جريمة الدخول غير المشروع للأنظمة المعلوماتية
دراسة مقارنة على ضوء القانون رقم ١٧٥ لسنة ٢٠١٨
بشأن مكافحة جرائم تقنية المعلومات

دكـــــتـــــور

عمر أبو الفتوح عبد العظيم الحمّامى

دكتوراه القانون الجنائى – جامعة القاهرة

مـقدمـة

الحمد لله رب العالمين، الذى علم الإنسان ما لم يعلم، وأسبغ عليه نعمه ظاهرة وباطنة، فله الحمد فى الأولى والآخرة، على جميع آلائه ونعمائه، والصلاة والسلام على المبعوث رحمة للعالمين، سيدنا محمد صلى الله عليه وسلم وعلى آله وصحبه أجمعين، الذى دل أمته على كل خير ونهاها عن كل شر وضير ... وبعد.

١- التطور التقنى إيجاباً وسلباً.

مرت الإنسانية بقفزات حضارية كان من أهمهما اختراع أول حاسب آلي في الولايات المتحدة الأمريكية سنة ١٩٤٦[١]، مروراً بإنشاء شبكة الإنترنت وانتهاءً بمواقع التواصل الاجتماعي مثل الفيسبوك وتويتر واليوتيوب، لذا كثرت النعوت والأوصاف التي أضفاها العلماء والمفكرون على المرحلة الحالية التي يمر بها المجتمع الإنساني، فمنهم من يطلق على هذا العصر، عصر ثورة المعلومات والاتصالات أو عصر المعلوماتية، أو عصر السماوات المفتوحة، أو عصر التكنولوجيا الرقمية أو عصر الإنترنت[٢]، وكل هذه النعوت والأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية والتكنولوجية التي تحققت في شتى مناحي الحياة في الآونة الأخيرة، الأمر الذي دعا بالمفكر الإنجليزي الشهير انتوني جيدنز Anthony Giddens إلى وصف العالم الذي نعيش فيه بأنه «عالم منفلت» Runaway world لا يمكن الإمساك بتلابيبه أو إخضاعه للسيطرة[٣].

---

(١) يعتبر عام ١٩٤٦ علامة بارزة في مجال المعلوماتية ونظم الحاسب، حيث تم في هذا العام اختراع أول حاسب آلى رقمى متكامل في الولايات المتحدة الأمريكية عُرفَ فيما بعد باسم الكمبيوتر، فبزوغ عصر المعلوماتية مرتبط بظهور واختراع الحاسب الآلي. انظر: د. شحاتة غريب محمد شلقامى، برامج الحاسب الآلي والقانون، دار النهضة العربية، سنة ٢٠٠٣، ص أ، د. حسن عبد الباسط جميعى، عقود برامج الحاسب الآلي، دار النهضة العربية، سنة ١٩٩٨، ص٤، وانظر كذلك فى هذا المعنى:

Liu Qian and others: Computer Forensics, Uppsala University, 8 Oct 2007, p.2.

(٢) يصف العديد من رجال الاقتصاد والاجتماع الثورة الحالية للمجتمعات الصناعية بأنها ثورة المجتمعات المعلوماتية، وهي ثورة صناعية ثانية بالمقارنة بالثورة الصناعية الأولي التي تحققت في القرنين ١٩،٢٠، وفي حين كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فإن هدف الثورة الثانية هو إحلال اللآلة محل = = النشاط الذهني للإنسان. انظر: د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية ١٩٩٨، ص٣.

(1) GIddens Anthony: Runaway world: How Globalization is reshaping our lives, London, Profle books, 1999.

- وقد ترجم هذا الكتاب إلى العربية. انتوني جيدنز «عالم منفلت. كيف تعيد العولمة صياغة حياتنا؟» ترجمة د.محمد محي الدين، ميريت للنشر والمعلومات، القاهرة، سنة ٢٠٠٠.

وكانت لهذه الثورة المعلوماتية فوائد عظيمة للإنسان، حيث سهولة التواصل واختصار المسافات وتوفير الوقت والجهد والنفقات، إلا أنه كان لها وجه سلبى آخر تمثل فى الأفعال الإجرامية التى نشأت معها وارتبطت بها، سواء كانت ماسة بشخص الإنسان أو بأمواله[١].

٢- التعريف بموضوع البحث وأهميته.

كانت أولى الأفعال الإجرامية التى ارتبطت بظاهرة المعلوماتية هى أفعال الدخول غير المشروع للأنظمة المعلوماتية، وهذا أمر منطقى وتمليه طبائع الأمور، لأن استخدام هذه الأنظمة يفترض بداءةً الدخول إليها، وهذا الدخول قد يكون مشروع إذا صدر من صاحب الحق فيه أو بإذنه وفى الحدود التى يسمح بها، وقد يكون غير مشروع إذا صدر ممن لا يملك الحق فيه، أو ممن

يملك هذا الحق لكن القائم به يتجاوز الحدود المسموح بها[٢].

وقد تقف الأفعال الإجرامية عند حد الدخول غير المشروع، وهذا فى ذاته كاف للقول بوجود جُرم جنائى[٣]، وقد يتعدى الأمر الدخول بالقيام بأفعال إجرامية أخرى، سواء كانت

---

(٢) يمكن القول بأن المعلوماتية أداة محايدة، قد تستخدم فى الخير وقد تستخدم في الشر، فمصدر سلامتها وقوتها هو الإنسان ذاته، وهو أيضاً مصدر انتهاكها وضعفها، فالمسألة مرتبطة بالإنسان في المقام الأول وشخصيته ودوافعه. انظر: د. محمد سامي الشوا، المرجع السابق، ص٣٣ وما بعدها.

(١) يُقسِّم البعض مجرموا المعلوماتية إلى ثلاث فئات: الفئة الأولى وهدفها النواحى المالية مثل السرقة والاحتيال، والفئة الثانية وتستهدف تعطيل أو إعاقة أجهزة الكمبيوتر أو الشبكات الإلكترونية عن العمل أو إتلاف المعلومات المخزنة بها أو تدمير النظام المعلوماتى ذاته، أما الفئة الثالثة وهى ما تهمنا فى هذا المقام، وهى نوعية خاصة من القراصنة يستهدفون المعلومات الشخصية والحكومية من خلال التجسس الإلكترونى، وتستخدم هذه الفئة في سبيل تحقيق أهدافها الفيروسات وبرامج التجسس والبرمجيات الخبيثة، وتحاول معرفة كلمات سر المستخدمين توصلاً إلى معلوماتهم وبياناتهم الخاصة، وضحايا هذه الفئة لا يقتصرون على كيانات أو أفراد معينين، بل تستهدف أجهزة الكمبيوتر سواء الخاصة بالأفراد أو الشركات أو الحكومات أو الجيش وما تتصل به من مواقع إلكترونية عبر الإنترنت. فى ذلك انظر:

Kristin Westerhorstmann: The Computer Fraud and Abuse Act: Protecting the United States from cyber-attacks, fake dating profiles, and employees who check Facebook at work, Uni. Miami. Nat Sec & Arm Conf. L. Rev,Vol .V, 2015, pp.168-169.

(٢) أوصت اتفاقية بودابست الخاصة بالإجرام المعلوماتى والموقعة في ٢٣ نوفمبر عام ٢٠٠١ في إطار مجلس أوروبا من أجل التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، فى المادة الثانية منها الدول الأعضاء فيها بتبنى تجريم خاص لما أسمته بالولوج غير القانونىAccesillegale والعمدى لكل جهاز الحاسب الآلى أو جزء منه بدون حق بقولها «يجب على كل طرف أن يتبنى التدابير التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبار الولوج العمدي لكل- أو لأى جزء من - جهاز الحاسب الآلى بدون حق جريمة جنائية وفقاً لقانونه الداخلى.... » ، ويجرى نص المادة المشار إليها كما يلى:

«…. Illegal access each party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law when committed intentionally the access to the whole or any part of a computer system without right …. ».=

أفعال تقليدية لكن تستخدم الأنظمة المعلوماتية كوسيلة أو أداة لارتكابها، أو لارتكاب أفعال أخرى تكون هذه الأنظمة وما تحتويه هدفاً لها، فجميع أحوال الجريمة المعلوماتية يسبقها عادة فعل ممهد لها وهو الدخول لهذه الأنظمة(١).

وفى مقام بحثنا سوف نكتفى بدراسة جريمة الدخول غير المشروع والمجرد للأنظمة المعلومانية، والتى لا تُتبع بثمة أفعال أخرى تتضمن المساس بمحتويات النظام المعلوماتى بأى صورة، لأن هذه الأفعال تُشكل جرائم متمايزة عن الجريمة موضوع البحث، وإن كانت هذه الجريمة كما سبق القول عادة ما تسبق هذه الجرائم الأخرى.

وأهمية دراسة هذه الجريمة تكمن فى أن بحثها من الناحية القانونية له أثر هام فى إتاحة أكبر قدر ممكن من الأمن والسلامة للأنظمة المعلوماتية من التسسل إليها والعبث بها، فضلاً عن الدور الوقائى فى حالة تجريمها والعقاب عليها على نحو مجرد فى انحسار مد ما قد يتبعها من جرائم أخرى.

= وهذا أيضاً ما أوجبته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ فى المادة الخامسة منها على الدول أطرافها بتجريم الأفعال التى نصت هذه الاتفاقية على تجريمها، وفقاً لتشريعاتها وأنظمتها الداخلية، وكانت أولى هذه الأفعال ما نصت عليه الفقرة الأولى من المادة السادسة من هذه الاتفاقية، والخاصة بتجريم الدخول غير المشروع والمجرد مع كل أو جزء من تقنية المعلومات أو الاستمرار فيه، وأوجبت الفقرة الثانية من ذات المادة تشديد العقوبات إذا ترتب على الأفعال المشار إليها بالفقرة الأولى: أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة، وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. ب -الحصول على معلومات حكومية سرية. حول هذه الاتفاقية انظر الموقع الإلكترونى:

http://fs8859.0za.in/legislation/HRIDRL0149_ArabConventionCyberCrime_Ar_2010.pdf

(١) قسم البعض جرائم الكمبيوتر إلى قسمين، القسم الأول يشمل الجرائم التقليدية المرتكبة باستخدام أجهزة الكمبيوتر مثل جرائم الغش وألعاب القمار وتوزيع الصور الإباحية عبر الإنترنت، ودور الكمبيوتر في هذا القسم هو تسهيل ارتكاب الجرائم التقليدية، وعلى سبيل المثال فالصور الإباحية كانت توزع وتنشر عن طريق طبعها سواء منفردة أو في شكل مجلة، لكن اليوم يستخدم الكمبيوتر في نشر وتوزيع هذه الصور عبر الإنترنت، فالكومبيوتر في هذه الحالة بمثابة وسيلة جديدة لارتكاب الجريمة التقليدية، أما القسم الثانى فيشمل جرائم إساءة استخدام الكمبيوتر، وهى تمثل نوعاً مستحدثاً من الجرائم، وتطرح تحديات جديدة للقوانين الجنائية، ومثال لهذه النوعية جرائم القرصنة الإلكترونية بأشكالها المختلفة، وجرائم نشر الفيروسات والبرمجيات الخبيثة، وهجمات الحرمان من الخدمة... إلخ. فى ذلك انظر:

Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, L. Rev of N.Y.Uni. School of Law, Vol. 78, Nov 2003, pp.1603-1604; Alden = = Anderson: Comment, The Computer Fraud and Abuse Act: Hacking into the Authorization Debate, 53 Jurimetrics J. (summer 2013), p.450.

٣- خطة البحث.

فى مقام تناولنا لجريمة الدخول غير المشروع للأنظمة المعلوماتية، كان لزاماً علينا أن نجرى بشأنها درسة مقارنة بين التشريع المصرى متمثلاً فى القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، والذى صدر بعد طول غياب، وبين بعض التشريعات الأخرى، وتخيرنا نموذجان من هذه التشريعات هما التشريعان الأمريكى والانجليزى، بوصف الولايات المتحدة الأمريكية المعقل والمهد الأول لظاهرة المعلوماتية، تلتها فى هذا الشأن وبصفة عامة قارة أوروبا، وكانت انجلترا من أوائل دول هذه القارة فى هذا المضمار، وانعكاس ذلك على كونهما من أوائل الدول التى طالتها الجرائم المصاحبة لهذه الظاهرة(١).

وفى هذا الإطار نبحث وضع هذه الجريمة فى ميزان الشرعية الجنائية من خلال معرفة الموقف القانونى فى هذه الدول قبل إصدارها لنصوص أو قوانين خاصة تعالج الأنماط المختلفة للجريمة المعلوماتية، والقوانين التى استحدثتها فى هذا الشأن، مع التركيز عند تناول ذلك على ما يخص جريمة الدخول غير المشروع بوصفها سنام البحث وعماده، ثم نعقب ذلك بدارسة البنيان القانونى لهذه الجريمة من حيث أركانها وعقوبتها.

واتصالاً بما تقدم وترتيباً عليه قسمنا هذا البحث إلى المقدمة التى نحن بصددها، نتبعها بفصلين رئيسيين، نعقبهما بخاتمة نورد فيها أهم نتائج البحث والتوصيات المقترحة فى هذا الصدد، وذلك على النحو التالى.

الفصل الأول: جريمة الدخول غير المشروع فى ميزان الشرعية الجنائية.

الفصل الثانى: البنيان القانونى لجريمة الدخول غير المشروع.

الخاتمة.

---

(١) جدير بالذكر أن ظاهرة الإجرام المعلوماتي شهدت ميلادها عالمياً في أواخر الستينيات من القرن الماضي في الولايات المتحدة الأمريكية ، ثم غزت بعد ذلك أوروبا. انظر: د. محمد سامى الشوا، المرجع السابق، ص ٢٢ =

= أما عن مصر فيمكن القول بأن بدايات ظاهرة الإجرام المعلوماتي بدأت فيها في غضون عام١٩٨٤ بما حدث في أحد فروع بنك مصر، حيث تم التحايل عن طريق استخدام شبكة المعلومات الإلكترونية، وتم اختلاس مبلغ مليون دولار أمريكي وذلك بعملية تمويهية في انتقال البيانات والتحويلات المالية. في ذلك انظر: د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، تقرير مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥ – ٢٨ أكتوبر سنة ١٩٩٣، والمنشور تقاريره بدار النهضة العربية سنة ١٩٩٣، ص ٤٢٥.

الفصل الأول
جريمة الدخول غير المشروع فى ميزان الشرعية الجنائية

٤- تمهيد وتقسيم:

يُعد مبدأ الشرعية الجنائية وبحق أحد المبادئ الرئيسية التى تهيمن على القوانين الجنائية فى مختلف الأنظمة القانونية، إذ لا جريمة ولا عقوبة إلا بنص فى القانون، وينبنى على هذا المبدأ ويتفرع عنه عدة مبادئ أخرى، تتمثل فى أن الأصل فى الإنسان البراءة، والشك يؤول لصالح المتهم، وضرورة التقيد بالتفسير الضيق للنصوص الجنائية.

وإزاء ما أفرزته الثورة التكنولوجية وما صاحبها من أفعال إجرامية مستحدثة، كان على المشرعين الجنائيين فى مختلف الأنظمة القانونية واجب التدخل بإستحداث نصوص تجريمية ملائمة لهذه الجرائم، وعدم الوقوف مكتوفى الأيدى تجاه هذه الأفعال بمحاولة تطويع وتطبيق بعض النصوص التقليدية عليها، إذ أن هذه النصوص قد وضعت لمواجهة الجرائم التقليدية وفي مرحلة سابقة على ظهور هذه الجرائم المستحدثة.

وفى هذا الفصل سوف نبحث الموقف القانونى فى التشريعات محل المقارنة من مسألة مدى ملائمة النصوص التقليدية للتطبيق على هذه الجرائم المستحدثة، والنصوص التجريمية المستحدثة فى هذا المقام، مع تركيزنا على الجريمة محل المقال بوجه خاص وذلك من خلال مبحثين على النحو التالى.

المبحث الأول: الموقف فى ظل النصوص التقليدية.

المبحث الثانى: النصوص المستحدثة فى التشريعات محل المقارنة.

المبحث الأول
الموقف فى ظل النصوص التقليدية

٥- تمهيد وتقسيم:

يُثار التساؤل إزاء موقف الفقه والقضاء فى التشريعات محل المقارنة حول كيفية التعامل مع الأنماط المختلفة للجرائم المعلوماتية بوجه عام، وجريمة الدخول غير المشروع للأنظمة المعلوماتية بوجه خاص قبل إصدارها لنصوص أو قوانين خاصة فى هذا الشأن؟.

نستطيع القول بتمسك واعتصام كل من الفقه والقضاء فى هذه الأنظمة بمبدأ الشرعية الجنائية، ورفضهما لتطبيق النصوص القائمة على هذه النوعية المستحدثة من الجرائم، ويتضح ذلك من إلقاء نظرة على الموقف فى هذه الأنظمة من جريمة الدخول غير المشروع للأنظمة المعلوماتية بوصفها أحد أنماط هذه الجرائم المستحدثة، فضلاً عن كونها موضوع البحث.

وترتيباً على ما تقدم نقسم هذا المبحث لثلاثة مطالب نبين فى كل مطلب منها موقف الفقه والقضاء فى التشريعات محل المقارنة من تطبيق النصوص العقابية التقليدية على هذه الجريمة، وذلك على النحو التالى.

المطلب الأول: الموقف فى الولايات المتحدة.

المطلب الثانى: الموقف فى انجلترا.

المطلب الثالث: الموقف فى مصر.

المطلب الأول
الموقف فى الولايات المتحدة

٦- تمهيد:

أثارت محاولات تطبيق النصوص الجنائية التقليدية على أنماط الجريمة المعلوماتية بوجه عام موجة عارمة من الجدل والانتقادات في الأوساط القانونية بالولايات المتحدة، وبخاصة إزاء تطبيق النصوص الخاصة بالتعدى على ملكية أو ممتلكات الغير على أفعال الوصول أو الدخول غير المشروع لأنظمة الحاسب.

٧- موقف الفقه والقضاء الأمريكيان.

قبل إصدار الولايات الأمريكية لقوانين خاصة بالجرائم الناشئة عن استخدام الحاسب الآلى، رفض الفقه الأمريكى تطبيق النصوص التقليدية على كافة أنماط الجريمة المعلوماتية، وبخاصة تجاه أفعال الدخول غير المشروع للأنظمة المعلوماتية، وذلك لعدم ملائمة هذه النصوص بالتطبيق على هذه الأفعال، تشبثاً بمبدأ الشرعية الجنائية ومقتضياته[١].

وهذا التوجه هو ما اعتنقته المحاكم الأمريكية، فقضت محكمة ولاية مينيسوتا برفض تطبيق مثل هذه النصوص فى دعوى مدنية مقامة من إحدى المؤسسات وتُدعى American Computer trust leasing ضد أحد الأشخاص ويُدعى Jack Farrell، والذى كان يعمل مطور لبرامج الكمبيوتر الخاصة بهذه المؤسسة، ولكنه ولج بغير تصريح إلى أجهزة الكمبيوتر الخاصة بعملاء هذه المؤسسة وعطَّل برامج هؤلاء العملاء، وقررت المحكمة أن نصوص التعدى على ممتلكات الغير في ولاية مينيسوتا تنطبق على الوقائع المادية، والتي لا ينطوى تحتها العناصر المعنوية المخزنة بالكمبيوتر[٢].

كما قضت محكمة الاستئناف بولاية واشنطن الأمريكية ببراءة شخص يُدعى Olsan من تهمة التعدى على ممتلكات الغير، في واقعة تتمثل في حصوله على إذن يقتصر فقط بالدخول على موقع جامعة واشنطن، إلا أنه قام بالحصول على معلومات عن طلاب هذه الجامعة مستخدماً هذه المعلومات في أغراض غير مصرح بها، لكن المحكمة قضت ببراءته مقررةً أن قوانين الحاسب الآلى تُجرم الدخول غير المصرح به، لكن لم تتطرق بالتجريم إلى

(1) Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p.1650.

(1)American Computer Trust Leasing v.Jack Farrell Implement Co., 763 F. Supp. 1473 (D. Minn. 1991).

استخدام ثمار هذا الدخول –الشرعى في هذه الحالة– وبالتالي لا مجال لانطباق نصوص التعدى على ممتلكات الغير(١).

المطلب الثانى
الموقف فى انجلترا

٨– تمهيد:

قبل إصدار المملكة المتحدة لقانون إساءة استخدام الحاسب الآلى سنة ١٩٩٠، وإزاء القلق المتزايد من كثرة التسللات إلى أجهزة الكمبيوتر ووقوف التشريعات القائمة مكتوفة الأيدى لعدم وجود نصوص جنائية تُجرِّم وتعاقب على جرائم الكمبيوتر بكافة صورها، كان لا مناص من محاولة تطبيق النصوص العقابية القائمة على هذه الأفعال، وهنا أدلى كل من الفقه والقضاء الانجليزيين بدلوهما فى هذا الشأن.

٩– موقف الفقه والقضاء الانجليزيان.

رفض الفقه والقضاء الانجليزيان تطبيق النصوص العقابية القائمة مثل النصوص الخاصة بالسرقة، وإتلاف الممتلكات، والتعدى على ممتلكات الغير، وهو ما يُعرف بالأذى الجنائى فى بعض الأنظمة القانونية، على جميع أنماط الجريمة المعلوماتية لتعارضها الصريح مع مبدأ الشرعية الجنائية حيث لا جريمة ولا عقوبة إلا بنص(٢).

ومن أوائل الواقعات التى عُرضت على القضاء الانجليزى فى هذا الشان، واقعة تتلخص فى أنه فى غضون عام ١٩٨٤ تمكَّن كل من Stephen Goldو Robert Schifreen من الدخول المحظور إلى الكمبيوتر الخاص بإحدى خدمات شركة الاتصالات البريطانية التى يطلق عليها Prestel والمعروفة اختصاراً بـ BTs، وذلك لاسترداد معلومات هاتفية خاصة بهما، ووجه الإتهام إليهما بموجب قانون التزوير والتزييف لسنة ١٩٨١، وتم إدانتهما أمام محكمة Southwark Crown Court، والتى قضت بتغريم الأول ٦٠٠ جنيه استرلينى، والثانى٧٥٠ جنيه استرلينى، وباستئنافهما لهذا الحكم قضت المحكمة الاستئنافية

(2) Washington v. Olson, 735 P.2d 1362 (Wash App. 1987).

(1)Mark D. Rasch: Criminal Law and The Internet, The Computer Law Association, Inc (USA).1996 .No.II.

ببراءتهما على أساس عدم وجود نص تجريمى يحكم الواقعة المطروحة إعمالاً لمبدأ الشرعية الجنائية(١).

وفى ذلك أورد اللورد(Lane C.J) القاضي بمحكمة الاستئناف والذى اتفق معه مجلس اللوردات البريطاني في وجهة نظره، من أن حكم الإدانة الصادر من محكمة أول درجة كان محاولة لفرض نصوص قانونية غير مصممة أو مشرَّعة على وقائع الدعوى، فالنبضات الإلكترونية التى شكلت كلمة سر لا ينطبق عليها وصف الأداة المتطلب وفقاً للقسم الأول من قانون التزوير والتزييف لسنة ١٩٨١، بما يتعارض مع مبدأ الشرعية الجنائية، ولذلك ألغت محكمة الاستئناف حكم أول درجة وقضت ببراءة المتهمين(٢).

المطلب الثالث
الموقف فى مصر

١٠ – تمهيد:

تعتبر مصر رائدة للدول العربية فى كثير من المجالات، وبوجه خاص فى مجال التشريعات القانونية، حيث دأبت هذه الدول على أن تستلهم فى تشريعاتها القانونية ما تبنته مصر من تشريعات فى مختلف المجالات، إلا أنه بالنسبة للجرائم التى استحدثتها المعلوماتية بصفة عامة، فقد تخلفت عن ركب هذه الدول(٣)، ولم تُصدر تشريع عام يعالج

(2)David Emm: Cybercrime and the law: a review of UK computer crime legislation, 29 May 2009; Edmand Dester Thipursian and others: Case Study – News of the World Phone Hacking Scandal (NoTW)-Posted in Hacking on April 3, 2014, no.7, this study available online at: http://resources.infosecinstitute.com/case-study-news-world-phone-hacking-scandal-notw;Computer Misuse Act 1990, from Wikipedia, the free encyclopedia, this page was published on (January 2009), and available online at: https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990.

(1) Derek Wyatt and others: Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, June 2004, no.7 ,p.3, this report available online at: http://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf; Stefan Frederick Fafinski: Computer use and misuse: the constellation of control, Ph.D, University of Leeds, Sep 2008, p.33.; Reform of the Computer Misuse Act 1990, Prepared by ICF Legal Subgroup in 30th April 2003, p.4, this study available online at: http://www.internetcrimeforum.org.uk/cma-icf.pdf

(٢) أصدرت جميع الدول العربية تقريباً قوانين خاصة بمكافحة الجرائم المعلوماتية، ومن أمثلة هذه القوانين النظام السعودى لمكافحة جرائم المعلوماتية الصادر بالمرسوم = = الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ، والقانون الاتحادى الإماراتى رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، والذى ألغى القانون الاتحادى رقم ٢ لسنة ٢٠٠٦ والخاص بمكافحة جرائم تقنية المعلومات، وقانون

هذه الجرائم حتى سنة ٢٠١٨، بإصدارها للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات[١]، وكانت مكتفية فى هذا الصدد ببعض التشريعات الخاصة التى تعالج وترتبط ببعض جوانب هذه الظاهرة، مما ولَّد حالة من الفراغ التشريعى[٢].

١١- الفراغ التشريعى المصرى وأثره:

نظراً لهذا الفراغ والسكوت التشريعى من جانب المشرع المصرى قبل إصداره للقانون المار ذكره، كان من المنطقى أن تُطرح عدة أسئلة على بساط البحث، والتى تتمحور حول مدى إمكانية تطبيق بعص النصوص العقابية القائمة على الأنماط المختلفة للجريمة المعلوماتية؟.

وبشأن الجريمة محل البحث فقد ثار التساؤل حول مدى إمكانية تطبيق نص المادة ٣٧٣ عقوبات والتى تنص على تجريم وعقاب « كل من دخل أرضاً زراعية أو فضاء أو مباني أو بيتاً مسكوناً أو معد للسكن أو فى أحد ملحقاته أو سفينة مسكونة أو فى محل معد لحفظ المال، ولم يخرج منه بناء على تكليفه ممن لهم الحق فى ذلك، يعاقب بالحبس مدة لا تجاوز ستة أشهر أو بغرامة لا تجاوز مائتي جنيه» ... وذلك على من« يدخل بطريق غير مشروع ولغرض إجرامي إلى الأنظمة المعلوماتية».

وبشأن هذا التساؤل ذهب بعض الفقه إلى عدم إمكانية تطبيق مثل هذا النص على الفعل المشار إليه، وذلك لعدم اندراج هذا السلوك بالوصف المتقدم تحت عباءة هذا النص[٣]، ونرى رجاحة هذا الرأى، لأن الدخول المعنى وفق نص المادة ٣٧٣ عقوبات هو الدخول المادى، فى حين أن الدخول المقصود للأنظمة المعلوماتية هو الدخول الفنى لهذه النظم عن طريق ضرب رموز شفرية معينة كالأكواد وكلمات السر.

كما نرى مع البعض الآخر أن النص الخاص بالجريمة المنصوص عليها في المادة ٣٢٤ من قانون العقوبات، والتي تعاقب على تقليد مفاتيح أو التغيير فيها أو وضع آلة ما وتوقع استعمال ذلك في ارتكاب جريمة لا محل لتطبيقه ... على ما إذا اقتضى الولوج أو

مكافحة جرائم تقنية المعلومات العمانى رقم ١٢ لسنة ٢٠١١، وقانون مكافحة جرائم تقنية المعلومات البحرينى رقم ٦٠ لسنة ٢٠١٤، وقانون مكافحة الجرائم الإلكترونية الأردنى رقم ٢٧ لسنة ٢٠١٥، وقانون مكافحة جرائم تقنية المعلومات الكويتى رقم ٦٣ لسنة ٢٠١٥، ومن الجدير بالذكر أن جل هذه القوانين قد استلهمت نصوصها من النصوص الواردة بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ والسابق الإشارة إليها.

(١) المنشور بالجريدة الرسمية العدد ٣٢ مكرر (ج) فى ١٤ أغسطس سنة ٢٠١٨.

(٢) مثل قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤.

(١) د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، سنة١٩٩٢، ص٢٤٦.

الدخول غير المشروع للأنظمة المعلوماتية استنساخ مفاتيح ورموز للوصول إلى النظام أو التغيير فيها بما يسمح باستعمالها في الوصول إلى أنظمة أخرى مشابهة في التصميم، ذلك أن المفتاح في مجال المعلوماتية ذات طبيعة تقنية وتكنولوجية كالبطاقة الممنغنطة والرقم السرى، وليس هو المفتاح الذي يستخدم في فتح الأقفال ومغاليق الأبواب(١).

وقد يُقال أن المشرع لم يُحدد أن يتم التقليد لهذه المفاتيح أو التغيير فيها بقصد ارتكاب جريمة معينة بالذات وهي السرقة، إلا أنه يمكن الرد على ذلك، بأن الفقه مُجمع على أن الجريمة المقصودة في هذه المادة(٣٢٤ع) هى السرقة أو إحدى الجرائم الملحقة بها، مثل اختلاس الأموال المحجوز عليها أو المرهونة.

ويمكن تبرير ذلك بأن النص ورد في باب السرقة، وجاءت عقوبة الجريمة المنصوص عليها فيه مساوية لعقوبة السرقة، ولو كان قصد الشارع أن يكون النص عاماً لوضعه ضمن الأحكام العامة في الكتاب الأول، كما فعل عندما رأى المعاقبة على إخفاء الأشياء المتحصلة من جناية أو جنحة أياً كانت، ولذلك فمن المتفق عليه أن الفاعل لا يؤاخذ إلا إذا كان يتوقع استعمال المفتاح أو الآلة في سرقة أو في جريمة من الجرائم الملحقة بها كاختلاس الأشياء المحجوز عليها أو المرهونة(٢).

وخلاصة ذلك أن النصوص العقابية العامة القائمة غير كافية لحماية الأنظمة المعلوماتية من أفعال الدخول غير المشروع أو الغير مصرح به من قبل، هذا من ناحية القواعد العامة، لكن من جهة التشريعات الخاصة نجد أن المشرع المصري في قانون الأحوال المدنية الرقيم ١٤٣ لسنة ١٩٩٤ قد جرَّم في المادة (٧٦) منه أفعال اختراق أو محاولة اختراق سرية المعلومات والبيانات الخاصة بمصلحة الأحوال المدنية، فى إطار العلاقة التى أنشأها بهذا القانون بين بيانات ومعلومات مصلحة الأحوال المدنية والأنظمة الآلية لمعالجة المعلومات، لكن رغم ذلك يظل نص المادة (٧٦) يبسط حماية خاصة على أنظمة الحاسبات الآلية المتضمنة لبيانات ومعلومات الأحوال المدنية، ولا تمتد إلى غيرها، فهذا القانون بمثابة تشريع خاص وضع لتقرير الحماية القانونية للمعلومات والبيانات والإحصاءات المجمعة الخاصة بالمواطنين والمخزنة بالحاسبات الآلية لمصلحة الأحوال المدنية.

(٢) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، سنة ١٩٩٩، ص١٤٠.

(١) د. محمود محمود مصطفى، شرح قانون العقوبات – القسم العام، مطبعة جامعة القاهرة – الطبعة العاشرة ١٩٨٣، ص ٥٢٥.

المبحث الثانى
النصوص المستحدثة فى التشريعات محل المقارنة

١٢- تمهيد وتقسيم:

كان من نتيجة رفض الفقه والقضاء فى التشريعات محل المقارنة تطبيق النصوص العقابية التقليدية على هذه النوعية المستحدثة من الجرائم، أن ولَّد دافع لمشرعى هذه الدول لإصدار نصوص أو قوانين خاصة تلائم هذه النوعية من الجرائم صوناً لمبدأ الشرعية الجنائية.

وفى هذا المبحث سوف نبرز النصوص التجريمية المستحدثة والتى رصدتها التشريعات محل المقارنة تجاه أفعال الدخول غير المشروع للأنظمة المعلوماتية، تاركين التعليق على ما جاء بها عند تناولنا للبنيان القانونى لهذه الجريمة فى الفصل الثانى من هذا البحث، وترتيباً على ذلك سوف نقسم هذا المبحث إلى ثلاثة مطالب على النحو التالى.

المطلب الأول: النصوص المستحدثة فى الولايات المتحدة.

المطلب الثانى: النصوص المستحدثة فى انجلترا.

المطلب الثالث: النصوص المستحدثة فى مصر.

المطلب الأول
النصوص المستحدثة فى الولايات المتحدة

١٣- تمهيد:

تُعد الولايات المتحدة الأمريكية بلا منازع مهد المعالجة الآلية للمعلومات، إذ أنها الدولة حائزة قصب السبق فى اختراع الحاسب الآلى، فضلاً عن التزايد المضطرد بها فى عدد مستخدميه ومستخدمى خدمات الإنترنت(١)، ونتيجة لذلك كانت أُولى الدول التى اجتاحتها الجرائم المعلوماتية على اختلاف انواعها، ومُنىَّ اقتصادها بخسائر فادحة من جرَّاء هذه الجرائم(٢).

(١) فى دراسة لمكتب الإحصاء الأمريكى (The US. Census Bureau) سنة ١٩٨٤ انتهت إلى أن ٨.٢% من الأسر الأمريكية لديها جهاز كمبيوتر منزلى، ونسبة ٥٩% من هؤلاء المستخدمين كانوا لا يزالون يتعلمون كيفية استخدامه والعمل عليه، وفى دراسة ثانية لذات المكتب سنة ٢٠١٢ أشارت إلى أن نسبة ٧٨.٩ % من الأسر الأمريكية أصبح لديها جهاز كمبيوتر منزلى، ونسبة ٩٤.٨% من هؤلاء المستخدمين لديهم اتصالات بالإنترنت، بالإضافة إلى أن نصف جميع الأمريكيين الذين بلغوا ٢٥ سنة فأكثر لديهم هواتف ذكية محمولة ومتصلة بالإنترنت. في ذلك انظر:

Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, NC. J.L & TECH 2014, p.212.

- في حين قدرت بعض الدراسات الأخرى من يستعملون أجهزة الكمبيوتر في الولايات المتحدة عام ١٩٨٦ بنسبة ٨.٢% فقط، وخدمة الإنترنت في هذا الوقت لم تكن متاحة للعامة، بل كانت تقتصر فقط على وزارة الدفاع الأمريكية والحكومة الاتحادية وبعض المؤسسات الأكاديمية، في حين أنه في عام ٢٠١٥ فقد وصلت نسبة من يستخدمون الكمبيوتر بها ٨٤% و٧٣% منهم يستخدمون الإنترنت، فضلاً عن الجودة الغير مسبوقة في كفاءة أجهزة الكمبيوتر المستخدمة حالياً، والتى قابلها تطور في أساليب ارتكاب الجرائم المعلوماتية. فى ذلك انظر:

Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, p.150.

- وفى إحصائية أخيرة أشارت إلى وصول عدد مستخدمى الإنترنت بالولايات المتحدة سنة ٢٠١٨ لنحو ٢٧٤.٨ مليون مستخدم بنسبة حوالى ٨٣% من مجموع = = السكان، ومن المتوقع وصول هذا الرقم لنحو ٢٨٣.٥ مليون مستخدم فى عام ٢٠٢٢. فى ذلك انظر:

An statistic about number of internet users in the United States from 2015 to 2022, this statistic available online at: https://www.statista.com/statistics/325645/usa-number-of-internet-users/

(١) في سنة ٢٠٠١ أُجرىَ مسح بمعرفة المباحث الفيدرالية الأمريكية FBI بالاشتراك مع معهد أمن الكمبيوتر Computer Security Institute وخلُص هذا المسح إلى أن الخسائر السنوية للجرائم المعلوماتية تُقدر بمليارات الدولارات، وضرب مثال على ذلك بالخسائر الناشئة عن فيروس الحب (I Love You) والذى انتشر في جميع أنحاء العالم في مايو ٢٠٠٠ والتى قُدرت بنحو ١٠ مليار دولار. انظر:

Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p.1605.

- وأشارت بعض التقديرات في سنة ٢٠١٣ إلى أن الخسائر الإجمالية العالمية للجرائم المعلوماتية عموماً وصلت لترليون دولار أمريكى. انظر:

Alden Anderson: Comment, The Computer Fraud and Abuse Act, P.R, p.484.

وإزاء رفض كل من الفقه والقضاء الأمريكيان تطبيق النصوص العقابية التقليدية القائمة على كافة أنماط الجريمة المعلوماتية على النحو المشار إليه، بدأت على الفور المجالس التشريعية في الـ ٥٠ ولاية بسن نصوص جنائية جديدة تتلائم مع هذا النوع المستحدث من الإجرام، وكانت أول ولاية أمريكية في هذا الشأن ولاية فلوريدا سنة ١٩٧٨، وآخر ولاية كانت فيرمونت سنة ١٩٩٩، وفي أثناء هذه الفترة وتحديداً سنة ١٩٨٤ أصدر المشرع الاتحادى الأمريكى قانون جرائم الكمبيوتر الاتحادى، والذى حل محله قانون الغش وإساءة استخدام الكمبيوتر الاتحادى لسنة ١٩٨٦،1986 Computer Fraud and Abuse Act والمعروف اختصاراً بـ CFAA، وقد أُدخلت عدة تعديلات على قانون١٩٨٦ أعوام ١٩٩٠، ١٩٩٤، ١٩٩٦، ٢٠٠١، وآخرها سنة ٢٠٠٨[١].

ويرى البعض أن قوانين بعض الولايات في سبيل إسباغها للحماية على الأنظمة المعلوماتية جاءت بصورة أوسع وأشمل من القانون الاتحادى[٢].

وفيما يلى نبذة عن الموقف القانونى لبعض الولايات الأمريكية، وكذلك موقف المشرع الإتحادى الأمريكى من جريمة الدخول غير المشروع للأنظمة المعلوماتية، مع تركيزنا على ما جاء بالقانون الاتحادى بوصفه يمثل الجانب المقارن للتشريع الأمريكى فى موضوع البحث الراهن.

- وفيما يخص الجريمة محل البحث فقد صدرت إحصائية عن فريق عمل الحاسب فى جامعة كارنيجى عام ١٩٩٤، خلصت إلى أنه فيما بين أعوام ١٩٩١ إلى ١٩٩٤ كان هناك تصاعداً خطيراً فى جرائم الاختراق والدخول غير المشروع وصل إلى ٤٩.٨% بالقياس إلى عام ١٩٩١، مشيرة أيضاً إلى أنه خلال هذه الفترة كان هناك أربعون ألف قد جهاز انتهكت فى ٢٦٤٠ حادثة. فى ذلك انظر:

  Federal guide lines for searching and seizing computers, available online at: http://www.usdoj.gov/criminal/cybercrime/searachdocs/toc.html

- وفى ولاية كارولاينا الشمالية سنة ٢٠٠٣ نجحت شرطة هذه الولاية فى القبض على حدث بعمر ١٥ سنة، والذى اتهم بتعمد تدمير أنظمة تشغيل الحاسبات الخاصة بأكبر المؤسسات المالية، حيث نجح فى كسر تشفير الوسائل الأمنية الخاصة بحاسباتها ودمر عدة برامج خاصة بها وبرامج أمنية خاصة بالحاسبات، ولم يكتفِ بذلك بل = = أطلق أحد الفيروسات الذى اخترق السجلات المالية والحساسة لهذه المؤسسة، كما حذف آلاف الملفات الخاصة بصفقات هذه المؤسسة. فى ذلك انظر:

  Yearwood Douglas L:Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys, May 2003, p.1, this study published by North Carolina Governor's Crime Commission and available online at:

  http://www.ncgccd.org/PDFs/Pubs/NCCJAC/cybercrime.pdf

(1) Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, pp. 1615 – 1616.

(2) Mark D. Rasch: Criminal Law and The Internet, P.R, pp.12-14.

١٤- موقف بعض مشرعى الولايات الأمريكية من جريمة الدخول غير المشروع.

فى هذا المقام سوف نعرض لموقف بعض مشرعي الولايات الأمريكية من جريمة الدخول غير المشروع للأنظمة المعلوماتية، ونماذج قضائية فى هذا الشأن، إذ أن المقال لا يتسع لعرض موقف مشرعى الـ ٥٠ ولاية من هذه الجريمة.

وبداءةً فقد أشار البعض إلى أن نقطة الانطلاقة فى التجريمات المتنوعة التى تندرج تحت وصف إساءة استخدام الحاسب الآلى سواء فى قوانين الولايات أو فى القانون الاتحادى تنبع من تجريم الدخول غير المصرح به أو تجاوز التصريح الممنوح بالدخول(١).

ومن أمثلة مشرعى الولايات الأمريكية فى هذا الشأن ما جرَّمه وحظره قانون العقوبات في ولاية كنساس الأمريكية فيما يخص جرائم الكمبيوتر والمعدل بالقانون رقم ٢١-٣٧٥٥ لسنة ٢٠٠٠ في الفقرة (ب) من المادة الأولى من تجريم الوصول العمدى للكمبيوتر أو الشروع في ذلك بقصد تعديل أو تغيير أو إتلاف أو نسخ أو الكشف عن البرامج والمعلومات المخزنة داخله أو الاستيلاء على جهاز الكمبيوتر أو نظامه المعلوماتى أو شبكته أو على أى أشياء أخرى يترتب عليها حدوث ضرر(٢).

وكذلك ما نص عليه قانون العقوبات في ولاية جورجيا(٣) بأن «الشخص يكون مرتكباً لجريمة التعدى على الكمبيوتر، إذا قام باستخدام جهاز كمبيوتر أو شبكة كمبيوتر مع علمه بأن هذا الاستخدام دون تصريح بقصد:

١- الحذف أو الإزالة بأى طريقة لبرنامج كمبيوتر أو بيانات من جهاز كمبيوتر أو من شبكة كمبيوتر سواء بشكل دائم أو مؤقت.

---

(1) Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, pp. 1615 – 1616; Mark D. Rasch: Criminal Law and The Internet, P.R, p.17.

(2) Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p. 1625.

(1)The relevant statute reads «Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (A) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network; (B) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or (C) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass».

٢- عرقلة أو تعطيل أو التدخل بأى طريقة فى استخدام برنامج أو بيانات كمبيوتر.

٣- الإتلاف أو التغيير بأى طريقة بما يتسبب في حدوث خلل لجهاز الكمبيوتر أو شبكته أو لبرنامج كمبيوتر، وبغض النظر عن مدة هذا الإتلاف أو التغيير أو التعطيل».

وينص قانون ولاية واشنطن الخاص بجرائم الحاسب الآلى والمعدل سنة ٢٠٠٠ في المادة 9A.52.100(1) على أن[١]«الشخص يُعد مرتكباً لجريمة التعدى على الكمبيوتر من الدرجة الأولى، إذا كان قد ولج عمداً وبدون إذن إلى نظام الكمبيوتر أو قاعدة بيانات إلكترونية لآخر و:

١- يكون الولوج بقصد ارتكاب جريمة أخرى... أو،

٢- ينطوى الولوج على انتهاك للكمبيوتر أو قاعدة بيانات محفوظة لدى وكالة حكومية».

ومن النماذج القضائية فى هذا الشأن ما قضت به محكمة ولاية واشنطن بإدانة أحد أفراد الشرطة ويُدعى Olson وذلك لولوجه للكمبيوتر الخاص بشرطة هذه الولاية دون تصريح، وقيامه باستخدام قاعدة بيانات هذا الكمبيوتر وطباعة صور رخص القيادة الخاصة بطالبات جامعة واشنطن[٢].

وما قضت به كذلك محكمة ولاية جورجيا بإدانة شخص يُدعى Fugarino، والذى كان يعمل مبرمج كمبيوتر في إحدى الشركات، وعند علمه بتوظيف مبرمج آخر مكانه قام بحذف برامج ومعلومات كثيرة من الكمبيوتر الخاص بالشركة، مما سبب لها أضراراً كثيرة، وذلك انتقاماً ونكاية في صاحب العمل[٣]، ويعلق البعض على هذا الحكم بالقول بأن المخالفة الأولى المنسوبة لـ Fugarino هى تجاوزه للإذن أو التصريح الممنوح له بالدخول، لأن الإذن أو التصريح بالدخول لا يشمل حذف البرامج والمعلومات[٤].

---

(2) Wash. Rev. Code Ann. § 9A.52.110 (1) reads «A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another; and (A)The access is made with the intent to commit another crime; or (B)The violation involves a computer or database maintained by a government agency».

(1) State. v Olson, 735 P.2d 1362 (Wash. Ct. App. 1987).

(2) State. v Fugarino, 531 S.E.2d 187 (Ga. Ct. App. 2000).

(3) Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p. 1635.

١٥- موقف المشرع الاتحادى الأمريكى من جريمة الدخول غير المشروع.

تضمن التشريع الاتحادي federal legislation لكود الولايات المتحدة في القسم رقم ١٨ منه الجرائم والإجراءات الجنائية ذات الصلة «Chapter 18.procedure crimes and criminal »، والذى أُدرجت فيه الجرائم المتعلقة بالغش وإساءة استخدام الكمبيوتر والواردة بالقانون الصادر سنة ١٩٨٤ والذى تم تعديله تماماً بالقانون الصادر سنة ١٩٨٦على النحو المار ذكره.

واشتملت المادة«١٠٣٠» من هذا القسم على الأحكام الخاصة بالاحتيال وعلاقته بالاتصال مع الحاسبات، ورأس التجريمات المختلفة التى تضمنتها هذه المادة - كما سبق القول - هو تجريم الدخول أو الولوج غير المشروع إلى الكمبيوتر، وتضمنت الفقرة الأولى من هذه المادة سبعة بنود لا يخلو أى بند منها من ذكر الدخول غير المشروع للكمبيوتر أو تجاوز الدخول المصرح به، وهذه البنود تتضمن تجريم:

١- كل من تعمد الولوج إلى جهاز الكمبيوتر بدون تصريح أو تجاوز الولوج المصرح به، وكان من نتيجة هذا الفعل الحصول على معلومات محددة بمعرفة حكومة الولايات المتحدة بموجب قانون أو أمر تنفيذى، يقضى بالحماية من الإفشاء غير المصرح به لأسباب تتعلق بالأمن القومي للولايات المتحدة الأمريكية أو علاقاتها بالدول الأخرى، أو أي بيانات خاصة على النحو الوارد في الفقرة (ذ) من القسم رقم «١١» من تشريع وكالة الطاقة الذرية لسنة١٩٥٤، وكان الهدف من ذلك الإضرار بالولايات المتحدة الأمريكية أو تحقيق ميزة لدولة أجنبية[١].

(1)Subsection 1030(A/1)« Whoever Having knowingly accessed a computer without authorization or exceeding = = authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it».

٢- كل من تعمد الولوج إلى الكمبيوتر بدون تصريح أو تجاوز الولوج المصرح به بقصد الحصول على[١]:

(أ) معلومات واردة بالسجل المالي لأي مؤسسة مالية، أو لإصدار بطاقة على النحو الوارد بالقسم رقم ١٦٠٢ (N) من الفصل «١٥»، أو حصل على ملف لأحد العملاء أو تقرير يخص عميل على النحو الوارد في تشريع الائتمان رقم ١٥ يو أس سي ١٩٨١.

(ب) معلومات من أى إدارة أو وكالة تابعة للولايات المتحدة، أو

(جـ) معلومات من أي كمبيوتر محمى.

٣- تعمد الولوج بدون تصريح إلى أى كمبيوتر غير عام عن طريق إدارة أو وكالة تابعة للولايات المتحدة، وكان الولوج لهذا الكمبيوتر من هذه الإدارة أو الوكالة يقتصر استخدامه على حكومة الولايات المتحدة، أو لا يقتصر عليها، ولكن يؤثر هذا السلوك على استخدام الكمبيوتر الحاصل بمعرفة أو من أجل حكومة الولايات المتحدة[٢].

٤- تعمد بنية الاحتيال الولوج إلى كمبيوتر محمي بدون تصريح، أو تجاوز الولوج المصرح به، للحصول على أى شيء له قيمة، مالم يكن الغرض من الاحتيال والشيء الذى تم الحصول عليه، يقتصر فقط على استخدام الكمبيوتر، وكانت قيمة هذا الاستخدام لا تتجاوز ٥٠٠٠ دولار فى السنة[٣].

---

(1) Subsection 1030(A/2) «Intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains: (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting (Act 15 U.S.C. 1981 et seq.); (B)Information from any department or agency of the united states. or; (C) Information from any protected computer».

(1) Subsection 1030(A/3) «Intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, access such a computer of that department or agency that is exclusively for the use of the Government of the United states or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States».

(2)Subsection 1030(A/4) «Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than 5000 $ in any one -year period».

٥- عقاب كل من[١]:

(١) تسبب عن قصد فى إحداث أضرار بكومبيوتر محمى عن طريق إرسال برنامج أو معلومات أو أكواد أو أوامر.

(٢) تعمد الولوج إلى جهاز كمبيوتر محمي دون تصريح، ونتيجة لهذا السلوك يتسبب برعونة فى حدوث ضرر:

(أ) لشخص أو أكثر، خلال فترة سنة أو محاولة ذلك، أو كانت المعلومات التي توصل إليها تتصل بأغراض التحقيق والمحاكمة المتعلقة بحدث داخل الولايات المتحدة، أو إذا ترتب على السلوك المرتكب أضرار واقعة على جهاز أو أجهزة كمبيوتر محمية تجاوز قيمتها خمسة آلاف دولار U.S.D، أو تسبب في الإضرار بعشرة أجهزة كمبيوتر محمية أو أكثر خلال فترة سنة.

(ب) إذا ترتب على السلوك المرتكب تعديل أو إفساد وقع فعلاً أو محتمل وقوعه بالنسبة لفحص طبي أو تشخيص أو علاج أو رعاية لفرد أو أكثر، أو أي إصابة جسدية لأي شخص تهدد السلامة والصحة العامة.

(جـ) الأضرار التي تؤثر على نظام الكمبيوتر المستخدم من قبل أو لصالح كيان حكومي، والمتعلق بالعدالة والدفاع والأمن القومي.

---

(3)Subsection1030(A/5) «(1)Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to protected computer. (2)Intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage: = = (A)caused (or, in the case of an attempted, would, if completed, have caused. lass to 1 or more persons during any 1 -year period (and for purpose of an) investigation, prosecution or other proceeding brought by united states only, lass resulting from related course of conduct affecting 1or more other protected computer aggregating at least U S D 5000$ in value or Caused a damage affecting 10 or more protected computers during any 1-year period. (B)The modification or impairment or potential modification or impairment, of the medical examination, diagnosis, treatment or care of, 1 or more individuals - physical injury to any person a threat to public health or safety. (C)Damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defenses or security».

٦- كل من تعمد الاحتيال بالإتجار- كما هو محدد فى المادة ١٠٢٩- فى أى كلمة مرور- سر-[١] أو معلومات مشابهة، يمكن من خلالها الولوج بدون تصريح إلى جهاز الكمبيوتر إذا كان[٢]:

(أ) هذا الإتجار يُؤثر على التجارة المتبادلة بين الولايات، أو التجارة الخارجية، أو،

(ب) هذا الكمبيوتر يُستخدم بمعرفة حكومة الولايات المتحدة أو من أجلها[٣].

٧- كل من توافرت لديه نية ابتزاز أي شخص، للحصول منه على أموال أو شيء آخر ذى قيمة، بهدف التأثير في العلاقات التجارية بين ولايتين أو مع دولة أجنبية، عن طريق أى اتصال يحتوى على[٤]:

---

(١) المادة (١٠٢٩) من القانون الاتحادى الأمريكى خاصة بالاحتيال والنشاط ذو الصلة بالولوج للكمبيوتر Fraud and related activity in connection with access devices، وقد عرَّف البند الخامس من الفقرة الرابعة من المادة المشار إليها مصطلح الإتجار بأنه «يعنى التنازل، أو التصرف بطريقة أخرى لآخر، أو السيطرة بنية النقل أو التصرف».

Subsection 1029(D/5) «The term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of».

(2) Subsection 1030(A/6) «Knowingly and with the intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization if: (a) Such trafficking affects interstate or foreign commerce; or (b) Such computer is used by or for the government of the United States».

(٣) قُدمت عدة اقتراحات من جانب البيت الأبيض لتعديل البند السادس المشار إليه، وكان الهدف من هذه الاقتراحات توسيع دائرة التجريم بعدم اشتراط أن ينتج عن الولوج غير المشروع التأثير في التجارة المتبادلة، أو التأثير في جهاز الكمبيوتر المحمى الذى تستخدمه الولايات المتحدة، بما مفاده توسيع نطاق جريمة الاتجار بكلمات السر الواردة في هذا البند، لكن لم يتم إقرار هذه الاقتراحات تشريعياً من جانب الكونجرس الأمريكى. انظر: =

= Eric A. Fischer: Federal Laws Relating to Cyber security: Overview and Discussion of Proposed Revisions, CRS 7-5700, June 20, 2013, p.33.

(1)Subsection 1030(A/7) «With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any: (A) Threat to cause damage to a protected computer;(B)Threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) Demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion».

(أ) التهديد بإتلاف جهاز كمبيوتر محمى،

(ب) التهديد بالحصول على معلومات من جهاز كمبيوتر محمي دون تصريح أو بتجاوز التصريح الممنوح، أو بإضعاف سرية المعلومات التى تم الحصول عليها من كمبيوتر محمى دون الحصول على تصريح بالولوج أو بتجاوز التصريح الممنوح بالولوج، أو

(جـ) طلب المال أو أي شيء آخر ذو قيمة، وفيما يتعلق بالضرر الذى لحق بالكمبيوتر المحمي، فإن هذا الضرر تسبب فى تسهيل الابتزاز.

المطلب الثانى
النصوص المستحدثة فى انجلترا

١٦- تمهيد:

احتلت قارة أوروبا بصفة عامة المركز الثانى فى استخدام الحاسبات الآلية والإنترنت بعد الولايات المتحدة الأمريكية[١]، وكانت المملكة المتحدة من طليعة دول هذه القارة فى هذا الشأن، وانعكس ذلك ليس على واقعية الجرائم المعلوماتية بها فحسب[٢]، بل على استفحالها وتضخم الخسائر الناشئة عنها[٣].

وإزاء موقف الفقه والقضاء بها والرافضان لتطبيق النصوص العقابية التقليدية على هذه النوعية الإجرامية المستحدثة، أصدر المشرع الانجليزى قانون إساءة استخدام الحاسب الآلى

(١) تُعد الصين الآن هى الدولة صاحبة المركز الأول عالمياً فى استخدام الحاسبات الآلية وخدمات الإنترنت، نظراً لكونها الدولة الأكثر سكاناً فى العالم والذى اقترب من المليار والنصف فى عام ٢٠١٨، فضلاً عن التطور التكنولوجى الهائل بها والذى يضاهى الدول المتقدمة من أمثال الولايات المتحدة والدول الأوروبية واليابان.

(٢) جاء فى تقرير اللجنة الخاصة لدراسة جرائم الحاسب الآلى فى المملكة المتحدة، والمعروفة بلجنة أوديت«Audit » والتي كانت مُشكَّلة من مستشاري الأمن العاملين في حقل الكمبيوتر، أن هناك ثلاثاً وسبعين محاولة غش كمبيوتر حققت خسائر قدرها ١.١ مليون جنيه إسترليني خلال الفترة من عام ١٩٨٧ إلى عام ١٩٩٠. انظر:

The recommandation No R (89- 9) adopted by the council of ministers on 12 September 1989, p.28.

(٣) فى سنة ١٩٩٠ وأثناء مناقشة مشروع قانون إساءة استخدام الحاسب الآلى الانجليزى، قدر مقدموا المشروع الخسائر الناجمة سنوياً من وراء أفعال إساءة استخدام الحاسب الآلى بنحو يتراوح ما بين ٤٠٠ مليون جنيه استرلينى إلى ٢ مليار جنيه استرلينى، وفى تطور لحجم الخسائر قدرت وزارة الداخلية البريطانية سنة ٢٠٠٦ أن أعمال القرصنة الإلكترونية بالإضافة إلى هجمات الحرمان من الخدمة خسائرها أكثر من ٣ مليار جنيه استرلينى سنوياً. فى ذلك انظر:

Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, pp.37, 74.

لسنة ١٩٩٠، Computer Misuse Act 1990، والذى دخل حيز النفاذ فى أغسطس ١٩٩٠[١].

ويرى البعض أن المصلحة الأولى المستهدفة بالحماية فى قانون ١٩٩٠هى أمن وسلامة نظم الكمبيوتر، وأن حماية هذا القانون للبرامج والبيانات والمعلومات المخزنة داخل الكمبيوتر من مخاطر الإتلاف أو التغيير هى حماية غير مباشرة، بل ذهب إلى أبعد من ذلك بالقول بأن التعدى على الممتلكات الغير مادية أساس المسئولية بشأنه مسئولية مدنية، فهذا القانون لم يجرم القرصنة أو الدخول غير المشروع بقصد ارتكاب جريمة بل جرَّم مجرد الدخول غير المشروع من الأساس[٢].

١٧- النصوص التجريمية المستحدثة بموجب قانون١٩٩٠.

وُضع قانون إساءة استخدام الكمبيوتر لسنة ١٩٩٠ في القسم الثامن عشر chapter 18 من قانون العقوبات الانجليزى من خلال ثلاث مواد رئيسية، أُضيفت إليها مادة رابعة بموجب التعديل الذى أدخله قانون الشرطة والعدالة لسنة ٢٠٠٦ على قانون ١٩٩٠.

ولما كان موضوع البحث الراهن يرتكز حول جريمة الدخول غير المشروع للأنظمة المعلوماتية، فليس بذى أهمية أن نُركِّز على المادتين الثالثة والرابعة من هذا القانون، وذلك لعدم تعلقهما بالجريمة محل المقال، وإن كان ذلك لا يمنع من الطواف حولهما، حتى يستقيم القول بصلتهما بموضوع البحث من عدمه.

فالمادة الثالثة تحظر التبديل أو التعديل العمدى فى مواد الكمبيوتر، عن طريق إعاقة تشغيل الكمبيوتر، أو منع أو إعاقة الوصول إلى أى برنامج أو بيانات مخزنة فى جهاز الكمبيوتر، أو منع أو إعاقة تشغيل عمل البرامج أو التشكيك فى صحة أية بيانات أياً كان

(1)The Hacking of Computers and the Criminal Law, an article written by selected team of legal experts, this article available online at:
http://www.inbrief.co.uk/offences/hacking-of-computers.htm; Relevant Penetration Testing Legislation in the UK, published on Tuesday, 3 April 2012, and available online at:
http://rewtdance.blogspot.com/2012/04/relevant-penetration-testing.html

(2)Neil Mac Ewan: The Computer Misuse Act 1990: lessons from its past and predictions for its future, Crim. L.Rev 2008, pp.956-958.

نوعها، ولا يشترط لقيام هذه الجريمة أن توجه الأفعال محل التجريم إلى جهاز كمبيوتر معين، أو إلى برنامج أو بيانات معينة أو من أى نوع[١].

أما المادة الرابعة[٢] المضافة بموجب التعديل الذى أدخله قانون الشرطة والعدالة لسنة ٢٠٠٦ على قانون ١٩٩٠، فخُصصت لحظر وتجريم صنع أو تجهيز أو توريد أو الحصول على مواد أو برامج بغرض استخدامها في ارتكاب أى جريمة من جرائم إساءة استخدام الحاسب الآلى الواردة في قانون ١٩٩٠[٣].

ولا يبقى والحال كذلك إلا المادتين الأولى والثانية من قانون ١٩٩٠، واللتان تتعلقان بجريمة الدخول غير المشروع، مما يستدعى التعرض لما ورد بهما على النحو التالى.

---

(١) بقيام المشرع الانجليزى بتعديل قانون إساءة استخدام الحاسب الآلى لسنة ١٩٩٠ بموجب قانون الشرطة والعدالة لسنة ٢٠٠٦ - Police and Justice Act 2006 (PJA)، وبمناسبة هذا المادة الثالثة تحديداً فقد أصابها تعديل بموجب القانون المذكور من ناحيتين هما: الأولى: أضحت عقوبة مخالفة هذه المادة السجن لمدة لا تتجاوز عشرة سنوات والغرامة أو إحدى هاتين العقوبتين، بعدما كانت قبل التعديل السجن لمدة لا تتجاوز خمس سنوات والغرامة أو إحدى هاتين العقوبتين، استجابة من المشرع لدعوات تشديد العقوبات الواردة في قانون ١٩٩٠، لتحقيق أكبر قدر من الردع بنوعيه العام والخاص، خاصة بعد زيادة نسبة هذه الجرائم والابتكار والتنوع في أساليب ارتكابها والأضرار الناجمة عنها. أما الناحية الثانية: فتم تعديل مسمى هذه المادة من التعديل والتبديل المحظور في مواد الكمبيوتر إلى القيام بأعمال غير مصرح أو مرخص بها عمداً أو عن طريق الرعونة لإتلاف أو إضعاف عمليات تشغيل الكمبيوتر. فى ذلك انظر:

David Emm: Cybercrime and the law, P.R; Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, pp.76-77; Relevant Penetration Testing Legislation in the UK, P.R; See also: An article entitled Crime, available online in June 2009 at: http://www.out-law.com/page-405; Computer Misuse = = Overview, 1 February 2007, this article available online at: http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx

(١) اقتُرحت هذه المادة من جانب عضو مجلس العموم البريطانى لورد نورسكLord Northesk، وأقرها المشرع الانجليزى ورصد لها عقوبة الحبس لمدة لا تتجاوز سنتان والغرامة أو إحدى هاتين العقوبتين. فى ذلك انظر:

Neil Mac Ewan: The Computer Misuse Act 1990, P.R, p.966; Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, pp.78-80; Police and Justice Act 2006: available online at: https://wiki.openrightsgroup.org/wiki/Police_and_Justice_Act_2006#Making.2C_supplying_or_obtaining_articles_for_use_in_computer_misuse_offences

(٢) وقد قوبلت هذه المادة الجديدة باعتراضات كثيرة من قبل العاملين في مجال أمن الكمبيوتر، لأن من شأنها إحاطة عمليات الإبداع في مجال أمن الكمبيوتر بقيود قانونية وتجريمية، وتُحرِم من اتخاذ خطوات التأمين المضادة لعمليات القرصنة والتسللات، فهذه المادة يمكن تطبيقها على الأدوات المشروعة التي يمكن أن يساء استخدامها فى أعمال القرصنة، وكذلك على البرامج التي يمكن استخدامها سواء بصورة مشروعة أو غير مشروعة، مما يلقى بعبء كبير على المحاكم عند ترسيمها للحدود بين ما هو مشروع وما هو غير مشروع . فى ذلك انظر:

Neil Mac Ewan: The Computer Misuse Act 1990, P.R, p.966; Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.80; Police and Justice Act 2006, P.R; David Emm: Cybercrime and the law, P.R.

المادة الأولى: الدخول المحظور على مواد الكمبيوتر: وجرى نص الفقرتان الأولى والثانية من هذه المادة والخاصتان بالتجريم على أن[١]:

١- يكون الشخص مرتكباً لجريمة فى حالة:

(أ) تسببه في قيام الكمبيوتر بأداء أي وظيفة بقصد تأمين الوصول إلى أي برنامج أو بيانات محفوظة في أي كمبيوتر.

(ب) تعمد الدخول المحظور للكمبيوتر. و

(جـ) علمه بكونه يرتكب جريمة فى الوقت الذى يتسبب فيه فى أداء الكمبيوتر للوظيفة.

٢- لا يُشترط لاعتبار الشخص مرتكباً لجريمة بموجب هذه المادة أن تتجه نيته إلى:

(أ) أي برنامج أو بيانات محددة.

(ب) برنامج أو بيانات من أى نوع معين، أو.

(جـ) برنامج أو بيانات محفوظة في كمبيوتر معين.

المادة الثانية: الدخول المحظور بقصد ارتكاب أو التسهيل لارتكاب جرائم أخرى، وجرى نص الفقرة الأولى من هذه المادة والخاصة بالتجريم على أن[٢]:

١- يُعد الشخص مذنباً بارتكاب جريمة بموجب هذه المادة إذا ارتكب الجريمة المنصوص عليها فى المادة الأولى بقصد:

---

(1) Section 1 – Unauthorised access to computer material.

(1)Aperson 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 unauthorised; and; (C) He knows at the time when he causes the computer to perform the function that is the case.

(2)The intent a person has to have to commit an 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».

(1) Section 2 – Unauthorised access with intent to commit or facilitate further offences « (1) A person is guilty of an offence under this section if he commits an offence under section 1 above (The unauthorised 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 by any other person); (C) and the an offense he intents to commit or facilitate is referred below in this section as the further offense».

(أ) ارتكاب جريمة تنطبق عليها هذه المادة أو;

(ب) تسهيل ارتكاب مثل هذه الجريمة، سواء بنفسه أو من قبل أي شخص آخر؛

(جـ) ويُشار إلى الجريمة التى ينوى ارتكابها أو تسهيلها وفقاً لهذه المادة بالجريمة الأخرى.

وبداءةً يُثار التساؤل حول المقصود بالجريمة الأخرى المعنية في هذا المقام؟ رأى البعض أن المقصود بهذه الجريمة، أية جريمة ينشأ عنها أضرار جنائية، وضرب أمثلة لها بجريمة الاحتيال المؤثمة بقانون الاحتيال، وجرائم التزوير والتزييف المنصوص عليها بقانون التزوير والتزييف لسنة ١٩٨١، وجريمة السرقة المنصوص عليها بقانون السرقة لسنة ١٩٨٦[١].

وجدير بالذكر أن هذه المادة لا يُشترط لانطباقها أن ترتكب الجريمة الأخرى فى ذات وقت ارتكاب جريمة الدخول المحظور أو مستقبلاً حسبما نُصَّ على ذلك فى الفقرة الثالثة منها[٢]، كما قرر المشرع العقاب على جريمة الدخول المحظور ولو كان وقوع الجريمة الأخرى بطريق الاشتراك مستحيلاً وفقاً لنص الفقرة الرابعة من ذات المادة[٣].

وهذه المادة خاصة بالاشتراك في جريمة الدخول المحظور، والذي يتخذ صور التحريض والتسهيل، والتجريم الوارد بها لا تكون فيه الجريمة قائمة على أساس الدخول غير المشروع وحده، وإنما يبغى الجانى من هذا الدخول غير المشروع ارتكاب جرائم أخرى أو تسهيل ارتكاب الغير لهذه الجرائم، فتفترض هذه المادة في بعض الأحوال ارتكاب الجانى للجريمة المنصوص عليها بالمادة الأولى والخاصة بالدخول المحظور، وذلك في حالة دخوله بداءة لمواد الكمبيوتر دخولاً محظوراً أو غير مصرحاً به – المادة الأولى – لكن لا يكتفى

(2) The Hacking of Computers and the Criminal Law, P.R; Paul Mobbsfor: Computer Crime - The law on the misuse of computers and networks, an article available online at:= =http://www.internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605

(1) Paragraph (3) from Section 2 « 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».

(2) Paragraph (4) from Section 2 «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».

بهذا الدخول المجرد، إذ أن القصد من الدخول في هذه الحالة ارتكاب أو التسهيل لارتكاب جرائم أخرى(١).

وقد تأتى الجريمة موضوع المادة الثانية مستقلة، وذلك في حالة وجود إذن أو تصريح بالدخول، فيعمد الجانى إلى استغلال هذا الدخول الشرعى أو المصرح به لارتكاب أو تسهيل ارتكاب جرائم أخرى.

ومن التطبيقات القضائية الانجليزية التى شهدت حالات إدانة لمخالفة المادتين الأولى والثانية من قانون١٩٩٠، ما قضت به محكمة Croydon Magistrates Court في١٩٩٣/١٢/٩ بمعاقبة شخص يُدعى Malcolm Farquharson بالحبس لمدة ستة أشهر، وذلك لمخالفته المادتين الأولى الخاصة بالدخول المحظور والثانية الخاصة بالدخول المحظور بقصد التسهيل والتحريض على ارتكاب الجرائم، لقيامه بتحريض أُخرى تُدعى Emma Pearce دون التدخل منه شخصياً في عمل الكمبيوتر للوصول إلى سجلات المكالمات الهاتفية فى محاولة لتغييرها والتى كان طرفاً فيها والمتضمنة لأعمال قرصنة.

أما بالنسبة للفاعل Emma Pearce فقضت المحكمة بمعاقبتها بالغرامة وقدرها ٣٠٠ جنيه استرلينى، وقد نُسب إليها مخالفتها للمادة الأولى سالفة الذكر، لولوجها بطريقة غير مشروعة بإيعاز من شريكها Malcolm Farquharson للوصول إلى سجلات المكالمات الهاتفية التي كان طرفاً فيها(٢).

---

(٣) أكد المشرع الانجليزى على هذا المعنى بنصه فى الفقرة الأولى من المادة (١٢) من قانون ١٩٩٠، وذلك فى حالة المحاكمة بشأن ارتكاب الجريمة موضوع المادة الثانية – محل المقال – أو الجريمة موضوع المادة الثالثة والخاصة بحظر التبديل أو التعديل العمدى فى مواد الكمبيوتر أو الشروع فى ذلك، ووجدت هيئة المحلفين أن المتهم غير مذنب بأى من الجرائم موضوع المادتين المشار إليهما، فلا يوجد ما يمنع من = = إدانته بالجريمة موضوع المادة الأولى - الدخول المحظور على مواد الكمبيوتر- إذا ثبت مقارفته إياها، لكن بشرط عدم فوات مدة انقضاء الدعوى الجنائية المقررة بالمادة (١١) من ذات القانون، والتى سوف نشير إليها لاحقاً، ونص هذه الفقرة كالتالى:

Paragraph (1) from Section 12 «If on the trial on indictment of a person charged with: (A) an o offence under ffence under section 2 above; or (B) an offence under section 3 above or any attempt to commit such an offence;

the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings».

(1) R. v Malcolm Farquharson and Emma Pearce (Croydon Magistrates Court 9/12/1993).

- وكانت هذه الواقعة مثار جدل فى الأوساط الانجليزية، لذا أشارت إليها والحكم الصادر فيها مجلة الكمبيوتر الأسبوعية الانجليزية في عدد ١٩٩٤/١/١٣.

(Computer Weekly 13 January 1994)

وكذلك ما قضت به محكمة Northampton Magistrates Court في ٢٠١٣/١١/٢٨ بمعاقبة شخص يُدعى Stephen Burrell بالعمل فى خدمة المجتمع لمدة سنة مع وضعه تحت المراقبة، وإلزامه كذلك بعمل غير مدفوع الأجر لمدة ١٥٠ ساعة، وذلك لمخالفته المادتين الأولى والثانية المار ذكرهما من قانون١٩٩٠ لتوصله بطريقة غير مشروعة إلى حسابات ٣٨٧٢ من لاعبى لعبة Run escape على الإنترنت بقصد سرقة متحصلاتهم من اللعبة، وقيامه بالفعل بتعديل حسابات ١٠٥ من هؤلاء اللاعبين(١).

كما قضت محكمة Birmingham Crown Court في ٢٠١٥/٤/٢٤ بمعاقبة شخص يُدعى Imran Uddin، بالحبس لمدة أربعة أشهر، لمخالفته المادة الثانية من قانون ١٩٩٠، حيث كان المتهم أحد طلبة جامعة برمنجهام University of Birmingham، وقام بتركيب أربعة أجهزة تجسس للتوصل لكلمات السر الخاصة بموظفى هذه الجامعة من أجل الدخول لنظام الكمبيوتر الخاص بالجامعة لتحسين درجاته الدراسية(٢).

كما قضت محكمة Bradford Crown Court في ٢٠١٥/٧/١٧ بمعاقبة شخص يُدعى Andrew Skelton بالسجن لمدة ثمان سنوات، وذلك لمخالفته المادتين الأولى والثانية من قانون١٩٩٠، حيث كان المتهم يعمل بوظيفة كبير مراجعى الحسابات بأحد المولات الضخمة ويُدعى Morrisons supermarket وقام بتحميل البيانات الشخصية السرية لأكثر من ١٠٠٠٠٠ – مائة ألف– موظف بهذا المول بما في ذلك أسمائهم وعناوينهم والتفاصيل المصرفية الخاصة بهم، ونشرها على شبكة الإنترنت وقدَّم نسخ منها للصحف، ووجهت إليه اتهامات بالغش والتحايل باستغلال وظيفته القائمة على الثقة والوصول غير المصرح به لمادة الكمبيوتر والكشف عن البيانات الشخصية للموظفين، وقُدرت تكلفة الأضرار الناتجة عن هذه الخروقات بنحو ٢ مليون جنيه استرلينى(٣).

(2) R. v Stephen Burrell (Northampton Magistrates Court 28 /11/ 2013)

(3) R. v Imran Uddin (Birmingham Crown Court 24 /4/ 2015).

(1) R. v Andrew Skelton (Bradford Crown Court 17 /7/ 2015).

المطلب الثالث
النصوص المستحدثة فى مصر

١٨- تمهيد:

تعد مصر من الدول النامية في مجال إنتاج تكنولوجيا المعلومات، ومن الدول الحديثة نسبياً في استخدام هذه التكنولوجيا مقارنة بالدول الحائزة للسبق في مجالى الانتاج والاستخدام(١)، كالولايات المتحدة الأمريكية وانجلترا، لكن هذا لم يمنع من اجتياح أنماط مختلفة من الجرائم المعلوماتية لها(٢).

وقد ألمحنا فيما سبق إلى عدم ملائمة تطبيق النصوص العقابية القائمة فى قانون العقوبات على الأنماط المختلفة للجرائم المعلوماتية، ومنها جريمة الدخول غير المشروع للأنظمة المعلوماتية.

وأخيراً وبعد أن بُحَّ الصوت من المناداة بضرورة إصدار تشريع عام لمكافحة الجرائم المعلوماتية، أصدر المشرع المصرى القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، ويُلاحظ بداءةً على هذا القانون تأثره جزئياً بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، سواء من حيث الاسم أو من حيث بعض المفردات والمصطلحات المستخدمة ومعانيها مثل البيانات والمعلومات الإلكترونية، وتقنية المعلومات، ومقدم الخدمة، والبرنامج معلوماتى، والنظام معلوماتى، والموقع، والواردة فى المادة الثانية من الاتفاقية والمادة الأولى الخاصة بالتعريفات من القانون المذكور، وكذلك من حيث نمط التجريمات الواردة بهذه الاتفاقية والتى استقى بعضها القانون المذكور.

١٩- جريمة الدخول غير المشروع فى إطار قانون مكافحة جرائم تقنية المعلومات الرقيم ١٧٥ لسنة ٢٠١٨.

---

(٢) ارتفعت معدلات استخدام التكنولوجيا المعلوماتية فى مصر فى الآونة الأخيرة، فقد كشف تقرير صادر عن وزارة الاتصالات وتكنولوجيا المعلومات سنة ٢٠١٧ إلى ارتفاع أعداد مستخدمى الإنترنت فى مصر إلى نحو ٣٣.١٩ مليون مستخدم فى إبريل ٢٠١٧، مقارنة ٢٦.٨ مليون مستخدم فى إبريل ٢٠١٦. تفاصيل هذا التقرير منشورة بتاريخ ٢٠١٧/٨/٢٠على الموقع الإلكترونى:

https://www.youm7.com/story/2017/8/20

(٣) تُشير تقارير مصلحة الأمن العام فى مصر بصفة عامة إلى احتلال جرائم التشهير المرتكبة باستخدام الحاسب الآلى وشبكة المعلومات للمركز الأول، تليها جريمة الاحتيال – النصب - المعلوماتى، ثم جرائم الاعتداء على حقوق الملكية الفكرية، = = ثم جرائم الاختراق والدخول غير المشروع وقطع الاتصال، ثم جرائم السب والقذف، وأخيراً جرائم التهديد.

حظت جريمة الدخول غير المشروع باهتمام المشرع المصرى فى هذا القانون، فأفرد لها عدة نصوص تجريمية نبرزها بداءةً، ثم نبين المثالب التشريعية التى حاقت بالقانون المذكور من ناحية هذه الجريمة، وذلك على النحو التالى:

١٩-١: النصوص المتعلقة بجريمة الدخول غير المشروع:

مايز المشرع المصرى بشأن جريمة الدخول غير المشروع وصورها، بين الدخول غير المشروع للأنظمة المعلوماتية الخاصة سواء كانت تتعلق بشخص طبيعى أو معنوى، وبين الدخول غير المشروع للأنظمة المعلوماتية الخاصة بالدولة أو بأحد الأشخاص الاعتبارية العامة.

فبالنسبة للأنظمة المعلوماتية الخاصة، فأفرد لها المشرع المادتين (١٤) و(١٥) من هذا القانون، وجاءت المادة (١٤) تحت مسمى جريمة الدخول غير المشروع، وخصص الفقرة الأولى منها لتجريم وعقاب فعلى الدخول غير المشروع والبقاء العمدى داخل الأنظمة المعلوماتية الحاصل فى بدايته بطريق الخطأ، إذ تنص هذه الفقرة على أن « يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه».

فى حين أورد المادة (١٥) تحت مسمى جريمة تجاوز حدود الحق في الدخول، لتجريم وعقاب أفعال تجاوز الدخول المصرح به، وتنص هذه المادة على أن « يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول».

أما بالنسبة للأنظمة المعلوماتية الخاصة بالدولة أو بأحد الأشخاص الاعتبارية العامة، فخصص لها نص الفقرة الأولى من المادة (٢٠) والتى جاءت تحت مسمى جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، والتى تُجرِّم وتعاقب على أفعال الدخول غير المشروع والبقاء العمدى داخل الأنظمة الحاصل فى بدايته بطريق الخطأ، وكذلك أفعال تجاوز الدخول المصرح به، إذ تنص هذه الفقرة على أن « يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدي هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز

حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها أو يخصها».

وبشأن الأنظمة المعلوماتية وما فى حكمها من مواقع وحسابات خاصة وبريد إلكترونى والخاصة بالدولة أو بأحد الأشخاص الاعتبارية العامة، يستوى لدى القانون فى الحماية أن تكون هذه الأنظمة تُدار بمعرفة بالدولة أو تعمل لأجلها أو مملوكة لها.

وتعتبر النصوص التى أوردها المشرع المصرى فى هذا القانون والمتعلقة بجريمة الدخول غير المشروع، أوفى النصوص المتعلقة بهذه الجريمة فى التشريعات محل المقارنة، لشمولها لجميع صور الدخول غير المشروع من البقاء العمدى داخل الأنظمة الحاصل فى بدايته بطريق الخطأ، وكذلك تجاوز الدخول المصرح به، فضلاً عن فعل الدخول غير المشروع من الأساس، فى حين لم يتضمن القانون الاتحادى الأمريكى سوى فعلى الدخول غير المشروع، وتجاوز الدخول المصرح به، ولم يتطرق لفعل البقاء العمدى داخل الأنظمة المعلوماتية الحاصل فى بدايته بطريق الخطأ، فى حين تضمن القانون الانجليزى فعل الدخول غير المشروع، ولم يتطرق صراحة لفعلى البقاء العمدى داخل الأنظمة الحاصل فى بدايته بطريق الخطأ، وتجاوز الدخول المصرح به على النحو المار ذكره.

١٩-٢: المثالب التشريعية المتعلقة بجريمة الدخول غير المشروع:

فيما يخص جريمة الدخول غير المشروع للأنظمة المعلوماتية نلحظ عدم دقة الصياغة التشريعية من ناحية بعض المفردات المستخدمة فى بعض النصوص التجريمية الواردة فى هذا القانون، وبخاصة إزاء لفظ الاختراق الوارد فى نص الفقرة الأولى من المادة (١٨) من هذا القانون، والتى جاءت تحت مسمى جريمة الاعتداء علي البريد الاليكتروني أو المواقع أو الحسابات الخاصة، والتى تنص على أن « يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونياً أو موقعاً أو حساباً خاصاً بآحاد الناس».

فمصطلح الاختراق المشار إليه يُعد أحد صور الدخول غير المشروع[١]، والتى تكفلت بها الفقرة الأولى من المادة (١٤) وكذلك المادة (١٥) من هذا القانون على النحو المار

(١) وهذا ما أشار إليه صراحة البند (١٨) من المادة الأولى الخاصة بالتعريفات من القانون المذكور بتعريفه للاختراق بأنه «الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلى أو شبكة

ذكره، ومن جهة أخرى فإن هذا المصطلح بوضعه الحالى يفيد تخصيص المشرع لجريمة اختراق البريد الإلكترونى- والذى كما سبق القول يُعد أحد صور الدخول غير المشروع - للعقوبة الواردة بالمادة (١٨) المار ذكرها، إذ أنه لم يورد البريد الإلكترونى ضمن محل الحماية الوارد فى المادتين (١٤،١٥) المنوه عنهما، والذى يقتصر على المواقع أو الحسابات الخاصة أو الأنظمة المعلوماتية الخاصة.

لهذا فإن المشرع بهذا المصطلح وبمعناه الدال عليه قد وقع فى خطأ بتقريره للعقوبة سالفة الإشارة فى نص المادة (١٨) فى حالة اختراق أحد المواقع أو الحسابات الخاصة بآحاد الناس، فى حين يُفرد لذات الجرم لكن باستخدام عبارة الدخول غير المشروع عقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، المقررة فى المادة (١٤) من القانون المشار إليه.

فضلاً عن أننا لا نرى وجهاً للمغايرة فى محل الحماية بين المواقع والحسابات والأنظمة المعلوماتية الخاصة الواردة فى المادتين (١٤،١٥) من جهة، والبريد الإلكترونى الوارد فى المادة (١٨) من جهة أخرى، ومن ثم فى العقوبة المقررة لانتهاك أياً منهم، وهو ما فطن إليه المشرع وتجنبه فيما يخص جريمة الدخول غير المشروع وصورها للأنظمة المعلوماتية الخاصة بالدولة أو بأحد الأشخاص الاعتبارية العامة، المقررة بالفقرة الأولى من المادة (٢٠) على النحو سالف الذكر، إذ أورد صراحة مصطلح الاختراق ضمن صور الدخول غير المشروع، وكذلك أورد صراحة البريد الإلكترونى كمحل للحماية بجانب الموقع والحساب الخاص والنظام المعلوماتي الخاص أيهم بالدولة أو بأحد الأشخاص الاعتبارية العامة، ولهذا كان جديراً بالمشرع عدم إيراد لفظ الاختراق فى نص المادة (١٨) وإيراده والنص عليه فى المادة (١٤)، وكذلك إدراج البريد الإلكترونى ضمن محل الحماية المقرر بالمادتين (١٤،١٥) من هذا القانون.

معلوماتية وما في حكمها»، ومما يؤكد ذلك أنه فى معرض تعليق المذكرة التفسيرية لاتفاقية بودابست لعام ٢٠٠١ على المادة الثانية منها والخاصة بالولوج غير القانوني والعمدى Accesillegale أكدت على أن جريمة الولوج غير المشروع للنظام المعلوماتى تضم فعل الاختراق الذى يحدث سواء للنظام بأكمله أو لجزء منه، أو الاختراق الذى يحدث لنظام معلوماتى متصل بشبكة اتصال عامة مثل الإنترنت أو لنظام معلوماتى متصل بشبكة محلية أو أى شبكة خاصة. انظر:

Draft explanatory memorandum to the draft convention cyber crime Shbujfhvdm hguhlmtrasbourg 14 February 2001.

الفصل الثانى
البنيان القانونى لجريمة الدخول غير المشروع

٢٠- تمهيد وتقسيم:

من المستقر عليه أن لكل جريمة[١] أركان عامة وهى العناصر التى يتعين توافرها للقول بوجودها قانوناً، بحيث إذا تخلف ركن منها لا توجد الجريمة، وهذه الأركان عامة لأنها مشتركة بين جميع الجرائم، فعلى المشرع الجنائى أن يراعى توافرها، ثم عليه أن يحدد شكل وطبيعة كل منها فى كل جريمة على حده[٢]، واستقر الفقه الجنائى على أن للجريمة ركنان مادى ومعنوى، وقد أضاف البعض ركناً ثالثاُ وهو الركن الشرعى، وإن كانت هذه فكرة منتقدة لدى أغلبية شرَّاح القانون الجنائى، وجريمة الدخول غير المشروع للأنظمة المعلوماتية شأنها شأن كافة الجرائم لها ركنان، الأول هو الركن المادى والثانى هو الركن المعنوى.

وفى هذا الفصل سوف نتناول البنيان القانونى لهذه الجريمة فى التشريعات محل المقارنة، موضحين ركنيها فضلاً عن العقوبات المقررة لها

فى هذه التشريعات، وذلك من خلال مبحثين على النحو التالى.

المبحث الأول: الركن المادى لجريمة الدخول غير المشروع.

المبحث الثانى: الركن المعنوى لجريمة الدخول غير المشروع وعقوبتها.

المبحث الأول
الركن المادى لجريمة الدخول غير المشروع

٢١- تمهيد وتقسيم:

الركن المادى للجريمة هو العمل المادى الذى تظهر به الجريمة للعالم الخارجى، سواء كان ذلك بفعل أو بقول، حسب ما يتطلبه المشرع فى كل جريمة على حده، ويتمثل هذا

(١) الجريمة بصفة عامة هى أى عمل أو امتناع يُرتب القانون على ارتكابه عقوبة أو تدبيراً احترازياً . انظر: د. السعيد مصطفى السعيد، الأحكام العامة فى قانون العقوبات – طبعة دار المعارف بمصر– الطبعة الرابعة ١٩٦٢، ص٤٢، د. محمود نجيب حسنى، شرح قانون العقوبات – القسم العام، تنقيح د. فوزية عبد الستار، دار النهضة العربية، الطبعة الثامنة ٢٠١٦، ص ٤٥، ويُعرّفها آخرون بأنها الواقعة التى تُرتكب إضراراً بمصلحة حماها المشرع فى قانون العقوبات ورتب عليها أثراً جنائياً متمثلاً فى العقوبة. انظر: د. مأمون سلامة، شرح قانون العقوبات – القسم العام، مطبعة جامعة القاهرة والكتاب الجامعى، ١٩٩٠-١٩٩١، ص٩٣، د. محمد عيد الغريب، شرح قانون العقوبات – القسم العام، طبعة ١٩٩٩-٢٠٠٠، ص٢١١.

(٢) د. عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات – الجزء الأول، طبعة نقابة المحامين بالجيزة ٢٠٠٨، ص٣٥٩.

العمل فى السلوك الذى يصدر عن الجانى والنتيجة المترتبة على هذا السلوك وعلاقة السببية بينهما، وهذا أول الركنين اللذين ترتكز عليهما نظرية الجريمة، وإذا تخلف هذا الركن كله أو بعضه، كان ذلك مانعاً من قيام الجريمة(١).

وفى سبيل بياننا للركن المادى لجريمة الدخول غير المشروع للأنظمة المعلوماتية، يجب التعرض للعناصر المتطلبة لقيام هذا الركن فى ضوء طبيعة هذه الجريمة والنماذج القانونية الخاصة بها فى التشريعات محل المقارنة، ثم نتبع ذلك ببيان الأساس الذى ترتكز عليه المسئولية الجنائية فى هذه الجريمة فى ضوء التشريعات المشار إليها، وذلك من خلال مطلبين على النحو التالى.

المطلب الأول: عناصر الركن المادى فى جريمة الدخول غير المشروع.

المطلب الثانى: أساس المسئولية الجنائية فى جريمة الدخول غير المشروع.

المطلب الأول
عناصر الركن المادى فى جريمة الدخول غير المشروع

٢٢- تمهيد:

يُحدد النموذج القانونى الخاص بكل جريمة صورة الركن المادى فيها، فهو الذى يرسم السلوك المحظور والنتيجة المترتبة عليه وعلاقة السببية بينهما، غير أن هذه العناصر الثلاثة قد لا تأتى مجتمعة، ففى بعض الأحيان يكتفى المشرع فى تحديده للواقعة موضوع التجريم بالسلوك فقط، ويُجرِّمه بغض النظر عما يترتب عليه من نتائج، وهذا النوع من الجرائم هو ما يُطلق عليه جرائم السلوك المجرد(٢).

وفى سبيل بيان عناصر الركن المادى لجريمة الدخول غير المشروع كان لابد من التعرض لتكييف هذه الجريمة من منظور هذا الركن من حيث عنصرى النتيجة والسلوك الإجرامى فيها، فإذا ما انتهينا من هذا التكييف، ينتقل بنا المقال لتبيان وتأصيل فعل الدخول غير المشروع للأنظمة المعلوماتية، ثم نختم ببيان محل هذا الدخول فى التشريعات محل المقارنة، وذلك على النحو التالى.

---

(١) د. السعيد مصطفى السعيد، القسم العام، المرجع السابق، ص٢٤٥، د. محمود محمود مصطفى، القسم العام، المرجع السابق، ص٣٨، د. عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص٣٧٦، د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٤٥٩.

(١) د. محمود نجيب حسنى، القسم العام، المرجع السابق، ص٣١٦، د. مأمون سلامة، القسم العام، المرجع السابق، ص١٢٣.

٢٣- تكييف جريمة الدخول غير المشروع من منظور الركن المادى.

تناول الفقه الجنائى تقسيمات عدة للجرائم من منظور الركن المادى لها، من بينها تقسيمها من حيث النتيجة فيها، إلى جرائم ذات نتيجة أو جرائم مادية، وأخرى ذات سلوك مجرد، وتقسيمها من حيث السلوك الإجرامى فيها، إلى جرائم وقتية وجرائم مستمرة، فإلى أى الجرائم تنتمى جريمة الدخول غير المشروع للأنظمة المعلوماتية فى ضوء التقسيمات المشار إليها؟.

نبحث بداءةً تكييف هذه الجريمة من حيث عنصر النتيجة، نعقبه ببيان تكييفها من حيث السلوك الإجرامى فيها، وذلك كما يلى.

٢٣- ١: تكييف جريمة الدخول غير المشروع من حيث النتيجة:

يطرح الركن المادى لجريمة الدخول غير المشروع للأنظمة المعلوماتية على بساط البحث تساؤل مبدئى وجوهرى، يتعلق بتكييف هذه الجريمة من منظور الركن المادى لها وبخاصة إزاء عنصر النتيجة، بانتمائها للجرائم المادية أم لجرائم السلوك المجرد؟ وأثر القول بأيهما على عناصر الركن المادى لها، والقول الفصل فى هذا أو ذاك هو بطبيعة هذه الجريمة، وما ورد بالنموذج القانونى الخاص بها.

من خلال عرضنا للنصوص المتعلقة بهذه الجريمة فى التشريعات محل المقارنة، نجد المشرع المصرى فى القانون رقم ١٧٥ لسنة ٢٠١٨ قد أورد تجريماً لأفعال الدخول غير المشروع والمجرد فى المواد(١/١٤) و(١٥) و(١/٢٠) على النحو المشار إليه، ولم يتطلب لقيام هذه الجريمة فى نماذجها التجريمية سالفة الإشارة نتيجة معينة لفعل الدخول غير المشروع، أو البقاء العمدى داخل الأنظمة الحاصل فى بدايته بطريق الخطأ، أو تجاوز الدخول المصرح به، كالحصول على المعلومات أو إتلافها أو تزويرها. ولكنه شدد من العقوبات إذا تُبعت هذه الأفعال بأفعال أخرى متمايزة عنها تتضمن المساس بالنظام المعلوماتى ذاته أو بمحتوياته.

وهذا هو ذات مسلك المشرع الانجليزى الذى أورد تجريماً خاصاً للدخول المجرد للأنظمة المعلوماتية، تحت مسمى الدخول المحظور على مواد الكمبيوتر فى المادة الأولى من قانون ١٩٩٠، مكتفياً فى قيام الركن المادى لهذه الجريمة بتحقق السلوك الإجرامى فقط

بغض النظر عن النتائج المتحققة من عدمه، فالجريمة تقوم بمجرد الدخول المحظور على مواد الكمبيوتر(١).

ونرى تميز المشرع المصرى- وكذلك الانجليزى- فى إفراد نصوص تجريمية خاصة بالدخول المجرد للأنظمة المعلوماتية، لأنه بداءةً يجب التمييز بين جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية فى حد ذاتها، وبين ما قد يتبعها من أفعال تمثل جرائم مستقلة ومتمايزة عنها، فالجانى قد يكتفى بالولوج لهذه الأنظمة دون أن يتبع ولوجه بثمة فعل آخر، والجرم المنسوب إليه فى هذه الحالة هو الدخول غير المشروع لهذه الأنظمة، أما إذا تبع فعل الدخول بأفعال إجرامية أخرى، فتلك جرائم متمايزة عن جريمة الدخول غير المشروع، ونتيجة لذلك يمايز المشرع فى الغالب الساحق من الأحوال فى العقوبة المقررة للدخول غير المشروع والمجرد، والدخول غير المشروع الذى يُتبع بأفعال إجرامية أخرى أو الذى يكون وراءه غاية يبغى الجانى تحقيقها(٢).

كما أن المستهدف فى المقام الأول بالحماية فى التشريعات محل المقارنة من وراء إصدار قوانين خاصة فى هذه التشريعات، هى حماية وسلامة الأنظمة المعلوماتية من الدخول غير المشروع إليها، فهذه الجريمة تتم بمجرد الانتهاك العمدى للأنظمة المعلوماتية، ولا يتوقف تمامها على حدوث نيجة معينة بسبب هذا الدخول غير المشروع كالحصول على معلومات أو تدميرها أو تعديلها أو المساس بأى صورة بمحتويات النظام المعلوماتى(٣).

أما المشرع الأمريكى فلم يفرد فى القانون الاتحادى لسنة ١٩٨٦ وتعديلاته تجريماً خاصاً بالدخول المجرد للأنظمة المعلوماتية على غرار المشرعين المصرى والانجليزى- وهذا من مساوئ هذا التشريع – بل اشترط أن يكون الدخول وراءه غاية يبغى الجانى تحقيقها،

(١) د.عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، بدون جهة نشر، الطبعة الثانية سنة ١٩٩٥، ص ١٢٤،١٢٥.

(٢) من ذلك تشديد المشرع المصرى للعقوبة فى الفقرة الثانية من المادة (١٤) لتكون الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه أو إحدي هاتين العقوبتين، إذا نتج عن الدخول غير المشروع إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة علي الموقع أو الحساب الخاص أو النظام المعلوماتي، وبالمثل تشديده للعقوبة فى الفقرة الثانية من المادة (٢٠) لتكون السجن والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه إذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، وكذلك تشديده للعقوبة فى الفقرة الثالثة من ذات المادة لتكون السجن والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه إذا ترتب على أى من الأفعال الواردة بالفقرتين الأولى والثانية من ذات المادة إتلاف البيانات أو المعلومات أو الموقع أو الحساب الخاص أو النظام المعلوماتى = = أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً بأى وسيلة كانت.

(١) خصص المشرع المصرى الباب الثالث من القانون رقم ١٧٥ لسنة ٢٠١٨ للجرائم والعقوبات، وجاء الفصل الأول من هذا الباب تحت مسمى (الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات)، والذى تضمن كل التجريمات الخاصة بجريمة الدخول غير المشروع.

كالحصول على معلومات معينة أو أى شيء له قيمة مثلاً...إلخ، طبقاً لما أورده بالبنود السبعة من الفقرة الأولى من المادة (١٠٣٠) على النحو المشار إليه.

لذا يمكن القول بأن المشرع الأمريكى لا يعرف جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية، وإنما أورد فى كل بند من البنود المشار إليها مجموعة من الجرائم المتمايزة والتى تتماثل إلى حد كبير من ناحية السلوك الإجرامى فيها، والمتمثل فى فعل الولوج العمدى إلى الكمبيوتر بدون تصريح أو تجاوز الولوج المصرح به، والذى لا يقوم الركن المادى بأى منهما منفرداً، بل لابد من تحقق النتيجة التى حددها المشرع فى كل بند، فضلاً عن ضرورة توافر علاقة السببية بين السلوك الإجرامى المشار إليه والنتيجة المبتغاة فى كل جريمة منها.

ولما كان موضوع بحثنا يرتكز على جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية، وفى ضوء الطبيعة المميزة لهذه الجريمة، فإنه يمكن القول بانتماء هذه الجريمة لجرائم السلوك المجرد، التى يُكتفى فى قيام ركنها المادى بتحقق السلوك الإجرامى فقط، والذى يتخذ صور الدخول غير المشروع من الأساس لهذه الأنظمة. أو البقاء العمدى داخل هذه الأنظمة والحاصل فى بدايته بطريق الخطأ، أو تجاوز الدخول المصرح به.

٢٣-٢: تكييف جريمة الدخول غير المشروع من حيث السلوك الإجرامى:

أما من حيث تكييف هذه الجريمة من ناحية السلوك الإجرامى فيها بانتمائها للجرائم الوقتية أم للجرائم المستمرة[١]، فيجمع الفقه على تكييف إحدى صور هذه الجريمة وهى صورة الإبقاء على الاتصال مع النظام والحاصل فى بدايته بطريق الخطأ بأنها من الجرائم المستمرة، فى حين اختلف الفقه فى صورتى الدخول غير المشروع من الأساس للنظام أو تجاوز الدخول المصرح به، فيرى بعض الفقه أن هاتين الصورتين ينتميان أيضاً للجرائم المستمرة، سواء تعلق الأمر بالدخول إلى النظام أو تجاوز الدخول المصرح به، لأن سلوك الجاني ممتد طالما شغل النظام بطريق غير مشروع[٢]، فى حين يرى البعض الآخر

(١) يقسم الفقه الجنائى الجرائم من حيث السلوك الإجرامى، إلى جرائم وقتية، وهى التى يستغرق تحقق أركانها برهة يسيرة من الزمن، مثل جرائم القتل والسرقة والضرب، وجرائم مستمرة، وهى التى يستغرق تحقق أركانها زمناً طويلاً نسبياً، مثل الحجز والحبس دون وجه حق والهروب من الخدمة العسكرية وإحراز الأسلحة والذخائر بدون ترخيص. انظر د. عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص ٣٩٧-٣٩٨، د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٤٨٩-٤٩٠.

(١) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، سنة ١٩٩٢، ص ١٥٠.

انتمائهما للجرائم الوقتية تأسيساً على اعتبار جريمة الدخول إلى النظام منتهية بمجرد إتيان الفاعل لسلوكه المجرَّم بدخول النظام كله أو جزء منه غير مصرح له بالدخول إليه، أو بمجرد إنهاءه لفعله المنم عن تجاوز التصريح الممنوح له ليجد نفسه أمام نظام أو جزء منه غير مسموح له بالدخول إليه[١]، وهذا الرأى الأخير هو ما نميل إليه لتمام السلوك الإجرامى بمجرد الدخول أو تجاوز الدخول المصرح به.

٢٤- أوصاف الدخول المعنى للأنظمة المعلوماتية.

انتهينا إلى أن فعل الدخول غير المشروع هو الممثل للسلوك الإجرامى المتطلب وحده لقيام الركن المادى فى جريمة الدخول غير المشروع للأنظمة المعلوماتية بوصفها من جرائم السلوك المجرد، لكن ما هو الدخول المعنى فى هذا المقام حتى يتحقق له الوصف القانونى الذى عنته التشريعات محل المقارنة؟ لا شك فى أن لهذا الدخول أوصاف تحدده من تعريف وحالات له، وكيفية إثباته وصعوبات ذلك، فضلاً عن محله، وهذا ما سنبينه فى الآتى.

٢٥- تعريف الدخول غير المشروع وحالات تحققه.

٢٥-١: تعريف الدخول غير المشروع:

يُعرَّف الدخول غير المشروع بصفة عامة بأنه إساءة استخدام الحاسب الآلى ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والبيانات المخزونة بداخله للإطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح فى اختراق الحاسب الآلى على الرغم من الاحتياطات التقنية التى يحتوى عليها نظامه[٢].

ولم يتضمن القانونين الأمريكى والانجليزى وكذلك القانون المصرى رقم ١٧٥ لسنة ٢٠١٨ تعريفاً للدخول غير المشروع، وإن كان الأخير قد أوضح معنى الاختراق الذى هو أحد صوره فى البند (١٨) من مادته الأولى الخاصة بالتعريفات كما سبق القول، فى حين عرَّفه المنظم السعودى فى نظام مكافحة جرائم المعلوماتية السعودى الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ، فى البند السابع من المادة الأولى منه والخاصة بالتعريفات بأنه « دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها»، فى حين عرَّفه

(٢) د. عباوى نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، بحث منشور بمجلة دفاتر السياسة والقانون الجزائرية، العدد (١٦)، يناير ٢٠١٧، ص٢٨٤.

(1)The recommendation No R (89-9) on computer-related crime and final report to the European committee on crime problems, Strasbourg, 1990, pp. 49-51.

المشرع الكويتى فى قانون مكافحة جرائم تقنية المعلومات الكويتى رقم ٦٣ لسنة٢٠١٥، فى البند رقم (١١) من مادته الأولى الخاصة بالتعريفات بأنه« النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح»[١].

وعلى ذلك فإن الدخول المعنى هنا لا يحمل المعنى المادي لهذا اللفظ، وإنما المقصود به الدخول بالطرق الفنية، أي يتم الاتصال بالنظام باستخدام طرق فنية، إما بتحطيم نظم الأمن باستخدام كارت ممغنط أو ضرب حروف شفرية معينة، أو بالتحايل على واحد أو أكثر من التدابير التكنولوجية – ككلمة السر – أو المادية التى يتم تصميمها لاستبعاد أو منع الأشخاص غير المرخص لهم بالدخول من الوصول للنظام، إلى غير ذلك من الطرق الفنية التى تتيح الدخول غير المشروع للنظام المعلوماتى[٢].

لذا يرى البعض أنه من الفاعلية بمكان لتأمين الأنظمة المعلوماتية وما تحتويه من برامج ومعلومات وبيانات يُخشى عليها من التسلل أو التعديل، وضع إجراءات أمنية فعالة[٣]، مثل تغيير كلمات السر من فترة لأخرى[٤]، واستخدام كلمات سر قوية يمكن تذكرها بسهولة[٥]، وكذلك أهمية استخدام ما يُعرف بالجدران النارية في خلق بيئة معلوماتية آمنة، بوصفها تمثل علاج
وحل ملائم لمشكلة اختراق الأنظمة المعلوماتية[٦].

---

(٢) انفرد هذان التشريعان دون بقية التشريعات العربية المشار إليها بإيراد تعريف للدخول غير المشروع.

(1)Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, pp.143-144; Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, P.R, p.229.

(٢) المذكرة التفسيرية لاتفاقية بودابست لعام ٢٠٠١ فى معرض تعليقها على المادة الثانية منها والخاصة بالولوج غير القانونى والعمدى، المرجع السابق.

(٣) كلمة السر أو المرور password لا يُشترط أن تكون من كلمة واحدة، فقد تتألف من مجموعة من الكلمات أو الرموز أو بالمزج بين الأسماء والرموز أو بأى طريقة أخرى من أجل الولوج للكمبيوتر. انظر:

Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, study published by Office of Legal Education Executive Office for United States Attorneys, 2015, p.50, this study available online at: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

(4) Bob Burls: How to report a computer crime: Unauthorised email account access, an article published on October 31, 2012, and available online at: https://nakedsecurity.sophos.com/2012/10/31/how-to-report-a-computer-crime-unauthorised-email-account-access/

(1) Derek Wyatt and others: Revision of the Computer Misuse Act, P.R, no.44, p.8.

٢٥-٢: حالات الدخول غير المشروع للأنظمة المعلوماتية:

إذا كان فعل الدخول غير المشروع هو الممثل للسلوك الإجرامى فى جريمة الدخول غير المشروع، فهل يتمثل هذا الدخول فى عمل إيجابى أم فى عمل سلبى[١]؟، يمكن القول بأن السلوك الإجرامى فى هذه الجريمة يتخذ صورة العمل الإيجابى، وله ثلاث حالات يتحقق فيها هذا الوصف، الحالة الأولى وهى حالة الدخول العمدى غير المشروع من الأساس للنظام المعلوماتى، ففى هذه الحالة فإنه لا يحق للجانى الاتصال أو الولوج بداءة للنظام المعلوماتى، والحالة الثانية بالتجاوز العمدى للتصريح الممنوح بالدخول لمناطق لا يمتد إليها هذا التصريح[٢]. فالولوج خارج الحدود المقررة يمثل فعل إيجابى فى هذه الحالة أيضاً، ومثال لذلك حالة قيام الموظف باستخدام كمبيوتر العمل وشبكته للوصول لمواقع التواصل الاجتماعى[٣].

أما الحالة الثالثة فتتحق بالدخول بداءةً للنظام المعلوماتى لكن بطريق الخطأ، والنشاط الإجرامي من جانب الجاني يتمثل في عمل إيجابي بطريق الامتناع عن قطع الاتصال مع النظام الذي حدث في البداية بطريق الخطأ، ومنذ لحظة اتجاه إرادة الجاني إلى عدم قطع هذا الاتصال أي الإبقاء عليه يتحقق النشاط الإجرامي المعاقب عليه[٤].

وتفاوتت التشريعات محل المقارنة فى تناول والنص على هذه الحالات، فالمشرع الانجليزى قد أورد الحالة الأولى فقط فى المادة الأولى من القانون الانجليزى لسنة١٩٩٠

---

(٢) السلوك الإجرامى بصفة عامة قد يتمثل فى عمل إيجابى وهذا هو الأصل، وقد يتمثل فى عمل سلبى بالامتناع عن إتيان فعل كالامتناع مثلاً عن قيد المواليد، ويُعرَّف بأنه حركة الجانى الاختيارية التى تحدث تأثيراً فى العالم الخارجى أو فى نفسية المجنى عليه، أو هو السلوك المادى الإرادى الخارجى الصادر عن إنسان، والذى حظره المشرع لتقديره أنه يسبب نتائج تمثل عدواناً أو تهديداً بالاعتداء على مصلحة يهم القانون الجنائى حمايتها، فمبدأ لا جريمة بغير نشاط مادى يقف على قدم المساواة مع مبدأ لا جريمة بغير نص، فالقانون لا يعاقب على النوايا والرغبات المجردة من التعبير بمظهر مادى. فى ذلك انظر: د. محمود نجيب حسنى، القسم العام، المرجع السابق، ص٣٠٤، د. مأمون سلامة، القسم العام، المرجع السابق، ص١٢٣ وما بعدها، د.عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص٣٨٣ وما بعدها، د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٤٦١.

(٣) يتخذ تجاوز الدخول المصرح به صورتان عبَّر عنهما المشرع المصرى فى المادتين (١٥) و(١/٢٠) بتعدى حدود الحق فى الدخول من حيث الزمان أو مستوى الدخول، وتعدى حدود الحق فى الدخول من حيث الزمان يكون بتجاوز التوقيت أو المدة المحددة للدخول، أما تعدى حدود الحق فى الدخول من حيث مستوى الدخول = = يكون بتجاوز المستوى أو النطاق المسموح بالدخول إليه، كأن يدخل المصرح له إلى ملفات أو برامج لا يشملها التصريح أو الإذن الممنوح له بالدخول.

(1) Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, pp.143-144; Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, P.R, p.229.

(٢) د.عمر الفاروق الحسينى، المرجع السابق، ص١٢٩،١٣٠، د.عباوى نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، المرجع السابق، ص٢٨٣.

والخاصة بالدخول المحظور على مواد الكمبيوتر، فى حين نص المشرع الأمريكى على الحالتين الأولى والثانية كما فى البنود (١،٢،٤) من المادة «١٠٣٠» من القانون الاتحادى الأمريكى لسنة ١٩٨٦[١]، أما المشرع المصرى فأورد الحالات الثلاث المتقدم ذكرها فى المواد (١/١٤) و(١٥) و(١/٢٠) على النحو المار ذكره.

٢٦- صعوبات إثبات الدخول غير المشروع.

تُعد جريمة الدخول غير المشروع للأنظمة المعلوماتية إحدى أنماط الجرائم المعلوماتية، والتى يحيط إثباتها ومكافحتها بصفة عامة صعوبات عدة[٢]، فمن ناحية إثباتها فإن أدلة الإثبات الكمبيوترية يمكن الطعن عليها[٣]، بل ويمكن للجانى أن يدمرها تدميراً ذاتياً وإلحاق أضرار بالنظام المعلوماتى بأكمله، وعدم ترك أى أثر على جرمه[٤]، فهذه الجرائم ليست لها آثار خارجية مادية، كالعنف وسفك الدماء، وإنما تتم بالاعتداء الإلكترونى على أرقام ودلالات بالتلاعب فيها، كضرب رموز شفرية أو بالتحايل لمعرفة كلمة سر المستخدم، فضلاً عن ارتكاب هذه الجرائم في الخفاء وعدم وجود أثر كتابي على ارتكابها[٥].

---

(٣) وإذا كان المشرع الاتحادى الأمريكى لم يتعرض لتعريف الدخول غير المشروع، إلا أنه عرَّف تجاوز الولوج المصرح به فى البند (٦) من الفقرة الخامسة من المادة (١٠٣٠) من القانون المشار إليه بأنه« استغلال التصريح الممنوح بالدخول، = = بقصد الحصول على المعلومات المختزنة بالكومبيوتر أو تغييرها فى حين لا يمتد التصريح بالدخول لذلك».

Subsection 1030(E/6) «The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter».

(١) د. عباوى نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، المرجع السابق، ص٢٨٢.

(٢) أعطى المشرع المصرى فى القانون رقم ١٧٥ لسنة ٢٠١٨ للأدلة الرقمية ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي، وذلك فى المادة (١١) منه والخاصة بالأدلة الرقمية، والتى تنص على أن «يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون».

- وقد أشار البعض إلى ضرورة الاستعانة بما يُعرف بعلم الطب الشرعى الكمبيوترى الذى يتعلق بتقديم أدلة مقنعة للمحاكم حول جرائم الكمبيوتر، ويُعرَّف بأنه العلم الذى يستخدم تقنيات التحليل والتحقيق والأدوات اللازمة لتحديد وجمع ودراسة والحفاظ على الأدلة والمعلومات سواء المخزنة مغناطيسياً أو كانت مشفرة، وهذا العلم يحتاج إلى قدر كبير من الحدس والحساسية والمهارة من قبل العاملين فيه، فضلاً عن التكنولوجيا المعلوماتية بالغة التطور، ومن وسائل إثبات جرائم الكمبيوتر فى إطار هذا العلم أن هناك بعض الأدلة التى يتم حذفها من قبل المجرم، لكن من الممكن أن يتم استردادها باستخدام تكنولوجيا معينة، وكذلك استعادة المعلومات الهامة من التلف = = العرضى الذى يكون على درجة من الأهمية بمكان وبخاصة لرجال الأعمال والأجهزة الحكومية، وكذلك فك تشفير المعلومات التى تم تدميرها. فى ذلك انظر:

Liu Qian and others: Computer Forensics, P.R, pp.2,4,9.

(1) Neil Mac Ewan: The Computer Misuse Act 1990, P.R, p.962.

(٢) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة بأسيوط، ١٩٩٤، ص١٦.

وأما من ناحية مكافحتها فتواجهها أيضاً عدة صعوبات، منها قلة نسب الإبلاغ عن هذه الجرائم من قبل الضحايا خوفاً على سمعتها الائتمانية والمالية[١] بالإضافة إلى عجز جهات الملاحقة والتحقيق والادعاء عن الإلمام بزمام هذه الظاهرة[٢].

كما أن الأساليب المستخدمة في ارتكاب هذه الجرائم باتت على درجة كبيرة من التطور وتستخدم فيها تقنيات عالية بالغة الدقة والتعقيد، فإذا كان النظام المعلوماتى محاط بسياج من الحماية الفنية والتقنية منعاً لمحاولات الوصول والاعتداء عليه بأي صورة، فإن المجرم المعلوماتي يحاول جاهداً، وغالباً ما ينجح . في تحطيم وكسر هذا السياج والوصول إلى هدفه الإجرامي غير المشروع، ولا يكتفي بذلك، بل يضرب بسور من التدابير الأمنية والفنية حول جريمته لمنع اكتشافه والوصول إليه، كاستخدام كلمات سر أو دس تعليمات خفية أو باستخدم تقنيات التشفير، حتى يجعل من الوصول إلى دليل يدينه أمراً صعب المنال، وتُعد هذه إحدى العقبات الأساسية في إثبات ومكافحة الجريمة المعلوماتية بصفة عامة[٣].

---

(3)Neil Mac Ewan: The Computer Misuse Act 1990, P.R, pp.961-962; Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.56; Eric A. Fischer: Federal Laws Relating to cyber security, P.R, p.30.

- بل قد تلجأ بعض الشركات والمؤسسات وبخاصة المالية وبعض المواقع الإلكترونية إلى تقديم مكافأت أو منح لقراصنة الكمبيوتر، وهذا أمر شائع بالتحديد في الولايات المتحدة، وذلك للذين يستطيعون التحايل بنجاح على النظام المعلوماتى لهذه الكيانات وكشف أى عيب أو خلل في هذه الأنظمة، خوفاً على سمعتها من جهة، ورغبة منها في حماية أنظمتها الأمنية والارتقاء بها إلى أعلى مستوى من جهة أخرى. انظر:

Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, p.159.

(٤) فعلى سبيل المثال لم تكن شرطة المملكة المتحدة على المستوى المطلوب من الكفاءة اللازمة لمحاربة جرائم الإنترنت والكمبيوتر، لذا فى إبريل سنة ٢٠٠٤ أنشأت = = الحكومة الانجليزية وكالة خاصة أطلقت عليها وحدة مرحبا الوطنية لمكافحة الجريمة التكنولوجية The National Hi - Tech Crim Unit والمعروفة اختصاراً بـ NHTCU، وهى وحدة شرطية متخصصة فى مكافحة الجرائم الإلكترونية، وتقوم هذه الوحدة بأعمالها بالتنسيق مع مجموعة من الوكالات المتخصصة فى هذا الشأن، بما فى ذلك فرقة الجريمة الوطنية ودائرة الجمارك ودائرة الاستخبارات الجنائية الوطنية. فى ذلك انظر:

David Emm: Cybercrime and the law, P.R.

- وفى الولايات المتحدة وفى دراسة عن جرائم الحاسب فى ولاية كارولاينا الشمالية سنة ٢٠٠٣ أعدها Yearwad Dauglas L انتهت إلى أن ٤٠% من العاملين التابعين للمدعى العام فى هذه الولاية يملكون معرفة جيدة ومتخصصة عن جرائم الحاسب، بينما ٦٠% منهم لا يملكون تلك المعرفة. فى ذلك انظر:

Yearwood Douglas L: Prosecuting Computer Crime in North Carolina, P.R, p.9.

(١) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص٢٢.

- لذا حرص القانون المصرى رقم ١٧٥ لسنة ٢٠١٨ فى المادة (١٠) منه والخاصة بالخبراء على إنشاء سجلان بالجهاز القومى لتنظيم الاتصالات لقيد الخبراء يُقيد = = بأولهما الفنيون والتقنيون العاملون به، ويُقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين بالجهاز، ويطبق على هؤلاء الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء.

فضلاً عن البعد الدولى لهذه الظاهرة في بعض الأحيان، فالحدود الدولية أصبحت لا تمثل عائقاً أمام الإجرام المعلوماتي، فمن المتصور عدم تواجد الفاعل في مسرح الجريمة، ووجود دولة أو عدة دول تفصل بينه وبين النتيجة الإجرامية المترتبة على جريمته(١).

ولذلك قيل بأن الحماية المثلى في الفضاء الإلكترونى(٢) هي مزيج بين القانون والأسوار الخاصة التي يُشيدها المجنى عليه(٣)، والمقصود بهذه الأسوار الخاصة ما يتخذه المجنى عليه من تدابير تكنولوجية لحماية نظامه المعلوماتى الذى يضم جهاز الكمبيوتر والشبكات والبرامج، مثل الجدران النارية والمراقبة الآمنة والصارمة لعمليات الدخول وإجراءات التشفير لبعض المعلومات والبيانات الهامة واحتفاظه بسجلات تفصيلية مؤمنة لعمليات النظام المعلوماتى، هذا كله يساعد على تقديم أدلة مقبولة ومقنعة في مجال المحاكمات الجنائية والمدنية على السواء، ويلعب كذلك دوراً حاسماً في منع وتفشى هذه النوعية من الجرائم(٤).

٢٧- محل جريمة الدخول غير المشروع.

أوردت التشريعات محل المقارنة عدة مصطلحات فى مجال بيانها للمحل الذى يقع عليه فعل الدخول غير المشروع، فبعض هذه التشريعات عبَّرت عن هذا المحل بمصطلح الدخول أو الولوج العمدى إلى الكمبيوتر كما فى التشريع الاتحادى الأمريكى، وبعضها استخدم مصطلح الدخول المحظور على مواد الكمبيوتر كما فى التشريع الانجليزى، واستخدم المشرع المصرى الدخول غير المشرع- بصوره -على المواقع أو الحسابات الخاصة أو الأنظمة المعلوماتية أو البريد الإلكترونى على النحو المشار إليه، لذا وجب علينا تحديد المقصود بهذه المصطلحات بوصفها تمثل محل جريمة الدخول غير المشروع، هادفين من ذلك وضع الحدود الفاصلة لما يندرج تحت عباءة هذه الجريمة وما يخرج عنها، موضحين

(1) Derek Wyatt and others: Revision of the Computer Misuse Act, P.R, nos. 101, 105, pp.15-16.

(٢) عرَّفت اللجنة القومية الأمريكية لأمن المعلومات الوطنية في تقرير لها سنة ٢٠١٠ الفضاء الإلكترونى Cyberspace بأنه « نطاق عالمى متضمناً بيئة معلوماتية، والذى يتألف من شبكة مترابطة من البنية التحتية لنظم المعلومات بما فيها شبكة الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمتضمنة لعمليات المعالجة والتحكم».

Cyberspace is defined as «A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers». About that see: Eric A. Fischer: Federal Laws Relating to Cyber security, P.R, p.1.

(3) Liu Qian and others: Computer Forensics, P.R, p.3.

(1)Neil Mac Ewan: The Computer Misuse Act 1990, P.R, pp.963-964.

هذا المحل بداءةً فى التشريعين الأمريكى والانجليزى، ثم نبينه فى التشريع المصرى وذلك على النحو التالى:

٢٨- محل الجريمة فى التشريعين الأمريكى والانجليزى.

فى هذا المقام نبين المقصود بالكمبيوتر المعنى، ثم نعرج لبيان بقية المصطلحات التى استخدمها التشريعين الأمريكى والانجليزى كمحل لجريمة الدخول غير المشروع.

٢٨-١: الكمبيوتر المعنى:

عرَّف البعض جهاز الكمبيوتر -المتعارف عليه- بأنه أداة أو مجموعة من الأجهزة المترابطة أو المتصلة والتى تقوم بالمعالجة التلقائية للبيانات وفقاً لبرنامج محدد(١).

وقد أُثير التساؤل حول المقصود بالكمبيوتر فى معرض تطبيق النصوص القانونية وبخاصة الجنائية المتعلقة بجرائم الحاسب الآلى والإنترنت، فهل المقصود به الكمبيوتر المتعارف عليه سواء التقليدى أو المحمول؟، أم أن هذا المفهوم يمتد ليشمل أجهزة أخرى وإن كانت مسمياتها تختلف عن مسمى كمبيوتر؟.

والغاية من التساؤل المتقدم ليست مجرد ترف نظرى أو علمى، لتعلق الأمر بالتجريم والعقاب، إذ لو كان الأمر يقتصر فقط على الكمبيوتر المتعارف عليه فلا يمكن تطبيق النصوص القانونية وبخاصة الجنائية المتعلقة بجرائم الحاسب الآلى والإنترنت كما سبق القول على أى فعل – يمكن أن يُشكل جريمة جنائية من منظور هذه القوانين – إذا ارتكب بواسطة هذه الأجهزة الأخرى، أما إذا كان هذا المفهوم يمتد ليشمل أجهزة أخرى فيمكن بذلك انطباق النصوص التجريمية المقررة في هذا الشأن، مثل الدخول غير المشروع وإتلاف وسرقة المعلومات والتزوير والاحتيال ... إلخ.

من ناحية التشريعات محل المقارنة، فإن المشرع الانجليزى فى قانون ١٩٩٠، لم يورد تعريفاً لمصطلحات« كمبيوتر، برامج، بيانات» اعتقاداً من اللجنة التشريعية بأن خطوات التقدم التكنولوجي السريعة سوف تجعل من مثل هذه التعريفات عقيمة Outdated(٢).

أما المشرع الأمريكى فقد عرَّف الكمبيوتر المعنى فى هذا المقام، وذلك فى البند الأول من الفقرة الخامسة من المادة (١٠٣٠) من القانون الاتحادى الأمريكى لسنة ١٩٨٦، بأنه«

(1) Reform of the Computer Misuse Act 1990, P.R, p.7.

(2) Martin Wasip: Computer crimes and other crimes against information technology in the U.K, Rev.int.dr. pén, 1993, p.631.

جهاز لمعالجة البيانات إلكترونياً أو مغناطيسياً أو بصرياً أو كهروكيميائياً أو أي جهاز آخر عالي السرعة يقوم بوظائف منطقية أو حسابية أو تخزينية، ويشمل أي وسيلة لتخزين البيانات أو مرفق اتصالات يرتبط مباشرة أو يعمل بالاقتران مع هذا الجهاز، ولكن لا يشمل هذا المصطلح الآلة الكاتبة اليدوية والآلة الكتابة الآلية والآلة الحاسبة المحمولة باليد أو أي جهاز آخر مماثل»[١].

ويرى البعض أن التعريف الأمريكى المتقدم للكمبيوتر أقرب لتعريف النظام المعلوماتى، والذى عرَّفه بأنه يعنى«أجهزة الكمبيوتر وشبكات الاتصال الإلكترونية والبيانات المخزنة داخل الكمبيوتر وما يتعلق بمعالجتها واسترجاعها ونقلها وكذلك ما يتعلق بنظم التشغيل والحماية والصيانة»[٢].

وتبعاً لذلك تدخل شبكات الاتصال بما تتضمنه من مواقع إلكترونية مجال الحماية الجنائية المقررة بموجب هذا القانون[٣]، لذا يمكن القول بأن محل جريمة الدخول المشروع فى

---

(1)Subsection 1030(E/1)«The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device».

(2) Reform of the Computer Misuse Act 1990, P.R, p.7.

(٣) تزايدت أعداد مستخدمى شبكة الإنترنت بشكل هائل، ففي سنة ١٩٩٨ بلغ عدد مستخدمى الإنترنت حوالى ٢٠٠ ميلون مستخدم، وتضخم هذا العدد ليصل إلى مليار و ٤٠٠ مليون مستخدم سنة ٢٠٠٧. فى ذلك انظر:

Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.52. =

= وفى بيان للأمين العام للاتحاد الدولى للاتصالات سنة ٢٠١٧، أشار فيه إلى وصول عدد مستخدمى خدمات الإنترنت عالمياً بنهاية هذا العام إلى ٤.٣ مليار مستخدم. فى ذلك انظر موقع أخبار الأمم المتحدة:

https://news.un.org/ar/story/2017/07/280202

- وبطبيعة الحال يقابل هذا التزايد المستمر فى استخدام هذه الشبكة تزايد فى مشاكل إساءة استخدامها، وما يتصل بها من أنظمة معلوماتية أخرى.

- ولم تسلم المواقع الإلكترونية من التسللات والخروقات الإلكترونية، ومن أمثلة ذلك قيام مجموعة من القراصنة فى غضون عام ٢٠١١ بشن مجموعة من جرائم هجمات الحرمان من الخدمة المعروفة اختصاراً بـ DDoS شملت الموقع الانجليزى الخاص بوكالة مكافحة الجرائم المنظمة والخطيرة Serious Organized Crim Agency والمعروفة اختصاراً بـــسوكا (SOCA) وكذلك موقع الاستخبارات المركزية الأمريكية (CIA)، ومن أشهر المواقع الإلكترونية التى تعرضت لهذه النوعية من الهجمات وتأثرت بها موقع الأخبار العالمية وموقع شركة سونى العالمية وكذلك موقع شرطة ولاية أريزونا الأمريكية، وفي استطلاع أُجرى سنة ٢٠١١ في الولايات المتحدة عن قراصنة الموسيقى عبر الإنترنت، أشار إلى أن ٩٥% من الملفات الموسيقية تم تحميلها من الإنترنت بطريقة غير قانونية، وأن أكثر من ٧٥% من أجهزة الكمبيوتر في الولايات المتحدة يوجد بها ما لا يقل عن ملف موسيقى واحد تم تحميله بطريقة غير شرعية، وأن المواقع الإلكترونية التى بها هذه الملفات تستقبل أكثر من ١٣٦ مليون زائر يومياً. فى ذلك انظر:

Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, pp.159,165,169.

ضوء هذا المفهوم يتسع ليشمل أنظمة الحاسبات الآلية وما تحتويه فضلاً عن شبكات المعلومات(١).

وفى معرض تعليق بعض الفقه حول الكمبيوتر المعنى فى هذا المقام، أشار إلى أنه في ضوء تسارع خطا التكنولوجيا المعلوماتية، فإن مصطلح الكمبيوتر أصبح من الاتساع بمكان بحيث ينطوى تحت مفهومه أى جهاز عالى السرعة يُستخدم في معالجة البيانات ويُؤدى وظائف منطقية وعمليات حسابية ويتضمن وحدات تخزين، ويشمل هذا المفهوم الكمبيوتر المتعارف عليه سواء الثابت أو المحمول، يُضاف إليه الهواتف الذكية وألعاب الفيديو والعديد من أجهزة التليفزيون الحديثة التى يمكن توصيلها بالإنترنت، فضلاً عن شبكات الاتصالات، وعلى وجه العموم أى جهاز يعالج ويخزن المعلومات الرقمية(٢).

واستدل هذا الرأى بموقف القضاء الأمريكى في قضية الولايات المتحدة ضد Nill Scot Kramer سنة ٢٠٠١، والذى استخدم هاتفه المحمول فى تهديد وإجبار فتاة قاصر على ممارسة الجنس مع شخص آخر، حيث اعتبرت المحكمة أن الهاتف الخلوى يمكن اعتباره كمبيوتر، فهو أداة صالحة لإجراء عمليات حسابية ومنطقية بالإضافة إلى قدرته على تخزين المعلومات(٣).

وفى انجلترا يُجرِّم قانون الاتصالات الانجليزى لسنة ٢٠٠٣ ما يسمى باستنساخ هوية الهاتف المحمول Mobile Phone Cloning وذلك في المادة ١٢٥ منه، وفيه يتم نسخ هوية هاتف محمول ويُجرى المخالف اتصالات تحسب قيمتها على الهاتف الأصلى(٤)، وقد

---

(١) أصبحت شبكة الإنترنت إحدى وسائل التواصل الاجتماعى العالمية الجديدة تماماً والفريدة من نوعها، لاستخدامها من قبل عشرات الملايين من البشر يومياً من أجل التواصل مع بعضهم البعض، والوصول إلى كم هائل من المعلومات من مختلف أنحاء العالم، لذا رأى البعض أن هذا العالم (الإنترنت) ينبع غذاؤه الأول من تجاهل مطالبات الملكية والسيطرة والتقييد، وأنه لا بد وأن تتاح حرية التواصل وحرية تدفق المعلومات، فى حين رأى البعض الآخر أنه يجب تقييد حرية استعمال الإنترنت للحفاظ على = = الحقوق المالية لبعض الكيانات والأفراد من ناحية، وحماية خصوصياتهم من ناحية أخرى، وتوسط رأى ثالث هذين الرأيين بالقول بضرورة تشييد إطار قانونى متوازن لحماية الخصوصية والملكية بأشكالها عبر الإنترنت من جهة، وحماية حرية تدفق المعلومات من جهة أخرى. فى عرض هذه الآراء انظر:

Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p.1650.

(1)Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, P.R, p.209; Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, P.R, p.103.

(2)U.S .v Scott, 250 F.3d 550, 552 (7th Cir. 2001).

(1)Communications Offences, General Charging Practice, available online at: http://www.cps.gov.uk/legal/a_to_c/communications_offences/

طبقت بعض المحاكم الانجليزية على هذا الفعل قانون١٩٩٠- قبل إصدار قانون الاتصالات المشار إليه- على أساس اندراج الهاتف المحمول فى إطار الكمبيوتر المعنى فى قانون ١٩٩٠[١].

٢٨-٢: المقصود بمواد الكمبيوتر:

يُثار التساؤل كذلك حول المقصود بعبارة مواد الكمبيوتر الواردة فى المادة الأولى من قانون إساءة استخدام الكمبيوتر الانجليزى لسنة ١٩٩٠، وبخاصة فى ظل عدم تحديد هذا القانون المقصود بذلك، والذى برره البعض بأن الأمر يتعلق بمجال تكنولوجى متجدد يصعب على التشريع الإحاطة به حصرياً[٢]، ونرى أن المقصود بمواد الكمبيوتر كل ما يحتويه الكمبيوتر بمعناه سالف البيان، من برامج وبيانات ومعلومات أياً كان نوعها، وسواء كانت مخزنة داخله أو على وسائط التخزين الملحقة به، أو على شبكات الاتصال المتصل بها.

٢٨-٣: المقصود بالكمبيوتر المحمى:

استخدم المشرع الأمريكى مصطلح كمبيوتر محمى فى الكثير من بنود الفقرة الأولى من المادة (١٠٣٠) من القانون الاتحادى الأمريكى لسنة ١٩٨٦ وتعديلاته على النحو المار ذكره، وأوضح المقصود بهذا المصطلح فى البند الثانى من الفقرة الخامسة من ذات المادة بأنه يعنى[٣]« جهاز الكمبيوتر:(أ) الذى يقتصر استخدامه على مؤسسة مالية أو حكومة

(٢) حيث قضت محكمة Bow Street Magistrates Court بمعاقبة شخص يُدعى Ross Pearlstone بغرامة قدرها ٩٠٠ جنيه استرلينى، وذلك لمخالفته المادة الأولى والخاصة بالدخول المحظور وكذلك المادة الثانية والخاصة بالدخول المحظور بقصد التسهيل والتحريض على ارتكاب الجرائم من قانون١٩٩٠، لقيامه بالدخول المحظور لحساب هاتف رب عمله السابق وإجراء مكالمات منه تحتسب قيمتها على هاتف رب العمل، ومن الجدير بالذكر أن هذا الحكم كان أول تطبيق بالإدانة لقانون ١٩٩٠ الخاص بإساءة استخدام الحاسب الآلى في انجلترا. فى ذلك انظر:

R. v Ross Pearlstone (Bow Street Magistrates Court).About this judgment see: Michael J L Turner: Computer Misuse Act 1990, Cases a database published in 2014, these cases available online at: http://www.computerevidence.co.uk/Cases/CMA.htm

(3) Martin Wasip: Computer crimes and other crimes against information technology in the U.K, P.R, p.631; The Hacking of Computers and the Criminal Law, P.R.

(1)Subsection 1030(E/2) «The term "protected computer" means a computer: (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institutionor the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States».

الولايات المتحدة، أو كان لا يقتصر على هذا الاستخدام، ولكن يؤثر السلوك الذي يشكل الجريمة على الاستخدام الحاصل من قبل أو من أجل المؤسسة المالية الحكومية؛ أو (ب) الذى يُستخدم فى أو يُؤثر على التجارة بين الولايات أو التجارة الخارجية أو الاتصالات، بما فى ذلك جهاز الكمبيوتر الذى يقع خارج الولايات المتحدة، لكنه يُستخدم بطريقة تُؤثر على التجارة بين الولايات أو التجارة الخارجية أو الاتصالات الخاصة بالولايات المتحدة»[١].

٢٩- محل الجريمة فى التشريع المصرى.

حسم المشرع المصرى أى جدل قد يُثار بشأن محل جريمة الدخول غير المشروع وصوره والواردة فى المواد (١/١٤) و(١٥) و(١/٢٠) من القانون رقم ١٧٥ لسنة ٢٠١٨ على النحو المشار إليه، بتحديده فى هذه النصوص لمحل هذه الجريمة الذى قد يكون موقعاً أو حساباً خاصاً أو نظاماً معلوماتياً أو بريداً إلكترونياً، وتعريفه لهذه المصطلحات فى المادة الأولى من هذا القانون والخاصة بالتعريفات، فعرَّف الموقع فى البند رقم (١٣) من المادة المشار إليها بأنه« مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة»، وعرَّف الحساب الخاص فى البند رقم (١٥) من ذات المادة بأنه « مجموعة من المعلومات الخاصة بشخص طبيعى أو اعتبارى، تخول له دون غيره الحق فى الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتى»، وعرَّف النظام المعلوماتى فى البند رقم (١١) بأنه « مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية»، وعرَّف البريد الإلكترونى فى البند رقم (١٦) بأنه « وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعى أو إعتبارى، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما في حكمها».

فضلاً عن تعريفه للكمبيوتر أو الحاسب فى البند (٢٣) من ذات المادة بأنه « كل جهاز أو معدة تقنية تكون قادرة على التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات».

---

(٢) يرى البعض أن مصطلح «كمبيوتر محمى» هو اصطلاح قانونى ليست له علاقة بنظم أمن الكمبيوتر. انظر:=

= Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, P.R, p.4; Charles Doyle: Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS 7-5700, October 15, 2014, p.18; Kristin Westerhorstmann:The Computer Fraud and Abuse Act, P.R, p.151.

المطلب الثانى
أساس المسئولية الجنائية فى جريمة الدخول غير المشروع

٣٠- تمهيد:

تقوم المسئولية الجنائية فى جريمة الدخول غير المشروع للأنظمة المعلوماتية فى حق من يقارف أية صورة من صور الدخول غير المشروع المار ذكرها وفقاً لقوانين إساءة استخدام الحاسب الآلى أو جرائم تقنية المعلومات فى التشريعات محل المقارنة.

لكن ما هو الأساس الذى تقوم وترتكز عليه المسئولية الجنائية وفقاً لهذه التشريعات؟ وبخاصة فى ظل اتخاذ بعض المحاكم المدنية الاتحادية الأمريكية من قواعد المسئولية التقصيرية أساساً للمسئولية المدنية الناشئة عن مخالفة القانون الاتحادى لعام ١٩٨٦، واستقاء بعض المحاكم الجنائية الاتحادية فى الكثير من الحالات لأحد أركان المسئولية التقصيرية، وهى علاقة العمل-الممثلة لعلاقة السببية بين الخطأ والضرر فى إطار المسئولية المدنية- كأساس للمسئولية الجنائية، مما أثار انتقاداً لتوجه المحاكم الجنائية فى هذا الشأن(١).

يدعونا هذا الحال لمعرفة الأساس الذى ترتكز عليه المسئولية الجنائية فى هذه الجريمة فى التشريعين الأمريكى والانجليزى، ثم نختم ببيان الضرر المتصور فى حالة الدخول المجرد للأنظمة المعلوماتية وذلك كما يلى.

٣١- أساس المسئولية الجنائية فى التشريع الأمريكى.

فى سبيل بياننا لأساس المسئولية الجنائية فى جريمة الدخول غير المشروع فى ضوء التشريع الأمريكى، يجب التعرض أولاً للوجهتين الأساسية والمضافة للقانون الاتحادى الأمريكى لسنة ١٩٨٦ وتعديلاته، ثم نعرض لأساس المسئولية المدنية الناشئة عن جرائم إساءة استخدام الحاسب الآلى، ونختم ببيان أساس المسئولية الجنائية عن هذه الجرائم.

٣١-١: الوجهة الأساسية للقانون الاتحادى الأمريكى:

---

(١) أشارت المذكرة التفسيرية لاتفاقية بودابست لعام ٢٠٠١ فى معرض تعليقها على المادة الثانية من هذه الاتفاقية والخاصة بالولوج غير القانوني والعمدى إلى تأسيس المسئولية الجنائية فى هذه الجريمة على كونها «الجريمة الأساسية التى تنطوي على تهديد وتعد على أمن النظام المعلوماتي، وبالتالي فإن مجرد التدخل غير المصرح = = به بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتى، كل ذلك يجب أن يعتبر غير قانوني فى حد ذاته كمبدأ عام». مشار لهذه المذكرة فيما سبق.

تُعد الوجهة الجنائية هى الوجهة الأساسية للقانون الاتحادى الأمريكى بشأن الغش وإساءة استخدام الكمبيوتر لسنة ١٩٨٦ وتعديلاته، فالمحاكم الأمريكية الاتحادية تطبق هذا القانون حصراً على الجرائم الفيدرالية بما يتوافق مع صريح نصوصه والغاية التى شُرِّع من أجلها، وعبَّر عن ذلك بعض الفقه الأمريكى بالقول بأن هذا القانون مصمم لحماية الحواسيب وما يرتبط بها من معلومات فيدرالية من الناحية الجنائية على النحو الوارد بنصوصه، أما في حالة وجود جريمة متعلقة بالحاسب الآلى وقعت ضد شخص طبيعى أو مؤسسة أو شركة أو وكالة خاصة، فتطبق في هذا الشأن النصوص الجنائية المتعلقة بجرائم الحاسب الآلى حسب قانون كل ولاية(١).

٣١-٢: الوجهة المضافة للقانون الاتحادى الأمريكى:

أجرى المشرع الاتحادى الأمريكى عدة تعديلات على القانون الاتحادى سالف الذكر، والتى بموجبها باتت حمايته تنبسط على جميع المصالح سواء الفيدرالية أو الخاصة، ويجب التأكيد قبل أى شيء على أن لفظ المصالح الخاصة المعنى ينصرف إلى الجانب المدنى فقط دون الجانب الجنائى(٢).

ففى سنة ١٩٩٤ أدخل المشرع الاتحادى على القانون المذكور تعديلاً بموجبه أجاز لأى شخص - بمعناه الذى حدده هذا القانون - إمكانية رفع دعوى مدنية بالتعويض أمام المحاكم الاتحادية في حالة مخالفة أحكام هذا القانون وترتب على ذلك ضرر أو خسارة من جرَّاء الفعل المجرَّم(٣).

---

(1)Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, p.151.

(١) وبناء على ذلك يجوز للمضرور من الجريمة سواء كان كيان حكومى أو خاص رفع دعوى مدنية بالتعويض أمام المحاكم الاتحادية، وجدير بالذكر أن المشرع الاتحادى الأمريكى استخدم لفظ «شخص» عند الحديث عن تعويض الضرر، وحدد المقصود بهذا اللفظ فى البند (١٢) من الفقرة الخامسة من المادة (١٠٣٠) من القانون المذكور بأنه يعني «أي فرد أو شركة أو مؤسسة أو مؤسسة تعليمية أو مؤسسة مالية أو كيان حكومي أو كيان قانوني أو أى كيان آخر».

Subsection 1030(E/12) «The term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity».

(٢) أجازت الفقرة السابعة من المادة (١٠٣٠) من القانون الاتحادى لأي شخص- بالوصف المشار إليه لمصطلح شخص- يعاني من ضرر أو خسارة بسبب انتهاك هذه المادة أن يقوم برفع دعوى مدنية ضد المخالف للحصول على التعويضات الجابرة للأضرار، ولكن قيد المشرع قبول دعوى التعويض برفعها فى غضون عامين من تاريخ اكتشاف الجريمة أو الضرر المترتب عليها.

Subsection 1030(G) «Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. … No action may be brought under this subsection unless such action is begun within 2 years of the date of the act = = complained of or the date of the discovery

٣١-٣: أساس المسئولية المدنية أمام المحاكم الاتحادية:

فى ضوء التعديل المشار إليه اتخذت بعض المحاكم الاتحادية الأمريكية من قواعد المسئولية التقصيرية أساساً للمسئولية المدنية فى دعاوى التعويض المرفوعة أمامها، سواء كان المضرور شخص خاصاً أو عاماً كالحكومة الاتحادية أو إحدى الولايات أو أية وكالة أو إدارة عامة بهما.

وبشأن عنصرى الخطأ وعلاقة السببية كركنان من أركان المسئولية التقصيرية، قضت إحدى الدوائر المدنية بالمحكمة الاتحادية الأمريكية سنة ٢٠٠٦ بإلزام أحد الموظفين بالتعويض، ويُدعى Citrin Jacob الموظف بإحدى الشركات الوطنية وتُدعى International Airport Centers لمخالفته البند الخامس من الفقرة الأولى من المادة (١٠٣٠) من القانون الاتحادى الأمريكى لسنة ١٩٨٦ وتعديلاته، لتجاوزه الإذن الممنوح له بالدخول، وقيامه بحذف ملفات ومعلومات من الكمبيوتر الخاص بالشركة قبل استقالته منها، وذلك بهدف إخفاء مخالفات ارتكابها أثناء عمله بها[١].

وذهبت المحكمة إلى أن رابطة السببة تتمثل فى علاقة العمل التى تربط بين الشركة المدعية والمدعى عليه، إذ أن هذه العلاقة هى التى منحت له حق استخدام الكمبيوتر الخاص بالشركة، أما عن الخطأ فيتمثل فى تجاوز المتهم للتصريح الممنوح له بالولوج للكمبيوتر، والذى لا يمتد إلى تبديل أو تغيير أو حذف المعلومات المخزنة فيه، وبقيام المتهم بزرع وتثبيت البرنامج الذى أدى إلى حذف الملفات والمعلومات المخزنة بالكومبيوتر الخاص بالشركة، فإنه قد ارتكب خطأً لمخالفته البند المشار إليه[٢].

---

of the damage, ….» . about this see: Warren Thomas: Civil Liability under the Computer Fraud and Abuse Act (CFAA), Law Library of the Georgia State University College of Law 2010, Paper 22, p.2; Alden Anderson: Comment: The Computer Fraud and Abuse Act, P.R, p.456; See also: Computer Fraud and Abuse Act (CFAA), an article From Internet Law Treatise, last modified on 24 April 2013, and available online at: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA).

(1) International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. March 8, 2006).

(1) Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, P.R, p.214; Alden Anderson: Comment, The Computer Fraud and Abuse Act, P.R, p.453, 458; See also: Computer Fraud and Abuse Act (CFAA), an article From Internet Law Treatise, P.R; Computer Fraud and Abuse Act, an article published on 2015, and available online at: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

أما بشأن الضرر[١] فهو يشمل ما لحق المضرور من خسارة وما فاته من كسب، ويندرج في إطاره أيضاً تكاليف تقييم الأضرار، واستعادة البرامج والمعلومات، وأجور الفنيين القائمين بهذه المهام، وقيمة المبيعات وعائدات الإعلانات التى فُقدت، وكذلك الضرر الحاصل بالنسبة للسمعة والشهرة والتكاليف الأخرى المعقولة، لكن لابد من الطلب الصريح من جانب المضرور بتعويض الأضرار مع بيان مواطنها[٢].

ونهجت المحاكم الأمريكية هذا النهج فيما يخص تقدير الضرر، وعلى سبيل المثال في قضية الولايات المتحدة ضد شخص يدعى Middleton والذى قضت المحكمة بإلزامه بالتعويض عن الضرر الناجم عن إتلافه لجهاز الكمبيوتر الخاص بالمقاطعة الشمالية لولاية كاليفورنيا، والذى ولج إليه بدون إذن ثم قام بحذف قواعد البيانات الداخلية المخزنة بداخله، وأدخلت المحكمة في تقديرها للتعويض نفقات إصلاح الضرر وكذلك نفقات القائمين على هذا الإصلاح، وأكدت على أن جبر الضرر حق للمضرورين سواء أكانوا أشخاصاً عامة أو خاصة[٣].

٣١-٤: أساس المسئولية الجنائية أمام المحاكم الاتحادية:

اتخذت بعض المحاكم الجنائية الاتحادية من علاقة العمل كأساس للمسئولية الجنائية فى حالتى الولوج لجهاز الكمبيوتر بدون إذن أو تجاوز التصريح الممنوح بالولوج، منها ما جاء بقضية الولايات المتحدة ضد Rodriguez الموظف بإدارة الضمان الاجتماعى لتجاوزه

---

(2) Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, P.R, pp.41, 44; See also: Charles Doyle: Cybercrime: An Overview of the Federal Computer Fraud, P.R, pp. 24,38; Alden Anderson: Comment, The Computer Fraud and Abuse Act, P.R, p.456 – 457; Warren Thomas: Civil Liability under the Computer Fraud and Abuse Act (CFAA), an article From Internet Law Treatise, P.R, P.3.

(٣) عرَّف البند(١١) من الفقرة الخامسة من القانون الاتحادى الأمريكى لسنة ١٩٨٦ وتعديلاته الخسارة بأنها تعني «أي تكلفة معقولة لأى ضحية، بما في ذلك تكلفة الإجراءات المتخذة حيال الجريمة، وإجراءات تقييم الأضرار، وتكلفة استعادة البيانات أو البرامج أو المعلومات أو النظام لحالته قبل ارتكاب الجريمة، وأي عائد مفقود أو تكلفة متكبدة أو أية أضرار تبعية أخرى ناتجة عن انقطاع الخدمة». =

= Subsection 1030(E/11)«The term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service».

(1)U.S .v. Middleton, 231 F.3d 1207 (9th Cir. 2000).

الوصول المصرح به للكمبيوتر الخاص بهذه الإدارة، وانتهاكه لقواعد العمل بعرضه لمعلومات شخصية للعديد من النساء المسجلات بهذه الإدارة(١).

وذهبت المحكمة فى حكمها إلى أن المسئولية الجنائية المثارة وفق القانون الاتحادى تتأسس نتيجة إخلال الموظفين – أو الموظف – بعقود أعمالهم مع أرباب أعمالهم – الحكومة الأمريكية الاتحادية أو المؤسسات أو الوكالات الحكومية– التى تقضى بعدم الولوج غير المشروع، أو تجاوز التصريح الممنوح بالولوج.

وقد لاقى هذا الاتجاه القضائى نقد شديداً في اعتماده على علاقة العمل كأساس للمسئولية الجنائية فى حالتى الولوج لجهاز الكمبيوتر بدون إذن أو تجاوز التصريح الممنوح بالولوج، فالمفترض وفقاً لهذا التوجه القضائى قيام رب العمل بتوجيه موظفيه إلى عدم القيام بهذا الفعل، سواء الولوج بدون إذن أو تجاوز الولوج المصرح به، ويتساءل منتقدى هذا التوجه عن الحل في حالة عدم قيام رب العمل بتوجيه موظفيه صراحة إلى هذه الالتزامات؟ لذا يرون أن تأسيس المسئولية الجنائية على معيار العلاقة الوظيفية معيار غير صحيح، وأن المعيار المناسب لقيامها سواء للموظف أو غيره، وسواء في حالة الولوج بدون إذن أو فى حالة تجاوز التصريح بالولوج، هو ثبوت قيام المستخدم بالتحايل على واحد أو أكثر من التدابير التكنولوجية أو المادية التى يتم تصميمها لاستبعاد أو منع الأشخاص غير المرخص لهم بالدخول أو لمنع تجاوز التصريح الممنوح بالدخول للجهاز (٢).

٣٢- أساس المسئولية الجنائية فى التشريع الانجليزى.

لم يُثر مثل هذا الخلاف فى التشريع الانجليزى، فالفقه والقضاء الانجليزيان متفقان على تأسيس المسئولية الجنائية فى حالة مخالفة قانون إساءة استخدام الحاسب الآلى لسنة١٩٩٠، وبخاصة في حالتى الدخول بدون تصريح وتجاوز التصريح الممنوح بالدخول، على ذات المعيار الذى اعتمده غالبية القضاء والفقه الأمريكيين، وهو ثبوت قيام المستخدم بالتحايل على واحد أو أكثر من التدابير التكنولوجية أو المادية التى يتم تصميمها لاستبعاد أو منع الأشخاص غير المرخص لهم بالدخول أو لمنع تجاوز التصريح الممنوح بالدخول للجهاز (٣)،

(2)U. S v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

(1) Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, P.R, pp.230, 234,235.

(١) لكن قيد المشرع الانجليزى قبول الدعوى الجنائية عن الجريمة موضوع المادة الأولى والخاصة بالدخول المحظور على مواد الكمبيوتر بمدتين وفقاً لما أورده بالفقرتين الثانية والثالثة من المادة (١١) من قانون١٩٩٠، الأولى: عدم مرور ستة أشهر من تاريخ إحاطة علم

وهذا المعيار يصلح كأساس للمسئولية الجنائية فى جريمة الدخول غير المشروع بصورها الواردة فى القانون المصرى المشار إليه.

ومن التطبيقات القضائية الانجليزية فى هذا الشأن ما قضت به محكمة Southwark Crown Court في ٢٠١٢/٧/٢٧ بمعاقبة شخص يُدعى Junaid Hussain، البالغ من العمر ١٨سنة، والملقب بالمخادع، بالحبس لمدة ستة أشهر، لمخالفته المادة الأولى من قانون إساءة الحاسب الآلى لسنة ١٩٩٠ والخاصة بالدخول المحظور، لقيامه باختراق حسابKaty Kay أحد المستشارين السابقين لتونى بلير– رئيس الوزراء البريطانى الأسبق– عبر Gmail ونشر التفاصيل الشخصية التى استقاها من ١٥٠ اتصال من موقع المجنى عليه بما في ذلك اتصالات لتونى بلير وأسرته(١).

وما قضت به محكمة Cardiff Magistrates Court(٢) بمعاقبة شخص يُدعى Oliver Baker بالحبس لمدة ٤ أشهر، لمخالفته المادة الأولى المار ذكرها من قانون١٩٩٠، لقيامه باختراق نظام الحاسب الآلى لإحدى الجمعيات فى ويلز والاطلاع على الرسائل البريدية الحساسة والخاصة بهذه الجمعية، وكذلك الرسائل الخاصة بمخالفات الوقوف المخالف للسيارات، وباستئناف المتهم لهذا الحكم أمام محكمة Cardiff Crown Court أيدت المحكمة الاستئنافية قضاء أول درجة في الجنحة رقم ٩٢٨ لسنة ٢٠١١(٣).

ووصل الأمر بالبعض تحت الرغبة الملحة فى مواجهة هذه النوعية من الجرائم وانحسار مدها، إلى المنادة بقيام المسئولية الجنائية لأرباب العمل إذا صدرت تلك المخالفات من أحد عماليهم أو موظفيهم مستخدماً في ارتكابها أجهزة الكمبيوتر أو الاتصالات الخاصة

المدعى العام بالأدلة التى تبرر اتخاذ الإجراءات الجنائية ضد الجانى، والثانية: وفى جميع الأحوال لا يجوز اتخاذ ثمة إجراء بعد مرور أكثر من ثلاث سنوات من تاريخ ارتكاب الجريمة، ونص هاتين الفقرتين:

- Paragraph (2) from section (11) «Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge».
- Paragraph (3) from section (11) « No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence».

(2) R .v Junaid Hussain (Southwark Crown Court 27/7/2012).

(1) R. v Oliver Baker (Cardiff Crown Court 2011, (2011 EWCA Crim 928).

(٢) وأكدت هذه المحاكم على تأسيس المسئولية الجنائية للمتهمين لقيامهم بالدخول المحظور على مواد الكمبيوتر عن طريق التحايل على التدابير التكنولوجية المصممة لمنع ذلك. انظر:

Edmand Dester Thipursian and others: Case Study – News of the World Phone Hacking Scandal, P.R, no.7.

بالعمل، تأسيساً ما يُعرف بالمسئولية بالإنابة أو المسئولية غير المباشرة Liability Vicarious، فيُعد صاحب العمل مسئولاً جنائياً عن الأفعال غير المشروعة أو المنطوية على إهمال جسيم والصادرة عن أحد عمَّاله أو موظفيه، لذا يجب عليهم عدم التهاون تجاه الدخول المحظور للأنظمة المعلوماتية من قبل العاملين لديهم سواء الخاصة بشخص خاص أو عام(١).

ومن جانبنا لا نستطيع التسليم بهذا الرأى، لأن مسئولية رب العمل فى هذا المقام مسئولية مدنية لجبر الأضرار الناشئة عن خطأ أو جريمة موظفيه، أما المسئولية الجنائية لرب العمل فلا تقوم فى هذا الشأن إلا بثبوت اشتراكه فى الجريمة التى ارتكبها عامله إعمالاً لمبدأ الشرعية الجنائية بمفهومه الواسع.

٣٣- الضرر المتصور فى حالة الدخول المجرد.

انتهينا فى المطلب السابق إلى أن جريمة الدخول غير المشروع للأنظمة المعلوماتية تُكيف من منظور الركن المادى لها، على أنها من جرائم السلوك المجرد، والتى يُكتفى فى قيام ركنها المادى بتحقق السلوك الإجرامى فقط، بغض النظر عن تحقق نتيجة له من عدمه، فمجرد تحقق السلوك الإجرامى المتمثل فى فعل الدخول المشروع بأى صورة له مع توافر الركن المعنوى كاف لقيام هذه الجريمة، وبالتالى فإن الضرر ليس بعنصر متطلب لقيام هذه الجريمة، ولكنه عنصر متطلب وفعال عند نظر دعاوى التعويض المدنية الناشئة عنها، وهذا يدعونا لمعرفة الضرر المتصور من الدخول غير المشروع والمجرد للأنظمة المعلوماتية، والذى لا يُتبع بثمة فعل آخر يتضمن المساس بأى صورة بمحتويات هذه الأنظمة.

نرى أن الضرر المتصور من فعل الدخول المجرد هو إمكانية الحصول على معلومات من النظام المعلوماتى، والتى قد تكون على قدر من الأهمية بمكان(٢)، وهذا ما اتجه إليه الفقه الأمريكى وهو بمعرض تفسير عبارة الحصول على معلومات الواردة في البند الأول من

(3) An article entitled Crime, P.R.

(١) على سبيل المثال فى غضون عام ١٩٨٨ نجح «Edward Austin Singh» البالغ من العمر ٢٣ عاماً في اختراق ٢٠٠ حاسب في دول مختلفة، من بينها أنظمة حاسبات تابعة لوزارة الدفاع البريطانية ووكالة ناسا«NASA» الأمريكية لأبحاث الفضاء وبعض الشبكات المعلوماتية العسكرية الأمريكية بما فيها شبكة«Mill net»، وذلك باستخدام بعض تسهيلات النظام المعلوماتي لإحدى الجامعات، كما نجح الألماني الغربى «Marcus Hess» البالغ من العمر ٢٤ عاماً في التغلغل بطريق الاتصال البعدي في منظومات ٣٠ حاسب بالولايات المتحدة الأمريكية تتعامل في معلومات عسكرية، والحصول منها على معلومات لها هذه الصفة، فضلاً عن = = بيانات تتعلق بأبحاث علمية.فى ذلك انظر: د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص١٣٨.

الفقرة الأولى من نص المادة (١٠٣٠) من القانون الاتحادى الأمريكى لسنة ١٩٨٦ وتعديلاته[١].

فيندرج في إطار الحصول على المعلومات بالإضافة إلى تحميلها أو نسخها مجرد المطالعة البصرية لها، والتى تظهر على شاشة الكمبيوتر، وفعل الحصول هنا – بالمطالعة البصرية – لا يتضمن الاستحواذ المادى على هذه المعلومات بواسطة أى كيان مادى كشريط ممغنط أو اسطوانة أو بطباعتها أو بأى أداة أخرى صالحة لتخزين المعلومات، وبالتالى حرمان صاحبها الشرعى منها، سواء كان جهة حكومية أو خاصة أو شخص طبيعى، وسواء بشكل مؤقت أو بشكل دائم[٢].

ومن الجدير بالذكر أن المحاكم الأمريكية كانت قبل تعديل القانون الاتحادى سنة ١٩٩٦ مترددة في اعتبار المطالعة البصرية للمعلومات والتى تظهر على شاشة الحاسب الآلى من قبيل الحصول على المعلومات أو تشكيلها لجريمة سرقة سواء بسواء مع سرقة العناصر المادية نظراً للطابع المعنوى للمعلومات.

المبحث الثانى
الركن المعنوى لجريمة الدخول غير المشروع وعقوبتها

٣٤- تمهيد وتقسيم:

لا يكفى لوقوع الجريمة أن يرتكب الشخص الفعل المكون للركن المادى لها كما هو موصوف به في نموذجها القانونى، وإنما يلزم أيضاً أن يكون قد ارتكب خطأً، وهذا الخطأ إما أن يكون خطأً عمدياً يمثل الركن المعنوى في الجرائم العمدية ويُعبَّر عنه بالقصد الجنائى، أو خطأ غير عمدى يمثل الركن المعنوى في الجرائم غير العمدية[٣].

وجريمة الدخول غير المشروع للأنظمة المعلوماتية تُعد من الجرائم العمدية، فيتمثل ركنها المعنوى في القصد الجنائى، والذى بتوافره إلى جانب توافر الركن المادى لها تقوم هذه الجريمة، وبالتالى تُستحق العقوبة التى رصدها المشرع لها.

---

(1)Kristin Westerhorstmann: The Computer Fraud and Abuse Act, P.R, p.150; Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, P.R, p.18; Charles Doyle: Cybercrime: An Overview of the Federal Computer Fraud, P.R, p. 17.

(٢) فى هذا المعنى انظر د. عباوى نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، المرجع السابق، ص٢٨٢.

(١) د. محمود نجيب حسنى، القسم العام، المرجع السابق، ص٦٤٤، د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٥٩٩ -٦٠٠.

وفى هذا المبحث نبين الركن المعنوى لهذه الجريمة، نتبعه ببيان عقوبتها فى التشريعات محل المقارنة، على أن نختمه بإيراد بعض التطبيقات القضائية لهذه الجريمة فى ضوء هذه التشريعات، وذلك من خلال ثلاثة مطالب على النحو التالى.

المطلب الأول: الركن المعنوى لجريمة الدخول غير المشروع.

المطلب الثانى: عقوبة جريمة الدخول غير المشروع.

المطلب الثالث: تطبيقات قضائية لجريمة الدخول غير المشروع.

المطلب الأول
الركن المعنوى لجريمة الدخول غير المشروع

٣٥- تمهيد:

يُمثل القصد الجنائى الركن المعنوى في الجرائم العمدية كما سبق القول، والذى نوضحه من خلال بيان تعريفه وعناصره ووقت توافره وكيفية إثباته، وهذا كله بالتطبيق على جريمة الدخول غير المشروع للأنظمة المعلوماتية.

٣٦- تعريف القصد الجنائى وعناصره.

يُعرَّف القصد الجنائى بأنه اتجاه إرادة الجانى نحو ارتكاب الجريمة، مع العلم بتوافر أركانها القانونية(١)، وبمعنى آخر توجيه الإرادة لإحداث أمر يعاقب عليه القانون عن علم بالفعل وبتجريمه قانوناً(٢)، ويُعد القصد الجنائى من الأمور الباطنية –غير الظاهرة– التى يضمرها الجانى، وتدل عليها بطريق مباشر أو غير مباشر الأعمال المادية المحسوسة التى تصدر عنه(٣).

ويتكون القصد الجنائى من عنصرين هما العلم والإرادة، أما العلم بأركان الجريمة فيتمثل في علم الجانى بالوقائع التى تقوم بها الجريمة، والتى يحددها نموذجها القانونى– والتى تشمل السلوك الإجرامى والنتيجة المترتبة عليه وعلاقة السببية التى تربط بينهما فى الجرائم المادية، والعلم بالسلوك الإجرامى فقط فى جرائم السلوك المجرد– فالعلم هو الصورة

(١) د. مأمون سلامة، القسم العام، المرجع السابق، ص٣٢٧، د. عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص٤٥٨.

(٢) د. السعيد مصطفى السعيد، القسم العام، المرجع السابق، ص٣٨٦، د. محمود نجيب حسنى، القسم العام، المرجع السابق، ص٦٥٠.

(٣) نقض ١٩٦٩/٤/٢١، مجموعة أحكام النقض، س٢٠ رقم٥٣١ ص١١١.

الذهنية التى تتولد لدى الجانى عن عناصر الجريمة[١]، أما الإرادة فيُقصد بها تلك القوة النفسية التى تدفع الجانى إلى ارتكاب جريمته، على الرغم من إحاطته علماً بكافة الوقائع المتعلقة بها، ويلزم أن تكون إرادة الجانى واعية ومدركة وتتوافر لديه حرية الاختيار، فإذا كانت إرادته معيبة إما لصغر السن أو الجنون أو السكر غير الاختيارى أو وقوعه تحت إكراه مادى أو معنوى، فإرادته يشوبها عيب من عيوب الإرادة تنتفى معها حرية الاختيار لديه، ومن ثم تنتفى عنه المسئولية الجنائية[٢].

وعلى ذلك يجب أن يتوافر القصد الجنائى بعنصريه المار ذكرهما لقيام الركن المعنوى لجريمة الدخول غير المشروع فى الحالات التى يمكن أن يتخذها السلوك الإجرامى فى هذه الجريمة، وهى حالة الدخول العمدى غير المشروع من الأساس للنظام المعلوماتى، وكذلك حالة التجاوز العمدى للتصريح الممنوح بالدخول. فيجب أن يكون الجانى على علم بأن سلوكه ينطوى على دخول غير مشروع للأنظمة المعلوماتية، أو أنه يتجاوز بفعله للتصريح أو الإذن الممنوح له بالدخول، فيلج إلى ملفات أو برامج وبصفة عامة إلى أى من محتويات النظام المعلوماتى، والتى لا يشملها التصريح أو الإذن الممنوح له، واتجاه إرادته للدخول المحظور من الأساس أو لتجاوز التصريح الممنوح بالدخول، وقد عبَّرت التشريعات محل المقارنة عن هاتين الحالتين فى مجال إشارتها للقصد الجنائى بالتعمد والعلم واتجاه النية إلى ارتكاب الأفعال موضوع التجريم، كما فى البنود (٤،٢،١) من الفقرة الأولى من المادة «١٠٣٠» من القانون الاتحادى الأمريكى لسنة ١٩٨٦. والمادة الأولى من القانون الانجليزى لسنة ١٩٩٠ والخاصة بالدخول المحظور على مواد الكمبيوتر[٣].

أما الحالة الثالثة فتتحقق بعلم وامتناع الجانى عن قطع الاتصال مع النظام المعلوماتى الذي حدث في البداية بطريق الخطأ، وإتجاه إرادته إلى عدم قطع هذا الاتصال والإبقاء عليه رغم علمه بأنه ليس له الحق فيه[٤]، وعبِّر المشرع المصرى فى مجال بيانه للقصد الجنائى فى هذه الحالات الثلاث بكلمة العمد فى المواد(١/١٤) و(١٥) و(١/٢٠) على النحو الوارد بنصوص هذه المواد.

---

(١) د. مأمون سلامة، القسم العام، المرجع السابق، ص٣٣١، د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٦١٢-٦١٣.

(٢) د. محمود محمود مصطفى، القسم العام، المرجع السابق، ص٤١٦ وما بعدها، د. محمود نجيب حسنى، القسم العام، المرجع السابق، ص٦٧٩، د.عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص٤٤٣ وما بعدها.

(1)Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.41; Computer Misuse Act 1990, from Wikipedia, P.R; Reform of the Computer Misuse Act 1990, P.R, pp.4,13.

(٢) د. عمر الفاروق الحسينى، المرجع السابق، ص ١٣٠.

لكن يجب فى جميع الأحوال أن تكون إرادة الجانى واعية ومدركة وتتوافر لديه حرية الاختيار، فلا يشوب إرادته عيب من عيوب الإرادة التى تنتفى معها حرية الاختيار لديه، ومن ثم تنتفى عنه المسئولية الجنائية. وفى ضوء ما تقدم ينتفى القصد الجانى فى هذه الجريمة، ومن ثم تنتفى الجريمة كلها فى الحالات الآتية.

١- الدخول المصرح به من مالك النظام المعلوماتى أو صاحب الحق فيه، وكذلك فى حالة ما إذا كان الدخول إلى النظام بالمجان ومتاحاً للجمهور[١].

٢- الدخول أو التجاوز فى الدخول الحاصل بطريق الخطأ، وقطع الاتصال بالنظام فور اكتشاف القائم بأيهما لذلك.

٣- ثبوت أن الدخول أو التجاوز فى الدخول كان نتيجة لإكراه مادى أو معنوى، أو لتوافر عيب من عيوب الإرادة التى تنتفى معها حرية الاختيار.

ومن التطبيقات القضائية لانتفاء المسئولية الجنائية فى مقام الجريمة محل البحث، ما قضت به محكمة Southwark Crown Court في ١٩٩٣/٥/٢١، بمعاقبة شخصين الأول يُدعى Strickland والثانى يُدعى Woods بالحبس لمدة ستة أشهر لمخالفتهما المادة الأولى والخاصة بالدخول المحظور، وكذلك المادة الثالثة والخاصة بالتعديل والتحويل غير المصرح به فى مواد الكمبيوتر من القانون الانجليزى لسنة ١٩٩٠، حيث قاما بأعمال قرصنة باختراق والتغيير فى عدة مواقع إلكترونية، منها موقع الشبكة الأكاديمية بانجلترا وموقع جريدة فايننشيال تايمز وموقع المفوضية الأوروبية، وقُدر الضرر الناتج عن أفعالهما بـ ١٢٠٠٠٠ جنيه استرلينى، في حين برأت المحكمة متهم آخر في ذات القضية ويُدعىPaul Bedworth استناداً إلى ما أثبته تقرير الخبير النفسى المقدم عن حالته، والذى انتهى إلى مرضه بالإدمان القهرى على أعمال القرصنة، ولذلك قررت المحكمة براءته لانتفاء القصد الجنائى لديه[٢].

(٣) انظر فى ذلك المذكرة التفسيرية لاتفاقية بودابست لعام ٢٠٠١، فى معرض تعليقها على المادة الثانية منها والخاصة بالولوج غير القانوني والعمدى، المرجع السابق.

(1) R. v Strickland, Woods and Paul Bedworth (Southwark Crown Court 21/5/1993).

٣٧- وقت توافر القصد الجنائى وكيفية إثباته.

أما عن وقت توافر القصد الجنائى فيجب أن يكون معاصراً مع ارتكاب الركن المادى، وتحديداً عنصر السلوك الإجرامى منه(١)، وعلى ذلك يجب أن يتعاصر القصد الجنائى مع وقت قيام الجانى بسلوكه الإجرامى المتمثل فى الدخول غير المشروع من الأساس، أو فى لحظة تجاوزه للتصريح أو الإذن الممنوح له بالدخول، أو منذ لحظة عدم قطعه للاتصال مع النظام الحاصل فى بدايته بطريق الخطأ(٢).

ويُعد إثبات القصد الجنائى من المسائل الموضوعية التي تختص بها محكمة الموضوع من حيث استخلاصه واستنباطه من كافة وقائع وملابسات الدعوى المعروضة أمامها، دون رقابة عليها في ذلك من محكمة النقض، بشرط أن يكون استخلاصها سائغاً(٣).

المطلب الثانى
عقوبة جريمة الدخول غير المشروع

٣٨- تمهيد:

تُعد العقوبة عنوان النهج العقابي الذي يأخذ به المشرع الجنائي في كافة الأنظمة للتعامل مع كافة الظواهر الإجرامية، وباكتمال البنيان القانونى لأى جريمة بتوافر أركانها حسب نموذجها القانونى، لا يبقى إلا بيان عقوبتها المحددة بهذا النموذج القانونى.

وفيما يخص جريمة الدخول غير المشروع للأنظمة المعلوماتية وصورها فقد رصدت التشريعات محل المقارنة نوعين من العقوبات المقابلة لها، وهما العقوبة السالبة للحرية والعقوبة المالية المتمثلة فى الغرامة، ثم منحا القاضى سلطة تفريد العقوبة، من خلال الجمع بينهما، أو الاقتصار على إحداها فقط، تبعاً لما يراه ملائماً فى ضوء كل واقعة على حده، وفيما يلى إطلالة على العقوبات التى رصدتها التشريعات محل المقارنة مقابل جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية.

---

(٢) د. محمود محمود مصطفى، القسم العام، المرجع السابق، ص٤٤٢، د. عبد الرؤوف مهدى، شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص٥١٠.

(١) وهو ما عبَّر عنه صراحة المشرع الانجليزى فى البند (جـ) من الفقرة الأولى من المادة الأولى من قانون ١٩٩٠ بقوله «علم الجانى بكونه يرتكب جريمة فى الوقت الذى يتسبب فيه فى أداء الكمبيوتر للوظيفة» على النحو السالف الإشارة إليه.

(٢) ليس هناك مظهراً بذاته يقطع بقيام القصد على سبيل الحتم، لأن المظاهر التى قد تدل عليه ليست هى القصد ذاته، وإنما هى أمارات تكشف عنه قد تصدق وقد لا تصدق، فلكل واقعة ملابساتها، وما يصح لإثبات القصد في واقعة قد يعجز عن إثباته في أخرى، فالأمر إذن موكول لقاضى الموضوع في كل حالة على حده. انظر في ذلك د. محمد عيد الغريب، القسم العام، المرجع السابق، ص٦٨٠.

٣٩- عقوبة الجريمة فى التشريع الأمريكى.

أورد المشرع الاتحادى الأمريكى العقوبات المقابلة للجرائم موضوع قانون الغش وإساءة استخدام الكمبيوتر لسنة ١٩٨٦ فى الفقرة الثالثة من المادة (١٠٣٠) من ذات القانون، وباستقراء الخطة العقابية للمشرع الاتحادى الأمريكى، تتجلى عدة أمور على بساط البحث وهى:

١- لم يُفرد المشرع الاتحادى الأمريكى عقوبة خاصة لقاء فعل الدخول غير المشروع والمجرد للأنظمة المعلوماتية، رغم استهلال معظم التجريمات التى أوردتها الفقرة الأولى من المادة (١٠٣٠) بتجريم أفعال الولوج غير المشروع أو تجاوز الولوج المصرح به، لكن جاءت أفعال الولوج فى هذه التجريمات متبعة بأفعال أخرى على نحو ما أشرنا إلى ذلك سلفاً، ويمكن أن نقرر أن العقوبات المرصودة من قبل المشرع الاتحادى الأمريكى تقابل فعل الدخول غير المشروع - أو تجاوز الدخول المصرح به - وما يتبع أحدهما من أفعال أخرى معاً، وليست لأيهما حصراً.

٢-باستقراء العقوبات التى تضمنتها الفقرة الثالثة من المادة (١٠٣٠)، يتضح تبنى المشرع الاتحادى الأمريكى لظرف العود كظرف مشدد للعقوبة، وعبَّر عنه بسبق إدانة المتهم بارتكاب إحدى الجرائم الواردة بالفقرة الأولى من المادة (١٠٣٠)، ومثال لذلك يقرر البند الأول/أ من الفقرة الثالثة رصد عقوبة الغرامة أو السجن مدة لا تزيد على عشر سنوات، أو كلتا هاتين العقوبتين، لقاء ارتكاب الجريمة الواردة بالبند الأول من الفقرة الأولى، وذلك في حالة عدم سبق إدانة المتهم بارتكاب إحدى الجرائم التى تضمنتها الفقرة الأولى أو بالشروع فى ارتكابها[١]، فإذا سبق وأن أدين المتهم بارتكاب إحدى تلك الجرائم أو بالشروع فى ارتكابها، تكون العقوبة لقاء مخالفة البند الأول من الفقرة الأولى الغرامة أو السجن مدة لا تزيد على عشرين سنة، أو كلتا هاتين العقوبتين، وذلك حسبما نص عليه البند الأول/ب من الفقرة الثالثة[٢].

(1) {1 /A } From Subsection 1030(C) «A fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph».

(2) {1 /B } From Subsection 1030(C) «A fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after

وكذلك ما نصت عليه جزئيتا البند الثالث من الفقرة الثالثة، فالبند الثالث/أ ينص على رصد عقوبة الغرامة أو السجن مدة لا تزيد على خمس سنوات، أو كلتا هاتين العقوبتين، في حالة ارتكاب إحدى الجرائم المنصوص عليها بالبندين(٧،٤) من الفقرة الأولى، ولم يسبق إدانة المتهم بارتكاب إحدى الجرائم الواردة فى الفقرة الأولى أو بالشروع فى ارتكابها [١]، فإذا سبق وأُدين المتهم بارتكاب إحدى الجرائم الواردة فى الفقرة الأولى أو بالشروع فى ارتكابها، تكون العقوبة المرصودة لمخالفة البندين (٧،٤) المشار إليهما الغرامة أو السجن لمدة لا تزيد على عشر سنوات، أو كلتا هاتين العقوبتين، حسبما نص على ذلك البند الثالث/ب من الفقرة الثالثة[٢].

٤٠- عقوبة الجريمة فى التشريع الانجليزى.

أفرد المشرع الانجليزى فى الفقرة الثالثة من المادة الأولى من قانون ١٩٩٠ عقوبة الحبس مدة لا تتجاوز ستة أشهر أو الغرامة التى لا تتجاوز المستوى الخامس العادى أو كلتا هاتين العقوبتين لقاء جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية، والتى أوردها تحت مسمى الدخول المحظور على مواد الكمبيوتر فى الفقرتين الأولى والثانية من ذات المادة[٣].

وإزاء استفحال جرائم إساءة استخدام الكمبيوتر فى انجلترا، فقد استجاب البرلمان الانجليزى لتوصيات لجنة التحقيق البرلمانية الخاصة بمراجعة قانون إساءة استخدام الحاسب الآلى لسنة١٩٩٠ لبحث الحاجة لتعديله من عدمه، والتى أوصت فى تقريرها المقدم سنة ٢٠٠٤ بضرورة تعديل هذا القانون، خاصة فيما يتعلق بالعقوبات الواردة فيه، وذلك لتحقيق

---

a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph».

(3) { 3/A } From Subsection 1030(C) «A fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph».

(1) { 3/B } From Subsection 1030(C) «A fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph».

(2)Paragraph (3) from section (1) « A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both».

أكبر قدر من الردع بنوعيه العام والخاص[١]، وهو ما قام به المشرع الانجليزى بالفعل بتعديله للقانون المذكور بموجب قانون الشرطة والعدالة لسنة ٢٠٠٦- Police and Justice Act 2006 (PJA) – [٢] وأضحت عقوبة مخالفة المادة المشار إليها الحبس بحد أقصى سنتان والغرامة أو إحدى هاتين العقوبتين[٣].

أما العقوبة التى أفردها المشرع الانجليزى لقاء جريمة الدخول المحظور بقصد ارتكاب أو التسهيل لارتكاب جرائم أخرى والواردة بالمادة الثانية، فهى السجن لمدة لا تتجاوز خمس سنوات أو الغرامة أو بكلتا هاتين العقوبتين، حسبما نصت على ذلك الفقرة الخامسة/ب من المادة الثانية من قانون ١٩٩٠[٤]، وكما طال التعديل الذى أدخله قانون الشرطة والعدالة لسنة ٢٠٠٦ على العقوبة المرصودة لمخالفة المادة الأولى المار ذكرها، فقد عدَّل من عقوبة

(٣) فى إحصائية استقت مصادرها من البيانات المسجلة فى مجلس العموم البريطانى House Of Commons، بشأن إجمالي عدد الجرائم المرتكبة بالمخالفة لقانون إساءة استخدام الحاسب الآلى لسنة ١٩٩٠ في كل من انجلترا وويلز في المدة ما بين عامي ٢٠٠٤ إلى ٢٠١٠، لبيان الأثر الذى أحدثه تعديل سنة ٢٠٠٦ = = بموجب قانون الشرطة والعدالة على قانون سنة ١٩٩٠، وبخاصة من ناحية تشديده للعقوبات الواردة فى قانون ١٩٩٠، مما انعكس أثره على تقلص عدد الجرائم المرتكبة فى هذا الشأن، فورد بهذه الإحصائية أنه فى عام ٢٠٠٤ بلغ عدد الجرائم المرتكبة بالمخالفة لقانون ١٩٩٠، ٢١ جريمة منها ٥ جرائم بالمخالفة لنص المادة الأولى والخاصة بالدخول غير المصرح به أو المحظور، و٦ جرائم بالمخالفة لنص المادة الثانية والخاصة بالدخول المحظور بغرض التسهيل والتحريض على ارتكاب الجرائم و١٠ جرائم بالمخالفة لنص المادة الثالثة والخاصة بحظر التبديل أو التحويل فى مواد الكمبيوتر، وفى سنة ٢٠٠٥ بلغ إجمالي عدد الجرائم ٢٤ جريمة منها ٥ جرائم بالمخالفة للمادة الأولى و١١ جريمة بالمخالفة للمادة الثانية و٨ جرائم بالمخالفة للمادة الثالثة، وفى عام ٢٠٠٦ بلغ إجمالي عدد الجرائم ٢٥ جريمة منها ٧ جرائم بالمخالفة للمادة الأولى و٥ جرائم بالمخالفة للمادة الثانية و١٣ جريمة بالمخالفة للمادة الثالثة، وفى عام ٢٠٠٧ بلغ إجمالي عدد الجرائم ١٩ جريمة منها ٨ جرائم بالمخالفة للمادة الأولى وجريمتان بالمخالفة للمادة الثانية و٩ جرائم بالمخالفة للمادة الثالثة، وفى عام ٢٠٠٨ بلغ إجمالي عدد الجرائم ١٧ جريمة منها ١١ جريمة بالمخالفة للمادة الأولى و٦ جرائم بالمخالفة للمادتين الثانية والثالثة، وفى عام ٢٠٠٩ بلغ إجمالي عدد الجرائم ١٩ جريمة منها ١١ جريمة بالمخالفة للمادة الأولى و٨ جرائم بالمخالفة للمادتين الثانية والثالثة، وفى عام ٢٠١٠ بلغ إجمالي عدد الجرائم ١٠ جرائم منها ٣ جرائم بالمخالفة للمادة الأولى و٧ جرائم بالمخالفة للمادتين الثانية والثالثة. مشار لهذه الإحصائية لدى:

: Computer Misuse Act 1990 Statistics: Total number of Computer Misuse Act Michael J L Turner 1990 Prosecutions in England and Wales 2004 – 2010, these statistics available online at: http://www.computerevidence.co.uk/Cases/CMA%20Stats.htm

- وأشارت إحدى الدراسات الأخرى إلى أنه في الفترة من ١٩٩١ إلى ٢٠٠٢ في كل من انجلترا وويلز تم تقديم ٣٣ متهماً للمحاكمة الجنائية لمخالفتهم المادة الأولى من قانون ١٩٩٠، و٢٨ متهماً لمخالفتهم المادة الثانية، و٧٠ متهماً لمخالفتهم المادة الثالثة، بالإضافة إلى حالات أخرى لم يتم إحالتها إلى المحاكمة الجنائية اعتماداً على المساءلة التأديبية للجناه لكونهم موظفين. فى ذلك انظر:

Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.56.

(١) دخلت التعديلات التى أدخلها قانون الشرطة والعدالة لسنة٢٠٠٦ على قانون ١٩٩٠ حيز التنفيذ اعتباراً من أكتوبر ٢٠٠٨.

(2) Derek Wyatt and others: Revision of the Computer Misuse Act, P.R, no.99, p.15; Paul Mobbsfor: Computer Crime - The law on the misuse of computers and networks, P.R; See also: Computer Misuse Act 1990, from Wikipedia, P.R; An article entitled Crime, P.R.

(3) Paragraph (5/ B) from section (2) « The maximum penalty on conviction on indictment to five years imprisonment, or a fine or both».

هذه المادة أيضاً لتكون مع هذا التعديل السجن لمدة لا تتجاوز عشر سنوات أو الغرامة أو كلتا هاتين العقوبتين[١].

٤١- عقوبة الجريمة فى التشريع المصرى.

يعاقب المشرع المصرى على فعلى الدخول غير المشروع للأنظمة المعلوماتية الخاصة والبقاء العمدى داخل تلك الأنظمة والحاصل فى بدايته بطريق الخطأ بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، وفقاً لما جاء بالمادة (١/١٤)، فى حين يعاقب على فعل تجاوز الدخول المصرح به فى الأنظمة المعلوماتية الخاصة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، حسبما نصت على ذلك المادة (١٥).

أما بالنسبة للأنظمة المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة، فعاقب المشرع على أفعال الدخول غير المشروع إليها والبقاء العمدى فيها والحاصل فى بدايته بطريق الخطأ، وكذلك تجاوز الدخول المصرح به إليها، بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدي هاتين العقوبتين، حسبما نصت على ذلك المادة (١/٢٠).

ومن خلال عرضنا للعقوبات التى أفردها المشرع المصرى لقاء جريمة الدخول غير المشروع وصورها تتجلى عدة ملاحظات بشأن هذه العقوبات تتمثل فى الآتى:

١- اعتبر المشرع المصرى جميع أفعال وصور الدخول غير المشروع من الجنح وأفرد لها عقوبة الحبس الذى تكفل بتحديد حده الأدنى فى كل جريمة، فضلاً عن عقوبة الغرامة التى تتفاوت فى مقدارها وفقاً لطبيعة الفعل المرتكب تارة، والحق محل الانتهاك تارة أخرى.

٢- منح المشرع للقاضى سلطة تفريد العقوبة، فهو بالخيار بين الحكم بالعقوبتين السالبة للحرية – الحبس – والمالية – الغرامة- أو الحكم بإحداهما دون الأخرى، فى ضوء الحدود المقررة لكلتا العقوبتين فى كل جريمة وفقاً لما يراه فى ضوء كل دعوى على حده.

(4) Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, pp.44-45; See also: An article entitled Crime, P.R.

٣- مايز المشرع فى العقوبات المقررة تبعاً لمحل الانتهاك ونوع الفعل المؤثم، أما عن محل الانتهاك فقد مايز المشرع فى العقوبة المقررة للدخول غير المشروع والبقاء العمدى داخل الأنظمة المعلوماتية الخاصة سواء بشخص طبيعى أو معنوى، وبين الأنظمة المعلوماتية الخاصة بالدولة أو بأحد الأشخاص الاعتبارية العامة، وأفرد للأولى عقوبة الحبس مدة لا تقل عن سنة، والغرامة التى لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو إحدى هاتين العقوبتين، وأفرد للثانية عقوبة الحبس مدة لا تقل عن سنتين، والغرامة التى لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو إحدي هاتين العقوبتين، لقاء أفعال الدخول غير المشروع والبقاء العمدى داخل الأنظمة الحاصل فى بدايته بطريق الخطأ، وكذلك أفعال تجاوز الدخول المصرح به.

- ومن ناحية نوعية الفعل المؤثم مايز أيضاً المشرع فى العقوبة الخاصة بالأنظمة المعلوماتية الخاصة بين فعلى الدخول غير المشروع والبقاء العمدى داخل هذه الأنظمة والحاصل فى بدايته بطريق الخطأ، وأفرد لهما عقوبة الحبس مدة لا تقل عن سنة، والغرامة التى لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو إحدى هاتين العقوبتين طبقاً لما ورد بالفقرة الأولى من المادة (١٤) المار ذكرها، فى حين أفرد لجريمة تجاوز الدخول المصرح به للأنظمة المعلوماتية الخاصة عقوبة الحبس مدة لا تقل عن ستة أشهر، والغرامة التى لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين، طبقاً لنص المادة (١٥) على النحو المتقدم.

المطلب الثالث
تطبيقات قضائية لجريمة الدخول غير المشروع

٤٢- تمهيد:

نظراً لحداثة القانون المصرى رقم ١٧٥ لسنة ٢٠١٨ فلم تتوافر بشأنه بعض التطبيقات القضائية المصرية، لذا سوف نكتفى فى هذا المقام بعرض بعض التطبيقات القضائية فى التشريعيين الأمريكى والانجليزى لجريمة الدخول غير المشروع للأنظمة المعلوماتية.

٤٣- التطبيقات القضائية الأمريكية.

ذكرنا فيما سبق أن المشرع الاتحادى الأمريكى لم يُفرد نص تجريمى خاص لقاء فعل الدخول غير المشروع والمجرد للأنظمة المعلوماتية، أو تجاوز الدخول المصرح به، وهذا ما تُشير إليه الفقرة الأولى من المادة (١٠٣٠) أمريكى، فى أى بند من بنودها المتضمنة لأى من الوصفين السابقين أو كلاهما، فلازم لتحقق الجريمة أن يقترن الدخول غير المشروع أو تجاوز التصريح الممنوح بالدخول بغاية أو هدف مما عناه المشرع فى أى بند من بنود هذه الفقرة على النحو المشار إليه.

وهذا ما حملته التطبيقات القضائية الأمريكية نفاذاً للتجريمات موضوع الفقرة الأولى المشار إليها، وبالإضافة إلى ما سقناه من تطبيقات قضائية فى ضوء هذا التشريع، نضيف إليها بعض التطبيقات الأخرى.

من ذلك تطبيق القضاء الأمريكى سنة ٢٠١٠ للقواعد الخاصة بقانون ١٩٨٦ وتعديلاته فيما يخص تجاوز الدخول المصرح به، والوارد في البند الثانى من الفقرة الأولى من المادة (١٠٣٠) على حالة استخدام الموظف لجهاز الكمبيوتر الخاص بالعمل في غير أغراض العمل، فقد أدان أحد الموظفين ويُدعى John الموظف بمؤسسة سيتى جروب، لتجاوزه الوصول المصرح به، وتقديمه حسابات العملاء السريين لشركته لشركة أخرى في شكل صور منسوخة ضوئياً (Scanned Images) من شيكات ومطبوعات وتعاملات من خلال شاشة الكمبيوتر الخاص بالشركة التى يعمل بها[1].

(1)U. S v. John, 597 F.3d 263 (5th Cir. 2010).

كما أدانت إحدى المحاكم الأمريكية سنة ١٩٩٧[١] أحد الموظفين بمصلحة الضرائب الأمريكية ويُدعى Richard Czubinski لمخالفته ذات البند المشار إليه، حيث كان يعمل ممثل الاتصال في مكتب بوسطن التابع لشعبة خدمات دافعى الضرائب في هذه الولاية، وكان من صلاحياته الوظيفية الوصول إلى بيانات ومعلومات الإيرادات الداخلية المتعلقة بدافعى الضرائب باستخدام كلمة مرور قانونية، لكن لم تكن من بين هذه الصلاحيات الدخول لملفات معينة، وهى ملفات دافعى الضرائب، والتى ولج إليها مرات عديدة، وأرسل هذه المعلومات لبعض أصدقاء ومعارفى والخصوم السياسيين لأصحاب هذه الملفات[٢].

فضلاً عن تطبيق القضاء الأمريكى للبند الخامس/١ من الفقرة الأولى من المادة (١٠٣٠) والذى يتعلق بتعمد إحداث أضرار متعلقة ببرامج أو معلومات، وذلك في قضية الولايات المتحدة ضد Sullivan سنة ٢٠٠٢ والذى قام بتصميم وزرع شفرات خبيثة في أحد البرامج وكتب التشغيل فى جهاز الكمبيوتر الخاص بالجهة الحكومية التى يعمل بها، وظلت هذه الشفرات الخبيثة خامدة لمدة أربعة أشهر تبعاً لتصميم المتهم لها، وكان دورها في هذه الفترة تنشيط واستقطاب شفرات خبيثة أخرى، وانتهت المحكمة إلى أن فعل المتهم على هذا النحو قد أضر بالملفات والمعلومات المخزنة بالحاسب مما جعلها غير صالحة للاستعمال، فضلاً عن تعمده انتقال هذه الشفرات الخبيثة وتصميمها لاستقطاب شفرات خبيثة أخرى[٣].

٤٤- التطبيقات القضائية الانجليزية.

أوردنا فيما سبق ونحن بمعرض بيان النصوص القانونية المستحدثة فى التشريع الانجليزى، بعض التطبيقات القضائية للجريمة موضوع المادة الثانية والخاصة بالدخول المحظور بقصد التسهيل والتحريض على ارتكاب الجرائم، لارتباطها فى بعض الأحوال بالجريمة موضوع البحث وهى الدخول غير المشروع للأنظمة المعلوماتية، وفى هذا المقام سوف نكتفى بإيراد بعض التطبيقات القضائية الخاصة بالجريمة موضوع البحث[٤].

---

(2)U.S .v. Czubinski, 106 F.3d 1069 (1st Cir. 1997).

(٣) أحدثت الواقعة موضوع هذا الحكم حالة من الجدل فى الأوساط الأمريكية، مما جعله موضع لكثير من التعليقات منها:

Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, P.R, pp.32-34; Computer Fraud and Abuse Act (CFAA), an article From Internet Law Treatise, P.R; Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, P.R, p.1634.

(1) U. S v. Sullivan, 40 Fed. Appx.740 (4th Cir.2002)

(٢) زخرت جريمة الدخول غير المشروع والمجرد للأنظمة المعلوماتية بالعديد من التطبيقات القضائية فى انجلترا، لإفراد المشرع الانجليزى نص خاص بهذه الجريمة، وهو نص المادة الأولى من قانون١٩٩٠، والخاصة بالدخول المحظور على مواد الكمبيوتر.

ومن أمثلة هذه التطبيقات ما قضت به محكمةLeicester Crown Court[١] في ٢٠١٣/١/١١ بمعاقبة كل من James Marks وJames McCormick لمخالفتهما المادة الأولى من قانون إساءة استخدام الحاسب الآلى لسنة ١٩٩٠ والخاصة بالدخول المحظور، بقيامهما باختراق الخوادم الإلكترونية لشركة سونى الموسيقية وتحميل ٩٧٠٠ ملف موسيقى بما فى ذلك مقطوعات للمطرب العالمى الراحل الفيس بريسلى، والمطربة بيونيسه ومقطوعات أخرى للمطرب مايكل جاكسون والتى لم تصدرها الشركة بعد، وقد حكم عليهما بالحبس لمدة ستة أشهر مع وقف التنفيذ لمدة سنة مع إلزامهما بالعمل المجانى فى خدمة المجتمع لمدة ١٠٠ساعة[٢].

كما قضت محكمة Swindon Magistrates Court في ٢٠١٢ /٨/١٧ بمعاقبة شخص يُدعى Astrid Curzon بغرامة قدرها ٢٠٠ جنيه استرلينى و٦٧٥ جنيه استرلينى كمصروفات قضائية و١٥جنيه استرلينى تعويض مؤقت للمجنى عليه، لمخالفته المادة الأولى المنوه عنها، لقيامه بالدخول بدون حق للنظام المعلوماتى الخاص بأكاديمية

(٣) جدير بالذكر أن المشرع الانجليزى عقد الاختصاص الأصيل بنظر الجرائم الناشئة عن مخالفة المادة الأولى من قانون ١٩٩٠ لمحاكم التاج Crown Courts، واستثناءً أناط بالمحاكم الجزئية المسماه بمحاكم الصلح Magistrates Courts نظر هذه الجرائم، وذلك فى حالتين: الأولى إذا كان المتهم فى دائرتها وقت مباشرته للفعل الذى تسبب فى أداء الكمبيوتر لعملية تأمين الوصول إلى أي برنامج أو بيانات محفوظة في الكمبيوتر، والحالة الثانية حالة كون جهاز الكمبيوتر الذى يحتوي على أي برنامج أو بيانات فى نطاقها، والذى كان المتهم قد أمن أو كان ينوى تأمين = = الوصول غير المصرح به لهذه البرامج أو البيانات، حسبما نصت على ذلك الفقرة الأولى من المادة (١١) من ذات القانون بقولها:

Paragraphs (1) from section (11) «A magistrates' court shall have jurisdiction to try an offence under section 1 above if:

(a) the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or (b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time».

- مع ملاحظة أن أقصى عقوبة يمكن لمحاكم الصلح توقيعها حتى بعد تعديل العقوبات الواردة في قانون ١٩٩٠ بموجب قانون الشرطة والعدالة لسنة ٢٠٠٦، هي الحبس لمدة ستة أشهر بحد أقصى فى جميع الجرائم التي تختص بنظرها، وذلك إعمالاً لقانون سلطات المحاكم الجنائية لسنة ٢٠٠٠. فى ذلك انظر:

Stefan Frederick Fafinski: Computer use and misuse, Ph.D, P.R, p.75.

(1)R. v James Marks and James Mc Cormick (Leicester Crown Court 11 /1/2013). وللمزيد حول هذا الحكم انظر: - Edmand Dester Thipursian and others: Case Study – News of the World Phone Hacking Scandal, P.R, no.7.

Wootton Bassett باستخدام معلومات الدخول وكلمة المرور الخاصة بأحد الموظفين وقراءة الرسائل الإلكترونية الخاصة بهذه الأكاديمية(١).

وقضت محكمة Hull Crown Court فى ٢٠١٠/٩/١٦ بمعاقبة شخص يُدعى Dale Trever بالحبس لمدة ستة أشهر مع إيقاف التنفيذ لمدة عامين، وذلك لمخالفته المادة الأولى من قانون ١٩٩٠، وذلك لدخوله غير المصرح به لإدارة بيانات السجلات الطبية السرية الخاصة بالإناث(٢).

كما قضت محكمة Cannock Magistrates Court في ٢٠١٠/٩/٩ بمعاقبة أحد ضباط الشرطة البريطانية ويُدعى Balwinder Basran بغرامة قدرها ٢٠٠٠ جنيه استرلينى، وذلك لمخالفته المادة الأولى المنوه عنها، حيث كان المتهم وبوصفه ضابط شرطة قد دخل لسجلات الشرطة الإلكترونية لأغراض شخصية(٣)، وكان هذا الجرم هو ذاته المنسوب لضابط شرطة آخر يُدعى Robert Campbell، والذى أدانته محكمةGuildford Crown Court في ٢٠١٠/٦/٨ بغرامة قدرها ١٢٠٠ جنيه استرلينى(٤).

كما قضت محكمة Coventry Magistrates Court بمعاقبة ضابط شرطة يُدعى Michelle Begley بالحبس لمدة ثلاثة أشهر لمخالفته المادة الأولى سالفة الذكر، واتهامه كذلك بالتحرش عن طريق إساءة استخدام جهاز الكمبيوتر الخاص بالشرطة الوطنية، لتجاوزه الدخول المصرح به بولوجه لموقع مركز رخص السيارات في محاولة منه لتعقب امرأه بتوصية من أحد أصدقائه والذى كانت تربطه علاقة بهذه المرأة، وفى ذات الشأن قضت إحدى المحاكم الإنجليزية بمعاقبة أحد أفراد الشرطة السابقين ويُدعى Bennett بغرامة قدرها ١٥٠ جنيه استرلينى والمصروفات القضائية، وذلك لمخالفته المادة الأولى من قانون ١٩٩٠، لقيامه باستخدام جهاز كمبيوتر الشرطة الوطنية لتعقب صديق زوجته السابقة(٥).

(1) R. v Astrid Curzon (Swindon Magistrates Court 17/8/2012).

(2) R. v Dale Trever (Hull Crown Court 16/9/2010).

(3) R. v Balwinder Basran (Cannock Magistrates Court 9/9/2010).

(4) R. v Robert Campbell (Guildford Crown Court 8/6/2010).

(١) مشار لهذين الحكم لدى:

Michael J L Turner: Computer Misuse Act 1990, cases

a database, P.R.

وقضت محكمة Westminster Magistrates Court فى ٢٠٠٧/٨/٩ بمعاقبة شخص يُدعى Mark Hopkins بالحبس لمدة خمسة أشهر مع وقف التنفيذ لمدة عامين وإلزامه بالعمل المجانى فى خدمة المجتمع لمدة ١٠٠ساعة، وإلزامه كذلك بدفع مبلغ ٥٠٠٠ جنيه استرلينى كتعويض للمجنى عليه – الموقع الإلكترونى– لمخالفته المادة الأولى من قانون١٩٩٠، لقيامه بالدخول لأحد المواقع الإلكترونية التجارية الخاصة بالإصدارات الجديدة للدرجات النارية لصالح إحدى الشركات المنافسة(١).

وقضت محكمة Horseferry Road Magistrates Court في ٢٠٠٥/١٠/٧ بمعاقبة شخص يُدعى Daniel Cuthbert بغرامة قدرها ٤٠٠ جنيه استرلينى، لمخالفته المادة الأولى من قانون ١٩٩٠، لدخوله غير المشروع إلى موقع لجنة الإغاثة الطارئة والخاصة بضحايا موجات تسونامى والاطلاع على بيانات هذا الموقع(٢).

كما قضت محكمة Exeter Crown Court في ٢٠١١/٢/٣ بمعاقبة شخص يُدعى Ashley Mitchell بالحبس لمدة سنتين لمخالفته المادة الأولى من قانون ١٩٩٠، حيث دفعه شغفه بلعبة البوكر على الإنترنت إلى اختراق موقع إحدى الشركات الأمريكية لألعاب البوكر، والاستيلاء على ٧ مليون جنيه استرلينى من فيشات اللعبة وبيعها من خلال الفيس بوك(٣).

وقضت كذلك محكمة Southwark Crown Court فى ٢٠١٠/٨/٢٠ بمعاقبة شخص يُدعى Daniel Woo بالحبس لمدة ثمانية أشهر مع إيقاف التنفيذ لمدة عامين ووضعه تحت المراقبة لمدة عامين وإلزامه بالعمل المجانى فى الخدمة العامة لمدة ٢٠٠ ساعة، وذلك لمخالفته المادة الأولى من قانون ١٩٩٠، بالتقاطه لكلمات المرور الخاصة بالبريد الإلكترونى لعدة أشخاص ومؤسسات والتى تحتوى على بيانات شخصية ومالية للمجنى عليهم(٤).

---

(2) R. v Mark Hopkins (Westminster Magistrates Court 9/8/2007).

(3) R. v Daniel Cuthbert (Horseferry Road Magistrates Court 7/10/2005).

(1) R. v Ashley Mitchell (Exeter Crown Court 3/2/2011).

(2) R. v Daniel Woo (Southwark Crown Court 20/8/2010).

الخاتمة

أثمر بحثنا والذى خصصناه لدراسة جريمة الدخول غير المشروع للأنظمة المعلوماتية على ضوء القانون المصرى رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات عن عدد من النتائج والتوصيات هى:

٤٥- نتائج البحث:

١- تُعد جريمة الدخول غير المشروع للأنظمة المعلوماتية الجريمة الأساسية التى تنطوى على تهديد وتعد على أمن وسلامة هذه الأنظمة، فضلاً عن أنها عادة ما تكون مقدمة لكثير من الجرائم المعلوماتية الأخرى، وفى مقام دراستنا لهذه الجريمة عقدنا بشأنها دراسة مقارنة بين تشريعات مصر والولايات المتحدة وانجلترا، وكان الدافع وراء اختيار هذه التشريعات استكشاف مقومات هذه الجريمة فى ثلاثة أنظمة تباينت فى تناولها.

٢- تمسك كل من الفقه والقضاء فى التشريعات محل المقارنة بمبدأ الشرعية الجنائية، برفض تطبيق النصوص العقابية التقليدية على الجرائم التى استحدثتها ظاهرة المعلوماتية، ومن بينها الجريمة محل البحث، وكان فى ذلك دافعاً لمشرعى هذه الدول بإصدار قوانين خاصة تعالج هذه الجرائم المستحدثة، فأصدر المشرع الاتحادى الأمريكى قانون جرائم الكمبيوتر الاتحادى لسنة١٩٨٤، والذى عدَّله وحلَّ محله تماماً القانون الاتحادى بشأن الغش وإساءة استخدام الكمبيوتر لسنة ١٩٨٦، فى حين أصدر المشرع الانجليزى قانون إساءة استخدام الحاسب الآلى لسنة ١٩٩٠، وبعد طول غياب أصدر المشرع المصرى القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

٣-تباينت التشريعات محل المقارنة فى تناولها لجريمة الدخول غير المشروع للأنظمة المعلوماتية، فالمشرع الأمريكى فى القانون الاتحادى الأمريكى لسنة ١٩٨٦ بشأن الغش وإساءة استخدام الكمبيوتر أشار لهذه الجريمة، لكن لم يتناولها بصورة منفردة وإنما كان دائماً حريصاً على وجود غاية أو هدف من فعل الدخول غير المشروع أو تجاوز الدخول المصرح به، على نحو ما حملته الفقرة الأولى من المادة (١٠٣٠) من تجريمات فى هذا الشأن، والمعنى أن هذا المشرع لم يورد تجريماً خاصاً بهذه الجريمة على نحو مجرد، ونرى أن إغفال مثل هذا التجريم يُمثل أحد أوجه الضعف فى التشريع الأمريكى، ونتساءل عن الوضع فى حالة اكتفاء الجانى بالدخول المجرد، أو بتجاوز الدخول المصرح به على

نحو مجرد، دون أن يتبع دخوله أو تجاوزه فى الدخول بأى غاية أو مصلحة مما عناها المشرع الأمريكى بالحماية فى البنود السبعة موضوع الفقرة الأولى من المادة (١٠٣٠)؟.

- أما المشرع الانجليزى فقد أفرد نص خاص بهذه الجريمة فى قانون إساءة استخدام الكمبيوتر لسنة ١٩٩٠، وهو نص المادة الأولى من هذا القانون، والتى أوردها تحت مسمى الدخول المحظور على مواد الكمبيوتر، وانعكس ذلك على كثرة التطبيقات القضائية لهذه الجريمة فى انجلترا.

- أما المشرع المصرى فقد تميز وبحق عن المشرعين الأمريكى والانجليزى فيما يخص جريمة الدخول غير المشروع، والتى حظت باهتمام القانون المصرى رقم ١٧٥ لسنة ٢٠١٨، وجرمها وعاقب عليها على نحو مجرد. وخصص لها ثلاث مواد هى المادة (١/١٤) التى تُجرم وتعاقب على فعلى الدخول غير المشروع للأنظمة المعلوماتية الخاصة والبقاء العمدى داخل تلك الأنظمة المعلوماتية والحاصل فى بدايته بطريق الخطأ، فى حين أفرد نص المادة (١٥) منه لتجريم وعقاب تجاوز الدخول المصرح به فى الأنظمة المعلوماتية الخاصة. أما بالنسبة للأنظمة المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة، فخصص لها نص المادة (١/٢٠) لتجريم وعقاب أفعال الدخول غير المشروع إليها، والبقاء العمدى فيها والحاصل فى بدايته بطريق الخطأ، وكذلك تجاوز الدخول المصرح به إليها، واعتبر المشرع كل هذه الجرائم من الجنح وأفرد لها عقوبات سالبة للحرية متمثلة فى الحبس الذى تكفل المشرع بتحديد حده الأدنى بالإضافة إلى عقوبة الغرامة، وتفاوتت مدد الحبس ومقدار الغرامة فى هذه الجرائم حسب الحق محل الانتهاك ونوعية الفعل المؤثم، ومنح القاضى الخيار بالحكم بالعقوبة السالبة للحرية وحدها أو بالغرامة وحدها أو بهما معاً فى ضوء الحدود المقررة لكلتا العقوبتين فى كل جريمة وفقاً لما يراه فى كل دعوى على حده

٤- تُكيف جريمة الدخول غير المشروع للأنظمة المعلوماتية من منظور الركن المادى لها وتحديداً من ناحية عنصر النتيجة فيها على أنها من جرائم السلوك المجرد التى يُكتفى فى قيام ركنها المادى بالسلوك الإجرامى فقط بغض النظر عن تحقق نتيجة له من عدمه، وفى هذا ضمانة أكبر لسلامة الأنظمة المعلوماتية من التسلل إليها، وخط دفاع أول من العبث بها أو بمحتوياتها، أما عن تكييفها من ناحية السلوك الإجرامى فيها، فالفقه مجمع على تكييف إحدى صور هذه الجريمة وهى صورة الابقاء على الاتصال مع

النظام بأنها من الجرائم المستمرة، أما بالنسبة لصورتى الدخول غير المشروع من الأساس للنظام أو تجاوز الدخول غير المصرح به، فالرأى الغالب والذى نميل إليه يذهب إلى اعتبارهما من الجرائم الوقتية تأسيساً على اعتبار جريمة الدخول إلى النظام منتهية بمجرد إتيان الفاعل لسلوكه المجرَّم بدخول النظام كله أو إلى جزء منه غير مصرح له بالدخول إليه، أو بمجرد إنهاءه لفعله المنم عن تجاوز التصريح الممنوح له ليجد نفسه أمام نظام أو جزء منه غير مسموح له بالدخول إليه.

٥- يتمثل السلوك الإجرامى فى هذه الجريمة فى فعل إيجابى يتخذ صورتان فى ضوء القانون الأمريكى وفقاً لما أورده فى بنود الفقرة الأولى من المادة (١٠٣٠) من القانون الاتحادى، وهاتان الصورتان هما حظر الولوج العمدى إلى الكمبيوتر بدون تصريح أو تجاوز الولوج المصرح به، أما المشرع الانجليزى فعبَّر عنه فى المادة الأولى من قانون ١٩٩٠ بصورة واحدة وهى حظر الدخول على مواد الكمبيوتر، فى حين أورد المشرع المصرى الثلاث صور، وهى الدخول غير المشروع من الأساس للنظام المعلوماتى، وتجاوز الدخول المصرح به، والإبقاء على الاتصال بالنظام الحاصل فى البداية بطريق الخطأ، وهذا وجه تميز القانون المصرى فيما يخص جريمة الدخول غير المشروع.

٦- أما عن محل هذه الجريمة فعبَّر عنه المشرع الأمريكى بالولوج غير المشروع للكمبيوتر، فضلاً عن استخدامه لمصطلح كومبيوتر محمى فى الكثير من بنود الفقرة الأولى من المادة (١٠٣٠)، والذى عرَّفه فضلاً عن تعريفه للكمبيوتر، فى حين عبَّر المشرع الانجليزى عن هذا المحل بمصطلح الدخول المحظور على مواد الكمبيوتر، ولكنه لم يتطرق إلى تعريف المصطلحات التى استخدمها مثل كمبيوتر، برامج، مواد الكمبيوتر، اعتقاداً من اللجنة التشريعية مقررة القانون الاتجليزى لسنة ١٩٩٠ بأن خطوات التقدم التكنولوجى ستجعل من هذه التعاريف عقيمة، لذا تطرقنا إلى تفصيل هذا المحل فى التشريعين الأمريكى والانجليزى لبيان ما يدخل تحت عباءة هذه الجريمة وما يخرج عنها.

- أما المشرع المصرى فأوضح هذا المحل بأنه قد يكون موقعاً أو حساباً خاصاً أو نظاماً معلوماتياً أو بريداً إلكترونياً، وتعريفه لهذه المصطلحات فى المادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨ والخاصة بالتعريفات، فضلاً عن تعريفه للكمبيوتر أو الحاسب فى ذات المادة.

٧- كما أن هذه الجريمة من الجرائم العمدية التى تستلزم توافر القصد الجنائى لدى مقارفها بعنصريه العلم والإرادة فى كل حالة من حالات الدخول غير المشروع.

٨- ومن ناحية العقوبات المرصودة لقاء هذه الجريمة، نجد أن المشرع الأمريكى لم يُفرد عقوبة خاصة بها، لأنه لم ينص عليها بصورة مجردة، على نحو ما أشرنا إليه فى صفحات هذا البحث، أما المشرع الانجليزى فقد رصد لقائها عقوبة الغرامة أو الحبس لمدة لا تتجاوز ستة أشهر أو كلتا هاتين العقوبتين، ومع تزايد معدلات هذه الجريمة عدَّل المشرع الانجليزى من هذه العقوبة لتكون الغرامة أو الحبس لمدة لا تتجاوز سنتان أو كلتا هاتين العقوبتين، بموجب التعديل الذى أدخله قانون الشرطة والعدالة لسنة ٢٠٠٦ على قانون ١٩٩٠، أما المشرع المصرى فيعاقب على فعلى الدخول غير المشروع للأنظمة المعلوماتية الخاصة والبقاء العمدى داخل تلك الأنظمة والحاصل فى بدايته بطريق الخطأ بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، وفقاً لما جاء بالمادة (١/١٤)، فى حين يعاقب على تجاوز الدخول المصرح به فى الأنظمة المعلوماتية الخاصة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، حسبما نصت على ذلك المادة (١٥).

- أما بالنسبة للأنظمة المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة، فعاقب على أفعال الدخول غير المشروع إليها، والبقاء العمدى فيها والحاصل فى بدايته بطريق الخطأ، وكذلك تجاوز الدخول المصرح به إليها، بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدي هاتين العقوبتين، حسبما نصت على ذلك المادة (١/٢٠).

٤٦- التوصيات:

أما عن التوصيات المقترحة فتتلخص فى دعوة المشرع المصرى إلى تعديل نص المادة (١٨) من القانون رقم ١٧٥ لسنة ٢٠١٨، بحذف لفظ الاختراق الوارد فى هذه المادة باعتباره أحد صور الدخول غير المشروع، وإضافة مصطلح البريد الإلكترونى الوارد أيضاً فى هذه المادة، إلى المادتين (١/١٤) و(١٥) كمحل للحماية المستهدفة بجانب المواقع والحسابات الخاصة والأنظمة المعلوماتية الخاصة الواردة بالمادتين المشار إليهما، والخاصتان بجريمة الدخول غير المشروع وصوره للأنظمة المعلوماتية الخاصة، فلا يوجد ما يبرر المغايرة فى الحماية ومن ثم العقوبة بين البريد الإلكترونى والمصطلحات السابقة، خاصة وأن المشرع فى المادة (١/٢٠) أدرج البريد الإلكترونى كمحل للحماية بجانب المواقع والحسابات الخاصة والأنظمة المعلوماتية الخاصة بالدولة ووحد العقوبات فى حال انتهاك أى منهم بالدخول غير المشروع أو بأى صورة من صوره.

وختاماً

أدعو الله العليَّ القدير، أن أكون قد نلت حظاً من التوفيق فى عرض وإيضاح الفكرة موضوع البحث ولو بالقدر اليسير، وما كان من توفيق فى ذلك فمن الله وحده، وما كان من خطأ فمنى ومن الشيطان .... وفقنا الله جميعاً لما فيه الخير... وآخر دعوانا أن الحمد لله رب العالمين .

تم بحمد الله،،،

قائمة المراجع

أولاً: مراجع باللغة العربية.

١- المراجع العامة:

- د. السعيد مصطفى السعيد: الأحكام العامة فى قانون العقوبات – طبعة دار المعارف بمصر – الطبعة الرابعة ١٩٦٢.
- د. عبد الرؤوف مهدى: شرح القواعد العامة لقانون العقوبات – الجزء الأول، طبعة نقابة المحامين بالجيزة ٢٠٠٨.
- د. مأمون سلامة: شرح قانون العقوبات – القسم العام، مطبعة جامعة القاهرة والكتاب الجامعى ١٩٩٠-١٩٩١.
- د. محمد عيد الغريب: شرح قانون العقوبات– القسم العام، طبعة ١٩٩٩-٢٠٠٠.
- د. محمود محمود مصطفى: شرح قانون العقوبات – القسم العام، مطبعة جامعة القاهرة – الطبعة العاشرة ١٩٨٣.
- د. محمود نجيب حسنى: شرح قانون العقوبات – القسم العام، تنقيح د. فوزية عبد الستار، دار النهضة العربية، الطبعة الثامنة ٢٠١٦.

٢- المراجع المتخصصة:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، والمنشورة على الموقع الإلكترونى:
http://fs8859.0za.in/legislation/HRIDRL0149_ArabConventionCyberCrime_Ar_2010.pdf
- د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، تقرير مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥ – ٢٨ أكتوبر سنة ١٩٩٣، والمنشور تقاريره بدار النهضة العربية سنة ١٩٩٣.
- د. جميل عبد الباقي الصغير:

* الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، سنة ١٩٩٩.
* القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، سنة ١٩٩٢.

- د. حسن عبد الباسط جميعى، عقود برامج الحاسب الآلي، دار النهضة العربية، سنة ١٩٩٨.

- د. شحاتة غريب محمد شلقامى، برامج الحاسب الآلي والقانون، دار النهضة العربية، سنة ٢٠٠٣.
- د. عباوى نجاة: الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات، بحث منشور بمجلة دفاتر السياسة والقانون الجزائرية، العدد (١٦)، يناير ٢٠١٧.
- د.عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، بدون جهة نشر، الطبعة الثانية سنة ١٩٩٥.
- د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية ١٩٩٨.
- د. هشام فريد رستم:

* الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة بأسيوط، ١٩٩٤.

* قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، سنة١٩٩٢.

ثانياً: مراجع باللغة الانجليزية.

- Alden Anderson: Comment, The Computer Fraud and Abuse Act: Hacking into the Authorization Debate, 53 Jurimetrics J. (summer 2013).
- An statistic about number of internet users in the United States from 2015 to 2022, this statistic available online at: https://www.statista.com/statistics/325645/usa-number-of-internet-users/
- An article entitled Crime: available online in June 2009 at: http://www.out-law.com/page-405.
- Bob Burls: How to report a computer crime: Unauthorised email account access, published on October 31, 2012, and available online at: https://nakedsecurity.sophos.com/2012/10/31/how-to-report-a-computer-crime-unauthorised-email-account-access/
- Charles Doyle: Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS 7-5700, October 15, 2014.
- Communications Offences, General Charging Practice: available online at: http://www.cps.gov.uk/legal/a_to_c/communications_offences/

- Computer Fraud and Abuse Act: An article published on 2015, and available online at: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
- Computer Fraud and Abuse Act (CFAA): An article From Internet Law Treatise, last modified on 24 April 2013, and available online at: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA)
- Computer Misuse Act 1990: from Wikipedia, the free encyclopedia, this page was published on (January 2009), and available online at: https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990
- Computer Misuse Overview: 1 February 2007, this article available online at: http://www.jisclegal.ac.uk/LegalAreas/ComputerMisuse/ComputerMisuseOverview.aspx
- David Emm: Cybercrime and the law: a review of UK computer crime legislation, 29 May 2009.
- Derek Wyatt, Richard Allan, Michael Fabricant, Brian White and Nick Palmer: Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, June 2004, this report available online at: http://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf
- Draft explanatory memorandum to the draft convention cybercrime Strasbourg 14 February 2001.
- Edmand Dester Thipursian, Sai Thogarcheti, Abdullah Al Fahad, Chintan Gurjar, Adam Mentsiev, and Alams Titus Mammuan : Case Study – News of the World Phone Hacking Scandal (NoTW) - Posted in Hacking on April 3, 2014 , this study available online at: http://resources.infosecinstitute.com/case-study-news-world-phone-hacking-scandal-notw/
- Eric A. Fischer: Federal Laws Relating to Cyber security: Overview and Discussion of Proposed Revisions, CRS 7-5700, June 20, 2013.
- Federal guide lines for searching and seizing computers, available online at: http://www.usdoj.gov/criminal/cybercrime/searachdocs/toc.html
- Kristin Westerhorstmann: The Computer Fraud and Abuse Act: Protecting the United States from cyber-attacks, fake dating

profiles, and employees who check Facebook at work, Uni. Miami. Nat Sec & Arm Conf. L. Rev, Vol.V, 2015.

- Liu Qian, Fredrik Höglin and Patricia Alonso Diaz: Computer Forensics, Uppsala University, 8 Oct 2007.
- Mark D. Rasch: Criminal Law and the Internet, The Computer Law Association, Inc (USA) 1996.
- Martin Wasip: Computer crimes and other crimes against information technology in the U.K, Rev.int.dr.pén, 1993.
- Michael J L Turner:

*Computer Misuse Act 1990, Cases a database published in 2014, and available online at: http://www.computerevidence.co.uk/Cases/CMA.htm

*Computer Misuse Act 1990 Statistics: Total number of Computer Misuse Act 1990 Prosecutions in England and Wales 2004 – 2010, these statistics available online at: http://www.computerevidence.co.uk/Cases/CMA%20Stats.htm

- Michael W. Bailie and H. Marshall Jarrett: Prosecuting Computer Crimes, study Published by Office of Legal Education Executive Office for United States Attorneys, 2015, this study available online at: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf
- Neil Mac Ewan: The Computer Misuse Act 1990: lessons from its past and predictions for its future, Crim. L. Rev 2008.
- Orin S. Kerr: Cybercrimes Scope: Interpreting access and authorization in computer misuse statutes, L. Rev of NY.Uni. School of Law, Vol. 78, Nov 2003.
- Paul Mobbsfor: Computer Crime - The law on the misuse of computers and networks, an article available online at: http://www.internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605
- Police and Justice Act 2006: available online at: https://wiki.openrightsgroup.org/wiki/Police_and_Justice_Act_2006#Making.2C_supplying_or_obtaining_articles_for_use_in_computer_misuse_offences

- Reform of the Computer Misuse Act 1990: Prepared by ICF Legal Subgroup in 30th April 2003, this study available online at: http://www.internetcrimeforum.org.uk/cma-icf.pdf
- Relevant Penetration Testing Legislation in the UK: published on Tuesday, 3 April 2012, and available online at: http://rewtdance.blogspot.com/2012/04/relevant-penetration-testing.html
- Ryan H. Niland: The CFAA'S vagueness problem and recent legislative attempts to correct it, NC. J.L & TECH, 2014.
- Stefan Frederick Fafinski: Computer use and misuse: the constellation of control, Ph.D. University of Leeds, Sep 2008.
- The Hacking of Computers and the Criminal Law: An article written by selected team of legal experts, this article available online at: http://www.inbrief.co.uk/offences/hacking-of-computers.htm
- The recommandation No R(89)9 on computer-related crime and final report to the European committee on crime problems, Strasbourg, 1990.
- Warren Thomas: Civil Liability under the Computer Fraud and Abuse Act (CFAA), Law Library of the Georgia State University College of Law, Paper 22. 2010.
- Yearwood Douglas L: Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys, May 2003, this study published by North Carolina Governor's Crime Commission and available online at: http://www.ncgccd.org/PDFs/Pubs/NCCJAC/cybercrime.pdf

ثالثاً: المختصرات الأجنبية.

CFAA	Computer Fraud and Abuse Act
Cir	Circuit
C R S	Congressional Research Service
ICF	Internet Crime Forum
Inc	Incorporation
L. Rev	Law Review
L. Rev of NY.Uni	Law Review of New York University
NC. J.L & TECH	North Carolina Journal of law & Technology
Ph.D	Doctor of philosophy
P.R	Previous Reference
Rev.int.dr.pén	Revue International de droit penal
UK	United kingdom
Uni Miami Nat Sec & Arm Conf. L. Rev	University of Miami National Security & Armed Conflict Law Review
US	United States
V	Versus