والدخول الذي يتم بتجاوز التصريح من خلال التمييز بين الأشخاص من داخل النظام والغرباء، فالأشخاص من الداخل هم الذين يمتلكون حقوق الوصول إلى الحاسب كالموظفين، أما الغرباء فهم الذين لا يمتلكون حقوق الوصول، واقترح هذا التقرير لاحقاً على الكونغرس والذي حظر أفعال الدخول التي تتم دون تصريح وليس تلك التي تتم بتجاوز التصريح، أي أن إرادته اتجهت إلى منع أفعال الدخول التي تتم من قبل الأشخاص الغرباء وليس تلك التي تتم من قبل أشخاص من الداخل، ووفقاً لذلك فقد اعتمد على أن له عدة حسابات مشروعة على الانترنت ليتوصل إلى أنه من داخل الانترنت، ولذلك يجب أن لا يجرم بالدخول غير المصرح به.

إلا أنَّ محكمة الاستئناف رفضت هذا الدفع وأيدت الحكم الذي أصدرته محكمة الموضوع، معللةً ذلك في أن الكونغرس عندما ميّز بين أولئك الذين يملكون حقوق الوصول وبين الذين لا يملكونها، كان يأمل بأن أولئك الذين يملكون تصريحاً سيكونون عرضة للمسؤولية بموجب نصوص الاحتيايل، فالأشخاص الذين يحصلون على الفائدة من أجهزة الكمبيوتر الفيدرالية سيكونون عرضة للمسؤولية بموجب نصوص الاحتيايل عن كل اكتساب للوصول غير مصرح به إلى فوائد على أجهزة أخرى.

وبهذا فإنَّ المحكمة تكون قد وضعت معياراً جديداً لتحديد متى يكون الدخول غير مصرحاً به، يقوم على اختبار تأدية الوظيفة المقصودة، وبحسب هذا المعيار فإنَّ موريس كان دخوله غير مصرحاً به، لأنَّه استغل نقاط الضعف في البرامج ليحصل على وصول يختلف عن الوظيفة المقصودة من البرنامج، حيث أنَّه لم يستخدم البرامج بأي شكل من الأشكال يتفق مع وظيفتها المقصودة، فهو استغل برنامج الإيميل والإصبع الخفي لا ليرسل ولا ليقراً الرسائل ولا لبحث عن معلومات عن المستخدمين الآخرين، وإنَّما لإيجاد ثغرات في هذه البرامج سمحت له إيجاد طريق خاص ووصول غير مصرح به إلى كمبيوتر آخر^(١).

وفيما يبدو أنَّ المحكمة قد أرادت من خلال هذا المعيار أن يكون باعثاً على الشعور بين مستخدمي الأجهزة الحاسوبية بأنَّ هناك معايير تحكم مجتمع المعلومات، وهذه المعايير تقضي بأن مصممي البرامج يقومون بتصميمها لأداء مهام معينة، ومقدمي خدمات الشبكة يسمحون بوجود هذه البرامج على شبكاتهم، ويصرحون ضمناً للمستخدمين باستخدام هذه البرامج بما يتفق مع الوظيفة المقصودة منها، إلا أنَّهم وفي المقابل لا يصرحون لهم باستغلال نقاط الضعف في هذه البرامج لاستخدامها في مهام غير مقصودة، وعندما يستغل أحد المستخدمين نقاط الضعف في أحد هذه البرامج

⁽¹⁾ United States of America, Appellee, v. Robert Tappan Morris, 1991, Retrieved 12\Aug\2014 from: <http://law.justia.com/cases/federal/appellate-courts/F2/928/504/452673/>

لتوظيفه في الوصول إلى حاسب يفترض القول عندها بأن هذا الاستخدام لم يكن مقصوداً^(١).

- ٢ - تجاوز الغرض الذي منح لأجله التصريح:

أثار تحديد مفهوم التصريح تساؤلاً حول مشروعية الدخول المصرح به والذي يستخدم لتحقيق أغراض تختلف عن تلك التي أعطي التصريح من أجلها، وقد تعرض القضاء الانكليزي لهذه المسألة في حكمين انتهى في كل منهما إلى أن الدخول كان مصرحاً به، وتتلخص وقائع القضية الأولى في قيام شرطين باستخدام حاسب الشرطة للتحقق من تفاصيل السيارات لأغراض خاصة لا تتصل بأعمال وظيفتهم، وقدما للمحاكمة بتهمة الدخول غير المصرح به تطبيقاً للمادة الأولى من قانون إساءة استخدام الحاسبات لعام ١٩٩١، وقد أدانت محكمة درجة أولى المتهمين بالجريمة المنسوبة لهما، إلا أن محكمة الاستئناف ألغت الحكم على أساس أن المتهمين كانا من ضباط الشرطة اللذين يملكون إذن الوصول إلى المعلومات وأن هذا الوصول كان جزءاً من حياتهم العادية^(٢).

أما القضية الثانية فتتعلق بطلب تقدمت به حكومة الولايات المتحدة إلى المملكة المتحدة لتسليم إحدى العاملات بشركة أمريكيان اكسبريس، لقيامها بالدخول إلى حاسب الشركة للحصول على بيانات خاصة بالعملاء لأغراض لا تتعلق بعملها، وقد رفضت محكمة الاستئناف الانجليزية هذا الطلب على اعتبار أن الفعل لا يشكل جريمة وفق القانون الانكليزي، معللة ذلك بأن المتهمة وهي محللة ائتمان تملك التصريح

(1) Kerr. Orin, op.cit, p.1632

(2) DPP v. Bignall and Another, 1998, Retrieved 16\Aug\2014 from: <http://www.publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm>

للدخول إلى النظام المعلوماتي للشركة، وبالتالي فإنَّ سلوكها لا يعد جريمة وفق القانون الانكليزي^(١).

وينسجم موقف القضاء الانكليزي في هاتين القضيتين مع ما ذهبت إليه اللجنة القانونية في البرلمان، في أنَّ مستخدم النظام الذي يستعمله لأغراض غير مصرح بها لا يعد مرتكباً لجريمة الدخول وإنَّما يمكن أن ينطوي هذا السلوك على خيانة الأمانة، وترى هذه اللجنة أنَّه ليس هناك ما يستدعي تدخل القانون الجزائي لتجريم إساءة استخدام الحاسب الآلي من قبل العاملين، إذ أنَّه ليس هناك ما يميز هذا السلوك عن إساءة استخدام الأجهزة الأخرى في مكان العمل، والتي يبدو أنَّه من المناسب أكثر مواجهتها من خلال الإجراءات التأديبية وليس من خلال تدخل تشريعي^(٢)، وقد تعرض الموقف الانكليزي للانتقاد باعتباره يضيق من تطبيق قانون إساءة استخدام الحاسبات الآلية، ويتعارض مع المفهوم الصحيح للتصريح بالدخول، حيث أنَّ الحق بالدخول إلى نظام الحاسب يبقى مقيداً بالغرض الذي أعطي من أجله، فإذا تعارض معه أصبح الدخول غير مصرح به^(٣).

وقد اتخذ القضاء الأمريكي موقفاً مغايراً في الحالات التي تنطوي على تجاوز الغرض المحدد من قبل المسؤول، ومن أبرز تلك القضايا التي عرضت أمامه هي قضية (Shurgard)، وهي قضية نزاع مدني تدور وقائعها حول قيام الشركة المدعى عليها باستدراج عدد من موظفي الشركة المدعية بمن فيهم مدير التنمية اريك ليلاند، والذي كان يملك تصريحاً بالوصول إلى كامل بيانات الشركة، والذي قام فيما بعد ومن دون علم الشركة بالإرسال الإلكتروني للأسرار التجارية والمعلومات السرية للشركة الأولى، وقد رفضت المحكمة اقتراح المدعى عليه باعتبار أنَّ الوصول كان مصرحاً

(1) Regina v. Bow Street Magistrates Court and Allison A.P. Ex Parte Government of the United States of America on Appeal from a Divisional Court of the Queens Bench Division, 1999, Retrieved 16\Aug\2014 from: <http://www.bailii.org/uk/cases/UKHL/1999/31.html>

(2) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.38

(3) محمد خليفة، المرجع السابق، ص ١٥٣.

به، وانتهت إلى أن سلوكه كان يشكل انتهاكاً للمادة ٢١٨/١٠٣٠، لأن وصوله إلى المعلومات كان دون إذن، معللة ذلك بأن سلطة الموظف انتهت عندما تصرف كوكيل للمدعى عليه، وكانت المحكمة قد استندت في ذلك إلى نظرية الوكالة للقول بأن التصريح الممنوح للعاملين ينتهي متى نال وبدون علم المدير مصالح ضارة أو كان مذنباً بإخلال جسيم في ولاءه لمديره^(١).

وقد تبنت المحاكم الأمريكية تفسيراً أضيق لمعيار الوكالة في القضايا الجزائية التي تنطوي على سوء سلوك موظف، ومن ذلك قرار محكمة الاستئناف في قضية (Fugarino)، والتي تدور وقائعها حول قيام المتهم، وهو أحد مبرمجي شركة مختصة، بتصميم برامج للمساحين بحذف كميات كبيرة من الملفات التي كان يعمل عليها بعد أن علم أنه قد تم التعاقد مع أحد الأشخاص ليحل مكانه في دائرة الدعم الفني، وتبعاً لذلك فقد أدانته محكمة الموضوع بجريمة التعدي على الكمبيوتر، وقد دفع المتهم أمام محكمة الاستئناف بأن دخوله لم يكن مقصوداً بدون تصريح، إلا أن المحكمة رفضت ادعاءه وأيدت محكمة الموضوع في حكمها، معللة ذلك بأن صاحب العمل لم يخوله السلطة أو الإذن لحذف أجزاء من برامج الشركة بالإضافة إلى أن الطريقة الانتقامية في حذف الملفات أثبتت بأنه كان يعرف يفتقر إلى هذه السلطة^(٢).

وقد استندت محكمة الاستئناف في ولاية واشنطن إلى ذات المعيار لتبرئة المتهم في قضية (Olson)، والتي قام فيها المتهم، وهو ضابط شرطة في ولاية واشنطن، باستخدام قاعدة بيانات الشرطة للوصول وطباعة صور رخصة القيادة للطلاب الذين ارتادوا جامعة قريبة من واشنطن، وكانت قد أدانته محكمة الموضوع بجريمة الدخول غير المصرح به إلى جهاز تابع للحكومة، إلا أن محكمة الاستئناف

(1) Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., W.D. Wash. 2000, Retrieved 22\Aug\2014 from: <http://law.justia.com/cases/federal/district-courts/FSupp2/119/1121/2327594/>

(2) Fugarino v. State, 2000, Retrieved 22\Aug\2014 from: <http://law.justia.com/cases/georgia/court-of-appeals/2000/a99a1781.html>

ألغت هذا الحكم معللةً ذلك بأن قواعد العمل كانت تحظر الاستخدام الشخصي للبيانات وليس الوصول ذاته^(١).

وهناك حالة واحدة في القضاء الأمريكي لم تُبنَ فيها القضية على أساس الدافع إلى الدخول، وإنما بُنيت على أساس السلوك وهي قضية (Briggs)، وهي لا تمثل قاعدة في القضاء الأمريكي^(٢)، وتدور وقائع هذه القضية حول قيام المتهم قبل وقت قصير من استقالته بتأمين بعض البرامج الموجودة على شبكة الشركة من خلال وضع كلمة مرور تاركاً صاحب العمل عاجزاً عن الدخول إلى هذه الملفات، وعندما طالبه الأخير في وقت لاحق بإعطائه كلمة المرور ادعى أنه نسيها، وذهبت محكمة الموضوع إلى إدانة المتهم بالوصول غير المصرح به باعتباره لم يكن مصرحاً له بالوصول يمثل هذه الطريقة لوقف تشغيل خدمات النظام، إلا أن محكمة الاستئناف ألغت هذا الحكم، معللةً ذلك بأنه على الرغم من أن المتهم تجاوز حدود التصريح الممنوح له، إلا أن قانون ولاية ميريلاند لا يعاقب إلا على تلك الحالات التي يتم فيها الدخول بدون تصريح، وإن كان من المفترض أن يشمل التجريم هذا السلوك فإن ذلك من واجب الهيئة التشريعية وليس المحكمة^(٣).

وعلى كل حال فإن الحالات التي يتجاوز فيها الفاعل التصريح الممنوح له تكون في إحدى ثلاثة سياقات: فإما أن يحظر المسؤول الدخول إلى النظام لتحقيق أغراض غير مصرح بها، وإما أن يحظر استخدام النظام لتحقيق أغراض غير مصرح بها دون أن يقيد الدخول إلى النظام على الامتثال لهذا الحظر، وإما أن يحدد الأغراض المصرح استخدام النظام لتحقيقها دون أن يحظر أيّاً من الاستخدام أو الدخول إلى النظام، والحالة الأولى هي الأقل إثارة للجدل ذلك لأنّ المسؤول عندما يضع قيوداً على

(1) State v. Olson 1987, Retrieved 22\Aug\2014 from: <http://courts.mrsc.org/mc/courts/zappellate/047wnapp/047wnapp0514.htm>

(2) Kerr. Orin, op.cit, p. 1637

(3) Briggs v. State 1998, Retrieved 22\Aug\2014 from: <http://law.justia.com/cases/maryland/court-of-appeals/1998/24a97-2.html>

وصول الفاعل إلى النظام، فإنَّه يفترض امتثاله لهذه القيود وإلا فإنَّ دخوله يعد غير مصرح به، أما في الحالة الثانية فإنَّه من الصعب إثبات أنَّ دخول الفاعل كان غير مصرح به لأنَّ المسؤول لم يضع قيوداً على وصول الفاعل إلى النظام، إلا أنَّ المحاكم تميل إلى اعتبار أنَّ وصول الفاعل كان غير مصرح به، والحالة الثالثة هي الأكثر جدلية ذلك لأنَّ المسؤول لم يضع قيوداً واضحة على استخدام النظام أو الدخول إليه، إلا أنَّ المحاكم الأمريكية قد فسرت أنَّ وصول الفاعل لتحقيق أغراض لم تحظر صراحة لا يمكن عده غير مصرح به، وقد خلصت في أغلب الحالات أنَّ الغرض غير مصرح به دون أن تعد الوصول في حد ذاته غير مصرح به^(١).

ومما تقدم يمكن القول بأنَّه في الحالات التي تتطوي على إساءة موظف فإنَّ المحاكم الأمريكية تميل إلى اعتبار سلوك الموظف في الحالات التي لا يكون له مصلحة صاحب العمل غير مصرح به، وبهذا تكون المحاكم قد جعلت من الضرر بديلاً عن التصريح، وهذا ما يؤيده العقل والمنطق السليم، ذلك لأنَّه في الحالات التي يسبب فيها الاستخدام ضرراً لصاحب العمل يعد استخداماً لا يريده وضماً لا يصرح بالوصول إليه^(٢).

وجريمة الدخول في القانون السوري تتحقق بتجاوز الغرض الذي منح التصريح من أجله، وذلك لأنَّ المادة ١٥ من قانون تنظيم التواصل على الشبكة نصت على أنَّ عدم مشروعية الدخول تتحقق في الحالة التي يتم فيها الدخول من غير صلاحية، وهذه الصلاحية تنتفي في الحالات التي يتم فيها الدخول لتحقيق أغراض لا تنتمي إلى التصريح الذي منحه المسؤول.

(1) Jarrett H. Marshall & Michael W. Bailie, op.cit, p.10

(2) Kerr. Orin, op.cit, p.1642

المطلب الثاني: الوصول إلى المعلومات

يمثل الوصول إلى المعلومات النتيجة الجرمية في جريمة الدخول، أو بعبارة أخرى هو ذلك التغيير الذي يحدث في العالم الخارجي كأثر لفعل الدخول، فجريمة الدخول _كغيرها من الجرائم_ تحدث أثراً في العالم الخارجي يتمثل بالوصول إلى المعلومات، وتتطلب دراسة النتيجة الإجرامية إيضاح موقف التشريعات من تحديد هذه النتيجة، وطبيعة جريمة الدخول تبعاً لذلك، وأثر تخلف الوصول على وصف الجريمة، والعلاقة التي تربط بين فعل الدخول والوصول إلى المعلومات.

أولاً: الاتجاهات التشريعية في تحديد النتيجة الإجرامية

تباينت التشريعات في تحديد النتيجة الجرمية التي يتطلبها النموذج القانوني لجريمة الدخول، ففي بعض التشريعات لا تتطلب النصوص القانونية سوى وصول الفاعل إلى أي من المعلومات التي تتكون منها النظام المعلوماتي كما هو الحال في القانون السوري^(١) والفرنسي^(٢) والسويسري^(٣) والهولندي^(٤) والفنلندي^(٥)، وهذا هو الحال أيضاً في بعض نصوص القانون الأمريكي حيث تسمح هذه النصوص بتطبيق العقوبة على الفاعل بمجرد وصوله إلى نظام الحاسب الآلي إذا كان هذا النظام يعمل لأجل أو بالنيابة عن حكومة الولايات المتحدة الأمريكية^(٦)، وبعد قانون إساءة استخدام الحاسبات الآلية الانكليزي من قبيل هذه التشريعات، فعلى الرغم من أن المادة الأولى من هذا القانون تتطلب وصول الفاعل إلى المعلومات أو البرامج التي يحتوي عليها الحاسب الآلي، إلا أنه ينظر إلى هذه المعلومات والبرامج بمفهومها الواسع أي أنها تشمل جميع المكونات المنطقية للحاسب الآلي^(٧).

(١) المادة ١٦ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

(٢) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

(٣) المادة ١٤٣ من قانون العقوبات السويسري.

(٤) المادة ١٣٨ من قانون العقوبات الهولندي.

(٥) القسم ٤ من الفصل ٣٨ من قانون العقوبات الفنلندي.

(٦) المادة ١٠٣٠\٣ من قانون إساءة استخدام الحاسبات الأمريكي.

(٧) Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.30

وإذا كان الأمر كذلك في بعض التشريعات فإنّه في تشريعات أخرى تتطلب وصول الفاعل إلى معلومات محددة في النظام كما هو الحال في بعض نصوص القانون الأمريكي^(١)، ويعد المشرع البلجيكي هذا الوصول من قبيل الظروف المشددة للعقوبة، فهو يعاقب على مجرد الوصول إلى نظام الحاسب الآلي، ويشدد العقوبة في الحالة التي يصل فيها الفاعل إلى أي من المعلومات التي يتم تخزينها أو التي يتم نقلها أو معالجتها بواسطة هذا الحاسب^(٢)، كما يشدد القانون البرتغالي عقوبة الدخول إذا تمّ الحصول على معلومات تتعلق بالأسرار التجارية أو على معلومات سرية يحميها القانون^(٣).

والى جانب هذه التشريعات فإنّ هناك تشريعات أخرى تشدد العقوبة في الحالة التي يترتب فيها على فعل الدخول نتائج أخرى تتجاوز الوصول إلى المعلومات، فالقانون البلجيكي يشدد العقوبة في الحالة التي يترتب فيها على فعل الدخول إلحاق أضرار بنظام الحاسب الآلي أو بالمعلومات التي يتم تخزينها أو معالجتها أو تبادلها بواسطة هذا النظام أو إذا تم الحصول على أي فائدة^(٤)، كما يشدد القانون البرتغالي العقوبة إذا تمّ الحصول على أي مكاسب من الدخول^(٥)، ويشدد القانون الايطالي العقوبة في حالة إتلاف البيانات أو المعلومات أو البرامج التي يخترنها نظام الحاسب الآلي^(٦)، ويشدد القانون الفرنسي العقوبة في الحالة التي يترتب على فعل الدخول محو أو تعديل البيانات أو تعطيل النظام عن القيام بعمله^(٧)، ويشدد المشرع القانون السوري العقوبة في حالة قيام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها أو قام بإلغائها أو تغييرها أو تشويهها أو تزيفها أو استخدامها أو إفشائها^(٨)، هذا وإنّ

(١) المادة ١٠٣٠ \ ١ \ و ٢ \ ١٠٣٠ من قانون اساءة استخدام الحاسبات الأمريكي.

(٢) المادة ٣ \ ٥٥٠ ب من قانون العقوبات البلجيكي.

(٣) الفقرة ٣ من المادة ٧ من الفصل الأول من القانون البرتغالي الخاص بحماية المعلومات.

(٤) المادة ٣ \ ٥٥٠ ب من قانون العقوبات البلجيكي.

(٥) الفقرة ٣ من المادة ٧ من القانون البرتغالي.

(٦) المادة ٦١٥ من قانون العقوبات الايطالي.

(٧) المادة ١٣٢٣ من قانون العقوبات الفرنسي.

(٨) المادة ١٦ ب من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

نهج المشرع السوري في تشديد العقوبة منتقد وذلك لاقتصاره على تجريم هذه الأفعال في إطار جريمة الدخول، ولتطلبه اتجاه إرادة الفاعل إلى هذه الأفعال، وكان من الأفضل لو اقتصر المشرع في تشديد العقوبة على الحالات التي يترتب فيها على الدخول إتلاف المعلومات فيما جرم الأفعال الأخرى في إطار منفصل عن جريمة الدخول.

ثانياً: طبيعة جريمة الدخول

للنتيجة مدلولان: أحدهما مادي والآخر قانوني، وتعرف النتيجة وفق مدلولها المادي بأنها التغيير الذي يحدث في العالم الخارجي كأثر للنشاط الإجرامي، والنتيجة الإجرامية بهذا المفهوم لا تعد من بين العناصر الأساسية في الجريمة، وإنما هي لازمة في بعض الجرائم دون بعضها الآخر، والمشرع هو الذي يحدد عناصر الجريمة، ويمكن أن يشترط في النموذج القانوني لإحدى الجرائم تحقق نتيجة معينة^(١).

وعلى ذلك فإن الجرائم وفق المفهوم المادي للنتيجة تصنف إلى جرائم مادية لا تتم إلا بتوافر نتيجة معينة، وجرائم شكلية لا يشترط فيها المشرع حصول نتيجة^(٢)، وجريمة الدخول وفقاً للتحديد السابق هل تعد جريمة مادية أو جريمة شكلية ؟

إنَّ جريمة الدخول لا تثير أي إشكالية في الحالة التي يتطلب نموذجها القانوني وصول الفاعل إلى معلومات محددة في النظام المعلوماتي، فهي تعد جريمة مادية تتطلب تحقق نتيجة محددة ألا وهي وصول الفاعل إلى المعلومات المحددة في النموذج القانوني.

إلا أنَّ الإشكالية تثار في الحالة التي لا يتطلب فيها النموذج القانوني للجريمة وصول الفاعل إلى أي من المعلومات التي يخترنها النظام، فيذهب رأي إلى أنَّ هذه

(١) د. محمود نجيب حسني، شرح قانون العقوبات اللبناني القسم العام، دار النهضة العربية، بيروت، ١٩٨٤، ص ٢٧٨.

(٢) د. معن أحمد محمد الحيارى، الركن المادي للجريمة، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠، ص ٢٠٥.

الجريمة تعد جريمة شكلية لا يتطلب نموذجها القانوني تحقق نتيجة متميزة عن نشاط الفاعل، وينظر أصحاب هذا الرأي إلى وصول الفاعل إلى النظام باعتباره أحد عناصر النشاط الإجرامي وليس أحد آثاره^(١).

إلا أنه ومن جهة أخرى فإن هذا القول بحاجة إلى التوضيح، فالجريمة الشكلية تعرف بأنها كل جريمة لا تستلزم في كيانها المادي تحقق أثر معين لنشاط الفاعل^(٢)، وإذا طبقنا هذا التعريف على جريمة الدخول لوجدنا عدم تطابقه مع نموذجها القانوني، فجريمة الدخول تتطلب وصول الفاعل إلى المعلومات، وجميع التشريعات تتطلب هذا الوصول وإن اختلفت في تحديد نطاقه، ففي حين تشترط بعض التشريعات وصول الفاعل إلى معلومات محددة، فإنّ تشريعات أخرى تكتفي بالوصول إلى أي من المعلومات التي يتكون منها النظام، وتطلب هذا الوصول هو أمر يحتمه الطابع المنطقي للدخول، كما أنّ وصول الفاعل إلى هذه المعلومات يعد أحد آثار السلوك الإجرامي وليس أحد عناصره، فمقياس التمييز بين النشاط الإجرامي وآثاره هو انقضاء السيطرة الإرادية على الحركة العضوية وآثارها^(٣)، وهذه السيطرة تنتهي بمجرد إجراء الاتصال مع النظام، أما وصول الفاعل إلى المعلومات فإنه يعد أحد آثار نجاح هذا الاتصال، ولتوضيح ذلك نفترض أن شخصاً يحاول الدخول إلى النظام من خلال تسجيل مفتاح المرور في النظام، فمجرد إدخال هذا المفتاح يشكل نشاط الدخول إلا أنه لا يكفي لإشادة الركن المادي، فجريمة الدخول تتطلب بالإضافة إلى ذلك وصول الفاعل إلى المعلومات والذي يشكل أثراً لصحة الإدخال، أما في الحالة التي يتعذر فيها هذا الوصول فإنّ الفاعل سيعد شارعاً في جريمة الدخول.

وإنّ الاختلاف بين هذين الرأيين مرده إلى الاختلاف في تحديد الأثر المادي الذي يترتب على نشاط الفاعل، ففي حين يرى أنصار الرأي الأول أنّ الأثر الذي

(١) د. هدى حامد قشقوش، المرجع السابق، ص ٤١.

(٢) د. رمسيس بهنام، النظرية العامة للقانون الجنائي، منشأة المعارف، طبعة الثالثة منقحة، ١٩٩٧، ص ٥٢٦.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ٤٢٥.

يترتب على نشاط الدخول هو وصول الفاعل إلى معلومات محددة يختزنها النظام، ويترتب على ذلك القول بأن جريمة الدخول جريمة شكلية في الحالات التي لا تتطلب هذا الوصول، إلا أنه وفي رأينا فإن الأثر الذي يترتب على نشاط الدخول هو وصول الفاعل إلى أي من المعلومات التي يتكون منها النظام، وتبعاً لذلك فإن جريمة الدخول جريمة مادية.

وللنتيجة أيضاً مدلولها القانوني الذي يعرف بأنه العدوان الذي ينال مصلحة أو حق قدر المشرع حمايته^(١)، ويتم هذا العدوان من خلال الإضرار بالمصلحة محل الحماية عن طريق تعطيلها أو إنقاصها أو من خلال تعريض هذه المصلحة للخطر، ولذلك يمكن القول بأن الجريمة وفق المفهوم القانوني للنتيجة إما أن تكون جريمة ضرر أو جريمة خطر^(٢)، وهذا ما يثير التساؤل حول أي من هذه الجرائم تنتمي جريمة الدخول ؟

كما أسلفنا سابقاً فإن المصلحة المراد حمايتها في جريمة الدخول هي سرية المعلومات، وجريمة الدخول هي من الجرائم التي تمثل عدواناً محتملاً على هذا الحق وليس من الجرائم التي تتمثل في تحقق العدوان على الحق الذي يحميه القانون، فجريمة الدخول تتحقق بمجرد وصول الفاعل إلى المعلومات دون أن تتطلب في سبيل تحققها أن يحدث واقعياً انتهاكاً لسرية المعلومات، وذلك مرده إلى الطابع الموضوعي للسرية المراد حمايتها، والتي تتحقق بمجرد وجود المعلومات في إطار محدد لا يسمح للغير بالاطلاع عليها دون موافقة المسؤول، ولذلك فإن جريمة الدخول تشكل جريمة خطر وليست بجريمة ضرر.

هذا وإن هناك صلة بين مدلولي النتيجة الجرمية، فالمدلول القانوني للنتيجة هو في الحقيقة تكييف قانوني لمدلولها المادي، فالقول بأن جريمة الدخول جريمة خطر هو تكييف قانوني للآثار المادية التي أنتجها نشاط الدخول، ويحدد المدلول القانوني للنتيجة

(١) المرجع ذاته، ص ٢٧٩.

(٢) د. معن أحمد محمد الحيارى، المرجع السابق، ص ٢٠٥.

نطاق مدلولها المادي، فالآثار التي تترتب على نشاط الدخول متعددة، وهي تتابع متلاحقة طبقاً لقوانين السببية وتصل إلى حد إتلاف المعلومات أو نسخها أو استعمالها أو حرمان الغير من الاستفادة منها، إلا أنَّ القانون لا تعنيه كل هذه النتائج وإنَّما ما يعنيه تلك النتائج التي تتمثل بالاعتداء على السرية موضوع الحق المحمي^(١) والتي تبرز بالوصول إلى المعلومات، إلا أنَّه ومن جهة أخرى يجب الأخذ بالحسبان الخطورة المتزايدة في بعض الحالات التي يتعدى فيها الأثر مجرد المساس بالسرية، وذلك من خلال تشديد العقوبة في الحالات التي يترتب فيها على فعل الدخول إحداث أضرار بالمعلومات.

ثالثاً: تخلف الوصول إلى المعلومات

قد يرتكب الفاعل النشاط الإجرامي دون أن يترتب على ذلك حصول النتيجة المحددة في النموذج القانوني، وذلك كأن يقوم بتسجيل بيانات الدخول أو بتشغيل الحاسب الآلي دون أن يترتب على ذلك وصول الفاعل إلى أي من المعلومات التي يتكون منها النظام المعلوماتي، وفي هذه الحالة يمكن أن ينظر إلى الفاعل باعتباره شارعاً في جريمة الدخول إذا لم يحل دون تحقيق النتيجة سوى ظروف خارجة عن إرادته^(٢)، كأن يكون المسؤول قد غيّر مفتاح المرور قبل وقت من محاولة الفاعل أو أن يكون قد أصاب الخلل أحد الأجهزة الالكترونية المحمول عليها النظام.

وإنَّ تجريم هذا السلوك يعد خروجاً عن القواعد العامة، لأنَّ المشرع عندما يتطلب عدة عناصر لقيام جريمة معينة فإنه يرتب على تخلف أحد هذه العناصر انتفاء الجريمة، ولمَّا كان الشروع يفترض تخلف النتيجة كان مقتضياً ذلك عدم توقيع العقاب على الفاعل، إلا أنَّه من ناحية أخرى فإنَّ هذا السلوك يهدد بخطر وشيك حدوث،

(١) د. محمود نجيب حسني، المرجع السابق، ٢٧٩.

(٢) د. عبود السراج، شرح قانون العقوبات القسم العام، منشورات جامعة دمشق، ٢٧/٤١٥١/٢٠٠٦م، ص ٣١٦.

والحماية الكاملة للحق تقتضي وقايته من كل صور الاعتداء وإن كان مجرد خطر يتهدهده^(١).

وتطبيقاً لذلك فإن الشروع في جريمة الدخول يشكل تهديداً لسرية المعلومات بوصول غير مصرح به، ولذلك فقد اتجهت بعض التشريعات إلى تجريم الشروع في جريمة الدخول كما هو الحال في القانون السوري^(٢) والفرنسي^(٣) والأمريكي^(٤) والبلجيكي^(٥) والفنلندي، حيث يعاقب على الشروع بذات العقوبات المقررة للجريمة الأصلية، ولم تكثف بعض التشريعات بهذا التجريم، وإنما تعدت ذلك إلى تجريم الأعمال التحضيرية التي تسبق وقوع الجريمة كما هو الحال في القانون السويدي^(٦)، وتبعاً لهذا التجريم فإن مجرد حيازة شيفرات الدخول لاستخدامها في الدخول سيعدّ سلوكاً غير مشروع، وتتجلى أهمية تجريم الشروع في جريمة الدخول في حماية النظام ذاته، ولا سيما في التشريعات التي تتطلب في جريمة الدخول وصول الفاعل إلى معلومات محددة كما هو الحال في بعض نصوص القانون الأمريكي.

والى جانب هذه التشريعات فقد اتجهت تشريعات أخرى إلى تجريم بعض الأفعال التي تساعد على ارتكاب جريمة الدخول، كما هو الحال في القانون الكندي الذي يجرم استخدام أو حيازة أو الاتجار أو السماح بالحصول على كلمات المرور الخاصة بأحد الأنظمة والتي من شأنها أن تمكن أحد الأشخاص من ارتكاب جريمة الدخول^(٧)، كما جرم القانون الأمريكي أفعال الاتجار بكلمات المرور أو معلومات مماثلة تُمكن من الدخول إلى الأنظمة التي تستخدم من قبل حكومة الولايات المتحدة الأمريكية أو بالنيابة عنها أو إذا كان من شأن هذا السلوك أن يسبب أضراراً

(١) د. محمود نجيب حسني، المرجع السابق، ص ٣٣٧.

(٢) المادة ٣١ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري.

(٣) المادة ٧٣٢٣ من قانون العقوبات الفرنسي.

(٤) المادة ١٠٣٠ ب من قانون إساءة استخدام الحاسبات الأمريكي.

(٥) المادة ٤٥٥ ب من قانون العقوبات البلجيكي.

(٦) القسم ٩ من الفصل ٤ من قانون العقوبات السويدي.

(٧) المادة ١١٣٤٢ د من قانون العقوبات الكندي.

بالتجارة^(١)، كما جرم القانون الايطالي أفعال الحيازة غير المشروعة أو نشر أكواد المرور التي تستخدم للوصول إلى الأنظمة المعلوماتية أو شبكات الاتصالات السلكية أو اللاسلكية^(٢)، وبتجلى أهمية هذا التجريم في أنه يعد أحد الوسائل الوقائية لحماية المعلومات من الوصول إليها.

ويرد على تجريم الشروع أنه من شأنه أن يؤدي إلى التوسع في التجريم دون أن يحقق حماية إضافية للمعلومات، وذلك لأنه من المتعذر الكشف عن محاولات الدخول ما لم يترتب عليها اختراق للإجراءات الفنية أو الوصول إلى المعلومات، ونحن نرى أن هذه الحجج يجب أن لا تشكل عائقاً يحول دون تجريم الشروع، وذلك لأنه وإن كان من شأنه أن يؤدي إلى التوسع في التجريم، إلا أن ذلك يظل مقيداً باتجاه قصد الفاعل إلى الوصول إلى المعلومات والبدء بفعل تنفيذي في الجريمة، كما أن الحماية الكاملة للمعلومات تستوجب التصدي للإجرام فيما يزال في مرحلة متقدمة من الوصول إلى هدفه، كما أن الكشف عن محاولات الدخول قد يتم من خلال تعدد إجراءات حماية المعلومات أو من خلال الضبط المادي لهذه المحاولات.

رابعاً: العلاقة السببية بين فعل الدخول والوصول إلى المعلومات

لا بد لتحقيق الكيان المادي في الجريمة من وجود صلة سببية تربط بين الفعل والنتيجة، أي أن يكون الفعل سبباً في وقوع النتيجة، أما إذا وقعت النتيجة مستقلة عن الفعل وأمكن فصلها عنه فإن الكيان المادي للجريمة لا يتحقق، وبالتالي لا يعود بالإمكان إسناد هذه النتيجة لمرتكب الفعل^(٣)، وتبرز أهمية العلاقة السببية في أنها تقيم

(١) المادة ٦١٠/٣ من القانون الأمريكي الفيدرالي لإساءة استخدام الحاسبات الآلية.

(٢) المادة ٤٦١٥ من قانون العقوبات الايطالي.

(٣) د. عبود السراج، المرجع السابق، ص ٢٨٨.

وحدة الكيان المادي من خلال الربط بين عنصريه الفعل والنتيجة^(١)، وهي شرط أساسي لقيام المسؤولية الجزائية باعتبارها هي التي تسند النتيجة إلى الفعل^(٢).

وتبعاً لما تقدم فإنه يتعين لقيام الكيان المادي في جريمة الدخول أن يكون نشاط الفاعل هو سبب وصوله إلى المعلومات، كأن يقوم الفاعل بتشغيل جهاز الحاسب الذي يحوي النظام أو أن يقوم بتسجيل بيانات الدخول في النظام، أما إن أمكن القول بأن هذا الوصول لم يكن ناشئاً عن نشاط الفاعل فإن الكيان المادي لجريمة الدخول ينتفي وإن كان يصلح من جهة أخرى لتكوين الكيان المادي لجريمة الشروع، أما إن انتفى النشاط الإجرامي من جانب الفاعل كأن يكون الوصول مرده إلى خلل في شبكة الاتصالات، فإنه يترتب على ذلك انتفاء كلاً من الكيان المادي للجريمة التامة وللشروع فيها، وتبعاً لذلك فإنه تنتفي كل مسؤولية كان يمكن أن تترتب على الفاعل.

(١) د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، دون دار نشر، دون مكان نشر، دون سنة نشر، ص ٥٧.

(٢) المرجع ذاته، ص ٥٦.

المبحث الثاني: الركن المعنوي

الركن المعنوي هو الجانب المعنوي من الجريمة والذي يدخل في تكوينها^(١)، فالجريمة ليست ظاهرة مادية خالصة قوامها ماديات الجريمة وإنما هي كذلك كيان نفسي^(٢)، والركن المعنوي هو علاقة تجمع بين ماديات الجريمة وشخصية الفاعل، وهذه العلاقة هي محل لوم القانون وجوهرها الإرادة الجرمية^(٣)، وتستمد الإرادة هذه الصفة من خلال اتجاهها إلى الماديات التي تقوم عليها الجريمة، ولاتجاه الإرادة على هذا النحو صورتان: الأولى وهي صورة القصد الجرمي وفيه تسيطر الإرادة على ماديات الجريمة سيطرة فعلية، والثانية وهي الخطأ وفيه تسيطر الإرادة على بعض ماديات الجريمة في حين تنحصر علاقتها بالبعض الآخر بإمكان السيطرة^(٤).

والركن المعنوي في جميع التشريعات التي تناولت جريمة الدخول يتخذ صورة القصد الجرمي، إلا أنَّ التساؤل يبقى قائماً عن إمكانية اتخاذ الركن المعنوي في هذه الجريمة صورة الخطأ، وعن ضرورة مواجهة هذه الأفعال إذا كان ذلك ممكناً، وعليه سوف نتناول في هذا المبحث القصد الجرمي كما نصت عليه النصوص القانونية، ثم نتعرض لصورة الخطأ في جريمة الدخول.

المطلب الأول: الدخول قصداً

يعرف القصد بأنه إرادة ارتكاب الجريمة على نحو ما عرفها القانون^(٥)، وجميع التشريعات التي تناولت جريمة الدخول تتطلب القصد العام والذي يقوم على عنصرين هما العلم بعناصر الجريمة والإرادة المتجهة إلى تحقيق هذه العناصر^(٦)، كما أنَّ هناك

(١) د. عبود السراج، المرجع السابق، ص ٢٢٢.

(٢) د. محمود نجيب حسني، قانون العقوبات اللبناني القسم العام، دار النهضة العربية، بيروت، ١٩٨٤، ص ٣٧٨.

(٣) د. محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٩.

(٤) د. محمود نجيب حسني، المرجع السابق، ص ٣٨٢.

(٥) المادة ١٨٧ من قانون العقوبات السوري.

(٦) د. عبود السراج، المرجع السابق، ص ٣٣٧.

بعض التشريعات تتطلب بالإضافة إلى ذلك أن تتجه إرادة الفاعل إلى تحقيق عناصر لا تعد من عناصر الركن المادي في الجريمة، وعليه سوف نتناول في هذا المطلب القصد العام المتطلب في جريمة الدخول، ثم نتعرض للقصد الخاص الذي تتطلبه بعض التشريعات في هذه الجريمة.

أولاً: القصد العام

تطلبت النصوص القانونية في التشريعات المختلفة القصد العام في جريمة الدخول، وقد تعددت العبارات التي استخدمتها للدلالة على هذا القصد، فقد عبر المشرع السوري والهندي عن القصد العام بتطلبه أن يكون الدخول مقصوداً وبطريقة غير مشروعة^(١)، وتطلب القانون الفرنسي بأن يتم الدخول عن طريق الغش والتدليس^(٢)، والقانون الأمريكي بأن يتم الدخول قصداً ودون تصريح أو بتجاوز التصريح، والقانون الانكليزي بأن يتجه قصد الفاعل إلى الدخول إلى البرامج والمعلومات^(٣)، والقانون الاسترالي بأن يتم الدخول قصداً وعلى نحو غير مشروع^(٤)، والقانون الكندي بأن يتم الدخول عن طريق الاحتيال ودون وجه حق^(٥).

ويتطلب القصد الجرمي أن يحيط علم الفاعل بعناصر الجريمة، وأن تتجه إرادته إلى تحقيق هذه العناصر.

- ١ - العلم:

يتطلب القصد الجرمي العام أن يحيط علم الفاعل بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما يتطلبه القانون لبناء أركان الجريمة ولاستكمال كل

(١) المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري، المادة ١٣٨ من قانون العقوبات الهولندي.

(٢) المادة ٣٢٣ من قانون العقوبات الفرنسي.

(٣) المادة ١٠٣٠ من القانون الأمريكي الفيدرالي لإساءة استخدام الحاسبات الآلية.

(٤) المادة ١١٤٧١ من قانون الجريمة الالكترونية الاسترالي.

(٥) المادة ٣٤٢ من قانون العقوبات الكندي.

ركن من عناصره يتعين أن يشمل علم الفاعل^(١)، ولكن علم الفاعل لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، وإنما يتعين أن يحيط علم الفاعل بالتكييف الذي تمتاز به بعض هذه الوقائع وتكتسب به أهمية في نظر القانون، ذلك أن عدداً من الوقائع التي تدخل في تكوين الجريمة لا تمثل أهمية في نظر القانون إلا إذا اكتسبت وصفاً معيناً، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية^(٢).

ومن جهة أخرى فإن هناك وقائع وتكيفات لا يشترط العلم بها لتوافر القصد الجرمي، ويعني ذلك أنه إذا ثبت جهل الفاعل بها فإن ذلك لا يحول دون اعتبار القصد متوافراً لديه^(٣).

أ - الوقائع التي يُتطلب العلم بها:

بتطبيق المبادئ العامة على جريمة الدخول غير المصرح به فإنه يتعين أن يحيط علم الفاعل بكل الوقائع التي تدخل في تكوين الركن المادي في الجريمة، فيتطلب القصد أن يحيط علم الفاعل موضوع الحق المعتدى عليه، وخطورة الفعل، والنتيجة الجرمية، وعلاقة السببية.

١ - العلم بموضوع الحق:

أولى العناصر التي يتعين أن يحيط علم الفاعل بها هي موضوع الحق المعتدى عليه^(٤)، ففي جريمة الدخول يتعين أن يعلم الفاعل بأنه يوجه اعتداءه إلى نظام المعلومات باعتباره المحل الذي ينصب عليه الحق الذي أراد المشرع حمايته، أما إذا اعتقد الفاعل بأن نشاطه لا ينصب على هذا المحل فإن القصد الجرمي ينتفي تبعاً لذلك، كأن يعتقد بأنه يقوم ببعض العمليات الحسابية، وإن كان هذا الفرض يؤدي إلى انعدام القصد الجرمي لديه فإنه يفتقر إلى الأهمية في الواقع العملي، وذلك لأن جريمة

(١) د. محمود نجيب حسني، المرجع السابق، ص ٥٩.

(٢) المرجع ذاته، ص ٦٠.

(٣) د. محمود نجيب حسني، شرح قانون العقوبات اللبناني - القسم العام، ص ٣٩٩.

(٤) د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، ص ٦٣.

الدخول هي من الجرائم التي تتطلب أن يكون لدى الفاعل قدراً من الخبرة في المجال المعلوماتي تحول دون إمكانية التسليم بهذا الافتراض^(١)، إلا أنه وفي جميع الأحوال التي يثبت فيها انتفاء علم الفاعل بموضوع الحق المعتدى عليه فإن القصد الجرمي ينتفي تبعاً لذلك.

- ٢ - العلم بخطورة الفعل:

يتعين أن يحيط علم الفاعل بالخطورة التي ينطوي عليها فعله على الحق الذي يحميه القانون^(٢)، وبناءً على ذلك فإنه يتعين أن يعلم الفاعل بأن فعله يشكل تعدياً على المعلومات محل الحق المحمي، أما إذا اعتقد الفاعل بأن سلوكه لا يشكل خطراً على هذه المعلومات فإن ذلك من شأنه أن ينفي القصد الجرمي لديه، كأن يعتقد الفاعل بأن سلوكه لا يشكل سوى تصفحاً لبعض المواقع على شبكة الانترنت، ويثار التساؤل هنا حول تأثير الدخول الذي يتم أثناء محاولة منع خطر يتهدد النظام على القصد الجرم، فهل يعد ذلك انتفاء للعلم بالخطورة التي ينطوي عليها سلوك الفاعل أم أنه يعد مجرد باعث على ارتكاب الجريمة لا ينفي القصد الجرمي؟ إن الإجابة على هذا التساؤل لا تثير أي صعوبة في الحالة التي يكون فيها للفاعل سلطة على نظام المعلومات أو أن القواعد التي تحكم عمل هذا النظام تجيز له هذا الدخول في حالة تعرضه للخطر، أما إذا كانت هذه القواعد لا تجيز له الدخول في أي حال من الأحوال فإن كون هذا الباعث يعد نافياً للقصد أو ليس كذلك هو نوع العلم الذي يتوافر لدى الفاعل، فإذا أتى الفاعل فعله وهو يعتقد بأنه يقوم بمجرد منع الخطر الذي يتهدد النظام إلا أن ذلك قد أدى إلى وصوله إلى المعلومات فإن القصد يعد منتفياً لديه، لعدم إدراك الفاعل للخطورة التي تنطوي على فعله، أما إذا أتى فعله وهو يعلم بأنه ليس هناك من وسيلة لدفع الخطر إلا بدخوله إلى النظام فإن القصد الجرمي يعد متوافراً لديه^(٣).

(١) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٦٥.

(٢) د. محمود نجيب حسني، المرجع السابق، ص ٦٥.

(٣) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٦٥.

كما يتعين للقول بتوافر القصد الجرمي أن يتوقع الفاعل حين يأتي فعله النتيجة التي سوف تترتب على فعله، والنتيجة حادثة مستقبلية لأنها لا تحدث إلا في وقت لاحق للفعل وتعد أثراً له، والتوقع يعني قراءة المستقبل ورسم صورة ذهنية لتسلسل الأحداث التي تترتب على فعل الفاعل، وتوقع النتيجة الإجرامية هي الأساس التي تقوم عليها إرادة النتيجة، فحيث لا يوجد توقع لا تتصور الإرادة^(١)، والنتيجة التي يتعين أن تتجه إليها توقع الفاعل هي النتيجة التي يحددها القانون، وتتمثل في جريمة الدخول بوصول الفاعل إلى نظام المعلومات أو البرامج أو المعلومات التي يخترنها، ولا يشترط أن يمتد علم الفاعل إلى الآثار التي قد تترتب على فعله والتي لا يتطلبها النموذج القانوني للجريمة، فلا يشترط مثلاً أن يتوقع الفاعل انهيار النظام الأمني الذي يحمي المعلومات، أو الخسائر المالية التي قد تترتب على الجهة التي ينتمي إليها النظام، أو الإلتلاف الذي قد يصيب المعلومات أو الخلل الذي قد يحدث في وظائف النظام.

كما لا يتطلب أن يتجه توقع الفاعل إلى عناصر أو حدود لا يتطلبها النموذج القانوني في فكرة النتيجة حتى ولو كان من شأنها أن تمنحها مزيداً من التحديد^(٢)، فلا يشترط أن يتوقع الفاعل تحقق الوصول إلى نظام محدد بذاته، ومعظم النصوص القانونية في التشريعات التي جرمت الدخول لا تتطلب أن يتحقق الدخول في موضوع معين، وتبعاً لذلك فإذا توقع الفاعل أن يتحقق الدخول في نظام أو معلومات محددة ثم ترتب على فعله الوصول إلى نظام أو معلومات أخرى فإنَّ القصد يظل متوافراً لديه، وتفسير ذلك أن تحقق النتيجة في موضوع بعينه ليس من العناصر التي يتطلبها القانون في تحديد جريمة الدخول، هذا وقد أشارت المادة الأولى من قانون إساءة الحاسبات الآلية صراحة على أنه ليس من عناصر القصد الجرمي توقع الفاعل وصوله

(١) د. محمود نجيب حسني، المرجع السابق، ص ٧٥.

(٢) المرجع ذاته، ص ٧٦.

إلى برامج أو معلومات محددة أو برامج أو معلومات من نوع معين أو أن يتوقع الفاعل وصوله إلى برامج أو معلومات مخزنة على نظام محدد .

- ٤ - توقع علاقة السببية:

كما يتعين أن يمتد علم الفاعل إلى توقع علاقة السببية التي تصل بين الفعل والنتيجة، وذلك بأن يتوقع الآثار المباشرة للفعل والتي تزداد جسامتها تدريجاً حتى تتحقق النتيجة الإجرامية^(١)، ففي جريمة الدخول يتطلب القصد الجرمي أن يتوقع الفاعل أن تشغيل الحاسب الآلي من شأنه أن يرسل الإشارات إلى وحدة المعالجة المركزية والتي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة والتي تقوم بدورها بتشغيل النظام المسؤول^(٢)، وإذا توقع الفاعل علاقة السببية على نحو مخالف لما جرى في الواقع فإن ذلك ليس من شأنه أن ينفي القصد الجرمي إلا إذا كان الغلط في توقع علاقة السببية جوهرياً، ويكون الغلط جوهرياً إذا كان الاختلاف بين التسلسل السببي الذي توقعه الفاعل والتسلسل السببي الذي تحقق يشكل قيمة قانونية^(٣)، وتبعاً لذلك ففي جريمة الدخول إذا توقع الفاعل بأن البرنامج الذي يستعين به في اجتياز الإجراءات الأمنية من شأنه تبديل كلمات المرور حتى يتوصل إلى كلمة مرور صحيحة تخوله الوصول إلى النظام إلا أن البرنامج قام بدلاً عن ذلك بتعطيل هذه الإجراءات، ففي هذه الحالة لا يعد هذا الغلط جوهرياً، وذلك لأن النصوص القانونية التي تجرم الدخول لا تتطلب أن يتم الدخول وفق تسلسل سببي معين، إلا أن الأمر يختلف فيما إذا كانت النصوص القانونية التي تجرم الدخول تتطلب أن يتم هذا الدخول من خلال تسلسل سببي معين، وفي هذه الحالة يعد الغلط في توقع علاقة السببية جوهرياً كما هو الحال في التشريعات التي تتطلب النصوص القانونية فيها أن يتم الدخول عن طريق اختراق الإجراءات الأمنية التي تحمي النظام.

(١) المرجع ذاته.

(٢) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٤٤.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ١٠٣.

وعلى كل حال فإنه في الحالات التي يوصف فيها الغلط بأنه غير جوهري يفترض أن يكون الفاعل قد بلغ في نشاطه مرحلة التنفيذ، أما إذا طرأ التطور في التسلسل السببي حين كان الفاعل ما يزال في مرحلة التحضير للجريمة، فإن الغلط يعد نافياً للقصد الجرمي^(١)، وذلك كأن يتفشى البرنامج الفيروسي الذي يعمل الفاعل على تحضيره على شبكة الانترنت مؤدياً إلى إنشاء اتصال مع الأنظمة التي ترتبط مع الشبكة.

- ب - العلم بالتكليف:

لا تقتصر فكرة القصد الجرمي على العلم بوقائع معينة، وإنما تتطلب بالإضافة إلى ذلك العلم باكتساب هذه الوقائع تكييفاً معيناً، ذلك أنه في بعض الجرائم يعد التكليف الذي تكتسبه بعض الوقائع من عناصرها الأساسية، ولذلك فإنه ينبغي أن يحيط الفاعل علماً بهذا التكليف^(٢)، وتطبيقاً لذلك فإنه يتعين أن يعلم الفاعل بأن دخوله غير مصرح به، فمفهوم عدم التصريح هو تكليف لواقعة الدخول التي يتعين أن ينصرف علم الفاعل إليها، فإن انتفى علم الفاعل على هذا النحو انتفى القصد الجرمي لدى الفاعل، كأن يعتقد الفاعل بأنه يقوم بالدخول إلى نظام متاح للجمهور أو يعتقد بأن التصريح الممنوح له شامل لكل أجزاء النظام.

- ج - الوقائع التي لا يتطلب العلم بها:

إذا كانت الوقائع السابقة مما يتعين أن يحيط علم الفاعل بها لما لها من أهمية قانونية في تكوين الجريمة فإن هناك وقائع يسأل عنها الفاعل دون أن يتطلب القانون علمه بها، فلا يشترط أن يحيط علم الفعل بعناصر الأهلية الجزائية، أو الشروط الموضوعية للعقاب، أو الظروف التي تتوقف على درجة جسامه الجريمة، أو الظروف التي تشدد العقوبة دون أن تغير من وصف الجريمة.

(١) المرجع ذاته، ص ١٠٥.

(٢) المرجع ذاته، ص ١١٥.

١ - عناصر الأهلية الجزائية:

لا يشترط أن يحيط علم الفاعل بعناصر الأهلية الجزائية، فهذه العناصر تنتج أثرها القانوني سواء علم الفاعل بها أو لم يعلم، وتفسير ذلك أن هذه العناصر لا تعد من بين أجزاء السلوك الإجرامي، أو مما يترتب عله من ضرر اجتماعي، أو ما يحيط به من وقائع تحدد خطورته على المجتمع^(١)، وتبعاً لذلك فإن اعتقد الفاعل خطأ وقت إتيانه للفعل بأنه دون السن التي حددها القانون للمسؤولية الجزائية فإن هذا الاعتقاد المغلوط لا يكون من شأنه أن ينفي القصد الجرمي.

٢ - الشروط الموضوعية للعقاب:

لا يشترط أن يمتد علم الفاعل إلى الشروط الموضوعية للعقاب، وتفسير ذلك أن هذه الشروط هي وقائع خارجة عن التكوين القانوني للجريمة تضاف إليها لا لكي يتحقق وجودها وإنما لكي تحدث أثرها القانوني في توقيع العقاب^(٢)، فعلى سبيل المثال القانون السوري لا يعاقب على جريمة الدخول التي يرتكبها أحد السوريين خارج إقليم الدولة إلا إذا كان قانون الدولة التي ارتكب الجريمة على أرضها يعاقب عليها، وتبعاً لذلك فإنه إذا ثبت أن الفاعل لم يعلم بأن قانون الدولة الأجنبية يجرم الدخول غير المصرح به جاز عقابه على الرغم من ذلك، لأن هذا الشرط هو أحد الشروط الموضوعية للعقاب والذي لا يشترط أن يحيط علم الفاعل بها^(٣).

٣ - الوقائع التي تحدد درجة جسامة النتيجة:

كما أنه لا يشترط أن يحيط علم الفاعل بالوقائع التي تحدد جسامة النتيجة وتشكل ظرفاً مشدداً للعقوبة، فالقانون لا يشترط أن ينصرف علم الفاعل إلى ما يترتب على فعله من إتلاف للمعلومات أو إلحاق أضرار بصاحب المعلومات ما لم تتطلب

(١) المرجع ذاته، ص ٨٢.

(٢) المرجع ذاته ص ٨٣.

(٣) المادة ٢٤ من قانون العقوبات السوري.

النصوص القانونية قصداً خاصاً، ولذلك فإن كان الظرف المشدد يرتبط بدرجة جسامة النتيجة المترتبة على الفعل وقع العقاب المشدد دون أن يتطلب القانون توقع النتيجة الأشد جسامة والتي أفضى فعله إليها، وإنما يتطلب فقط انصراف إرادته إلى توقع النتيجة الأقل جسامة، وبهذا فإنَّ الفاعل يسأل عن النتيجة الأشد جسامة على الرغم من عدم توقعه لها^(١)، ومن التشريعات التي نصت على تشديد العقوبة تبعاً لجسامة النتيجة القانون الفرنسي، فالفقرة الثانية من المادة ١١٣٢٣ من قانون العقوبات تشدد عقوبة الدخول إذا ترتب على نشاط الفاعل محو أو تعديل البيانات أو تعطيل النظام عن القيام بعمله، ولا يتطلب المشرع الفرنسي توقع الفاعل للنتيجة الأشد جسامة. ولذلك فقد اتجه بعض الفقه على اعتبار التجريم على هذا النحو جريمة إتلاف غير مقصودة، إلا أنَّ اعتبار هذه الفقرة من الظروف المشددة يعد الأدق من الناحية التأصيلية في قانون العقوبات، وذلك لأنه يشترط لتطبيق هذه الفقرة أن يكون الفاعل مرتكباً لجريمة الدخول والتي تتمتع باستقلالية عن جريمة الإتلاف^(٢).

- ٤ - الوقائع التي يقتصر أثرها على تشديد العقوبة:

لا يشترط أن يمتد علم الفاعل إلى الوقائع التي تشدد العقوبة دون أن تغير من وصف الجريمة ولم تمس بالتعديل أحد أركانها وإنما اقتصر أثرها على تشديد العقوبة^(٣)، وبناءً على ذلك فإنَّ شدد القانون عقوبة الدخول غير المصرح به إذا دخل الفاعل عن طريق اختراق الإجراءات الأمنية التي تحمي النظام، فإنَّ العقوبة المشددة تطبق على الفاعل دون أن يتطلب انصراف علمه إلى ذلك، وتفسير ذلك أنَّ هذه الوقائع تثبت ازدياد الخطورة الكامنة في شخصية الفاعل بما يجعل العقوبة العادية غير كافية لردعه.

(١) د. محمود نجيب حسني، المرجع السابق، ص ٨٤.

(٢) د. أيمن فكري، المرجع السابق، ص ٢٠٧.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ٨٥.

- ٢ - الإرادة:

إذا ما توافر العلم على النحو السابق تعين للقول بتوافر القصد أن تنتج إرادة الفاعل إلى إتيان فعل الدخول وإلى تحقيق الوصول إلى المعلومات غير المصرح للفاعل الوصول إليها، وإرادة الفعل مفترضة، حيث يفترض أن الإنسان لا يصدر عنه فعل إلا بإرادته^(١)، إلا أن هذه القرينة ليست قاطعة فهي تقبل إثبات العكس إذا ثبت أن هذه الإرادة لا تنتمي إلى نفسية الفاعل كأن تكون وليدة إكراه أو قوة قاهرة^(٢)، كما هو الحال عند إجبار الفاعل بالدخول إلى نظام غير مصرح له بالدخول إليه تحت قوة السلاح، كما يستوي في إرادة النتيجة أن تنتج إرادة الفاعل إلى تحقيق الوصول إلى المعلومات باعتباره الغرض الذي يتوخاه الفاعل من فعله، أو أنه يرتبط على نحو لازم بالغرض الذي أراد تحقيقه^(٣)، أو أن تنتج إرادة الفاعل إلى قبول هذا الأثر باعتباره أثراً ممكناً لفعل الدخول^(٤).

وإذا تحقق القصد الجرمي على النحو السابق فلا عبرة بعد ذلك للدافع أو الغاية فهما لا يحسبان بين عناصر القصد الجرمي وإذا كانا نبيلين فلا ينفيان^(٥)، ويترتب على ذلك أن ادعاء الفاعل بأن دخوله كان بغاية الكشف عن أوجه القصور في الإجراءات الفنية التي تحمي المعلومات لا ينفي القصد الجرمي^(٦).

(١) د. محمد الفاضل، المرجع السابق، ص ٢٦٨.

(٢) د. رمسيس بهنام، المرجع السابق، ص ٩٢.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ٢١٨.

(٤) المرجع ذاته، ص ٢٧٤.

(٥) المرجع ذاته، ص ٢٠٤.

(٦) United States of America, Appellee, v. Robert Tappan Morris, 1991.

ثانياً: وقت توافر القصد

الأصل في الجريمة أن يعاصر القصد الجرمي عناصر الركن المادي للجريمة، فينبغي توافره وقت الفعل وأن يبقى قائماً حتى تحقق النتيجة الجرمية^(١)، وبتطبيق ذلك على جريمة الدخول فإنه يتعين أن يتوافر القصد الجرمي ساعة إتيان الفاعل لفعل الدخول ووقت تحقق الوصول إلى المعلومات.

ولكن قد يحدث أحياناً أن يعاصر القصد أحد عناصر الركن المادي في الجريمة دون عناصره الأخرى، فقد يتوافر القصد لحظة إتيان نشاط الدخول ثم ينتفي في الوقت الذي يتحقق فيه الوصول إلى المعلومات، وذلك كأن يقوم شخص بتشغيل الحاسب الآلي أو بإدخال بيانات المرور بقصد الوصول إلى المعلومات التي يحتويها النظام، إلا أنه وقبل الوصول إلى هذه المعلومات يحاول إيقاف النظام عن معالجة الأوامر، بحيث يثبت انتفاء القصد الجرمي لديه، كما أنه قد يطرأ القصد حين تحقق الوصول إلى المعلومات دون أن يكون متوافراً ساعة ارتكاب نشاط الدخول، ذلك كأن يقوم أحد الأشخاص بتشغيل الحاسب الآلي ظناً منه أنه مصرح له بالدخول إليه، إلا أنه وفي مرحلة معالجة النظام للأوامر يدرك الفاعل خطأه، إلا أنه وعلى الرغم من ذلك لا يحاول إيقاف ذلك، وبدلاً من ذلك يوجه إرادته إلى تحقيق الوصول إلى المعلومات، وإن كان هذا الفرض بعيد الاحتمال، وذلك لأنه مع التقدم المستمر في مجال نظم المعلومات أصبحت تتم معالجة المعلومات بسرعة هائلة، وأصبح من المستبعد وجود فترة زمنية بين نشاط الدخول والوصول إلى المعلومات تكفي للقول بإمكانية تغيير الفاعل إرادته، إلا أنه وبعيداً عن هذه الحقيقة الفنية فقد أثّرنا ذكر هذه النقطة في التحليل القانوني.

والقاعدة في القصد الجرمي هي أن يعاصر فعل الدخول، ذلك لأنَّ القصد إرادة، والإرادة هي عنصر في الفعل ينبعث منها ويتحقق وجوده في العالم الخارجي، ومن ثم كان وقت إتيان الفعل هو الوقت الذي يجب أن تتحقق فيه الإرادة ويتحدد

(١) د. محمد الفاضل، المرجع السابق، ص ٢٨٣.

اتجاهها وقيمتها القانونية، أما إذا لم يتوافر القصد إلا في المرحلة التي تتلو نشاط الدخول والتي توشك فيها النتيجة على التحقق عدّ قصداً لاحقاً لا اعتداد به، وشرط ذلك هو انتهاء فعل الدخول قبل تحقق القصد، ومعيار ذلك هو انقضاء السيطرة على الحركة العضوية وآثارها، أما إذا استمر الفاعل بالسيطرة على هذه الحركة فهذا يعني أن الفعل لم ينته، وبالتالي فإنّ هناك تعاصر بين فعل الدخول والقصد الجرمي بما يكفي لإشادة الركن المعنوي في جريمة الدخول^(١).

وهناك من يرى أنّه يكفي لإشادة الركن المعنوي في جريمة الدخول أن يعاصر القصد الجرمي نشاط الدخول أو الوصول إلى المعلومات، وذلك مرده إلى نظرهم إلى جريمة الدخول كجريمة مستمرة يستمر فيها النشاط الإجرامي من لحظة تحققه في العالم الخارجي كحركة عضوية تتبع من إرادة الفاعل، وحتى خروج الفاعل من النظام الذي يحتوي المعلومات التي تم الوصول إليها^(٢)، إلا أنّ هذا منتقد، وذلك لأن جريمة الدخول جريمة وقتية ينتهي فيها النشاط الإجرامي بمجرد الوصول إلى المعلومات، وتبعاً لذلك فإن تحقق القصد في المرحلة التي تتلو هذا النشاط لا اعتداد به في جريمة الدخول وإن كان يصلح من جهة أخرى لإشادة الركن المعنوي في جريمة البقاء.

ثالثاً: القصد الخاص

قد تتطلب بعض النصوص القانونية في التشريعات التي جرمت الدخول غير المصرح به قصداً خاصاً إلى جانب القصد العام، وذلك بأن تتطلب انصراف العلم والإرادة إلى وقائع لا تعد من أركان الجريمة وتمثل غاية معينة للفاعل^(٣)، وتختلف التشريعات في تحديد الأثر القانوني للقصد الخاص، ففي بعض التشريعات يعد القصد الخاص عنصراً في الركن المعنوي للجريمة بحيث ينتفي هذا الركن ما لم يتوافر هذا

(١) د. محمود نجب حسني، قانون العقوبات اللبناني القسم العام، دار النهضة العربية، بيروت، ١٩٨٤، ص ٤٢٤.

(٢) د. أيمن فكري، المرجع السابق، ص ٢٤١.

(٣) د. رمسيس بهنام، المرجع السابق، ص ٩٠٦.

القصد، وفي بعضها الآخر قد يقتصر دوره على تحدد الوصف القانوني للجريمة أو تشديد العقوبة^(١).

فالقانون السعودي في نظام مكافحة الجريمة المعلوماتية يتطلب قصداً خاصاً في جميع صور جريمة الدخول، فالمادة الثالثة تجرم الدخول الذي يرتكب بقصد تهديد شخص أو ابتزازه أو بقصد العبث بمحتويات موقع الكتروني، والمادة الخامسة تجرم الدخول الذي يرتكب بقصد العبث بالبيانات الخاصة، والمادة السابعة تجرم الدخول الذي يرتكب بقصد الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني، وتبعاً لذلك فإنَّ القصد الخاص يعد عنصراً في الركن المعنوي لجريمة الدخول ولذلك فإنه يترتب على تخلف هذا القصد انتفاء الركن المعنوي وبالتالي انتفاء الجريمة.

وقد يقتصر أثر القصد الخاص في بعض التشريعات على تشديد العقوبة، كما هو الحال في القانون الدانماركي الذي يشدد عقوبة جريمة الدخول متى ارتكبت بقصد الاطلاع على المعلومات المتعلقة بالأسرار التجارية للشركات^(٢)، كما أنَّ القانون البلجيكي يشدد عقوبة الجريمة إذا ما ارتكبت بقصد الاحتيال أو إلحاق ضرر بالغير^(٣).

كما يشدد المشرع السوري في الفقرة ب من المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية عقوبة جريمة الدخول إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها أو إلغائها أو تغييرها أو تشويهها أو تزيفها أو استخدامها أو إفشائها، ويتطلب المشرع السوري انصراف إرادة الفاعل إلى ارتكاب هذه الوقائع اللاحقة، إلا أنه لا يشترط أن تتعاصر نية ارتكاب هذه الوقائع اللاحقة مع نية ارتكاب جريمة الدخول، فلا يغير من الأمر شيئاً إذا ما اتجهت إرادة الفاعل إلى ارتكاب الوقائع اللاحقة والتي تشكل الظرف المشدد للعقوبة في المرحلة التي تتلو ارتكاب جريمة الدخول، كما أنه في بعض الحالات فإن انصراف

(١) د. محمود نجب حسني، المرجع السابق، ص ٤٧٢.

(٢) المادة ٢٦٤ من قانون العقوبات الدانماركي.

(٣) المادة ٥٥٠ من قانون العقوبات البلجيكي.

إرادة الفاعل إلى ارتكاب هذه الوقائع اللاحقة من شأنه أن يشيد كلاً من القصد العام الذي تتطلبه جريمة الدخول والقصد الخاص الذي يتطلبه الظرف المشدد، ذلك أنه في هذه الحالات يعد الدخول أحد النتائج اللازمة لسلوك الفاعل والتي لا يتصور تحقق الوقائع التي اتجهت إرادة الفاعل إليها دون الدخول إلى النظام، ولا يغير من الأمر شيئاً أن يكون الفاعل مصرح له بالدخول إلى النظام إذا ما كان غير مصرح له بإتيان الوقائع اللاحقة، ذلك لأنّ المشرع السوري جرم كلاً من الدخول غير المصرح به والدخول الذي يتم من دون صلاحية أي الدخول الذي يتم بتجاوز التصريح الممنوح للفاعل، إلا أنه ومن جهة أخرى فإنّ العقاب يغدو متعذراً في الحالات التي تتجه إرادة الفاعل إلى ارتكاب هذه الوقائع بعد أن أتم دخوله إلى النظام وكان هذا الدخول مصرحاً به ابتداءً، وذلك لأنّ جريمة الدخول الأساسية والتي يبنى على أساسها التشديد تعد منتفية في هذه الحالة، إلا أنه وعلى كل حال فإنّ نهج المشرع السوري في تشديد العقوبة منتقد، وذلك لأنه من شأنه أن يضيق من نطاق هذا التشديد حيث أنه يشترط لإيقاع العقوبة المشددة أمرين اثنين: أولهما أن تتصرف إرادة الفاعل إلى تحقيق الوقائع اللاحقة، وثانيهما أن يتحقق الاعتداء اللاحق فعلاً، ولتفادي هذا الانتقاد كان من الأفضل لو انتهج المشرع السوري نهج المشرع الدانماركي أو البلجيكي بأن يشدد العقوبة بمجرد انصراف إرادة الفاعل إلى إتيان الوقائع اللاحقة دون أن يتطلب تحقق الاعتداء فعلاً.

وفي المملكة المتحدة ينص قانون إساءة استخدام الحاسبات الآلية في المادة الثانية على جريمة الدخول بقصد ارتكاب أو تسهيل ارتكاب جريمة، وتتوافر أركان هذه الجريمة متى ارتكب الفاعل جريمة الدخول التي نصت عليها المادة الأولى من هذا القانون بقصد ارتكاب أو تسهيل ارتكاب جريمة لاحقة، وقد أشارت اللجنة المكلفة بوضع القانون على أنّ هذه الجريمة قد صيغت أساساً لمواجهة الحالات التي ترتكب فيها جريمة الدخول بقصد ارتكاب جرائم أخرى، إلا أنه لا يمكن العقاب عليها لأنها لم

تتم ولم يتم الشروع فيها حتى^(١)، كما أشارت هذه اللجنة أيضاً على أنه لا يشترط أن تكون الجريمة اللاحقة موضوعها نظام الحاسب، كما أنه يستوي أن تتجه إرادة الفاعل إلى ارتكابها بنفسه أو من قبل غيره^(٢)، ونصت الفقرة الثالثة من المادة الثانية على أنه لا يشترط أن تتعاصر نية ارتكاب الجريمة اللاحقة مع نية ارتكاب جريمة الدخول، وإنما لا يغير من الأمر شيئاً أن تتوافر هذه النية بعد ارتكاب جريمة الدخول، كما نصت الفقرة الرابعة من المادة ذاتها على أنه لا يغير من الأمر شيئاً أن يكون ارتكاب الجريمة اللاحقة مستحيلاً، ونصت الفقرة الخامسة على أن يعاقب الفاعل بالحبس لمدة لا تتجاوز خمس سنوات.

⁽¹⁾ Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.52

⁽²⁾ Law Com. No.186, Computer Misuse. Cm.819 1989, para.3.49

المطلب الثاني: الدخول الخطأ

الخطأ هو الصورة الأخرى التي يتخذها الركن المعنوي في الجريمة، وجميع التشريعات التي تناولت جريمة الدخول لم تجرم الدخول الذي يرتكب عن طريق الخطأ، وهذا ما يبقي التساؤل قائماً عن مدى إمكانية ارتكاب جريمة الدخول عن طريق الخطأ، وعن ضرورة مواجهة هذا الدخول الذي يرتكب عن طريق الخطأ.

أولاً: الخطأ في الدخول

الخطأ هو صورة الركن المعنوي في الجريمة غير المقصودة، وهو في ذلك يتفق مع القصد، إلا أنهما يختلفان في أن الإرادة تتجه في القصد دون الخطأ إلى النتيجة الإجرامية، فتسيطر بذلك سيطرة فعلية على عناصر الجريمة في حين تقتصر سيطرتها على بعض العناصر في حالة الخطأ، ولذلك فإنه لا محل للبحث عن الخطأ إلا إذا ثبت انتفاء القصد، إلا أن ذلك ليس معناه أن انتفاء القصد يعني حتماً توافر الخطأ^(١)، إذ أن للخطأ عناصره الذاتية والذي لا يمكن القول بتوافره إلا بتوافر هذه العناصر وهي اثنتين: أولهما الإخلال بواجبات الحيطة والحذر، وثانيهما وجود علاقة ذهنية ونفسية بين الفاعل والنتيجة^(٢).

وواجب الحيطة والحذر هو واجب عام ملقى على عاتق كل شخص في سلوكه وأعماله ليتجنب الإضرار بالآخرين، والمصدر العام لهذه الواجبات هو الخبرة الإنسانية العامة والتي تقرر مجموعة من القواعد التي تحدد النحو الصحيح الذي يجب أن يباشر وفقاً لها أحد أنواع السلوك، وقد يعترف القانون بجانب من هذه الخبرة فيصبح القانون هو مصدر هذه الواجبات^(٣)، وإن مصادر هذه الواجبات من شأنها أن تقرر مجموعة من القواعد العامة التي يتوجب على الفاعل أن يلتزم بها أثناء إتيانه لسلوكه، وتبعاً لذلك فإذا التزم الفاعل بمقدار الحيطة والحذر التي تتطلبها هذه القواعد انتفى الخطأ من جانبه، أما إذا أخل بهذه القواعد كان من شأن ذلك أن يشيد الخطأ الذي يقوم به الركن

(١) د. محمود نجيب حسني، المرجع السابق، ص ٤٣٣.

(٢) د. عبود السراج، المرجع السابق، ص ٣٧١.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ٤٣٥.

المعنوي في الجريمة، ومن الحالات التي يمكن القول فيها بأن الفاعل قد أخل بقواعد الحيطة والحذر عدم تحقق الفاعل من أن اتفاقية الترخيص باستخدام النظام لا تصرح له بالدخول إلى أحد أجزاء النظام الذي يقوم بالدخول إليها، أو عدم تحقق الفاعل من أن النظام المصرح له بالدخول إليه هو النظام الذي يقوم بالدخول إليه، أو عندما يهمل الفاعل اتخاذ الاحتياطات اللازمة لمنع انتشار أحد البرامج الضارة عبر شبكة الاتصالات.

وحتى يقوم الخطأ لا يكفي أن ينزل الفاعل عن قواعد الحيطة والحذر، وإنما يتطلب بالإضافة إلى ذلك أن يفضي السلوك إلى نتيجة معينة، ومن ثم كان متعيناً أن تتوافر علاقة ذهنية ونفسية بين الفاعل والنتيجة الجرمية^(١)، وتتخذ هذه العلاقة إحدى صورتين: الصورة الأولى وهي الخطأ غير الواعي، وفيها لا يتوقع الفاعل حدوث النتيجة الجرمية في حين كان باستطاعته وبإمكانه توقعها فلا يبذل جهداً للحيلولة دون وقوعها، أما الصورة الثانية فهي الخطأ الواعي وفيها يتوقع الفاعل إمكان حدوث النتيجة الجرمية، إلا أن إرادته لا تتجه إلى ذلك ويعتقد - معتمداً على احتياط أو غير معتمد - بأنها لن تحدث^(٢).

ومما تقدم نرى أن جريمة الدخول يمكن تصور وقوعها بصورة غير مقصودة، كأن يعتقد الفاعل بأن دخوله إلى نظام المعلومات مصرحاً به، أو يعتقد بأنه يقوم ببعض العمليات الحسابية، وفي هاتين الحالتين يفترض الفاعل بأنه لم يتوقع حدوث النتيجة الجرمية، إلا أنه كان من الممكن توقعها لو أنه التزم بالمقدار الواجب من الحيطة والحذر، كما أن الخطأ يمكن أن يتخذ صورة توقع النتيجة الإجرامية، كأن يتوقع الفاعل بأن قيامه بأحد الإجراءات من شأنها أن تؤدي إلى الدخول إلى أحد أجزاء النظام غير المصرح للفاعل بالدخول إليها، إلا أنه وجه إرادته إلى عدم تحقيق هذه النتيجة إلا أن الاعتداء تحقق على الرغم من ذلك.

(١) د. عبود السراج، المرجع السابق، ص ٣٧٧.

(٢) د. محمود نجيب حسني، المرجع السابق، ص ٤٣٩.

ثانياً: مواجهة الدخول الخطأ

كما أشرنا سابقاً أن وصف جريمة الدخول بأنها مقصودة أو غير مقصودة هو وصف ينصرف إلى النشاط الذهني والنفسي للفاعل الذي كان عليه ساعة إقدامه على ارتكاب الجريمة، ففي الجريمة المقصودة يوجه الفاعل إرادته إلى إتيان فعل الدخول وإلى تحقيق الوصول إلى المعلومات، أما في الجريمة غير المقصودة فيوجه الفاعل إرادته إلى إتيان فعل الدخول دون الأثر الذي يترتب عليه، ولهذا فإن كون الدخول مقصوداً أو غير مقصود لا يغير من حقيقة الأمر أنه يشكل تعدياً على المعلومات المراد حمايتها، هذا وإن كان من المسلم به أن خطورة الفاعل الذي تتجه إرادته إلى تحقيق الاعتداء أشد من خطورة الفاعل الذي تتراخى إرادته عن منع تحقق الاعتداء^(١)، فإنّ هذا التمييز ينبغي أن تقتصر آثاره على مقدار اللوم الذي يستحقه الفاعل ومحلّه^(٢)، كما أنّ تجريم الدخول الذي يتم عن طريق الخطأ له فائدة من الناحية العملية حيث أنّ إثبات الخطأ أيسر وأسهل من إثبات القصد، وإثبات القصد يتطلب إثبات اتجاه إرادة الفاعل إلى إتيان الفعل الخطر والأثر الناجم عنه، في حين أنّ إثبات القصد لا يتطلب سوى إثبات اتجاه الإرادة إلى إتيان الفعل الخطر، وهي إرادة مفترضة، وإخلال الفاعل بواجبات الحيطة والحذر التي تتطلبها القواعد العامة.

إلا أنّه من جهة أخرى فإنّ عمليات الدخول أصبحت تتكرر كل يوم مئات المرات وتتم من قبل عدد هائل من المستخدمين، وأصبح ليس من المستبعد في ظل ذلك أن تكون هناك عمليات دخول غير مقصودة، ولو تم تجريم هذه الأفعال فإنّه سيؤدي إلى إحجام عدد كبير من مستخدمي الأنظمة عن استخدامها خشية وقوع أفعالهم تحت طائلة التجريم، ولذلك فإنّ المنطق يحتم الموازنة بين حماية المعلومات وحماية حق المستخدمين في استخدام الأنظمة وتبادل المعلومات بين هذه الأنظمة،

(١) د. محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ١١.

(٢) د. رمسيس بهنام، المرجع السابق، ص ٩٢٨.

وذلك من خلال اقتصار التجريم على أفعال الدخول المقصودة دون تلك التي تتم عن طريق الخطأ^(١).

إلا أنه من جهة ثالثة فإنَّ عدم تجريم أفعال الدخول التي تتم عن طريق الخطأ لا يحيله سلوكاً مشروعاً، وإنما يستمر بالاتسام بعدم المشروعية ذلك أنه يظل على الرغم من ذلك يشكل تعدياً على المعلومات، ولذلك فإنَّ المنطق يحتم مواجهة هذا السلوك بإحدى الوسائل التي يكون من شأنها حماية المعلومات دون أن تهدر الحقوق المشروعة للمستخدمين، هذا وتتضمن بعض التشريعات نصوصاً تكفل هذه الموازنة، وهي النصوص التي تجرم الإبقاء على اتصال تم بطريق الخطأ مع نظام المعلومات والنصوص التي تجرم الدخول إلى أجزاء نظام المعلومات.

- ١ - مواجهة الدخول الخطأ من خلال جريمة البقاء:

تتضمن بعض التشريعات نصوصاً تجرم البقاء في نظام المعلومات، ويعرف البقاء بأنه التواجد داخل النظام المعلوماتي ضد إرادة من له الحق في السيطرة عليها، هذا وقد صيغت هذه الجريمة أساساً لمواجهة أفعال الدخول التي تتم عن طريق الخطأ^(٢)، ولذلك فإنَّ جريمة البقاء تتطلب أمرين: أولهما أن يتم الدخول عن طريق الخطأ إلى نظام المعلومات، وثانيهما أن تنتج إرادة الفاعل إلى البقاء في هذا النظام، ويذهب بعض الفقهاء إلى القول بأنَّ جريمة البقاء على هذا النحو هي جريمة سلبية، حيث أنها تقوم بمجرد امتناع الفاعل عن الخروج من النظام الذي تم الدخول إليه عن طريق الخطأ، ذلك أنَّ هذا الدخول يولد التزاماً على عاتق الفاعل بالخروج من النظام وامتناع الفاعل عن تأدية هذا الالتزام يشكل الركن المادي في جريمة البقاء، ونحن نرى أنَّ جريمة البقاء هي جريمة إيجابية، ذلك أنَّ الامتناع عن الخروج من النظام ليس مناط التجريم وإنما هو بقاء الفاعل في النظام الذي دخل إليه عن طريق الخطأ^(٣).

(١) محمد خليفة، المرجع السابق، ص ١٦٣.

(٢) د. أيمن فكري، المرجع السابق، ص ٢٣٧.

(٣) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٤٩.

وتأتي أهمية تجريم البقاء في أنها لا تتطلب تحقق أثراً معيناً لسلوك الفاعل وإنما تتم بمجرد انصراف إرادته إلى البقاء في النظام، كما أن جريمة البقاء هي جريمة مستمرة حيث أنض الاعتداء على المعلومات يستمر كلما استمر البقاء في النظام، ولذلك فإنَّ الفاعل يعد مرتكباً لجريمة البقاء متى أدرك الخطأ الذي وقع فيه واتجهت إرادته إلى تحقيق البقاء في أي لحظة خلال الفترة الممتدة من دخول الفاعل إلى النظام وحتى تسجيل خروجه منه.

- ٢ - مواجهة الدخول الخطأ من خلال جريمة الدخول ذاتها:

قد لا تنص التشريعات على جريمة البقاء، وفي هذه الحالة فإنَّه يمكن مواجهة الدخول الذي يتم عن طريق الخطأ من خلال جريمة الدخول ذاتها، ذلك أنَّه في بعض التشريعات تجرم النصوص القانونية الدخول إلى كل البرامج والمعلومات أو إلى كل جزء من أجزاء النظام، وفي هذه التشريعات فإنَّ الدخول الذي يتم عن طريق الخطأ لا يشكل مانعاً دون إمكانية ارتكاب جريمة دخول لاحقة، حيث يمكن القول بأنَّه من الناحية التقنية فإنَّ أفعال الدخول تتكرر في كل حركة دخول إلى كل معلومة أو برنامج وإلى كل جزء من أجزاء النظام^(١)، إلا أنَّه لإيقاع العقوبة على الفاعل في هذه الحالة، لا بد من أن يتحقق أمرين: أولهما أن تتجه إرادة الفاعل إلى الدخول إلى أي من البرامج أو المعلومات أو إلى أي من أجزاء النظام الأخرى، وثانيهما أن يتحقق هذا الدخول فعلاً.

إلا أنَّ مواجهة الدخول على هذا النحو يثير صعوبة في حالة النصوص التي تتطلب أن يتم الدخول عن طريق اختراق الإجراءات الأمنية، ففي هذه الحالة فإنه يتعين أن تكون كل معلومة وكل برنامج أو كل جزء من أجزاء النظام محمياً بهذه الإجراءات^(٢)، هذا وإن كان في الغالب أن هذه الإجراءات تشكل عائقاً يحول دون الدخول إلى النظام أو أنها تشكل قرينة على قصد الفاعل ذلك لأن تجاوز هذه

(١) د. أيمن فكري، المرجع السابق، ص ٣٤٩.

(٢) د. نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٤٩.

الإجراءات يتطلب استخدام وسائل تكنولوجية في سبيل ذلك، إلا أنَّ هذه القرينة ليست قاطعة، فقد يوصف الدخول بأنه تم عن طريق الخطأ بسبب غلط الفاعل في توقع علاقة السببية أثناء إعداده لأحد البرامج في مرحلة التحضير للجريمة، كما أنَّه لا يمكن مواجهة الدخول الذي يتم عن طريق الخطأ من خلال هذه النصوص فيما إذا اكتفى الفاعل بإبقاء الاتصال مع النظام دون أن يقوم بحركة تنقل داخل هذا النظام.

خلاصة الفصل الثاني

- ١ - يتحقق نشاط الدخول بأي وسيلة يتم من خلالها الوصول إلى المعلومات.
- ٢ - جريمة الدخول جريمة مادية، ويتمثل الأثر المادي للدخول بالوصول إلى المعلومات.
- ٣ - للدخول نطاقه الخاص ومجاله الذي لا يتداخل به مع غيره، ويمكن تحديده بجميع الأفعال التي يتم من خلالها الوصول إلى المعلومات.
- ٤ - إنَّ الصفة غير المشروعة للدخول تتحقق في حالتين: حالة الدخول الذي يتم دون تصريح من المسؤول عن النظام، وحالة الدخول الذي يتم من خلال تجاوز التصريح، وهذه الحالة تتعلق إما بتجاوز المجال المكاني أو الزماني للتصريح، أو بتجاوز الغرض الذي منح لأجله التصريح.
- ٥ - يتخذ الركن المعنوي في جريمة الدخول صورة القصد الجرمي.
- ٦ - إنَّ مواجهة الدخول الذي يتم عن طريق الخطأ يتم من خلال تجريم البقاء في نظام المعلومات.

الخاتمة

تناولنا من خلال دراستنا لجريمة الدخول موضوع هذه الجريمة، فبينما المحل المادي الذي يتحقق فيه نشاط الدخول، ونوع الحق المحمي في هذه الجريمة، ثم تناولنا ركني جريمة الدخول، فبينما مفهوم الدخول وحدوده وطبيعته والوسيلة التي يتحقق من خلالها والأثر الناجم عنه والحالات التي يسبغ بها بعدم المشروعية، كما بينا صورة الركن المعنوي في التشريعات التي تضمنت نصوصاً تجرم الدخول، ثم تعرضنا لحالات الدخول التي تتم عن طريق الخطأ وكيفية التصدي لها.

- ١ - النتائج:

انتهت دراستنا إلى مجموعة من النتائج نورد أبرزها:

- ١- تمثل المعلومات مجموعة من الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلاً محدداً يجعلها قابلة للتبادل والتفسير والمعالجة بواسطة الأفراد أو بوسائل الكترونية، وهي تشمل كل المكونات المنطقية لنظام المعلومات.
- ٢- إنّ المعلومات التي تشكل محلاً للحماية في جريمة الدخول يجب أن تتصف بالإلكترونية، ويكون لها هذه الخاصية من خلال علاقتها بوسائل التقنية الحديثة التي يتم من خلالها معالجة المعلومات.
- ٣- إنّ التدخل التشريعي في مواجهة الدخول يمكن أن يبنى على أساس حماية حق الملكية، أو سرية أو سلامة المعلومات.
- ٤- إنّ المحل المادي الذي ينصب عليه النشاط الجرمي هو المعلومات الالكترونية التي يتكون منها نظام المعلومات.
- ٥- إنّ نشاط الدخول يتحقق بأي وسيلة يتم من خلالها الوصول إلى المعلومات.

٦- إنّ الصفة غير المشروعة للدخول تتحقق في حالتين: حالة الدخول الذي يتم دون تصريح من المسؤول عن النظام، وحالة الدخول الذي يتم من خلال تجاوز التصريح، وهذه الحالة تتعلق إما بتجاوز المجال المكاني أو الزماني للتصريح، أو بتجاوز الغرض الذي منح لأجله التصريح.

٧- ينبغي مواجهة الدخول الذي يتم عن طريق الخطأ، وذلك من خلال جريمة البقاء غير المصرح به.

٨- إنّ الظروف المشددة للعقوبة نوعين:

- الظروف المادية: وتتعلق هذه الظروف إما بكيفية ارتكاب الجريمة كالدخول الذي يتم عن طريق اختراقات الإجراءات الأمنية التي تحمي المعلومات، وإما تتعلق بدرجة جسامه النتيجة وهي الدخول الذي يترتب عليه إتلاف للمعلومات أو تعديلها أو أضرار أخرى أو الحصول على معلومات محددة أو مكاسب من الدخول.

- الظروف الشخصية: وتتعلق هذه الظروف إما بالجانب المعنوي من الجريمة وهي الدخول الذي يتم بقصد ارتكاب أو تسهيل ارتكاب جريمة أو التمهيد لها أو بقصد إلحاق ضرر، وإما تتعلق بشخص الفاعل وهي الدخول الذي يتم من خلال استغلال المركز الوظيفي لارتكاب الجريمة.

٩- إنّ مواجهة الوصول إلى المعلومات التي تنتقل عبر الشبكات المعلوماتية يتم إما من خلال التجريم الموسع للدخول، أو من خلال أفراد نصوص خاصة بجريمة الاعتراض.

١٠- إنّ مواجهة الاستعمال غير المصرح به لنظام المعلومات يتم إما من خلال جريمة الدخول أو من خلال أفراد نصوص خاصة بجريمة الاستعمال غير المصرح به.

- ٢ - التوصيات:

على ضوء النتائج السابقة نوصي بما يلي.:

١- يجب تجريم الدخول غير المشروع إلى نظام المعلومات على أن تكون الغاية من التجريم هي حماية سرية المعلومات، وأن يتم تحديد محل الجريمة بالمعلومات التي يتكون منها النظام المعلوماتي، وتحديد مفهوم الدخول على أنه النشاط الذي يتم من خلاله الوصول إلى المعلومات، وتحديد الصفة غير المشروعة للفعل بالحالات التي يتم فيها الدخول دون تصريح من المسؤول أو بتجاوز التصريح.

٢- يجب تشديد عقوبة الدخول في الحالات التالية:

- إذا تم الدخول من خلال اختراق الإجراءات الفنية التي تحمي المعلومات.

- إذا ترتب على الدخول إحداث أضرار بالمعلومات.

- إذا تم الدخول بقصد ارتكاب أو تسهيل ارتكاب جريمة أو التمهيد لها أو بقصد إلحاق ضرر بالمعلومات.

- إذا ارتكب الدخول من خلال إساءة السلطات الوظيفية من قبل أحد الأشخاص.

٣- يجب تجريم البقاء غير المصرح به في نظام المعلومات.

٤- يجب تجريم الاعتراض غير المصرح به للمعلومات المتداولة على شبكة المعلومات.

٥- يجب تجريم الاستعمال غير المصرح به لنظام المعلومات.

اقتراح تعديل نص المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية:

أ- يعاقب بالغرامة من عشرين ألفاً إلى مئة ألف ليرة سورية كل من دخل قصداً إلى نظام معلوماتي، أو إلى أحد أجزائه، دون أن يملك الصلاحية أو التصريح للقيام بذلك.

ب- يعاقب بذات العقوبة كل من أبقى على اتصال تمّ عن طريق الخطأ مع نظام معلوماتي.

ج- وتكون العقوبة الحبس من ثلاث أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية إذا تمّ الدخول عن طريق اختراق الإجراءات الأمنية، أو إذا ترتب على فعل الدخول إتلاف أو محو أو تعديل المعلومات التي تمّ الوصول إليها، أو إذا تمّ الدخول بقصد ارتكاب أو تسهيل ارتكاب جريمة أو التمهيد لها، أو بقصد إلحاق ضرر بالمعلومات، أو إذا تمّ الحصول على أي منفعة من الدخول.

قائمة المراجع

أولاً: المراجع باللغة العربية:

المؤلفات العامة:

- د. رمسيس بهنام، النظرية العامة للقانون الجنائي، منشأة المعارف، طبعة
ثالثة منقحة، ١٩٩٧.
- د. عبود السراج، شرح قانون العقوبات القسم العام، منشورات جامعة دمشق،
٢٠٠٦/١٤٢٧.
- د. محمود نجيب حسني، شرح قانون العقوبات اللبناني القسم العام، دار
النهضة العربية، بيروت، ١٩٨٤.

المؤلفات المتخصصة:

- د. أيمن فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة
للنشر، الإسكندرية، ٢٠٠٧.
- بيل جيتس، المعلوماتية بعد الانترنت، ترجمة عبد السلام رضوان، عالم
المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ١٩٩٨.
- د. حسن طاهر داود، الحاسب وأمن المعومات، معهد الإدارة العامة،
المملكة العربية السعودية، الرياض، ١٤٢١.
- د. حشمت قاسم، مدخل لدراسة المكتبات وعلم المعلومات، مكتبة غريب،
بدون مكان وسنة نشر.
- د. خالد ممدوح ابراهيم، الجرائم المعلوماتية ، دار الفكر الجامعي،
الإسكندرية، ٢٠٠٩.

- د. عماد الصباغ، نظم المعلومات ماهيتها ومكوناتها، مكتبة دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٠.

- د. قاسم عبد الرزاق، نظام المعلومات المحاسبة الحاسوبية، مكتبة الثقافة للنشر والتوزيع، عمان، ١٩٩٨.

- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، ٢٠٠٧.

- د. محمد السعيد خشبة ، المعالجة الالكترونية للمعلومات ، بدون دار نشر ، ١٩٩١.

- د. محمد الفاضل، الجرائم الواقعة على الأشخاص، مطابع فتى العرب، الطبعة الثالثة، دمشق، ١٩٦٥\١٣٨٤.

- د. محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقاتها، دار الشروق، دون مكان نشر، ١٩٨٩.

- د. محمود نجيب حسني، علاقة السببية في قانون العقوبات، دون دار نشر، دون مكان نشر، دون سنة نشر.

- د. محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٩.

- د. معن أحمد محمد الحياوي، الركن المادي للجريمة، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠.

- د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية تطبيقية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٤.

- د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، ١٩٩٢.

- د. ياسر يوسف عبد المعطي، مقدمة في الحاسب الآلي وتطبيقاته، شركة المكتبات الكويتية، ١٩٩٤.

- د. يحيى مصطفى حلمي، أساسيات نظم المعلومات، مكتبة عين شمس، القاهرة، ١٩٩٨.

- د. يحيى مصطفى حلمي ومحمد السعيد خشبة، الكمبيوتر ونظم المعلومات ، مكتبة عين شمس، القاهرة، ١٩٩٠.

مقالات وأبحاث متخصصة:

- د. أحمد علي، مفهوم المعلومات في إدارة المعرفة، مجلة جامعة دمشق، المجلد الأول، العدد الأول، ٢٠١٢.

- د. صبري حمد خاطر، التأسيس لنظام قانوني للمعلومات، المجلة الدولية للملكية الفكرية، جامعة البحرين، المجلد الأول، العدد الأول، ٢٠١٣.

- د. مصطفى محمد عرجاوي، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤.

- د. علي عبد القادر القهوجي، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، الطبعة الثالثة، ٢٠٠٤.

الرسائل العلمية:

- آمال قارة، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، ٢٠٠١-
استخرج من: [http://djelfa.info/csrct/wp-](http://djelfa.info/csrct/wp-content/uploads/2014/03/content.pdf)
<http://djelfa.info/csrct/wp-content/uploads/2014/03/content.pdf>

- عبد الرحمن جميل محمود حسين، الحماية القانونية لبرامج الحاسب الآلي،
رسالة ماجستير، جامعة النجاح الوطنية، نابلس، ٢٠٠٨، استخرج
من: <http://dspace.univ-tlemcen.dz/bitstream/112/2818/3/rassa3.pdf>

- رصاع فتحية، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة
ماجستير، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، ٢٠١١-
٢٠١٢، استخرج من:

http://scholar.najah.edu/sites/default/files/allthesis/legal_protection_of_computer_programs.pdf

المعاجم:

- أحمد محمد الشامي وسيد حسب الله، المعجم الموسوعي لمصطلحات
المكتبات والمعلومات، دار المريخ، الرياض، ١٤٠٨-١٩٨٨.

- د. أحمد مختار محمد، معجم اللغة العربية المعاصرة، المجلد الثاني، عالم
الكتب، القاهرة، ٢٠٠٨.

- أندريه لوغارف، المعجم الموسوعي في الكمبيوتر والإلكترونيك، الطبعة
الثانية، ترجمة د. عبد الحسن الحسيني، المؤسسة الجامعية للدراسات والنشر والتوزيع،
بيروت، ١٩٨٨.

- د. شعبان خليفة، قاموس البنهاوي الموسوعي في مصطلحات المكتبات والمعلومات، دار العربي للنشر والتوزيع، القاهرة، ١٩٩٠.

- د. عبد الغفور عبد الفتاح قاري، معجم مصطلحات الكمبيوتر، مطبوعات مكتبة الملك فهد (السلسلة الثالثة)، الرياض، ٢٠٠٠/١٤٢٠.

- معجم الحاسبات، الطبعة الثانية الموسعة، مجمع اللغة العربية، مصر، ١٩٩٥.

القوانين واللوائح :

١- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري الصادر بالمرسوم التشريعي رقم (١٧) للعام ٢٠١٢.

٢- قانون مكافحة جرائم تقنية المعلومات الإماراتي الصادر بالقانون الاتحادي رقم (٢) للعام ٢٠٠٦.

٣- نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (٣٩) لسنة ١٤٢٨ هـ والمصادق عليه بالمرسوم الملكي رقم (م/١٧) لسنة ١٤٢٨ هـ.

٤- قانون الأونيسترال النموذجي بشأن التجارة الالكترونية مع دليل التشريع ١٩٩٦.

ثانياً: المراجع باللغة الفرنسية:

– Christophe Geiger, La privatisation de l'information par la propriété intellectuelle, Revue internationale de droit économique, 2006, 20 (4) en publié surle site: http://www.cairn.info/resume.php?ID_ARTICLE=RIDE_204_0361

– Michel Vivant, La privatisation de l'information par la propriété intellectuelle, Revue internationale de droit économique, 2006, 20 (4) en publié surle site: http://www.cairn.info/resume.php?ID_ARTICLE=RIDE_204_0361

ثالثاً: المراجع باللغة الانكليزية:

– Council of Eroup, Computer Related Crime: Recommendation No. R 89 9 on Computer-related crime and final Report of the European Committee on Crime Problems, Strasbourg 1990 at: http://www.oas.org/juridico/english/cyber_links_coe.htm

– Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001 at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

– Council of Europe, Explanatory Report for Convention on Cybercrime at: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

– Convention for The protection of individuals with regard to automatic processing of personal data, Strasbourg, 28.I.1981 at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

– Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 pp: 0031 – 0050 at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

– Global Information Assurance Certification Paper at: <http://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264>

– H. Marshall Jarrett & Michael W. Bailie ,Prosecuting Computer Crimes: Crimes Computer Crime and Intellectual Property Section Criminal Division, Office of Legal. Education Executive Office for United States Attorneys at: <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf>

– Law Com. No.186, Computer Misuse. Cm.819 1989 at: <http://www.bailii.org/ew/other/EWLC/1989/186.pdf>

– Martin. Paul, NASA Cybersecurity: An Examination of the Agency's Information Security at: http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

– Neil Macewan, 2008 ,The Computer Misuse Act 1990: lessons from its past and predictions for its future ,Criminal Law Review, University of Salford, Manchester at: http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf

– OECD Guidelines for the Security of Information Systems 26 November 1992 at: <http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm>

– Orin S. Kerr, 2003, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 New York University Law Review 1596 at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740##

– Robert M. Losee, 1988, A Discipline Independent Definition of Information, J. of the American Society for

Information Science, U. of North Carolina–Chapel Hill at:
<http://www.ils.unc.edu/~losee/book5.pdf>

– Scot Law Com. No 106, Report on Computer
Crime.Cm.174 1987 at::
http://www.scotlawcom.gov.uk/download_file/view/391

– Tom Stonier, 1990, Information and the Internal
Structure of the Universe, an exploration into information physics,
new york ,springer – verlag at:
<http://www.burlgrey.com/xtra/infola/infolap3.htm>

Laws code:

Australia, The Cybercrime Act 2001, Article 478.

Belgium, Criminal Code 2000, Article 550 b.

Canada, Criminal Code 2003, Section 342.

Denmark, Penal Code 2004, Section 263.

Finland, Penal Code 1995, Chapter 38, Section 8.

France, Penal Code 2004, Article 323.

Germany, Penal Code 2006, Section 202.

Greece, Criminal Code 1988, Article 370.

Italy, Penal Code 2008, Article 615.

The Netherlands, Criminal Code 2006, Article 143 .

Norway, The General Civil Penal Code 2005, Section 145.

Portugal, Criminal Information Law 1991, Chapter 1, Article 7.

Sweden, Penal Code 1998, Chapter 4, Section 9.

Switzerland, Penal Code 2005, Article 143 bis.

United Kingdom, Computer Misuse Act 1990.

At: <http://www.cybercrimelaw.net/Cybercrimelaws.html>

California penal code, Part 1, Title 13, Chapter 5, Section 502.

Florida Computer Crimes Act 2012, Title XLVI, Chapter 815.

New York penal code, Part 3, Title J, Article 156.

United State Code, Title 18, Part I, Chapter 47, section 1030.

At: <http://law.justia.com/>

المحتويات

- ١ - مقدمة
- ٩ - الفصل الأول: موضوع الدخول
- ١٠ - المبحث الأول: محل الدخول
- ١٠ - المطلب الأول: الاتجاهات التشريعية في تحديد محل الدخول
- ١٤ - المطلب الثاني: المعلومات
- ١٤ - أولاً: التعريف اللغوي للمعلومات
- ١٥ - ثانياً: المعلومات اصطلاحاً
- ١٦ - ثالثاً: المعلومات فقهاً
- ١٨ - رابعاً: المعلومات تشريعاً
- ٢١ - المطلب الثالث: نظام المعلومات
- ٢١ - أولاً: مفهوم نظام المعلومات
- ٢٥ - ثانياً: مكونات النظام المعلوماتي
- ٣٦ - المبحث الثاني: المصلحة المحمية
- ٣٦ - المطلب الأول: المصلحة المحمية في الجريمة المعلوماتية
- ٣٦ - أولاً: الاتجاه الأول
- ٣٨ - ثانياً: الاتجاه الثاني
- ٤٠ - ثالثاً: الاتجاه المختلط
- ٤١ - المطلب الثاني: المصلحة المحمية في جريمة الدخول
- ٤١ - أولاً: سرية المعلومات
- ٤٢ - ثانياً: معيار سرية المعلومات

- ٥٠ - الفصل الثاني: ركني الدخول
- ٥١ - المبحث الأول: الركن المادي
- ٥١ - المطلب الأول: فعل الدخول
- ٥٢ - أولاً: مفهوم الدخول
- ٥٦ - ثانياً: وسيلة الدخول
- ٥٨ - ثالثاً: نطاق الدخول
- ٦٣ - رابعاً: الصفة غير المشروعة للدخول
- ٧٧ - المطلب الثاني: الوصول إلى المعلومات
- ٧٧ - أولاً: الاتجاهات التشريعية في تحديد النتيجة الإجرامية
- ٧٩ - ثانياً: طبيعة جريمة الدخول
- ٨٢ - ثالثاً: تخلف الوصول إلى المعلومات
- ٨٤ - رابعاً: العلاقة بين فعل الدخول والوصول إلى المعلومات
- ٨٦ - المبحث الثاني: الركن المعنوي
- ٨٦ - المطلب الأول: الدخول قصداً
- ٨٧ - أولاً: القصد العام
- ٩٦ - ثانياً: وقت توافر القصد
- ٩٧ - ثالثاً: القصد الخاص
- ١٠١ - المطلب الثاني: الدخول الخطأ
- ١٠١ - أولاً: الخطأ في الدخول
- ١٠٣ - ثانياً: مواجهة الدخول الخطأ
- ١٠٨ - الخاتمة
- ١١٢ - قائمة المراجع