المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢٠٢ ٢٥٤٨١٠٥٠ + محمول: ٠٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

جرائم القرصنة الرقمية وانعكاساتها الاقتصادية دولياً ومحلياً

القاضي/ سامح سامي عرابي

جرائم القرصنة الرقمية وانعكاساتها الاقتصادية دولياً ومحلياً

القاضي/ سامح سامي عرابي

تقديم:

عرفت المنظمة العالمية للملكية الفكرية [1] [WIPO] World International Property Organization الملكية الفكرية: بأنها "ما تمخضت عنه إبداعات العقل". وإبداعات العقل التي تقصدها المنظمة هنا تشمل الاختراعات والأعمال الأدبية والفنية والرموز والأسماء والصور المستخدمة في التجارة، بالإضافة إلي ذلك تقسم المنظمة "الأعمال الفكرية" إلي فئتين:

الفئة الأولي: هي الملكية الصناعية والتي تشمل الاختراعات والتصميمات الصناعية والدوائر المتكاملة والعلامات التجارية والمؤشرات الجغرافية.

وبالنسبة للفئة الثانية: فهي حقوق الطبع والنشر والتأليف وتضم الكتب والأشعار والمسرحيات والأفلام والأعمال الموسيقية واللوحات والرسومات والصور الفوتوغرافية والتصميمات المعمارية ... الخ [2].

وقد استقر قضاء محكمة النقض المصرية في هذا الخصوص علي أن مفاد النص في المادتين ١٣٨ ، ١٤٠ من القانون رقم ٨٢ لسنة ٢٠٠٢ بشأن حماية حقوق الملكية الفكرية أن المشرع وفقًا لقانون حماية حقوق الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ ومن قبله القانون رقم ٣٥٤ لسنة ١٩٥٤ المعدل بالقانون رقم ٣٨ لسنة ١٩٩٢ بشأن حماية حق المؤلف، أسبغ الحماية الواردة بهما على مؤلفى المصنفات أيًا كان نوعها أو طريقة التعبير عنها أو أهميتها أو الغرض منها، بشرط أن يكون هذا المصنف قد

---

[1] أنشئت المنظمة العالمية للملكية الفكرية بمقتضي معاهدة استكهولم في الرابع عشر من يوليو عام ١٩٦٧م، ومقرها الرئيسي مدينة جنيف بسويسرا ولها مكتب تنسيق لدي الأمم المتحدة في مدينة نيويورك، وحلت محل المكاتب الدولية المتحدة لحماية الملكية الفكرية، وأصبحت واحدة من المنظمات المتخصصة التابعة لهيئة الأمم المتحدة، ولعبت دوراً كبيراً في تدعيم حماية واستخدام حقوق الملكية الفكرية علي المستوي العالمي من خلال التنسيق بين التشريعات الوطنية بوضع قواعد نموذجية تهتدي بها الدول، علي النحو الذي يحقق الاستفادة لجميع الأطراف المعنية.

[2] كوك، كرتيس (٢٠٠٦). **حقوق الملكية الفكرية. من إعداد قسم الترجمة بدار الفاروق** (مترجم إلي اللغة العربية من الأصل باللغة الإنجليزية). ط.١.- القاهرة: دار الفاروق للنشر والتوزيع. ص ص ٤٥-٤٦.

انطوى على شيء من الابتكار بحيث يبين منه أن المؤلف أضفى عليه شيئًا من شخصيته، وأن يتم إفراغه في صورة مادية يبرز فيها إلى الوجود ويكون معدًا للنشر، وبغير ذلك فلا يرقى إلى مرتبة المصنف الجدير بالحماية. وبذلك فإن جوهر حقوق الملكية الفكرية أنها ثمرة الابتكار ونتاج الإبداع في شتى مناحي النشاط الإنساني، وكلاهما – الإبداع والابتكار – يعدان نمطاً من أنماط التفكير ومستوى متقدم في سلم القدرات الذهنية للإنسان يتميز به عن غيره ويتسم بالخروج عن المألوف.

فدلالة الإبداع في اللغة تعنى إحداث شيء جديد على غير مثال سابق وهو ما اصطلح عليه بأنه إيجاد شيء غير مسبوق بالعدم، وهو أعلى مرتبة من التكوين والإحداث وكليهما يقابل الإبداع من وجه وهما مترتبان عليه، فالإبداع مزيج من القدرات والاستعدادات والخصائص الشخصية التى إذا ما وجدت في بيئة مناسبة يمكن أن ترقى بالعمليات العقلية لتؤدى إلى نتاجات أصيلة وجديدة على مستوى الاختراعات الإبداعية في ميادين الحياة الإنسانية، ويندرج فيه كل من الاختراع والإبداع الأدبى أو الفني، والتفكير الإبداعى هو العملية الذهنية التى نستخدمها للوصول إلى الأفكار والرؤى الجديدة أو التى تؤدى إلى الدمج والتأليف بين الأفكار، أو الأشياء التى تعتبر سابقًا أنها غير مترابطة، فالتفكير الإبداعى يصف العمليات وأسلوب التفكير الذى أنتج هذا الإبداع. ويعبر التفكير الإبداعى عن نفسه في صورة إنتاج شيء جديد أو الخروج عن المألوف أو ميلاد شيء جديد سواء كان فكرة أم اكتشافًا أم اختراعًا. وتبرز أهمية الإبداع في أنه يمثل إطلاقًا لطاقات الخلق والاجتهاد دون قيد على العقل إلى الحد الذى ينال فيه المجتهد أجرًا حتى لو أخطأ، بشرط الالتزام بإطار أخلاقى وإنسانى لا يحكمه الهوى، وإنما يحكمه الضمير، لكى يكون ملائمًا وهادفًا إلى دعم القيم الإنسانية.

وأن الدلالة الاصطلاحية لابتكار الشيء فى اللغة هو الاستيلاء على باكورته، بمعنى أن يكون وليد أفكار المرء بالمبادرة إليه وإدراك أوله متسمًا بالحداثة والإبداع وبطابعه الشخصى. ويقصد بالابتكار .. في نطاق الحماية القانونية لحق المؤلف .. الطابع الشخصى الذى يعطيه المؤلف لمصنفه، الذى يسمح بتمييز المصنف عن سواه من المصنفات التى تنتمى إلى ذات النوع، حيث تبرز شخصية المؤلف إما في مقومات الفكرة التى عرضها أو في الطريقة التى اتخذها لعرض الفكرة، فالجوهرى في الأمر هو تميز

الإنتاج الذهنى بطابع معين يبرز شخصية صاحبه سواء في جوهر الفكرة المعروضة أو في مجرد طريقة العرض أو التعبير أو الترتيب أو التبويب أو الأسلوب. والابتكار إما أن يكون مطلقًا وإما أن يكون نسبيًا، فيكون مطلقًا إذا لم يكن المصنف يستند إلى إنتاج سابق، ويكون نسبيًا إذا ما كان المصنف يقتبس عناصر شكلية لإنتاج سابق، ولكن في كلتا الحالتين لابد من خلق ذهنى جديد في جملته لكى يكون شرط الابتكار متوافرًا، ليتقرر حق المؤلف على مصنفه أو ليتمتع بالحماية أو ليستحق صاحبه الاعتراف بملكيته الفكرية وما يترتب عليها من حقوق، ويكفى في ذلك أن يضيف المؤلف إلى فكرة سابقة ما يجعل للفكرة طابعًا جديدًا تختلف به عما كانت عليه من قبل فإذا ما اتضح أن ما تحققه الفكرة لا يعدو أن يكون تطورًا عاديًا وطبيعيًا للقدر القائم أو مألوفًا لأهل الاختصاص فإنه عندئذ يتخلف عنصر الابتكار [1].

بينما يعرف الفقه المصري الملكية الفكرية بأنها عبارة عن "سلطات يخولها القانون لشخص علي شيء معنوي هو ثمرة فكره وانتاجه الذهني".

---

[1] راجع الطعن رقم ٣٣٥٤ لسنة ٨٥ ق "تجاري" – جلسة ٢٠١٦/١٢/٢٧ – لم ينشر بعد.=
=كما قضت بأن "الابتكار كأساس تقوم عليه حماية القانون للمصنف هو الطابع الشخصى الذى يعطيه المؤلف لمؤلفه، إذ يكفى أن يضفى على فكرة ولو كانت قديمة شخصيته فيضفى على مصنفه طابعاً إبداعياً يسبغ عليه أصالة تميزه عن غيره وهو ما قننه المشرع بنص المادة ١/١٣٨ من قانون حماية حقوق الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢، وأن معنى المؤلف ليس مقصوراً على المعنى الضيق المتمثل فى تأليف كتاب وإنما يشمل كل صور الابتكار لأى نوع من المصنفات، وأن الدلالة الاصطلاحية لابتكار الشىء فى اللغة، هو الاستيلاء على باكورته، بمعنى أن يكون وليد أفكار المرء، بالمبادرة إليه، وإدارك أوله، متسماً بالحداثة والإبداع، وبطابعه الشخصى" (الطعن رقم ٧٦٧٨ لسنة ٨٥ ق "تجاري" – جلسة ٢٠١٦/٣/١٣ – لم ينشر بعد).
وفي حكم آخر لها قضت بأنه "إذا كان المقصود بعبارة حقوق الملكية الفكرية هو تأكيد أن حق المؤلف أو المخترع يستحق الحماية كما يستحقها المالك لأن الحقان من ثمرات الفكر والابتكار فهو صحيح، إلا أنه لتنافى طبيعة الملكية مع طبيعة الفكر فإنه ليس حق ملكية، بل هو حق عينى أصلى يستقل عن حق الملكية بمقوماته التى ترجع إلى أنه يقع على شىء غير مادى، فهو اذن حق عينى أصلى منقول، وأن النص فى المواد ١ ، ٢ ، ٣ من قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ يدل على أن الشروط الواجب توافرها فى الاختراع لمنح براءة تحميه هى أن ينطوى الأختراع على ابتكار يستحق الحماية أى يكون جديداً، بمعنى أنه ينطوى على خطوة إبداعية تجاوز تطور الفن الصناعى المألوف، وأنه لم يكون معروفاً من قبل بأن يكون المخترع الذى يطلب براءة الاختراع قد سبق غيره فى التعريف بهذا الاختراع، وألا يكون سبق النشر عنه فى أى بلد، فشرط الجدة المطلقة الذى يجب توافره فى الابتكار محل الاختراع لا يشترط في الإبتكار كأساس تقوم عليه حماية القانون للمصنف، ويشترط أن يكون الاختراع قابلاً للاستغلال الصناعـــى، والمقصود به استبعاد الأفكار المجردة والابتكارات النظرية البحتة وهى ما تعرف بالملكية العلمية، لكن يلزم أن يتضمن الاختراع تطبيقاً لهذه الابتكارات فالبراءة تمنح للمنتج الصناعى، ويشترط أخيراً لا يكون فى الاختراع مساس بالأمن القومى أو إخلال بالآداب أو بالنظام العام أو البيئة" (الطعن رقم ١١٣٥٧ لسنة ٨٣ ق "تجاري"– جلسة ٢٠١٤/١١/٢٤ – لم ينشر بعد).

وقد أشارت إلي هذا النوع من الحقوق المادة ٨٦ من القانون المدني المصري بقولها "الحقوق التي ترد علي شيء غير مادي تنظمها قوانين خاصة". ولقد سار الغالبية من رجال القانون في مصر علي النهج المتبع في معظم دول العالم نحو تقسيم حقوق الملكية الفكرية – أو الحقوق الذهنية كما يسميها جانب كبير من الفقه – إلي قسمين رئيسيين:

القسم الأول: هو عبارة عن حقوق الملكية الصناعية والتجارية.

أما القسم الثاني: فهو خاص بحقوق الملكية الأدبية والفنية، أو حقوق المؤلف كما تسمي في معظم الأحيان [١].

ومع بزوغ عصر الثورة المعلوماتية [٢] ظهرت لأول مرة في تاريخ البشرية مشكلة التعامل مع شكل جديد من أشكال الملكيات يمكن تسميتها بالملكيات الرقمية؛ ويقصد بها (برامج الحاسب وبياناتها) [٣].

---

[١] مأمون، عبد الرشيد، محمد سامي عبد الصادق (٢٠٠٦-٢٠٠٧). حقوق المؤلف والحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم ٨٢ لسنة ٢٠٠٢. القاهرة: دار النهضة العربية. ص ٦ وما بعدها.

[٢] يعيش العالم اليوم عصر التقنية؛ أي عصر التقدم التكنولوجي في الأنشطة الحياتية المختلفة، وإذا كان التقدم العلمي قد ظهر في العديد من الأنشطة منذ زمن بعيد، فقد ظهر حديثاً في مجال مهم هو مجال البيانات والمعلومات – أدي إلي تطورها تطوراً وتقدمها تقدماً مذهلاً، كما سهل انتشارها وذيوعها علي الصعيدين الوطني والدولي. فالمعلومات تعد – بلا شك – عنصراً جوهرياً في كافة الأنشطة الحياتية وباتت أساساً ضرورياً لإصدار القرارات الصحيحة والسريعة، لذلك فقد قيل بأن المعلومات أظهرت نوعاً ثالثاً من الذهب هو الذهب الرمادي إلي جانب الذهب الأبيض (القطن)، والذهب الأسود (البترول) (أحمد محمود، سيد (٢٠٠٩). دور الحاسوب (الكمبيوتر) أمام القضاء المصري والكويتي: نحو إلكترونية القضاء والقضاء الإلكتروني. القاهرة: دار النهضة العربية. هامش ص ٥/ بند ١).

[٣] أوجبت اتفاقية التريبس (TRIPS) – واختصارها (Agreement on Trade Related Aspects of Intellectual Property Rights)؛ وهي اتفاق دولي يتعلق بالجوانب التجارية لحقوق الملكية الفكرية أدارته منظمة التجارة العالمية (WTO) في نهاية جولة الأوروجواي وانبثق عن الاتفاق العام بشأن التعريفات الجمركية والتجارة (الجات / Gatt) في عام ١٩٩٤، يحدد المعايير الدنيا للقوانين المتعلقة بالعديد من أشكال الملكية الفكرية (IP) التي تنطبق على أعضاء منظمة التجارة العالمية. فتحتوي اتفاقية التريبس على الشروط الواجب توافرها في قوانين الدول فيما يتعلق بحقوق المؤلف؛ بما في ذلك حقوق فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة، المؤشرات الجغرافية؛ بما في ذلك تسميات المنشأ، الرسوم والنماذج الصناعية، تصاميم الدوائر المتكاملة، براءات الاختراع، العلامات التجارية، والمعلومات السرية. كما تحدد اتفاقية التريبس أيضاً إجراءات التنفيذ وسبل التحكيم وإجراءات تسوية المنازعات المتعلقة بقوانين حقوق الملكية الفكرية بين الدول الأعضاء الموقعة عليها بما يسهم في تعزيز الابتكار التكنولوجي ونقل وتعميم التكنولوجيا عالمياً – على موقعيها تمديد غطاء الحماية لمختلف حقوق الملكية الفكرية ليستوعب مجالات جديدة لم تكن تشتمل عليها قوانين العديد من الدول ومنها مصر ومن بين تلك المجالات المضافة المؤشرات الجغرافية والتصميمات التخطيطية للدوائر المتكاملة، المعلومات غير المفصح عنها، الحقوق المجاورة لحق المؤلف، وفي نطاقها نظمت حماية برامج الحاسب وقواعد

لذا يبدو منطقياً تقسيم هذه الدراسة إلي مطلبين رئيسيين نعرض في أولهما إلي الأحكام العامة للجرائم المعلوماتية من خلال بيان ماهيتها وخصائصها وأنماط مرتكبيها، ثم في ثانيهما إلي أحكامها الخاصة في مجال الملكية الفكرية باختيار نموذج إجرامي ذائع الصيت لها يعرف بجرائم القرصنة الرقمية نوضح مفهومها وأخطارها الاقتصادية علي الصعيدين الدولي والمحلي، وسبل مكافحتها للحد من أضرارها علي النحو التالي:

المطلب الأول
الأحكام العامة للجرائم المعلوماتية

نتناول في هذا المطلب ماهية الجرائم المعلوماتية وتمييزها عما يشتبه بها وخصائصها وأنماط مرتكبيها علي التفصيل التالي:

أولاً: ماهية الجرائم المعلوماتية:

أسهم التقدم التكنولوجي عبر القرون الماضية في تغيير الحياة الإنسانية، مما أثر علي السلوك الإنساني للأفراد وعلي المجتمع بأسره. ولا شك أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني يضع إطاراً للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال ويحدد الواجبات تجاهها. فالتقدم العلمي والتكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته ويضع الحلول لما يطرأ من مشكلات بسبب استعماله، وهو ما يوجب علي القانون أن تمتد نصوصه إلي الأنشطة الجديدة التي تفرزها التكنولوجيا حتي تحدد الجريمة في نصوص منضبطة ولا يترك بحثها إلي نصوص قانون العقوبات التقليدي

البيانات (م ١٠)، وبذلك= =أضيفت هذه المصنفات إلى مصنفات الملكية الأدبية من خلال استخدام اتفاقية التربس وسيلة الإحالة المقررة في اتفاقية جنيف للمعاهدات، حيث أجرت تعديلاً فعلياً على المصنفات محل الحماية المقررة في اتفاقية برن (لحماية المصنفات الأدبية والفنية ١٨٨٦)، كما نظمت الحقوق المجاورة لحق المؤلف والعلامات التجارية والمؤشرات الجغرافية والتصميمات الصناعية وبراءات الاختراع والدوائر المتكاملة والأسرار التجارية والممارسات غير التنافسية في الرخص (سامي عرابي، سامح (٢٠١٦). **نظرة تحليلية للمنافسة غير المشروعة في إطار قانون حماية الملكية الفكرية المصري**. بحث مقدم إلي **المركز القومي للدراسات القضائية** بمناسبة التدريس في الدورة التدريبية الأولي للسادة المستشارين والرؤساء والقضاة بالمحاكم الاقتصادية وأعضاء النيابة العامة في قانون حماية الملكية الفكرية. ص ص ٤– ٥).

والتي تتسم بعدم اليقين القانوني عند التوسع في تفسيرها أو قد لا تتسع لملاحقة الأنماط الجديدة من الإجرام إضافة إلي عدم إمكانية اللجوء إلي القياس في مجال القانون الجنائي الموضوعي [١].

وقد بدأت الجريمة الإلكترونية في الانتشار مع ظهور برامج قياس درجات الأمان في أنظمة الحاسبات الآلية، حيث تم استخدام هذه البرامج لالتقاط المعلومات والتلاعب بأنظمة الحاسبات التي تحتوي عليها، وذلك لأغراض غير مشروعة. وباستخدام هذه البرامج والتعرف علي نقاط الضعف في نظام الحاسب الآلي الخاص بالمجني عليه، يستطيع الجاني أن يسيطر علي النظام ثم يقوم بنشاطه غير المشروع ويحول هذا النشاط إلي مكاسب غير مشروعة وينتهي بمحو كل أثر يمكن أن يكشف عن الجريمة. ولما كانت الجرائم الإلكترونية تتم داخل أروقة أنظمة الحاسبات الآلية حيث يمكن التنبؤ مقدماً بكافة الاحتمالات والنتائج التي قد تترتب عليها، فإنه يمكن تنفيذ الجريمة الواحدة عدة مرات في الظروف المحيطة ذاتها، بحيث تؤدي إلي إحداث ذات النتيجة في كل مرة [٢].

ويتسع مفهوم الجريمة الإلكترونية ليشمل مجموعة الجرائم التي ترتكب ضد أو بواسطة نظام للمعلومات يعمل من خلال شبكة اتصال، فوجود هذه الشبكة هو شرط مفترض لوقوع هذه الجريمة، فجميع الأعمال التي تقع ضد أمن وسرية المعلومات، وسلامتها، أو توافرها، أو عملية معالجتها، تقع في بيئة إلكترونية داخل شبكة اتصال تقع بها الجريمة

---

[١] سرور، أحمد فتحي (٢٠٠٨). **الجريمة الإليكترونية**، بحث منشور في **مجلة النيابة العامة**. س.١٧، ع.١، مارس. ص ص ٣-٤.

[٢] عادل قورة، نائلة (٢٠٠٥). جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية. ط.١.- بيروت: منشورات الحلبي الحقوقية. ص ٣٦.

ويري الأستاذ باركر Parker أن الجريمة الإلكترونية الخالصة تنطوي علي ست خطوات أساسية، يتم تنفيذها آلياً بواسطة برنامج أو عدة برامج، دون تدخل العنصر البشري، ويمكن تحديد هذه الخطوات فيما يأتي:

البحث عن نظام الحاسب الآلي الذي يحتوي علي المعلومات أو البرامج المطلوبة.

الوصول إلي نقاط الضعف في النظام الذي يحتوي علي هذه المعلومات أو البرامج.

الاستفادة من نقاط الضعف التي تعتري النظام للدخول إليه ثم التحكم فيه.

تنفيذ السلوك الإجرامي الذي تم تحديده مسبقاً.

تحويل هذا السلوك إلي ربح غير مشروع يحصل عليه الفاعل أو إلي خسارة تلحق بالمجني عليه.

إخفاء جميع الأدلة تجنباً لكشف الفاعل وسلوكه الإجرامي.

- Parker (Donn B.), Fighting Computer Crime: A New Framework for Protecting Information, New Jersey: John Wiley & Sons, 1998, pp: 130–132.

الإلكترونية، فالقيمة التي يحرزها نظام الحاسب تكمن عادة فيما يحتويه من برامج وبيانات (Software and Data) أكثر من قيمته كآلة لها أجزاء (Hardware). وفي غالب الأحوال يكون نظام المعلومات محوراً في الجريمة الإلكترونية في حالتين:

الأولي: عندما تتمثل الجريمة في تدمير نظام المعلومات أو البرامج التي يحتوي عليها، من خلال التسلل إلي مواقع الأشخاص والهيئات وبث الفيروسات أو البرامج المخربة التي تمحو البيانات وتشل سير العمل، بل ترسل معلومات مضللة غير حقيقية تؤدي إلي خسائر اقتصادية فادحة، وقد تقع الجريمة بالسطو علي المعلومات أو البرامج كنتيجة لهذا التسلل.

الثانية: أن يكون نظام المعلومات موقعاً للجريمة أو مساعداً علي وقوعها، كأن يستخدم لإرسال رسائل إلكترونية تدعو لإيداع أموال أو تحويل مبالغ أو إعطاء أرقام حسابات أو المشاركة في مشروعات في ظاهرها مربحة، لكنها بالقطع تقع ضمن أعمال النصب، أو للترويج لمنتجات غير أخلاقية أو لشبكات تجارة الرقيق والأطفال، ودون ذلك من الأعمال المخلة والمنافية للآداب [١].

مما سبق يتضح أن الجريمة الإلكترونية تستهدف المساس بالبنية المعلوماتية والتكنولوجية داخل أروقة أنظمة الحاسبات الآلية، وتتنوع وسيلة ارتكابها بين استخدام الحاسب في الاعتداء علي سلامة المعلومات وهو ما يسمي بالجريمة المعلوماتية (جرائم الحاسب Computer Crime)، أو استخدام الشبكة الدولية العنكبوتية International Network – واختصاراً يطلق عليها شبكة الإنترنت Internet [٢] – في هذا الاعتداء وهو

---

[١] فتحي سرور، أحمد. مصدر سابق. ص ص ٤–٥.

[٢] تتكون كلمة "الإنترنت" من مقطعين؛ الأول إنتر Inter، وهو اختصار لكلمة دولي International، والثاني نت Net، وهو اختصار لكلمة Network، وتعني الشبكة. فلفظ الإنترنت هو اختصار لتعبير "International Network"؛ أي الشبكة الدولية، ويطلق عليها بالفرنسية تسمية "شبكة الشبكات"Réseau de Réseaux، ويطلق عليها بالإنجليزية تسمية Network of Network، كما تطلق عليها تسمية الشبكة الأم Réseau mére. في حين اعتبر البعض أن كلمة [إنترنت Internet] مشتقة من العبارة الإنجليزية [interconnection Network]؛ أي شبكة التشبيك أو الشبكة المتصلة أو البينية، وتعني أنها شبكة تربط مجموعة من أجهزة الحاسب المتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها (عبيد الكعبي، محمد (٢٠٠٩). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت: دراسة مقارنة. ط.٢.– القاهرة: دار النهضة العربية. ص ٢٠). ويطلق البعض علي الإنترنت "الطريق السريع الرقمي" أو "شبكة المعلومات الرقمية" أو "طريق البيانات أو المعلومات فائق السرعة" أو

ما يسمي بجرائم الإنترنت Cybercrime، وهو ما يدعونا إلي التمييز بينهما وصولاً لوضع تعريف جامع مانع للجرائم المعلوماتية محور هذه الدراسة.

التمييز بين جرائم المعلوماتية والإنترنت:

أرجع الفقه الجنائي جرائم الحاسب (المعلوماتية) إلي عام ١٩٦٠، أما جرائم الإنترنت فإنه يمكن القول إنها بدأت مع عام ١٩٨٨، وكانت أول الجرائم التي ترتبط عضوياً بالإنترنت هي جرائم العدوان الفيروسي فيما يعرف بجريمة دودة موريس ٢ نوفمبر ١٩٨٨ [١].

ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يستشعر الحرج في التمييز بين كل من جرائم الحاسب وبين تلك الناجمة عن استخدام الإنترنت، حتي أن تقرير الأمم المتحدة عن منع الجريمة عام ١٩٩٥ تبني الموقف المقارن المذكور فصدر عنوان التقرير Computer crimes & other crimes related to computer. لذلك نجد أن تعريف جرائم

"شبكة الخدمات الرقمية المتصلة" أو "كود النقل اللا متزامن" (سمير، محمد. "جرائم الإنترنت وعلاقاتها بالتحولات الاقتصادية". ورقة بحثية قدمت إلي **المؤتمر الدولي الخامس للبحوث العلمية وتطبيقاتها**. القاهرة: ٢١ –٢٤ ديسمبر. ٢٠٠٩. ص٥).

وجدير بالذكر أنه ينبغي عدم الخلط بين الإنترنت Internet ونظام الإنترانت Intranet؛ الذي يعني استخدام التكنولوجيا وبروتوكولات الإنترنت في وسط مغلق. مثال ذلك: المنشأة التي تقيم شبكة للربط بين فروعها المختلفة، باستخدام تقنية تصميم صفحات الإنترنت، حيث يتم وضع لوائح العمل بالشركة أو أسعار بيع منتجاتها أو التطبيقات الخاصة بها، لكي يستفيد منها موظفوا البيع أو أي بيانات أخري تريد المنشأة اطلاع موظفيها عليها، ولا يمكن لأي شخص خارجها الاطلاع علي تلك الصفحات (عبد الباقي الصغير، جميل (٢٠١١). جرائم الإنترنت: الأحكام الموضوعية والجوانب الإجرائية. القاهرة: نادي القضاة. هامش ص ٢/ بند٢).

[١] تعتبر دودة موريس من أولى ديدان المعلومات التي انتشرت عبر الإنترنت، حيث بدأ الأمر في ٢ نوفمبر ١٩٨٨ كتجربة أجراها روبرت تابان موريس، طالب بمعهد MIT لتكنولوجيا المعلومات، ليختبر فيها تأثير دودته الإلكترونية، والتي حملت اسمه فيما بعد، في إصابة الأجهزة المتصلة بالإنترنت رغبة منه في معرفة عددها، وبالتالي الحجم الفعلي لشبكة الإنترنت ، إلا أنها لم تتمكن إلا من إصابة ٦٠٠٠ جهاز فقط، من إجمالي ٦٠ ألف جهاز متصلين بالإنترنت حينها، أي ١٠٪ فقط، في حين تمكنت الـ٩٠٪ الباقية من الصمود. واستدعى ذلك من موريس أن يقوم بتطوير الكود الجديد ليتمكن من تثبيت نفسه، على الأجهزة المتصلة بالإنترنت، ونجح في ذلك، فخلال ساعات قليلة ضربت الدودة "موريس" جميع الأجهزة المتصلة بالإنترنت. وقد وصل إجمالى الخسائر لما يقرب من ١٠٠ مليون دولار. وهو ما تسبب في مثوله أمام القضاء، الذي حكم عليه بالخضوع للمراقبة لمدة ٤ سنوات، و٤٠٠ ساعة من العمل المجتمعي، إلى جانب غرامة مالية قدرها ١٠ آلاف دولار، ليكون بذلك أول من يتم محاكمته بموجب قانون الاحتيال الإلكتروني الأمريكي. وبعد أن تم شفاء شبكة الإنترنت من نشاط الدودة المخربة، تم الاحتفاظ بنص الكود الخاص بتكوينها على قرص مرن Disk Floppy داخل متحف العلوم بمدينة بوسطن الأمريكية.
- www.dotmsr.com/605/1/116269. 2/1/2020.

الحاسب في الفقه والتشريع يسوده اتجاه يجمع بين الجرائم التي تقع علي الحاسب ذاته وتلك التي يكون الحاسب وسيلة ارتكابها، فهي لدي هذا الاتجاه تعرف بأنها "فعل غير مشروع يتورط نظام الحاسب فيه، سواء كان الحاسب كآلة هو موضوع الجريمة أو كان الوسيلة إلي ارتكابها أو مستودع الدليل المرتبط بالجريمة" [١]. وذهب اتجاه يضيق من مفهوم جريمة الحاسب الآلي إلي أنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخري" [٢]. وفي تضييق آخر لمفهوم جريمة الحاسب الآلي، يري البعض أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلي المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه" [٣]. في حين ذهب اتجاه آخر يوسع من مفهوم جريمة الحاسب الآلي إلي أنها "كل سلوك إجرامي يتم بمساعدة الحاسب الآلي أو هي كل جريمة تتم في محيط الحاسبات الآلية" [٤].

ويلاحظ علي هذه التعريفات التي تنوعت بين الضيق والسعة أنها قد اعتمدت معياراً مشتركاً في تمييز جرائم الحاسب الآلي استند إلي الحاسب ذاته سواءً كان هو وسيلة ارتكابها أو توافرت في خصوصها العلم بتقنيته أو كان موضوعها أو وقعت في محيطه، فالمعلومة هي الأساس المشترك لهذه النوعية من الجرائم، وهو ما أدي إلي تسميتها بالجرائم المعلوماتية، التي سنتناولها بمزيد من الشرح والتفصيل في الفصل الثاني والأخير من هذه الدراسة، ومن ثم يكفي للقول أننا بصدد جريمة حاسب أن يكون الأخير في حالة عمل وفي مرحلة تالية يقع النمط التجريمي الخاص به المؤثم من قبل المشرع الجنائي، أما في جرائم الشبكة الدولية للمعلومات (الإنترنت) فلا يكفي لقيامها أن يكون الحاسب في حالة عمل، وإنما تستلزم فوق ذلك أن يقوم الجاني بالولوج إلي الشبكة من خلاله بالاتصال بوسيط هو مزود

---

[١] رسلان، أيمن، عبد العال الديربي ومحمد إسماعيل (٢٠١٢). جرائم المعلوماتية والإنترنت بين العالم الافتراضي والواقع بالتطبيق علي مصر والوطن العربي. القاهرة: نادي القضاة. ص ٦.

[3] Taber (J .K.), on Computer Crime, **C.L.J**., Vol. 1, 1979, p. 517.

[٣] محمد فريد رستم، هشام (١٩٩٢). قانون العقوبات: مخاطر تقنية المعلومات. أسيوط: مكتبة الآلات الحديثة. ص ٣١.

[2] Norman (Adrian R. D), Computer Crime and the law, **C.L.J.**, Vol. 15, 1991, p. 399.

الإنترنت Provider ليتمكن من التعامل مع الخادم Surver واستهداف أنظمة الشركات المتصلة حواسيبها بذات الشبكة، وكذلك التشهير بالأفراد المتواجدين عليها (Online) أو أثناء غيابهم عنها (Off line) للإضرار بهم وغير ذلك من الأنماط التجريمية التي تجد مسرحها داخل أروقة الشبكة الدولية للمعلومات.

ثانياً: خصائص الجرائم المعلوماتية:

تتميز هذه الجرائم بعدة خصائص نعرض لأبرزها فيما يلي:

١) خفاء الجريمة وسرعة التطور في ارتكابها:

تعد جرائم المعلوماتية في أكثر صورها خفية لا تترك آثاراً مادية خارجية يمكن متابعتها [١]، فلا يوجد جثث قتلي ولا آثار دماء [٢]، حيث يتم الإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها بحكم توافر المعرفة والخبرة في مجال الحاسبات غالباً لدي مرتكبيها. كما يستفيد المجرمون في نطاق الشبكة العنكبوتية من تبادل الأفكار والخبرات الإجرامية فيما بينهم، ويبدو ذلك جلياً في مختلف المواقع الإلكترونية [٣] ومنتديات القراصنة الهاكرز (Hackers) [٤]، التي تضمن لهم

[١] ممدوح إبراهيم، خالد (٢٠٠٨). أمن الجريمة الإلكترونية. الإسكندرية: الدار الجامعية. ص ٤٥.

[٢] أحمد عبابنة، محمود (٢٠٠٩). جرائم الحاسوب وأبعادها الدولية. عمان: دار الثقافة للنشر والتوزيع. ص ٣٧.

[٣] الموقع الإلكتروني؛ هو عبارة عن مجموعة من صفحات الويب ذات الصلة مع بعضها البعض، يمكن الوصول إليها عبر شبكة مثل الإنترنت أو الشبكة المحلية الخاصة. والصفحة الواحدة تحتوي علي نص، أو صور، أو مقاطع فيديو وغيرها. وهذه الصفحة ممكن أن تشارك في الإقناع والشراء والبيع وأغراض أخري لا تقل أهمية عن هذه الأمور (عبد القوي علي مصري، عبد الصبور (٢٠١٢). المحكمة الرقمية والجريمة المعلوماتية. ط.١.– الرياض: مكتبة القانون والاقتصاد. ص١٦٩).

[٤] بدأ مصطلح الهاكرز (Hackers) في كسب شعبيته عام ١٩٨٣ عندما تحدثت مجلة النيوزويك الأمريكية – واسعة الانتشار – عن هؤلاء الأشخاص ووصفتهم بأنهم ممن يفضلون البحث والتنقيب في أعماق الحاسب الآلي بدلاً من استخدامه فقط، كما قالت عنهم المجلة حينها أنهم لعوبون وفضوليون وأذكياء ويفضلون العمل الفردي ولهم شغف كبير تجاه الحاسب والشبكات. أضافت المجلة أنهم كابوس مديري الشبكات وخدمات الأمن وأيضا المباحث الفيدرالية الأمريكية (الـ FBI)، وأن بعض هؤلاء الهاكرز تركوا تاريخاً تكنولوجياً مثيراً خلال علاقتهم بالحاسب وأصبحوا مثلاً أعلى لطبقة كاملة من مستخدمي الحاسب الأكثر حداثة والأصغر سناً حول العالم. بعض هؤلاء يمكنهم خرق أي دفاع أو حماية موجودة على وجه الأرض وبعضهم لعب دور الهارب في مطاردات خيالية لا تصدق عبر الشبكات اشتركت فيها قوى أمنية كبيرة.

- https://ar-ar.facebook.com/notes, 1/1/2020.

الاتصال فيما بينهم من أجل تبادل المعارف والخبرات في مجال القرصنة وذلك من أجل ارتكابهم لجرائمهم بعيداً عن أعين الأمن. ففي الولايات المتحدة الأمريكية وتحديداً في مدينة لاس فيجاس ينعقد سنوياً مؤتمر يسمي DEF CON الذي يجمع المراهقين من جميع أنحاء العالم ضمن أكبر التجمعات التي تقلق خبراء أمن المعلومات والحكومات علي حد سواء، حيث يسمح هذا التجمع المريب للقراصنة بتبادل المعلومات والشفرات الخبيثة مما يؤدي إلي تكوين شبكات القراصنة التي تمتد في جميع أنحاء العالم [١].

٢) ذاتية في تنفيذها:

تبرز هذه الذاتية بصورة أكثر وضوحاً في أسلوب ارتكابها. فإذا كانت الجرائم التقليدية – كما سبق القول – تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة ... فإن جرائم المعلوماتية هي جرائم هادئة بطبيعتها (Soft crime) لا تحتاج إلي العنف، بل كل ما تحتاج إليه هو وجود حاسب آلي يستعان به كوسيلة لتنفيذها، فهو من المتطلبات الرئيسية لارتكابها "أداة الجريمة". وفضلاً عن ذلك يتطلب ارتكابها أن يكون الجاني لديه إلماماً كافياً بمهارات ومعارف استخدام الحاسب الآلي فنياً كالمعرفة

ويعود الفضل في الكشف عن مصطلح الهكترة Hacking إلي كاتب الخيال العلمي الكندي الأمريكي/ ويليام جيبسون W. Jibson في أولى رواياته The NeuRomancer التي صدرت عام ١٩٨٤، ونالت شهرة واسعة كأحد أشهر أوائل روايات السيبربنك رشحتها لحصد عدد من الجوائز. وتجدر الإشارة إلى أن الرواية تحدثت عن مفاهيم تدور حول الذكاء الصناعي، والواقع الافتراضي، وهندسة الجينات، وهيمنة الشركات متعددة الجنسيات بحيث بات لديها نفوذ يفوق الدول الوطنية التقليدية، وقد تحدثت الرواية عن كل تلك المفاهيم في حقبة الثمانينات، أي قبل وقت طويل من شيوع تلك المفاهيم في ثقافة الناس كما هو الحال اليوم. قصة الرواية تدور حول قرصان حاسب يستأجره شخص غامض للقيام بعملية قرصنة حاسوبية هامة. الهدف النهائي كان ربط جهازي حاسب فائقين يتمتعان بذكاء صناعي= =عالي، لينتج عن ذلك جهاز حاسب جديد بمستوى ذكاء صناعي يتجاوز الحدود المسموح بها وفق القوانين في الرواية. مساعي الاندماج هذه قادها أحد الحاسبين رغبة منه في الاندماج مع الحاسب الثاني.
- https://ar.wikipedia.org/wiki. 2/1/2020.

[١] يوسف، صغير (٢٠١٣). **الجريمة المرتكبة عبر الإنترنت**. أطروحة ماجستير. قسم القانون الدولي للأعمال. كلية الحقوق والعلوم السياسية. جامعة مولود معمري– تيزي وزو. ص ١٥.

التقنية به وكيفية تشغيله واستخدامه، وكلما زادت المعرفة التقنية لديه زادت احتمالية توظيفه لها بطريقة غير مشروعة [١].

٣) صعوبة إثبات الجريمة وسرعة محو دليلها:

تتميز جرائم المعلوماتية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلي افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناهي القصر [٢]. فجرائم الإنترنت تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسب والإنترنت مما يجعل الأمور تزداد تعقيداً لدي سلطات الأمن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غاية السهولة. ففي إحدي الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلي الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير [٣].

٤) جريمة مستحدثة:

تعد الجرائم الإلكترونية، وخاصة جرائم المعلوماتية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها. وعلي الرغم من المزايا والمنافع الإيجابية المترتبة علي هذه العولمة وثورة المجتمع الإلكتروني، إلا أنها ساعدت علي ظهور وتعزيز أنواع جديدة من الجرائم، من أبرزها جرائم غسل الأموال،

---

[١] عبد العزيز أبازيد، محمود (٢٠١٦). الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية. أطروحة دكتوراه. قسم القانون الجنائي. كلية الحقوق. جامعة القاهرة. ص ص ١٦٥–١٦٦.

[٢] رسلان، أيمن، عبد العال الديربي ومحمد إسماعيل. مصدر سابق. ص ٤٣.

[٣] عبد القادر المومني، نهلا (٢٠١٠). الجرائم المعلوماتية. عمان: دار الثقافة للنشر والتوزيع. ص ٥٦.

وتهريب المخدرات، واختراق قطاع الأعمال، والإفلاس بالتدليس والغش، والفساد ورشوة الموظفين العموميين، وسرقة الملكيات الفكرية، والاتجار غير المشروع في الأسلحة وفي النساء والأطفال، والاتجار غير المشروع في الأعضاء البشرية، وسرقة المقتنيات الفنية والثقافية، والغش في التأمين، والجرائم الإلكترونية [١].

٥) جريمة متعدية أو عابرة للحدود الدولية – National Trans:

إن من أهم الخصائص التي تميز جرائم المعلوماتية إذ ما تم استخدام شبكة الإنترنت في ارتكابها؛ هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، وهو ما أدي إلي تمييزها عن الجرائم التقليدية بصورة كبيرة. وتظهر هذه المشكلة – طبيعتها المتعدية للحدود – بصفة خاصة في مجال البنوك، حيث أدي التوسع الكبير في إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلي إعطاء بعد دولي لجرائم الاحتيال المعلوماتي بصفة خاصة. فربط وسائل الاتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية التي تتم بوسائل إلكترونية وبصفة خاصة من خلال التحويل الإلكتروني للأموال "Electronic Funds Transfer"، والتبادل الإلكتروني للمعلومات "Electronic Data Interchange"، ولا يقتصر الأمر علي المعاملات المالية فقط، بل إن الطبيعة الدولية لجرائم الإنترنت تظهر في أنماط أخري من السلوك الإجرامي، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلي ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصاً آخر موجود في بلد ثالث. وكذلك فيما يتعلق بالإتلاف المعلوماتي، فإعداد أحد البرامج الخبيثة (الفيروسات) يمكن أن يحدث في دولة ما، ثم يتم نسخ هذا البرنامج آلاف المرات ويرسل إلي عدة دول متفرقة من العالم [٢]. ومن ثم لا يقتصر الضرر المترتب علي الجريمة علي المجني

---

[١] ممدوح إبراهيم، خالد. مصدر سابق. ص ص ٥١–٥٢.

[٢] عادل قورة، نائلة. مصدر سابق. ص ص ٥٢–٥٣.=

=ومن القضايا التي لفتت النظر إلي البعد الدولي لجرائم الإنترنت – عقب قضية دودة موريس سنة ١٩٨٨ التي سجلت أول اعتداء أمني تم باستخدام الشبكة العنكبوتية علي التفصيل المتقدم – تلك القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز)، وتتلخص وقائع هذه القضية التي حدثت عام ١٩٨٩ في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج – بواسطة شبكة الإنترنت – الذي هدف في ظاهره إلي إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي علي فيروس (حصان طروادة)؛ إذ كان يترتب علي تشغيله تعطيل جهاز الحاسب

عليه وحده، وإنما قد يتعداه إلي متضررين آخرين في دول عدة، وهذا هو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي أو التربوي أو الاقتصادي [١].

٦) عدم كفاية القوانين القائمة لمواجهتها:

لم تعد القوانين القائمة التي كانت سائدة قبل ظهور جرائم المعلوماتية والإنترنت وانتشارهما قادرة علي مواكبة هذه السرعة الهائلة في التكنولوجيا، والتي أدت إلي تطور هذه الأنماط الإجرامية، وباتت القوانين التقليدية القائمة عاجزة عن مواجهة هذه الجرائم مما استلزم تدخل المشرع في بعض الدول لسن تشريعات حديثة لمواجهتها للمحافظة علي مبدأ الشرعية الجنائية الذي يقضي بأنه [لا جريمة ولا عقوبة إلا بنص]، وذلك لعدم اللجوء للقياس في المسائل الجنائية، الأمر الذي أوجب علي القائمين علي القوانين أن يسيروا بخطوات مواكبة للتطورات السريعة التي تشهدها هذه التقنيات الحديثة [٢]. مع تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في مجال المعلوماتية زيادة علي التعاون الدولي لمكافحتها [٣].

عن العمل ثم تظهر بعد ذلك عبارة علي الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل علي عنوان معين حتي يتمكن المجني عليه من الحصول علي مضاد للفيروس، وفي الثالث من فبراير من عام ١٩٩٠ تم إلقاء القبض علي المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية ، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي علي تسليم المتهم، وتم توجيه إحدي عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:- الأولي: أنها المرة الأولي التي يتم فيها تسليم متهم في جريمة بهذه النوعية. الثانية: أنها المرة الأولي التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث "فيروس" (يوسف، صغير. مصدر سابق. هامشي ص ص ١٧/ بند ٤٨-١٨).

[١] عبيد الكعبي، محمد. مصدر سابق. ص ص ٣٩-٤٠.

[٢] المصدر السابق. ص ٤٤.

[٣] وتعد اتفاقية بودابست لمكافحة جرائم الفضاء المعلوماتي أو جرائم الحاسب الآلي، المُوقعة ببودابست في ٢٣ نوفمبر ٢٠٠١ وبروتوكولها الإضافي الموقع بستراسبورغ في ٢٨ يناير ٢٠٠٣ – أول معاهدة دولية بالجرائم الجنائية المرتكبة عبر الإنترنت والشبكات المعلوماتية الأخرى والتي تركز بصفة خاصة على الجرائم الملحقة بحقوق المؤلف الناتجة عن الاحتيال المعلوماتي واستغلال الأطفال في المواد الإباحية وكذلك الجرائم المتعلقة بأمن الشبكات المعلوماتية. وهي تهدف بالإضافة إلى بروتوكولها الإضافي إلى مواصلة سياسة جنائية مشتركة تروم حماية المجتمع من الجرائم المعلوماتية خاصة باعتماد التشريعات المناسبة وتعزيز التعاون الدولي. ويؤكد البروتوكول الإضافي لهذه الاتفاقية ما جاءت به مقتضيات هذه الأخيرة من ضرورة جعل المعلومات والتكنولوجيات الحديثة فرصاً مهمة لتسهيل حرية التعبير والتواصل عبر العالم، كما تضمنت الإتفاقية قواعد إجرائية متعلقة بالإختصاص القضائي في المادة (٢٢) منها ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية، مؤكدة على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية و تدابير أخرى لإقرار الإختصاص القضائي على الجرائم الواردة في

الإتفاقية، فالمادة (٢٢) وضعت مجموعة من المعايير والتي بمقتضاها تنسق الأطراف المتعاقدة حدود صلاحياتها المتعلقة بالجرائم الواردة في الإتفاقية، وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها وكذا على كل جريمة مرتكبة من جانب أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الإختصاص القضائي لأية دولة، كما نصت الإتفاقية على عدم استبعاد الإختصاص الجنائي الذي ينص عليه أحد الأطراف وفقا لقانونه الوطني ومطالبة الدول الأطراف في الإتفاقية بالتشاور حول الإختصاص القضائي الأكثر ملاءمة لمحاكمة مرتكبي الجرائم الإلكترونية في حالة تعدد المطالبة من طرف الأطراف بإختصاصه القضائي حول واقعة معينة، كما تضمنت هذه الإتفاقية= =آليات في مجال التعاون بين الدول في مجال الإجراءات، حيث يمكن لإحدى الجهات أن تطلب من جهة أخرى أن تأمر أو تفرض حماية سريعة وبطريقة مختلفة لبيانات مخزنة في نظم معلوماتية داخل حدود هذه الجهة الثانية لتسهيل عملية البحث عنها والوصول إليها، فبهذه الآلية يصبح الوصول إلى البيانات المخزنة خارج الحدود ممكناً وسهلاً لأي جهة تود أو تطلب ذلك.

وفي ذات الإطار السابق أبرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المُوقعة في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠م، بهدف تعزيز التعاون بين الدول العربية وتدعيمه في مجال مكافحة جرائم تقنية المعلومات، وكانت دولة الإمارات العربية المتحدة من أول الدول الموقعة عليها، ثم إنضمت إليها مصر بالقرار بقانون رقم ٢٧٦ لسنة ٢٠١٤ – الصادر بتاريخ ٢٠١٤/٨/١٩ والمعمول به اعتباراً من ٢٠١٤/١٠/٨ – والمنشور بالجريدة الرسمية في العدد ٤٦ الصادر في ١٣ نوفمبر ٢٠١٤م – وتم إقراره من مجلس النواب – مع التحفظ بشرط التصديق؛ الذي يعني إعلان من جانب الدولة باستبعاد أو تعديل الأثر القانوني لأحكام معينة في الاتفاقية من حيث سريانها على هذه الدولة، وتعليقه علي إقرار السلطة المختصة بها كيما تكون نافذة علي إقليمها، وبإجراء التصديق تكون الدولة قد قبلت رسمياً بالاتفاقية ونفاذها في إقليمها. ولا يوجد أجل معين لإجراء التصديق قبل انقضائه إلا إذا حدد مثل هذا الأجل صراحة في الاتفاقية. وبذلك لاتزال أحكام الاتفاقية المعنية غير سارية في النطاق الإقليمي للدولة المصرية بسبب عدم تصديق مجلس النواب عليها لدخولها حيز التنفيذ.

وقد جاءت أحكام الإتفاقية العربية المعنية مطابقة لأحكام اتفاقية بودابست خاصة على مستوى القواعد الإجرائية، حيث نصت على مجموعة من القواعد الإجرائية أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يتعلق بالأبحاث الجنائية كتدابير التحفظ على بيانات الحاسب المخزنة وكشفها وإصدار الأوامر بتسليمها، وإجراءات التفتيش على المعلومات المخزنة وحجزها والتجميع الفوري لها واعتراض محتواها، كما تناولت الاتفاقية الاختصاص في المادة (٣٠) منها، حيث نصت على التزام كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في هذه الإتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت في إقليمها أو على متن سفينة تحمل علم هذه الدولة أو على متن طائرة مسجلة تحت قوانينها أو من قبل أحد مواطنيها إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة أو إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

ويتضح مما سبق، أن ضوابط الاختصاص القضائي التي وضعتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لا تخرج في مضمونها عن تلك التي أقرتها اتفاقية بودابست في خصوص الجريمة الإلكترونية بصفة عامة وجرائم المعلوماتية والإنترنت علي وجه الخصوص، وفي هذا السياق يمكن القول بأن تلك الضوابط قادرة علي حل بعض إشكاليات الجرائم الأخيرة لا سيما ما يتعلق منها بالقانون الواجب التطبيق علي الوقائع الإجرامية العابرة للحدود الوطنية، وإن كانت قد جعلت ذلك مشروطاً بتوافق الدول الأطراف المعنية بها، وهو أمر يتعذر حدوثه في كثير من الأحيان باعتباره ماساً بسيادة هذه الدول، والتي تتجسد أهم مظاهرها في اختصاص قضائها الوطني بنظر تلك الجرائم ومحاكمة مرتكبيها.

بيد أن هناك إشكاليات كثيرة لم تتعرض لها الاتفاقيات السابقة منها علي سبيل المثال: موضع النتيجة الإجرامية المعتبر في جرائم المعلوماتية والإنترنت متتابعة الأفعال – والتي يشكل كل فعل منها جريمة في حد ذاته وصولاً لتنفيذ غرض إجرامي واحد – إذا امتدت خارج الحدود الوطنية لتشمل دولاً أخري، وكذلك الحال بالنسبة للأعمال التحضيرية التي بمنأي عن العقاب في جرائم الإنترنت، والتي تعد تمهيداً لازماً لاقتراف مثل هذه الجرائم علي نحو يتناقض مع أهداف السياسة الوقائية الحديثة للتجريم. ومن ثم **نوصي** بتعديل الاتفاقيات السابقة من خلال سن قواعد وضوابط إلزامية علي الدول أطرافها لتتواءم مع هذه

ثالثاً: أنماط المجرم المعلوماتي:

يتمثل عالم القراصنة في مجال الحاسب الآلي والشبكة الدولية للمعلومات في قراصنة المعلومات، وهم عادة مبرمجون من أصحاب الخبرة يهدفون للدخول إلي الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكننا تصنيف القراصنة إلي صنفين هما:

١) القراصنة الهواة – Hackers:

ويطلق علي هذه الطائفة مصطلح الهاكرز (Hackers) [١] الذي ينصرف مدلوله إلي الشخص المتطفل الذي يدخل علي شبكات وحاسبات الآخرين بدون وجه حق. وأطلق هذا المصطلح لأول مرة في الستينات من القرن المنصرم، بواسطة مجموعة من الطلبة صغار السن الذين يدرسون في الجامعات الأمريكية [٢]، ممن يتميزون بقدر عال من الكفاءة التقنية، ويتفاخرون بإلمامهم بعلوم الحاسب، وبقدرتهم علي اختراق شبكات الحاسب

المستجدات المتطورة (سامي عرابي، سامح (٢٠٢٠). جرائم الإنترنت الاقتصادية: دراسة مقارنة بين التشريعين المصري والإماراتي مدعمة بالتطبيقات القضائية. القاهرة: دار النهضة العربية– قيد الطبع. هامش ص ١١٨).

[١] راجع في خصوص ما تقدم، هامشي ص ص ١٢/ بند ٤–١٣ من هذا البحث.

[٢] يمكن القول إنه استدعي الأمر المرور بأربعة أجيال لكي يصل مصطلح المجرم المعلوماتي إلي ما هو عليه الآن من حيث الإجرام، فقد تشكل الجيل الأول لمصطلح الهاكر أو الهكرة في فترة الستينات من القرن العشرين ليتم اطلاقه علي المبرمجين المبدعين Creative programmers من طلبة الحاسب والاتصالات وبصفة خاصة طلاب معهد ماساشوستس للتكنولوجيا في الولايات المتحدة الأمريكية لما أشتهر عنهم من براعة كبيرة في مجال الحاسب الآلي، ثم امتد ليطلق علي مطوري علوم الحاسب وتقنية الاتصالات Computer evolutioners، فقد مثل هؤلاء الجيل الثاني لمصطلح الهاكر وكان ذلك في سبعينات القرن العشرين وهؤلاء أطلق عليهم أيضاً مصطلح Phreaker الذي يعني كل شخص لديه القدرة التقنية علي استكشاف نظام الهاتف لكي يحصل علي خدمة اتصالات هاتفية مجانية من منطلق التجربة، وفي الثمانينات من القرن المذكور اطلق هذا المصطلح علي مخترقي الألعاب الإلكترونية وحقوق النسخ Games & copyright breaking عبر خدمات الشبكة الحاسوبية Bulletin Board Service(BBS) ويمثلون الجيل الثالث أو جيل الحاسب الشخصي PC، ولقد قامت تنظيمات عصابية منذ ذلك التاريخ ومن ذلك التنظيم العصابي (S 414) الذي قام بأكثر من أربعين حالة اختراق آنذاك، ثم تطور أخيراً إلي ما هو عليه الآن ليستقر عند المجرمين والتافهينCriminals & Cyberpunk وهم العناصر البشرية للجيل الرابع الذين يعدون في قمة الخطورة الإجرامية، وأشهر هكرة الجيل الرابع، ليس هو من قام بالاختراق ثم أمكن التعرف عليه ومحاكمته، وإنما يظل أشهرهم علي الاطلاق هو ذلك المجهول الذي يخترق ثم إنه يمكث لفترات طويلة دون أن يدري به أحد ويخرج تاركاً ورائه لا شيء سوي ذلك التعبير الذي يعتري وجوه العاملين في المكان الذي كان متواجداً فيه حين يتم اكتشاف آثار له لا تدل علي شخصيته، وإنما علي وجود مجهول فقط (عبد الحميد نبيه، نسرين (٢٠٠٨). الجريمة المعلوماتية والمجرم المعلوماتي. الإسكندرية: منشأة المعارف. ص ص ١٠–١١).

الآلي بجهدهم الذاتي، وبدون الاستعانة بأية تعليمات من أية مصادر [١]. كما يطلق أيضاً مصطلح الهاكرز علي ذلك المقتحم التقليدي الذي يقوم بالتلصص علي الغير ويتاجر في قطاع المعلومات، وإذا ما واجهته حماية، لا يستطيع تخطيها إذ ليس له علاقة بتكنولوجيا المعلومات [٢]. ويضم هذا الصنف من القراصنة الأشخاص الذين يستهدفون من الدخول إلي أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض [٣]، وذلك بهدف اكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات القدرة علي اختراق هذه الأنظمة [٤]، وهم غالباً من الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، وبعضهم يطلق عليهم صغار نوابغ المعلوماتية [٥]، أو المتلعثمين باعتبارهم طائفة ممن يقومون باستخدام الحاسب الآلي بصورة غير مصرح بها ولأغراض خاصة أو لمجرد التخريب الأعمي أو العبث لمجرد العبث بواسطة خطوط الهاتف بعد إيجاد كلمة السر [٦].

وهذا القسم من القراصنة أو ما اصطلح علي تسميتهم "بالهاكرز" يرون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية، فهم يرتكبون جرائم التقنية بدافع التحدي الإبداعي، ويجدون أنفسهم متفقين إلي درجة أنهم ينصبون أنفسهم أوصياء علي أمن نظم المعلومات في المؤسسات المختلفة. فالباعث الأساسي لهذه الطائفة هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية لإثبات مهاراتهم وقدراتهم باكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية [٧]. وهذه الطائفة غالباً ما تكون من هواة الحاسب؛ فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون علي اقتحام المواقع الأمنية أحياناً أو لمجرد ترك بصماتهم التي تثبت وصولهم إلي تلك المواقع أحياناً أخري. وهم يدعون دائماً أنه لا توجد دوافع تخريبية وراء أعمالهم، بل

---

[١] أحمد عبابنة، محمود. مصدر سابق. ص ص ٤٠-٤١.

[٢] فتحي أحمد عبد الكريم، مني (٢٠١١). الجريمة عبر الشبكة الدولية للمعلومات (Internet): صورها ومشاكل إثباتها. القاهرة: دار النهضة العربية. ص ٢٦.

[٣] رسلان، أيمن، عبد العال الديربي ومحمد إسماعيل. مصدر سابق. ص ٤٩.

[٤] عادل قورة، نائلة. مصدر سابق. ص ٦١.

[٥] سامي الشوا، محمد (٢٠٠٣). ثورة المعلومات وانعكاساتها علي قانون العقوبات. القاهرة: الهيئة المصرية العامة للكتاب. ص ٣٩.

[٤] أحمد عبابنة، محمود. مصدر سابق. ص ٤١.

[٧] بيومي حجازي، عبد الفتاح (٢٠٠٧). مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت. المحلة الكبرى: دار الكتب القانونية. ص ٤٦.

قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول. ومجرمو الإنترنت من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمهارة المطلوبة في مجال الحواسيب والشبكات الإلكترونية. فعلي سبيل المثال خرق استشاري تقنية معلومات أحد الأنظمة الأمنية لشبكة الإنترنت البريطانية لمجرد كشف الفجوات الأمنية. وقد نجح في الحصول علي أسماء لأكثر من (٢٤) ألف شخص وعناوينهم وكلمات السر ومعلومات البطاقات الإئتمانية من بينهم خبراء عسكريون وموظفون حكوميون وكبار مديري الشركات، وفي مقابلة سرية أجرتها صحيفة التايمز مع هذا القرصان قال "إن اختراق الموقع الأمني مسألة سهلة جداً فهي أشبه بمن يبحث عن مفتاح معين في مجموعة صناديق ثم يجد أمامه بوابة جانبية مفتوحة علي مصراعيها" [١]. ومن ثم فالهاكرز مخترقون متطفلون يتحدون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة [٢].

وهناك القراصنة الأخلاقيون الذين يقولون أنهم يعملون من أجل المصلحة العامة، فشكلوا لهم منظمات خاصة مثل منظمة القراصنة ضد مواقع إباحية الأطفال التي استطاعت القيام بحملات تأديبية لتعطيل قدرة بعض المواقع الإلكترونية عن عرض مواد غير أخلاقية. وفي الحقيقة هناك سمة غالبة علي أعضاء هذه الطائفة من القراصنة هي صغر السن يضاف إليها قلة الخبرة وعدم التمييز بين الأنظمة محل الأختراق. والسمة المميزة الأخري لهذه الطائفة تبادلهم المعلومات فيما بينهم، وتحديداً التشارك في وسائل الاختراق وآليات نجاحها، وإطلاعهم بعضهم البعض علي مواطن الضعف في نظم المعلومات والشبكات خاصة عن طريق النشرات الإعلامية الإلكترونية ومجموعات الأخبار. إلا أن الحقيقة التي يجب أن لا نخفيها هي أن هؤلاء القراصنة الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي قد يقوم بها مجرمو المعلوماتية والإنترنت، ويشاع في بعض المنشآت التي يضبط بها أحد قراصنة

[١] عبد القادر المومني، نهلا. مصدر سابق. ص ٨٣.
[٢] محمود مصطفي، أحمد (٢٠١٠). جرائم الحاسبات الآلية في التشريع المصري: دراسة مقارنة. القاهرة: دار النهضة العربية. ص ٢١.

المعلومات أن يتم إلحاقه بالفريق المعلوماتي المكلف بأمن النظام المعلوماتي فيها [1].

أما عن الوضع القانوني لهذه الطائفة، فقد تعددت وتباينت الآراء بشأنها، حيث يري البعض أنه: "لا يبدو من المناسب أن نصنف هؤلاء الشباب في طائفة أو أخري من الطوائف الإجرامية لأن لديهم ببساطة ميلاً للمغامرة والتحدي والرغبة في الاكتشاف ونادراً ما تكون أهداف أفعالهم المحظورة غير شريفة، وهم لايدركون ولا يقدرون مطلقاً النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة، أو شركة تجارية" [2]. بينما هناك اتجاه آخر يناصر هذه الفئة ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار ويتمادي هذا الاتجاه في تقديره لهذه الفئة باعتبارهم لا يسببون ضرراً للنظام ولا يقومون بأعمال احتيال وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات [3] – إلي حد وصفهم بالأبطال الشعبيين الحديثين الذين يقدمون خدمة للتقنية، وذلك بإظهار نقاط الضعف وعيوب أمن المعلومات، ومن أنصار هذا الاتجاه الإنجليزي (هو جوكونول) الذي نشر كتاباً بعنوان (الدليل الجديد للمتلعثمين) [4]. ويذهب اتجاه أخير إلي أن أفعال هذه الطائفة هي من الأفعال المحظورة التي تطالها يد القانون، وذلك كي يستطيع مكافحة هذه الطائفة التي قد ينزلق أفرادها للدخول في طوائف محترفي جرائم الإنترنت، إضافة إلي احتمالية انضمامهم إلي منظمات أو أفراد غير شرفاء [5]، فهم مثل غيرهم من المجرمين الذين تنصرف أعمالهم إلي انتهاك الأنظمة واختراق الحواجز الأمنية في البيئة الإلكترونية، وهي تعد أعمالاً خطيرة من الناحية العملية، بل إن أفعالهم لا تقف عند حدود دولة وإنما تتعدي الحواجز الجغرافية، وللتدليل علي خطورة أفعال هذه الفئة نذكر علي سبيل المثال تلاميذ المدرسة الثانوية في ولاية مانهاتن الأمريكية الذين استخدموا في عام

---

[1] سامي الشوا، محمد. مصدر سابق. ص ٣٦.
[2] عبد القادر المومني، نهلا. مصدر سابق. ص ص ٨١–٨٢.
[3] عرب، يونس (٢٠٠٢). دليل أمن المعلومات والخصوصية: جرائم الكمبيوتر والإنترنت. مج.١. ط.١.– بيروت: اتحاد المصارف العربية. ص ٢٨٦.
[4] أحمد عبابنة، محمود. مصدر سابق. ص ص ٤١–٤٢.
[5] يوسف، صغير. مصدر سابق. ص ٢٧.

١٩٨٠ غرف الدروس للدخول إلي شبكة اتصالات ودمروا ملفات زبائن الشركة في هذه العملية [١].

ويتفق الباحث مع ما ذهب إليه أنصار الاتجاه الأخير في أن أفعال المنتسبين لطائفة القراصنة الهواة تعد أفعالاً إجرامية لابد من محاسبة مرتكبيها، بيد أنه ينبغي أن ننظر بعين الاعتبار إلي أن غالبية هؤلاء الهواة من الطلبة حديثي السن، وهو ما يتطلب معاملتهم معاملة عقابية خاصة تهدف لإعادة إصلاحهم وتأهيلهم ليعودوا أفراداً صالحين مندمجين في مجتمعاتهم، حيث يبدو الأمر دقيقاً بوجه خاص بالنسبة إلي القضاء الجنائي بعد أن أصبح الهدف من العقوبة هو إعادة إدماج المجرم في المجتمع، وهو أمر يتطلب من القاضي القدرة علي فحص شخصيته من جميع الزوايا النفسية والاجتماعية والعضوية، ومناقشة تقارير الخبراء في هذا الشأن [٢]. لذا نري أن عقوبة الغرامة هي الملائمة لهذه النوعية من الجرائم بدلاً من عقوبة الحبس، بحسبان أن هناك مخاوف جمة من احتضان أعضاء منظمات الجريمة المنظمة لهذه الفئة إبان تواجدهم في السجون للإستفادة من مهاراتهم وتطويرها من أجل تحقيق مآربهم وغاياتهم الإجرامية من خلال التقنيات الرقمية، حيث إن هذه الفئة تكون أكثر تقبلاً لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها [٣].

٢) القراصنة المحترفون – Crackers:

يطلق علي هذه الطائفة مصطلح الكراكرز (Crackers) [٤] الذي ينصرف مدلوله إلي الشخص المقتحم الخبير في مجال المعلومات واستخدام

---

[١] عبد القادر المومني، نهلا. مصدر سابق. ص ٨٢.

[٢] فتحي سرور، أحمد (١٩٧٧). الشرعية والإجراءات الجنائية. القاهرة: دار النهضة العربية. ص ١٨٢.

[٣] بيومي حجازي، عبد الفتاح (٢٠٠٢). الأحداث والإنترنت. ط.١.– الإسكندرية: دار الفكر الجامعي. ص ٥٦.

[٤] لقد برز هذا المصطلح مع العام ١٩٨٥ أثناء محادثات كامب ديفيد الثانية بين الفلسطينيين والإسرائيليين (الجولة الرابعة) برعاية الولايات المتحدة الأمريكية، حيث حدث اختراق لنظام توزيع البريد الإلكتروني للصور التابعة لوزارة الخارجية الأمريكية، فقد أرسل القراصنة فيروساً جديداً غير معروف إلي مجموعة من الموظفين والصحفيين ترتب عليه عدم إمكانية تحميل صور الرؤساء المجتمعين، وكانت الرسائل مرسلة إلي عنوان وزارة الخارجية / مكتب الدبلوماسية العامة gov.state.pd تحمل عنوان نكت ضاحكة Jokes Funny، وبمجرد فتح الرسالة يبدأ الفيروس (غير المعروف) في تدمير القرص الصلب، ثم يرسل تلقائياً إلي كل عنوان بريدي موجود في الجهاز. وجدير بالذكر أن أول من اكتشف هذا الفيروس= =هو السيد/ موفق حرب مراسل جريدة الحياة اللندنية، وقد اعترفت وزارة الخارجية الأمريكية بوجود هذا الفيروس فيما بعد (عبد الحميد نبيه، نسرين. مصدر سابق. ص ١٩–٢٠).

الحاسب الآلي ويعتمد عمله علي كسر الحماية الموجودة حول الشبكات وأجهزة الحاسب الآلي. ولذلك فإن الكراكرز يستطيعون اختراق الشبكات واقتحام البرامج [١]، حيث يتميزون بالذكاء، وسعة الخبرة، والتخصص العالي في مجال الحاسب الآلي، والإدراك الواسع للمهارات التقنية، وأغلبهم من الشباب الذين تتراوح أعمارهم ما بين خمسة وعشرين وأربعين عاماً ممن يعملون في منشآت تستخدم الحاسب الآلي باستمرارية، وهم بحكم وظيفتهم يتصلون بالحاسب الآلي اتصالاً وثيقاً، الأمر الذي يجعلهم يطلعون باستمرار علي محتويات الحاسب وأسرار العمل [٢]، وهو ما حدا بالبعض للقول: "بأنهم من المتخصصين في مجال المعالجة الآلية للمعلومات" [٣].

كذلك يتميز أفراد هذه الطائفة بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها. لذا تعكس اعتداءاتهم ميولاً إجرامية خطيرة تنبيء عنها رغباتهم في إحداث التخريب لتحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب مثل هذه الجرائم، كما تهدف اعتداءات بعضهم إلي تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية [٤]، حيث

---

[١] فتحي أحمد عبد الكريم، مني. مصدر سابق. ص ٢٦.

[٢] أحمد عبابنة، محمود. مصدر سابق. ص ٤٢-٤٣.

[٣] عبد الباقي الصغير، جميل (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة: الجرائم الناشئة عن استخدام الحاسب الآلي. مج.١. ط.١.- القاهرة: دار النهضة العربية. ص ١٥.

[٤] محمود مصطفي، أحمد. مصدر سابق. ص ٢١-٢٢.=

=ويعد كيفين ميتنيك Kevin Mitnick الأكثر شهرة على الإطلاق في طائفة الكراكرز وبلا شك الأكثر موهبة في التاريخ، حيث قام علي مدار عشرين عاماً بارتكاب عدد كبير من الجرائم الإلكترونية، حيث كان بإمكانه الدخول إلي أي نظام معلوماتي مرتبط بأجهزة الحاسب الآلي وتعلم كيفية كسر كلمة المرور بسلاسة فائقة، وأتيحت له بذلك فرصة التبحر في مجال المعلومات والبيانات ليستولي علي كل ما يريد، وكذلك يدمر ما يشاء بالإضافة إلي قدرته علي زرع أي نوع من الفيروسات بدءً من الفيروسات الخفيفة التي لا يترتب عليها سوي إزعاج الحاسب الآلي والمستخدمين، وانتهاءً بالفيروسات الشديدة التي قد تنسف قاعدة البيانات وتدمر شبكة الاتصالات (دكتورة / مني فتحي أحمد عبد الكريم، مرجع سابق، ص ٢٦). فقد كتب ميتنيك اسمه في التاريخ عام ١٩٨١ عندما كان في السابعة عشرة من عمره بعدما تمكن من الدخول على شبكات الهاتف والتحكم فيها، الأمر الذي مكنه من تحويل مكالمات المشتركين إلى أي اتجاه أراد. وفي عام ١٩٨٣ أنجز ميتنيك عمله الأكبر الذي وصف بأنه أول ثورة في تاريخ الكراكرز عندما كان ميتنيك طالباً في جامعة جنوب كاليفورنيا. وباستخدام أحد الحواسيب الموجودة في الجامعة وكانت من نوع TRS-80المزودة بمعالج Zilog 1.77 MHz قام ميتنيك بالدخول على شبكة الـ ARPANet وهي الشبكة الأم للإنترنت وكانت في حينها تستخدم فقط من قبل الجيش والشركات الكبرى والجامعات. وباختراق هذه الشبكة، تمكن ميتنيك من الدخول على أكثر الحواسيب حماية في هذا الوقت، حواسب وزارة الدفاع الأمريكية (البنتاجون). تمكن ميتنيك من الاطلاع على ملفات وزارة الدفاع الأمريكية ولكن لم يوجد أي= =دليل على سوء استخدام البيانات أو محاولة سرقتها. كان ميتنيك فقط يتبع فضوله ويختبر قدراته. تم اكتشاف الاختراق من قبل أحد مديري نظام الحاسب ونشر الإنذار وفتح التحقيق في الموضوع وألقي

تدل الاعتداءات التي يقترفها أفرادها علي جانب كبير من الخطورة الإجرامية التي قد تصل لإلحاق أضراراً كبيرة بالمؤسسات المعنية بعكس طائفة الهواة (Hackers). وعادة ما يعود المجرم المحترف بالجريمة عبر الإنترنت إلي ارتكاب الجريمة مرة أخري، حيث تزداد سوابقه القضائية وهو يعيش لسنوات طويلة من عائد جرائمه، وهذا المجرم لا يفضل عادة الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح الشخصية [١]، فهو يسهدف من وراء نشاطه الإجرامي تحقيق أقصي ربح مادي بطريق غير مشروع [٢]. ويعمل المنتمون إلي هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق علي أفعالهم وصف الجريمة المنظمة، أو علي الأقل يشترك في النشاط الإجرامي أكثر من فاعل، ومن ثم يقترب مجرم هذه الطائفة في سماته من المجرم التقليدي [٣].

وتوضح الدراسات التي أجراها معهد (Stanford Research) أن محترفي جرائم الإنترنت من الجيل الحديث هم غالباً من الشباب الذين تتراوح أعمارهم من ٢٥ إلي ٤٥ سنة، وتبين الإحصاءات في هذا المجال ما يلي: [٤]

- أن ٢٥٪ من أفعال الغش المعلوماتي قام بها المحللون.

- أن ١٨٪ من هذه الجرائم قام بها المبرمجون.

- أن ١٧٪ منها قام بها المستخدمون الذين لديهم أفكار خاصة بنظام المعلومات.

- أن ١٦٪ منها قام بها الصرافون.

القبض على ميتنيك في حرم الجامعة. بدأت محاكمة ميتنيك وكانت أول مرة يقضي فيها عقوبة حقيقية بتهمة الدخول على نظام حاسب بطريقة غير مشروعة. حكم على ميتنيك حينها بالسجن لمدة ستة أشهر في سجن للإحداث. ثم حكم عليه بالسجن لخمس سنوات في التسعينيات لاختراقه الحاسب الخاص بأحد منافسيه شيمومورا بتقنية لم تكن معروفة في هذا الوقت وكانت تسمى IP Spoofing وتعتمد هذه التقنية على استخدام IP مزيف لتفادي الانكشاف خلال الهجوم على احد الأهداف. وهو الآن مستشار أمني ويدير شركته الخاصة ميتنيك للحماية Mitnick Security.

– https://ar-ar.facebook.com/notes, 15/1/2020.

[١] عبد القادر المومني، نهلا. مصدر سابق. ص ٨٤.

[٢] رسلان، أيمن، عبد العال الديربي ومحمد إسماعيل. مصدر سابق. ص ٦٢.

[٣] عادل قورة، نائلة. مصدر سابق. ص ٦٢.

[٤] سامي الشوا، محمد. مصدر سابق. ص ص ٤٢–٤٣.

– أن ١٢٪ منها قام بها الأشخاص الأجانب عن المكان الذي تتواجد فيه نظم المعلومات.

– أن ١١٪ منها قام بها المشغلون (فنيو التشغيل).

ومن الملاحظ حالياً أنه قد بدأت في الظهور منظمات لمحترفي ارتكاب جرائم الإنترنت، هذه المنظمات صعدت من حدة الهجمات التي تقوم بها علي مواقع الإنترنت الحكومية؛ من ذلك موقع شركة (MBCE) المتخصصة في الأعمال الهندسية والاستشارية الذي تعرض لعدة هجمات من مجموعة من المحترفين، يعتقد أنهم موجودون في البرازيل، وكان موقع الشركة علي الإنترنت (Com. Sawww Mbs). وقد غير المحترفون الصفحة الرئيسية للموقع، وظهرت فيه رسالة مكتوبة باللغة البرتغالية تعلن عن إنشاء ما يسمي بفريق النخبة (Elite Team). ووصفت المجموعة نفسها بأنها مجموعة جديدة لعصر جديد. كما سخرت الرسالة من مدير الموقع لعدم قدرته علي حماية مزودات الموقع وتفاخرت الرسالة بقدرات ومهارات أعضاء الفريق، وتضمنت الرسالة مقولة "من كانت لديه المعرفة يجب أن يكون قادراً، ومن كانت لديه سلطة فهو يمتلك زمامها" [١].

تمييز طائفتي الهاكرز والكراكرز:

يستدعي بحث معايير تمييز طائفتي الهاكرز والكراكرز التطرق إلي نظرة القضاء المقارن الأمريكي لمعيار الهكترة Standard of Hectares (أو المهارة الخاصة) من ناحية، ومن ناحية أخري التعرض لتفسير مصطلح هاكر.

فمن ناحية فإن القضاء الأمريكي اعتمد معيار الهكترة بكونه تعبير عن المهارة الخاصة Special Skill، حيث أورد القاضي الأمريكي Kleined تعريفاً للمستوي المهاري الخاص بأنه "المستوي المهاري الذي لا يمكن التوصل إليه من قبل جمهور العامة، وعادة يتطلب تعليم إضافي مع التدريب أو الحصول علي ترخيص، ويمكن التمثيل لذلك بالطيارين والمحامين والأطباء والمحاسبين والصيادلة وكذلك خبراء الجريمة". فالهكترة

[١] أحمد عبابنة، محمود. مصدر سابق. ص ٤٤.

إذن هي مستوي مهاري خاص يتمتع به الهكرة، وهو مستوي يفيد في دلالته التعبير عن الكفاءة والصلاحية والأهلية التقنية التي يتمتع بها الهاكر، حيث يملك الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الافتراضي لا يستطيع مباشرتها العامة من الناس حتي ولو كانوا يملكون خصيصة التعامل الحاسوبي [١].

ولقد كان أول بروز للمعيار القضائي (المهارة الخاصة) في قضية الولايات المتحدة الأمريكية ضد بيترسين أمام القضاء الفيدرالي، حيث أدين Justin Tanner Petersen وفقاً للقسم 18 usc sec. 1030 (2) (a) لقيامه بالهكترة لكونه – نتيجة لتمتعه بمهارات خاصة في التعامل مع الحوسبة والرقمية – مارس نشاطاً تقنياً عالي المستوي تمثل في قيامه بممارسة النصب المعلوماتي باختراقه لنظم حاسب مؤسسة كروت الإئتمان National Credit Card Reporting Agency، واختلاس بيانات شخصية عن المتعاملين بها واستغلال هذه البيانات في الحصول علي كروت إئتمان، كما أنه اخترق حاسب شركة الهاتف وتحكم في خطوط الهاتف المتصلة بالراديو Radio Station، وقام بتنظيم حصوله علي جائزة تتكون من عدد اثنين سيارة Porsche قيمة كل واحدة ٤٠.٠٠٠ $ وكذلك رحلتان إلي جزر هاواي، ثم اخترق حاسب مؤسسة الاقتراض التجارية الوطنية The National Commercial Lender's Computer وحصل لنفسه علي ١٥٠.٠٠٠ $ مودعاً إياها في بنوك عدة. ولقد جاء في حيثيات حكم الدائرة التاسعة أن "بيترسين يملك معرفة ومهارة غير عادية في كيفية عمل الحواسيب وكيف يتم تخزين البيانات والحركة الاسترادادية للمعلومة وكيف يمكن التحكم في النظام الأمني للحواسيب أو تجنب التعامل معه" [٢].

ولقد كانت أحد أهم القضايا التي ناقشت معيار المهارة الخاصة الذي يميز الهكرة عن غيرهم هي قضية الولايات المتحدة الأمريكية ضد Lee، حيث ذهب القاضي Andrew j. Kleinfeld – وهو أحد كبار القضاة في محكمة الاستئناف في الولايات المتحدة (الدائرة التاسعة) [٣] – إلي ضرورة

---

[١] عبد الحميد نبيه، نسرين. مصدر سابق. ص ١٦.

[٢] عبيد الكعبي، محمد (٢٠١٠). الحماية الجنائية للتجارة الإلكترونية. القاهرة: دار النهضة العربية. هامشي ص ص ٢٣٧/ بند ٢–٢٣٨.

[3] https://ar.wikipedia.org/wiki. 4/1/2020.

الاستناد إلي الكفاءة في تمييز المهارة الخاصة والهكترة وبالتالي الهكرة، وذلك وفقاً للمعرفة غير العادية Extraordinary Knowledge، فالهاكر يتمتع بمستوي مهاري خاص يمكنه من القيام بممارسة أنشطة خطرة حقاً مثل الاختراق والتعامل الحوسبي والرقمي بطريقة لا يمكن للعامة القيام بها، فلكي يمكن مباشرة الهكترة فإن ذلك يحتاج من الهاكر أن يلم بهذا المستوي المهاري الخاص. لذلك لا يمكن تسوية الهكترة بالعدوان علي موقع ونسخه (قضية لي) وكذلك التزييف والتزوير عبر المجتمع المعلوماتي والعالم الافتراضي [1].

ومن ناحية أخري لم يتوقف مصطلح هاكر عن التطور، ولقد أخذ التطور المذكور صيغة تقليص تفسير مصطلح الهاكر والهكترة، وبحيث اتخذ كلاهما طابعاً مزدوجاً من حيث النظر إلي هذه الفكرة علي أساس المعيار الشخصي والموضوعي معاً.

[1] محمد بن يونس، عمر (٢٠٠٣). المجتمع المعلوماتي والحكومة الإلكترونية: مقدمة إلي العالم الافتراضي. القاهرة: دار النهضة العربية. ص ٢٣.=
=العالم الافتراضي أو المرئي The Virtual World، ويطلق عليه أحياناً The Second Life؛ هو المجال الحيوي للبيانات وحركتها المعلوماتية المختفي في الآلة التقنية. فهو نظام محاكاة رقمي عبر الحاسب تم صنعه ليعيش به الناس ويتفاعلوا ويمارسوا أنشطة مثل التي تحدث في الحياة الواقعية أو بافتراض أشكال فانتازية من الحياة غير موجودة بالفعل من خلال شخصيات افتراضية يصنعها الناس لأنفسهم يطلق عليها Avatars، وأول أشكال العوالم الافتراضية علي الإنترنت كانت غرفة الدردشة الجماعية chatting rooms، حيث يمكن التواصل بالكتابة وتبادل الملفات والصور بشكل محدود، ثم تعددت لاحقاً أشكال العوالم الافتراضية علي الإنترنت مثل مواقع ألعاب الفيديو الجماعية، ثم تطور الأمر لتسقط الحدود شيئاً فشيئاً بين العالم الواقعي وتلك العوالم الافتراضية فيما أطلق علية الدائرة السحرية Magic Circle. وتعد من أحدث صور العالم الافتراضي ما يعرف بالجامعة الافتراضية The Virtual University التي تقدم كافة البرامج التعليمية لدارسيها المسجلين علي موقعها الإلكتروني بطريقة التعلم عن بعد، كما تمنحهم المصادقات اللازمة علي شهادات إتمامهم للبرامج المذكورة. وجدير بالذكر أن الفقه قد درج علي تسمية جرائم المعلوماتية والإنترنت بجرائم العالم الافتراضي أو الفضاء الإلكتروني نظراً لاتساع مسرحها الذي قد يمتد ليشمل كافة أرجاء الكرة الأرضية.

المطلب الثاني
جرائم القرصنة الرقمية

لقد كانت مسائل حماية حقوق التأليف في الماضي تعني بحماية ملكية المصنفات الموثقة مادياً (مطبوعات، رسوم، تسجيلات ...)، أو الملموسة حسياً (محاضرات وخطابات وألحان مسموعة، أو مسرحيات، أو رقصات مرئية ...). أما المنتجات المعلوماتية الرقمية فهي شكل جديد من (أوعية المعرفة) لها خصوصياتها وتحتاج لمعاملة خاصة. وتتميز بتكاليفها الباهظة بالنظر إلي سهولة تداولها واستنساخها [1]. لذا عمد المشرع في غالبية النظم المقارنة إلي إسباغ الحماية القانونية علي هذا الشكل الجديد من أشكال الملكيات الرقمية (برامج الحاسب وبياناتها) من أجل المحافظة علي حقوق منتجو التكنولوجيا من إساءة استخدامها من قبل قراصنة البرمجيات، وهو ما أدي إلي ظهور نمط إجرامي جديد في أروقة هذه البيئة الرقمية أطلق عليه جرائم القرصنة الرقمية، وهو ما يدعونا إلي بيان مفهومها وأخطارها الاقتصادية علي الصعيدين الدولي والمحلي، وسبل مكافحتها للحد من هذه الأضرار علي النحو التالي:

أولاً: مفهوم جرائم القرصنة الرقمية:

تعني كلمة القرصنة السرقة أو الاختلاس أو السلب لشيء مادي مملوك للغير من أجل تملكه، وفي حالة القرصنة علي البرمجيات – علي سبيل المثال – يكون محل الجريمة هو البرامج الموجودة بجهاز الحاسب، والبرمجيات Software تعني جميع العناصر غير المادية أو غير الملموسة لتشغيل أجهزة الحاسب الآلي سواء كانت مخزنة في الحاسب أو تم طرحها عبر شبكة الإنترنت، فيقوم شخص بسرقتها وبعد سرقتها إما أن يقوم بنشرها أو تدميرها أو تحويلها، مما يؤثر بالسلب علي اقتصاد الشركات الأصلية صاحبة هذه البرمجيات [2]. لذلك أصبح من المستقر عليه في كافة النظم

---

[1] عبد الغني، فتحي (٢٠٠٦). **اقتصاديات الملكية الفكرية عبر الإنترنت**، بحث منشور ضمن أعمال المؤتمرات الخاصة بالمنظمة العربية للتنمية الإدارية: المعاملات الرقمية وقانون الإنترنت. القاهرة: المنظمة العربية للتنمية الإدارية. ص ٢٣.

[2] عبد الحميد نبيه، نسرين (٢٠١٠). القرصنة علي البرمجيات وأثر ذلك علي الاقتصاد العالمي. الإسكندرية: المكتب الجامعي الحديث. ص ص ١٢–١٣.

القانونية تمتع برمجيات الحاسب الآلي بالحماية القانونية وفقاً لقوانين حماية حقوق الملكية الفكرية والمعاهدات الدولية.

وفي رأي الباحث تعني قرصنة البرمجيات Software piracy؛ تلك العملية التي يتم فيها النسخ غير القانوني لمعلومات محمية بمقتضي قوانين حماية حقوق الملكية الفكرية والمعاهدات الدولية.

وإذا كان هذا المفهوم الموسع لبرمجيات الحاسب الآلي يقتضي منا التوسع أيضاً في نطاق هذا البحث بالتعرض تفصيلاً إلي خطوات إعدادها المشمولة أيضاً بالحماية القانونية. ولكن يبدو ملاءماً قصره علي برامج الحاسب وقواعد البيانات باعتبارهما الأكثر عرضة لجرائم القرصنة، واللتين شملتهما المادة (١٠) من اتفاقية التربس بالحماية القانونية.

١) برنامج الحاسب الآلي Computer Program:

يقتضي الوقوف علي ماهية البرنامج منا بداءة بيان مبسط لخطوات إعداده التي تتجسد في أربع خطوات نعرضها فيما يلي [١]:

الخطوة الأولي:

وضع التصميم الفني ثم كتابته علي هيئة معادلات، وتعتبر هذه الخطوة هي وضع الأساس المنطقي الكفيل بإنشاء برنامج متميز عن غيره ويمكنه أن يؤدي إلي إنجاز وتنفيذ العمليات المستهدفة من وجوده. ويطلق علي هذه المرحلة مسمي Algorithm ويتم تعريفها بأنها "مجموعة من الأوامر المحددة اللازمة لحل المشكلة من خلال عدد محدد من العمليات". ويتضح من هذه الخطوة إنقسامها إلي مرحلتين تتوجه الأولي منهما إلي تحليل الأغراض والنتائج التي يتوجه تصميم البرنامج وإعداده من أجلها، أما المرحلة الثانية فهي مرحلة وضع التصميم الفني للبرنامج وكتابته في صيغة معادلات قابلة للتنفيذ.

[١] راجع في عرض هذه الخطوات تفصيلاً: حجازي، محمد (٢٠٠٨). دليل العمل والإجراءات لإنفاذ حقوق المؤلف. القاهرة: د ن. ص ص ٢٣-٢٤.

الخطوة الثانية:

وهي المرحلة التي يتم فيها ترجمة المعادلات الرياضية إلي أوامر البرنامج، ويطلق علي البرنامج مكتوباً بهذه اللغة اسم "كود المصدر" Source Code.

الخطوة الثالثة:

هي ترجمة البرنامج إلي لغة الألة، حيث لا يتمكن جهاز الحاسب من التعرف علي أي لغة أخري غير لغة الألة Language Machine والتي تترجم كافة المصطلحات والمعادلات سالفة البيان إلي معادلات مكونة من وحدات من أرقام صفر وواحد " ٠ – ١ "، وبترجمة البرنامج إلي هذه اللغة يتمكن جهاز الحاسب من التعرف علي الأوامر التي تنتقل إليه في شكل نبضات – شحنات سلبية وإيجابية – من خلال الحروف المكونة من الأرقام ذات الشحنات الموجبة أو المتعادلة، ويطلق علي البرنامج مكتوباً بهذه اللغة "اسم كود الهدف" Object Code.

الخطوة الرابعة:

يتم تحميل البرنامج علي الوسيط المادي – الدعامة – الذي قد يكون أقراص مرنة Floppy Disk أو أسطوانات مدمجة CD أو من خلال التحميل المباشر علي الأسطوانة الصلبة Hard Disk الخاص بالجهاز كما يضاف إلي ذلك كافة الوثائق والمستندات الفنية والقانونية اللازمة لاستخدامه.

وعلي ضوء ماسبق يمكن تعريف برنامج الحاسب الآلي تقنياً بأنه مجموعة من الأوامر والإرشادات التي تحدد للحاسب العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة، هذه التعليمات تُحمل أو تُثبت علي وسيط معين يمكن قراءته عن طريق الحاسب، وحينئذ يمكن للبرنامج عن طريق معالجة البيانات أن يؤدي وظائف معينة يصل من خلالها إلي تحقيق النتائج المطلوبة منه [١].

[١] حجازي، محمد. مصدر سابق. ص ٢٤.

أما من الناحية القانونية فقد عرفت المنظمة العالمية للملكية الفكرية WIPO برنامج الحاسب بأنه "مجموعة تعليمات يمكنها إذا ما نقلت علي ركيزة تستوعبها الألة أن تشير – تؤدي – تساعد في الوصول إلي خاصية ما، أو هدف، أو نتيجة خاصة، بواسطة آلة يمكنها التعامل مع المعلومة". وقد عرف القانون الأمريكي الصادر عام ١٩٨٠ الخاص بحماية حق المؤلف البرنامج بأنه "مجموعة توجيهات أو تعليمات، يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلي نتيجة معينة". أما في فرنسا فقد صدر قراراً وزارياً في الثاني والعشرين من ديسمبر ١٩٨١ بتعريف برنامج الحاسب الآلي بأنه "مجموعة الخطوات والإجراءات – بالإضافة إلي الوثائق المتعلقة بها – التي تهدف إلي تشغيل نظام معالجة البيانات وتوظيفها وفقاً للغرض المنشود". وجدير بالملاحظة أن الفقه الفرنسي يسبغ الحماية علي البرامج وملحقاتها من الوثائق والمستندات ورخص الاستخدام [١].

بينما تبني المشرع المصري تعريفاً موسعاً لبرنامج الحاسب (البرنامج المعلوماتي) في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات [٢] حين عرفه في المادة الأولي منه بأنه "مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال. ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي". ومن ثم لم يشترط المشرع لإسباغ الحماية القانونية علي البرنامج المعلوماتي أن تكون الأوامر والتعليمات المكونة له مكتوبة بلغة الآلة وإنما بأية لغة أو رمز أو إشارة علي النحو الوارد في تعداد هذه المادة وبالجملة إذا اتخذت أي شكل من الأشكال.

وجدير بالملاحظة أنه يجب عدم الخلط بين برنامج الحاسب ذاته باعتباره مصنفاً محمياً وفقاً للقواعد القانونية وبين الوسيط المادي وهو الدعامة أو الوعاء الذي خُزن أو حُمل أو ثُبت فيه البرنامج سواء كان هذا

[١] حجازي، محمد. مصدر سابق. ص ٢٥.
[٢] مصر. قانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات. السنة ٦١. (الجريدة الرسمية: العدد ٣٢ مكرر. تاريخ ٢٠١٨/٨/١٤). (ج). ص ٣ وما بعدها.

الوعاء ورقي أو قرص مرن Floppy Disk ، أو قرص مضغوط CD ، أو شريط ممغنط Magnetic Tape أو أية وسيلة أخري قد يتم التوصل إليها مستقبلاً. ولئن كان الوسيط أو الدعامة أو غير ذلك مما يفرغ فيه المصنف لتثبيته، هو شرط لازم لتقرير الحماية القانونية للمصنف، إلا أن هذه الحماية لا يقررها القانون ولا ينزل مقتضاها إلا علي البرنامج ذاته (المصنف)، دون الوسيط أو الدعامة التي أفرغ فيها وثُبت عليها البرنامج [١].

٢) قواعد البيانات:

يمكن تعريف قواعد البيانات بأنها تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز ويكون مخزناً بواسطة الحاسب ويمكن استرجاعه بواسطته أيضاً، أو هي تنظيم وترتيب للبيانات في صورة مناسبة للاستخدام والبحث بسرعة وكفاءة مع قدرة علي استنباط العلاقات البينية بصورة تفوق أساليب التعامل اليدوية [٢].

ويتطلب بناء قواعد البيانات [٣]:

- تجميع ضخم للبيانات قد يستمر عبر عدة سنوات.
- تحليل عميق للوصول إلي الأسلوب الأمثل للتنظيم والترتيب.
- بناء لعلاقات وقواعد تنظم عمليات البحث والاسترجاع.

عمليات معقدة لتقليل أزمنة البحث والوصول إلي المعارف المطلوبة.

- تكلفة ضخمة ومرتبطة بإدخال ومراجعة البيانات لضمان الدقة.

ومناط حماية قواعد البيانات – بوجه عام – هو الابتكار كما عبرت عنه المادة (٢/١٠) من اتفاقية التربس، حيث أسبغت الحماية

---

[١] حجازي، محمد. مرجع سابق، ص ٢٦.

[٢] حجازي، محمد (٢٠٠٨). حقوق المؤلف وحماية البرمجيات وقواعد البيانات. القاهرة: د ن. ص ١٥.

[٣] المصدر السابق. ص ١٦.

القانونية علي البيانات المجمعة إذا كانت تشكل خلقاً فكرياً نتيجة ترتيب محتواها.

وبناءً علي ذلك، فإن البيانات أو المعلومات المُخزنة بشكل مجرد في نظم الحواسيب ليست محل حماية مثل: القوانين وأحكام المحاكم، لكنها متي ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معينة ومتي ما خضعت لعمليات معالجة تتيح ذلك، فإنها تتحول من مجرد بيانات إلي قاعدة بيانات وينطوي إنجازها بهذا الوصف علي جهد ابتكاري وإبداعي يستوجب الحماية [١].

وقد عرف المشرع المصري قواعد البيانات (البيانات والمعلومات الإلكترونية) في المادة الأولي من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات بأنها "كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها". وبذلك يكون المشرع قد استوجب عامل الابتكار لإسباغ الحماية القانونية علي البيانات المجمعة أياً كانت وسيلة تجميعها وسواءً كانت عن طريق الإنشاء أو التخزين أو المعالجة أو التخليق أو النقل أو المشاركة أو النسخ علي النحو الوارد تعداده في هذه المادة.

أنواع القرصنة الرقمية:

أشارت دراسة قامت بها جمعية منتجي برامج الحاسب التجارية إلي وجود خمسة أنواع للقرصنة الرقمية وهي [٢]:

النوع الأول/ قرصنة المستخدم النهائي End User Piracy:

تحدث عندما يقوم أحد موظفي الشركة أو أي مستخدم نهائي بنسخ نسخة من البرنامج بدون الحصول علي إذن أو ترخيص، وقد يحدث هذا النوع بواسطة أخذ نسخة واحدة وتنصيب البرنامج علي أكثر من جهاز حاسب، أو نسخ الأقراص لغرضي التنصيب أو التوزيع، أو الاستغلال غير

[١] حجازي، محمد. دليل العمل والإجراءات لإنفاذ حقوق المؤلف. مصدر سابق. ص ص ٢٦-٢٧.
[٢] عبد الحميد نبيه، نسرين. القرصنة علي البرمجيات. مصدر سابق. ص ص ١٢-١٣.

القانوني لقرص ترقية البرنامج بدون الحصول علي النسخة الأصلية لذلك الإصدار من البرنامج، أو تبادل الأقراص داخل أو خارج مكان العمل.

النوع الثاني/ الاستعمال المفرط للبرنامج من قبل المستخدمين:

يحدث هذا النوع من القرصنة عندما يستخدم عدد كبير من المستخدمين من خلال الشبكة نسخة مركزية للبرنامج في الوقت ذاته، فإذا كان الموظفون يعملون ضمن شبكة مجلة وتقوم بتنصيب البرنامج علي الخادم وذلك لكي تستطيع جميع الشاشات الطرفية الوصول إلي البرنامج، ففي هذه الحالة يجب أن يتم الحصول علي ترخيص بذلك إذا كان عدد المستخدمين مجاوزاً لما هو منصوصاً عليه في الرخصة.

النوع الثالث/ قرصنة الإنترنت:

يحدث هذا عندما يحمل برنامج من الإنترنت في حين أن القاعدة العامة يجب أن تطبق في شراء تلك البرامج عن طريق online مثل عمليات الشراء التقليدية، والقرصنة عبر الإنترنت يمكن أن تأخذ إحدي الطريقتين التاليتين:

الطريقة الأولي: هي طريقة قرصنة ومهاجمة موقع كامل وبذلك يصبح تحميل البرامج مجاناً منها، والطريقة الثانية: هي طريقة إرسال البرامج غير القانونية التي لا تحمل رخصة بها عبر شبكة peer-to-peer [1].

النوع الرابع/ تحميل الهارد ديسك:

يحدث هذا النوع من أنواع القرصنة غالباً في أماكن بيع الأجهزة وذلك عندما تقوم محلات بيع أجهزة الحاسب بعمل نسخ من البرامج وجعل

[1] وتعني عبارة (Peer–to–Peer): الند للند أو القرين للقرين أو النظير للنظير؛ وهي عملية تبادل الملفات والبيانات بين جهازين شخصيين على شبكة الانترنت، ويستخدم هذا البروتوكول بكثرة في برامج مشاركة الملفات وتقاسمها. وتعتمد شبكات الند لند على حواسب المستخدمين وسرعتهم، فكل فرد في شبكة الند لند يساهم أولاً بالملفات وثانياً بالسرعة، حيث تربط شبكات الند لند الأطراف بعضهم البعض وتتم مشاركة الملفات. فعلي سبيل المثال في حالة تحميل لملف من شبكة Donkey network يتم تحميل البرنامج المخصص لذلك (edonkey2000 أو emule أو mldonkey)، وبعدها يمكن البحث عن الملف الذي نريده، فيقوم البرنامج بالبحث عن الكلمة في الملفات المشاركة من قبل المستخدمين، وعند اختيار تحميل الملف سيقوم البرنامج بتحديد الأطراف الذين يملكون هذا الملف ويبدأ تحميله منهم.
- https://ar.wikipedia.org/wiki. 6/1/2020.

هذه النسخة في أجهزة الحاسب التي تقوم ببيعها للمستخدمين، ويؤدي ذلك إلي زيادة كفاءة عملية الشراء من خلال تحفيز المشتري الذي يجد نسخ البرامج التي يحتاجها علي جهاز الحاسب الذي يريد شراءه.

النوع الخامس/ إعادة انتاج وتقليد البرامج:

يحدث هذا النوع عن طريق تزييف وإنتاج برامج تشبه البرامج الأصلية ويتم ذلك بشكل غير قانوني، في حين يتم بيع هذه البرامج علي أنها برامج قانونية، إلا أنه يمكن كشف هذا النوع من القرصنة عن طريق دليل المستخدم الخاص بالبرنامج ورخصة الاستعمال.

ثانياً: الآثار الاقتصادية لجرائم القرصنة الرقمية:

نعرض فيما يلي للآثار الاقتصادية التي انتجتها جرائم القرصنة الرقمية علي الصعيدين الدولي والمحلي:

١) علي الصعيد الدولي:

تشير نتائج التقرير السنوي للعام ٢٠٠١ أن قرصنة البرمجيات لا تزال تشكل تحدياً لصناعة البرمجيات، وللمرة الأولي خلال تاريخ هذه الدراسة فقد استمر ارتفاع المعدل العالمي للقرصنة لسنتين متتاليتين ٢٠٠٠ و ٢٠٠١، في العام ٢٠٠١ بلغ معدل القرصنة ٤٠٪ مرتفعاً بذلك عن العام ٢٠٠ بينما كان العام ١٩٩٩ الأصغر بنسبة القرصنة التي بلغت ٣٦٪.

وتعد أكثر المناطق في العالم قرصنة للبرمجيات، منطقة أسيا / المحيط الهادي التي تتميز بمعدل قرصنة مرتفع، فقد شهدت خلال العام ٢٠٠١ أكبر نمو في معدل القرصنة بالصين التي لا تشهد ركوداً اقتصادياً، كما أظهرت الدراسات أن أكبر معدل للقرصنة في فيتنام بمعدل ٩٤٪، أما لبنان وقطر بالمرتبة السادسة بمعدل ٧٩٪.

وتقدر حجم الخسائر اليومية التي تسببها عمليات القرصنة علي برامج الحاسب نحو ٤١.٦ مليون دولار، مما جعل الخبراء يطلقوا رسائل التحذير من مخاطر هذه العمليات التي تهدد الشركات العاملة في مجال

الحاسب والإنترنت بالتوقف عن نشاطها [١]. وتقدر الخسائر السنوية بين ٥١ و٧١ بليون دولار أمريكي تتحملها الصناعة بسبب خرق نظام الحقوق الفكرية، وقد قدرت رابطة ناشطي البرامج أن برامج بقيمة ٤.٧ بليون دولار أمريكي قد تم نسخها بشكل غير مشروع عام ١٩٩٣، منها بليونا دولار أمريكي تم الاستيلاء عليها من شبكة الإنترنت [٢].

وقد أكد السيد/ ديفيد لامى – وزير الدولة السابق لشؤون الملكية الفكرية فى المملكة المتحدة – أن الجرائم الماسة بأمن المعلومات مسألة عالمية خطيرة، تسبب خسائر بالبلايين من الجنيهات الاسترلينى– منها ٩٠٠٠ مليون جنيه استرلينى تخص الانتهاكات التى تقع على حقوق الملكية الفكرية [3]. ويشير السيد/ جيمس ب. دوناهو – قاضي تحقيق المنطقة الغربية في واشنطن بالولايات المتحدة الأمريكية – إلي أنه وصلت نسبة قرصنة البرمجيات في عام ٢٠١١ إلى ٦١٪، بقيمة تجارية تعادل ١٧٢ مليون دولار. ووفقاً لما توصلت إليه إحدى الدراسات التي نشرت في عام ٢٠١٠، قد يساهم الحد من قرصنة برمجيات الحاسب الشخصي بنسبة ١٠٪ على مدى أربع سنوات في زيادة الناتج المحلي الإجمالي بنحو ٢٥٤ مليون دولار، وزيادة الإيرادات الضريبية بنحو ٣٣ مليون دولار وتوفير ١٩٧٨ فرصة عمل جديدة في مجال تكنولوجيا المعلومات [٤].

وفي دراسة قام بها الاتحاد العالمى لمنتجى البرمجيات التجارية Business Software Alliance (BSA) حول حجم الخسائر التي تتعرض لها شركات تطوير البرمجيات حول العالم بسبب عمليات القرصنة على برامجها، وجد أن شركات البرمجة تعرضت لخسائر فادحة في عام ٢٠٠٩ بزيادة بنسبة ٢ % عن عام ٢٠٠٨. أوضحت الدراسة أن مجموع الخسائر حول العالم بلغ ٥٠.٤ مليار دولار أمريكى. كما أشارت إلى أن عام ٢٠٠٩

---

[١] عبد الحميد نبيه، نسرين. القرصنة علي البرمجيات. مصدر سابق. ص ٣٤ وما بعدها.

[٢] عبيد الكعبي، محمد. الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. مصدر سابق. ص ص ٥١–٥٢.

[3] محمد شكرى، عمرو. "نطاق حماية الحقوق الاستئثارية الرقمية على شبكة الانترنت ودور مقدم الخدمة فى إنفاذ القانون". ورقة بحثية قدمت في **ورشة عمل حول الملكية الفكرية: حق المؤلف**. القاهرة: ١٦–١٧ نوفمبر. ٢٠١٦. ص ٣.

[٤] ب. دوناهو، جيمس. "حق المؤلف" ورقة بحثية قدمت في **ورشة عمل حول الملكية الفكرية: حق المؤلف**. القاهرة: ١٦–١٧ نوفمبر. ٢٠١٦. ص ٦.

شهد زيادة فى معدلات استخدام البرمجيات المسروقة «التى تعرضت للقرصنة» فكانت ٤٣% من البرمجيات المتوافرة على أجهزة الحاسب حول العالم «مقرصنة»، بالمقارنة بنسبة ٤١ % فى عام ٢٠٠٨.

كما أوضحت الدراسة أن منطقة آسيا والباسيفيكى هى أكبر المناطق التى تنشط فيها عمليات القرصنة وبلغت حصتها من مجموع الخسائر نحو ١٦.٥ مليون دولار أمريكى، فنسبة تواجد البرامج «المقرصنة» فى هذه المنطقة بلغت ٥٩%، بما يعادل ٩٠٠ مليون جهاز حاسب تعمل ببرامج مسروقة. وجاءت كل من البرازيل والصين والهند كأكثر الدول التى تشهد أراضيها عمليات قرصنة منظمة، فيما جاءت جورجيا – الجمهورية السوفيتية السابقة – كأكثر الدول فى العالم اعتماداً على البرمجيات المقرصنة، فنحو ٩٥% من الأجهزة المتوافرة فيها تعمل ببرامج مسروقة غير قانونية. وجاءت بعدها دول زيمبابوى وبنجلاديش ومولودوفا وأرمينيا واليمن، فيما حققت الولايات المتحدة أقل معدل استخدام للبرامج المسروقة بنسبة ٢٠% فقط، ثم جاءت بعدها كل من لوكسمبورج ونيوزيلندا وأستراليا [1].

٢) علي الصعيد المحلي:

كشف تقرير لاتحاد منتجي برامج الحاسب المصري صدر في عام ٢٠٠٨ عن ارتفاع معدلات القرصنة علي البرامج من جانب شركات القطاع الخاص المتوسطة والصغيرة. وأشار إلي أن معدل القرصنة علي البرامج في مصر يصل إلي ٦٧٪ من إجمالي المبيعات، كما أن حجم خسائر صناعة البرمجيات الوطنية والخزانة العامة يصل إلي ٤٦٤ مليون دولار سنوياً منها ٣٨١ مليون دولار خسائر الشركات المنتجة و ٨٣ مليون دولار خسائر الخزانة العامة بسبب الفاقد في حصيلة الضرائب المتوقعة علي نشاط القرصنة في مجال البرمجيات.

وأكد التقرير معاناة صناعة البرمجيات في مصر بشدة بسبب ارتفاع حجم ظاهرة نسخ البرامج بطرق غير مشروعة بالإضافة إلي التأثيرات السلبية لانتشار ظاهرة القرصنة علي البرامج وما يترتب عليه من ضياع فرص المبيعات وزيادة الفاقد في الإنتاج الرسمي للبرمجيات.

[1] https://gss.bsa.org, 2/4/2020.

وقدر التقرير نسبة اختراق الحاسب الآلي لقطاع البرمجيات في القاهرة بحوالي ٣٨٪ من إجمالي النشاط مما أدي إلي تقسيم الشركات والجهات إلي ٣ فئات وفقاً لعدد أجهزة الحاسب في كل منها، مشيراً إلي أن متوسط عدد الأجهزة بالفئة الأولي من الشركات حوالي ٥٥ جهاز حاسب آلي ويصل عددها إلي ٥ آلاف شركة والفئة الثانية ١١ ألف شركة بكل منها ٩ أجهزة في المتوسط والثالثة تضم ٣٤ ألف شركة ويبلغ متوسط عدد الأجهزة بها ما بين ٣ إلي ٤ أجهزة فقط، وأوضح أن نسبة القرصنة في الفئة الأولي من هذه الشركات تصل إلي ٥٣٪ بينما تصل إلي ٧٤٪ في الفئة الثانية و ٦٨٪ في شركات الفئة الثالثة [١].

ثالثاً: سبل مكافحة جرائم القرصنة الرقمية:

هناك طريقتان رئيسيتان لحماية الملكية الفكرية الرقمية:

الطريقة الأولي/ الحماية التقنية – الفيزيائية:

وهي السائدة في أوروبا ودول العالم الثالث، وتعتمد علي وضع عقبات تقنية تمنع أو تعيق إساءة الاستخدام لبرامج الحاسب أو قواعد البيانات، مثل الحماية من خلال مفاتيح إلكترونية أو كلمات سر ... الخ [٢]. وقد تكون المعطيات أحياناً أكثر أهمية من البرنامج ولابد من حمايتها ضد النسخ أو السرقة، وبالتالي يمكن القول بأن الحماية تهتم بعاملين أساسيين: حماية المعطيات الهامة وحماية البرنامج وقواعد البيانات بحسب الأحوال، وفيما يلي نعرض لأهم طرق الحماية التقنية [٣].

١) رقم القرص الصلب:

يقوم المبرمج بتخزين رقم القرص الصلب للحاسب الذي سيعمل عليه البرنامج، وعند تشغيل البرنامج علي أي حاسب يقوم بقراءة رقم القرص الصلب، فإذا كان الرقم مطابقاً للرقم المخزن في البرنامج فإن البرنامج يتابع عمله، أما إذا كان غير مطابق فهذا يعني أن الحاسب غير مصرح له

[١] عبد الحميد نبيه، نسرين. القرصنة علي البرمجيات. مصدر سابق. ص ٣٨.
[٢] عبد الغني، فتحي. مصدر سابق. ص ٢٤.
[٣] عبد الحميد نبيه، نسرين. القرصنة علي البرمجيات. مصدر سابق. ص ٣٥ وما بعدها.

باستخدام البرنامج، وتظهر رسالة تطلب من المستخدم الاتصال بالمبرمج للحصول علي نسخة شرعية.

٢) استخدام قرص مرن:

يقوم المبرمج بربط برنامجه بقرص مرن معين حيث لا يعمل البرنامج دون وجود هذا القرص.

٣) مفتاح الحماية ذو الذاكرة – Memory Protection Key:

يقوم المبرمج بربط برنامجه بقطعة إلكترونية دونكل [١] يتم وصل هذه القطعة بالحاسب من خلال أحد منافذ الاتصال التالية: (COM– LPT– USB)، حيث يقرأ البرنامج معلومات معينة ثابتة موجودة داخل الدونكل، فإذا كانت المعلومات صحيحة فإن ذلك يعني أن الدونكل موجود وأن الحاسب مصرح له باستخدام البرنامج.

٤) مفتاح الحماية ذو خوارزميات التشفير:

تعتبر هذه الطريقة أفضل طريقة لحماية البرنامج لكون المفتاح يعتمد علي خوارزميات تشفير لا يمكن محاكاتها، حيث يرسل البرنامج إلي مفتاح الحماية سلسلة من المحارف فيقوم المفتاح بتشفيرها (وفق المعاملات الخاصة لخوارزمية التشفير المخزنة في المفتاح) ويعيد الجواب إلي البرنامج. وتنبع قوة هذه الطريقة من اعتمادها علي خوارزميات تشفير قوية وكون السلسلة شبه العشوائية لها طويلة جداً. ويمتاز هذا المفتاح عن المفتاح ذو الذاكرة بأن عدد الحالات المختلفة للمعطيات القادمة من المفتاح يكون محدوداً (مهما كبر)، أما في حالة التشفير فيكون عدد الحالات غير محدود (نظرياً)، إذ بإمكاننا زيادة هذا العدد كما نريد وذلك بزيادة سلاسل المحارف المختلفة المرسلة إلي المفتاح لتشفيرها. ومن الممكن أن يستخدم

[١] دونكل أو دونجول أو دونجل بالإنجليزية (Dongle): هي قطعة صغيرة إلكترونية من أجزاء الحاسب الآلي (دعامة إلكترونية) يتم تركيبها به لتزويده بوظائف إضافية غير التي يمكنه القيام بها أو إنجازها. ويقوم الدونجل بعمل حماية للبرنامج المستخدم معه بحيث يتوقف عن التشغيل بدونه وذلك من خلال ملف أساسي – ضمن البرنامج – هو sentinel.vxd المسؤول عن التأكد من الحماية، وعند إزالة قطعة الدونجل من مكانها يتوقف البرنامج مباشرة عن العمل.
– https://www.rise.company/forum/threads/26116, 4/4/2020.

مفتاح الحماية لتشفير المعطيات الهامة بحد ذاتها، فمثلاً في موسوعة علمية للنصوص والصور أهمية أكثر من البرنامج الذي يعرضها وقد تكون هذه النصوص والصور وفق صيغة قياسية (Standard Format) مما يظهر أهمية تشفيرها.

الطريقة الثانية/ الحماية القانونية – المنطقية:

وهي السائدة في الولايات المتحدة الأمريكية، وتعتمد علي التحذير قبل الاستخدام والمعاقبة بعد إساءة هذا الاستخدام، وقد ساعدت التشريعات الجديدة في تقليل معدلات القرصنة بشكل كبير. وقد انتهج المشرع المصري الطريقة الأخيرة لحماية الملكية الفكرية الرقمية في المادة ١٨١ من القانون رقم ٨٢ لسنة ٢٠٠٢ بشأن إصدار قانون حماية حقوق الملكية الفكرية [1]، حيث نص علي أنه "مع عدم الإخلال بأية عقوبة أشد في قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، كل من ارتكب أحد الأفعال الآتية:

رابعاً : نشر مصنف أو تسجيل صوتى أو برنامج إذاعى أو أداء محمى طبقاً لأحكام هذا القانون عبر أجهزة الحاسب الآلى أو شبكات الانترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابى مسبق من المؤلف أو صاحب الحق المجاور.

سادساً– الإزالة أو التعطيل أو التعييب بسوء نية لأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.

وتتعدد العقوبة بتعدد المصنفات أو التسجيلات الصوتية أو البرامج الإذاعية أو الأداءات محل الجريمة.

وفي حالة العود تكون العقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه.

[1] مصر. قانون رقم ٨٢ لسنة ٢٠٠٢ بإصدار قانون حماية حقوق الملكية الفكرية. (الجريدة الرسمية: العدد ٢٢ مكرر. تاريخ ٢٠٠٢/٦/٢). ص ٢ وما بعدها.

وفي جميع الأحوال تقضي المحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها وكذلك المعدات والأدوات المستخدمة في ارتكابها.

ويجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المحكوم عليه في ارتكاب الجريمة مدة لا تزيد على ستة أشهر، ويكون الغلق وجوبياً في حالة العود في الجرائم المنصوص عليها في البندين (ثانياً, وثالثاً) من هذه المادة.

وتقضى المحكمة بنشر ملخص الحكم الصادر بالإدانة في جريدة يومية أو أكثر على نفقة المحكوم عليه ".

كما نص في المادة ٢٣ من القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات [1] علي أنه " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

(هـ) توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته.

وتكون العقوبة على مخالفة المادة (١٣) من هذا القانون، الغرامة التي لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه.

وفي الحالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى.

وفي جميع الأحول يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه".

[1] مصر. قانون رقم ١٥ لسنة ٢٠٠٤ بتنظيم التوقيع الالكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات. (الجريدة الرسمية: العدد ١٧ تابع. تاريخ ٢٠٠٤/٤/٢٢). (د). ص ٣ وما بعدها.

كما نص في المادة ١٧ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات علي أن "يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة".

تطبيقات قضائية:

نعرض فيما يلي لتطبيقات قضائية تخص برامج الحاسب الآلي ثم قواعد البيانات.

١) برامج الحاسب الآلي:

– في قضية تتلخص وقائعها فيما هو ثابت بمحضر جمع الاستدلالات المحرر بمعرفة المقدم / ... المفتش بالإدارة العامة لمباحث المصنفات وحماية حقوق الملكية الفكرية المؤرخ ../../٢٠١٣ من أنه بناء على تكليفه بالتوجه لمدينة الإنتاج الإعلامى لفحص بعض القنوات الفضائية للوقوف على مدى قانونية العمل بها والتزامها بالقوانين الخاصة بالملكية الفكرية وبالدلوف داخل قناة ... تقابل مع المتهم/ ... مدير القناة ومذيع بها وبفحص القناة والاستعلام عن تراخيص البرامج المحملة على أجهزة الحاسب المتواجدة بالقناة تبين عدم وجودها بالمكان، فقام بفحص أجهزة الحاسب الآلى المتواجدة بالمكان تم ضبط عدد ٢ قرص صلب محملين بالبرامج المقلدة والمنسوخة ، القرص الأول ماركة سامسونج محمل ببرنامج Windows XP professional ، القرص الثانى ماركة ويسترن ديجيتال محمل ببرامج Windows 7 ultimate ، Office 2007 ، EastNod 32 Antivirus ، وبسؤال المتهم عما نتج عنه الفحص أنكر صلته وقرر أن المسئول هو مورد الأجهزة وأنه ليس فنياً، وتم التحفظ على المضبوطات للعرض على النيابة العامة والتى قررت عرض تلك المضبوطات على هيئة تنمية صناعة تكنولوجيا المعلومات – مكتب حماية

حقوق الملكية الفكرية – والذى أودع تقريراً مؤرخ فى ../../٢٠١٣ انتهى فيه إلى أن:

– القرص الصلب الأول محمل بنظام تشغيلMicrosoft Windows7

برقم مسلسل: 9CW99-79BBF-D4M3X-4RPH9

– القرص الصلب الثانى محمل بنظام تشغيل Microsoft Windows XP professional

برقم مسلسل: BQB7T-3C4FF-393QD-RF3W4-GBRQ3

وترى لجنة الخبراء ضرورة إحضار المتهم للتراخيص الخاصة باستخدام واستغلال هذه البرامج، وفى حالة عدم إحضاره يعتبر استخدام واستغلال هذه البرامج هو استعمال غير قانونى ومخالفاً لأحكام قانون حماية حقوق الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ ولوائحه وقراراته التنفيذية.

أسندت النيابة العامة إلي المتهم أنه:

اعتدى على الحق المالى والأدبى للمؤلفين وأصحاب الحقوق المجاورة على النحو المبين بالأوراق.

وطلبت عقابه بالمواد ١٤٣، ١٤٥، ١٥٠، ١٨١ فقرة ١ بند / سابعاً فقرة ٢ ،٤ ،٥ ،٦ من القانون ٨٢ لسنة ٢٠٠٢ بشأن حماية الملكية الفكرية.

قدم المتهم للمحاكمة الجنائية وعدلت محكمة جنح القاهرة الاقتصادية القيد بجعله جنحة بالمواد ١/١٣٨ ، ١٤٠ بند ٢ ، ١٤٣ ، ١٥٠ ، ١٨١ فقرة ١ بند / سابعاً فقرة ٢ ، ٤ ، ٥ ، ٦ من القانون ٨٢ لسنة ٢٠٠٢ بشأن حماية الملكية الفكرية. وقضت بتغريم المتهم/ ... مبلغ خمسة آلاف جنيه وتتعدد العقوبة بتعدد المصنفات ومصادرة النسخ المضبوطة ونشر الحكم الصادر بالإدانة على نفقته فى جريدة الجمهورية وألزمته المصاريف الجنائية – عملاً بمواد القيد المعدلة.

وأسست حكمها علي الأدلة السابقة مستخلصة منها قيام المتهم/ ... – حال إدارته لقناة ... الفضائية بارتكاب جريمة نسخ مصنفات محمية قانوناً – برامج حاسب آلى (Microsoft Windows 7 برقم مسلسل : 9CW99-79BBF-D4M3X-4RPH9 , Microsoft Windows XP professional برقم مسلسل : BQB7T-3C4FF-393QD-RF3W4-GBRQ3) – واستخدامها في تشغيل النظام الحاسوبي لديه دون ترخيص من الشركة منتجتها وصاحبة حق استغلالها المالي معتدياً بذلك علي حقها الأدبي والمالي بما يتحقق معه الركن المادى للجريمة مع علمه بنسخها واتجاه إرادته إلى استعمال نسخ غير أصلية فيما نسخت من أجله بما يتحقق معه الركن المعنوى للجريمة [1].

٢) قواعد البيانات:

– في قضية تتلخص وقائعها في بلاغ محامى بصفته وكيل عن رئيس مجلس إدارة شركة ... بمحضر جمع الاستدلالات من تضرره من المتهم / ... الذى يعمل بقسم نظم المعلومات بالشركة ذاتها لقيامه بنسخ معلومات مهمة خاصة بالشركة من أحد أجهزة الحاسب الآلى الرئيسية والخاصة بالإدارة المالية وهى بيانات ومعلومات خاصة بالعاملين بالشركة من حيث المرتبات والحوافز وبياناتهم الشخصية والوظيفية وقيامه بتخزينها على حاسب آلى أخر بمكتب "تكنولوجيا المعلومات IT"، وقد علمت الشركة بذلك لأن النظام مصمم على التنبيه فور نسخ واختراق البيانات الموجودة بنظام المعالجة. وورد تقرير فحص فنى من قبل مدير قسم نظم المعلومات بالشركة ثابت به قيام أحد الأشخاص باختراق وسرقة المعلومات الخاصة بالشركة بتاريخ ... من جهاز حاسب آلى يحمل رقم تعريفى (...) والجهاز مسمى (...) وأن اسم المستخدم القائم بنسخ البيانات هو (...) وأن ذلك المسمى خاص بالمتهم / ... حيث قام بنسخ البيانات الهامة المتعلقة بالشركة والتى تشمل مرتبات العاملين بالشركة وحوافزهم وبياناتهم الوظيفية وقام بنسخها على فلاشة وأسطوانة مدمجة. ثم ورد تقرير الفحص الفنى

[1] حكم محكمة جنح القاهرة الاقتصادية في القضية رقم ٢٦٧ لسنة ٢٠١٤ جنح اقتصادية القاهرة – جلسة ٢٠١٤/١١/٢٩، وقد صار نهائياً بعدم استئنافه.

المحرر بمعرفة نقيب مهندس / ... الضابط بالإدارة العامة للمعلومات والتوثيق الذي انتهي فيه إلي ذات النتيجة السابقة.

أسندت النيابة العامة إلي المتهم أنه:

أولاً/ توصل إلى الحصول بغير وجه حق على محرر الكترونى (بيانات خاصة بشركة ... مخزنة الكترونياً) وذلك بأن قام بنسخ تلك البيانات من أحد أجهزة الحاسب الآلى الخاصة بالشركة سالفة الذكر التى يعمل بها إلى حاسبه الآلى بالشركة ونقلها إلى حيازته عبر اسطوانة مدمجة وكارت ذاكرة بيانات دون أن يكون من المخول لهم وظيفياً الإطلاع على تلك البيانات أو الحصول عليها وذلك على النحو المبين بتقرير إدارة مكافحة جرائم الحاسبات وشبكات المعلومات وبالأوراق.

ثانياً/ اخترق الوسيط الالكترونى (النظام الأمنى لنظم المعالجة الآلية) خاص بشركة ... بأن قام بإتيان الأفعال محل الاتهام الأول وذلك على الوجه المبين بتقرير إدارة مكافحة جرائم الحاسبات والمعلومات وبالأوراق.

وطلبت عقابه بالمادتين ١/ ب، د، ٢٣/ فقرة ١ بند هـ، وفقرة ٤ من القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الالكترونى.

قدم المتهم للمحاكمة الجنائية وقضت محكمة جنح القاهرة الاقتصادية بتغريمه مبلغ عشرين ألف جنيه ونشر حكم الإدانة فى جريدتى الأهرام والأخبار وعلى شبكات المعلومات الالكترونية المفتوحة على نفقته وألزمته بالمصاريف الجنائية – عملاً بمواد الاتهام السابقة.

وأسست حكمها علي الأدلة السابقة مستخلصة منها قيام المتهم بوصفه موظفاً بالشركة المعنية بارتكاب جريمة اختراق وسيط الكتروني من خلال استخدامه الكود المعنون به (...) فى الدخول على جهاز الحاسب الآلى رقم (...) والمسمى(...) واخترق بواسطته الوسيط الالكترونى (النظام الآمنى لنظام المعالجة الآلية) الخاص بالشركة مرؤسته بتاريخى .../ ... لنسخ بيانات العاملين بها على وحدة تخزينه الالكترونية (فلاشة) واسطوانه

مدمجة (سى دى) مع علمه بأن هذا الاختراق مؤثم قانوناً وتعمد إتيانه على النحو المتقدم[1].

وجدير بالذكر أن النيابة العامة قد أسندت للمتهم الجريمة ذات العقوبة الأشد وهي الواردة في قانون تنظيم التوقيع الإلكتروني، رغم انطباق الوصف التجريمي الوارد بقانون حماية حقوق الملكية الفكرية وهو الإزالة بسوء نية لأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور، علي فعل المتهم.

– وفي قضية أخري تتلخص وقائعها فيما أبلغ به المدعي بالحق المدني/ ... من أن المتهمين قاموا بالاستيلاء على قواعد بيانات موقع شركته/ ... وذلك بنسخ كامل للموقع الالكتروني المتضمن على الأحكام والتشريعات الخاصة بالدول العربية. وباستجواب المتهم الثاني/ ... قرر بعمله مستشاراً قانونياً بالشركة مرؤسة المدعي بالحق المدني واعتياده إجراء عملية نسخ للبيانات بصورة مستمرة وذلك حفاظاً منه على قواعد البيانات من التلف دون قصد الاستيلاء عليها. وورد تقرير الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية ثابت به أنه بفحص ملف التسجيل تبين إنزال الملف الخاص بمجلة شبكة "..." بتاريخ ../../٢٠٠٨ وأن الرقم التعريفي الذي استخدم في التنزيل متصل بجهاز مرتبط بخط تليفوني باسم المتهم الثالث/ ... ، وبفحص الروابط الاليكترونية الخاصة بالشركة تبين أنهم احدي عشر رابط اليكتروني تتضمن ملفات قانونية، وبفحص الروابط الاليكترونية الخاصة بالمتهم الثاني/ ... تبين احتوائها على أقسام لمختلف القوانين ورابط تقديم خدمه ترجمة النصوص القانونية لجميع اللغات.

أسندت النيابة العامة إلي المتهمين أنهم:

طرحوا للتداول بالبيع مصنف برامج حاسب آلي محمل عليها أحكام وقوانين محمية قانوناً بدون إذن كتابي مسبق من المؤلف وأصحاب الحقوق المجاورة على النحو المبين بالأوراق.

[1] حكم محكمة جنح القاهرة الاقتصادية في القضية رقم ١١٧٥ لسنة ٢٠١٣ جنح اقتصادية القاهرة – جلسة ٢٠١٤/٤/٢٦، وقد صار نهائياً بعدم استئنافه.

اعتدوا على الحق المالي والأدبي للمؤلفين وأصحاب الحقوق المجاورة على النحو المبين بالأوراق.

وطلبت عقابهم بالمواد ١٣٨ ، ١٤٠ ، ١٤١ ، ١٨١ من قانون حماية حقوق الملكية الفكرية الصادر بالقانون رقم ٨٢ لسنه ٢٠٠٢.

قدم المتهم للمحاكمة الجنائية وندبت محكمة القاهرة الاقتصادية خبيراً من هيئة تنمية صناعة تكنولوجيا المعلومات لمباشرة المأمورية الواردة بحكمها والذي أودع تقريراً انتهي فيه إلى أن موقع المدعي بالحق المدني (...) تم رفعه Upload وتشغيله على شبكة الانترنت بتاريخ ../../٢٠٠٨ بينما موقع المتهم الثاني (...) قد تم رفعه Upload وتشغيله على شبكة الانترنت بتاريخ ../../٢٠٠٩. وتتطابق قاعدة بيانات الأحكام القضائية في كلا الموقعين مع وجود تعديلات طفيفة على الهيكل البنائي لقاعدة بيانات الأحكام القضائية الخاصة بموقع المتهم الثاني/ ... فيما يخص خواص الجداول المكونة لقاعدة البيانات. وأن موقع المدعي بالحق المدني (...) يحتوي على هيكل قاعدة بيانات تشريعات تحت الإنشاء ولكنة يحتوي على بيانات خاصة (Data) بتشريعات بلاد أخري (لا تحتوي على بيانات خاصة بتشريعات مصر) حتى تاريخ الفحص. وأن موقع المدعي بالحق المدني (...) يحتوي على موسوعات قانونية وقضائية لمجموعة من الدول العربية (مصر، السعودية، الكويت، الإمارات، البحرين، قطر) بينما موقع المتهم الثاني (...) يحتوي على موسوعات قانونية وقضائية لجمهورية مصر فقط.

قضت المحكمة ببراءة المتهمين من الجرائم المسندة إليهم ورفض الدعوى المدنية وألزمت رافعها بمصاريفها ومبلغ خمسة وسبعين جنيهاً مقابل أتعاب المحاماة.

طعن كل من النيابة العامة والمدعي بالحق المدني علي هذا الحكم بالاستئناف

قضت محكمة جنح مستأنف القاهرة الاقتصادية بقبول الاستئنافين شكلاً وفى الموضوع برفضهما وتأييد الحكم المستأنف وألزمت المدعى بالحق المدنى مصاريف الدعوى المدنية ومبلغ مائة جنيهاً مقابل أتعاب المحاماة.

وأسست حكمها علي أن التقرير المودع في ملف الدعوى قد جزم بأن موقع المدعى بالحق المدنى عبارة عن بيانات تشريعية تحت الإنشاء ولا تحتوى على بيانات خاصة بتشريعات جمهورية مصر العربية أى أنها تُعد مشروع لا يزال قيد النظر والتنقيح والتغيير والتبديل أى أنه لم يظهر بعد للوجود كاملاً، إذ أن المحمى هو المصنف فى صورته المادية النهائية أى فى شكله الملموس، ومن ثم لا تسرى عليه الحماية القانونية مما يتعين معه تأييد الحكم المستأنف[1].

خاتمة وتوصيات :

تعرضنا من خلال بحثنا في جرائم القرصنة الرقمية وانعكاساتها الاقتصادية دولياً ومحلياً، إلي الأحكام العامة للجرائم المعلوماتية من خلال بيان ماهيتها وخصائصها وأنماط مرتكبيها ثم تناولنا أحكامها الخاصة في مجال الملكية الفكرية باختيار نموذج إجرامي ذائع الصيت لها يعرف بجرائم القرصنة الرقمية أوضحنا مفهومها وأخطارها الاقتصادية علي الصعيدين الدولي والمحلي، وسبل مكافحتها للحد من أضرارها. وقد رأينا حجم الخسائر المترتبة علي ارتفاع معدلات القرصنة في مجال البرمجيات لا سيما فيما يتعلق ببرامج الحاسب وقواعد البيانات، وهو ما من شأنه التأثير علي الناتج المحلي في الدول النامية ومنها مصر بطبيعة الحال.

فالثورة التكنولوجية من أجهزة الحاسب وشبكات الاتصالات وشبكة الإنترنت فرضت تحديات كبيرة مما أدي إلي إزدياد مخاطر هذه الجرائم وآثارها الاقتصادية، لذلك يجب علي الجهات المعنية باكتشاف تلك الجرائم وعلي الجهات القضائية المعنية بالتحقيق فيها القيام بما يلي:

١- تعريف العاملين في مجالات جمع المعلومات والضبط والتحقيق في تلك الجرائم بالجوانب الأساسية للطبيعة الفنية التقنية لتكنولوجيا المعلومات والاتصالات.

[1] حكم محكمة جنح مستأنف القاهرة الاقتصادية في القضية رقم ٤٣٨ لسنة ٢٠١٤ جنح مستأنف – جلسة ٢٠١٥/٣/٥ طعناً علي الحكم الصادر في الجنحة رقم ٦٢٥ لسنة ٢٠١٢ اقتصادى القاهرة.

٢- وضع خطط لتطوير وتدريب الكوادر البشرية القائمة علي أنشطة جمع المعلومات والتحري والتحقيق في تلك الجرائم.

٣- مراقبة ومتابعة المحال ومراكز بيع أجهزة الحاسب الآلي وأعمال النسخ عن طريق القيام بأعمال التفتيش الدوري.

٤- تكثيف الدورات التدريبية والمؤتمرات التي تنظمها الجهات المعنية والشركات صاحبة الحقوق للتعرف علي أحدث أشكال الإنتهاكات وأحدث المستجدات في مجالات تأمين المعلومات.

٥- وضع الاستراتيجيات المستقبلية لخطط وبرامج مكافحة جرائم القرصنة الرقمية.

قائمة المصادر العربية

المؤلفات:

- فتحي سرور، أحمد (١٩٧٧). الشرعية والإجراءات الجنائية. القاهرة: دار النهضة العربية.

- محمود مصطفي، أحمد (٢٠١٠). جرائم الحاسبات الآلية في التشريع المصري: دراسة مقارنة. القاهرة: دار النهضة العربية.

- رسلان، أيمن، عبد العال الديربي ومحمد إسماعيل (٢٠١٢). جرائم المعلوماتية والإنترنت بين العالم الافتراضي والواقع بالتطبيق علي مصر والوطن العربي. القاهرة: نادي القضاة.

- عبد الباقي الصغير، جميل (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة: الجرائم الناشئة عن استخدام الحاسب الآلي. مج.١. ط.١.- القاهرة: دار النهضة العربية.

- عبد الباقي الصغير، جميل (٢٠١١). جرائم الإنترنت: الأحكام الموضوعية والجوانب الإجرائية. القاهرة: نادي القضاة.

- ممدوح إبراهيم، خالد (٢٠٠٨). أمن الجريمة الإلكترونية. الإسكندرية: الدار الجامعية.

- أحمد محمود، سيد (٢٠٠٩). دور الحاسوب (الكمبيوتر) أمام القضاء المصري والكويتي: نحو إلكترونية القضاء والقضاء الإلكتروني. القاهرة: دار النهضة العربية.

- مأمون، عبد الرشيد، محمد سامي عبد الصادق (٢٠٠٦-٢٠٠٧). حقوق المؤلف والحقوق المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديد رقم ٨٢ لسنة ٢٠٠٢. القاهرة: دار النهضة العربية.

- عبد القوي علي مصري، عبد الصبور (٢٠١٢). المحكمة الرقمية والجريمة المعلوماتية. ط.١.- الرياض: مكتبة القانون والاقتصاد.

- بيومي حجازي، عبد الفتاح (٢٠٠٢). الأحداث والإنترنت. ط.١.- الإسكندرية: دار الفكر الجامعي.

- بيومي حجازي، عبد الفتاح (٢٠٠٧). مباديء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت. المحلة الكبرى: دار الكتب القانونية.

- محمد بن يونس، عمر (٢٠٠٣). المجتمع المعلوماتي والحكومة الإلكترونية: مقدمة إلي العالم الافتراضي. القاهرة: دار النهضة العربية.

- كوك، كرتيس (٢٠٠٦). حقوق الملكية الفكرية. **من إعداد قسم الترجمة بدار الفاروق** (مترجم إلي اللغة العربية من الأصل باللغة الإنجليزية). ط.١.- القاهرة: دار الفاروق للنشر والتوزيع.

- حجازي، محمد (٢٠٠٨). حقوق المؤلف وحماية البرمجيات وقواعد البيانات. القاهرة: د ن.

- حجازي، محمد (٢٠٠٨). دليل العمل والإجراءات لإنفاذ حقوق المؤلف. القاهرة: د ن.

- سامي الشوا، محمد (٢٠٠٣). ثورة المعلومات وانعكاساتها علي قانون العقوبات. القاهرة: الهيئة المصرية العامة للكتاب.

- عبيد الكعبي، محمد (٢٠٠٩). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت: دراسة مقارنة. ط.٢.- القاهرة: دار النهضة العربية.

- عبيد الكعبي، محمد (٢٠١٠). الحماية الجنائية للتجارة الإلكترونية. القاهرة: دار النهضة العربية.

- أحمد عبابنة، محمود (٢٠٠٩). جرائم الحاسوب وأبعادها الدولية. عمان: دار الثقافة للنشر والتوزيع.

- فتحي أحمد عبد الكريم، مني (٢٠١١). الجريمة عبر الشبكة الدولية للمعلومات (Internet): صورها ومشاكل إثباتها. القاهرة: دار النهضة العربية.

- عادل قورة، نائلة (٢٠٠٥). جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية. ط.١.- بيروت: منشورات الحلبي الحقوقية.

- عبد الحميد نبيه، نسرين (٢٠٠٨). الجريمة المعلوماتية والمجرم المعلوماتي. الإسكندرية: منشأة المعارف.

- عبد الحميد نبيه، نسرين (٢٠١٠). القرصنة علي البرمجيات وأثر ذلك علي الاقتصاد العالمي. الإسكندرية: المكتب الجامعي الحديث.

- عبد القادر المومني، نهلا (٢٠١٠). الجرائم المعلوماتية. عمان: دار الثقافة للنشر والتوزيع.

- محمد فريد رستم، هشام (١٩٩٢). قانون العقوبات: مخاطر تقنية المعلومات. أسيوط: مكتبة الآلات الحديثة.

- عرب، يونس (٢٠٠٢). دليل أمن المعلومات والخصوصية: جرائم الكمبيوتر والإنترنت. مج.١. ط.١.- بيروت: اتحاد المصارف العربية.

الرسائل العلمية:

- يوسف، صغير (٢٠١٣). **الجريمة المرتكبة عبر الإنترنت**. أطروحة ماجستير. قسم القانون الدولي للأعمال. كلية الحقوق والعلوم السياسية. جامعة مولود معمري- تيزي وزو.

- عبد العزيز أبازيد، محمود (٢٠١٦). **الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية**. أطروحة دكتوراه. قسم القانون الجنائي. كلية الحقوق. جامعة القاهرة.

الأبحاث:

- سرور، أحمد فتحي (٢٠٠٨). **الجريمة الإليكترونية**، بحث منشور في **مجلة النيابة العامة**. س.١٧، ع.١، مارس.

- سامي عرابي، سامح (٢٠١٦). **نظرة تحليلية للمنافسة غير المشروعة في إطار قانون حماية الملكية الفكرية المصري**. بحث مقدم إلي **المركز القومي للدراسات القضائية** بمناسبة التدريس في الدورة التدريبية الأولي للسادة المستشارين والرؤساء والقضاة بالمحاكم الاقتصادية وأعضاء النيابة العامة في قانون حماية الملكية الفكرية.

- عبد الغني، فتحي (٢٠٠٦). **اقتصاديات الملكية الفكرية عبر الإنترنت**، بحث منشور ضمن أعمال **المؤتمرات الخاصة بالمنظمة العربية للتنمية الإدارية: المعاملات الرقمية وقانون الإنترنت**. القاهرة: المنظمة العربية للتنمية الإدارية.

الأوراق البحثية:

- ب. دوناهو، جيمس. "حق المؤلف" ورقة بحثية قدمت في **ورشة عمل حول الملكية الفكرية: حق المؤلف**. القاهرة: ١٦-١٧ نوفمبر. ٢٠١٦.

- محمد شكرى، عمرو. "نطاق حماية الحقوق الاستئثارية الرقمية على شبكة الانترنت ودور مقدم الخدمة فى إنفاذ القانون". ورقة بحثية قدمت في **ورشة عمل حول الملكية الفكرية: حق المؤلف**. القاهرة: ١٦-١٧ نوفمبر. ٢٠١٦.

- سمير، محمد. "جرائم الإنترنت وعلاقاتها بالتحولات الاقتصادية". ورقة بحثية قدمت إلي **المؤتمر الدولي الخامس للبحوث العلمية وتطبيقاتها**. القاهرة: ٢١ -٢٤ ديسمبر. ٢٠٠٩.

المواقع الإلكترونية:

- https://ar-ar.facebook.com/notes.

- https://ar.wikipedia.org/wiki.

- www.dotmsr.com/605/1/116269.

- https://gss.bsa.org.

المصادر والمراجع الأجنبية

Books:

- Parker (Donn B.), Fighting Computer Crime: A New Framework for Protecting Information, New Jersey: John Wiley & Sons, 1998.

Articles:

- Norman (Adrian R. D), Computer Crime and the law, **C.L.J.**, Vol. 15, 1991,

- Taber (J .K.), on Computer Crime**, C.L.J**., Vol. 1, 1979.