مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً

د. سامي حمدان الرواشدة*

د. أحمد موسى الهياجنة

تاريخ تقديم البحث: ٢٠٠٩/٣/٨ تاريخ القبول: ٢٠٠٩/٨/١٣

ملخص

يقدم هذا البحث دراسة قانونية تحليلية للجرائم التي ترتكب عبر الانترنت وشبكات المعلومات في القانون الإنجليزي. فقد أصدرت المملكة المتحدة قانوناً يسمى "قانون إساءة استخدام الحاسوب" لعام ١٩٩٠. دخل هذا القانون حيز التنفيذ في التاسع والعشرين من شهر آب لعام ١٩٩٠، وقد تم بموجبه استحداث ثلاث جرائم يمكن أن تقع باستخدام الحاسوب، أو قد تقع على الحاسوب. عالج هذا التشريع المشاكل القانونية التي نشأت عن التقدم العلمي والتكنولوجي في مجال تكنولوجيا المعلومات. وقد تناول هذا البحث هذه الجرائم، كما تضمنت هذه الدراسة تحليلاً للاجتهادات القضائية الانجليزية فيما يتعلق بالقانون المشار إليه. ومن الجدير بالذكر أن اختيار القانون الإنجليزي محلا لموضوع هذه الدراسة يعود لسببين هما: إن القانون الإنجليزي يعتبر قانونا نموذجاً تبنته بعض التشريعات الجزائية واقتبسته باعتباره قانونا عصرياً في مجال مواجهة الجريمة المعلوماتية. والثاني يتجسد في أن قواعد القانون الموضوعية لم تكن مجرد مبادئ للحماية، بل كان لها صدى واسعٌ في التطبيق العملي ممثلا بالاجتهاد القضائي.

تهدف هذه الدراسة إلى تسليط الضوء على الجريمة المعلوماتية، وتعرض بالتفصيل للأنشطة غير المشروعة التي تتم باستخدام الحاسوب والانترنت مستعينة للوصول إلى هذا الهدف بالحلول القانونية والقضائية التي أخذت بها التشريعات المقارنة خاصة القانون الإنجليزي بالنظر إلى أن النظم القانونية الغربية هي مهد هذه الحلول. إن هذه الدراسة تتيح لنا فرصة الإطلاع على الوسائل التي تبناها المشرع الجزائي المقارن لمعالجة جرائم الحاسوب ومن ثم بيان مدى نجاحها في التصدي للانعكاسات السلبية الناجمة عن استخدام الحاسوب لغايات غير مشروعة. ونأمل أن يلبي المشرع الأردني الدعوة لتدارك أوجه القصور في التشريع الجزائي وإصدار تشريع خاص يواجه الجريمة المعلوماتية على غرار القانون الانجليزي.

* كلية الحقوق، الجامعة الأردنية.

Abstract

Control of Cybercrime: The English Law Approach

This research paper is an analytical legal study on crimes committed via the internet and other computer networks in English law. The United Kingdom issued the "Computer Misuse Act 1990". wich came into force on 29 August 1990. The Act has created three new offences, and deals with some of the difficult questions created by advances in information technology. This research deals only with the substantive changes wrought in the criminal law by the Act. It also reviews case law, and highlights the response of the courts to the new Act. This research study was chosen for two reasons. First, United Kingdom is one of the foremost countries in which the legal system is suitably prepared for fighting cybercrime. Moreover, the Computer Misuse Act 1990 provisions have been adopted by other jurisdictions. Secondly, the Computer Misuse Act 1990 does go considerable way in providing an effective and adequate legislative framework to deal with this form of criminal activity. This was reflected by an extensive case law.

This study highlights computer and information technology crime, and explores criminal acts conducted and committed through computers and Internet. In order to address these issues, the research paper will consider comparative laws, specially the, English law. The aim of this approach is to explore new directions of thinking and to look abroad in order to learn about better ways of preventing and combating cyber crime. It is very important to look at what other legal systems have done to fight such crimes. From the analysis, one main concluding point seem to be most evident. Control of Cyber crime legislation, similar to English law, should be enacted by the Jordanian legislature. This legislation should be kept up to date with technological changes, especially with the current rapid development of technology.

مقدمة

يقول أحد المفكرين الفرنسيين "إن الكمبيوتر بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة ومن عدم نسيان ما يختزن فيه، قد يقلب حياتنا رأساً على عقب يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا ومعاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد"[1]. إن فتوحات عصر المعلومات وما تحقق في بيئة شبكات المعلومات والعالم الإلكتروني يتجاوز كثيراً ما أشار إليه هذا المفكر. حيث إن مراحل التطور التي وصلت إليه عالم المعلوماتية أمكنها أن تجمع شتات المعلومات عن كل فرد وتحيلها إلى بيان تفصيلي بتحركاته وهوياته واهتماماته ومركزه المالي.

إن الثورة المعلوماتية أصبحت تلعب دوراً بارزاً في الوقت الراهن وأصبحت قوة لا يستهان بها في أيدي الدول والأفراد، فالمحور الأساسي للثورة في عالم المعلوماتية تتمثل في التطور الهائل الذي شهده قطاعا تكنولوجيا المعلومات والاتصالات، وفيما لا شك فيه أن الثورة المعلوماتية وما تضمنته من استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها تركت أثاراً إيجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول إذ تعتمد القطاعات المختلفة في أدائها لأعمالها بشكل أساسي على استخدام الأنظمة المعلوماتية ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات.

كما أصبحت هذه الأنظمة مستودعاً لأسرار الأشخاص سواء تلك المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية. وكذلك أسست مستودعاً للمعلومات الحربية والصناعية والاقتصادية للدول وقد كانت تعتبر على قدر كبير من السرية، إلا أن مخاطر التقنيات الحديثة على حماية المعلومات الشخصية كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الإلكترونية وقواعد البيانات الشخصية ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها، أصبح أمراً لايمكن التغاضي عنه. ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في مجال تحليل المعلومات واسترجاعها، وجمع البيانات الشخصية وتخزينها ومعالجتها لأغراض متعددة فيما يُعرف ببنوك ومراكز المعلومات الوطنية، ظهر بشكل متسارع الشعور بمخاطر تقنية المعلومات، والذي نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية المختزنة على أجهزة الحاسوب. وعليه فإنه يمكن إجمال المعالم الرئيسية لمخاطر الحواسيب وبنوك المعلومات فيما يلي:

---

(١) أشار إليه المحامي يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، بحث منشور على شبكة الانترنت: *www.arblaws.com*

إن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة تجمع من الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل، وتستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل، وقد يفتح مجالاً أوسع لإساءة استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً، بالإضافة إلى مراقبة الأفراد وتعرية خصوصياتهم. كما إن شيوع (النقل الرقمي) خلق مشكلة أمنية وطنية إذ سهل استخدام السمع والتجسس الإلكتروني. إن من أكثر معالم خطر الحواسيب وبنوك المعلومات على الحياة الخاصة هو ما تحويه من بيانات قد تكون غير دقيقة أو معلومات غير كاملة لم يجرى تعديلها بما يكفل اكتمالها وتصويبها. إن المعلومات الشخصية التي كانت منعزلة ومتفرقة والوصول إليها صعب ومتعذر، أصبحت بوجود بنوك المعلومات مجتمعة ومتوافرة ومتكاملة وسهلة المنال. وبصورة موجزه نقول إن الانعكاسات السلبية التي أفرزتها التقنية الحديثة واستخدام الحاسوب هو إساءة استخدام الحاسوب واستغلاله على نحو غير مشروع أبرز أنماطاً مستحدثة من الجرائم يطلق عليها: "جرائم الحاسوب" أو "الجرائم المعلوماتية". وهي من أكثر المواضيع إثارة للجدل في أيامنا هذه، بل ومن أكثرها أهمية بالنظر لآثارها المالية والقانونية على حد سواء.

لقد ظهر مصطلح "جرائم الحاسوب" في نهاية التسعينيات من القرن الماضي وأستخدم هذا المصطلح من أجل وصف الجرائم المتعلقة بالحاسوب بشكل عام. لكن أصبح هنالك تمييز الآن بين الجرائم التي ترتكب باستخدام الحاسوب وبين الجرائم التي يكون دور الحاسوب فيها عارضاً. لقد اقترحت الهيئة الأوروبية (European Commission) استخدام المصطلحات التالية مترادفات للتعبير عن الجريمة المعلوماتية وهي: (Computer Crime) و(Computer-related crime) و(High tech Crime) و(Cybercrime)[1]. وتمتاز الجريمة المعلوماتية بعدد من الخصائص أهمها: أن هذه الجرائم لا يمكن أن تنجح إلا من خلال استخدام الشبكة العالمية دون أن تتقيد بالوقت أو المساحة، ولذلك فإنها تختلف عن تلك الجرائم التي يمكن أن يُستخدم الحاسوب لارتكابها. وقد أصبحت الشبكة المعلوماتية تستخدم من أجل ارتكاب عدد من الأنشطة المجرمة مثل: الجرائم المالية، ومراقبة الاتصالات بصورة غير قانونية، ونشر الصور الخلاعية. إذ إن كل هذه الأنشطة الجرمية تشكل قلقا للأفراد والدول على حد سواء وأصبحت تشكل مشكلة عالمية للحكومات

(1) Communication from Commission to European Parliament: 2000, Creating a safer Information Society by Combating Computer-related Crime.

والقطاعين التجاري والصناعي في مختلف الدول. ومن أكبر العثرات التي تواجه عملية مكافحة الجريمة المعلوماتية هي اكتشاف النشاط الإجرامي، وتحديد هوية الفاعل، وحماية النظام المعلوماتي، والملاحقة الجزائية لمرتكبي هذه الجرائم عندما يتعلق الأمر بأفراد يقومون بارتكابها في الخارج وما ينشأ عن ذلك من مشاكل قانونية تتعلق بالاتهام والاختصاص القضائي. ويمكن تعريف الجريمة المعلوماتية بأنها[١] "نشاط أو سلوك يرتكب بواسطة الحاسوب ويعتبر نشاطا غير قانوني أو محرماً في بعض التشريعات، ويمكن ارتكابه عن طريق استخدام الشبكة الالكترونية العالمية"[٢].

إن الجريمة المعلوماتية أصبحت-بحق- "الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة أو هي المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات"[٣] إن الجريمة المعلوماتية تكشف أن ضحايا هذا النوع من الجرائم هم الأفراد، والمؤسسات، والشركات وحتى المراكز الأمنية التابعة للدولة، وأن هذه الجرائم ترتكب من قبل أشخاص قد يصعب في كثير من الأحيان معرفتهم أو تحديد هويتهم يتوصلون من خلال ارتكاب هذه الأفعال من الاستيلاء على المعلومات الخاصة والأسرار التجارية للشركات والمؤسسات، والحسابات البنكية للأفراد والمؤسسات على حد سواء. إن حماية المجتمع ضد هذا النوع من الإجرام الجارف يقتضي تعميق وظيفة الردع للقانون الجنائي. وهذه الوظيفة لا يمكن أن تتحقق إلا من خلال وضع آليات فاعلة من شأنها أن تساعد في الكشف عن هذه الجرائم وملاحقة مرتكبيها ومعاقبة فاعليها. إن من أهم حقوق ضحايا الجرائم المعلوماتية هو تقديم الجناة إلى العدالة لمحاكمتهم عن الأفعال التي اقترفوها. وإن إنشاء أجهزة شرطة متخصصة تمتلك الصلاحيات القانونية والوسائل المناسبة لملاحقة هؤلاء الجناة هو أمر لا مفر منه. كما أن الحق في الحياة الخاصة يعتبر من الحقوق الأساسية في المجتمعات الديمقراطية كما نصت عليه المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان لعام ١٩٥٠التي صادق عليها حوالي (٥٦) دولة. وإن التطورات الجديدة في مجال المعلوماتية مكنت الأفراد من ممارسة حياتهم الخاصة بمعزل عن أي رقيب أثناء إطلاع الآخرين على المواقع المختلفة على الشبكة العنكبوتية من خلال بقاء الشخص مجهول الهوية بحيث تبقى أقواله وأفعاله بعيدة عن المراقبة والتتبع، إلا إن ذلك لا يمنع من القول إن فتوحات التطور التكنولوجي تركت الباب مفتوحا أمام إساءة الإستخدام. فقد شهدت

(1) D. Thomas and B. Loader: Cyber Crime, P. 3.

(٢) للمزيد حول تعريف "الجريمة المعلوماتية" انظر: المحامي يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات: جرائم الكمبيوتر والانترنت (Cyber Crime)، الجزء الأول، اتحاد المصارف العربية، الطبعة الأولى، ٢٠٠٢، ص: ٢٠٧-٢٢٥.

(٣) محمود صالح العادلي، الجرائم المعلوماتية: ماهيتها وصورها، ورقة مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان، ٢-٢٠٠٦/٤/٤.

التسعينات من القرن الماضي استخدام الحاسوب والانترنت في ارتكاب الكثير من الأنشطة غير القانونية. وللتدليل على نمو هذا النوع المستحدث من الإجرام يكفي أن نشير هنا إلى الإحصاءات التي نشرها مكتب التحقيقات الجنائية الفدرالي الألماني عام ٢٠٠١ والتي تبين ارتفاع جرائم الحاسوب من (٥٠٠٠) جريمة عام ١٩٩٠ إلى (٤٥٠٠٠) جريمة عام ١٩٩٩[١]. كما تشير إحدى الدراسات التي قامت بها مؤسسة (Price Waterhouse) البريطانية عام ٢٠٠١ على (٣٤٠٠) شركة ومنظمة ومؤسسة حكومية إلى أنّ ٤٣% منها قد كانت ضحية للاستخدام غير المشروع للحاسوب أو الشبكة المعلوماتية[٢].

إن موضوع الجريمة المعلوماتية أصبح يهيمن على جدول أعمال معظم الحكومات في العالم. في بريطانيا، أنشأت وزارة الداخلية البريطانية وحدة خاصة مهمتها التحقيق في الجرائم الخطيرة والمنظمة التي ترتكب باستخدام تكنولوجيا المعلومات. كما أن صلاحيات وكالة الشرطة الأوروبية التي باشرت عملها رسمياً في عام ١٩٩٩ امتدت لتشمل هذا النوع من أنماط السلوك الإجرامي مثل: الاحتيال، والدخول إلى الأنظمة المعلوماتية وتعطيل الشبكات. وقد تم اعتماد هذه الصلاحيات والنص عليها في اتفاقية المجلس الأوروبي المتعلقة بالجريمة المعلوماتية لعام ٢٠٠١ (Councilof Europe's Convention on Cyber crime) التي تهدف إلى تبني حلول قانونية لحماية المجتمع من الجرائم المعلوماتية وتوثيق التعاون الدولي في مكافحتها[٣]. في الماضي لم يكن ينظر إلى مرتكبي هذا النوع من السلوك على أنهم مجرمون وكانت الأعمال التي يقومون بها توصف بأنها "بحث عن المعلومات بقصد إضاعة الوقت والتسلية" أو "عملية فكرية تشبه أحجية الكلمات المتقاطعة". لكن وجهة النظر تلك تغيرت الآن؛ ذلك إن قراصنة الحاسوب يبحثون دوما عن مواقع الضعف في النظام المعلوماتي الأمر الذي يمكنهم من الحصول على معلومات خاصة وسرية للأفراد والمؤسسات. إن نشاط قراصنة الحاسوب من شأنه إلحاق أضرار فادحة وتعريض السلامة العامة للخطر. ويكفي للتدليل على ذلك أن نشير إلى أن القضاء الأمريكي قضى بإدانة أحد الأحداث لقيامه باختراق النظام المعلوماتي الخاص بمطار (Worcester) الأمر الذي أدى إلى تعطيل عمل برج المراقبة الخاص بسلطة الطيران المدني الفدرالية لمدة ست ساعات كاملة وذلك في عام ١٩٩٧ [٤].

(1) Statistics of the Federal Office of Criminal Investigation (Germany, per Germany's Interior Minister, Otto Schilly, *Financial Times Supplement "Connectus" Issue 15, October 2001.*

(2)European Economic Crime Survey 2001, Financial Times "Connectus" , October 2001.

(3) Natasha Jarvic, "Control of Cybercrime: Is an End to our Privacy on the Internet a Price Worth Paying? Part 1, ***Computer and Telecommunications Law Review*** 2003, 9(3), 76–81.

(4) Natasha Jarvic, "Control of Cybercrime: Is an End to our Privacy on the Internet a Price Worth Paying? Part 1, Computer and Telecommunications Law Review 20003, 9(3), 78.

كما أن استخدام برامج الفيروسات ألحق خسائر مالية بعدد كبير من الشركات والمؤسسات التجارية. ففي إحدى القضايا في الولايات المتحدة الأمريكية تمكن أحد الأشخاص من زرع فايروس في النظام المعلوماتي العائد إلى إحدى الشركات التجارية مما أدى إلى تعطيل النظام المعلوماتي المستخدم مـــن قبل أكثر من (٢٠٠٠) موظف في الشركة عن العمل. وقدرت الخسائر المباشرة التي لحقت بالشركة بمبلغ وقدره مائة ألف دولار(١).

مبررات اختيار الموضوع:

كان لظهور هذا النوع من الجرائم الأثر الهام في خلق تحديات كثيرة في مواجهة النظام القانوني القائم في عدد من الدول وخاصة في مواجهة قانون العقوبات، الأمر الذي دعى الفقه والقضاء إلـــى البحث فيما إذا كانت النصوص القانونية في قانون العقوبات كافية لمواجهة هذا النوع مـــن الجـــرائم بشتى أنواعها، أم أن الأمر يستدعي استحداث قواعد قانونية جديدة أو نصوص خاصة قـــادرة علـــى احتواء هذا النوع من الجرائم تراعي طبيعتها وخصوصيتها.

إن هذه الدراسة تهدف إلى تسليط الضوء على الجريمة المعلوماتية وخاصة جـــرائم الحاســـوب والإنترنت باعتبارها جرائم تتميز بالحداثة. وسنحاول من خلال هذه الدراسة التعـــرض بالتفـــصيل للأنشطة المتعلقة بإساءة استخدام الحاسوب مستعينين للوصول إلى هذا الهـــدف بـــالحلول القانونيـــة والقضائية التي أخذت بها التشريعات المقارنة وعلى الأخص القانون الإنجليزي بالنظر إلى أن النظم القانونية الغربية هي مهد هذه الحلول. إن الإطلاع على القانون والقضاء المقارن سيتيح لنا فرصـــة التعرف على الوسائل التي تبناها المشرع الجزائي لمعالجة جرائم الحاسوب، وبيان مدى نجاح هـــذه الوسائل والحلول في التصدي للإنعكاسات السلبية الناجمة عن اســـتخدام الحاســـوب لغايـــات غيـــر مشروعه على أمل أن يلبي المشرع الأردني الدعوة لتدارك أوجه القصور والنقص فـــي التـــشريع الجزائي وتبنى الحلول المقترحة إذا ما ثبت نجاحها.

بناء على ما تقدم، فإن هذه الدراسة لن تبحث في مدى كفاية وملائمة القواعد القانونية التقليديـــة الواردة في قانون العقوبات الأردني في الانطباق على الجرائم المستحدثة، وبيان فيما إذا كانت تقـــع تحت طائلة التجريم أم لا في ظل النصوص القائمة؟ هناك من الدراســـات القانونيـــة عالجـــت هـــذا الموضوع وتوصلت إلى عدد من النتائج نجملها فيما يلي:

أن النصوص القائمة حالياً في قانون العقوبات الأردني لا تجـــرم هـــذه الأنـــشطة وأن قـــانون العقوبات عاجز عن مواجهة هذا النوع من الجرائم. كما إن هنالـــك عقبـــات تحـــول دون تطبيـــق النصوص التقليدية على الجرائم المعلوماتية وأهم هذه العقبات هي أن نـــصوص قـــانون العقوبـــات

(1) *U.S v. Sullivan* (WD NC) (2001).

وضعت ابتداء لحماية الأموال ذات الكيان المادي الملموس ولم توضع لحماية الأموال المعنوية كالمعلومات ذلك أن فكرة المال المعلوماتي لم تكن قد تبلورت لدى المشرع وقت سن القانون لعدم اعتماد المجتمع على تكنولوجيا المعلومات في ذلك الوقت. إن المبدأ الأساسي الذي يحكم القانون الجنائي هو مبدأ شرعية الجرائم والعقوبات، حيث لا جريمة ولا عقوبة إلا بنص صريح وكذلك عدم جواز التوسع في تفسير النصوص الجنائية مما يشكل عائقاً أمام إمكانية إدراج الجرائم المعلوماتية ضمن النصوص التقليدية في قانون العقوبات الأردني. إذ لا بد من تدخل المشرع الجزائي الأردني لتعديل النصوص الجزائية الواردة في قانون العقوبات بحيث تراعي أيضاً طبيعة المعلومات وخصوصيتها واستحداث نصوص خاصة تكفل الحماية الجزائية للمعلوماتية. فلا بد من أن يتخلى المشرع الأردني عن الدعوة لتطويع نصوص قانون العقوبات لمواجهة الجديد في عالم الإجرام، ودعوة المشرع مسلحاً بإدراك عميق لماهية هذه الجرائم وخصائصها للتدخل من أجل توفير الحماية الجنائية للمعلومات وكيفية استخدام الحاسوب ومعطياته، ومواجهة كافة صور الاعتداء على معطيات الحاسوب من بيانات ومعلومات وبرامج. وهذا التدخل يتوجب مراعاة مرتكزات حماية الحق في المعلومات، والحق في الحياة الخاصة، ومراعاة التحديد الواضح لصور السلوك الإجرامي المنوي تجريمها، والأثر التقني على الصياغة القانونية، وأنواع العقوبات الملائمة إلى جانب مدّ نطاق التدخل ليطال القواعد الإجرائية إلى جانب القواعد الموضوعية حتى لا نكون أمام مجرد مبادئ للحماية لا تجد صدى لها في الواقع العملي. إن أهم مرتكزات التشريع في مجال مواجهة جرائم الحاسوب هو توحيد أداة الحماية، لتطال صور جرائم الحاسوب عموماً.

تتميز هذه الدراسة بإلقاء نظرة قانونية تحليلية للجرائم المستحدثة والمتعلقة بالحاسوب في القانون والقضاء الإنجليزي، فقد أصدرت المملكة المتحدة قانوناً يسمى قانون إساءة استخدام الحاسوب (Computer Misuse Act) في عام ١٩٩٠ تم بموجبه استحداث ثلاث جرائم يمكن أن تقع باستخدام الحاسوب أو قد تقع على الحاسوب. كما تضمنت هذه الدراسة تحليلاً للاجتهادات القضائية الإنجليزية فيما يتعلق بالقانون المشار إليه وهذا ما يميز هذه الدراسة عن غيرها من الدراسات القانونية في هذا الشأن. ومن الجدير بالذكر أن هنالك جملة من الأسباب دعت إلى جعل القانون الانجليزي محلا لموضوع هذه الدراسة أهمها: إن القانون الانجليزي يعتبر قانونا نموذجاً تبنته بعض التشريعات الجزائية واقتبسته باعتباره قانونا عصرياً في مجال مواجهة الجريمة المعلوماتية. ومن الأمثلة على هذه التشريعات: كندا، واستراليا وهونغ كونغ وسنغافورا. كما إن القواعد الموضوعية لهذا القانون لم تكن مجرد مبادئ للحماية بل كان لها صدى واسع في التطبيق العملي. ومما يدلل على ذلك غزارة الأحكام القضائية التي صدرت عن المحاكم الانجليزية بما في ذلك المحكمة العليا الممثلة بمجلس اللوردات (House of Lords).

مشكلة البحث:

تهدف هذه الدراسة للوقوف على أبرز صور السلوك الإجرامي التي تقـع علـى الحاسـوب أو بواسطته وخاصة تلك التي تستهدف البيانات الشخصية في بيئة المعالجة الآلية. إن الحقيقـة الأكيـدة هي أن القوانين الوطنية وفي نطاق حمايتها للعديد من تطبيقات حق الخصوصية بمفهومه المادي قـد جرّمت الاعتداءات التي تطال حرمة السكن، والمراسلات، والوثائق الـسرية وإفـشاء طائفـة مـن الأسرار المهنية، إلا إن القانون الأردني لم يسبغ حمايته القانونية على البيانات الشخصية خاصة من مخاطر المعالجة الآلية وتحديات توظيف التقنية في أنشطة جمع ومعالجة البيانات واستخدامها ونقلها وكذلك فإن القوانين الوطنية العقابية لم تجرم صور الاعتداء على البيانـات الشخـصية فـي البيئـة الرقمية. إن حماية خصوصية البيانات تستدعي ردع أنشطة الجمع غير المشروع للبيانات، وأنـشطة النقل غير المرخصة، وردع إفشاء البيانات الشخصية لغير المصرح لهم الاطلاع عليهـا، وأنـشطة حرمان أصحابها من حقوق الإطلاع والوصول والتصحيح والتحديث؛ لذلك فإن هذه الدراسة تهـدف إلى وضع إطار عام لصور الجرائم المعلوماتية التي تقع عن طريق استخدام الحاسـوب و صـور الاعتداء على البيانات الشخصية المعالجة في نظم المعلومات بالإضافة إلى الجرائم التي تقـع علـى أجهزة الحاسوب من خلال دراسة قانون إساءة استخدام الحاسوب الانجليزي لعام ١٩٩٠، آمـلاً أن يلبي المشرع الجزائي الدعوة ويوفر حماية جزائية للبيانـات والمعلومـات المتـوافرة فـي البيئـة الالكترونية على غرار القانون الإنجليزي.

حدود المشكلة:

نتناول هذه الدراسة الإطار العام لصور الإجرام التي تستهدف سلامة النظام المعلومـاتي كمـا ورد النص عليها في قانون إساءة استخدام الحاسوب الانجليزي لعام ١٩٩٠. وعليه فإن هذه الدراسة لن تتناول الجرائم التي تقع على حرمة الحياة الخاصة بواسطة أخـرى غيـر الحاسـوب كجـرائم المساس بسرية المراسلات، وجرائم إفشاء الأسرار، وجرائم الاستماع أو التسجيل أو التصنت أو نقل أو إذاعة الأحاديث الخاصة، وجرائم التقاط ونقل الصور. إن هذه الجرائم ليست محلاً للبحث في هذه الدراسة وكذلك المسائل المتعلقة بحرمة الحياة الخاصة أو أي تطبيقات لها خـارج نطـاق علاقتهـا بالحاسوب والتقنية الحديثة، وذلك لأن هذه المسائل كانت قد خضعت لبحث تفصيلي من قبـل الفقـه وكانت محل تنظيم قانوني في القوانين المدنية والجزائية لدى مختلف دول العالم، كمـا أنهـا كانـت محلاً لعشرات المؤلفات العربية والأجنبية.

الفرضيات:

تتجه بحوث جرائم الكمبيوتر والإنترنت للإجابة بشكل أساسي عن التساؤلات التالية: **أولاً:** هل تطال نصوص التجريم التقليدية في قانون العقوبات الأردني كالسرقة والاحتيـال وإسـاءة الأمانـة

والاختلاس وإتلاف المال والممتلكات وإفشاء الأسرار والتزوير واستعمال المزور والأفعال الجرميه في نظم الحواسيب والاستيلاء على الأرصدة المالية الإلكترونية والتقاط البيانات المالية وتحويلها وتدمير نظم الحواسيب والملفات الإلكترونية بتقنيات الفيروس والقنابل الموقوتة، والاستيلاء على البيانات وإساءة استخدامها والتغيير في البيانات المختزنة وتعطيل عمل الأنظمة ومواقع المعلوماتية. **ثانياً:** هل تطال النظريات العامة والنصوص الخاصة للقانون الجنائي ما شهدته أنماط الجريمة وبواعثها ومحلها من تحول من كيان مادي ملموس إلى مجرد صفة معنوية ذات قيمة قد تفوق المال المادي. **ثالثاً:** هل تحمي قوانين العقوبات المعلومات والبيانات ومعالجتها ونقلها وتبادلها؟ وما الذي تحتاجه من نصوص موضوعية كافية لمواجهة جرائم الكمبيوتر والإنترنت؟ **رابعاً:** ما هي الحلول القانونية والقضائية في القانون والقضاء المقارن لجرائم الكمبيوتر، وما هي المشاكل القانونية التي نجمت عن تطبيق القوانين الخاصة بإساءة استخدام الحاسوب، وكيف تصدى لها القضاء؟ وهذه التساؤلات هي التي ستشكل الموضوع الرئيس لهذه الدراسة.

المنهجية:

نقوم هذه الدراسة على المنهج التحليلي والتأصيلي للنصوص. كما ستعتمد هذه الدراسة بشكل أساسي على التشريع والقضاء الإنجليزي بغية الإفادة منها والوقوف على الحلول القانونية للمشاكل التي قد تظهر من تطبيق أية نصوص قانونية تجرم هذا النوع من الأنشطة، لهذا فإن هذه الدراسة ستلقي الضوء على الاجتهاد القضائي في القانون الانجليزي بسبب تعرضه في أكثر من مناسبة لتوضيح ما غمض من نصوص القانون. وسيتم تقسيم هذه الدراسة إلى ثلاثة مباحث على النحو التالي: يتناول المبحث الأول الجريمة المعلوماتية قبل صدور قانون إساءة استخدام الحاسوب الإنجليزي لعام ١٩٩٠. ويتناول المبحث الثاني جرائم المعلوماتية كما ورد النص عليها في التشريع الانجليزي. أما المبحث الثالث فإنه يتناول التطبيق القضائي لقانون إساءة استخدام الحاسوب وموقف الفقه منه، ثم الخاتمة وعرض أهم النتائج التي توصلت اليها الدراسة.

المبحث الأول:

لمحة تاريخية عن جرائم المعلوماتية في القانون الانجليزي

قبل صدور قانون إساءة استخدام الحاسوب الانجليزي(Computer Misuse Act ١٩٩٠)، كان القضاء البريطاني يستخدم القوانين السارية المفعول في ذلك الوقت من أجل إخضاع الصور المستحدثة من الجرائم الناشئة عن التطور التكنولوجي إلى أحكامها. ولذلك كان الاستعمال غير

المشروع لجهاز الحاسوب يعاقب عليه بموجب النصوص التقليدية للقانون الجنائي بطريقة وصـفت بأنها طريقة عشوائية وغير مرضية[١].

ومن أبرز التشريعات الانجليزية التي استخدمـت في هذا المجال قانون السـرقة لعـام ١٩٦٨ (The Theft Act ١٩٦٨) الذي يعتبر الاستيلاء على الكيان المادي للحاسوب جريمة سـرقة بـالمعنى المقصود في القانون. وقد ترتب على ذلك نتيجة مفادها أن الاستيلاء على المعلومات المخزنة فـي جهاز الحاسوب أو نسخها يقع خارج نطاق قانون السرقة لعام ١٩٦٨[٢]. ولذلك أصـبحت الحاجـة ملحة إلى إصدار قانون جديد يتعامل مع الأنماط المستحدثة من الجرائم التي يستخدم فيها الحاسـوب. ومما زاد الحاجة إلى إصدار مثل هذا التشريع الاعتقاد الخاطئ بأن الاستيلاء على المعلومات يمكـن أن يشكل جريمة وفق أحكام قانون السرقة الانجليزي. لقد استقرت أحكام القضاء الإنجليـزي إلـى عدم اعتبار الاستيلاء على المعلومات أو البرامج سرقة وذلك لأن السرقة لا تقع إلا على المـال ذي الطبيعة المادية وليس للمعلومات والبرامج والبيانات وكل الأشياء المعنوية ليس لهـا كيـان مـادي ملموس حتى لو كانت المعلومات سرية وذات قيمة عالية، بالإضافة إلـى أن هـذه الأشـياء تـأبى بطبيعتها الحيازة التي تتطلب أشياء ذات طبيعة مادية يمكن نقلها أو انتزاعها أو تحريكها من مكـان إلى آخر[٣]. ويشترط المشرع الإنجليزي في قانون السرقة لعام ١٩٦٨ (Theft Act ١٩٦٦) أن يقـع استيلاء على المال (Appropriation) وهذا يتطلب تبعاً لذلك شيئاً يمكن حيازته.

وهنالك العديد من الأحكام القضائية في بريطانيا أقرت بأن المعلومات لا تصلح محـلاً لجريمـة السرقة ومن ثمَ فأنه لا تنطبق عليها النصوص المتعلقة بجريمة السرقة. ونكتفي هنا بالإشـارة إلـى قضيه[٤] **Oxford v. Moss**؛ وتتلخص وقائع هذه القضية بقيام طالب يسمى (Moss) بالاستيلاء علـى النسخة الأولى المطبوعة من ورقة الامتحان الذي كان عليه أن يجريه في وقت لاحـق فـي كليـة الهندسة في جامعة ليفربول. وبعد حصوله على تلك النسخة قام بنقل الأسئلة الموجودة على النـسخة المذكورة قبل أن يتم إعادتها إلى مكانها. وعند اكتشاف فعلته ثار التساؤل عما إذا كان فعلـه يـشكل جريمة سرقة أم لا؟ في هذه القضية قررت محكمة صلح جزاء ليفربـول (Liverpool Magistrate) بالحكم بالبراءة مستندة في ذلك إلى عدم إمكانية اعتبار المعلومات أموالاً تـصلح أن تكـون محـلاً لجريمة السرقة، وقد تم تأييد هذا الحكم من قبل محكمة(Divisional Court) . ومن الجـدير بالـذكر

(1) Napier, B; "The Law Commission's Report on Computer Misuse, **Journal of Business Law**, 1989, 524.

(2)Gringras, C., To Be Great is To Be Misunderstood: The Computer Misuse Act 1990, *"Computer and Telecommunications Law Review*, 1997 3(5), 213–215.

(٣) كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دراسات جنائية معمقة في الفقه والقانون والقضاء المقارن، دار الثقافة، عمان، ٢٠٠٢، ص ٤٣ – ٤٤.

(4) (1979) Cr. APP. R 183 at 186.

أن موقف القضاء الإنجليزي يتطابق مع موقف محكمة التمييز الأردنية التي قضت في إحدى قراراتها بأن "مجرد الاطلاع على أسئلة الامتحانات وإفشائها لا يشكل سرقة مال بالمعنى القانوني"[١].

ويتبنى القضاء الإنجليزي عدم إمكان تطبيق النصوص الجزائية التقليدية على جريمة التزوير في معطيات الحاسوب. ففي قضية[٢] **R. v. Gold** قام المدعو Gold بالاشتراك مع شخص آخر يدعى (Schifreen) باختراق غير مرخص به لنظام حاسوب شركة (British Telecom) للهواتف، ونجحا في التوصل إلى قاعدة بيانات نظام (Prestel) العائد للشركة والحصول على خدمات دون مقابل. وقد تم توجيه تهمة اصطناع مستند لكل منهما بموجب قانون التزوير والتزييف لعام١٩٨١(Forgery and Counterfeiting Act 1981) والمتمثلة باستخدام الرقم السري وكلمة المرور العائدة لأحد المشتركين. وتم إدانتهما من محكمة (Crown Court) إلا إن محكمة الاستئناف أسقطت التهم الموجه إليهما وأعلنت براءتهما. وقد أيد مجلس اللوردات قرار محكمة الاستئناف ورفض تطبيق أحكام قانون التزوير والتزييف الإنجليزي الصادر عام ١٩٨١ على معطيات الكمبيوتر رغم تبني المشرع الجزائي الإنجليزي لمفهوم واسع لمعنى السند،[٣] مستندا في ذلك إلى حجة مفادها أن الإشارات والنبضات الالكترونية التي تكون كلمة السر لا يمكن اعتبارها "مستندا" بالمعنى القانوني "للمستند" الوارد في المادة الثامنة من القانون المشار إليه. كما أكد مجلس اللوردات على انه لا يمكن إخضاع وقائع الدعوى لتشريع لاينطبق عليها[٤].

لجأ القضاء الإنجليزي إلى تطبيق قانون (The Criminal Damage Act 1971) قبل صدور قانون إساءة استخدام الحاسوب عندما يتعلق الأمر بتدمير أو محو أو إلغاء البرامج والبيانات المخزنة في الحاسوب . إن المتتبع لقرارات القضاء الانجليزي يجد أمثلة على حالات يمكن من خلالها إعمال القواعد التقليدية في القانون الجزائي على حالات تدخل ضمن ما يسمى بالجرائم المعلوماتية. في قضية[٥] **Cox v. Riley**، التي تتلخص وقائعها بقيام المتهم بتعديل برامج الحاسوب المخزنة على قطعة بلاستكية والغائها مما أدى إلى جعل القطعة البلاستكية غير صالحة للاستعمال حيث إن البرنامج المخزن على القطعة البلاستكية كان يتضمن أوامر لمنشار ميكانيكي يقوم بصناعة أشكال معينة. قضت محكمة (Divisional Court) بإن وقائع الدعوى تقع تحت نص المادة الأولى من

(١) تمييز جزاء ٨١/٩٣، مجلة نقابة المحامين، تشرين أول ١٩٨١، ص ١٧٧٦.

(2) [1988] 2 WLR 984.

(٣) كامل السعيد، جرائم الكمبيوتر، مرجع سابق، ص ٢٠ – ٢٥.

(4) Gringras, C., To Be Great is To Be Misunderstood: The Computer Misuse Act 1990, **"Computer and Telecommunications Law Review,** 1997 3(5), 213.

(5) Cr. App. R. 540. 83) 1986

قانون (The Criminal Damage Act) التي تقضي باعتبارها جريمة معاقب عليها بموجب القانون المذكور قيام أي شخص بإتلاف أو تحطيم أي مال تعود ملكيته للغير بدون سبب مشروع. فقد جاء في حيثيات الحكم في معرض رد المحكمة على دفوع المشتكى عليه بأنه وعلى الرغم إن المادة العاشرة من القانون المذكور تعرف "المال" بأنه المال ذو الكيان المادي الملموس إلا إن نص المادة الأولى تطبق على وقائع هذه الدعوى على اعتبار أن البرنامج – وإن كان يعتبر مالا معنويا– إلا أن إلغاء البرنامج أدى إلى تلف البطاقة ذاتها. كما أن قرار المحكمة اعتبر أن كلمة الإتلاف (Damage) من الناحية اللغوية معناه "تجريد الشيء من قيمته أو منفعته". وقد أصبحت البطاقة عديمة الفائدة بعد أن تم إلغاء البرنامج المخزن فيها[1].

ومن الجدير بالذكر،أن قضية[2] **R v Whiteley** كانت آخر قضيه تتعلق بجرائم الحاسوب تم نظرها في ظل قانون (The Criminal Damage Act). فقد قضت محكمة الاستئناف البريطانية في هذه القضية، بعد فترة وجيزة من صدور قانون إساءة استخدام الحاسوب أن التعديل القصدي للمعلومات الموجودة في الحاسوب الذي أدى إلى تعطيل عدد من أنظمة المعلومات التي تم استخدام بعضاً منها في أبحاث طبية يعتبر جريمة معاقباً عليها وفق أحكام قانون (The Criminal Damage Act). لقد اعتبرت المحكمة أن إتلاف المعلومات المخزنة في الحاسوب يعتبر إتلافا جنائيا تماما كما لو وقع الإتلاف على الأموال المادية بالمعنى المقصود في قانون(The Criminal Damage Act) على الرغم من أن التغييرات في الجسيمات الممغنطة في جهاز الحاسوب لم يكن من السهل ملاحظتها. وتتلخص وقائع هذه القضية بقيام شاب يبلغ من العمر واحداً وعشرين عاما بالدخول إلى شبكة المعلومات الخاصة بإحدى الجامعات خلال الفترة الممتدة بين شهر آذار وتموز من عام ١٩٨٨، حيث قام بحذف عدد من الملفات المخزنة وأنشأ ملفات خاصة به، كما قام بإلغاء كافة الملفات التي من شأنها أن تسجل الأعمال التي قام بها. وقد ترتب على ذلك تعطيل النظام المعلوماتي لفترات مختلفة من الزمن. وقد تم إدانته بعشر تهم تتعلق بإتلاف الممتلكات خلافا لأحكام المادة الأولى من قانون (The Criminal Damage Act). جاء في حيثيات الحكم أن القانون يتطلب لقيام أركان الجريمة وعناصرها أن يقوم الفاعل بإتلاف مال ذي طبيعة مادية. ولكن القانون لا يتطلب أن يكون الإتلاف مادياً وملموساً. ولما كان من الثابت أن المشتكى عليه قام بتعديل الجسيمات الممغنطة التي تشكل جزءاً من الأشرطة الخاصة بالحاسوب من أجل تجريدها من قيمتها ومنفعتها، فإن ذلك يعتبر إتلافاً بالمعنى المقصود في القانون. كما قضت المحكمة أيضاً بأن كلمة

(1) Gringras, C., To Be Great is To Be Misunderstood: The Computer Misuse Act 1990, "**Computer and Telecommunications Law Review,** 1997 3(5), 213.

(2) [1993] FSR 168 (CA).

"الإتلاف" لاتقتصر على الإضرار المادي سواء حدث ذلك بصورة دائمة أو بصورة مؤقتة، بل يشمل أيضا تجريد المال من قيمته أو منفعته بصورة دائمة أو مؤقتة. وعليه فإن أي تعديل للطبيعة المادية للمال يعتبر "إتلافا" بالمعنى المقصود في القانون. ومن الجدير بالذكر أنه وبعد صدور قانون إساءة استعمال الحاسوب، فإن أي إتلاف للبيانات والمعلومات المخزنة في جهاز الحاسوب من شأنه أن يدخل ضمن نطاق نص المادة الثالثة[1].

أما جرائم الاحتيال التي تتم بواسطة الحاسوب، فهناك وفرة في النصوص القانونية التي تجرم بشكل صريح عدداً من الأنشطة غير المشروعة، ومن بينها تحويل الأموال بالطرق الالكترونية إذا تمت بالغش و الخداع. وعلى الرغم من أن النصوص المتعلقة بالاحتيال لا تطبق على الإستيلاء على الأموال التي تتم بواسطة الحاسوب باعتبار أن الاحتيال يمارس على الإنسان وليس على الآله، فإن ذلك لا يمنع من اعتبار أن الواقعة تشكل جريمة سرقة عملاً بأحكام قانون السرقة البريطاني لعام ١٩٦٨[2]. ونتيجة للاهتمام العالمي والمحلي في المملكة المتحدة حول مخاطر إساءة استخدام الحاسوب وعدم وجود نصوص جزائية تعاقب على هذه الأفعال، ظهرت الدعوات التي تنادي بتجريم الاستخدام غير المشروع للحاسب الآلي. ومن الأمثلة على هذه الدعوات الدعوة التي قامت بها منظمة التعاون الاقتصادي والتنمية التي طالبت بتجريم الدخول غير المصرح به للنظام المعلوماتي وذلك في دراسة نشرتها عام ١٩٨٦[3]. وكانت أول محاولة لتجريم إساءة استخدام الحاسوب في بريطانيا قد ظهرت عام ١٩٨٩ على يد أحد أعضاء مجلس العموم البريطاني السيدة (Emma Nicholson, MP)، إلا إن هذه المحاولة لم يكتب لها النجاح. وفي نهاية عام ١٩٨٩ نشرت هيئة قانونية متخصصة مشروع قانون يهدف إلى تجريم إساءة استخدام الحاسوب تم اعتماده من الحكومة البريطانية. وقد تضمن هذا المشروع النص على ثلاث جرائم هي: الدخول غير المصرح به للنظام المعلوماتي (Unauthorized Access to a Computer)، الدخول غير المصرح به بقصد ارتكاب جريمة أخرى (Hacking with intent to commit a serious crime)، تعديل أو تدمير برامج الحاسوب أو البيانات بصورة عمدية(Intentional destruction of or alteration to computer programs or data).

(1) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] **3 Web Journal of Current Legal Issues.**

(2) Smith, The Law of Theft, 6th edn 1989, para. 163.

(3) Computer Related Crime: Analysis of Legal Policy (Paris, 1986).

وقد تعرض هذا المشروع إلى عدة انتقادات نلخصها بما يلي[١] أن مشروع القانون لـم يـذهب بعيدا بما فيه الكفاية، حيث أن التصور الأساسي لأعضاء اللجنة القانونية التي تولت وضـع مـسودة مشروع القانون قام على مبدأ مفاده أن العقاب على إساءة استخدم الحاسوب يجب أن يكون الهـدف منه حماية سلامة النظام المعلوماتي من الدخول إليه من قبل أشخاص غير مخولين بذلك، ولم يكـن الهدف من التجريم هو حماية المعلومات ذاتها. هذا التوجه شكل خيبة أمـل للـذين كـانوا يـسعون لإصدار تشريع مبني على أساس حماية البيانات والمعلومات. كما فشل مشروع القانون بالتعامل مع بعض القضايا الهامة وعلى رأسها أنه لا يعاقب بشكل صريح على بعض الأفعال التي تشكل انتهاكـا لحق الإنسان في الحياة الخاصة منها استراق السمع بواسـطة اسـتخدام الحاسـوب (Electronic Eavesdropping). وهو أمر لم يكن مستغربا بالنظر إلى الغاية من وضع مشروع القانون.ذلـك أن استراق السمع وإن يكن تصرفا خطيرا إلا انه لا يلحق ضررا بسلامة النظـام المعلومـاتي، وإنمـا يهدف إلى الحصول على معلومات تصنف بأنها سرية. الانتقاد الثالث الذي تم توجيهه من قبل الفقـه إلى مشروع القانون يتأتى من وجهة نظر اللجنة بأنه لا يوجد حاجة ماسة لتعديل القواعـد الجزائيـة التقليدية. فبالرغم إن اللجنة قد قبلت بأن هنالك حاجة ماسة إلى تعديل القواعد الخاصة بالاختـصاص الجنائي وذلك لمواجهة جرائم الحاسوب على المـستوى الـدولي، إلا أنّ اللجنـة رفـضت تعـديل النصوص الجزائية التقليدية لمواجهة جرائم الاحتيال التي تتم بواسطة استخدام الحاسـوب متجاهلـة بذلك الثغرات التي تعاني منها النصوص التقليدية في القانون الجزائي. بالإضافة إلى ذلك لم يعـالج مشروع القانون مسألة على قدر كبير من الأهمية وهي مسألة إثبات جرائم الحاسوب وكيفية تعامـل القضاء مع الأدلة المتولدة من الحاسوب، فقد اكتفت اللجنة بالتأكيد على أنه ليس هنالك حاجة لتعـديل النصوص المتعلقة بالإثبات، كما أنه من الخطأ التركيز على قضية الإثبات فيمـا يتعلـق بالجريمـة الأولى (جريمة الدخول غير المصرح به للنظام المعلوماتي). فقد أوضحت اللجنة أن تجريم الـدخول غير المصرح به له قيمة رمزية فحسب لإظهار أن هذا السلوك غير مقبول دون التركيز على قضية أن هذه الجريمة ستلقى تطبيقا في الواقع العملي من عدمه. فإذا كان هذا التبرير يمكن قبولـه حيـال الجريمة الأولى فإنه لا ينسحب على الجرائم الأخرى من حيث إن القانون لن يؤدي وظيفته المتمثلـة بالردع إلا إذا تم تطبيقه بصورة فعالة. وقد رفضت اللجنة وضع تعريف للحاسوب بـدعوى أن أي تعريف له سيكون عملية معقدة وسرعان ما يصبح هذا التعريف غير مواكب للتطـورات الحديثـة. فبالرغم من وجاهة هذه الحجج إلا أن ذلك لن يمنع من قيام جدل حول بعض الأجهزة الحديثة التـي

(1) Napier, B; "The Law Commission's Report on Computer Misusc, **Journal of Business Law**, 1989, 526-527.

تستخدم في تخزين بعض المعلومات وتحتوي على بعض البرامج، وفيما إذا كانت تعتبر "حاسوباً" لأغراض تطبيق القانون مثل الأجهزة الهاتفية التي تحتوي على ذاكرة كالتي تستخدم في البنوك.(amemory-bank telephone) و (an electronic personal organizer) .

ورغم الانتقادات السابقة، فقد أعلن هذا المشروع عن ولادة قانون إساءة استخدام الحاسوب لعام ١٩٩٠ باعتباره خطوة في الاتجاه الصحيح وان التغيير في هذا المجال هو أمر محتّم لا مفر منه.

المبحث الثاني

قانون إساءة استخدام الحاسوب البريطاني لعام ١٩٩٠

صدر قانون إساءة استخدام الحاسوب البريطاني في عام ١٩٩٠ ودخل حيز التنفيذ في ١٩٩٠/٨/٢٩. كان الهدف من إصداره تحقيق غايتين رئيسيتين هما: (١) تجريم الاستخدام غير المشروع لجهاز الحاسوب من خلال خلق ثلاث جرائم مختلفة؛ (٢) تسهيل مهمة القضاء في التعامل مع هذه الجرائم دون حاجة إلى البحث عن الحلول باللجوء إلى قانون العقوبات التقليدي عن طريق تطويع نصوصه لمواجهة هذا النوع من الإجرام المستحدث. والجرائم التي استحدثها القانون سيتم مناقشتها بالتفصيل في ثلاثة مطالب على النحو التالي:

المطلب الأول:

جريمة الدخول غير المصرح به إلى النظام المعلوماتي

جرم المشرع الإنجليزي الدخول غير المصرح به للنظام المعلوماتي بموجب المادة الأولى[١] من قانون إساءة استخدام الحاسوب لعام ١٩٩٠[٢].تم صياغة نص هذه المادة بعناية فائقة، إذ تضمنت مسألتين هامتين: أولهما، أن الحاسوب قد يشكل المحيط الخارجي للجريمة، فالركن المعنوي في الجريمة يتطلب أن تنصرف إرادة الجاني نحو الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب. لهذا فإن هذا القانون يوفر الحماية الجزائية للجانب المعنوي للحاسوب. أما الجانب المادي للحاسوب فيتم حمايته من خلال قانون السرقة والتشريعات الأخرى ذات العلاقة. أما الأمر الثاني. أن النص المشار إليه لا يتطلب حتى تقوم الجريمة أن يستخدم الفاعل جهاز حاسوب واحداً؛ إذ تقوم الجريمة لو استخدم الفاعل جهاز حاسوب للولوج إلى البيانات والمعطيات المخزنة في جهاز آخر.

(1) Section (1) of the Computer Misuse Act provides that "(1) A person is guilty of an offence if: (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorized; and (c) he knows at the time when he causes the computer to perform the function that this is the case. (2) The intent a person has to have to commit the offence under this section need not be directed at: (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer. (3) A person guilty of an offence under this section shall on summary conviction be liable to imprisonment for a term not exceeding six months or to a fine not exceeding level five on the standard scale or to both".

(2) See, Peter Alldridge, "Computer Misuse Act 1990" **International Banking Law** 1990, (9)6, 339 – 342.

بالإضافة إلى ذلك فإن المادة المذكورة أعلاه لا تشترط حتى تتحقق الجريمة أن يتمكن الفاعـل مـن الدخول النظام المعلوماتي وذلك لأن الهدف من هذه المادة إخـضاع بعـض الأفعـال للنـصوص العقابية. مثال ذلك محاولة معرفة كلمة السر بهدف الدخول للنظام المعلوماتي عن طريـق اسـتخدام جهاز حاسوب متصل بجهاز (modem)، أو خط هاتفي أرضي. فمما لاشك فيه أن هذا النـوع مـن التصرفات يخضع لنص المادة الأولى من قانون إساءة استخدام الحاسوب والذي يهدف إلـى حمايـة سلامة النظام المعلوماتي؛ كما أن هذا السلوك يجعل الحاسوب يقوم بتنفيذ مهاماً معينة بهدف الولـوج للنظام المعلوماتي بالمعنى المقصود في المادة الأولى مما يجعل التصرف خاضعاً للنص العقابي[١].

تجرم المادة الأولى عدداً كبير من التصرفات والأفعال مثل: (١) نسخ البرامج وتوزيعها داخـل الشركة لاستخدامها من قبل موظفين آخرين خلافا لاتفاقية الرخصة الخاصة بالبرنامج؛ (٢) استخدام النسخ المقلدة من البرنامج بدون موافقة صاحب الرخصة؛ (٣) السماح باستخدام البرنامج المـرخص باستخدامه من قبل شركات أو أشخاص آخرين غير مرخص لهم باستخدامه خلافا لاتفاقية الرخـصة دون أن ينطوي ذلك على نسخ البرنامج؛ (٤) استخدام البرنامج لغاية أخرى غير الغاية المتفق عليها في اتفاقية الرخصة[٢].

وقد بينـت المـادة (٥/١٧) مـن القـانون مفهـوم عبـارة "الـدخول غيـر المـصرح بـه" (UnauthorizedAccess). إذ يتحقق ذلك عندما يكون الشخص المعني لا يملـك ابتـداءً الحـق فـي الدخول للبرامج والبيانات المخزنة، ولم يحصل على موافقة مـسبقة مـن أجـل الـدخول للنظـام المعلوماتي من الشخص الذي يملك السلطة بمنح هذه الموافقة. وبهذا يكون القانون البريطـاني قـد تجاوز مشكلة هامة تتعلق بتحديد مفهوم "الدخول غير المصرح به" الذي أحجمت بعض التـشريعات عن تعريفه مثل قانون (The Computer Fraud and Abuse Act) الأمريكي الـصادر عـام ١٩٨٤ والذي تم تعديله في عدة مناسبات[٣]. ومن الجدير بالذكر أن تعريف "الدخول غيـر المـصرح بـه" الوارد في المادة (٥/١٧) من قانون إساءة استخدام الحاسوب جاء مقصوراً علـى الـدخول علـى البيانات والبرامج المخزنة في جهاز الحاسوب. وعلى الرغم من القيود الواردة على التعريف، إلا أن جانبا من الفقه يرى أن التعريف يمتد ليشمل جميع أنواع الدخول إلى البرامج والبيانات المخزنـة[٤].

(1) See, Peter Alldridge, "Computer Misuse Act 1990" *International Banking Law* 1990,(9) 6, 339.

(2) E. Susan Singleton, "Computer Misuse Act 1990 – Recent Developments" 1993 **Company Lawyer** 14 (1), 22– 23.

(3) See Orin S. Kerr, "Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes', 78 **New York University Law Review** (2003), 1596.

(4) Mary W.S. Wong, "Cyber-Trespass and "Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience"15 **International Journals of Law and Information Technology** 2007, 90 at 119.

وهذا المنهج قد تبناه القضاء الانجليزي في قضية[1] (**R V. Bow Street Metropolitan Stipendiary Magistrate**)، إذ بيّن مجلس اللوردات مفهوم "الدخول غير المصرح به"، وهو ما سنتعرض له فيما بعد. إن قانون إساءة استخدام الحاسوب البريطاني لا يسمح بإقامة دعوى مدنية للتعويض عن الضرر ضد الفاعل. ويترتب على ذلك نتيجة مفادها أن أي تعريف من قبل القضاء المدني لعبارة "الدخول غير المصرح به" لن يؤثر على الكيفية التي سيطبق فيها هذا المفهوم على الدعاوى الجزائية من قبل القضاء الجزائي وذلك لأن المصالح المستهدفة بالحماية في القانون المدني قد تختلف بشكل أساسي عن المصالح التي يمكن حمايتها بموجب قواعد القانون الجزائي.

ويتحقق الركن المعنوي في الجريمة بمجرد أن يتوافر العلم لدى الفاعل بأن الدخول للنظام المعلوماتي غير مصرح به. ومن الجدير بالذكر أن القانون الإنجليزي لا يشترط لتحقق الركن المعنوي- على خلاف التشريعات الأخرى- أن يعلم الفاعل أن نشاطه الجرمي من شأنه أن يجعل الحاسوب يقوم بتنفيذ مهمة معينة[2].

وتجدر الإشارة هنا أن الدخول إلى النظام المعلوماتي بقصد مراقبة الاتصالات المرسلة عبر شبكة الاتصالات الخاصة خلافا للحالات التي نص عليها القانون وبغير تفويض من السلطة المختصة، يشكل جريمة معاقباً عليها بموجب المادة الأولى من قانون تنظيم السلطات التحقيقية الإنجليزي لعام ٢٠٠٠(Regulation of Investigatory Powers Act ٢٠٠٠). وكانت أول قضية نظرها القضاء الإنجليزي تتعلق بهذه الجريمة هي قضية[3] (**R v. Stanford (Clifford)**. وتتلخص وقائع هذه القضية بقيام شخص كان عضوا في مجلس إدارة إحدى الشركات ومساهما فيها بالطلب من موظف يعمل في الشركة بمراقبة البريد الالكتروني الخاص برئيس مجلس الإدارة وذلك بعد أن تم تزويده بالتفاصيل المتعلقة بكلمة المرور واسم المستخدم المتعلقة بالنظام المعلوماتي من قبل احد الأشخاص المصرح له بالتعامل مع النظام المعلوماتي حتي يتمكن ذلك الموظف من الدخول إلى النظام المعلوماتي ومراقبة الرسائل الالكترونية ونسخها. في هذه القضية أيدت محكمة الاستئناف البريطانية قرار محكمة الدرجة الأولى بإدانة المستأنف بجريمة مراقبة الاتصالات المرسلة عبر شبكة الاتصالات الخاصة بالشركة بعد استقالته من عضوية مجلس الإدارة تأسيساً على أن المستأنف لم يكن مخولا بالتحكم بالنظام المعلوماتي. وقد فسرت المحكمة كلمة تحكم (Control) الواردة في المادة الأولى بأنها القدرة على منح (Authorize) أو منع (Forbid) استخدام النظام المعلوماتي، وعليه فأن كلمة (تحكم) لا تقتصر على المعنى المادي المتمثل بالحق في الدخول إلى النظام المعلوماتي وتشغيله فقط[4].

---

(1) (1999) WLR 620 (H L).

(٢) راجع قانون إساءة استخدام الحاسوب السنغافوري لعام ١٩٩٣ والذي يتشابه إلى حد كبير مع نظيره الانجليزي.

(3) [2006] 1 WLR 1554.

(4) D.C. Ormerod, Case Comment: Interception of Communications: Meaning of "Control" of the Operation Use of A Private Telecommunications System, [2006] Criminal Law Review 1068-1071.

ومن الجدير بالذكر أن مراقبة الاتصالات لا تقتصر مخاطره على الخسائر المالية التي يمكن أن تلحق بالشركات والمؤسسات، بل تشكل خطرا أيضا على السلامة العامة. وتتم مراقبـــة الاتـــصالات باستخدام طرق مختلفة منها: تسجيل المكالمات الهاتفية، وزرع أجهزة التصنت، وتعقب الاتـــصالات ومراقبة الترددات.

وفي عام ٢٠٠٦ صدر قانون الشرطة والعدالة (The Police and Justice Act ٢٠٠٦) وقد تم بموجبه تعديل نص المادة الأولى من قانون إساءة استخدام الحاسوب وذلك بموجب المادة (٣٥) من قانون الشرطة والعدالة لعام ٢٠٠٦[١]. و جاء هذا التعديل استجابة إلى قرار الاتحاد الأوروبي فيما يتعلق بانتهاك أنظمة المعلومات الذي أعتمده من قبل مجلس وزراء الاتحاد الأوروبي الصادر بتاريخ ٢٠٠٥/٢/٢٤[٢]. ويهدف هذا القرار إلى تحقيق التقارب بين القوانين الجزائية للدول الأوروبية من حيث الجرائم والعقوبات والاختصاص. وعليه، فإن تعديل قانون إساءة استخدام الحاسوب جاء لتحقيق الانسجام مع القرار الصادر عن الاتحاد الأوروبي الذي ألزم كافة دول الاتحاد الأوروبي ضرورة العمل على تنفيذ مضمون القرار عن طريق تعديل التشريعات الوطنية ذات العلاقة قبل ٢٠٠٧/٢/٢٤ وذلك من أجل التأكد من وجود عقوبات كافية وفاعلة للمعاقبة على هذا النوع الخطير من السلوك الإجرامي. وأهم التعديلات التي أجريت على المادة الأولى هي:

١. إن المسئولية الجزائية تنهض في مواجهة الفاعل إذا تمكن من الدخول إلى النظام المعلوماتي بنفسه أو إذا مكن شخصاً آخر من الدخول إليه. إن هذا التعديل جاء منسجما مع الاجتهاد القضائي من جهة كما أنه وسع من نطاق التجريم على نحو يمكن القول بان القانون أصبح أكثر فاعلية في التعامل مع هذا النوع المستحدث من الإجرام.
٢. شدد المشرع العقوبة لتصبح الحبس لمدة لا تزيد عن سنتين بعد أن كانت العقوبة لا تتجاوز ستة أشهر.

---

(1) 35 Unauthorized access to computer material
- In the Computer Misuse Act 1990(c - 18) ("the 1990 Act"), section 1 (offence of unauthorized access to computer material) is amended as follows.
- In subsection —
(a) in paragraph (a), after "any computer" there is inserted ", or to enable any such access to be secured";
(b) in paragraph (b), after "secure" there is inserted ", or to enable to be secured,".
- For subsection - there is substituted—
"- A person guilty of an offence under this section shall be liable—
(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;
(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

(2) The European Union Framework Decision on Attacks Against Information Systems, adopted by the European Union and Justice and Home Office Affairs Council of Ministers on 24 February 2005.

٣. ترتب على زيادة العقوبة آثار قانونية بالغة الأهمية وهي:[١]

أ- يمكن ملاحقة الفاعل جزائيا عن الشروع في الجريمة.

ب-أصبح بالإمكان ترحيل فاعل الجريمة إلى دولة أخرى بناء على طلبها إذا ما توافرت الشروط المتطلبة للترحيل.

ج- أصبحت هذه الجريمة من الجرائم التي يجوز التوقيف فيها.

د- أصبح من السهل الحصول على إذن بأجراء التفتيش وفق الشروط التي نصت عليها قانون الشرطة والأدلة الجنائية (Police and Criminal Evidence Act ١٩٨٤). وبعبارة موجزة إن هذه التعديلات وما ترتب عليها من آثار جعل القانون أكثر انسجاما مع الاتفاقية الاوروبية الخاصة بالجريمة المعلوماتية لعام ٢٠٠١ (The Council of Europe Convention on Cybercrime).

إن الدخول أو البقاء غير المصرح به للنظام المعلوماتي بشكل ظاهرة ساهم في انتشارها تطور الاتصالات وتنامي شبكة المعلوماتية. ويستخدم الدخول غير المصرح به للنظام المعلوماتي في الغالب مرحلة سابقة وهامة لارتكاب جرائم أخرى، كسرقة المعلومات أو تزويرها، أو التجسس المعلوماتي، أو جريمة الاحتيال المعلوماتي أو الاعتداء على حرمة الحياة الخاصة، وغير ذلك من الجرائم[٢]. ورغم ذلك، فقد يهدف مرتكب الفعل الدخول إلى النظام المعلوماتي ذاته دون أن يقصد ارتكاب جريمة أخرى[٣].

ولذلك ثار خلاف فقهي حول إن كان هذا السلوك ينطبق عليه وصف الجريمة المعلوماتية ومن ثمّ إن كانت الحماية الجزائية هامة وضرورية؟ يرى جانب من الفقه بأنه لا يوجد حاجة ملحة لتجريم الدخول غير المصرح به إلى النظام المعلوماتي في الوقت الذي لم تتجه نية الجاني إلى ارتكاب جريمة أخرى.إذ لا يعدوالفعل من أن يكون عرضاً للقدرات الذهنية والعقلية التي يتمتع بها من قام بالفعل. بينما يرى الجانب الآخر من الفقه ضرورة تجريم الفعل حتى لو لم يقصد الجاني ارتكاب جريمة أخرى،[٤] ويعود ذلك إلى سببين:

أولاً: أن هذا السلوك يعد مرحلة أساسية لارتكاب جرائم معلوماتية أخرى.

---

(1) See: www.derekwyattmp.co.uk/news_item.aspx?!_PageID=113214.

(٢) نائلة قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، الطبعة الاولى٢٠٠٤، ص ٣٢٣.

(٣) نهلا المومني، ٢٠٠٥ الجريمة المعلوماتية في قانون العقوبات الاردني، جرائم الحاسوب والانترنت، رسالة ماجستير، الجامعة الأردنية. ص ١٢٤.

(٤) أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة،٢٠٠٠، ص: ٢٥٩؛ حجازي عبدالفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، الطبعة الأولى، القاهرة،،٢٠٠٢ ص ٢٩٥؛ عمرالفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية القاهرة، ١٩٩٥، ص: ١٢٢.

ثانياً: أن المعلومات التي تكون محلاً لهذا السلوك قد تكون على قدر كبير من الأهمية فيمـا يتعلـق بالمعلومات الخاصة بالأسرار العسكرية، والبيانات الخاصة بالعملاء في البنوك. وأن تـرك الجـاني دون عقاب يشجع غيره على الاعتداء على الأنظمة المعلوماتية.

ويقصد بالدخول جميع الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطـة أو الـسيطرة على المعطيات التي يتكون منها[١]. والدخول هنا يقصد به الدخول باستخدام الوسائل الفنية والتقنيـة إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني[٢]. ويستوي أن يكـون الـدخول قـد تـم بطريق مباشر إلى المعلومات أو أن يتم عن طريق الاعتراض غير المشروع لعمليات الاتـصال[٣]. والدخول إلى النظام المعلوماتي لا يشكل جريمة بحد ذاته إلا في الأحوال التي يكون الدخول قد تـم بدون وجه حق أو بصورة غير مصرح بها. ويكون الدخول غير مصرح به عنـدما يقـوم الفاعـل بالدخول إلى النظام المعلوماتي دون موافقة المسؤول عن النظام أو مالكه، أو عندما يكـون الفاعـل مصرحاً له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويـدخل إلـى كامـل النظام أو إلى أجزاء أخرى يحظر الدخول إليها. ويكون الدخول غير مصرحاً به أيضاً عندما يكون الدخول إلى النظام مسموحاً به شريطة وضع ثمن محدد إلا أن الفاعل يقوم بالدخول إلى النظام دون تسديد الثمن[٤]. وتعتبر جريمة الدخول المصرح به جريمة شكلية، إذ إن الركن المـادي فـي هـذه الجريمة يتحقق بمجرد الدخول بغض النظر إن ترتب على الدخول نتيجة أو لم يتحقق نتيجة[٥].

والسؤال الذي يدور في هذه الحالة يتعلق بمدى وجوب إضفاء الحماية الجزائيـة علـى الـنظم المعلوماتية في حال الدخول إليها بصورة غير مشروعة إذا كانت تلك الـنظم لا تحميهـا أي نظـم حماية؟ يرى جانب من الفقه أن هذا النوع من الأنظمة المعلوماتية ليست جديرة بالحماية الجزائيـة حتى لو حدث ولوج للنظام المعلوماتي دون تصريح بحجة أن القانون الجنائي لا ينبغـي أن يتـدخل لحماية الأشخاص الذين لا يأخذون الاحتياط اللازم، فالقانون الجنـائي لا يتـدخل لحمايـة الـنظم المعلوماتية التي تركت دون إجراءات أمنية تكفل لها الحماية اللازمة[٦].

---

(١) نائلة قورة، مرجع سابق، ص ٣٤٣.

(٢) نهلا المومني، مرجع سابق، ص ١٢٦.

(٣) نائلة قورة، مرجع سابق، ص ٣٢٥.

(٤) هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، الطبعة الأولى، ٢٠٠٣، دار النهضة العربية، القاهرة، ص: ٧٢ – ٧٣ .

(٥) جميل عبدالباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، القـاهرة، ١٩٩٢، ص: ١٥٠. والحسيني، مرجع سابق، ص١٢٨.

(٦) احمد حسام تمام، مرجع سابق، ص ٢٦٠.

ويرى اتجاه آخر من الفقه إلى ضرورة التدخل لحماية النظم المعلوماتية سواء أكانت هنالك تدابير حماية تحيط بها أم لم تكن لأن القول بغير ذلك يؤدي إلى نتيجة مفادها أن الحماية الجنائية ستكون مقتصرة على الأنظمة المحمية فقط دون الأنظمة المفتوحة للجمهور مثل الدليل الإلكتروني[١]. ويضيف أصحاب هذا الرأي حجة أخرى مفادها أنه لا ينبغي أن ينظر إلى الأنظمة الأمنية باعتبارها شرطاً لتجريم الدخول غير المصرح به إلى النظام المعلوماتي، وإنما يمكن النظر إليها باعتبارها قرينة على توافر القصد الجنائي[٢]. وأخيراً فإن جريمة الدخول غير المسموح به تعتبر من الجرائم الوقتية، من حيث أن هذه الجريمة تتحقق بمجرد فعل الدخول غير المصرح به[٣]. ويقصد بالبقاء غير المشروع داخل النظام المعلوماتي التواجد داخل النظام بالمخالفة لإرادة صاحب النظام أو من له السيطرة عليه[٤].

ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام المعلوماتي عن طريق الخطأ أو الصدفة إلا أنه يبقى داخله ولا يقطع الاتصال به[٥]. فالركن المادي لا يتمثل في إقامة الاتصال مع النظام لأن الاتصال بالنظام لا يقصده الجاني. ويمكن تصور قيام الركن المادي في هذه الجريمة عندما يقوم الشخص في سبيل الدخول إلى نظام معلوماتي له الحق في الدخول إليه ولكنه يجد نفسه داخل نظام آخر بسبب استخدام شيفرة خاطئة مثلاً، ومع ذلك يبقى هذا الشخص متصلاً بالنظام.

لقد ثار تساؤل في الفقه فيما إذا كانت جريمة الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون إذن يشكل تعدداً مادياً للجرائم أم أنه يشكل جريمة واحدة؟ يذهب جانب من الفقه إلى القول أننا أمام جريمة واحدة، نظراً لأن الفاعل أراد بالدخول غير المشروع البقاء داخل النظام المعلوماتي[٦]. ويرى جانب آخر من الفقه إلى أن ذلك يشكل تعدداً مادياً للجرائم[٧]. و حيث أنه لا يوجد نص في قانون العقوبات الأردني يجّرم هذا السلوك، وفلا بد للمشرع من التدخل لتجريمه بنص صريح. ومن الجدير بالذكر أن قانون سلطنة عُمان يعاقب بالسجن مدة لا تقل عن (٣) أشهر ولا تزيد على سنتين وبغرامه لا تقل عن (١٠٠) ريال إلى (٥٠٠) ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب الدخول غير المشروع إلى أنظمة الحاسوب. وقد أشارت المادة الثانية من اتفاقية بودابست لمكافحة الإجرام المعلوماتي إلى هذا النوع من السلوك الإجرامي

---

(١) جميل الصغير، مرجع سابق، ص: ١٥١.

(٢) نائلة قورة، مرجع سابق، ص ٣٧١؛ حجازي، مرجع سابق، ص:٢٤؛ قشقوش، مرجع سابق، ص ٣٥ .

(٣) نهلا المومني، المرجع السابق، ص ١٢٨ .

(٤) حجازي عبدالفتاح، الدليل الجنائي، مرجع سابق، ص ٢٣٥ .

(٥) نهلا المومني، مرجع سابق، ص ١٢٨ .

(٦) مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٥٢.

(٧) علي القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط١، الدار الجامعية للطباعة والنشر ١٩٩٩، ص ١٣٤.

حيث نصت على ما يلي: "يجب على كل طرف في الاتفاقية أن يتبنى الإجراءات التـشريعية أو أي إجراءات يرى أنها ضرورية من أجل اعتبار جريمة جنائية الولوج العمدي لكل أو لجزء من جهـاز الحاسوب بدون حق، كما يمكن أن تشترط التشريعات أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن"[١].

المطلب الثاني

جريمة الدخول غير المصرح به إلى النظام المعلوماتي بهدف ارتكاب جريمة أخرى

ورد النص على هذه الجريمة في المادة الثانية من قانون إساءة استخدام الحاسـوب البريطـاني لعام١٩٩٠[٢]. وتفرض هذه المادة عقوبة الحبس لمدة تصل إلى خمسة سنوات. وتعتبر هذه الجريمة من الجرائم المركبة التي لا تشترط ارتكاب الجريمة الأخرى التي تم الدخول إلى النظام المعلومـاتي من أجلها. ولذلك تعتبر هذه الجريمة أكثر خطورة من الجريمة المنصوص عليها في الفقرة الأولـى من القانون ذاته. وتشمل هذه المادة جميع الجرائم التي ورد النص عليها في التشريعات الجزائية مثل الاحتيال أو تلك الجرائم التي تعتبر من جرائم القانون العام. وغاية ما في الأمر أن تكون الجريمـة الأخرى من الجرائم التي يجوز التوقيف فيها سواءٌ أكانت جناية أو جنحة.

وقد أنتقد جانب من الفقه الصياغة التشريعية لهذه المادة باعتبار أن المشرع قد وسع من نطـاق قانون العقوبات في هذا النوع من الجرائم على نحو غير مبرر. إن فاعل الجريمة سيتعرض للعقوبة المنصوص في القانون سواء تمكن من ارتكاب الجريمة الأخـرى أم لـم يـتمكن. أي أن الجـاني سيلاحق جزائيا حتى لو لم يتمكن من ارتكاب الجريمة الأخرى لأي سبب من الأسباب، الأمر الـذي يشكل خروجا على حكم القواعد العامة التي تقضي بعدم العقاب على الأعمال التحضيرية من حيـث المبدأ[٣]. وتشدد المشرع الإنجليزي حيال مرتكبي هذا النوع من الجـرائم. وتتجلـى مظـاهر هـذا الموقف المتشدد في الأمرين التاليين:

---

(١) هلالي عبداللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، الطبعة الأولى، القاهرة، دار النهضة العربية، ص ٦٨.

(2) Section (2) of the Computer Misuse Act provides that " (1) A person is guilty of an offence(1) A person is guilty of an offence under this section if he commits an offence under s 1 above ("the unauthorized access offence") with intent:

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or another person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences:

(a) for which the penalty is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by s 33 of the Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorized access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible".

(3) Peter Alldridge, "Computer Misuse Act 1990", **International Banking Law** 1990,(9) 6, 340.

١. ان الفاعل يبقى عرضة للمسئولية الجزائية سواء ارتكب الجريمة الأخرى في الوقت ذاته الذي تمكن فيه من الدخول إلى النظام المعلوماتي، أو تمكن من ارتكابها في وقت آخر أو بمناسبة أخرى. وقد نص المشرع الجزائي الإنجليزي على ذلك صراحة في الفقرة الثالثة من المادة الثانية من القانون.

٢. أن المسؤولية الجزائية للفاعل لا تزول حتى ولو تبين من ظروف الدعوى أو ملابساتها أن ارتكاب الجريمة الأخرى أصبح مستحيلاً لسبب أو لآخر. وقد نص المشرع صراحة على ذلك في الفقرة الرابعة المادة ذاتها.

وقد أوردت اللجنة القانونية التي أوكل إليها مهمة وضع مشروع القانون مثالين على هذا الجريمة هما:

١. إذا تمكن شخص ما من الدخول إلى النظام المعلوماتي الخاص بأحد البنوك دون تصريح بقصد تحويل مبلغ من المال من حساب أحد الزبائن إلى حسابه الخاص. فإذا نجح في التعرف على كلمة السر وتمكن من تحويل الأموال فإنه يعتبر مرتكبا لجريمة السرقة، إلا أن السؤال الذي يبقى قائما: هل يعتبر هذا الشخص مرتكباً لجريمة الشروع في السرقة إذا لم يتمكن من معرفة كلمة السر رغم محاولة استخدام عدداً منها؟

٢. إذا تمكن شخص ما من الدخول إلى الحاسوب المملوك لشخص ما للحصول على معلومات شخصية وسرية بهدف استخدامها في ابتزازه. مما لاشك فيه أنه لن يلاحق على جريمة الشروع في جريمة الابتزاز لأنّ فعله في هذه المرحلة لا يعدو أن يكون عملاً تحضيرياً فحسب إلا أنه عرضة للمسؤولية الجزائية وفق أحكام المادة الثانية من القانون[1].

مما لا شك فيه إن كلا المثالين لم يقدما جواباً مقنعاً يسوّغ الخروج على حكم القواعد العامه التي لا تعاقب على الأعمال التحضيرية. إذا كان لا بد من الخروج على حكم القواعد العامة فإن ذلك يجب ألا يقتصر على الجرائم الخاصة بالحاسوب، بل يمكن أن يمتد إلى كل الجرائم بما في ذلك السرقة أو البحث في الملفات التي تتضمن معلومات خاصة بهدف الابتزاز سواء تمت حوسبتها أم لا، وهو أمر لا يمكن القبول به بسهولة وخاصة أن الأثر المترتب على ذلك هو توسيع نطاق قانون العقوبات على نحو كبير[2].

(1) Law Commission, LC No 186, paras 3.52–3.53.

(2) Peter Alldridge, "Computer Misuse Act 1990", *International Banking Law* 1990,(9) 6, 340.

المطلب الثالث

جريمة إتلاف المعلومات والبيانات

الإتلاف هو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الانتقاص من كفاءته للاستعمال المعد له[١]. إن جوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله[٢] أو تعطيله[٣]. وفعل الإتلاف في مجال المعلوماتية قد يقع على المكونات المادية للنظام المعلوماتي، وقد يقع على المكونات المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي. وفي الحالة الأولى يقع الإتلاف على المكونات المادية للنظام المعلوماتي كإتلاف شاشات العرض والأشرطة والاسطوانات والأقراص الممغنطة والكابلات وشبكات الربط ومعدات الإدخال والإخراج وغيرها[٤]. ويتحقق الركن المادي لإتلاف المال المعلوماتي (المادي) بإتلافه أو تخريبه أو تعطيله أو بجعله غير صالح للاستعمال[٥].

وفعل الإتلاف بهذا المعنى يخضع للنصوص التقليدية في قانون العقوبات التي تتناول تجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول المملوك للغير وذلك سنداً لنص المادة (٤٤٥) من قانون العقوبات الأردني. التي تنص على ما يلي: "كل من ألحق باختياره ضرراً بمال الغير المنقول، يعاقب بناءً على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامه لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين". وتثور في بعض الأحيان مسألة إتلاف بعض أوراق الحاسب الإلكتروني وشبكاته مما يؤثر على برامجه وبياناته أو على سير عمل النظام المعلوماتي.

وقد عالج المشرع الأردني – بشكل خاص – مسألة الإتلاف المادي الذي يقع على منشآت الاتصالات التي تشمل بالضرورة شبكة الإنترنت ومنشآتها المادية وذلك في قانون الاتصالات رقم (١٣) لسنة ١٩٩٥، إذ نصت المادة (٧٢) من هذا القانون على ما يلي:

"أ- كل من أقدم قصداً على تخريب منشآت الاتصالات أو ألحق بها ضرراً عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على ستتين أو بغرامه لا تقل عن (٢٠٠) دينار

---

(١) جميل الصغير، المرجع السابق، ص ١٥٣.

(٢) نهلا المومني، المرجع السابق، ص ٩٥ .

(٣) هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، ١٩٩٣، ص ٥٦٤ .

(٤) نهلا المومني، المرجع السابق، ص ٩٥ .

(٥) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة، عمان،٢٠٠٤، ص: ٢١٩ .

ولا تزيد على (٥٠٠٠) دينار أو بكلتا العقوبتين وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات.

ب – كل من تسبب إهمالاً في تخريب منشآت الاتصالات أو ألحق الضرر بها، يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على (١٠٠) دينار أو بكلتا هاتين العقوبتين".

وبذلك كفل المشرع حماية منشآت الاتصالات ومنها منشآت شبكة الإنترنت المادية من الاعتداء بإتلافها أو إلحاق الضرر بها، بالإضافة للحماية التي كفلها للأموال المعنوية من الإتلاف في المواد (٧٦، ٧٧، ٨٠) من ذات القانون[١]. أما فيما يتعلق بالحالة الثانية وهي حالة وقوع الإتلاف على المعلومات المختزنة في جهاز الحاسوب أو المتبادلة عبر الشبكات المحلية أو العالمية، فالتساؤل قائم حول الحماية التي وفرها المشرع الأردني في قانون العقوبات لهذه الحالة.

فقد ذهب أغلب الفقه[٢] – بحق – الى القول إن جريمة الإتلاف لا تقع إلا على الأموال المادية فقط دون المعنوية، مما ينأى بالقول عن حماية النص للأموال المعنوية، فالمشرع قيّد النص على الأموال المنقولة بضرورة أن تكون مادية. ويذهب البعض الآخر الى أن المعلومات والبرامج يمكن أن تكون محلاً لجريمة الإتلاف ذلك أن المشرع قد نص على أن محل الجريمة هي الأموال المنقولة، وهي لا تقتصر على الأموال المادية، مما يعني أنها تنطبق على الأموال المنقولة المادية والمعنوية، فالنص جاء بعبارات عامة بصدد المنقول، والقول بغير ذلك يترتب عليه أن تكون المعلومات مجردة من أية حماية جنائية الأمر الذي يفتح المجال على مصراعيه للاعتداء عليها[٣].

ونحن بدورنا نؤيد الاتجاه القائل بعدم انطباق النص التقليدي المتعلق بجريمة الإتلاف على إتلاف المعلومات وذلك أن المعلومات المبرمجة آلياً بمثابة نبضات كهربائية تفتقر إلى الطبيعة المادية. فالمشرع بتجريمه فعل الإتلاف يحمي حق الملكية، سواء الملكية العقارية أو المنقولة. ويتحقق ذلك عن طريق حماية موضوعه من الأفعال التي تفني مادته أو قيمته في صورة كلية أو جزئية، فتقضي بذلك على منفعة الشيء. وينعين أن يكون لذلك الشيء طبيعة مادية. وعلى الرغم من أن الشارع لم يصرح بهذا الشرط فهو مستخلصٌ من وقوع هذه الجريمة على حق الملكية وهذا الحق لا ينصب إلا على أشياء ذات كيان مادي[٤].

---

(١) محمد الشوابكة، المرجع السابق، ص: ٢١٩.

(٢) جميل عبدالباقي الصغير، المرجع السابق، ص ١٥٦؛ هدى قشقوش، المرجع السابق، ص ٥٦٥؛ نائلة قورة، مرجع سابق، ص ١٩٤.

(٣) علي القهوجي، المرجع السابق، ص ١١١؛ أسامة المناعسة وآخرون، جرائم الحاسب الآلي والانترنت، الطبعة الأولى، عمان، دار وائل للنشر، ص: ١٥٦؛ عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى، بدون ناشر، ٢٠٠٠، ص: ١٨٨.

(٤) محمود نجيب حسني، ١٩٦٩، جرائم الاعتداء على الأموال، الطبعة الأولى، بدون ناشر، ص ٤٨٧، ٤٨٨ .

يضاف إلى ذلك أن التفسير الواسع للنصوص الجنائية أو الاجتهاد أو القياس عليها يخـرج بهـا عن قاعدة الشرعية. فبالرغم من أهمية حماية المعلومات من أفعال الإتلاف والتخريب إلا أن الحـل لا يكون في التوسع في تفسير النصوص التقليدية، بل يستلزم توفير حماية للمعلوماتية عـن طريـق نصوص تشريعية تراعي خصوصية المعلومات التي تختلف عن الأموال الماديـة الملموسـة التـي وضعت نصوص قانون العقوبات ابتداءً لحمايتها. وتراعي مبدأ التفسير الضيق لنـصوص القـانون الجنائي بما يتفق مع التطور التكنولوجي في حقول المعلوماتية[١].

وتجدر الإشارة إلى أن المشرع الأردني في قانون الاتصالات رقم (١٣) لسنة ١٩٩٥ كفل نوعاً من الحمـاية للمعلومات والبيانات المتبادلة عبر شبكات الاتصال من خطر الإتـلاف. فقـد نـصت المادة (٧٦) من القانون المذكور على ما يلي: "كل مـن اعتـرض أو أعـاق أو حـوّر أو شـطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر، وبغرامة لا تزيد على (٢٠٠) دينار أو بكلتا العقوبتين".

كما نصت المادة (٧٧) على أن "كل من أقدم على كتم رسالة عليـه نقلهـا بواسـطة شـبكات الاتصال إلى شخص أو رفض نقل رسائل طلب منه نقلها سواء من قبل المرخص لـه أو الهيئـة أو نسخ أو أفشى أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غيـر المعلنـة والرسائل المرسلة أو المستقبلة، يعاقب بالحبس لمدة لا تزيد على ستة أشهر أو بغرامة لا تزيد علـى ألف دينار أو كلتا العقوبتين". كما نصت المادة (٨٠) من قانون الاتصالات الأردني على مـا يلـي: "كل من قام متعمداً باعتراض موجات مخصصة للغير أو بالتشويش عليهـا أو باسـتخدام موجـات كهرومغناطيسية بـدون ترخيص يعاقـب بالحبس مدة لا تـزيد على ستة أشهر أو بغرامه لا تقـل عن (٥٠) دينار ولا تزيد على (٢٠٠) دينار أو بكلتا هاتين العقوبتين".

إن النصوص الواردة في قانون الاتصالات تنطبق على شبكة الاتصالات العامة (الإنترنـت) أو شبكات الاتصالات الداخلية. فالنص يشمل أي إعاقة وتعطيل لحركة الاتصالات سواء كان بالدخول إلى نظم المعلوماتية أو بالتأثير عليها وتشويشها دون الولوج إلى النظام المعلوماتي نفسه. ومما يجدر ذكره أن بعض الدول وخاصة المتقدمة منها في مجال التعامل مع المعلوماتية قد وضعت نـصوصاً صريحة تجرم الأفعال التي تستهدف إتلاف المعلومات ومن هذه الدول فرنسا والولايـات المتحـدة الأمريكية وكندا[٢]. وأهم ما يميز هذه النصوص التي جرمت إتلاف المعلومات أنهـا تخلّـت عـن

---

(١) محمد الشوابكة، المرجع السابق، ص ٢٢١ ؛ نهلا المومني، المرجع السابق، ص ١٠٩ .

(٢) نائلة قورة، مرجع سابق، ص: ٢٠٩.

اشتراط صفة المنقول أو العقار في المال الواقع عليه فعل الإتلاف واكتفت بتوافر الصفة المادية للشيء الواقع عليه فعل الإتلاف[١].

إن صورة إتلاف المال المعلوماتي المعنوي عبر شبكة الإنترنت تتمثل بالاعتداء على سير نظام المعالجة الآلية للبيانات بمختلف التصرفات التدليسية المتمثلة بالدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه، وبما يترتب من إتلاف للبيانات والبرامج أو بما يؤدي إليه من تعطيل أو إفساد نظام التشغيل[٢].وتتعدد صور الاعتداء على النظام المعلوماتي عن طريق إعاقة سير العمل في نظام المعالجة الآلية للبيانات والاعتداء على البيانات الموجودة داخل نظام المعالجة الآلية للبيانات[٣]. ويمكن رد الاعتداء على البيانات والبرامج داخل النظام المعلوماتي بإتلافها إلى صورتين: أولاً: أن يتم محو البيانات والمعلومات كليا أو تدميرها إلكترونياً، ثانياً: أن يتم تشويه المعلومات أو البرامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل انتقالها[٤].

وتتنوع أساليب الإتلاف التي قد تكون نتيجة فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون إذن أو قد تكون نتيجة استخدام الطرق التقنية والفنية كاستخدام فيروسات الحاسب الآلي. والاعتداء على البيانات والبرامج داخل نظام المعالجة الآلية لبيانات متنوعة بحسب ما إذا اتخذت صورة التدخل في المعطيات أو اتخذت صور التدخل في الكيان المنطقي. فالتدخل في المعطيات يكون عن طريق إدخال معلومات وهمية في النظام المعلوماتي أو بتزوير المعطيات الموجودة. أما التدخل في الكيان المنطقي فإنه يكون بتعديل البرنامج أو بخلق برنامج جديد[٥].

أما الطرق الفنية والتقنية المستخدمة لإتلاف البيانات والبرامج فهي متنوعة تشمل استخدام الفيروسات (Programs Virus) وبرنامج الدودة، (Worms) واستخدام القنبلة المنطقية أو الزمنية (Logic Bomb). ويمكن تعريف الفيروسات بأنها "برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكن أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم، وهو يسمى عادة باسم أول مكان اكتشف فيه، والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً

---

(١) الحسيني، عمر الفاروق الحسيني، مرجع سابق، ص: ٧٥.

(٢) محمد الشوابكة، المرجع السابق، ص ٢٢٢ .

(٣) وهذا ما فعله المشرع الفرنسي في قانون العقوبات لعام ١٩٩٢ بموجب المواد من (٣٢٢/١ - ٣٢٢/١٤)، المرجع السابق، ص ٢٢٢.

(٤) هدى حامد قشقوش، المرجع السابق، ص: ٥٦٧.

(٥) محمد الشوابكة، المرجع السابق، ص: ٢٢٩ – ٢٣٧.

يدل عليها، وعلى الرغم من تدميرها للبرامج والمعلومات إلا أنها لا تسبب عادة تـدميراً لأي مـن المكونات المادية للنظام[١].

وتتمتع الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسوب والـشبكات المعلوماتيـة وتعطـل الاتصالات وتشوه البيانات، بل وتضلل المستخدم أحياناً ببيانات خاطئة، فالفيروس قـد يـؤدي إلـى تغيير في الحقيقة أو تعديل المعلومات[٢]. وتستخدم الفيروسات بشكل عام لتحقيـق غـرض دفـاعي وذلك لحماية النسخة الأصلية من خطر النسخ غير المـرخص بـه أو تـستخدم لغـرض تخريبـي للحصول على منافع شخصية[٣]. أما الدودة فإنها برامج تكون مصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر، وهو ما يؤدي إلى عجز النظام المعلوماتي عن أداء عمله عن طريق محو عـدة أجزاء من المعلومات، وهذه الوسيلة تؤدي إلى تعطيل النظام المعلوماتي وإيقافه بصورة كاملة. فهـذا الفيروس ينسخ نفسه عدة مرات. وتنتشر الدودة عبر خطوط التوصلة الإلكترونية وتصدر معلومـات غير صحيحة تؤدي في النهاية إلى إغلاق النظام[٤]. أما القنابل المنطقية أو الزمنيـة فإنهـا تـسمى القنبلة المعلوماتية. ويمكن تعريف القنابل المنطقية بأنها "برنامج أو جزء من برنامج، ينفذ في لحظـة محددة أو في كل فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالـة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع"[٥]. فالقنابل المنطقية تهدف إلى تدمير بـرامج ومعلومات النظام وتغييرها في محطة محددة أو في فترة زمنية منتظمة، وهي تعمـل علـى مبـدأ التوقيت. أما القنابل الزمنية فهي عبارة عن برنامج يتم إدخاله بطرق مشروعة متخفية مـع بـرامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام أو تغييرها، وتعمل على مبـدأ التوقيـت حيـث تنفجر في وقت معين[٦]. جرم المشرع الجزائي الإنجليزي هذا الفعل بصريح نص المادة الثالثة مـن

---

(١) نائلة قورة، مرجع سابق، ص: ١٩١- ١٩٢؛ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٩٨، ص: ١٨٩.

(٢) نهلا المومني، المرجع السابق، ص ٩٨.

(٣) محمد حسام لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة في الفترة من ٢٥- ٢٨، أكتوبر ١٩٩٣، ص: ٤٩٦.

(٤) هدى حامد قشقوش، مرجع سابق، ص ١٢٣.

(٥) سامي الشوا، مرجع سابق، ص ١٩٤.

(٦) عوض، اسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان: "الجرائم الواقعة في مجال تكنولوجيا المعلومات" المنعقد بالقاهرة ما بـين ٢٥ – ١٩٩٣/١٠/٢٨، دار النهضة العربية، ص ٤٢٧.

قانون إساءة استخدام الكمبيوتر[1] التي تعاقب على إتلاف عمل الحاسوب أو إعاقة الدخول إلى أي بيانات موضوعه في أي كمبيوتر، أو إتلاف عمل أي برنامج أو تؤثر في صحة أي بيانات أو تعديل أو تحوير غير مصرح به لمعطيات الحاسوب بقصد إضعاف أو تعطيل النظام المعلوماتي.

لقد اختارت اللجنة القانونية المكلفة بوضع مشروع قانون إساءة استخدام الحاسوب أعتبار هذا الفعل جريمة قائمة بذاتها بدلاً من الاعتماد على قانون The Criminal Damage Act ١٩٧١ وذلك للأسباب التالية:

١. أن القانون المذكور لا يطبق إلا على الأموال المادية دون المعنوية.
٢. أن من الصعوبة تقدير قيمة المال المعنوي الذي تم إتلافه ومن ثمّ فان ذلك سيخلق مشكلة حقيقية في تحديد المحكمة المختصة قيمياً بنظر الدعوى.
٣. أن الجريمة المنصوص عليها في المادة الثالثة تطبق فقط في حالة الإتلاف القصدي أو العمدي للمال المعلوماتي، ويمكن تطبيق قانون الإتلاف الجنائي لعام ١٩٧١ المشار إليه أعلاه إذا كان الإتلاف ناشئاً عن الإهمال أو عدم الاحتراز[2].

جرمت المادة الثالثة من قانون إساءة استخدام الحاسوب تعديل البيانات الموجودة داخل النظام المعلوماتي دون تصريح بذلك بهدف تعطيل أو إتلاف العمليات التي يقوم بتنفيذها الحاسوب، أو بهدف منع أو إعاقة الدخول إلى أي برنامج أو بيانات مخزنة في الحاسوب، أو من اجل إتلاف أو تعطيل عمل أي برنامج، أو التأثير في مصداقية المعلومات المخزنة في الحاسوب. وتتحقق أركان هذه الجريمة وعناصرها بتعديل البيانات المخزنة في أي جهاز حاسوب بغض النظر عن نوعه

(1) Section (٣) of the Computer misuse Act 1990 provides that "(1) A person is guilty of an offence if:
(a) he does any act which causes an unauthorised modification of the contents of any computer; and
(b) at any time when he does the act he has the requisite intent and the requisite knowledge.
(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing:
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer; or
(c) to impair the operation of any such program or the reliability of any such data.
(3) The intent need not be directed at:
(a) any particular computer;
(b) any particular program or data or a program or data of any particular kind; or
(c) any particular modification or a modification of any particular kind.
(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorized.
(5) It is immaterial for the purposes of this section whether an unauthorized modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.
(6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition".
(2) Law Commission, LC No. 186, para. 3.63.

ونوع البيانات والمعلومات والبرامج التي تم تعديلها أياً كانت طبيعـة التعـديل وفحـواه . كمـا أن المسئولية الجزائية تنهض في مواجهة مرتكب هذه الجريمة سواء كان التعديل الذي تم إحداثـه فـي البيانات أو البرامج المخزنة دائمة أو مؤقتة. فقد أكدت المادة الثالثة على أن تعديل البيانات والبرامج المخزنة بأي طريقة كانت لا يعتبر بالمعنى المقصود في قـانون ١٩٧١ The Criminal Damage Act ما لم يتضمن التعديل إتلافا للكيان المادي للنظام المعلوماتي. ويترتب على ذلـك نتيجـة مفادهـا أن قانون عام ١٩٧١ سيطبق على الحالات التي يكون فيها التعديل في البيانات والبرامج منطويا علـى إتلاف الكيان المادي للحاسوب. ومن الجدير بالذكر أن المادة (١٧) من قـانون إسـاءة اسـتخدام الحاسوب بينت أن المادة الثالثة تشمل نطاقا واسعا من الأنشطة المجرمة نحو الأعمال التي تنطـوي على تعديل البيانات والبرامج المخزنة وحذفها بصورة عمدية طالما كانت الغاية تعطيل عمل النظـام المعلوماتي أو إعاقة أو منع الدخول إلى النظام المعلوماتي من قبل الشخص المـصرح لـه بـذلك. ويجب أن يؤدي التعديل إلى واحدة من النتائج التالية:

١. تعطيل عمل الحاسوب.
٢. إعاقة أو منع الدخول إلى البرامج والبيانات المخزنة في الحاسوب.
٣. تعطيل عمل البرامج أو التأثير في مصداقية البيانات المخزنة.

وقد عرفت المادة (٧/١٧) من القانون ذاته معنى كلمة "تعديل" (modification) بأنـه أي تغييـر أو إلغاء أي برنامج أو بيانات أو إضافة برامج أو بيانات إلى محتوى الحاسب الآلي. وهذا التعريف يشمل استخدام الفيروسات بشكل عام، وفيروس حصان طروادة و القنابل الزمنية والمنطقيـة. وأول حالة استخدم فيها فيروس (حصان طروادة) في المملكة المتحدة كانت قبل صـدور قـانون إسـاءة استخدام الحاسوب. ففي نهاية عام ١٩٨٨ تم توقيف شخص يـدعى الـدكتور (Popp) مـن ولايـة (أوهايو) الأمريكية من قبل مكتب التحقيقات الفدرالي الأمريكي بالتعاون مع الـشرطة البريطانيـة ويبلغ من العمر تسعة وثلاثين عاما بتهمة الشروع في ابتزاز الآلاف من مستخدمي الحاسـوب فـي مختلف دول العالم، إذ قام بإرسال أشرطة حاسوب مزيفة إلى ما يقارب عشرين ألف شـخص فـي بريطانيا وعدد من دول العالم تتضمن برنامجاً لمساعدة المـستخدمين لتفـادي الإصـابة بمـرض (الإيدز). ولم تكن تلك الأشرطة في الحقيقة إلا عبارة عن فايروس (حصان طروادة)، وقد تم برمجة الفيروس على أن يعمل بعد أن يتم استخدام الحاسوب أكثر من مائة مرة. تسلّم مستخدمو الحواسـيب رسالة تحذيرية مفادها بأن الحاسوب سيتوقف عن العمل إذا لم يتم دفع مبلغ ومقداره (٢٢٥) جنيهـاً إسترلينياً إلى حساب معين في أحد البنوك في بنما. وبعد القبض على الفاعل تم ترحيله إلى المملكـة المتحدة لمحاكمته عن جرائمه إلا أن المحاكمة لم تنعقد بسبب أن محامي الدفاع قدموا للادعاء العـام ما يثبت بأن المشتكى عليه يعاني من اضطرابات عقلية تجعله غير لائق من الناحية الصحية للمثـول

أمام المحكمة. وإنه لمن المؤكد بأن الدكتور (Popp) كان سيحاكم وفق أحكام المادة الثالثة من القانون فيما لو قدّم للمحاكمة[1].

إن من أهم العقبات القانونية التي تعترض معاقبة مرتكبي هذه الجرائم في ظل قواعد القانون البريطاني تتعلق بمدى قبول الدليل المتحصل من أجهزة الحاسوب وفقا لإحكام المادة (٦٩) من قانون الشرطة والأدلة الجنائية لعام ١٩٨٤ وتعديلاته (Police and Criminal Evidence Act). إذ يتطلب هذا النوع من القضايا إثبات أن جهاز الحاسوب كان يعمل بصورة عادية قبل إتلاف البيانات المخزنة فيه، وهو أمر يصعب إقامة الدليل عليه في كثير من القضايا وذلك لأن مرتكبي هذه الجرائم يعمدون إلى تدمير القرص الصلب الخاص بجهاز الحاسوب و إلغاء الملفات التي يحتويها من خلال زرع الفيروسات[2].

وقد تم تعديل المادة الثالثة من قانون إساءة استخدام الحاسوب بموجب المادة (٣٦) من قانون (Police and Justice Act 2006). ومن أهم التعديلات التي نص عليها القانون الجديد زيادة العقوبة لتصبح السجن لمدة عشر سنوات بدلا من خمس سنوات، وأصبحت عقوبة الغرامة غير محددة. إن الهدف من التعديل هو التعامل مع ما يسمى (Denial of Service attacks) أو أنشطة منع أو حجب الخدمة كخدمة الانترنت مثلا من خلال زيادة حمولة النظام المعلوماتي ومنع المستخدم من استعمال الخدمة عن طريق إرسال عدد كبير من الرسائل الالكترونية. وبعبارة أخرى فإن هذا يعني وقف النظام المعلوماتي ومنعه من أنجاز مهامه بصورة متعمدة. إن تعديل نص المادة الثالثة جاء بهدف تحقيق الانسجام بين قانون إساءة استخدام الحاسوب وبين المادة الخامسة من الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية، والمادة الثالثة من قرار الاتحاد الأوروبي المتعلق بأنشطة الاعتداء على أنظمة المعلومات. إنّ كل هذه النصوص تتطلب تجريم إعاقة عمل الحاسوب بصورة قصدية من خلال إدخال، ونقل، وتدمير، وتعديل، وإتلاف، وإلغاء البيانات ومنع الدخول إليها. إن إعاقة عمل الحاسوب يمتد ليشمل استخدام البرامج التي من شأنها حجب الخدمة عن المستخدمين، وزرع البرامج الضارة بأنظمة المعلومات كالفيروسات. وعليه فقد أصبحت أنشطة إعاقة عمل النظام المعلوماتي وحجب الخدمة جريمة يعاقب عليها بموجب التعديل.

---

(1) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] **3 Web Journal of Current Legal Issues.**

(2) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] 3 Web *Journal of Current Legal Issues.*

وعلى الرغم من أن التعديلات الآنفة الذكر تعتبر قفزة في الاتجاه الـصحيح إلا أنهـا أثـارت المخاوف من أن التعديلات ستجرّم استعمال بعض برامج الحماية. فالقانون الجديد قد جرّم تزويـد أو تقديم عرض لتزويد أي مواد من شأنها أن تستخدم في المساعدة فـي ارتكـاب جـرائم الحاسـوب المنصوص عليها في قانون إساءة استخدام الحاسوب وذلك بموجب المادة (3A) التي تـم إضـافتها بموجب المادة (٣٧) من قانـون (Police and Justice Act 2006). فقد عرفت الفقرة الرابعـة مـن المادة ذاتها كلمة مادة (Article) "بأنها أي برنامج أو بينات وضعت في شكل الكتروني". إنّ بعـض برامج الحاسوب التي يستخدمها المشتغلون في حقول المعلوماتية قد تـستخدم لإحـداث كثيـر مـن الأضرار رغم أنها أنشئت لغاية معاكسة تماما. فعلى سبيل المثال، يـستخدم المختـصون برنـامج (nmap) في أنظمة الحماية لفحص الشبكة المعلوماتية الخاصة بالنظام المعلوماتي لمعرفـة فيمـا إن كانت آمنة أو لا، إلا أن ذات البرنامج نفسه قد يستخدمه قراصنة الحاسوب للبحث عن أي ثغـرات في النظام المعلوماتي تمهيدا لمهاجمته أو اختراقه. وهنالك مخاوف أخرى من هذا التعديل تتمثل فـي إمكانية مد أحكام القانون المعدل ليجرم التحذيرات التي يتم إطلاقها بخصوص وجود عيوب في نظام الحماية التي قد يستخدمها قراصنة الحاسوب لاختراق النظام المعلوماتي. فالقانون المعدل لم يعـالج مسألة الاستخدام المزدوج للبرامج (Dual Use) التي تستخدم لأغراض قانونية وفـي الوقـت نفـسه يمكن أن تستخدم لأغراض ضارة مثل برامج تصفح الانترنت[1].

المبحث الثالث

موقف القضاء والفقه من قانون إساءة استخدام الحاسوب

منذ صـدور قانون إسـاءة استخدام الكمبيـوتر الإنجلـيزي لعـام ١٩٩٠، صار محلاً لعـدد من القرارات القضائية التي أزالت مـن الغموض ما شـاب بعـض نـصوصه. ففـي قـضية[2] (Attorney General' Reference . No.1 of 1991) كانت المادة الأولى من القانون محـلاً للبحـث. وتتلخص وقائع هذه القضية بقيام شخص يدعى (Cropp) باستخدام جهاز الحاسوب التـابع لرئيـسه السابق فأعطى لنفسه خصماً مقداره (٣٠%) من قيمة المشتريات التي كان قد اشـتراها مـن محـل رئيسه التجاري. وعند اكتشاف الأمر كان السؤال المطروح أمام محكمة الدرجة الأولى فيما إذا كان فعل السيد (Cropp) يشكل الجريمة المنصوص عليها في المادة الأولى من قانون إسـاءة اسـتخدام الحاسوب. لقد كان إجابة محكمة الدرجة الأولى على هذا التساؤل بالنفي وأن فعل السيد (Cropp) لا يشكل جريمة يعاقب عليها القانون المشار إليه بدعوى أن هذه الجريمـة لا تتحقـق إلا فـي حالـة

(1) See: www.theregister.co.uk/2006/11/22/cma_cpild_ban_security_tools/print.html.

(2) (1992) 3 WLR 432 (CA).

استخدام جهاز حاسوب للدخول إلى النظام المعلوماتي الموجود في جهاز حاسوب آخر وهو الأمر الذي لم يتحقق في هذه القضية، ذلك أن السيد (Cropp) قد استخدم جهازاً واحداً فقط. لقد ترتب على هذا الحكم نتيجة هامة مفادها أن الأشخاص المصرح لهم باستخدام النظام المعلوماتي لا يمكن لهم ارتكاب الجريمة المنصوص عليها في المادة الأولى من قانون عام ١٩٩٠ إلا في حالة واحدة فقط وهي استخدام جهاز حاسوب للدخول إلى النظام المعلوماتي لجهاز حاسوب آخر[١].

كان لهذا القرار القضائي صدى واسع في الأوساط القانونية التي رأت إن الحكم قد اضعف من فاعلية القانون في تحقيق الغاية من إصداره وهي حماية "سلامة النظام المعلوماتي"[٢] خاصة وان معظم مرتكبي جرائم الحاسوب هم من الأشخاص المصرح لهم باستخدام النظام المعلوماتي[٣]. و قد طعنت النيابة العامة في القرار القضائي السابق أمام محكمة الاستئناف الإنجليزية (The Appeal Court) التي قررت فسخ قرار محكمة الدرجة الأولى وجاء في حيثيات الحكم بأن قواعد التفسير السليم للنصوص القانونية تقتضي القول بأن كلمة "أي حاسوب" "Any Computer" الواردة في المادة الأولى من القانون المشار إليه يجب أن تُعطي معناها الحقيقي وهي لا تعني بالضرورة أن جريمة الدخول غير المصرح به لا تتحقق إلا باستخدام جهاز حاسوب للدخول إلى جهاز حاسوب آخر. فالجريمة تتحقق حتى لو تمكن أحد الأشخاص من الدخول مباشرة إلى جهاز حاسوب للغير دون حاجة إلى استخدام جهاز آخر. وقد بدّد صدور هذا القرار المخاوف المشار إليها أعلاه. ورحب فقهاء القانون الجنائي الإنجليزي بقرار محكمة الاستئناف الإنجليزية على أساس أنه لو لم يفسخ قرار محكمة الدرجة الأولى لنتج عن ذلك إيجاد ثغرة تشريعية في قانون إساءة استخدام الحاسوب[٤].

ومن الجدير بالذكر أن القضاء البريطاني أصدر عدداً من الأحكام القضائية أثبتت فاعلية قانون إساءة استخدام الحاسوب في التصدي لمرتكبي هذا النوع من الجرائم خاصة اولئك الذين يحاولون الدخول إلى نظام الحاسب الآلي من بُعد باستخدام نظام معلوماتي آخر. ويتجلى ذلك بكل وضوح بالقرار القضائي الذي أصدرته إحدى المحاكم الإنجليزية والقاضي بإدانة شاب بريطاني بالجريمة المنصوص عليها في المادة الأولى من قانون إساءة استخدام الحاسوب بعد أن تمكن من خرق النظام المعلوماتي الخاص بوزارة الدفاع الأمريكية[٥]. ومما لا شك فيه أن هذا القرار يؤكد نجاح القانون

(1) Gringras, C., To Be Great is To Be Misunderstood: The Computer Misuse Act 1990, "**Computer and Telecommunications Law Review**, 1997 3(5), 214.
(2) Michael Colvin, MP., Hansard H.C. Vol. 166, Column 1134.
(3) DTI, Dealing with Computer Misuse, HMSO), 1992, para. 223.
(4) E. Susan singleton, "Computer Misuse Act 1990 – Recent Developments" 1993 **Company Lawyer** 14 (1), 22– 23; Clive Gringras, "To Be Great is to be Misunderstood: The Computer Misuse Act 1990" 1997 **Computer and Telecommunications Law Review**, 3 (5), 213– 215.
(5) R. v. Pryce (Unreported, Bow Street Magistrates, March, 21, 1997.

في تحقيق الهدف الذي سنّ من أجله، إلا أن السؤال الذي يطرح نفسه هو: هل نجـح القـانون فـي تحقيق الغاية الرئيسية التي أُصدر من أجلها؟

إن الهدف الرئيس لإصدار قانون إساءة استخدام الحاسوب هو تجريم الدخول غير المصرح بـه من الأشخاص الذين يعملون في النظام المعلوماتي ذاته (The Insider). إن هذه الغاية التـي سـعى القانون إلى تحقيقها كانت في أذهان أعضاء اللجنة التي أوكل إليها مهمة وضـع مـشروع القـانون (The Law Commission) التي أكدت على أن القانون يجب ألا يقتصر على تجريم الممارسات غير المشروعة التي تتم من الأشخاص غير المصرح لهم بالدخول إلى النظام المعلوماتي[١]. وهذه الحقيقة أكدها عضو البرلمان البريطاني (Michael Colvin, MP) الذي تبنى مشروع القانون، فقد أكـد أنـه يستهدف كذلك معاقبة الأشخاص المصرح لهم باستخدام النظام المعلوماتي إذا تم الدخول إلى أجـزاء في النظام لا يسمح بالدخول إليه[٢].

وعلى الرغم من وضوح الغاية من إصدار هذا القانون ومن وضوح الـصياغة التـشريعية، ألا أنّ القضاء البريطاني تردد في توفير الحماية للمعطيات والبيانات ضد الأنشطة غير المشروعة التي يمارسها الأشخاص المصرح لهم بالدخول للنظام المعلوماتي. إن تردد القضاء في تطبيـق القـانون على الأشخاص الذين يستخدمون النظام المعلوماتي لغايات غير الغاية التي صرح لهم بها ظهر جليا في قضية[٣] DPP v. Bignell. وتتلخص وقائع هذه القضية بأن السيد Bignell، وكان يعمل ضـابطاً في الشرطة، قد طلب من أحد العاملين على أجهزة الحاسوب التابعة للشرطة بأن يزوده بمعلومـات وافية عن مالك سيارتين وأرقامهما. وعند افتضاح الأمر قدم المشتكى عليه للمحاكمة عن ارتكابـه لجريمة الدخول غير المصرح به خلافاً للمادة الأولى من قانون إساءة اسـتخدام الحاسـوب وكـان القرار الصادر عن محكمة الدرجة الأولى يقضي بالإدانة إلا أن محكمـة (Crown Court) فـسخت الحكم وقضت بأن المشتكى عليه لم يرتكب الجريمة المنصوص عليها في المادة الأولى مـن قـانون إساءة استخدام الحاسوب لعام ١٩٩٠ وذلك بدعوى أن السيد Bignell مخوّلٌ بحكم وظيفته الـدخول إلى هذا النوع من المعلومات والبيانات بموجب المادة (١٧) من القانون حتى ولو كان الدخول إلـى النظام المعلوماتي لأغراض خاصة وليس لاعتبارات المصلحة العامة. وقد جاء في حيثيات الحكم أن الدخول يكون غير مصرح به وفقا لأحكام المادة (٥/١٧) من القانون في حالتين: إذا تم الدخول إلى النظام من شخص غير مصرح له بذلك، أو إذا تم الدخول دون الحصول على موافقـة أو تفـويض مسبق من الشخص المفوض بإعطاء مثل هذا التفويض أو الموافقة. وعليه، فإن لدى المشتكى عليـه

(1)Report of the Law Commission on "Computer Misuse" 1989 and CM 1819 Report No. 186.
(2) Hansard, H.C. Vol. 166, Column 11380.
(3) [1998] 1 Cr. App. R.1.

الصلاحية للدخول للنظام حتى لو كان الدخول لغاية غير الغاية التي صرح له باستخدامه. وقد تم تأييد هذا القرار من (Divisional Court) وأضافت أن الغاية من إصدار قانون إساءة استخدام الحاسوب هو الحفاظ على سلامة النظام المعلوماتي وليس الحفاظ على سلامة المعلومات المختزنة داخل النظام المعلوماتي.

لقد تعرض هذا القرار القضائي إلى انتقاد شديد من شراح القانون الإنجليزي على أساس أن القرار القضائي خلق ثغرة كبيرة في التشريع المعني يمكن أن يستغلها أي شخص من أمثال السيد Bignell للتلاعب بالنظام المعلوماتي والدخول إلى البينات المخزنة والاعتداء على حرمة الحياة الخاصة للآخرين دون أن يتعرض للمسؤولية الجزائية بدعوى انه يملك الحق في الدخول للنظام المعلوماتي حتى ولو كانت الغاية من الدخول تحقيق هدف غير مصرح به أو غير مشروع[1]. إن هذا الاجتهاد القضائي يتعارض مع الغاية من سن القانون. فقد جاء هذا الاجتهاد بسبب التفسير غير السليم لنصوص التشريع وإن الغاية من وضع النص ليس معاقبة الأشخاص الذين يستخدمون أجهزة الحاسوب، بل معاقبة اولئك الذين يستخدمون تلك الأجهزة بهدف الدخول للبيانات والمعطيات المخزنة فيه، والفارق كبير بينهما وهو أمر لم يتنبه له القضاء. إن استخدام أجهزة الحاسوب في معالجة البيانات أصبح أمرا متزيداً. إن ما يدعو إلى القلق أن لا يعاقب القانون أولئك الذين يسيء بعضهم استخدام الصلاحيات الممنوحة لهم بالدخول إلى تلك البيانات والبرامج[2]. والأمر الأكثر خطورة من ذلك كله أن هؤلاء قد لا يكونون عرضة للمسئولية الجزائية عن الجرائم المنصوص عليها في المادتين الثانية والثالثة من قانون إساءة استخدام الحاسوب بدعوى أنه يملك الصلاحية للدخول للنظام المعلوماتي حتى لو كان الهدف من الدخول تسهيل ارتكاب جريمة أخرى، أو تعديل أو إتلاف البيانات المخزنة في النظام. إن هذا التحليل- لو صح- يلقي الضوء ساطعا على ثغرات يعاني منها التشريع القائم، الأمر الذي يجعل الحياة الخاصة للأفراد تقع خارج نطاق الحماية الجزائية إذا ما تم الحصول على المعلومات ممّن يملك صلاحية النفاذ إلى النظام المعلوماتي[3].

جاء هذا الاجتهاد القضائي في أعقاب قرار مجلس اللوردات البريطاني في قضية[4] R v. Brown وهي قضية تتشابه وقائعها مع قضية (Bignell). وتتلخص وقائعها بأن السيد (Brown)

(1) Robert Sumroy, "Computer Misuse and Data Protection" 1997 **Computer and Telecommunication Law Review** 4 (5), 119–120.

(2) Gringras, C., "To Be Great is to be Misunderstood: The Computer Misuse Act 1990" 1997 **Computer and Telecommunications Law Review**, 3 (5), 215.

(3) Robert Sumroy, "Computer Misuse and Data Protection" 1997 **Computer and Telecommunication Law Review** 4 (5), 120.

(4) [1996] 1 All.E.R. 545(HL).

الذي يعمل ضابطا في الشرطة وجه له الاتهام بالقيام بالدخول إلى الحاسـوب الخـاص بالـشرطة وحصل على معلومات خاصة بأرقام لوحات عدد من المركبات التي يمتلكها عدد مـن الأشـخاص المدينين بمبالغ معينة لإحدى الشركات التي يديرها أحد أصدقائه. وقد وجهت النيابة العامـة تهمـة استخدام معلومات مخزنة في جهاز الحاسوب لغايات شخصية (using personal information) خلافا لأحكام المادة الخامسة من قانون حماية البيانات لعـام ١٩٨٤ (Data Protection Act 1984). وقـد أيد مجلس اللوردات قرار محكمة الاستئناف القاضي بان المـشتكى عليـه لـم يرتكـب الجريمـة المنصوص عليها في المادة الخامسة بدعوى أن الدخول للنظام المعلوماتي للحصول على معلومـات لأغراض شخصية لا يعتبر استعمالا للبيانات بالمعنى المقصود في القانون، إذ لم تقدم النيابة العامـة أي دليل يثبت بأن المشتكى عليه قد قام بتمرير تلك المعلومات إلى صديقة. لقد ترتـب علـى هـذا القرار القضائي نتيجة مفادها أن الاطلاع على البيانات دون استخدامها لا يـشكل جريمـة يعاقـب عليها بمقتضى المادة الخامسة من قانون حماية البيانات. إن إلقاء نظرة متفحصة على قـرار الحكـم في هذه الدعوى وحيثياته يجعل من الصعب القول بأن المشتكى عليه فـي هـذه الـدعوى سـيكون عرضة للمسئولية الجزائية وفقاً لأحكام المادة الأولى من قانون إساءة استخدام الحاسوب في ضـوء الحكم الصادر في قضية (Bignell) السابقة، على فرض أن الإتهام وجه سندا له[1].

إن الاجتهادات القضائية في قضيتي (Bignell) و (Brown) قـضّت مـضجع المعنيـين بـأمن المعلومات وأثارت قلقهم وساورتهم الشكوك حول فاعلية هذه القوانين في توفير الحمايـة الجزائيـة اللازمة. ولكن القلق والشكوك لم تـدم طويلا بعد الاجتهاد القضائي لمجلس اللوردات في قـضية[2] Rv. Bow Street Metropolitan Stipendiary Magistrate. فقد فسر مجلس اللوردات عبارة "الدخول غير المصرح به" (Unauthorized Access) تفسيراً صحيحاً ينسجم مع الغاية من التشريع، إذ أكـدت المحكمة العليا على إمكانية تطبيق المادة الأولى من القانون على مرتكبي هذه الجريمة حتى لو كانوا من الموظفين العاملين في النظام المعلوماتي والمصرح لهم بالدخول إليه.

وتتلخص وقائع هذه القضية بقيام المدعوة (Ojomo) التي كانت تعمل بوظيفة محللة مالية في شركة American Express بالدخول إلى كافة حسابات العملاء على الرغم من أنها كانت مخولة للدخول على بعض الحسابات. وتمكنت من الحصول على معلومات سرية من هذه الحسابات وإعطائها لشخص يدعى (Allison). وتم استخدام هذه المعلومات للحصول على الأرقام السرية للحسابات وبعض بطاقات الائتمان ثم استخدمت هذه المعلومات للاستيلاء على مبالغ نقدية كبيرة من

(1) Robert Sumroy, "Computer Misuse and Data Protection" 1997 Computer and Telecommunication Law Review 4 (5), 120.
(2) (1999) WLR 620 (H L).

أجهزة الصراف الآلي. عند اكتشاف الأمر قررت محكمة الجزاء الابتدائية أن الفعل الذي قامت به (Ojomo) لا يشكل انتهاكاً لنص المادة الأولى من قانون إساءة استخدام الكمبيوتر في ظل القرار الصادر في قضية (Bignell) وقد تم تأييد هذا القرار من قبل محكمة الاستئناف. ولكن تم الطعن في هذا القرار لدى مجلس اللوردات، وكان السؤال المطلوب الإجابة عليه هو هل يمكن للموظف المخول الدخول للمعلومات المختزنة في النظام المعلوماتي أن يرتكب جريمة الدخول غير المصرح به خلافاً لأحكام المادة الأولى؟

قرر مجلس اللوردات أن سلوك (Ojomo) يشكل جريمة الدخول غير المصرح به التي يعاقب عليها بموجب أحكام المادة الأولى من قانون إساءة استخدام الحاسوب. وذلك لأنها استخدمت نظام الحاسوب للحصول على معلومات لم تكن مخولة الدخول لها أو أنها لم تحصل على التصريح اللازم للدخول لتلك المعلومات. فصلاحية الدخول إلى النظام المعلوماتي لا تتعلق فقط بالبيانات والبرامج بل يجب أن تمتد لتشمل النوع الحقيقي للدخول للنظام المعلوماتي المراد تحقيقه. فكلمة تحكم "Control" لا يقصد بها القدرة على تشغيل جهاز الحاسوب فقط. إن المادة (٥/١٧) من قانون إساءة استخدام الحاسوب تعني أن صلاحية الدخول إلى نوع معين من المعلومات لا يعطي الصلاحية للدخول إلى معلومات أخرى حتى ولو كانت من ذات الصنف. فالمادة الأولى من القانون تشير إلى إرادة الدخول إلى النظام المعلوماتي دون تصريح. كما قضى مجلس اللوردات بان قرار محكمة (Divisional Court) في قضية (Bignell) لم يكن صحيحا، إذ فسرت المحكمة المادة (٥/١٧) تفسيرا خاطئاً بسبب سوء استقراء النصوص القانونية والتعامل مع المفاهيم والتعابير الواردة في القانون بصورة موجزة وسطحية. وبعد أن استعرض مجلس اللوردات تقرير اللجنة القانونية التي أعدت مشروع القانون والتي بينت إن القانون يهدف إلى معاقبة هؤلاء المخوّلين بالدخول إلى النظام المعلوماتي و يسيئون استخدامه، خلص إلى نتيجة مفادها أن التفسير الضيق لنصوص القانون في قضية (Bignell) من شأنه أن يفوت الغاية من إصدار القانون ويحد من فاعليته في التعامل مع الصور المختلفة لإساءة الاستخدام.

امتدح شراح القانون الإنجليزي القرار القضائي لأنه أزال الغموض من قانون إساءة استخدام الحاسوب وقضى بإمكانية تطبيقه حتى على الموظفين المخوّلين للدخول للمعلومات المختزنة في النظام المعلوماتي. كما أن القرار الصادر من مجلس اللوردات عالج ثغرة قانونية يمكن أن يترتب عليها أن تبقي الوقائع السابقة خارج نطاق التجريم[1]. ويرى الفقه أن منهج مجلس اللوردات عقلاني

(1) Kelly Stein, "Unauthorized Access and the Computer Misuse Act 1990: House of Lords Leaves no Room for Ambiguity" *2000* **Computer and Telecommunications Law Review** 6 (3), 63-66 .

وعملي لأنه يضع بصورة ضمنية قواعد قانونية تنسجم مع المعايير الاجتماعية والتجارية على حد سواء من خلال تطوير مفهوم عبارة "الدخول غير المصرح به" الواردة في القانون دون التقيد بالدلالات اللغوية لها[١]. كما أن قرار مجلس اللوردات يتعامل مع قضية في غاية الأهمية وهي أن المشرع الانجليزي لم يجرّم بنصوص صريحة الأفعال التي تنطوي على تجاوز الشخص للصلاحيات الممنوحة له قانونا أو استخدم الشخص صلاحياته للدخول لغاية أخرى ممنوعة أو غير مشروعة. وعليه فإن قرار مجلس اللوردات يرسل إشارة قوية مفادها أن القانون يجرّم أفعال أولئك الأشخاص الذين يتجاوزون الصلاحيات الممنوحة لهم (exceeding authorized access).

ومن الجدير بالذكر أن بعض جرائم الاحتيال المالي التي تتم عن طريق الشبكة المعلوماتية تقع خارج نطاق القانون لأن الدخول إلى الشبكة المعلوماتية لا يتضمن بالضرورة دخولاً غير مصرح به إلى النظام المعلوماتي كما يتطلب القانون لتحقق أركان الجرائم وعناصرها المنصوص عليها[٢]. والتساؤل الذي يطرح نفسه هو: هل تتحقق أركان الجريمة وعناصرها المنصوص عليها في المادة الأولى من قانون إساءة استخدام الحاسوب لعام ١٩٩٠ إذا تم الدخول إلى النظام المعلوماتي من أحد الأشخاص بناء على طلب من شخص آخر؟ أجاب القضاء البريطاني على هذا السؤال بالإيجاب وذلك في قضية[٣] R. v. Pearce. وتتلخص وقائعها بقيام هذه بقيام المدعو (Farqugarson) بالطلب من السيدة (Pearce) بالولوج إلى النظام المعلوماتي الخاص برب العمل من أجل الحصول على بينات وتفاصيل تتعلق بالشيفرات الالكترونية التي تسهل عملية استنساخ أجهزة الهواتف الخلوية. وقد تم إدانة (Farqugarson) بالجريمة المنصوص عليها في المادة الثانية من قانون إساءة استخدام الحاسوب بالرغم من أنه لم يمس جهاز الحاسوب.

يرى جانب من الفقه أن قانون إساءة استخدام الحاسوب أثبت عجزه في مواجهة التطورات الحديثة، فالمادة الثالثة من القانون لا تشمل بعض أنماط السلوك المستحدثة التي جاءت نتيجة للتطورات التكنولوجية الحديثة. ومن ابرز الأمثلة على ذلك استخدام ما يسمى ببرامج (Botnets) وهي مجموعة من البرامج التي يمكن التحكم فيها عن بعد إذ يتم ربطها على شبكة المعلومات ومن ثم يمكن تشغيلها على جهاز حاسوب مستقل أو مجموعة من الحواسيب المرتبطة مع بعضها والموصولة بشبكة المعلومات. وقد يتم تركيب هذا البرنامج وحده أو باستعمال برامج ضارة أخرى

(1) Mary W.S. Wong, "Cyber-Trespass and "Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience"15 **International Journals of Law and Information Technology** 2007, 90 at 121.

(2) Natasha Jarvie, "Control of Cybercrime: Is an End to our Privacy on the Internet a Price Worth Paying? Part 1,**Computer and Telecommunications Law Review** 2003, 9(3), 80.

(3) Unreported, Croydon Magistrates Court, December 9, 1993.

كالفيروسات. ويستخدم هذا البرنامج على نطاق واسع لارتكاب عددٍ من الأفعال التي تجرمها بعض التشريعات مثل سرقة الأسرار التجارية، وسرقة المعلومات، ونشر الفيروسات وغيرها من البرامج الضارة بالأنظمة المعلوماتية. كما أن هذه البرامج قد تُستخدم من أجل حجب الخدمة (خدمة الانترنت على سبيل المثال) عن المستفيدين وهو ما يسمى باللغة الانجليزية Denial of Service (Attacks). إن استخدام هذه الوسيلة يؤدي إلى فصل الشبكة وتعطيل الخدمة من خلال استهلاك سعة الشبكة أو زيادة حمولة النظام المعلوماتي[1]. ففي عام ٢٠٠٥ قضت محكمة جزاء ويمبلدون (Wimbledon Magistrates Court) بأن المادتين (٣) و (١٧) من قانون إساءة استخدام الحاسوب لا يطبق على أنماط السلوك المستحدثة والمتمثلة في حجب الخدمة عن المستخدمين لها وذلك في قضية تتلخص وقائعها بقيام أحد الأشخاص باستخدام برنامج خاص أدى إلى إرسال ما يقارب خمسة ملايين رسالة الكترونية إلى إحدى الشركات التي كان يعمل فيها المشتكى عليه سابقا مما أدى إلى تعطيل النظام المعلوماتي في تلك الشركة[2]. وقد أشرنا سابقا إلى إن التعديل الذي أجراه المشرع الجزائي الانجليزي على قانون إساءة استخدام الحاسوب بموجب قانون الشرطة والعدالة لعام ٢٠٠٦ قد تجاوز هذه المآخذ.

وفي قضية[3] R v. Levin أيدت محكمة الاستئناف البريطانية القرار الحكم القاضي بإدانة أحد الأشخاص بجريمة الدخول إلى النظام المعلوماتي بقصد ارتكاب جريمة التزوير. كما أيدت المحكمة ذاتها إدانته بالجريمة المنصوص عليها في المادة الثالثة أيضا. وتتلخص وقائع تلك الدعوى بقيام شخص يدعى (Levin) بالدخول إلى النظام المعلوماتي الخاص ببنك (Citibank) في مدينة نيوجرسي من مدينة سانت بطرسبرغ حيث يقيم باستخدام جهاز الحاسوب الخاص به وتمكن من تحويل بعض الأموال من الحسابات العائدة لبعض عملاء البنك إلى حسابات خاصة به في بريطانيا.

ومن التطبيقات القضائية الإنجليزية الحديثة على المادة الثالثة من قانون إساءة استخدام الحاسوب قضية[4] Zezev v. United States. وتتلخص وقائع هذه الدعوى بقيام شخص يعمل في شركة مقرها كازاخستان باختراق النظام المعلوماتي العائد لشركة تعمل في ولاية نيويورك الأمريكية تقوم بتزويد الأخبار والمعلومات المالية إلى كافة أرجاء العالم، و تمكن المشتكى عليه من الدخول إلى البريد الالكتروني الخاص بمدير الشركة ومدير الأمن فيها الأمر الذي مكنه من الحصول على معلومات بالغة السرية. بعد ذلك قام بإرسال عدد من الرسائل الالكترونية إلى مدير الشركة لإخباره

(1) Rychiicki, Tomasz, "Legal Issues of Criminal Acts Committed Via Botents" **Computer and Telecommunications Law Review**, 2006 12(5), 161–167.
(2) See http:// news.com.
(3) [1997] Q.B. 65.
(4) [2002] Crim.L.R. 648.

بأن النظام المعلوماتي الخاص بالشركة قد تم اختراقه، وطالب بمبلغ وقدره مائتي ألف دولار مقابـل عدم قيامه بنشر واقعة اختراق النظام المعلوماتي الخاص بالشركة وهو أمر لو تحقق فإنـه سيـضر بسمعة الشركة وسيلحق بها خسائر مالية كبيرة. تم اعتقال المشتكى عليه فـي مدينـة لنـدن أثنـاء حضوره لاستلام المبلغ المتفق عليه بعد أن أخبر مدير الشركة الشرطة بـذلك. وطلبـت الولايـات المتحدة ترحيله إليها لمحاكمته بعد أن تم توجيه ست تهم إليه من بينهـا التـآمر لإتـلاف البيانـات المخزنة وهي الجريمة التي يعاقب عليها بمقتضى المادة الثالثة من القانون. قضت محكمة الاستئناف بتأييد قرار محكمة الدرجة الأولى بالموافقة على تسليم المشتكى عليه إلى الولايات المتحدة الأمريكية باعتبار أن فعل الشخص المطلوب تسليمه أرتكب جريمة يعاقب عليها بموجب المـادة الثالثـة مـن قانون إساءة استخدام الحاسوب لعام ١٩٩٠. وقد جاء في حيثيات الحكم إن إرسال بريد الكترونـي بطريقة يفهم منها أنه مرسل من شخص ما إلا أنه في الواقع تم إرساله من شخص آخر الأمر الـذي أدى إلى جعل جهاز الحاسوب يسجل معلومات غير صحيحة أضـرت بـشكل واضـح بمـصداقية البيانات المخزنة في الحاسوب (Reliability of such data). بناء على ذلك فإن هذا التصرف يـدخل ضمن نطاق المادة ٣/٢/ج من القانون باعتبار أن المعلومات هي بيانات بدون أدنـى شـك. كمـا قضت المحكمة بأن إدخال بينات غير صحيحة إلى النظام المعلوماتي من خلال التظاهر بأنه صاحب البريد الإلكتروني مع أنه في الواقع ليس كذلك يفسد عمل الحاسوب ويعتبر تعديلا لمحتوياتـه مـن المعلومات، ولهذا لا يقبل الاحتجاج بأن نص المادة الثالثة يقتصر على إتلاف الحاسوب وأن تعـديل المعلومات يتحقق بإضافة معلومات أخرى إليها. ويرى الفقه أن قرار المحكمة يشير بكـل وضـوح إلى أن نص المادة الثالثة يتطلب قصدا جرميا ذا طبيعة مزدوجة: اتجاه الإرادة نحو تعديل محتويات الحاسوب والمعلومات المخزنة فيه، وانصراف الإراده نحو الإضرار بمصداقية المعلومات إلا أنـه عندما يتطلب الأمر أن يترتب على تعديل المعلومات الإضرار بمـصداقيتها، فـإن كـلا القـصدين يتداخلان ليصبح القصد المتمثل بإرادة تسجيل معلومات غير صحيحة في الحاسوب يعني أن الإرادة الجرمية قد اتجهت حتما نحو الإضرار بمصداقية البيانات[1].

ويعتبر من قبيل التعديل في بيانات الحاسوب ضمن نطاق نص المادة الثالثة قيام المشتكى عليـه وهو موظف سابق في إحدى الشركات بإرسال عدد كبير جداً من رسائل البريـد الإلكترونـي إلـى صاحب العمل السابق بصورة بدت معها أن تلك الرسائل الإلكترونية صادرة من أحد كبار الموظفين في الشركة الأمر الذي ترتب عليه تعديلاً في محتويات النظام المعلوماتي بـالمعنى المقـصود فـي

(1) J.C.Smith, Computer Misuse: Whether Sending An E-mail Which Did not Come from Purported Source Affected the Reliability of Data, Case Comment, [2002] **Criminal Law Review** 648 at 650.

المادة ١٧/٧/ب من القانون. وقد جاء في حيثيات الحكم في هذه القضية أن رب العمل وإن وافق ضمنياً على استقبال الرسائل طالما أنه يملك بريداً إلكترونياً إلا أنه لا يمكن اعتبار ذلك الرضا الضمني مطلقا. فالرضا يشمل بطبيعة الحال إرسال بريد الكتروني بقصد التواصل مع صاحب العمل وليس إعاقة وتعطيلاً لعمل النظام المعلوماتي في الشركة. كما أنه لا يوجد موافقة على إرسال بريد الكتروني بأسم أحد كبار موظفي الشركة، ولا يوجد رضا بإرسال بريد إلكتروني من شأنه إلحاق الضرر بالنظام المعلوماتي[1].لهذا، فإنه يدخل ضمن نص المادة الثالثة من قانون إساءة استخدام الحاسوب تعطيل النظام بشكل كامل أو منع استخدامه. ففي قضية[2] R v. Goulden، اعترف السيد Goulden بارتكابه الجريمة المنصوص في المادة الثالثة. إذ قام بالدخول إلى مقر إحدى الشركات المدين لها بمبلغ من المال وتمكن من تركيب جهاز خاص على جهاز الحاسوب الرئيسي العائد للشركة باستخدام كلمة سر لا يعرفها أحد غيره، الأمر الذي أدى إلى تعطيل النظام المعلوماتي بصورة لم يتمكن موظفو الشركة من استخدامه فالحق بالشركة خسائر مالية بلغت ستة وثلاثين ألف جنيه إسترليني. فقضت المحكمة بالحكم على المشتكى عليه بالحبس لمدة عامين مع وقف التنفيذ وغرامة مقدارها ألف وستمائة وخمسون جنيه إسترليني.

وفي عام ١٩٩١ أوقفت الشرطة ثلاثة أشخاص بتهمة التعاون من أجل الدخول للنظام المعلوماتي لعدد من الجامعات وعدد من المؤسسات العامة والشركات التجارية في عدد من دول العالم. وقد أطلقوا على أنفسهم اسم (Eight Legged Groove Machine). إذ قاموا بترك رسائل على أجهزة الحاسوب التي دخلوا إليها موقعة بالأحرف الأولى الخاصة بهم (8LGM).ولم يسبق لهؤلاء الأشخاص أن تقابلوا مسبقاً، كما أنهم لا يعرفون أسماء بعضهم الحقيقية حتى تم توقيفهم. تم توقيف الأشخاص الثلاثة في منتصف الليل أثناء قيامهم بأعمال القرصنة على أجهزة الحاسوب. وقد وجهت لهم تهم التآمر لارتكاب الجريمة المنصوص عليها في المادة الثالثة من قانون إساءة استخدام الحاسوب والتآمر للحصول بطريقة غير مشروعة على خدمات الاتصال العائدة لشركة الاتصالات البريطانية.

وقد أقر المتهمان (Karl Strickland) و(Neil Woods) باقتراف الجرائم المسندة إليهما، كما اعترف (Woods) بإلحاق خسائر مادية بإحدى المؤسسات التعليمية في لندن تقدر بمبلغ خمسة عشر ألف جنيه إسترليني. واعترف (Strickland) بقيامه بالدخول إلى النظام المعلوماتي الخاص بوكالة الفضاء الأمريكية (NASA) (ITN). وشركة فحكم على كل منهما بالسجن لمدة ستة أشهر. وقد

(1) **DPP v. Lennon** [2006] EWHC 1201(Admin); [2006] All.E.R. (D) 147.

(2)(1992), Unrepoted; see E. Susan singleton, "Computer Misuse Act 1990 – Recent Developments" 1993 **Company Lawyer** 14 (1), 23.

اعتبرت المحكمة أن عقوبة السجن هي العقوبة المناسبة لهما بسبب ما قاما به مـن أفعـال ولـردع الآخرين عن القيام بأفعال مماثلة انطلاقاً من أن الحاسوب يؤدي دوراً حيوياً في حياتنا. فالحاسـوب يحتوي على معلومات شخصية ومالية ومعلومات سرية تتعلق بالشركات ومؤسسات الدولـة، وهـي تقدم خدمات متنوعة للمواطنين بعضها خدمات طوارئ يتم تقديمها بالاعتماد على أجهزة الحاسـوب بالدرجة الأولى. ولذلك لا بد من ضمان سلامة النظام المعلوماتي لأن أفعـال القرصـنة تعرضـه للخطر. كما أكدت المحكمة أن فرض العقوبة المناسبة على مثل هذه الأفعال أمر لا بد منه من اجـل إرسال رسالة واضحة إلى مرتكبي هذه الجرائم مفادها أن هذه الأفعال لا يمكن التغاضي عنها. أمـا بالنسبة للمتهم الثالث ويدعى (Paul Bedworth) فقد قام بالدخول إلى النظـام المعلومـاتي الخـاص بصحيفة (Financial Times) وألحق بها خسائر تقدر بخمسة وعشرين ألف جنيه إسترليني. كما قـام باختراق الحاسوب الرئيسي للمنظمة الأوروبية لأبحاث ومعالجة السرطان وأجرى اتصالات هاتفيـة كلفت المنظمة عشرة آلاف جنيه إسترليني. وقد اتهم بالتآمر لارتكاب الجريمة المنصوص عليها فـي المادة الثالثة من قانون إساءة استخدام الحاسوب (التعديل في بينات الحاسوب) والتآمر للحصول على خدمات اتصالات بطريقة غير مشروعة. وأعلن (Bedworth) في أثناء المحاكمة أنـه غيـر مـذنب بالجرائم المسندة له بدعوى أنه قد "أدمن" على استخدام الحاسوب وأنه يعاني مـن مـرض يـدعى (Computer Tendency Syndrome) وبسبب هذا الإدمان لم يتكون لديه قصد جرمي. وتوصلت هيئة المحلفين في نهاية المحاكمة إلى إعلان براءته رغم أن قاضي الحكم قد نبـه هيئـة المحلفـين بـأن "الإدمان" على استخدام الحاسوب (Obsession) لا يعد مانعا للمسئولية الجزائية. وقد تعرض قـرار الحكم إلى انتقاد شديد إذ وصف القرار بأنه "ميثاق القراصنة" أو "ترخيص بالقرصنة". كما أنه كـان بالإمكان صدور حكم بالإدانة لو أن الادعاء العام قد أسند للمشتكى عليه الجرائم المنصوص عليهـا في المواد (١) و(٣) من قانون إساءة استخدام الحاسوب بدلاً من اتهامه بالتآمر الذي يتطلب أركـان وعناصر يصعب إثباتها[1].

وفي قضية أخرى تتعلق بالمادة الثالثة من قـانون إسـاءة اسـتخدام الحاسـوب هـي قـضية (Whitaker)، قضت محكمة صلح جـزاء (Scunthorpe) بإدانـة المـدعو (Whitaker) بارتكابـه الجريمة المنصوص عليها في المادة الثالثة من قانون إساءة استخدام الحاسوب. وتتلخص وقائع هـذه الدعوى بقيام (Whitaker) بتطوير برنامج لأحد زبائنه مقابل مبلغ من المال، وقد تم إبرام عقد بينهما لهذه الغاية إلا أنه نتيجةً لخلافٍ حول دفع قيمة البرنامج قام المشتكى عليـه بـزرع فيـروس فـي

(1) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] 3 Web **Journal of Current Legal Issues.**

البرنامج الأمر الذي أدى إلى عدم إمكانية استخدامه. أثار المشتكى عليه دفعا مفاده بأنه يملك الحق في فعل ذلك بدعوى أنه لا يزال يملك حقوق التأليف الخاصة بالبرنامج. ولم تقبل المحكمة هذا الدفع بدعوى أن هذا الأمر لم يرد النص عليه في العقد المبرم بينهما[1].

وفي نهاية عام ١٩٩٥ أصدرت محكمة (Crown Court) في مدينة (Exeter) حكما يقضي بإدانة شخص يدعى (Christopher Pile) والحكم عليه بالسجن لمدة عام ونصف بعد اتهامه بارتكاب خمس جرائم خلافا لأحكام المادة الأولى من قانون إساءة استخدام الحاسوب، وخمس جرائم أخرى خلافا لأحكام المادة الثالثة من ذات القانون، وتهمة تتمثل بتحريض آخرين على نشر فيروسات قام بصنعها. لقد قام المدعو (Pile) بأعداد نوعين من الفيروسات الخطيرة هما (Pathogen) و (Queeg). وجاء في حيثيات قرار الحكم أن "أولئك الأشخاص الذين يحاولون إلحاق الضرر بصورة متعمدة بإحدى الأدوات الأساسية في عصرنا الحاضر يجب ألا يتوقعوا معاملة متساهلة من القضاء". لقد ألحقت أفعال المشتكى عليه أضرارا جسيمة بعدد من الشركات البريطانية المعروفة. وقدرت الخسائر التي ألحقتها هذه الفيروسات بإحدى الشركات بمبلغ وقدره خمسمائة ألف جنيه إسترليني. واضطرت الشركة إلى قضاء (٤٨٠) ساعة من أجل فحص أكثر من مليون ملف مخزن على أجهزة الحاسوب. كما تم نشر هذه الفيروسات إلى عدد من دول العالم عن طريق شبكة الانترنت. وعلى الرغم أنه لم يتسنى معرفة حجم الخسائر بدقة جراء نشر هذه الفيروسات إلا أنه مما لا شك فيه أنها كانت كبيرة.

إن قضية المدعو (Christopher Pile) كانت على قدر كبير من الأهمية وذلك لعدة أسباب. أولها أنها كانت أول قضية تتعلق بصناعة برامج الفيروسات تعرض على القضاء البريطاني. وثانيها أن هذه القضية تشير على أنه ورغم الصعوبات العملية التي تتعلق بتطبيق قانون إساءة استخدام الحاسوب إلا أنه اثبت فاعليته في ملاحقة مرتكبي هذا النوع من الجرائم. وعلى الرغم من ذلك أصبحت صناعة الفيروسات تجارة رابحة إذ لا يعرف في معظم الحالات من الذي قام بإعدادها وصناعتها، كما أنه يصعب إثباتها وذلك لأن الفيروسات تعمل على تعديل البرامج دون أن تترك أي اثر.

ومن الجدير بالذكر أن الشركات التي تتعرض لغزو الفيروسات تتردد في تقديم شكوى إلى القضاء ضد مرتكبي هذه الجرائم لعدة أسباب. أولا: أن الإبلاغ عن هذه الجرائم من شأنه الإساءة إلى سمعة الشركة ويلقي بظلالٍ من الشك حول متانة النظام المعلوماتي للشركة الضحية. ثانيا: أن

(1) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] 3 **Web Journal of Current Legal Issues.**

قانون إساءة استخدام الحاسوب لا يتـضمن الـنص علـى عنـصر التعويـــض عـن الـضرر (Restitutional Element) جراء الأفعال المرتكبة. ولذلك لا يمكن المطالبة بالتعويض عن الـضرر في ظل قانون إساءة استخدام الحاسوب. إن الحل الأمثل لحمل الشركات المستهدفة على الإبلاغ عن هذا النوع من الجرائم هو إجبار تلك الشركات على ضرورة إبرام عقود تأمين لدى شركات التـأمين التي بدورها ستلقى على عاتق تلك الشركات التزاما بضرورة الإبلاغ عن تلك الممارسات. كمـا أن تطوير أجهزة الشرطة وتدريبها للتعامل مع هذا النوع المستحدث من الجرائم أمر على قدر كبير من الأهمية. إن قطاع الأعمال والتجارة في بريطانيا أبدى اهتماما حول أمتلاك رجال الشرطة المهارات الكافية للتحقيق في هذا النوع المستحدث من الجرائم[1].

خاتمة وتوصيات

إن ميلاد شبكة الإنترنت لعب دوراً جوهرياً في تحطيم الحدود السياسية والجغرافية. وانـصهار العالم في بوتقة المعلومات أصبح أمراً محتماً رافق التطور التكنولوجي والتقني في مختلف نـواحي الحياة. فالمعلومات أصبحت بحق مصدراً للقوة والمعرفة. لقد أوجبت علينـا الثـورة المعلوماتيـة العمل على تحقيق نوعٍ من التوازن بين الاستخدام الحر والكامل للمعلوماتية من ناحية، وبين حمايـة حقوق وحريات المواطن من ناحية أخرى.

إن عصر المعلوماتية خلق آثاراً سلبية نشأت عن الاستخدام غير المشروع للمعلوماتية في غيـر الغرض الذي أعدت له، الأمر الذي أثر على حقوق الأفراد وحرياتهم. ووفرّت الأنظمة المعلوماتية وسيلة جديدة في أيدي المجرمين لارتكاب العديد من الجرائم، بل إن النظام المعلوماتي أصبح محـلاً للاعتداء وإساءة الاستخدام؛ فالتطور العلمي الهائل وما نتج عنه من ثورة فـي المعلوماتيـة جلبـت مخاطر عدة ناجمة عن استخدام شبكة الإنترنت وتطويعها للمجـرم المعلومـاتي ليمـارس نـشاطه الإجرامي، ثم مهد الطريق لظهور نوعٍ مستحدثٍ من الجرائم تسمى "الجرائم المعلوماتية".

عجزت النصوص التقليدية في قانون العقوبات عن مواجهة ما أستحدث من الجرائم، وباتـت قاصرة عن مواجهة الجرائم المرتكبة بواسطة الحاسوب والإنترنت، ذلك أن القواعد القانونية التقليدية في قانون العقوبات وضعت أساساً لحماية الأموال ذات الطبيعة المادية الملموسة التي لها كيان فـي الفضاء الخارجي الأمر الذي يتعذر معه حماية القيم غير المادية المتولدة عن المعلوماتية.

---

(1) Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] 3 *Web Journal of Current Legal Issues*.

ألقى هذا البحث نظرة متفحصة على قانون إساءة استخدام الحاسوب الانجليزي لعام ١٩٩٠ باعتباره تشريعا قانونيا وضع لمواجهة هذا النوع المستحدث من الأجرام. وقد تم دراسة هذا الموضوع في ضوء ما أمكن الإطلاع عليه من اجتهادات القضاء الإنجليزي. وقد تعرضت الدراسة إلى قصور النصوص التقليدية في قانون العقوبات في مواجهة الإجرام المعلوماتي وعجزها عن شمول هذه الجرائم ضمن نطاقها، وذلك لأن النصوص العقابية التقليدية تقصر نطاق الحماية على الأموال المادية الملموسة دون الأموال المعنوية، الأمر الذي يتطلب مراجعة تشريعية شاملة لسد أوجه الفراغ التشريعي القائم بما ينسجم مع مبدأ الشرعية الجنائية ومبدأ عدم جواز القياس في النصوص الجزائية من خلال إصدار تشريع خاص يواجه الجريمة المعلوماتية على غرار القانون الإنجليزي.

وفي ضوء ذلك كله، خلصت الدراسة إلى التوصيات الآتية:

أولاً: ضرورة تدخل المشرع الجزائي الأردني لاستحداث نصوص قانونية في قانون العقوبات تحت عنوان "الجرائم المعلوماتية" تحدد بشكل واضح ودقيق صور الجرائم المعلوماتية والعقوبات المقررة لها.

ثانياً: ضرورة أن يتخلى المشرع الجزائي عن المفهوم التقليدي للمال بحيث يتبنى مفهوماً أوسع وأشمل للمال المنقول بحيث يشمل المعلومات وذلك بإصدار نصوص خاصة لهذه الغاية.

ثالثاً: زيادة الوعي لدى المواطن بخطورة الجريمة المعلوماتية ولآثارها الاقتصادية المدمرة في بعض الأحيان، وتعزيز فهم المواطن للحكومة الإلكترونية وإحاطة المشروع بالضمانات القانونية الكافية والإجراءات الأمنية اللازمة لحمايته من إختراق مجرمي المعلوماتية. ويتوجه الأردن في الوقت الحاضر إلى تنفيذ مشروع رائد يقوم على فكرة التخلص من البيروقراطية والإجراءات الروتينية. وهذا يتمثل في مشروع الحكومة الإلكترونية الذي يهدف إلى تسهيل المعاملات الحكومية والارتقاء بمستوى الخدمات المقدمة للمواطن وزيادة كفاءة المؤسسات العامة. ويمكن تعريف الحكومة الإلكترونية بأنها "تحول الإجراءات الحكومية سواء الداخلية أو الخارجية والمتركزة حول توفير أو إيصال الخدمات للمتعاملين معها بفاعلية وكفاءة بصورة فضلى من خلال تقنيات المعلومات والاتصالات الحديثة[1]. كما يمكن تعريفها بأنها "البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم وتتحقق فيها الأنشطة الحكومية للدائرة

(١) ورقة عمل بعنوان "مستقبل صناعة تقنية المعلومات في دول مجلس التعاون الخليجي" مقدمة من الأمانة الفنية لتقنية المعلومات بوزارة الاقتصاد الوطني في سلطنة عمان لمؤتمر الصناعيين التاسع لدول مجلس التعاون الخليجي، ٢٠٠٣، ص ١٨ .

المعنية من دوائر الحكومة بذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد"[١].

هناك عدد من المعطيات أو العناصر التي يجب توافرها حتى يكون السعي إلى استخدام تقنية المعلومات والاتصالات والتقدم العلمي وتوفير البيانات في القطاعين العام والخاص ناجحاً وهي: المعطيات البشرية، والمتطلبات الإدارية، والمتطلبات القانونية والتشريعية. ولعل المتطلبات القانونية والتشريعية هي أكثر المتطلبات أهمية لأنها تضمن أمن المعلومات وسريتها وخصوصية الأفراد، إذ إن غياب البيئة التشريعية سيجعل الباب مفتوحاً على مصراعيه أمام القراصنة ومجرمي المعلوماتية للتطاول على محتوى الحكومة الإلكترونية بكل ما تشمله، بالإضافة إلى التلاعب بالبيانات والأرقام خاصة في النواحي الاقتصادية المالية[٢]. إن التطبيق الفعال لمشروع الحكومة الإلكترونية يستدعي إيلاء عناية خاصة للتشريعات التي تحمي المعلوماتية من الجرائم التي تقع عليها[٣].

رابعاً: توحيد الجهود الدولية وتكثيفها لمكافحة هذا النوع من الجرائم من خلال الدخول في اتفاقيات ومعاهدات دولية تجرّم كل صور هذا النوع من الجرائم، وتبين قواعد الاختصاص المكاني في حالة وقوعها، وكيفية تسليم مجرمي المعلوماتية، وتبادل الخبرات والأبحاث، والتدريب على المسائل المتعلقة بجرائم الإنترنت. وتكون هذه المعاهدات الدولية مصدراً تستمد منه التشريعات الوطنية النصوص القانونية المتعلقة بالجريمة المعلوماتية. ومن الجدير بالذكر أن المشرع الجزائي الأردني قد عدّل المادة الخامسة من قانون أصول المحاكمات الجزائية بموجب القانون المعدل رقم (١٥) لسنة ٢٠٠٦. وأضاف إلى المادة المذكورة أعلاه فقرة تتضمن حكماً جديداً يقضي بجواز إقامة دعوى الحق العام على المشتكى عليه أمام القضاء الأردني إذا ارتكبت الجريمة بوسائل إلكترونية خارج المملكة وترتبت آثارها فيها، كلياً أو جزئياً، أو على أي من مواطنيها. إن هذا التعديل على قانون أصول المحاكمات الجزائية لن يحقق الغاية المرجوة منه إلا إذا اصدر المشرع الجزائي الأردني تشريعاً جديداً يعاقب ويجرم الاستخدام غير المشروع لتقنية المعلومات.

خامساً: تدريب أفراد الضابطة العدلية والنيابة العامة ورجال القضاء وتأهيلهم على كيفية التعامل مع هذا النوع من الجرائم، وجمع الأدلة والتفتيش والملاحقة في بيئة النظام المعلوماتي، والتعاون مع الخبراء في الحقول الإلكترونية وعقد الدورات التدريبية لهذا الغرض.

---

(١) يونس عرب، قانون الكمبيوتر، بيروت: منشورات اتحاد المصارف العربية، ٢٠٠١، ص: ٤٤٧.

(٢) أحمد حسين العزام، (٢٠٠١)، الحكومة الإلكترونية في الأردن، رسالة ماجستير، جامعة اليرموك، اربد، الأردن.

(٣) نهلا المومني، مرجع سابق، ص ٤٧ .

مراجع البحث

أولاً: الكتب:

١. أحمد حسام تمام، **الجرائم الناشئة عن استخدام الحاسب الآلي**، دار النهضة العربية، القاهرة، ٢٠٠٠.

٢. أحمد هلالي عبداللاه، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية**، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٣.

٣. جميل عبد الباقي الصغير، **الجرائم الناشئة عن استخدام الحاسب الآلي**، ط١، دار النهضة العربية، القاهرة، ١٩٩٢.

٤. حجازي عبدالفتاح بيومي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، الطبعة الأولى، القاهرة،،٢٠٠٢

٥. عفيفي كامل، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى**، بدون ناشر، ٢٠٠٠.

٦. علي القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، الطبعة الأولى، الدار الجامعية للطباعة والنشر ١٩٩٩.

٧. عمر الفاروق الحسيني، **المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية**، الطبعة الثانية، دار النهضة العربية القاهرة، ١٩٩٥.

٨. محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت**، الطبعة الأولى، دار الثقافة، عمان، ٢٠٠٤.

٩. محمد سامي الشواء، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، الطبعة الثانية، دار النهضة العربية، ١٩٩٨.

١٠. محمود نجيب حسني، ١٩٦٩، **جرائم الاعتداء على الأموال**، الطبعة الأولى، بدون ناشر.

١١. مدحت رمضان، **الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)**، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠١.

١٢. المناعسة وآخرون، **جرائم الحاسب الآلي والانترنت**، الطبعة الأولى، عمان، دار وائل للنشر، ٢٠٠١.

١٣. نائلة قورة، **جرائم الحاسب الاقتصادية**، دار النهضة العربية، القاهرة، الطبعة الاولى٢٠٠٤.

١٤. هدى قشوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، الطبعة الأولى دار النهضة العربية، القاهرة، ١٩٩٢.

١٥. يونس، عرب، **دليل أمن المعلومات والخصوصيات (الجزء الأول) جرائم الكمبيوتر والإنترنت**، الطبعة الأولى، اتحاد المصارف العربية، بيروت ٢٠٠٢.

١٦. يونس عرب، **قانون الكمبيوتر**، بيروت: منشورات اتحاد المصارف العربية، ٢٠٠١.

ثانياً: الأبحاث والمقالات وأوراق العمل:

١. جميل، عبد الباقي الصغير، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي**، ٢٥- ٢٨ تشرين أول، ١٩٩٣.

٢. كامل، السعيد، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**، دراسات جنائية معمقة في القانون والفقه والقضاء المقارن، عمان، ٢٠٠٢.

٣. محمد، حسام لطفي، **الجرائم التي تقع على الحسابات أو بواسطتها**، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانوني الجنائي، المنعقد في القاهرة الفترة من (٢٥- ٢٨) أكتوبر (١٩٩٣).

٤. محمد، محي الدين عوض، **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)**، ورقة عمل مقدمة على المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ٢٥- ٢٨، تشرين أول ١٩٩٣.

٥. محمود، صالح العادلي، **الجرائم المعلوماتية: ماهيتها وصورها**، ورقة مقدمة الى ورشة العمل الاقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان، ٢-٤/٤/٢٠٠٦.

٦. هدى، قشقوش، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانوني الجنائي، المنعقد في القاهرة الفترة من (٢٥-٢٨) أكتوبر (١٩٩٣).

٧. ورقة عمل بعنوان "مستقبل صناعة تقنية المعلومات في دول مجلس التعاون الخليجي" مقدمة من الأمانة الفنية لتقنية المعلومات بوزارة الاقتصاد الوطني في سلطنة عمان لمؤتمر الصناعيين التاسع لدول مجلس التعاون الخليجي، ٢٠٠٣.

٨. يونس، عرب، **المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي**، بحث منشور على شبكة الانترنت.

ثالثاً: الرسائل الجامعية:

١. العزام، أحمد حسين، (٢٠٠١)، **الحكومة الإلكترونية في الأردن:** إمكانات التطبيق، رسالة ماجستير، جامعة اليرموك، اربد، الأردن.

٢. المومني، نهلا، ٢٠٠٥، **الجريمة المعلوماتية في قانون العقوبات الأردني**، جـرائم الحاسـوب والإنترنت، رسالة ماجستير، الجامعة الأردنية، كلية الحقوق.

رابعاً: المراجع باللغة الإنجليزية:

1. Clive Gringras, "To Be Great is to be Misunderstood: The Computer Misuse Act 1990" 1997 Computer and Telecommunications Law Review, 3 (5), 213 – 215.
2. Computer Related Crime: Analysis of Legal Policy (Paris, 1986).
3. D.C. Ormerod, Case Comment: Interception of Communications: Meaning of "Control" of the Operation Use of A Private Telecommunications System, [2006] Criminal Law Review 1068-1071.
4. E. Susan Singleton, "Computer Misuse Act 1990 – Recent Developments" 1993 Company Lawyer 14 (1), 22– 23.
5. J.C.Smith, Computer Misuse: Whether Sending An E-mail Which Did not Come from Purported Source Affected the Reliability of Data, Case Comment, [2002] Criminal Law Review 648.
6. John Smith, The Law of Theft, 6th edn 1989.
7. Kelly Stein, "Unauthorized Access and the Computer Misuse Act 1990: House of Lords Leaves no room for Ambiguity" 2000 Computer and Telecommunications Law Review 6 (3), 63–66.
8. Mary W.S. Wong, "Cyber-Trespass and "Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience"15 International Journals of Law and Information Technology 2007, 90.
9. Napier, B; "The Law Commission's Report on Computer Misuse, Journal of Business Law, 1989, 524.
10. Natasha Jarvie, "Control of Cybercrime: Is an End to our Privacy on the Internet a Price Worth Paying? Part 1, Computer and Telecommunications Law Review 20003, 9(3), 76-81.
11. Orin S. Kerr, "Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes', 78 New York University Law Review (2003), 1596.
12. Peter Alldridge, "Computer Misuse Act 199٠" International Banking Law 1990, (9)6, 339 – 342.
13. Robert Sumroy, "Computer Misuse and Data Protection" 1997 Computer and Telecommunication Law Review 4 (5), 119 –120.
14. Rychiicki, Tomasz, "Legal Issues of Criminal Acts Committed Via Botents" Computer and Telecommunications Law Review, 2006 12(5), 161-167.
15. Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for computer Viruses" [1996] 3 Web Journal of Current Legal Issues.