حماية الملكية الفكرية في الأمن السيبراني

الدكتور / عبد الله بن سعيد أبو داسر

الأستاذ المساعد في قسم الأنظمة

بكلية العلوم الإدارية بجامعة نجران

الكلمات المفتاحية

عربي	إنجليزي
حماية	Protection
ملكية فكرية	Intellectual property
الأمن السيبراني	Cybersecurity

ملخص البحث

عربي

باتت الحاجة ملحة لحماية مجالات الملكية الفكرية في مجال الأمن السيبراني؛ وذلك لتوفير حماية ذات طابع مخصوص للحفاظ على سرية المعلومات بشتى أنواعها ومجالاتها؛ وذلك باتخاذ كافة التدابير لكف أيدي العابثين بها.

وحتى نصل إلى حماية شاملة فلا بد من معرفة جملة تلك التهديدات والاعتداءات على حقوق الملكية الفكرية حتى نستطيع توفير حماية لمجالات الملكية الفكرية، وعليه كان من الضرورة بحث هذا الموضوع والعمل على إيجاد وسائل آمنة ومتجددة من خلال تطوير منظومة أمن الفضاء السيبراني وتفعيل برامج حماية الهوية الرقمية ولا تقف الحماية عند هذه الوسائل الإليكترونية، بل يتعدى الأمر إلى تطوير الاتفاقيات الدولية والتشريعات القانونية لمواكبة التقدم التكنلوجي، حتى نضمن الوقاية من مخاطر الاعتداءات ومهددات الملكية الفكرية في مجال الأمن السيبراني.

Intellectual property protection in cybersecurity

Abstract

There is an urgent need to protect the intellectual property in cybersecurity in order to provide protection of a special nature to preserve the confidentiality of information of all kinds and fields by taking all measures to stop the hands of those who abuse it.

To reach comprehensive protection, it is necessary to know the totality of those threats and attacks on intellectual property rights so that experts can protect the fields of intellectual property. However, protection does not stop at these electronic means, but rather it goes beyond to develop international agreements and legal legislations to keep pace with technological progress to ensure the prevention from the risks of attacks and threats to intellectual.

بسم الله الرحمن الرحيم

المقدمة

الحمد لله رب العالمين، والصلاة والسلام على أشرف المرسلين، سيدنا محمد صلى الله عليه وسلم، وعلى آله وصحبه وسلم أجمعين.

وبعد:

تعتبر الملكية الفكرية من الأفكار المستحدثة في الأنظمة الوضعية، لذلك كانت فكرة حماية المفكر أو المبتِكر لأفكاره ومبتكراته هي فكرة وليدة القرن الماضي، ولم يكن لها وجود في الأزمنة المتقدمة، إذ هي فكرة نشأت كنتيجة طبيعية للتطور الحديث في عالم المعرفة والابتكار، ولذا فقد نشأت هذه الفكرة لدى رجال القانون اهتماماً بالغاً، وتلقتها التنظيمات المعاصرة لتؤسس لها مركزاً قانونياً.

ما الأمن السيبراني:

بقصد بالأمن السيبراني: ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية.[١]

[١] السيبراني: كلمة انجليزية، مأخوذة من اصطلاح" cyber" وهي تعني وهي تعني الإلكترونية، وقد أُصطلح على أن تُطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، راجع:جبور: منى الأشقر: الأمن السيبراني: التحديات ومستلزمات المواجهة، من منشورات جامعة الدول العربية، المركز العربي للبحوث القانونية

١١ – حماية الملكية الفكرية في الأمن السيبراني

أهمية الموضوع وسبب اختياره:

لما كانت العولمة الإلكترونية هي الضرورة الملحة في عالمنا اليوم، إذ لا تستطيع الدول إدارة منظومة أعمالها في شتى أجهزتها الحكومية إلا عن طريق الحواسب والمنصاتالإلكترونية، فقد أصبحت المعلومات المتعلقة بالأمن للدول في مسيس الحاجة إلى الحفاظ عليها وحمايتها من الهجمات الإلكترونية التي قد تسبب أضراراً بالغة بأمن الدول وسلامة معلوماتها الإلكترونية، ومن هنا أصبحت حماية الملكية الفكرية في مجال الفضاء السيبراني من الحاجات الملحة، التي يفرضها واقع المعلومات الأمنية المعاصر. حيث تظهر أهمية حماية الملكية الفكرية في مجال الأمن السيبراني من خلال العناصر الآتية:

١. توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها، وذلك بعدم السماح لغير المخولين بالوصول إليها باستخدامها.

٢. الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.

٣. تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.

٤. حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درعٌ واقٍ للبيانات والمعلومات.

والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبرانيبيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢، صـ٢، وانظر: مجلة محطات، مقال منشور بتاريخ ٢٠١٩/٣/٩م، على الرابط: https://www.mahat.net

٥. استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

٦. استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

٧- توفير بيئة عمل آمنة جدًا خلال العمل عبر الشبكة العنكبوتية.

لكل ما سابق فقد اخترت هذا الموضوع لبيان المخاطر ووسائل الحماية للملكية الفكرية في مجال الأمن السيبراني.

تساؤلات البحث:

يتحدد سؤال هذا البحث في الآتي:

ما هو الأمن السيبراني، وما هي المخاطر الأمنية التي تهدد الملكية الفكرية في مجال الأمن السيبراني، وما هي الوسائل التي يمكن من خلالها حماية الملكية الفكرية في مجال الأمن السيبراني؟

هذا ما سوف يحاول الباحث الإجابة عنه في ثنايا هذا البحث.

هدف البحث:

يهدف هذا البحث إلى التعريف بمفهوم الأمن السيبراني، وبيان المخاطر الأمنية في الفضاء السيبراني، وبيان الوسائل التي يمكن من خلالها حماية الملكية الفكرية في مجال الأمن السيبراني.

الدراسات السابقة:

لم أجد حسب اطلاعي دراسة تتحدث عن هذا الموضوع، ولا تتناول جوانبه المختلفة ولا موضوعاته المتفرعة، وإنما هو منشور ومتحدث عنه في عدة مقالات وورقات عمل متناثرة على المواقع الإلكترونية، ولم أجد حتى اليوم دراسة وافية قد استوفت هذا الموضوع من شتى جوانبه.

ومن تلك الموضوعات المتناثرة:

١. **الأمن السيبراني: التحديات ومستلزمات المواجهة،** ورقة عمل أعدتها د. منى الأشقر جبور، وهي من منشورات جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢ وقد تحدثت الورقة عن مفهوم الأمن السيبراني، وبعض المخاطر التي تتهدد الأمن السيبراني في عبارة مختصرة.

٢. **أمن المعلومات أحد السبل لحماية الملكية الفكرية،** مقال للباحث: ابن ضيف الله فؤاد، منشور بمجلة cybrarians العدد ٢٤، ديسمبر ٢٠١٠م، وقد تحدث فيه الباحث عن أهمية الأمن السيبراني، ونماذج لبعض الجرائم التي ترتكب في مجال الفضاء السيبراني.

٣. **عرض موجز لإطار الملكية الفكرية القانوني والتنظيمي في الولايات المتحدة الأمريكية، معلومات أساسية عامة،** مقال منشور على موقع:

https://wipolex.wipo.int، وقد تحدث المقال عن حماية الملكية الفكرية في القانون الأمريكي في عناصر مختصرة.

منهج البحث:

اعتمدت في هذا البحث على المنهج الاستقرائي وذلك من خلال استقراء النصوص التشريعية في مجال حماية المعلومات الإلكترونية في الدول المختلفة كما اعتمدت على المنهج التحليلي، من خلال التأمل والنظر فيما تحتويه هذه النصوص، وذلك للوصول إلى حماية الملكية الفكرية من الجرائم المعلوماتية في مجال الأمن السيبراني.

خطة البحث:

فقد قسمت الحديث حول موضوع هذا البحث إلى مقدمة، وثلاثة مباحث وخاتمة:

ـ أما المقدمة فقد تحدثت فيها عن أهمية الموضوع وسبب اختياره، والهدف من البحث، وسؤاله، والدراسات السابقة، ومنهج البحث وخطته.

المبحث الأول:مفهوم الحماية الفكرية في الأمن السيبراني

وفيه ثلاثة مطالب:

المطلب الأول: مفهوم حماية الملكية الفكرية لغة واصطلاحاً.

المطلب الثاني: مفهوم الأمن السيبراني وعناصره. لغة واصطلاحاً

المطلب الثالث: علاقة الأمن السيبراني بحقوق الملكية الفكرية.

المبحث الثاني: مهددات الملكية الفكرية في الأمن السيبراني

وفيه مطلبان:

المطلب الأول: الاعتداءات الخاصة بأمن المعلومات وقيمتها.

وفيه فرعان:

الفرع الأول: الاعتداءات الخاصة بأمن المعلومات المعالجة آلياً.

الفرع الثاني: الاعتداءات الخاصة بقيمة المعلومات المعالجة آلياً

المطلب الثاني: الاعتداءات الخاصة بحقوق الملكية الأدبية والفكرية لبرامج الحاسب ونظمه.

وفيه فرعان:

الفرع الأول: الاعتداءات المتعلقة بالنصب والاحتيال في عالم النشر.

الفرع الثاني: الاعتداءات المتعلقة بالحصول على مال الغير عن طريق الغش المعلوماتي (بطاقات الائتمان ونحوها)

المبحث الثالث: وسائل حماية الملكية الفكرية في الأمن السيبراني.

وفيه مطلبان:

المطلب الأول: وسائل الحماية الإلكترونية.

المطلب الثاني: وسائل الحماية في التشريعات القانونية

خاتمة البحث وتشمل:

. نتائج وتوصيات البحث.

المبحث الأول

مفهوم حماية الملكية الفكرية في الأمن السيبراني

في هذا المبحث سوف أطرح نظرة شاملة حول مفاهيم حماية الملكية الفكرية، حيث سأوضح معاني مصطلحات حماية الملكية الفكرية في اللغة والاصطلاح، كذلك نتعرض

لمفهوم الأمن السيبراني مع بيان عناصره، ثم نسلط الضوء على علاقة الأمن السيبراني بحقوق الملكية الفكرية، وهذا كله يتأتى وفقاً للمطالب التالية:

المطلب الأول

مفهوم حماية الملكية الفكرية لغة واصطلاحاً

لابد لنا أن نتعرف على مصطلح حماية الملكية الفكرية، حيث أن هذا المصطلح مكون من ثلاث كلمات ولكل واحد منها معنى مختلف، فالأولى تتعلق بالحماية والثانية بالملكية والثالثة بالفكرية، ومن هنا كان من الأهم تناول هذه المصطلحات على حدة لغةً واصطلاحاً ثم نخلص إلى تعريفاً لهذا المصطلح مركباً.

الحماية لغة واصطلاحاً:

الحماية: مصدر من الفعل حَمَى، فيقال حَمَى الشيء يحميه حَمْياً، وحماية بالكسر: أي مَنَعَهُ، وحمى المريض ما يضره: منَعَه إياه، واحتمى هو من ذلك وتحمَّى: امتنع، والحَمِيُّ: المريض الممنوع من الطعام والشراب.[١]ويقال: حَميتُ المكان: مَنَعتُه

[١]الرازي: زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي: مختار الصحاح، تحقيق: يوسف الشيخ محمد، نشر المكتبة العصرية - الدار النموذجية، بيروت – صيدا، ط٥ ١٤٢٠هـ / ١٩٩٩م، جـ١، صـ٨٣.

أن يُقرب، واحتمى الرجل من كذا: أي اتقاه.[١] وفي الحديث النبوي: (ألا وإن حمى الله في أرضه محارمه).[٢]

ويقال حَمَى يحْمي، حمياً الرجل الشيء، ومنه: مَنَعه، ودَفعه عنه –القوم حماية: أي قام بنصرهم، والمرض حمية: منعه ما يضره.[٣]

ويقال: هذا شيء حَمِيٌّ؛ أي: محظور لا يقرب، وحَمَيتُه حمايةً: إذا دفعت عنه، ومنعت منه من يقرَبَهُ، والحمِيمُ: القريبُ المشفقُ، وسمي بذلك لأنَّه يحتدُ حمايةً لذويه، فهو يدافع عنهم، كما قال تعالى:{وَلَا يَسْـَٔلُ حَمِيمٌ حَمِيمًا ﴿١٠﴾} [سورة المعارج:١٠]

أما معنى الحماية في الاصطلاح يختلف معناه بحسب ما يضاف إليه، فمثلاً حماية المواطنين تعني صيانتهم ووقايتهم، وحماية البيئة تعني منع إصابتها بالتلوث، وحماية المستهلك تعني منع استغلالهم، ويوجد أيضًا حماية الاقتصاد وحماية التجارة وغيرها من الاصطلاحات الكثيرة لهذا المفهوم الواسع.[٤]

---

[١] مادة (حَمَى)، الزمخشري: أبو القاسم محمود بن عمرو بن أحمد، الزمخشري جار الله ، أساس البلاغة، تحقيق: محمد باسل عيون السود، نشر دار الكتب العلمية، بيروت – لبنان، ط١، ١٤١٩ هـ - ١٩٩٨م، جـ١، صـ٢١٦.

[٢] جزء من حديث طويل، رواه البخاري في صحيحه، كتاب الإيمان، باب فضل من استبرأ لدينه، رقم: (٥٢) (٣٤/١)، ومسلم في صحيحه، كتاب المساقاة، باب أخذ الحلال وترك الشبهات، رقم: (٤٠٧٠)، ١٢١٩/٣.

[٣] علي بن هادية وآخرون، القاموس الجديد الألفبائي، ص ٢٤٣.

[٤] معجم المعاني الجامع - معجم عربي عربي، https://www.almaany.com/، بتصرف، تاريخ ١٤٤١/٠٨/٠٥هـ.

وخلاصة الأمر: يخلص الباحث إلى وجود تناسب بين المعنى اللغوي والاصطلاحي فمصطلح الحماية يدور بين معنى المنع والدفع، إلا أن لفظ مصطلح الحماية يختلف معناه بحسب ما يضاف إليه.

الملكية لغة واصطلاحاً:

الملكية لغة: مأخوذة من الفعل ملك يملك تملكاً ومملوكاً، والمعنى حيازة الشيء والاحتواء له، ومن ثم إمكان القدرة على الفعل فيه بالاستبداد والتصرف، فهو مالك وتملك الشيء امتلكه أو ملكه قهرا.[١]

الملكية في الاصطلاح: لابد من بيان مصطلح الملكية من الجانب الشرعي ومن جانب شراح القانون المدني، أما ما يتعلق بتعرف مصطلح الملكية من الجانب الشرعي أو بمعنى ما توصل له فقهاء الشريعة الإسلامية.

أولا: تعريف مصطلح الملكية في الشريعة الإسلامية:

تعددت آراء الفقهاء اتجاه مصطلح الملكية، ويعود سبب هذا التنوع إلى اختلافهم في ضبط الملك، وما يعتبر مالاً مملوكا، وما لا يعتبر كذلك،[٢]وجاء في تعريف الملكية بأن الملك "هو الاختصاص بالمحل في حق التصرف، أو شرع للتمكن من التصرف في المحل"[٣]،وقيل: "الملك حكم شرعي مقدر في العين أو المنفعة، يقتضي تمكن من

---

[١] ابن منظور: محمد بن مكرم بن على، أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعى الإفريقى، دار صادر - بيروت ط٣ ١٤١٤هـ جـ١٠/٤٩٢، أبو العباس: أحمد بن محمد بن علي الفيومي ثم الحموي: المصباح المنير في غريب الشرح الكبير، نشر: المكتبة العلمية – بيروت، جـ٢، صـ٥٧٩، أبو الحسين:أحمد بن فارس بن زكرياء القزويني الرازي، أبو الحسين: معجم مقاييس اللغة، تحقيق: عبد السلام محمد هارون، نشر دار الفكر ١٣٩٩هـ /١٩٧٩م. جـ٥، صـ٣٥٢.

[٢] لحرش: أسعد المحاسن: الملكية الفكرية بين تشجيع الابتكار وتحريم الاحتكار، منشور بموقع https://platform.almanhal.com، بتاريخ ١٤٤١/٨/٥هـ.

[٣]علاء الدين، أبو بكر بن مسعود بن أحمد الكاساني الحنفي: بدائع الصنائع في ترتيب الشرائع، دار الكتب العلمية الطبعة: الثانية، ١٤٠٦هـ - ١٩٨٦م، جـ٧، صـ١٢٨.

يضاف إليه من انتفاعه بالمملوك، والعوض عنه من حيث هو كذلك"،[١]وعرفها القرافي بقوله:" حكم شرعي مقدر في العين أو المنفعة، يقتضي تمكين من يضاف إليه من انتفاعه بالشيء وأخذ العوض عنه من حيث هو كذلك"[٢]ومن المعلوم والذي استقر عليه الفقه الإسلامي أن الحقوق كلها لا تثبت إلا بإثبات الشارع لها وتقريره لأسبابها ومنها حق الملكية وهذا ما نبه عليه القرافي في تعريفه،[٣] وبعد هذا العرض للتعاريف أجد أن تعريف العبادي يجمع كل المراد إثباتها في تعريف الملك، حيث عرفه بأنه" اختصاص إنسان بشيء يخوله شرعاً الانتفاع والتصرف وحده ابتداءً إلا لمانع".[٤]

أولا: تعريف مصطلح الملكية في عند القانونين:

قيل في تعريف الملكية هي: " حق الاستئثار باستعماله وباستغلاله والتصرف فيه على وجه دائم، وكل ذلك في حدود الشرع"[٥]، وبمعنى آخر قيل هي: " اختصاص أو استئثار إنسان بشيء يقتضي له وحده حق استعماله واستغلاله والتصرف فيه ابتداءً إلا لمانع في حدود القانون".[٦]

---

(١) القرافي: أبو العباس شهاب الدين أحمد بن إدريس بن عبد الرحمن المالكي الشهير بالقرافي: أنوار البروق في أنواء الفروق، نشر عالم الكتب، د.ط١ن د. ت، الفرق الثمانون بعد المائة، جـ٣، صـ٢٠٩.
(٢)المرجع والموضع السابق.
(٣) شبير: محمد عثمان: المدخل إلى فقه المعاملات المالية، دار النفائس، الطبعة الثانية، ١٤٣٠هـ-٢٠١٠م، ص ١١٨.
(٤)العبادي: عبد السلام: الملكية في الشريعة الإسلامية، مكتبة الأقصى، عمان، ١٩٧٧م، جـ١، صـ١١٥.
(٥)السنهوري: عبد الرازق: الوسيط في شرح القانون المدني – حق الملكية-، دار إحياء التراث العربي، بيروت لبنان، جـ٨، صـ٤٩٣.
(٦)العبادي: عبد السلام: مرجع سابق، جـ١، صـ١٥٣، ١٥٤.

وخلاصة الأمر: فملكية الشيء حق كفل الشرع والنظام لصاحبها كل التصرفات التي ترد على هذا الشيء، كالاستعمال والاستغلال والتصرف فله أن يمارس أي نوع من هذا التصرفات كيف يشاء ولا يمانعه أحد من ذلك؛ إلا ما تم تقيده في الشرع والنظام.

الفكرية لغة واصطلاحاً:

الفكرية لغة:

جاءت مادة فكر في معاجم اللغة بمعنى: التَّفَكُّرُ أي التأمل، والاسم والفكر والفِكرة والمصدر الْفَكْرُ بِالفتح وَبَابُهُ نَصَرَ. وأَفْكَرَ في الشَّيء وفَكَّرَ فِيهِ بالتشديد، وتَفَكَّر فيه بِمَعْنًى، ورجلٌ فِكِّيرٌ بِوَزْنِ سُكَيْتٍ كَثِيرُ التَّفَكُّرِ[١]، وقيل: إعْمال الخاطر في الشَّيء، والتدبر والتأمل فيه، وإعمال العقل فيه.[٢]

الفكرية في الاصطلاح:

والفكر اصطلاحاً: هو إعمال العقل في المعلوم للوصول إلى معرفة المجهول.[٣]

الملكية الفكرية مصطلح قانوني نتيجةَ ما ينتجه العقل البشري من أفكار، تتم ترجمتها إلى حقائق ملموسة، فيدخل في نطاقها كافة الحقوق الناتجة من النشاط الفكري

---

[١]الرازي: زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي: مختار الصحاح، المكتبة العصرية ـ الدار النموذجية، بيروت ـ صيدا الطبعة: الخامسة، ١٤٢٠هـ / ١٩٩٩م، ص: ٢٤٢.

[٢]ابن منظور: مرجع سابق، جـ٥، صـ٦٥, الفيومي، مرجع سابق، جـ٢، صـ٤٧٩.

[٣]مختار: أحمد: معجم اللغة العربية المعاصرة، عالم الكتب الطبعة: الأولى، ١٤٢٩ هـ ـ ٢٠٠٨ م، جـ٣، صـ٧٣٤.

للإنسان في الحقول الأدبية والفنية، لذا ذاع لدى الفلاسفة الحديث عن العقل ودوره في حياة صاحبه، إذ به يعز المرء أو يذل.[١]

وقد تنوعت آراء الباحثين في تعريف الملكية الفكرية فجاء في تعريفها لدى علماء الفقه الإسلامي المعاصرين بأنها حقوق معنوية، فالحق المعنوي هو سلطة لشخص على شيء غير مادي، هو ثمرة فكره أو خياله، أو نشاط؛ كحق المؤلف في مؤلفاته، وحق الفنان في مبتكراته الفنية، وحق المخترع في مخترعاته الصناعية، وحق التاجر في الاسم التجاري والعلامة التجارية وثقة العلماء.[٢]

وعرفها آخر بحق الابتكار؛ فقال: هو اختصاص شرعي حاجز، يمنح صاحبه سلطة مباشرة على انتاجه المبتكر أياً كان نوعه، ويمكنه من الاحتفاظ بنسبة هذا الناتج لنفسه.[٣]

---

[١] قدري: كامل: الحماية الجنائية للملكية الفكرية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، قسم القانون الجنائي، ٢٠١٤م، ص: ١٣.

[٢] النشمي: عجيل جاسم: الحقوق المعنوية: بيع الاسم التجاري، مجلة البحوث الإسلامية، مكة، مجمع الفقه الإسلامي، ص: ٢٢٨٤.

[٣] العثماني: محمد تقي: بيع الحقوق المجردة: بحوث الدورة الخامسة لمؤتمر مجمع الفقه الإسلامي، بجده، مجلة المجمع، العدد الخامس، (٢٣٨٥/٣).

وأما تعريفها لدى شراح القانون فعرفها البعض بأنها: "الأفكار والتعبيرات الخلاقة للعقل البشري التي لها قيمة تجارية وتحظى بالحماية القانونية كحق من حقوق الملكية".[١]

وأشارت المنظمة العالمية للمكية الفكرية لمعنى الملكية الفكرية فذكرت أنها إبداعات العقل من اختراعات ومصنفات أدبية وفنية وتصاميم وشعارات وأسماء وصور مستخدمة في التجارة، وأبانت أن الملكية الفكرية محمية قانوناً بحقوق منها مثلاً البراءات وحق المؤلف والعلامات التجارية التي تمكّن الأشخاص من كسب الاعتراف أو فائدة مالية من ابتكارهم أو اختراعهم، ويرمي نظام الملكية الفكرية، من خلال إرساء توازن سليم بين مصالح المبتكرين ومصالح الجمهور العام، إلى إتاحة بيئة تساعد على ازدهار الإبداع والابتكار.[٢]

ومما سبق بيانه في تعريفات الملكية الفكرية فنجد أنها تدور حول الملكية الأدبية والفنية والصناعية والتجارية ومهما تعدد هذه المسميات وهذا التنوع يعود إلى الجهة التي ينظر لها كل الباحثين.

---

[١] جامع: أحمد: اتفاقيات التجارة العالمية، دار النهضة العربية، ٢٠٠١م، ص: ١٠٦٦.
[٢] موقع المنظمة العالمية للمكية الفكرية، https://www.wipo.int/about-ip/ar، تمت الزيارة بتاريخ ١٤٤١/٠٨/٢٣هـ.

المطلب الثاني

مفهوم الأمن السيبراني وعناصرهلغة واصطلاحاً

الأمن في اللغة:

يدور الأمن في اللغة على سكون القلب وهدوء النفس وعدم الخوف، جاء في مقاييس اللغة: الهمزة والميم والنون أصلان متقاربان: أحدهما الأمانة التي هي ضد الخيانة، ومعناها سكون القلب والآخر التصديق.[١] وكذلك يدور حول الثقة والطمأنينة، جاء في أساس البلاغة فلان أُمَنةٌ أي يأمن كل أحد ويثق به، ويأمنه الناس ولا يخافون غائلته[٢].

السيبراني في اللغة:

مصطلح السيبراني يعتبر واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير الأبحاث على أن لفظة (CYBER) يونانية الأصل ومشتقة من كلمة (kybernetes) بمعنى الشخص الذي يدير دفة السفينة.

وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي NorbertWieners ١٨٩٤-١٩٦٤ وذلك للتعبير عن التحكم الآلي، فهو

---

[١] ابن فارس: مقاييس اللغة، مرجع سابق،جـ١، صـ١٣٣.
[٢] الزمخشري: أساس البلاغة، مرجع سابق، جـ١، صـ٣٥.

الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير: Cybernetics or control and communication in" the Animal and the machine، وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب.[١]

الأمن السيبراني اصطلاحا:

وردت العديد من التعاريف لمفهوم الأمن السيبراني، ومنها مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة."[٢]

جاء في تعريف الهيئة الوطنية للأمن السيبراني: " حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من عتاد وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع".[٣]

---

[١] مقال بعنوان: الأمن السيبراني، منشور على الموقع https://political-encyclopedia.org/dictionary تاريخ الزيارة ١٤٤٢/١/٢٧هـ.

[٢] المرجع السابق.

[٣] موقع الهيئة الوطنية للأمن السيبراني، https://nca.gov.sa/index.html تاريخ الزيارة ٦/ ١٤٤٢/٢هـ.

ويشير عدد من الباحثين إلى أن الأمن السيبراني عبارة عن " جميع العمليات التي تستهدف حماية أصول تكنلوجيا المعلومات المُكونِة للفضاء السيبراني".[١]

عناصر الأمن السيبراني

الهدف الذي الأساسي الذي يقوم عليه الأمن السيبراني هو حماية الهوية الخاصة بالأشخاص أو المنظمات سواءً كانت حكومية أم خاصة؛ كذلك حماية أجهزة الحواسب والخوادم البيانات والمعلومات الشخصية للأفراد أو المنظمات، وحتى يتحقق الهدف والغاية لابد من توفر مجموعة من العناصر ليكتمل الدور في ذلك، ومن أهم تلك العناصر[٢] ما يلي:

أولًا: التقنية (technology): تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

ثانياً: الأشخاص(People) :يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية

---

[١] الشايع: خالد: الأمن السيبراني، مفهومه، وخصائصه، وسياساته، دار العالمية، الأولى، ١٤٤٠هـ، ص ٢٥.
[٢] مقال منشور بموقع https://www.mah٦at.net/ ، إيمان الحيارى تاريخ النشر ٩ مارس ٢٠١٩م، تاريخ الزيارة ١٤٤٢/٢/٦هـ.

كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.

ثالثاً: الأنشطة والعمليات(Process) :يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

ومما سبق بيانه يمكن إعطاء تعريفاً للأمن السيبراني في مجال حماية المليكة الفكرية بأنه: النشاط الذي يحمي أنواع المليكة الفكرية المرتبطة بالتقنيات الحديثة للاتصالات والمعلومات، مع ضمان الحد من الخسائر والأضرار الواقعة أو محتملة الوقوع.

المطلب الثالث

علاقة الأمن السيبراني بحقوق الملكية الفكرية

لا شك أن البيئة الرقمية ساعدت في انتشار المعرفة بشتى أنواعها، وأضحى ذلك إلى سهولة النقل والتحميل والاختزال لكل أبواب المعرفة، وهذا الأمر أحدث قضية سلبية أمام حماية حقوق الملكية الفكرية بشتى أنوعها، حيث أصبح الأمن السيبراني كقضية ناشئة في حقل حماية الملكية الفكرية من خلال حداثته أمام مجالات الملكية الفكرية.

وآية ذلك أنه تتوفر في البيئة المعلوماتية إمكانية إقتباس وتعديل ونشر البرمجيات مما يجعلها عرضة للسطو عليها وإعادة إنتاجها، إضافة إلى امكانية الاطلاع على معلومات الآخرين وسرقتها، تحريفها أو تخريبها والتشويش عليها، حيث يعيش العالم أجمع عصر المعلومات، حيث أضحت الاتصالات والمعلومات من أعلى القيم المستحدثة، باعتبارها عماد جميع الأنشطة السياسية والاقتصادية والاجتماعية في حياة الأفراد والدول، إذ يعتمد الأفراد وكذا القطاع العام والخاص في الأنشطة اليومية على تكنولوجيا المعلومات والاتصالات ويظهر ذلك في النقل البري والجوي والبحري والاتصالات السلكية

واللاسلكية والمستشفيات والخدمات العامة والتجارة الإلكترونية والمؤسسات المالية والعسكرية وغيرها [١].

ومعلوم أن الجريمة تستهدف ما له قيمة في الحياة، لذا ظهرت الجريمة الإلكترونية وهي تتشـــابه مع الجريمة التقليدية في ضـــرورة وجود مجرم وضـــحية وأداة ومكان للجريمة. ويختلفان في أن الجريمة الإلكترونية تتطلب وجود بيئة رقمية واتصـــال بالانترنت، مما يعني أن جمع الأدلة من مسرح الجريمة يقتضي البحث عن تلك الأدلة من خلال مسرحين:

المسرح التقليدي، وهو الواقع خارج البيئة المعلوماتية، كالبصمات التي يتركها الجاني ومتعلقاته ونحوها.

المســـرح الســـيبراني، وهو الواقع داخل البيئة الحاســـوبية، ويشـــتمل على البيانات والمعلومات في الذاكرة والأقراص والشبكة، والتعامل مع هذا النوع من الأدلة لا يتم إلا من خلال خبير متخصص في الأدلة الرقمية[٢].

[١] فكري. أيمن عبد الله: جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر ٢٠٠٧م، صـ٩٤.
[٢] عبد الرحمن: محمد جلال: الجرائم الاليكترونية، ط١ مكتبة القانون والاقتصاد، ١٤٣٦هـ/٢٠١٥م، صـ١٠٩.علي. عبد الله حسين: حماية المعلومات المخزنة على الحاسب الآلي، رسالة دكتوراه من جامعة عين شمس ٢٠٠١م، صـ١٩.

ومن ناحية أخرى فإن أداة الجريمة الإلكترونية ذات تقنية عالية، كما أن مكان الجريمة الإلكترونية لا يتطلب انتقال الجاني إليه وإنما تتم الجريمة عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان تنفيذ الجريمة، فضلا عن البعد الدولي لهذا النوع من الجرائم، ومن ثم فإن الساحة الإجرامية في الجرائم المعلوماتية تثير تحديات واسعة حيث يمكن التخطيط للجريمة في دولة ويكون المنفذون في دولة أخرى، وتقع آثار الجريمة في مكان ثالث، مما يثير مشاكل نظامية تتعلق بالاختصاص والإثبات ونحو ذلك؛ بالإضافة إلى أن الجريمة المعلوماتية يصعب التحقق منها، ويصعب القبض على مرتكبيها، إضافة إلى صعوبة المحاكمة لعدم توافر الأدلة المادية والشهود غالبا[١].

وقد كانت المملكة من أولى الدول التي سارعت إلى الوقوف أمام هذا النوع من الجرائم المستحدثة بسن نظام مكافحة جرائم المعلوماتية، وهو يتمثل في مجموعة من القواعد النظامية التي تبين ماهية الأفعال التي تعد جرائم في مجال المعلوماتية وتحدد العقوبات التي تطبق على مقترفها؛ وهي قواعد خاصة، تقرر أعمالا محظورة ووقائع – صادرة عن إرادة جنائية – مضرة بالصالح العام.

[١] الصغير: جميل عبد الباقي: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ٢٠٠١م، صـ١٣.

وقد تناول نظام مكافحة جرائم المعلوماتية – محل الشـرح – جميع أنواع السـلوك الإجرامي الذي يتصـــور وقوعه في البيئة الرقمية، وهي تدور حول الدخول غير المشـروع والمسـاس بالحياة الخاصـة والتشـهير بالآخرين، والاسـتيلاء على الأموال المنقولة والوصـــول دون مســـوغ نظامي الى المعلومات البنكية والائتمانية، وإتلاف البرامج والبيانات وإعاقة الوصـــول الى الخدمة، وكذا الجرائم الماســـة بالنظام العام والآداب العامة وأمن المجتمع وغير ذلك.

وتتميز الجريمة الإلكترونية بجملة من الخصـــائص أهمها خفاء الجريمة وعدم السهولة في ملاحظتها، وكذا سهولة تنفيذها وخلوها من العنف المادي. وكونها جريمة عابرة للحدود. إضافة إلى صعوبة الوصول الى الجرائم المعلوماتية.

حيث إن هذا النوع من الجرائم يتسم بسرعة التنفيذ وسهولة الاخفاء وسرعة محو الآثار، وبالتالي تواجه أجهزة البحث والتحقيق صعوبات كثيرة في كشفها، مما يقتضي اعداد برامج تدريب وتأهيل لتلك الكوادر لتحقيق المهام المطلوبة منها بدقة وكفاءة،

إضافة الى ضرورة الاستعانة بذوي الخبرة الفنية في مجال المعلوماتية، لاقتضاء حق الدولة في العقاب[١].

وقد تعود صعوبة الكشف عن هذه الجرائم الى عدم رغبة المجني عليه في التبليغ عن الجريمة خشية التشهير سيما إن وقعت الجريمة على المؤسسات المالية التي تخشى من تراجع الثقة فيها، أو لعدم جدوى التبليغ لصعوبة الوصول الى المجرم المعلوماتي، وسرعة محو الأدلة، أو توافر الوسائل التقنية التي تعرقل الوصول إلى تلك الأدلة.

وتتعدد صور هذه الجرائم فقد تتم من خلال الرسائل النصية وذلك عن طريق كتابة رسائل الكترونية وبثها للغير sms أو بلوتوث أو بالبريد الاكتروني أو عن طريق غرف الدردشة، بأن ينسب شخص الى غيره أفعالا مشينة لابتزاه مثلا، وقد تقع تامة وقد تقف عند حد الشروع.

[١]حجازي. عبد الفتاح بيومي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية ٢٠٠٧م، صـ٤٧.

ومنها استخدام ذاكرة التليفون ونحوه لتخزين المواد غير المشروعة، وقد ترتكب من خلال الكاميرا بتصوير المقاطع الفيديوية أو الصور العادية للضحية في أوضاع غير لائقة للابتزاز أو الترويج للاباحيات.

وقد تتم تلك الجرائم من خلال نشر البرامج العدائية كالفيروسات وبرامج التجسس للاعتداء على خصوصيات الآخرين وأسرارهم العائلية أو التجارية، أو إشعال الفتن الطائفية أو لبث الشائعات، وسرقة الملفات وانتحال الشخصيات.

وتتعدد الأغراض الدافعة لارتكاب الجريمة المعلوماتية، فقد تكون أهدافا مادية كتحقيق الكسب المالي، أو معنوية كالتعلم واكتساب المهارات الذهنية، أو مجرد الانتقام ونحو ذلك.

ومما ينم عن حجم وخطورة الجرائم المعلوماتية ما أفصحت عنه أحد الدراسات من وجود أكثر من ٢٣ مليون عملية هجوم الكترونية صدرت عن ١٢٦ دولة حول العالم على أنظمة الحاسب الآلي كما واجه مستخدمو أجهزة الحاسب الآلي في ٢١٥ دولة في عام ٢٠١٠ ما يزيد على ٣٢ مليون عملية هجوم الكترونية وفقا لاحصائية مستقاة من دراسة لأمن الانترنت خلال الملتقى العلمي لمكافحة الجرائم المعلوماتية لمنتدى

الرياض، وقد كانت المملكة العربية السعودية من أولى الجهات المستهدفة نمن تلك العمليات غير المشروعة حيث كان معدل الانتهاكات بشأنها ٢,٢٧٣٪ من جملة الاعتداءات[١].

ضرورة اللجوء إلى التظلل بمظلة حماية الملكية الفكرية للبرامج المعلوماتية.

إن تطور تقنيات البرمجيات وتنامي شبكة الانترنت وإدخال المعلوماتية إلى جميع النشاطات البشرية قد أدى بدروه إلى تعاظم إنتاج برامج وقواعد البيانات والأعمال الرقمية، بل تطور الأمر حتى ظهر ما يعرف بالاقتصاد الرقمي. فتنامت وصناعة البرمجيات وتم بحث سبل حماية هذا الإنتاج الرقمي، الذي يقوم على الابتكار والجدة.

ومن جهة أخرى تزايدت أعمال التعدي على هذا الإنتاج من خلال النسخ غير المشروع والتحميل من الإنترنت، ونحوها من أعمال التعدي على حقوق أصحاب البرامج وقواعد البيانات والأعمال الرقمية، مما يشكل عائقا أمام ازدهار هذا القطاع وتشجيع الاستثمار فيه.

والحل هو فرض حماية قانونية فعالة، تردع المنتهكين، وتحفظ حقوق المنتجين والمبدعين، وتحفزهم للتطوير، ويلزم لفرض تلك الحماية على تلك الأعمال الرقمية أن

[١] حمودة. عبد الرحمن: مكافحة الجرائم المعلوماتية دراسة تحليلية، الرياض ٢٠٠٩م، صـ١٤.

تتخذ البرامج المعلوماتية صورة في الواقع الملموس، حتى وإن كانت تظهر وتختفي على الشاشة ولا يمكن رؤيتها إلا بالوسيط الإلكتروني، ولا تقف عند حد كونها فكرة ذهنية لم تخرج للواقع. فهي محمية وإن كانت مدمجة ضمن التجهيزات لتشغيله[١].

كما تشمل الحماية أعمال التصميم التحضيرية شريطة توافر عنصر الجدة والابتكار، والتعبير عنه في شكل ما.

وحقوق مؤلف العمل الرقمي تتمثل في حق نِسبة العمل إلى مبتكره، وحق المؤلف في نشر العمل أو إشهار العمل، وحق المؤلف في منع أي تحوير أو تعديل أو تغيير في العمل ضمن شروط معينة، وهو حق محدود جداً في حالة البرامج المعلوماتية، أما حق المؤلف في سحب العمل فلا يمكن سريانه في حالة البرامج المعلوماتية.

وبشأن الحقوق المادية التي تتعلق باستثمار أو استغلال البرنامج المعلوماتي فلمؤلف العمل الرقمي وحده حق نسخ وإعادة إنتاج العمل بشكل دائم أو مؤقت للبرنامج المعلوماتي جزئياً أو كلياً بأية وسيلة كانت وبأي شكل كان، كما له الحق في ترجمة البرنامج وتكييفه وإعادة ترتيبه وكل تعديل أو تحويل أو إعادة إنتاج، مع حفظ حقوقه

[١] عرب، يونس. ثلاث طوائف لجرائم الكمبيوتر وثلاث مجموعات تشريعية لمواجهتها، مجلة حماية الملكية الفكرية، ع٣٠، الربع الثاني، ١٩٩٣. صـ٥٨، محمد: فتحي عبد الهادي. أخلاقيات المعلومات في مراكز المعلومات والمكتبات، العربية ٣٠٠٠، ع١، شتاء٢٠٠٠، ص. ٤٢.

كاملة في النشر والتوزيع والنقل والبيع والتأجير للجمهور للنسخة الأصلية أو المأخوذة عن الأصل.

كما يكون للشخص الذي له الحق في استخدامه صنع نسخة لحفظ هذا البرنامج طالما أنها ضرورية للاستخدام، وله مراقبة طريقة عمل البرنامج أو دراستها أو فحصها، من أجل دون اشتراط موافقة صاحب حق المؤلف، كما أن له حل شيفرة البرنامج أو ترجمة شكل هذه البرمجيات من أجل الحصول على المعلومات اللازمة لتشغيل البرنامج مع برامج معلوماتية أخرى.

وبشأن حماية قواعد البيانات بموجب قانون حقوق المؤلف، فإننا نشير إلى أن قواعد البيانات هي مجموعة أعمال أو بيانات أو عناصر أخرى مستقلة منظمة بطريقة منهجية وممكن للوصول إليها بوسائل إلكترونية أو بأية وسيلة، وهي قد تكون أعمال أدبية أو فنيةّ أو موسيقية أو نصية أو صوتية أو مجموعة صور أو أرقام أو وقائع أو بيانات أو غيرها. فقواعد البيانات هي الوعاء الذي يسمح بحفظ كميات هائلة من المعلومات وإدارتها للجهة التي تضيفها، ومن ثم يكون لهذه الجهة حق الإضافة والتعديل والاسترجاع[١].

[١] تمام: أحمد حسن طه: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ٢٠٠٠م، صـ٨٥.

ولهذا تتعين التفرقة بين قاعدة البيانات، وهي الظرف الذي يحتوي على البيانات، والبيانات نفسها ومنتج أو صانع قاعدة البيانات هو الشخص الذي يقوم بإنشائها، فله منع أي شخص آخر من استخراج وإعادة استعمال محتوى قاعدة البيانات، سواء كان ذلك يهدف ذلك لصنع منتج آخر منافس.

ومن أمثلتها أسماء المواقع فهارسها وصفحاتها ومحركات البحث والرسوم والصور وألعاب الفيديو والوسائط المتعددة.

المبحث الثاني

مهددات الملكية الفكرية في الأمن السيبراني

تحظى الملكية الفكرية اهتماماً بالغاً على كل الأصعدة المحلية والدولية، ويأتي هذا الاهتمام بالتصدي لكل أنواع الاعتداءات والمهددات بشكل عام وفي فضاء الأمن السيبراني بشكل خاص، ويأتي هذا المبحث للحديث عن جملة من التهديدات لمجالات الملكية الفكرية في الأمن السيبراني وفق المطالب التالية.

المطلب الأول

الاعتداءات الخاصة بأمن المعلومات وقيمتها

برزت الثورة المعلوماتية مع بداية القرن العشرين نتيجة للتقدم العلمي والتكنولوجي سيما تقنية الحاسب الآلي والشبكات الإلكترونية، وقديما قيل: يحدث للناس من الأقضية بقدر ما يحدثوا من الفجور، فظهرت جرائم ليست مجرد جرائم تقليدية في ثوب جديد، أو بوسائل مختلفة فحسب بل ظهرت جرائم تمثلت في عمليات الاقتحام والهجوم على الحاسبات والنظم المعلوماتية تخربها وتدمرها وتسرق محتوياتها وتنشر الفيروسات، بالإضافة إلى ظهور الجرائم التقليدية في ثوب معلوماتي كاتصال أفراد العصابات المنظمة لتدبير جرائمهم وكذا جرائم التهريب والمخدرات والاتجار في الرقيق والبغاء

والاتجار في الاسلحة ونحوها. ومن ثم ظهرت العديد من أنواع الاعتداءات بأمن المعلومات وقيمتها التي أثّرت على حقوق مجالات الملكية الفكرية، وتختلف وفقاً لطبيعة الحقوق التي تُهاجمها، وفي هذا المطلب سأتحدث عن تلك الاعتداءات الخاصة بأمن المعلومات وقيمة المعلومات المعالجة آلياً، وذلك في فرعين.

الفرع الأول

الاعتداءات الخاصة بأمن المعلومات المعالجة آلياً

ظل هذا المجال من الأمن حتى اواخر السبعينات معروفا باسم أمن الاتصالات والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بأنه: " المعايير والاجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات".

وفي الثمانينات مع النمو للحاسبات الشخصية بدأت حقبة جديدة من الأمن سميت أمن الحواسيب، والتي حددت بكونها" المعايير والاجراءات التي تضمن سرية

كمال توافر مكونات انظمة المعلومات بما فيها التجهيزات والبرامجيات والمعلومات التي تم معالجتها وتخزينها ونقلها"[١].

وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن السابقين ليعرف هذا النظام بأمن أنظمة المعلومات، الذي يعرف بأنه: "حماية أنظمة المعلومات ضد أي وصول غير مرخص أو تعديل المعلومات أثناء حفظها، أو معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين بما في ذلك جميع الإجراءات الضرورية لكشف توثيق ومواجهة هذه التهديدات[٢].

وتكمن الاعتداءات الخاصة بأمن المعلومات على المعطيات السرية المحمية قانوناً وغير المصرح بتداولها، والبيانات التي تمس الخصوصية.

ويقصد بالخصوصية أو السرية تلك الخصوصية للمعلومات المتعلقة بالعملاء أو بالمنظمة، فهذه المعلومات يتعين أن تكون بعيدة عن وصول غير المصرح لهم بالاطلاع عليها. وتحمى هذه الخصوصيات عن طريق نظام التشفير، الذي يوفر مستوى عالٍ

[١] العريان: محمد علي: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر ٢٠٠٤م، صـ٧٣. حماد: عادل حماد عثمان: حماية المعلومات في التشريع الجنائي السوداني، صـ١٥٦.
[٢] المري: راشد محمد: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية ٢٠١٨م، صـ١٥.

من الأمن للمعلومات مع المحافظة على المرونة في تداول تلك البيانات، كما يحمي السلامة للمعلومات والأنظمة: بحيث يمكن التأكد من عدم تعرضها لأي نوع من التغيير الغير مصرح به، وبعبارة أخرى فإن البيانات لا يمكن أن يحدث لها استحداث أو تغيير أو حذف من غير تصريح، وكذلك تعني أن البيانات المخزنة في أحد أجزاء جداول قواعد البيانات متوافقة مع ما يقابلها من البيانات المخزنة في جزء آخر من قواعد البيانات، ويراعى أن ضمان عناصر أمن المعلومات كلها او بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الافشاء، وليس كل المعلومات في منشأة واحدة بذات الاهمية من حيث الوصول لها او ضمان عدم العبث بها[1].

صور السلوك الإجرامي في الاعتداءات الخاصة بأمن المعلومات المعالجة آلياً:

تتمثل أنماط السلوك الإجرامي في هذا الصدد فيما يلي:

الصـورة الأولى: التنصـت على ما هو مرسـل عن طريق الشـبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

[1] لطفي. محمد حسام محمود: الحماية القانونية لبرامج الحاسب الإلكترونية، دار الثقافة للطباعة والنشر ١٩٨٧م، صـ٧.

أ- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح.

ويشمل ذلك كل ما يرسل عن طريق الشبكة المعلوماتية أو أجهزة الحاسب الآلي، سواء تعلق بالحياة الخاصة أو المسائل المالية أو غيرهما، كالمراسلات الكتابية والصوتية والمكالمات وغيرهما.

والتنصت من نصت، والإنصات: السكوت والاستماع، وأنصت له استمع لحديثه[١]، فهو جريمة سمعية بمعنى أنه يستهدف الأصوات المسموعة المرسلة عبر الشبكة المعلوماتية، أو الموجودة على أحد أجهزة الحاسب الآلي، سواء أكانت أصوات أشخاص أو غيرها.

والتنصت المعلوماتي من جرائم انتهاك الخصوصية والاعتداء على حرمة الأشخاص وخصوصياتهم، والاطلاع غير المصرح به على لمعلومات المخزنة أو المتداولة آليا، ويلزم لقيامها وجود الجاني بيئة المعالجة الآلية للمعلومات[٢].

---

[١] مختار الصحاح: مرجع سابق، صـ٣٥٦، القاموس المحيط: الفيروزآبادي: مجد الدين أبو طاهر محمد بن يعقوب الفيروزآبادى، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالةبإشراف: محمد نعيم العرقسُوسي، نشر: مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت – لبنان ط٨ ١٤٢٦ هـ - ٢٠٠٥ م، صـ١٦١٤.

[٢] العريان. محمد علي: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر ٢٠٠٤م، صـ٧٣.

ويلزم لقيام تلك الجريمة أن يكون الجاني قادرا على السمع ولو لم يكن يفهم اللغة المسموعة، فإن لم يكن قادرا على التسمع لصمم أو لأن المادة المرسلة غير مسموعة فتنتفي هذه الجريمة[١] على نحو لا يمنع من قيام جريمة الاطلاع أو الاعتراض حسب الأحوال.

وقد يقع التنصت عن طريق الهاكرز أو الاختراق، وهو الوصول بطريقة غير مشروعة الى هدف معين عن طريق ثغرات في المنافذ، كالثغرات في نظام الحماية الخاص بالهدف، للتجسس والاستماع أو التسجيل أو تحويل سير البيانات والاستيلاء عليها[٢].

وقد يتم التنصت عن طريق المحاكاة أو انتحال الشخصية للدخول الى النظام، والوصول الى عنوان المرسل أو المرسل إليه والتواصل معه على أنه عنوان مقبول وساري المفعول وقادم من جهاز معين، بينما هو في الحقيقة غير ذلك.

وتستخدم في عمليات التنصت المعلوماتي مكبرات الصوت والميكروفات الصغيرة، كما أن هناك مراكز للتنصت، حيث يقوم قراصنة الحاسب الآلي باستخدام

[١] حماد: عادل حماد عثمان: حماية المعلومات في التشريع الجنائي السوداني، مرجع سابق، صـ١٥٦.
[٢] محمود: عمر: الجرائم المعلوماتية والإلكترونية، مرجع سابق، صـ٥١٩.

البرامج التي تتيح لهم التجسس على المعلومات الخاصة بالشركات والمؤسسات التجارية العاملة على شبكة الانترنت، للحصول على ما يريدونه من معلومات.

ولا يمنع من قيام تلك الجريمة أن يكون الجاني له الحق في تلقي واستقبال البيانات، إذا قام باستعمالها في غير الأغراض المسموح بها[١].

ولا تتحقق جريمة التنصت إذا أعلن ذو الشأن رضاه بهذا التنصت أو أذن فيه، أو كانت تلك المواد منشورة بصورة علنية تمكن الجميع من الاطلاع عليها وسماعها.

ب–التقاط ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح.

فالواقع أن المعلومات تظهر على شاشة الحاسب، كما أنها مخزنة في ذاكرة داخلية أو خارجية، وكذا هي في حركة مستمرة مما يجعلها مهددة في أي لحظة بالالتقاط أو التسجيل والنسخ غير المشروع، مما يقتضي ضرورة تفعيل تأمين الدخول الى المراكز المعلوماتية للحفاظ على البث المعلوماتي.

وقد عرفت المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي، الالتقاط بأنه: "مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح".

[١] العريان. محمد علي: الجرائم المعلوماتية، مرجع سابق، صـ٧٥.

ويستوي أن يتم الالتقاط والاعتراض عن طريق الدخول إلى الشبكة أو دون الدخول، كما في حالة التقاط الإشارات التي يحدثها جهاز الكتروني دون الحاجة الى الدخول المباشر الى الشبكة[١].

ويستوي أن ينصب الالتقاط على المعلومات أو التوقيع السري أو الأرقام التشفيرية ونحو ذلك. وهناك طرائق عديدة يمكن من خلالها التقاط المعلومات ومنها:

أ- الالتقاط الذهني للمعلومات، وذلك عن طريق المشاهدة أو الاستماع لما يصدر عن الأجهزة.

ب- التقاط المعلومات الموجودة بين الحاسب والنهاية الطرفية، وذلك من خلال توصيل تحويلة الى الطرف القائم بالتجسس ترسل إشارات الكترونية مكبرة، تمثل المعلومات المسروقة.

ج- التقاط الذبذبات الصادرة عن هوائي مستقبل لإرسال القمر الصناعي.

د- التوصيل المباشر على خط تليفوني عن طريق وضع مركز تنصت يسجل كل الاتصالات، أو بواسطة ميكروفونات صغيرة.

[١]قورة. نائلة عادل: جرائم الحاسب الآلي الاقتصادية، مرجع سابق، صـ٣٢١.

هـ – التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي وترجمتها عن طريق أجهزة معينة الى معلومات.

ز – التدخل عن طريق نقاط الاتصال[١].

وهناك وسائل تقنية لحماية سرية المعلومات والاتصالات، ومنها تشفير المعلومات المرسلة حتى لا يتمكن من الاطلاع عليها سوى المصرح له بذلك.

والالتقاط أشـــبه ما يكون بالســـرقة حيث إن الجاني يقوم بالدخول إلى محل لا يسمح له بالدخول إليه ثم يسرق أو يستولي على ما به من معلومات قابلة للتملك ولها قيمتها الاقتصادية من خلال نسخها على مستندات أو شرائط أو حتى مجرد الاحتفاظ بها في الذاكرة، وسواء حصل على تلك المعلومات والبيانات خلسة أو عنوة.

ت–اعتراض ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح.

[١]الشوا. محمد سامي: ثورة المعلومات وانعكاساتها على قانون العقوبات، صـ٦٩.

والاعتراض يقتضي وجود اتصال بين طرفين أو أكثر، ثم يحصل تفريع سري خفي أو تفريعة تقدمها شركات التليفونات، تقوم باعتراض الإشارة فحسب دون تفكيكها وتحليلها، لأن التفكيك والتحليل يدخل في نطاق الالتقاط[١].

وغالبا ما تتم هذه الأفعال من خلال الهاكرز أو المتسلل، وهم أشخاص بارعون في استخدام الوسائل الحديثة لاختراق حسابات الآخرين، بهدف التجسس أو التخريب والتدمير أو السرقة أو مجرد الاطلاع على المعلومات الشخصية والمالية، أو بدافع الفضول والتحدي لإجراءات أمن المعلومات، والأنظمة الأمنية للحاسب، والبحث عن الثغرات الأمنية في النظام محل الاعتداء[٢].

الصورة الثانية: الدخول غير المشروع أو غير المصرح به (الاختراق).

تولي الأنظمة اتجاه الجرائم المعلوماتية المواقع الإلكترونية والصفحات والمعلومات الإلكترونية أهمية في نصوصها، لذا فإنها تجرم مجرد الدخول غير المشروع الى تلك الكيانات كما تجرم الاعتداء على محتوياتها بالتدمير أو التزوير، أو التدخل بأي شكل غير مشروع كالنصب والاحتيال الالكتروني؛ ومن ناحية أخرى تهتم المواقع والأنظمة

[١]محمود: عمر: الجرائم المعلوماتية، مرجع سابق، صـ٥٢١.
[٢]عبد الرحمن. محمد جلال: الجرائم الالكترونية: مرجع سابق، صـ١٤٠.

الإلكترونية والمؤسسات المعلوماتية بالوقوف ضد تلك التعديات من خلال الحوائط النارية والتقنيات والبرامج المختلفة.

وجريمة الدخول غير المشروع جريمة بسيطة يكفي لقيامها ارتكاب فعل واحد، والجريمة البسيطة تختلف عن جرائم الاعتياد التي لا يكفي لقيامها ارتكاب فعل واحد بل تتكون من تكرار الفعل والاعتياد عليه، وحالتئذ يكون الركن المادي المكون لجريمة الاعتياد هو ركن الاعتياد ذاته[١].

وتقوم جريمة الدخول غير المشروع سواء كان هذا الدخول وقتيا او مستمرا ومتجددا، فلا يلزم لقيامها أن يكون الدخول متجددا ومتتابعا، وسيأتي الكلام عن جريمة البقاء غير المشروع، وهذه الأخيرة قد تكون متتابعة الأفعال وذلك إذا تكونت من دخول غير مشروع وتلاه بقاء غير مشروع، وقد تأتي في شكل أولي لا تتابع فيه كما في حالة الدخول المصرح به مع استمرار البقاء غير المشروع.

كما أن جريمة الدخول غير المصرح به من الجرائم العمدية التي يتخذ الركن المعنوي فيها صورة القصد الجنائي أي ارادة الفعل والنتيجة وتوافر كافة العناصر

[١] حجازي:عبد الفتاح بيومي: جرائم الكمبيوتر والانترنت، مرجع سابق، صـ٣٨.

النظامية المتطلبة لقيام الجريمة، وبناء على ذلك فلو كان الدخول غير المشروع قد تم بغير العمد وانما بطريق الخطأ المتمثل في الاهمال والرعونة وعدم الاحتياط وعدم الاحتراز فلا تقوم جريمة الدخول، وآية ذلك أن يخرج من النطاق غير المرخص له بدخوله فور علمه بعدم مشروعية الدخول، لكن بقاءه مع علمه يعد قرينة على القصد الجنائي المقرر للعمدية([1]).

كما ينبغي الاشارة الى أن جريمة الدخول غير المصرح به تكون جريمة عادية وجريمة سياسية، وتتحقق هذه الأخيرة حال وقوع الاعتداء على النظام السياسي للدولة كشكل الدولة ونظامها السياسي والحقوق الأساسية للأفراد، ومن ثم فهي أخطر في آثارها من الجريمة العادية، مما يترتب عليه أن تكون عقوباتها أشد وأنكى.

ويتمثل الركن المادي لجريمة الدخول غير يعني المظاهر الخارجية المكونة لماديات الجريمة، أي الشكل الذي تظهر فيه الجريمة الى العالم الخارجي المحيط بالجاني، والكيان الملموس الذي يظهر على الأجهزة والمواقع ونحوها من الكيانات المعلوماتية، وهذا الركن هو الذي يبرر تدخل النظام بالتجريم، فلو انعدم وجوده فليس

[1] الرومي: محمد أمين: جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية ٢٠٠٤م، صـ٢٦.

ثمة جريمة، إذ لا جريمة دون سلوك مادي، فالإثبات للجريمة يقع على الماديات، لأن الماديات هي التي يمكن اثباتها.

والركن المادي لأي جريمة يتكون من السلوك الاجرامي والنتيجة التي يسفر عنها هذا السلوك والسببية بينهما، فمتى اكتملت هذه العناصر كانت الجريمة تامة ووجب توقيع العقاب على مرتكبها، أما إذا لم تتحقق النتيجة وكان عدم التحقق راجعا الى أِباب لا دخل لإرادة الجاني فيها فحالتئذ يقف الفعل عند حد الشروع ويعاقب مقترف الفعل بناء على هذا الوصف وهو الشروع إن كان ثمة عقاب على الشروع([1]).

كما أن السلوك الإجرامي يقدم عليه الجاني بمفرده وقد يستعين بمساهمين في ارتكاب السلوك الاجرامي بأي من صور المساهمة، وقد تكون المساهمة بأدوار رئيسة وحالتئذ يكون كل فاعل مساهم أصلي في الجريمة، وقد تكون بأدوار ثانوية وحالتئذ يكون كل مساهم تبعي شريك مع الفاعل الأصلي([2]).

[1] أبو عامر: محمد زكي: دراسة علم الإجرام والعقاب، الدار الجامعية بيروت ١٩٨٢م، ص١٧.
[2] إبراهيم: خالد محمود: الجرائم المعلوماتية، مرجع سابق، صـ٥٤.

ويتم الاختراق غالبا عن طرق الكترونية وذلك باستخدام كلمة سر حقيقية وصحيحة لا يحق للجاني استخدامها؛ وقد يتم باستخدام برامج أو شفرة خاصة، سواء من خلال التليفون أو الكمبيوتر أو غيرهما من الأجهزة.

وقد يقف الأمر عند مجرد تشغيل الجهاز المقفل دون موافقة صاحبه والوصول الى الملفات الموجودة بداخله، لكن إن كان نظام المعالجة مقفل فلا تتم جريمة الدخول غير المشروع وإن قامت جريمة الشروع في الدخول.

وقد يقوم الجاني بالدخول من حاسبه الشخصي الى حسابات أخرى ويطلع على ما فيها من معلومات مع عدم وجود دائرة مشتركة بينهما؛ وقد يتمثل الدخول في استعمال كارت تشغيل أو تليفون لسحب مبالغ الية من بنك. وقد يتم الدخول بطرق مادية وذلك باقتحام خزانة الملفات وسرقة الهوية الشخصية.

وقد يكون المتهم مسموحا له بالدخول في حدود معينة بأن يحق له الدخول الى أجزاء معينة من النظام دون غيرها، فإذا به يتجاوز الحدود المسموحة ويتجول داخل النظام المعلوماتي بأكمله أو يدخل الى نطاقات لم يسمح له بدخولها، كما هي الحال في موظف الشؤون الإدارية بالاطلاع على البريد الصادر والوارد والمتابعة في حدود

معينة دون أن يكون مسموحا له بالدخول الى النظام المالي، فإن تجاوز الحد المسموح له وتعدى الى غيره كان مسؤولا ولو كان النطاق الممنوع من ولوجه غير محمي([1]).

ويتحقق فعل الدخول المحظور متى ولج الجاني الى الكيان المعلوماتي أو بعض أجزائه، ولا أهمية بعد ذلك للباعث على الدخول، فقد يكون لمجرد التسليةا، وقد يكون بهدف التلاعب والعبث كالقيام بإضافة معطيات جديدة على النظام المعلوماتي القائم، سواء أكانت الدعامة التي أضيفت اليها المعلومات خالية أم مشغولة بالمعلومات، ويستوي أن يقوم بها أي شخص، من خارج النظام المعلوماتي أو من داخله وهو الغالب كالموظف المسؤول عن المحاسبة مثلا[٢].

ويوجد هذا النمط من أنماط الإجرام المعلوماتي بشأن بطاقات السحب الممغنطة، كأن يقوم شخص بسرقتها أو التقاطها بعد فقد صاحبها لها، أو تزويرها، واستخدامها ممن لا يشرع له استخدامها، وكذا بإدخال الفيروسات ونحوها.

ويتحدد النطاق المكاني للدخول غير المشروع بالتسلل الى داخل النظام، كما يتحدد النطاق الزماني بتجاوز حدود الفترة الزمنية المسموح بها للدخول.

[1] حسني. محمود نجيب: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ط١٩٨٩/٦م، صـ٨٨٠.
[٢]حجازي. عبد الفتاح بيومي: جرائم الكمبيوتر والانترنت، مرجع سابق، صـ٣٨.

الفرع الثاني

الاعتداءات الخاصة بقيمة المعلومات المعالجة آلياً

يمكن تقسيمها إلى نوعين منها الواقعة على ذات المعلومات كجرائم الإتلاف والتشويه والتخريب، والسطو على مجالات المليكة الفكرية.

ومن صور الاعتداءات في هذا الصدد ما يلي([1]).

١- تغيير تصاميم الموقع.

حيث يقوم الجاني باختراق الموقع لتشويهه وتغيير تصاميمه، كأن يغير تصميم الصفحة الرئيسية متحديا الإجراءات الأمنية للشبكة بكسر نظم الحماية، كأن يتم اختراق صفحة رسمية ووضع علم دولة أخرى عليها.

٢- إتلاف الموقع.

ومعنى الإتلاف إخراج الشيء من أن يكون منتفعا به منفعة مطلوبة منه عادة، عن طريق قيام الجاني بتعييبه على نحو يفقده قيمته الكلية أو الجزئية، ويجعله غير

[1] زين الدين: بلال أمين: جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، ٢٠٠٨م، صـ٥٧. خالد ممدوح ابراهيم: الجرائم المعلوماتية، مرجع سابق، صـ٣٨٣

صـــالح للاســـتعمال. والإتلاف المعلوماتي يســـتهدف إتلاف أو محو البرامج أو المعلومات والبيانات ذاتها، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

وإتلاف المواقع أو تدميرها يتم عن طريق الدخول غير المشروع الى نقطة ارتباط شـبكية بهدف تخريب النظام، وتسـتخدم في إتلاف المواقع وسـائل عديدة، كأن يقوم الجاني بضخ آلاف الرسائل الإلكترونية الى الموقع المستهدف، للضغط على السعة التخزينية للموقع، مما يؤدي الى تفجير الموقع وانتقال المعلومات المخزنة إلى جهاز الجاني[١]، ويستوي أن يكون الإتلاف كليا أو جزئيا.

ويراعى أن البرامج والمعلومات المســـجلة على دعامات مادية منفصـــلة عن الحاســـب الآلي يكون التعدي عليها من باب إتلاف منقولات الغير، أو المصـــنفات الأدبية له حسب تكييفها، أما البرامج الموجودة على جهاز الحاسب فأن التعدي عليها يكون من باب التعدي المعلوماتي.

ويأخذ الإتلاف المعلوماتي صوراً متعددة، فقد يكون بـ:

محو البيانات الكترونيا بتدميرها كليا أو جزئيا.

[١] إبراهيم: خالد ممدوح: الجرائم المعلوماتية، مرجع سابق، صـ٣٨٣.

ويحصـــل المحو أو الحذف أو الإتلاف أو التدمير بإزالة جزء من المعلومات المسجلة على الحاسب ونحوه. وهي تعني البرامج الخبيثة التي تستخدم لإتلاف أنظمة المعالجة الألية للمعلومات، وهي عبارة عن برامج مشـفرة ومصـممة على نحو يجعلها قادرة على التكاثر والانتشـار من مجال الى آخر، بواسـطة الأقراص أو عبر الشـبكة، ولو في أي مكان في العالم، وتسـتهدف الفيروسـات المعلومات المخزنة على الأجهزة المستهدفة لتغييرها أو حذفها أو سرقتها أو نقلها، أو تدميرها كليا أو جزئيا أو تحريفها.

تعديل البيانات أو تغيير مسارها وطرق انتقالها.

ويكون التعديل أو التغيير أو التزوير بتغيير المعطيات الموجودة داخل النظام واســـتبدالها بأخرى، أو بإدخال بيانات غير مســـموح لهم بإدخالها في نظم معالجة البيانات مما يؤدي الى التشـــويش على البيانات الموجودة. ويســـتخدم لذلك برامج متخصـصـة وقنابل وفيروسـات معلوماتية كحصـان طروادة وفيروس الدودة وهو عبارة عن برنامج معلوماتي له قدرة عالية على تعطيل وإيقاف الحاســب الآلي كاملا[١]. ولا تقف هذه الصور عند حد معين بل هي متجددة وفقا لطبيعة النظام المعلوماتي.

[١]المهيري. خالد: جرائم الكمبيوتر والانترنت والتجارة الإلكترونية، ط٢ / ٢٠٠٤م، صـ٥٧٠، د. أحد حسام طه تمام: جرائم الحاسب الآلي، دار النهضة العربية، صـ٣٦٠.

٣- شغل عنوان الموقع.

وهو من قبيل التعطيل للموقع، أو التعييب، وعن طريق شغل عنوان الموقع يبدو ظاهرا لأي مستخدم أن الموقع مشغول لكثرة الزائرين، في حين أنه إشغال وهمي بهدف الحجب عن الجمهور ومنعهم من الوصول إليه.

ويستوي في الإشغال ونحوه أن يتم عن طريق الشبكة المعلوماتية الدولية أو عن طريق شبكة محلية، أو بأي وسيلة من وسائل تقنية المعلومات لأن الوسائل في هذا الباب متجددة ولا تقف عند حصر(١).

ومن وقع عليه التزام بالحماية أو التأمين للموقع، وتم الاختراق أو الدخول غير المشروع فإن الملتزم بتلك الحماية ونحوها يكون مسؤولا، وهو التزام بتحقيق نتيجة لا مجرد بذل عناية.

لذا تعد برامج التأمين لحماية معلومات المنظمة أو المنشأة المعنية لمنع أو تقليل المخاطر التي قد تؤثر على توافر المعلومات وسريتها وسلامتها، ذلك أن الأضرار التي تنجم عن قصور وفشل إجراءات الأمن تؤدي إلى خسارة مباشرة تعود بالضرر علي

١ سليم د طارق عبد الوهاب: الجرائم المرتكبة بواسطة الانترنت وسيل مكافحتها، تونس١٩٩٧م، ص١٥.

المنظمة المعنية. ومن أهم تلك الخسائر خسارة الاعتمادات أو الملكية الفكرية؛ وكذا خسارة الرغبة في العمل الكفء المتسم بالجودة العالية للعملاء أو الموردين. لذا تصبح مهمة حماية وتأمين البيانات والمعلومات لها الأولوية القصوى والمطلقة في تخطيط وعمل نظم المعلومات على كافة أنواعها وتوجهاتها.

الجدير بالذكر أن حماية الملكية الفكرية هي المرجع والأساس القانوني في حماية برامج الحاسوب والبيانات وبرامج الحاسوب لأن هذه البرامج لا تخرج عن كونها إنتاجات فكرية، وعلى الرغم من ذلك فقد جرى العمل على إيجاد أنظمة خاصة تحمي هذه البرامج المعلوماتية، دون الوقوف عند حد أنظمة حماية حق المؤلف، فعلى الرغم من أن قوانين حماية حق المؤلف وحقوق الملكية الفكرية والصناعية قد تلبي حاجة حمايةبرامج الحاسوب والبرمجيات، إلا أن تخصيص أنظمة لحماية هذه الحقوق في مجال الفضاءالسيبراني هو الأكمل، لأن التخصيص يراعي مختلف الحالات التي تنفرد فيها حقوق الملكية الفكرية في الفضاء السيبراني([1]).

فحماية تلك البرامج من خلال حقوق الملكية الفكرية يحفظ حق إعادة الإنتاج من خلال إعطاء الحق الحصري بالترخيص أو منعه بشكل مباشر أو غير مباشر، وإعطاء

[1] الجنيهي: منير محمد: جرائم الانترنت والحاسب الآلي ووسائل مكافحتها – دار الفكر الجامعي الإسكندرية ٢٠٠٥م، ص٤٢. المشهداني: أكرم عبد الرزاق: القانون والجرائم التكنلوجية بغداد ٢٠٠١م، ص٢٠.

المؤلفين الحق بترخيص أو منعترخيص إيصال الأعمال إلى الجمهور سلكياً أو لاسلكياً، كما يحفظ حق التوزيع بإعطاء الحق للمؤلفين بترخيص أو منع ترخيص توزيع أعمالهم. كما توفر الحماية القانونية ضد الاستعمال غير المشروع لحقإدارة المعلومات([1]).

المطلب الثاني

الاعتداءات الخاصة بحقوق الملكية الأدبية والفكرية لبرامج الحاسب ونظمه

يتناول هذا المطلب بيان الاعتداءات المتعلقة بالنصب والاحتيال في عالم النشر، وكذا الاعتداءات المتعلقة بالحصول على مال الغير عن طريق الغش المعلوماتي (بطاقات الائتمان ونحوها)، وذلك من خلال بيان صور هذه الاعتداءات والتعريج على بيان أركانها، وذلك في الفرعين التاليين:

[1] ابراهيم. خالد ممدوح: أمن الجريمة الالكترونية، الدار الجامعية للنشر ٢٠٠٨م، صـ٧١، الشوابكة: محمد أمين: جرائم الحاسوب والانترنت مرجع سابق، صـ٣٠.

الفرع الأول

الاعتداءات المتعلقة بالنصب والاحتيال في عالم النشر

ويراد بالنصب المعلوماتي هو سلوك طرق احتيالية عبر الوسائل الإلكترونية بغية الحصول على مال أو ما في حكمه.

حيث تقوم هذه الجريمة كغيرها من الجرائم على ركنين مادي ومعنوي؛ ويتمثل الركن المادي في الوسائل التي يتخذها الجاني في سبيل تحقيق النتيجة الاجرامية التي يرمي الى تحقيقها ليستولي لنفسه أو لغيره على مال منقول في حيازة الغير أو على سند، أو توقيع هذا السند، وقد أشارت المادة محل الشرح الى جانب من تلك الوسائل بقولها: "وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة".

أما الركن المعنوي فيقوم وفقا للمادة محل الشرح على قصد عام وقصد خاص، فالقصد العام هو علم الجاني بأنه يأتي أعمالا وادعاءات مكذوبة تشكل مجافاة للحقيقة وتغييرا لها، وأن تتجه ارادته الى ارتكاب السلوك الاجرامي وهو سلب مال الغير ونحوه من ماديات الجريمة المقررة في المادة محل الشرح، وأن يعلم أن هذه الوسائل من

شأنها خداع المجني عليه وحمله على تسليم ماله، وأن يتوافر له القصد المعاصر وقت الاستيلاء أو التلاعب، أما القصد اللاحق فلا عبرة به([1]).

ومن صور الاعتداء على الأعمال الإلكترونية النسخ غير الشرعي، وسرقة المعلومات، وسرقة البرامج، إضافة إلى التدمير والإتلاف ونحوها.

[1] رمضان: عمر السعيد: شرح قانون العقوبات الاتحادية لدولة الإمارات العربية المتحدة – القسم الخاص، دار النهضة العربية، القاهرة ١٩٨٦م، ص٤٠٨.

الفرع الثاني

الاعتداءات المتعلقة بالحصول على مال الغير عن طريق الغش المعلوماتي (بطاقات الائتمان ونحوها)

تتنوع صور الاعتداء على تلك البطاقات ونحوها حيث يتصور استخدامها من قبل غير صاحب الحق بعد سرقتها أو سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات.

فهناك جرائم معلوماتية تستهدف مراكز معالجة البيانات والمعلومات المختزنة على أجهزة الحاسوب لاستخدامها بطريقة غير مشروعة، كالولوج الى أحد الأنظمة للحصول على أرقام بطاقات الائتمان ذات الدفع الالكتروني للاستيلاء على أرقامها وشفرتها وتقليدها للحصول على مبالغ من حساب مالكيها(١). أو من خلال استخدام بطاقات الدفع الالكتروني المزورة، حيث يقوم المجرم المعلوماتي بتقليد برامج التشغيل، أو الحصول على هذه الأرقام والتقاطها عبر قنوات الانترنت واستخدامها، حيث يقوم العميل بالدخول الى موقع التاجر على الشبكة المعلوماتية ويشتري السلع ثم يقدم

(١)الصغير. جميل عبد الباقي: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ٢٠٠١م، صـ١٧، علي. عبد الله حسين: حماية المعلومات المخزنة على الحاسب الآلي، رسالة دكتوراه من جامعة عين شمس ٢٠٠١م، صـ٥٠.

بطاقة الائتمان التي زورها، مما يتعين معه وضع حماية فاعلة لتلك البرامج والبطاقات وحمايتها من الدخول غير المصرح وفك شفرتها وتقليدها.

وتقع تلك الاعتداءات على ما تمثله المعلومات والبيانات المعالجة آليا، والتي تستهدف الحصول على مال الغير شرعي عن طريق الغش والنصب والاحتيال بالحاسب الآلي (كالتعدي على بطاقات الائتمان).

فقد ترتب على شيوع التعاملات الإلكترونية ضرورة إجراء التحويلات والمبادلات المالية حول العالم من خلال البطاقات الائتمانية ونحوها، وهذا وإن سهل المعاملات إلا أن له مخاطره التي تكمن في إمكانية التلاعب في البيانات المخزنة في الحاسوب ونحوها، وإجراء تحويلات للأرصدة أو لبعض منها، بمجرد الوصول الى كلمة المرور الخاصة بالحساب المجني عليه.

ويحصل المجرم المعلوماتي على كلمة المرور الخاصة بالمجني عليه بالتقاطها أثناء التواجد في النظام المعلوماتي، سواء أكان عاملا في مجال إدخال البيانات، أو متواجدا على الشبكة أثناء تبادل تلك المعلومات، أو من خلال البرامج التي تسرق كلمات المرور.

وتقوم هذه الجريمة على عدد من أشكال التنكر والخفاء والتعمية التي تعمل على خداع الطرف الآخر وجعله يتقبل المعلومات الخاطئة أو المزيفة، ومن ذلك سرقة هوية شخص آخر واستخدام اسمه أو رقمه الوطني أو بطاقته الائتمانية أو أرقام حساباته ليقوم بالسحب النقدي أو تحويل مبالغ مالية أو تسجيل مشتريات على بطاقة الائتمانات أو تحرير شيكات أو نحو ذلك؛ وفي هذه الحالات لا تتوف الجريمة عند مجرد الخسارة المالية بل تتعدى الى الجانب المعنوي الذي يشمل الاطلاع على حسابات ومعلومات الضحية.

ويشتمل الركن المادي لهذه الجريمة على عناصر ثلاثة هي:

١- استخدام الجاني لوسائل الخداع والتدليس المنصوص عليها على سبيل الحصر، وهي الاحتيال واستخدام اسم كاذب وانتحال صفة غير حقيقية.

٢- نتيجة إجرامية أو أثر للنشاط الإجرامي يتمثل في تسليم المال المنقول الى الجاني.

٣- علاقة السببية بين السلوك والنتيجة.

طرق الاستيلاء على المال المنقول.

يتم الاســـتيلاء على المال المنقول من خلال عدة طرق أوردها النظام([1])وهي الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

أولا: الاحتيال.

والاحتيال هو: كل تظاهر أو إيحاء يكون صالحا لإيقاع المجني عليه في الغلط بطريقة تؤدي الى الاقتناع المباشـــر بالمظهر المادي الخارجي، ويكون المجني عليه هو: من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله[٢].

ومن أســـاليب الاحتيال أن يقنعه بوجود مشـــاريع وهمية وكاذبة، أو يعرض له مشروعا حقيقا ويقنعه بأرباح وهمية، أو قيام محتالين بإنشاء تأمينات بنكية وهمية، أو نشـر وإعلان مواقع تتعلق بتجارة سـلع أو تقديم خدمات وهمية، أو يوهمه بوجود سـند دين غير صحيح أو سند مخالفة مزور ونحو ذلك؛ فيتصيدون أموال الناس عن طريق

[1] نصت المادة الرابعة من نظام مكافحة جرائم المعلوماتية على أنه: يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: ١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة. ٢- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

[٢] المغايرة: علاء الدين منصور: الأوجه الحديثة للجرائم المعلوماتية، رسالة ماجستير قدمت لجامعة الحكمة بيروت ٢٠٠٠م، صـ٣١.

وســائل الدفع المختلفة والتي من أهمها بطاقات الائتمان، وقد يســتغل موظفو البنوك والشركات النظام المعلوماتي لتلك المؤسسات للوصول الى الكسب المالي عن طريق عقد صفقات زائفة والعبث بأنظمة المعلومات.

وقد يحصـــل المجرم المعلوماتي على هوية المســـتخدم الحقيقي للجهاز بطريق غير مشروع ويتعامل مع الجهاز على أنه المستخدم الحقيقي حتى يحصل على الشفرة الخاصــة بالتشـغيل ويقوم بعملية تحويل الأموال والاسـتيلاء عليها بالاحتيال. والتحايل يقع على الشخص الطبيعي والشخص المعنوي[١].

وهناك برامج تعمل على خصـــم مبالغ قليلة القيمة من حســـابات الفوائد على الودائع المصرفية، وذلك بإغفال الكسور العشرية فقط، حيث يتحول الفارق مباشرة الى حساب الجاني، ورغم ضـخامة المحصـلة، إلا أنه يصـعب اكتشـافها لأنها تعتمد على التكرار الآلي لمعالجة معينة، مع ضـآلة المبلغ المخصـوم من كل حسـاب على نحو

[١]قشقوش. هدى: جرائم الحاسب الالكتروني، مرجع سابق، صـ١٣٣. الصغير. جميل عبد الباقي: الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠١م، ص١٣ وما بعدها.

يصـــعب معه تنبه العميل إليه[١].ومن أشـــهر وســـائل الاحتيال تصـــميم برامج تقوم بعمليات التحويل الآلي من حساب لآخر.

وصـــدر تقرير عن إدارة العدالة الأمريكية عام ١٩٨٢م بعنوان جرائم الحاســـب الآلي نظم التحويل الالكتروني للأموال([٢]) ومن هذه الوسائل:

١- التلاعب في المكونات المادية لنظم التحويل الالكتروني للأموال، ويتضـــمن ذلك اســـتعمال خطوط الاتصـــال لخلق أو تدمير البيانات أو الطلبات الخاصـــة بعمليات التحويل.

٢- اســـتعمال البرامج الخاصـــة بنظم التحويل الالكتروني للأموال والتلاعب بها بغرض البدء في إجراء عملية تحويل غير مشروعة أو بغرض إخفائها.

٣- التلاعب عن طريق إصدار بطاقات ائتمان مزدوجة.

٤- استخدام بطاقة شخص آخر لسحب مبالغ نقدية من الرصيد الخاص بصاحب البطاقة.

[١]عبد الرحمن. محمد جلال: الجرائم الإلكترونية، مرجع سابق، صـ٢٦٥. رمضان: مدحت، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص١٧

[٢]العريان: محمد علي: الجرائم المعلوماتية – كلية الحقوق – جامعة الإسكندرية – دار الجامعة الجديدة للنشر -: عام ٢٠٠٤ – ص٧٤.

٥- استخدام أسلوب تقليدي في ارتكاب الجريمة مثل كسر ماكينة الصرف الآلي وسرقة ما بها من أموال.

ويشترط في الطرق الاحتيالية أن تحتف وتقترن بادعاءات كاذبة من شأنها خداع المجني عليه وحمله على تسليم المال المنقول أو السند أو التوقيع أو الغائه أو اتلافه أو تعديله، كما يشترط أن تكون تلك الادعاءات مدعومة بمظاهر خارجية من شأنها ايهام المجني عليه وايقاعه في شرك الاحتيال؛ ومن تلك الأعمال الاحتيالية التلاعب في المعلومات واخراجها بشكل غير صحيح، وكذا استخدام الفيروسات للاضرار بذاكرة الحاسوب على نحو يغير أو يحرف في البيانات.

الوسائل الفنية للتحويل الالكتروني للأموال.

يتم تحويل الأموال إلكترونيا عبر وسائل منها ما يلي:

١- استخدام برامج معدة لتنفيذ الاختلاس.

٢- التحويل المباشر للأرصدة.

التلاعب بالبطاقات المالية.

حيث تتنوع صور الاعتداء على تلك البطاقات حيث يتصور استخدامها من قبل غير صاحب الحق بعد سرقتها أو سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات. وهناك جريمة الاستيلاء على النقود الإلكترونية

ثانيا: اتخاذ اسم كاذب.

من الطرق التي يسلكها المجرم المعلوماتي للاستيلاء على المال المنقول اتخاذ اسم كاذب، ويشمل ذلك اتخاذ اسم فرد أو اتخاذ اسم موقع ونحو ذلك من البيانات الكاذبة التي تعمل على إيهام الحاسب والاحتيال عليه فيسلم المال([1]).

فيلجأ المجرم المعلوماتي الى جمع المعلومات الشخصية عن المجني عليه، وينتحل شخصيته ليستولي على الرصيد البنكي، أو يسحب من بطاقته الائتمانية[2] وقد يحوز البطاقة الائتمانية ورقمها السري بالفقد أو السرقة ويستعملها على أساس أنه صاحبها.

[1] رستم:هشام محمد فريد: قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة ١٩٩٢م، صـ٤٢.
[2] الصغير. جميل عبد الباقي: الانترنت والقانون الجنائي، دار النهضة العربية ٢٠٠٢م، صـ٣٤.

وقد ينشئ المجرم المعلوماتي موقعا وهميا على الشبكة على غرار الشركات والمؤسسات الفعلية، بحيث يظهر في صورة الموقع الفعلي لمقدم الخدمة.

ثالثا: انتحال صفة غير صحيحة([1]).

من الطرق التي يسلكها المجرم المعلوماتي للاستيلاء على المال المنقول انتحال صفة غير صحيحة. وهذه الجريمة كسابقتها من جرائم النصب أو التزوير المستحدثة.

فعلى سبيل المثال تستخدم البنوك والمؤسسات المالية الشبكة العالمية في تعاملاتها المالية، ويتم دخول العملاء على صفحة المؤسسة وإبرام التعامل معها، وتظل تلك الطرق في التعامل عرضة لانتهاك المخربين حيث يعملون على انتحال صفة المستخدم الشرعي والتصرف على أساس أنه صاحب الهوية على خلاف الحقيقة.

وانتحال المواقع الإلكترونية وتحويل الاتصالات من على الموقع الأصلي إلى المزيف يتم من خلال برامج تصمم لهذا الهدف، وتؤدي الى انتقال كافة المعلومات والمحررات الى سيطرة من قام بانتحال الموقع الالكتروني.

[1] داود: حسن طاهر: جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠، صـ٢٣٣.

ومن أمثلة ذلك أن يقوم شخص بالدخول على الحاسب الآلي الخاص بغيره، وقام بإنجاز تصرف معين من خلال استخدام البرامج الخاصة بصاحب الحاسوب، مما أدى إلى إتمام معاملة أو إبرام تصرف بشكل غير مطلوب أو مخالف للحقيقة.

ومن الصور الاستيلاء على البطاقة الائتمانية لشخص فقدها أو بالسرقة منه، مدعيا أنها له، ثم يقوم بسحب مبالغ مالية منتحلا صفة الغير.

- **انتحال شخصية الفرد.**

ويتم ذلك من خلال تجميع المعلومات والبيانات عن الشخص المجني عليه، كأن يقوم المجرم بالإعلان عن جائزة قيمة لمن يدخل الى الموقع ويقوم بالاشتراك فيه، ودفع رسوم رمزية لجهة خيرية مثلا، وهذا يقتضي الإفصاح عن بعض البيانات الشخصية، كالاسم والعنوان ورقم بطاقة الائتمان لخصم المبلغ المطلوب، فيقوم الجاني بالاستيلاء على الرصيد البنكي أو السحب من البطاقة الائتمانية من خلال البرامج الاحتيالية([1]).

[1] علي: محمد محرم محمد: جريمة النصب والإحتيال والتجارة الالكترونية القاهرة ١٩٩٨م، ص٨، مكي: محمد عبد الحميد: الاحتيال في قانون العقوبات – دراسة مقارنة – رسالة دكتوراه – جامعة القاهرة، ١٩٨٨م، صـ١٨٣.

ويتم الاحتيال عادة عن طريق سرقة أو تخمين الأسماء وكلمات المرور، وعندما ينتحل شخص شخصية غيره فإنه يستطيع أن يفعل ما يفعله صاحب الشخصية الفعلية، ويمكن للمحتال المنتحل لصفة غيره أن يؤذي صاحب النظام بإرسال رسائل سيئة باسمه أو يدمر سمعته المالية أو الشخصية.

- انتحال شخصية الموقع.

وهو أشد خطورة من انتحال شخصية الفرد، كأن يقوم المجرم المعلوماتي باختراق الموقع المجني عليه، ثم يوم بتصميم البرنامج الخاص به، ويضعه على صفحة موقعه مما يؤدي الى توجه الباحث عن الموقع الى الموقع المزور بمجرد كتابة الاسم على محرك البحث([1]).

[1] المناعسة: أسامة أحمد: جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، ط١ دار وائل للنشر عمان الأردن،٢٠٠١م، ص ٢٣٦.

– الاستيلاء على السندات.

والسندات هي الصكوك التي تنشئ حقا أو تثبت انقضائه، كصكوك الدين والمخالصات ووثائق الزواج والطلاق، وأذون الاستيراد والتصدير والعقود، ونحوها. ويتم ذلك بالاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة[١].

الجريمة الثانية: وصول المجرم المعلوماتي – دون مسوغ نظامي صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

ويعرف هذا النوع من الجرائم بجرائم البطاقات الممغنطة، أو جرائم النقود الإلكترونية، وهي عبارة عن قيمة نقدية مختزنة بطريقة الكترونية على وسيلة الكترونية وتكون مقبولة كوسيلة دفع للتعامل بين الجمهور، بواسطة متعهدين، حيث يتم وضعها في متناول المستخدمين لاستعمالها كبديل عن العملات النقدية والورقية؛ أو هي مخزون الكتروني لقيم نقدية على وسيلة تقنية تستهدف القيام بمدفوعات لمتعهدين دون حاجة

[١] قنديل. سعيد السيد: التوقيع الالكتروني، ماهيته وصوره وحجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة للنشر ٢٠٠٤م، صـ٥٨، عبد الحميد. ثروت: التوقيع الالكتروني: مرجع سابق، صـ٦٢. أبو هيبة. نجوى: التوقيع الالكتروني، تعريفه مدى حجيته في الإثبات، دار النهضة العربية ٢٠٠٤م، صـ٥١، المري. عايض راشد: مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه من حقوق القاهرة ١٩٩٨م، صـ١١٢، يوسف. أمير فرج: المحاكم الإلكترونية المعلوماتية والتقاضي الالكتروني: مرجع سابق، صـ١٥٠.

الى وجود حساب بنكي عند اجراء الصفقة وتستخدم كأداة محمولة مدفوعة مقدما، ولذا فإنها تختص بما يلي:

ولهذا النوع من النقود في المجتمعات الحديثة شأنا عمليا كبيرا وعلى مستوى الأفراد أصبحت من متطلبات السفر والترحال. ذلك أنها تحقق للإنسان أمانا على أمواله حال حملها معه، فتتعرض للفقد أو السرقة، وكذلك يتمكن بها من شراء ما يبدو له شراؤه في ظروف مفاجئة لم يستعد لها بحمل ما يكفي لهذه المشتريات، فضلا عن أن البطاقة تيسر لحاملها السداد بأي عملة دون أن يحتاج لحمل العملات المختلفة التي توجد إجراءات لدخولها وخروجها في بعض البلاد التي بها قيود على تحويل العملة، ثم إنها تشكل وسيلة للمحاسبة وضبط المصاريف وتوثيق السداد للمطالبات. وهذه البطاقات على أنواع:

١- بطاقة السحب الآلي، ومن خلالها يستطيع حاملها سحب المبالغ النقدية من حسابه من خلال أجهزة السحب الآلي، بحد أقصى مقرر[١].

[١]سالم. عمر: الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية ١٩٩٥م، صـ١٠.السعيد: كامل: شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن ط٢ دارالفكر للنشر والتوزيع – عمان ١٩٨٣م، ص١١.

٢- بطاقة الشيكات، ومن خلالها يتعهد البنك الذي أصدرها لحاملها بسداد الشيكات التي يحررها العميل من البنك وفقا لشروط إصدارها[١].

٣- بطاقة الائتمان، وتخول حاملها الحق في الحصول على التسهيلات الائتمانية من مصدرها، بحيث يمكنه الحصول بموجبها على السلع والخدمات، ثم تقوم الجهة المصدرة بالسداد[٢].

٤- بطاقة الوفاء، وهي التي يكون لحاملها رصيد بالبنك فيسحب منه مباشرة قيمة مشترياته وأجور الخدمات المقدمة له، في حدود الرصيد الموجود، ويتم الحسم منه فورا، ولا يحصل صاحبها على إقراض[٣].

وتحتوي هذه البطاقات على شريط ممغنط تخزن فيه البيانات الشخصية لحامل البطاقة، وبيانات مصدرها، وبيانات البطاقة نفسها، بل هناك نوع من البطاقات يشتمل على ذاكرة أو دوائر الكترونية تسمح بتخزين آلاف البيانات[٤].

---

[١] حجازي. عبد الفتاح بيومي جرائم الكمبيوتر والانترنت، دار النهضة العربية ٢٠٠٩م، صـ١٣٤.
[٢] عثمان. عبد الحكيم: أحكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، دار الفكر الجامعي ٢٠٠٧م، صـ١٥٢.
[٣] الزحيلي. وهبة: بطاقات الائتمان، بحث بمجلة مجمع الفقه الإسلامي، جـ١٥، عدد٣، صـ٤٦.
[٤] حماد. عادل حماد عثمان: حماية المعلومات في التشريع الجنائي السوداني، مرجع سابق، ٢٦٩.

ويتمثل النشاط الإجرامي المقررة في الفقرة محل الشرح في وصول المجرم المعلوماتي – دون مسوغ نظامي صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

ومن صور الجريمة المذكورة ما يلي:

١- حصول شخص على بطاقة ائتمان صحيحة بناء على مستندات مزورة، حيث يتقدم الجاني الى البنك بمستندات غير صحيحة كأن ينتحل فيها صفة الغير مثلا، أو يعتمد على بيانات كاذبة، فتصدر له البطاقة ويستخدمها في شراء السلع والخدمات، ولا يتمكن البنك من استرداد القيمة بعد ذلك لعد الاستدلال على صاحب البطاقة أو لعدم كفاية الأدلة[١].

٢- استعمال البطاقة بعد انتهاء مدتها أو رغم إلغاء البنك لها.

٣- حصول الغير على البطاقة كما لو فقدت أو سرقت، وحصوله على الرقم السري لها.

[١] حجازي. عبد الفتاح بيومي: جرائم الكمبيوتر والإنترنت، مرجع سابق، صـ١٣٦.

٤- اتفاق موظف البنك مصدر البطاقة مع حاملها على استخراجها ببيانات مزورة، أو السماح للعميل بالسحب بما يتجاوز حد البطاقة، أو اتفاق موظف البنك مع التاجر على اعتماد إشعارات بيع صدرت الى بطاقة وهمية أو مزورة أو منتهية الصلاحية.

٥- قبول التاجر استخدام بطاقات ليست لها أرصدة كافية للصرف، أو قبول البطاقات المزورة من العملاء، بالتلاعب في البرامج الخاصة بالماكينة الإلكترونية بحيث لا تكتشف التزوير[١].

٦- حصول القراصنة على بيانات بطاقات الدفع الالكتروني واستعمالها بطرق غير مشروعة للحصول على السلع والخدمات، سواء تم ذلك الحصول بطريق الاختراق لخطوط الاتصالات التي تربط بين العميل والتاجر، أو عن طريق الخداع بإنشاء مواقع وهمية على غرار المواقع الفعلية، أو عن طريق إنشاء أرقام بطاقات من خلال معادلات رياضية في تبديل وتوفيق الأرقام للحصول في النهاية على رقم سري أو كود خاص ببطاقة متداولة[٢].

[١] حجازي. عبد الفتاح بيومي: التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول، صـ١٢٧.
[٢] حماد. عادل حماد عثمان: حماية المعلومات، مرجع سابق، صـ٣١٤. حسن: سعيد عبد اللطيف: إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الانترنت ط١ دار النهضة العربية ١٩٩٩م، القاهرة – ص١٤.

وتكمن الحماية القانونية لبرمجيات الحاسوب المقررة بموجب قانون براءات الاختراع. تتعلق بالبرمجيات التي لديها مفعول تقني أو صناعي أي التي تؤدي دوراُ تقنيا أو صناعياً، وهي برامج تتميز بالتحليل والتصميم والترميز والتكامل والتوثيق.

وهذا الأخير مرحلة هامة من مراحل بناء النظام البرمجي حيث يتم توثيق البناء الداخلي للبرنامج، وذلك بغرض الصيانة والتطوير ، وهناك أكثر من طريقة للتوثيق أهمها توثيق المبرمج وذلك بإضافة تعليقات داخل الشفرة البرمجية.

إن مؤلف العمل الرقمي سواء أكان هذا العمل برنامجاً للحاسوب أو قاعدة بيانات أو تصميماً هندسياً جديداً، لم يعد نتيجة عمل فرد واحد، بل يغلب أن يكون عمل عدد من المبتكرين، لذا وجب حماية الأعمال الرقمية من التعدي، بأن تنزل الأعمال الرقمية منزلة الأعمال الذهنية المبتكرة لأجل حمايتها بواسطة أنظمة حماية الملكية الفكرية.

وتتطلب حماية الأعمال الرقمية من برامج وقواعد بيانات بموجب أنظمة حماية امللكية الفكرية على اعتبارها أعمالا ذهنية ضرورة مراجعة تلك الأنظمة والعمل على تعديلها لتشمل الأعمال الرقمية، كما يتعين توسيع نطاق تطبيق المعاهدات الدولية الخاصة بحماية الملكية الفكرية لتشمل الأعمال الرقمية.

المبحث الثالث

وسائل حماية الملكية الفكرية في الأمن السيبراني

تتضـــمن وســـائل حماية الملكية الفكرية في الأمن الســـيبراني الحماية الإلكترونية والحماية التنظيمية أو القانونية.

وتقوم الحماية الإلكترونية على حماية الأنظمة المتصـــــلة بالإنترنت مثل الأجهزة والبرامج والبيانات من التهديدات السيبرانية، لمنع الوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسـبة الأخرى، وذلك من خلال توفير وضـع أمني جيد لأجهزة الكمبيوتر والخوادم والشـــبكات والأجهزة المحمولة والبيانات المخزنة على هذه الأجهزة والتطبيقات والبرامج وغيرها ضـــد المهاجمين ذوي النوايا الخبيثة، وصـــد الهجمات الإلكترونية للوصول إلى البيانات الحساسة للمؤسسة أو المستخدم أو حذفها أو تقليدها ونحو ذلك.

إضافة إلى وسائل الحماية القانونية، ونتناول فيما يلي بيان تلك الوسائل على النحو التالي.

المطلب الأول

وسائل الحماية الإلكترونية

يعد الأمن السيبراني مهماً ومع نمو حجم وتعقيد الهجمات الإلكترونية، فإنه يتعين على الشركات والمؤسسات وخاصة تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي أو الصحة أو السجلات المالية، اتخاذ خطوات لحماية معلومات الأعمال والموظفين الحساسة الخاصة بهم.

ويراعى أن التحدي الأكثر صعوبة في الأمن السيبراني هو الطبيعة المتطورة باستمرار للمخاطر الأمنية نفسها، وهذا يقضي بتطوير أنظمة الحماية، وتتمثل وسائل الحماية الإلكترونية في إجراءات متعددة منها([1]):

أولا: تطوير منظومة أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات وذلك بإعداد وتفعيل ما يعرف بفرق الاستجابة لطوارئ الحواسب أو فرق مواجهة حوادث أمن الحاسوب، في القطاعات الحيوية لمواجهة أية أخطار سيبرانية أو هجمات سيبرانية توجه اليها، وعن التوعية([2]).

[1] أحمد: هلالي عبد اللاه: اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، ط١ دار النهضة العربية ٢٠٠٧م، ص٤٧.

[2] الحسيني: عمر الفاروق: تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، مجلة المحاماة، س١٢ عدد نوفمبر/ديسمبر١٩٨٩ ص ١٣ .

ثانيا: تفعيل برامج حماية الهوية الرقمية مثل بنية المفتاح المعلن التي يعتمد عليها التوقيع الإلكتروني مما يؤدي إلى توفير متطلبات الأمن السيبراني والتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

كما يدخل في هذه التقنية التعمية أو التشفير بشكل عام هو عملية الحفاظ على سرية المعلومات (الثابت منها والمتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات الى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف الغير مفهومة، يتم تشفير الملف وفك التشفير عن طريق آلمة السر، التي يجب ان تكون معروفة للطرفين (المرسل والمستقبل) وهذا ما يسمى بالتشفير المتناظر([1]).

كما يجب التأكد الدوري من أمن الشبكة لحماية الشبكة من المستخدمين غير المرغوب فيهم والهجمات والاقتحامات. وكذا أمان التطبيق بالعمل على توفير تحديثات

[1] رستم: هشام محمد فريد: الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤م، ص٧٠، احمد: هلالى عبدالاه: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى، مرجع سابق، ص٧٧.

واختبارات مستمرة للتأكد من أن هذه البرامج آمنة من الهجمات. فضلا عن الاهتمام بالتعافي من الكوارث والتخطيط لاستمرارية الأعمال في حالة الهجوم والتعدي

وقد أثبت نظام التشفير فعاليته، ففي نطاق التوقيع الإلكتروني مثلا نجد التشفير يعتمد على مفتاح خاص وآخر عام، تصدرهما الشركة المختصة بإصدار التوقيع الالكتروني؛ فالمفتاح الخاص عبارة عن أداة الكترونية خاصة بصاحبها ولا تتكرر كالبصمة، وتنشأ بواسطة عملية حسابية خاصة، ومن خلاله يوضع التوقيع الالكتروني على المحرر الالكتروني، ثم يحفظ ذلك المحرر في بطاقة ذكية مؤمنة، فإذا رغب الشخص في التعاقد إلكترونيا فعليه أن يقوم بكتابة رسالته وتوقيعها الكترونيا باستخدام مفتاحه الخاص، ثم تمريرها من خلال برنامج خاص بالتشفير في الحاسب الآلي، حيث يقوم هذا البرنامج بتشفير المعاملة بعمليات حسابية معقدة تحول الرسالة المكتوبة إلى رقمية، ثم يأتي بعد ذلك دور المفتاح العام.

والمفتاح العام لا بد منه لفك شفرة الرسالة المرسلة من صاحب المفتاح الخاص، ليقوم البرنامج الخاص بالمستقبل بإرسال نسخة من التوقيع الالكتروني إلى الجهة التي أصدرت الشهادة، لتقوم أجهزة تلك الهيئة بمراجعة قاعدة البيانات الخاصة بها، والتعرف على صحة التوقيع، ثم إعادة النتيجة والمعلومات الخاصة بالشهادة إلى المستقبل، ليقوم

بقراءة تلك الرسالة مستخدما المفتاح العام، ثم يعاود التواصل مع المرسل مكررا نفس الطريقة؛ ومن ثم فالمفتاح العام وإن كان مختصا بشخص لكنه معلن للكافة، ويستخدم في التحقق من شخصية الموقع على المحرر الالكتروني للتأكد من سلامة المحرر والتوقيع، ويوضع رقم سري على الشريحة لئلا تستخدم من الغير حال ضياعها أو سرقتها[١].

لذا يسعى المبدعون والمبتكرون في مجال الأمن السيبراني إلى تطوير أنظمة البرمجيات والشبكات ومراكز البيانات من خلال البحث عن نقاط الضعف والمخاطر في الأجهزة والبرامج وإيجاد أفضل طريقة لتأمين البنية التحتية لتكنولوجيا المعلومات ببناء جدران الحماية في البنية التحتية للشبكة والمراقبة المستمرة للهجمات والاقتحامات وإغلاق الثغرات الأمنية[٢].

[١] يوسف: أمير فرج: المحاكم الالكترونية المعلوماتية والتقاضي الالكتروني: مرجع سابق، صـ١٥٤.
[٢] البشري: محمد الأمين: التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة منن ١ – ٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات، ص١٠٧٨.عوض: محمد محي الدين: مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ٢٥ ـ٢٨ أكتوبر ، ١٩٩٣م، ص ٣٦٢.

المطلب الثاني

وسائل الحماية في التشريعات القانونية

إن وجود أي فراغ تشريعي بشأن التعديات السيبرانية، قد يضر ضرراً بالغاً بمنظومة المعاملات والخدمات الإلكترونية مما يتعين معه وضع النصوص القانونية لحماية الملكية الفكرية في مجال الأمن السيبراني.

وقد وضعت الاتفاقيات الدولية لحماية المصنفات الرقمية وبرامج الأمن السيبراني، ومن ذلك الاتفاقيات الدولية المبرمة لحماية الملكية الفكرية بكافة أشكالها كاتفاقية برنلحماية المصنفات الأدبية والفنية والتي انضمت إليها المملكة العربية السعودية، وهي أهم هذه الاتفاقيات لثرائها وشدة أحكامها فيما يخص حقوق المؤلف، فضلا عن تطورها ومواكبتها لكل ما هو جديد في عالم التقنية والمعرفة.

ثم تأتي اتفاقية تربس للتدابير المتعلقة بأثر التجارة على حقوق الملكية الفكرية، التي أبرمت عام ١٩٩٤م، وقد تضمنت قواعد خاصة في مجال حماية المصنفات الرقمية،

ثم كانت اتفاقية الويبو لحماية حقوق التأليف التي أبرمت عام ١٩٩٦م، وقد أولت هذه الاتفاقية اهتماما خاصا بالوسائط الإلكترونية[١].

وتهدف هذه الاتفاقيات جميعها إلى حماية الحق في الإبداع في مجال مصنفات التقنية المعلوماتية، ومنح المبتكر الحق في الاستغلال العادل والمشروع لعائدات هذه المصنفات ضمن أطر وقواعد إدارية.

وفي التشريعات الداخلية للدول نجد أن أغلبية القوانين المتعلقة بحقوق المؤلف في معظم الدول على نوعين من طرق الحماية القانونية لحقوق المؤلف ، أحدهما مدني والآخرجزائي.

أما الوسائل المدنية فهي تمكن المؤلف من اتخاذ الإجراءات اللازمة لمصادرة المصنفات المزورة أو المقلدة وإتلافها ،أو وقف التعدي على المصنف، والمطالبة بالتعويض عن الضرر المادي والمعنوي الذي لحق بالمصنف أو بسمعة المؤلف(٢).

---

[١]لطفي. محمد حسام: تأثير اتفاقية تربس على التشريعات العربية، ندوة الويبو بالتعاون مع الجامعة الأردنية، فبراير ٢٠٠٢م.

[٢]يونس: عمر محمد أبوبكر: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية ، القاهرة ٢٠٠٤ م ص ٩٦٩.
قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط١ دار هومة للطباعة،الجزائر، ٢٠٠٦م،ص١١٢.

أما الحماية الجزائية فقد تقتصر على الغرامة المالية أو إغلاق المؤسسة التي شاركت في ارتكاب أعمال التعدي على حقوق المؤلف، أو فرض عقوبة الحبس على كل من يخالف أحكام قوانين حقوق المؤلف أو يتعدى على تلك الحقوق([1]).

كما تعطي القوانين للجهات القضائية صلاحية الأمر باتخاذ إجراءات و تدابير تحفظية مؤقتة فورية وفعالة لغرض الحيلولة دون حدوث تعدي على الحقوق المحمية و كذا لصون الأدلة ذات الصلة بالتعدي، وذلك بطلب من مالك الحقوق المتضرر أو ممثله حيث يجوز لمالك الحقوق المتضرر أن يطلب من الجهة القضائية المختصة اتخاذ التدابير التحفظية اللازمة لمنع الاعتداء الوشيك الوقوع على حقوقه، أو لوضع حد لكل مساس معاين مع طلب تعويض الضرر اللاحق به وكذا المطالبة بحجز الدعائم المقلدة و الإيرادات المتولدة عن الاستغلال غير المشروع للمصنف وحجز كل مؤلف تقني مستخدم لصنع الدعائم المقلدة.

وفي النهاية فإن جميع وسائل الحماية القانونية تقوم على ما يلي:

[1] سلامة: مأمون محمد: الإجراءات الجنائية في التشريع الليبي ، الجزء الثاني، ط٢ منشورات المكتبة الوطنية، بنغازي ،٢٠٠٠، ص ١٧٦، حسني: محمود نجيب: شرح قانون الإجراءات الجنائية ، الجزء الأول، ط٢ دار النهضة العربية، القاهرة ١٩٨٨م، ص٤٨٣.

١- اتخاذ تدابير تعتمد الامن كعنصر ضروري في الانتاج، لاسيما ما يخص البرامج والاجهزة المستخدمة في تقنيات الاتصال.

٢- اعتماد مبادىء خلقية للسلوك السيبراني، على مثال خلفيات وأصول التعامل القائمة في المجتمع التقليدي، وتكون بمثابة عقد اجتماعي، يؤسس لسلوك، يضمن سلامة الجماعة، وسلامة مواردها.

٣- وضع استراتيجية، وسياسة أمنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات، وبادراة وسائل الاتصالات، والبنى التحتية، كما لاولئك المعنيين بصناعة ادوات وبرامج الاتصال، وخزن المعلومات ومعالجتها.

٤- أخذ جميع ابعاد الامن السيبراني، بعين الاعتبار، لدى وضع اي استراتيجية او سياسة، بما في ذلك، حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم، بحيث تأتي الخطة متكاملة، ومنسجمة مع ما يمكن توقع الالتزام به، من قبل المعنيين، بامن مجتمع المعلومات.

الخاتمة

وتتضمن أهم النتائج والتوصيات.

أولا: النتائج:

١- إن حماية الملكية الفكرية في مجال الفضاء السيبراني أصبحت من الحاجات الملحة، التي يفرضها واقع المعلومات الأمنية المعاصر.

٢- تقوم حماية الملكية الفكرية في مجال الفضاء السيبراني على النشاط الذي يحمي أنواع المليكة الفكرية المرتبطة بالتقنيات الحديثة للاتصالات والمعلومات، مع ضمان الحد من الخسائر والأضرار الواقعة أو محتملة الوقوع.

٣- تقتضي حماية الملكية الفكرية في مجال الفضاء السيبراني بحث أهم الأساليب في مجال إدارة نظام امن المعلومات للوقوف على عوامل نجاحها والصعوبات والمعوقات التي تواجهها. وبناء بنية تحتية معلوماتية تكون قادرة على العمل بكفاءة وفاعلية.

٤- العمل على تطوير الاوجه القانونية والتشريعية لتكون متوازنة مع التقدم التكنولوجي، ولتضمن الوقاية من مخاطر الاعتداء على المعلومات والتهيوء للحالات الطارئة ووضع الخطط اللازمة لمواجهتها.

ثانيا: التوصيات:

١– نهيب بالمنظم السعودي استصدار نظام خاص بحماية الملكية الفكرية في مجال الفضاء السيبراني يتوافق مع طبيعة تلك الأعمال.

٢– ضرورة تشجيع المبدعين على إنشاء برامج تتسم بالجدة والابتكار لحماية المعلوماتية وتحقيق الأمن السيبراني، والعمل على حفظ حقوق هؤلاء المبدعين.

٣– إدخال مادة حماية الملكية الفكرية في مجال الفضاء السيبراني لكليات الدراسات القضائية والأنظمة ليتم تدريسها حتى تكون لدى هؤلاء الطلاب الذين هم قضاة ومحامو المستقبل تصور كامل عن هذه المستجدات.

٤– تأهيل الاجهزة القضائية المختصة، والشرطة القضائية، بحيث تتمكن من القيام بواجبها، في مجال ملاحقة ومحاكمة المجرمين السيبرانيين.

٥– إنشاء هيئات تحكيم وطنية، متخصصة في القضايا السيبرانية، وخدمات استشارات، مسبقة ولاحقة لاي نشاط الكتروني، يمكن لمن يرغب، اللجوء اليها.

فهرس المراجع

١) ابراهيم. خالد ممدوح: أمن الجريمة الالكترونية، الدار الجامعية للنشر ٢٠٠٨م، الشوابكة.

٢) إبراهيم: خالد ممدوح: الجرائم المعلوماتية.

٣) ابن فارس: مقاييس اللغة،جـ١،.

٤) ابن منظور: محمد بن مكرم بن على، أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعى الإفريقى، دار صادر – بيروت ط٣ ١٤١٤هـ جـ١٠.

٥) أبو الحسين:أحمد بن فارس بن زكرياء القزويني الرازي، أبو الحسين: معجم مقاييس اللغة، تحقيق: عبد السلام محمد هارون، نشر دار الفكر ١٣٩٩هـ /١٩٧٩م. جـ٥.

٦) أبو العباس: أحمد بن محمد بن علي الفيومي ثم الحموي: المصباح المنير في غريب الشرح الكبير، نشر: المكتبة العلمية – بيروت، جـ٢.

٧) أبو عامر: محمد زكي: دراسة علم الإجرام والعقاب، الدار الجامعية بيروت ١٩٨٢م.

٨) أبو هيبة. نجوى: التوقيع الالكتروني، تعريفه مدى حجيته في الإثبات، دار النهضة العربية ٢٠٠٤م.

٩) أحمد حسام طه تمام: جرائم الحاسب الآلي، دار النهضة العربية.

١٠) احمد: هلالى عبدالاه: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى.

١١) أحمد: هلالي عبد اللاه: اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، ط١ دار النهضة العربية ٢٠٠٧م.

١٢) البشري: محمد الأمين: التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة منن ١ – ٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات .

١٣) تمام: أحمد حسن طه: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ٢٠٠٠م.

١٤) جامع: أحمد: اتفاقيات التجارة العالمية، دار النهضة العربية، ٢٠٠١م.

١٥) الجنيهي: منير محمد: جرائم الانترنت والحاسب الآلي ووسائل مكافحتها – دار الفكر الجامعي الإسكندرية ٢٠٠٥م.

١٦) حجازي. عبد الفتاح بيومي ، جرائم الكمبيوتر والانترنت، دار النهضة العربية ٢٠٠٩م.

١٧) حجازي. عبد الفتاح بيومي: التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول.

١٨) حجازي. عبد الفتاح بيومي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية ٢٠٠٧م.

١٩) حسن: سعيد عبد اللطيف: إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الانترنت ط١ دار النهضة العربية ١٩٩٩م، القاهرة.

٢٠) حسني. محمود نجيب: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ط٦/١٩٨٩م.

٢١) حسني: محمود نجيب: شرح قانون الإجراءات الجنائية ، الجزء الأول، ط٢ دار النهضة العربية، القاهرة ١٩٨٨م.

٢٢) الحسيني: عمر الفاروق: تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، مجلة المحاماة، س١٢ عدد نوفمبر/ديسمبر ١٩٨٩.

٢٣) حماد: عادل حماد عثمان: حماية المعلومات في التشريع الجنائي السوداني.

٢٤) حمودة. عبد الرحمن: مكافحة الجرائم المعلوماتية دراسة تحليلية، الرياض ٢٠٠٩م.

٢٥) خالد ممدوح ابراهيم: الجرائم المعلوماتية.

٢٦) داود: حسن طاهر: جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠.

٢٧) الرازي: زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي: مختار الصحاح، تحقيق: يوسف الشيخ محمد، نشر المكتبة العصرية – الدار النموذجية، بيروت – صيدا، ط٥ ١٤٢٠هـ / ١٩٩٩م، جـ١.

٢٨) رستم :هشام محمد فريد: قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة ١٩٩٢م.

٢٩) رستم: هشام محمد فريد: الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤م.

٣٠) رمضان: عمر السعيد: شرح قانون العقوبات الاتحادية لدولة الإمارات العربية المتحدة – القسم الخاص، دار النهضة العربية، القاهرة ١٩٨٦م.

٣١) رمضان: مدحت، جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٠.

٣٢) الرومي: محمد أمين: جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية ٢٠٠٤م.

٣٣) الزحيلي. وهبة: بطاقات الائتمان، بحث بمجلة مجمع الفقه الإسلامي، جـ١٥، عدد٣.

٣٤) الزمخشري: أساس البلاغة، جـ١.

٣٥) زين الـدين: بلال أمين: جرائم نظم المعـالجـة الآليـة للبيـانـات، دار الفكر الجامعي، ٢٠٠٨م

٣٦) سالم. عمر: الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية ١٩٩٥م.

٣٧) السعيد: كامل: شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن ط٢ دارالفكر للنشر والتوزيع – عمان ١٩٨٣م.

٣٨) سلامة: مأمون محمد: الإجراءات الجنائية في التشريع الليبي ، الجزء الثاني، ط٢ منشورات المكتبة الوطنية، بنغازي ،٢٠٠٠.

٣٩) سليم د طارق عبد الوهاب: الجرائم المرتكبة بواسطة الانترنت وسيل مكافحتها، تونس١٩٩٧م.

٤٠) السنهوري: عبد الرازق: الوسيط في شرح القانون المدني – حق الملكية–، دار إحياء التراث العربي، بيروت لبنان، جـ٨.

٤١) جبور: منى الأشقر: الأمن السيبراني: التحديات ومستلزمات المواجهة، من منشورات جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبرانيبيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢، وانظر: مجلة محطات، مقال منشور بتاريخ ٢٠١٩/٣/٩م، على الرابط: https://www.mahat.net

٤٢) الشايع: خالد: الأمن السيبراني، مفهومه، وخصائصه، وسياساته، دار العالمية، الأولى، ١٤٤٠هـ.

شبير: محمد عثمان: المدخل إلى فقه المعاملات المالية، دار النفائس، الطبعة الثانية، ١٤٣٠هـ-٢٠١٠م.

٤٣) الشوا. محمد سامي: ثورة المعلومات وانعكاساتها على قانون العقوبات.

٤٤) الصغير. جميل عبد الباقي: الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠١.

٤٥) الصغير. جميل عبد الباقي: الانترنت والقانون الجنائي، دار النهضة العربية ٢٠٠٢م.

٤٦) الصغير. جميل عبد الباقي: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ٢٠٠١م.

٤٧) العبادي: عبد السلام: الملكية في الشريعة الإسلامية، مكتبة الأقصى، عمان، ١٩٧٧م، جـ١.

٤٨) عبد الحميد. ثروت: التوقيع الالكتروني.

٤٩) عبد الرحمن: محمد جلال: الجرائم الاليكترونية، ط١ مكتبة القانون والاقتصاد، ١٤٣٦هـ/٢٠١٥م.

٥٠) عثمان. عبد الحكيم: أحكام البطاقات الائتمانية في القانون والآراء الفقهية الإسلامية، دار الفكر الجامعي ٢٠٠٧م.

٥١) العثماني: محمد تقي: بيع الحقوق المجردة: بحوث الدورة الخامسة لمؤتمر مجمع الفقه الإسلامي، بجده، مجلة المجمع، العدد الخامس، (٣/٢٣٨٥).

٥٢) عرب، يونس. ثلاث طوائف لجرائم الكمبيوتر وثلاث مجموعات تشريعية لمواجهتها، مجلة حماية الملكية الفكرية، ع٣٠، الربع الثاني، ١٩٩٣،

٥٣) العريان: محمد علي: الجرائم المعلوماتية – كلية الحقوق – جامعة الإسكندرية – دار الجامعة الجديدة للنشر –: عام ٢٠٠٤.

٥٤) علاء الدين، أبو بكر بن مسعود بن أحمد الكاساني الحنفي: بدائع الصنائع في ترتيب الشرائع، دار الكتب العلمية الطبعة: الثانية، ١٤٠٦هـ – ١٩٨٦م، جـ٧.

٥٥) علي بن هادية وآخرون، القاموس الجديد الألفبائي.

٥٦) علي. عبد الله حسين: حماية المعلومات المخزنة على الحاسب الآلي، رسالة دكتوراه من جامعة عين شمس ٢٠٠١م.

٥٧) علي: محمد محرم محمد: جريمة النصب و الإحتيال والتجارة الالكترونية القاهرة ١٩٩٨م.

٥٨) عوض: محمد محي الدين: مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ٢٥ –٢٨ أكتوبر ، ١٩٩٣م.

٥٩) فكري. أيمن عبد الله: جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر ٢٠٠٧م.

٦٠) الفيروزآبادي: مجد الدين أبو طاهر محمد بن يعقوب الفيروزآبادى، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالةبإشراف: محمد نعيم العرقسُوسي، نشر: مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت – لبنان ط٨ ١٤٢٦ هـ – ٢٠٠٥ م.

٦١) قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط١ دار هومة للطباعة، الجزائر، ٢٠٠٦م.

٦٢) قدري: كامل: الحماية الجنائية للملكية الفكرية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، قسم القانون الجنائي، ٢٠١٤م.

٦٣) القرافي: أبو العباس شهاب الدين أحمد بن إدريس بن عبد الرحمن المالكي الشهير بالقرافي: أنوار البروق في أنواء الفروق، نشر عالم الكتب، د.ط١ن د.ت، الفرق الثمانون بعد المائة، جـ٣.

٦٤) قشقوش. هدى: جرائم الحاسب الالكتروني، مرجع سابق.

٦٥) قنديل. سعيد السيد: التوقيع الالكتروني، ماهيته وصوره وحجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة للنشر ٢٠٠٤م.

٦٦) قورة. نائلة عادل: جرائم الحاسب الآلي الاقتصادية، مرجع سابق.

٦٧) لحرش: أسعد المحاسن: الملكية الفكرية بين تشجيع الابتكار وتحريم الاحتكار، منشور بموقع https://platform.almanhal.com، بتاريخ ١٤٤١/٨/٥هـ.

٦٨) لطفي. محمد حسام محمود: الحماية القانونية لبرامج الحاسب الإلكترونية، دار الثقافة للطباعة والنشر ١٩٨٧م.

٦٩) لطفي. محمد حسام: تأثير اتفاقية تربس على التشريعات العربية، ندوة الويبو بالتعاون مع الجامعة الأردنية، فبراير ٢٠٠٢م.

٧٠) محمد أمين: جرائم الحاسوب والانترنت.

٧١) محمد: فتحي عبد الهادي. أخلاقيات المعلومات في مراكز المعلومات والمكتبات، العربية ٣٠٠٠، ع١، شتاء ٢٠٠٠.

٧٢) محمود: عمر: الجرائم المعلوماتية والإلكترونية ،.

٧٣) مختار: أحمد: معجم اللغة العربية المعاصرة، عالم الكتب الطبعة: الأولى، ١٤٢٩ هـ – ٢٠٠٨ م، جـ٣.

٧٤) المري. عايض راشد: مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه من حقوق القاهرة ١٩٩٨م.

٧٥) المري: راشد محمد: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية ٢٠١٨م.

٧٦) المشهداني: أكرم عبد الرزاق: القانون والجرائم التكنلوجية بغداد ٢٠٠١م.

٧٧) المغايرة: علاء الدين منصور: الأوجه الحديثة للجرائم المعلوماتية، رسالة ماجستير قدمت لجامعة الحكمة بيروت ٢٠٠٠م.

٧٨) مكي: محمد عبد الحميد: الاحتيال في قانون العقوبات – دراسة مقارنة – رسالة دكتوراه – جامعة القاهرة، ١٩٨٨م.

٧٩) المناعسة: أسامة أحمد: جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، ط١ دار وائل للنشر عمان الأردن،٢٠٠١م.

٨٠) المهيري. خالد: جرائم الكمبيوتر والانترنت والتجارة الإلكترونية، ط٢ / ٢٠٠٤م

٨١) النشمي: عجيل جاسم: الحقوق المعنوية: بيع الاسم التجاري، مجلة البحوث الإسلامية، مكة، مجمع الفقه الإسلامي.

٨٢) يوسف. أمير فرج: المحاكم الإلكترونية المعلوماتية والتقاضي الالكتروني.

٨٣) يونس: عمر محمد أبوبكر: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية ، القاهرة ٢٠٠٤ م.