دولة الإمارات العربية المتحدة

جامعـــة الشارقة

كلية الدراسات العليا والبحث العلمي

قسم القانون العام

- اسم البرنامج: ماجستير في القانون العام
- التخصص: القانون الجنائي
- اسم الباحثة: شما راشد الكندي

  Shamma Rashid Alkindi
- الرقم الجامعي: U20102264
- العام الجامعي: ٢٠٢١-٢٠٢٢
- اسم المشرف: د. احمد هياجنة

جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

The crime of cyber penetration of the information systems of state institutions in accordance with Federal Decree-Law No. (34) of 2021.

الملخص

بتطور التقنيات الحديثة أصبحت الجرائم الإلكترونية تتخذ طابعاً متطوراً، وأصبح الاختراق الالكتروني يتم عبر التقنيات الحديثة نفسها، وخاصة الهجمات التي تستهدف مؤسسات الدولة، حيث يعتمد مرتكبو جريمة الاختراق على ميزات التقنيات الحديثة لارتكاب جريمة الاختراق، وهو ما يشكل هجمات سيبرانية على الأنظمة المعلوماتية.

لذلك فإن مجرد الدخول إلى نظام الحاسب الآلي لا يمثل فعلاً غير مشروع، ولكن يستمد هذا الدخول عدم مشروعيته؛ من كونه غير مصرح به، ويتحقق الدخول غير المصرح به إلى جهاز الحاسب الآلي بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الحاسب الآلي دون رضاء المسئول عن النظام، أو بعبارة أخرى إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مصرح له باستخدامه والدخول إليه للوصول إلى البيانات والمعلومات المخزونة بداخله

تتمحور مشكلة البحث في التساؤل التالي: ما مدى فعالية قواعد التجريم والعقاب على جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة؟

تتمثل أهمية البحث من الناحية العلمية في أنه يبين موقف المشرع الإماراتي من حيث التجريم والعقاب في جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

وتوصلنا في نهاية البحث إلى أن الاختراق وما يتبعها من جرائم الكترونية، لا يمكن أن تتم إلا عن طريق هذه الشبكة فالمعلومات المدونة في الحاسوب الخاص، الذي لم يرتبط بالإنترنت لا يمكن اختراقه.

ومن توصيات البحث تهيب الباحثة بالمشرع الإماراتي تخصيص مادة قانونية في قانون الشائعات والجرائم الإلكترونية تجرم استخدام أنظمة الاختراق في ارتكاب الجريمة.

الكلمات الدالة: الأنظمة المعلوماتية الحكومية- الاختراق الإلكتروني- الإعاقة- الاعتراض- الجريمة – العقوبة.

ABSTRACT

With the development of modern technologies, cybercrimes have taken on an advanced character, and electronic penetration is carried out through modern technologies themselves, especially attacks targeting state institutions, where the perpetrators of the crime of hacking rely on the features of modern technologies to commit the crime of penetration, which constitutes cyber-attacks on information systems.

Therefore, the mere entry into the computer system does not constitute an illegal act, but this access derives its illegality; from the fact that it is unauthorized, and unauthorized access to the computer is achieved by accessing the information and data stored inside the computer system without the consent of the administrator of the system, or in other words, misuse of the computer and its system by an unauthorized person to use and access it to access the data and information stored inside it.

The research problem revolves around the following question: How effective are the rules of criminalization and punishment for the crime of cyber penetration of the information systems of state institutions?

The importance of the research from a scientific point of view is that it shows the position of the UAE legislator in terms of criminalization and punishment in the crime of cyber penetration of the information systems of state institutions in accordance with Federal Decree Law No. (34) of 2021.

At the end of the research, we found that the penetration and the subsequent electronic crimes, can only be done through this network, as the information recorded in the private computer, which is not connected to the Internet, cannot be penetrated.

Among the recommendations of the research, the researcher calls on the UAE legislator to allocate a legal article in the Law of Rumors and Cybercrimes that criminalizes the use of hacking systems in committing crime.

Keywords: Government Information Systems - Electronic Hacking - Disability - Interception - Crime - Punishment.

المقدمة:

إن النظـام المعلومـاتي قـد يتعـرض إلـى الاختـراق مـن قبـل أفـراد غيـر مصـرح لهـم بالـدخول إليـه والبقـاء فيـه، وقـد سـاهم فـي انتشـار هـذه الظـاهرة تطـور الاتصـالات وتنـامي شـبكات المعلوماتيـة، ويقصـد بالـدخول غيـر المصـرح بـه توجيـه هجمـات إلـى نظـام حاسـوبي أو معلومـاتي ، بقصـد المسـاس بالسـرية أو المسـاس بالسـلامة والمحتـوى والتكامليـة ، أو تعطيـل القـدرة والكفـاءة للأنظمـة للقيـام بأعمالهـا، وهـدف هـذا الـنمط الإجرامـي هـو نظـام الكمبيـوتر وبشـكل خـاص المعلومـات المخزونـة داخلـه ، بهـدف السـيطرة علـى النظـام دون تصـريح أو المسـاس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر[1].

لـذلك فـإن مجـرد الـدخول إلـى نظـام الحاسـب الآلـي لا يمثـل فعـلاً غيـر مشـروع، ولكـن يسـتمد هـذا الـدخول عـدم مشـروعيته؛ مـن كونـه غيـر مصـرح بـه، ويتحقـق الـدخول غيـر المصـرح بـه إلـى جهـاز الحاسـب الآلـي بالوصـول إلـى المعلومـات والبيانـات المخزونـة داخـل نظـام الحاسـب الآلـي دون رضـاء المسـئول عـن النظـام، أو بعبـارة أخـرى إسـاءة اسـتخدام الحاسـب الآلـي ونظامـه عـن طريـق شـخص غيـر مصـرح لـه باسـتخدامه والـدخول إليـه للوصـول إلـى البيانـات والمعلومات المخزونة بداخله[2].

ويـرتبط مفهـوم عـدم مشـروعية الـدخول بمعرفـة مـن لـه الحـق فـي الـدخول إلـى نظـام الحاسـب الآلـي، ومـن لـيس لـه هـذا الحـق، ولا يثيـر الأمـر مشـكلة فـي حالـة الـدخول غيـر المصـرح بـه مـن قبـل أشـخاص مـن خـارج الجهـة التـي يوجـد بهـا نظـام الحاسـب الآلـي، إذ يتحقـق بـه فعـل الاختـراق غيـر المشـروع، إلا أن المشـكلة تثـار فـي حالـة الـدخول غيـر المشـروع مـن قبـل العـاملين فـي الجهـة التـي يوجـد بهـا نظـام الحاسـب الآلـي، ففـي هـذه الحالـة يتجـاوز العامـل اختصاصـه والصـلاحيات الممنوحـة لـه، ولهـذا يجـب تحديـد اختصاصـات العـاملين وصـلاحياتهم فـي الجهـة بخصـوص اسـتخدام الحاسـب الآلـي ونظامـه تحديـداً

---

[1] د. إبـراهيم خالـد ممـدوح: التقاضـي الإلكترونـي (الـدعاوى الإلكترونـي وإجراءاتهـا أمـام المحـاكم)، دار الفكـر الجـامعي، الإسـكندرية، ٢٠٠٨م، ص٣٦٣-٣٦٤. المستشـار القـانوني- الـدكتور طـارق إبـراهيم أحمـد فيـاض العبـد اللـه: جـرائم الروبـوت وكيانـات الـذكاء الاصـطناعي، دار النهضـة العربيـة، القـاهرة، ٢٠٢٢.

[2] د. سـويلم، محمـد علـي: شـرح قـانون جـرائم تقنيـة المعلومـات- القـانون رقـم ١٧٥ لسـنة ٢٠١٨ فـي شـأن مكافحة تقنية المعلومات، دار المطبوعات الجامعية، ط ١، ٢٠١٩ م.ص٣٤

دقيقاً، حتى يسهل تحديد حدوث التجاوزات، كما يصعب في بعض الأحيان معرفة ما إذا كان هذا التجاوز قد حدث بشكل متعمد أو بدون قصد[٣].

مشكلة البحث:

تتمحور مشكلة البحث في التساؤل التالي: ما مدى فعالية قواعد التجريم والعقاب على جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة؟

تساؤلات البحث:

١) ما تعريف الاختراق للأنظمة المعلوماتية الحكومية؟
٢) ما الطبيعة القانونية لجريمة الاختراق السيبراني للأنظمة المعلوماتية بمؤسسات الدولة؟
٣) ما هي أركان جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١؟
٤) ما هي عقوبة جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١؟

أهمية البحث:

١) الأهمية النظرية: تتمثل أهمية البحث من الناحية النظرية في أنه يبين تعريف الاختراق وطبيعته القانونية ووسائله.
٢) الأهمية العلمية: تتمثل أهمية البحث من الناحية العلمية في أنه يبين موقف المشرع الإماراتي من حيث التجريم والعقاب في جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

[٣] يوسف، امير فرج: جرائم تقنية المعلومات بدول الخليج العربي والجهود الدولية والمحلية لمكافحة جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي، دار الكتب والدراسات العربية، الطبعة الأولى، ٢٠١٧، ص٢٤.

أهداف البحث:

١) بيان ماهية الاختراق السيبراني ووسائله؟

٢) تحديد أركان جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

٣) بيان العقوبات على جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١.

منهج البحث:

يعتمد البحث على المنهج الوصفي التحليلي من خلال وصف الموضوع من الناحية النظرية، وتحليل المواد الخاصة بالاختراق الواردة في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢١٠ بشأن الشائعات والجرائم الإلكترونية.

تقسيم البحث:

المبحث الأول: جريمة اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة

- **المطلب الأول:** طبيعة المحل لجريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة
- **المطلب الثاني:** اركان جريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة

المبحث الثاني: الأحكام الخاصة بالقعاب والتدابير على جرائم الاختراق السيبراني

- المطلب الأول: الاحكام الخاصة بالعقوبات في قانون مكافحة الشائعات والجرائم الالكترونية.
- المطلب الثاني: الاحكام الخاصة بالتدابير المتعلقة بالعقوبات المذكورة في قانون مكافحة الشائعات والجرائم الالكترونية.

الخاتمة تتضمن

اولاً: النتائج

ثانياً: التوصيات

المبحث الأول

جريمة اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة

نبين في المبحث الأول من البحث جريمة اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة من خلال تقسيم المبحث لمطلبين على النحو الآتي:

- **المطلب الأول:** طبيعة المحل لجريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة
- **المطلب الثاني:** اركان جريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة

المطلب الأول

طبيعة المحل لجريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة

إن محل جريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة، هو نظم المعلومات الحكومية، وحتى نتمكن من بيان محل الجريمة لابد لنا بأن نبين أنواع الانظمة المعلوماتية الحكومية محل الجريمة:

الفرع الأول

أنواع الأنظمة المعلوماتية الحكومية محل الجريمة

حدد المشرع الإماراتي في المرسوم بقانون اتحادي أنواع الأنظمة المعلوماتية الحكومية محل الجريمة، وعليه سنبين تلك الأنواع محل الجريمة على النحو الآتي:

١) معلومات مؤسسات الدولة

عرف المشرع الإماراتي المؤسسات الحكومية في المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية،

بأنهـــا:" مؤسســـات الدولـــة: أي جهـــة حكوميـــة اتحاديـــة أو محليـــة أو شـــركة أو منشـــأة مملوكة لأي من تلك الجهات بنسبة لا تقل عن ٢٥% من رأسمالها[٤]".

ومـــن هـــذا التعريـــف نلاحـــظ بـــأن المشـــرع الإمـــاراتي وفـــق مـــا جـــاءت بـــه هـــذه المـــادة يميـــز بـــين نـــوعين مـــن المعلومـــات، الأول هـــو المعلومـــات الخاصـــة بالأشـــخاص، والمعلومـــات الخاصـــة بالمؤسســـات الحكوميـــة، كمـــا أنـــه يميـــز وفـــق هـــذا التعريـــف بـــين المؤسســـات الخاصـــة التـــي تكـــون ملكيتهـــا بنســـبة ١٠٠% للأشـــخاص والمؤسســـات الحكوميـــة التـــي تكـــون للدولـــة فيهـــا نســـبة معينـــة، وقـــد أحســـن المشـــرع في ذلك كونه يسهم في تحديد محل الجريمة محل البحث بشكل دقيق.

٢) البيانات والمعلومات

كمـــا عـــرف (المرســـوم بالقـــانون الاتحـــادي رقـــم ٣٤ لســـنة ٢٠٢١ الصـــادر بتـــاريخ ٢٠ / ٠٩ / ٢٠٢١ نشـــر بتـــاريخ ٢٦ / ٠٩ / ٢٠٢١ فـــي الجريـــدة الرســـمية)، البيانـــات أو المعلومـــات بأنهـــا:" مجموعـــة منظمـــة أو غيـــر منظمـــة مـــن المعطيـــات، أو الوقـــائع أو المفـــاهيم أو التعليمـــات أو المشـــاهدات أو القياســـات تكـــون علـــى شـــكل أرقـــام أو حـــروف أو كلمـــات أو رمـــوز أو صـــور أو فيـــديوهات أو إشـــارات أو أصـــوات أو خـــرائط أو أي شـــكل آخـــر، يـــتم تفســـيرها أو تبادلهـــا أو معالجتهـــا، عـــن طريـــق الأفـــراد أو الحواســـيب، والتـــي ينـــتج بعـــد معالجتهـــا أو تـــداولها مـــا يطلـــق عليه مصطلح معلومات[٥]".

ومـــن نـــص هـــذه المـــادة نســـتنتج أن المشـــرع الإمـــاراتي حـــدد بدقـــة البيانـــات والمعلومـــات بهـــدف عـــدم الخلـــط بينهـــا وبـــين غيرهـــا مـــن المفـــاهيم، حيـــث أن المعيـــار القـــانوني الـــذي اعتمـــده المشـــرع الامـــاراتي للتمييـــز بينهـــا وبـــين غيرهـــا مـــن حيـــث طريقـــة المعالجـــة، حيـــث تـــتم المعالجـــة عـــن طريـــق الانســـان او الحاســـب الآلـــي، وأيضـــاً ينـــتج عـــن تلـــك المعالجـــة معلومـــات، وهـــذا يـــدل علـــى الفـــرق مـــا بـــين البيانـــات والمعلومـــات، بـــأن البيانـــات هنـــاك خضـــعت علـــى التنقـــيح والتلخـــيص والمعالجة للتحول الى معلومات توضع في الأجهزة التقنية.

٣) المعلومات الحكومية:

[٤] مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠ / ٠٩ / ٢٠٢١ نشر بتاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.

[٥] مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠ / ٠٩ / ٢٠٢١ نشر بتاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.

كما أن المرسوم بالقانون الاتحادي ذاته قد عرف المعلومات الحكومية بأنها:" البيانات أو المعلومات الإلكترونية غير المتاحة للكافة، والخاصة أو العائدة إلى إحدى مؤسسات الدولة[٦]".

ومن هذا النص يتضح لنا أن المشرع الإماراتي قد اعتبر معيار التفريق بين المعلومات الحكومية والمعلومات غير الحكومية معيار الملكية، فإذا كانت مملوكة لمؤسسات الدولة فهي معلومات حكومية، وإذا كانت مملوكة للأشخاص فهي معلومات خاصة.[٧]

والمعلومات من حيث مدلولها اللغوي مشتقة من المصدر علم ولهذه المشتقات العديد من المعاني منها ما يتصل بالعلم أي إدراك طبيعة الأمور والمعرفة أي القدرة على التمييز والتعليم والتعيين والإرشاد والتوعية والإبداع والشهرة والتمييز والتيسير ... إلى آخر ذلك من المعاني المتصلة بوظائف العقل،[٨]ومصطلح Information هو المقابل الإنكليزي للمعلومات وهي كلمة إنكليزية مشتقة من اللاتينية والتي كانت تعني في الأصل الاتصال أو التلقي، ويوجد لها في اللغة العربية معنيان متقابلان متميزان وهما: الإعلام كعملية أو نشاط والمعلومات التي يتم الإعلام بها،[٩] وهناك مصطلح آخر للمعلومة مشتق من التصور informatum والذي يعني الرسم أو التخطيط، وهذين المعنيين وجهان لحقيقة واحدة إذ أن الأول يوضح الجانب الحركي للمعلومة والثاني يوضح الجانب الوصفي لها،[١٠]ويعرف المنجد المعلومة بأنها كل ما يعرفه الإنسان عن قضية أو حادث أما معجم اللغة العربية

---

[٦] عرعارة، نبيل محمّد عثمان: الحماية الجنائيّة للحق في حرمة المراسلات عبر البريد الإلكتروني، (ماجستير في القانون الجنائي)، المصريّة للنشر والتوزيع، القاهرة، مصر، الطبعة الأولى ١٤٣٩ ه/ ٢٠١٨ مـ، ص ١٣٢.

(٧) المستشار القانوني- الدكتور طارق إبراهيم أحمد فياض العبدالله: جرائم الروبوت وكيانات الذكاء الاصطناعي، ، دار النهضة العربية، القاهرة، ٢٠٢٢.

(٨) د. علي، احمد: مفهوم المعلومات في إدارة المعرفة، مجلة جامعة دمشق، المجلد ١، العدد ١، ٢٠١٢ م، ص ٤٧٨.

(٩) د. قاسم، حشمت: جريمة الدخول غير المشرع لنظام معلوماتي، منشورات أطلس، دمشق، ٢٠٢١، ص ١٢.

(١٠) فتيحة، رصاع: الحماية الجنائية للمعلومات على شبكة الإنترنت، رسالة ماجستير، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، ٢٠١١ – ٢٠١٢ م، ص ٢٦، استخرج بتاريخ ٢٠ كانون الثاني ٢٠١٤ من الموقع الإلكتروني:
http://scholar.naiah.edu/sites/default/files/all-thesis/legal」)rotection—of—computer programs.pdf

المعاصرة فعرفها بأنها أخبار وتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور واتخاذ القرارات.[١١]

أما اصطلاحاً فهناك بعض التعريفات الاصطلاحية فيما ورد في المعاجم والموسوعات المتخصصة، ومن هذه التعريفات الاصطلاحية للمعلومات، هو التعريف الذي ورد في المعجم الموسوعي في الكمبيوتر والإلكتروني بأنها: "معطيات تم تسجيلها أو تصنيفها وتنظيمها وتفسيرها ووصفها في إطار معين لإظهار معانيها".[١٢]

ومن هذا التعريف نستنتج أن المعلومات ما هي إلا بيانات تصنف وفق طريقة معينة، وإطار معين، وما يؤخذ على هذا التعريف أنه جاء قاصراً من حيث تحديده لعناصر المعلومات الحكومية وتكلم فقط عن المعلومات المحوسبة بشكل عام.

كما عرفها قاموس المنهاوي الموسوعي:" بأنها الحقائق الموصلة أو رسالة تستخدم لتمثيل حقيقة او مفهوم استخدام وحدة وسط بيانات ومعناه او هي عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة.[١٣]

ومن هذا التعريف نلاحظ كذلك بأنه مثل التعريف السابق، جاء بتعريف للمعلومات بشكل عام ولم يبين خصائصها ولم يحدد معيار قانوني للتمييز بين المعلومات الحكومية وغير الحكومية.

أما المعجم الموسوعي لمصطلحات المكتبات والمعلومات فعرفها بأنها:" البيانات التي تمت معالجتها لتحقيق هدف معين او لاستعمال محدد لأغراض اتخاذ القرارات أي البيانات التي أصبح لها قيمة بعد تحليلها او تفسيرها أو تجميعها في شكل ذي معنى وإلى يمكن تداولها وتسجيلها ونشرها وتوزيعها

---

(١١) د. محمد، أحمد مختار: معجم اللغة العربية المعاصرة، المجلد ٢، عالم الكتب، القاهرة، ٢٠١٦، ص ١٤٢٩.

(١٢) لوغاريف، أندريه : المعجم الموسوعي في الكمبيوتر والإلكترونيك، ترجمة د. عبد الحسيني، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، الطبعة ٢، ٢٠٠٩، ص ٣٧٢.

(١٣) د. خليفة، شعبان: قاموس البنهاوي الموسوعي في مصطلحات المكتبات والمعلومات، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٤ م، ص ٨.

في صورة رسمية أو غير رسمية وفي أي شكل وعرفها بأنها المقومات الجوهرية في أي نظام للتحكم".[١٤]

ومن هذا التعريف نرى بأنه جاء أوسع من التعريفات السابقة من حيث توسعه في تعريف المعلومات وبيان بعض الخصائص لها من حيث أنها يتم تداولها بصورة رسمية غير رسمية، ولكنه لم يبين خصائص ومميزات المعلومات الحكومية.

يذكر أن أحد الفقهاء عرف المعلومات بأنها:" المعرفة المتحصلة بشأن حقيقة أو ظرف معين.[١٥]

وهنا نرى بأنه عرف المعلومات بسياقها العام دون تخصيص للمعلومات الحكومية، وهو ما يجعله تعريف عام.

وعرفها آخر بأنها:" التعبير الأول وصياغة مصممة لجعل الرسالة قابلة للنقل أو الإبلاغ".[١٦]

وانتقد جانب من الفقه هذا التعريف لاشتراطه وصول الرسالة إلى المتلقي ولذلك فقد تم اقتراح تجاهل هذا الشرط من خلال اعتبار المعلومات شيء ويكون ذلك عندما يكون لها وجود في العالم الخارجي من خلال الدعامة المادية التي تجسدها كالإشارات والحروف.[١٧]

وانتقد البعض هذا الاتجاه لأنه يؤدي إلى تلاشي المفهوم الحسي للمعلومة والتركيز على النموذج الذي لا يشكل هدفا عندما يتعلق الأمر بالمعلومات ولأنه يتجاهل ضرورة وجود وسيلة للاتصال ولذلك فقد تم تعريفها بأنها عمل

---

(١٤) الشامسي أحمد محمد وحسب الله سيد: المعجم الموسوعي لمصطلحات المكتبات والمعلومات، دار المريخ، الرياض، ١٤٠٨- ١٩٨٨، ص ١.

(١٥) د. الملا، إبراهيم حسن عبد الرحيم: الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون صادرة عن أكاديمية شرطة دبي، السنة السادسة والعشرون، العدد الأول، يناير ٢٠١٨ م.ص٢١٧

(١٦) د. العريان، علي محمد: الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١١ م، ص ٥٣

(١٧) د. احمد هلالي عبد اللاه: جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، ٢٠١٥ م – ٢٠١٦ م، ص ١١٤. الشريف، عمر: التنظيم التشريعي لجرائم الاتصالات في مصر، التشريع، السنة الأولى، العدد الثاني يوليو ٢٠٠٤، ص ٣٤.

من أعمال الاتصال للحقائق والأفكار،[١٨] أو هي فعل التواصل الذي يبلغ المعرفة.[١٩]

نلاحظ أن تلك الانتقادات للتعريف السابق هي انتقادات محقة كونها تربط بين الوجود المادي للمعلومات، وبين وجود وسيلة الاتصال التي تخرج بها المعلومة للوسط الخارجي.

ويرى بعض الفقهاء أن المعلومات ليست مقصورة على الكائنات الحية والجانب الأساسي لها ليس بناء العقل البشري، وإنما هي تشكل ظاهرة كونية ولذلك تم تعريفها بأنها إحدى الخصائص الأساسية للكون، وهي بذلك شأنها شأن الطاقة يمكن النظر إليها بشكل تدريجي، بغض النظر عن شكلها فهي ليست بالمدركات الحسية وليست بالمحتوى المحدد للرسالة، وإنما هي حامل العلاقات المتبادلة والتفاعل بين المدركات والمحتويات.[٢٠]

ونحن نتفق مع هذا الرأي؛ لأن المعلومات الإلكترونية هي نوع مستحدث من المعلومات، لها خصائصها الإلكترونية التي تنفرد بها عن غيرها من الأنواع الأخرى من المعلومات.

وقام بعض الفقهاء بتعريف المعلومة من خلال علاقتها مع البيانات:" فالمعلومات تتكون من عنصرين مادي يتمثل بالوسيط أو الكيان الذي يحوي أو تتجسد فيه المعلومة ومعنوي يتمثل في الدلالة او الفحوى أو المعنى ، ويشكل العنصر الأساسي للمعلومة، أما البيانات ففي صورتها الإلكترونية تتجسد بكيان مادي، يتمثل بالنبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة، وفي هذه الصورة تكون البيانات شيء له وجود في العالم الخارجي

---

[١٨] د. المري، راشد محمد المري: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، المرجع السابق، ص ٢١٢و ٢٩٠. د. خليل، عزة محمد محمود: مشكلات المسئولية المدنية في مواجهة فيروس الحاسب، دراسة في القانون المدني والشريعة الإسلامية برسالة دكتوراه، كلية الحقوق جامعة القاهرة، ١٩٩٤ ص ٣٧ وما بعدها. الدكتورة قشقوش، هدى حامد: جرائم الحاسب الإلكتروني، رقم ٣٦ ص١١٦-١١٧.

[١٩] د. فضل، سليمان أحمد: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ١٤١٣ه/٢٠١٣م، ص ١٧ إلى الصفحة ٢٣. قوره، نائلة عادل: جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى ٢٠٠٥، ص ٣٦٩-٣٧٠.

[٢٠] د. قاسم حشمت: المرجع السابق، ص ١٦. د. الجندي، حسني: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات ص ١٣٦ -١٣٨.

أما في صورتها التقليدية فليس لها وجود مستقل وإنما تكون للكيان المادي الموجودة فيه وبالتالي فهي تعد شيء معنوي".[٢١]

وفي نهاية التعريفات السابقة استنتجنا بأن التعريف الذي جاء به المشرع الإماراتي في المادة الأولى من القانون هو التعريف الأفضل، كونه بين بدقة ماهية المعلومات الحكومية محل البحث، وميز بينها وبين المعلومات غير الحكومية.

٤) المعلومات السرية:

وعرف المشرع الإماراتي البيانات والمعلومات السرية بأنها:" أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق يملك هذا الإذن"[٢٢].

من خلال هذا التعريف، فإنّ المشرع الإماراتي قد وضع معيار دقيق للسرية في المعلومات الحكومية، وهو معيار عدم إمكانية إطلاع العامة عليها، وهو ما يجعلها تتميز عن غيرها من المعلومات الأخرى المتاحة للجميع.

٥) بيانات خط السير:

كما أنه عرف بيانات خط السير بانها:" بيانات وسيلة تقنية المعلومات ينتجها نظام معلوماتي تبين مصدر الاتصال وواجهتي إرساله واستقباله، وساعته وتاريخه وحجمه ومدته ونوع الخدمة."

نلاحظ أن المشرع الاماراتي قد حدد في القانون الجديد نوع جديد من البيانات لم يكن معروفا سابقاً، ألا وهي معلومات وبيانات خط السير، والتي يتم من خلالها تتبع المعلومات الحكومية. وقد نص عليها في القانون الجديد في المادة الأولى حيث أن هذه البيانات لم تكن معروفاً مسبقاً في قانون مكافحة جرائم تقنية المعلومات. وهي تفيد الدولة من خلال تتبع أي معلومات ينشرها او يقوم بها أي شخص، وتفيد كذلك من ناحية أنها تسهل الوصول الى الجاني في حال قيامه بأي جريمة الكترونية.

---

[٢١] د. فكري، أيمن: جرائم نظم المعلومات رسالة دكتوراه كلية الحقوق جامعة المنصورة ٢٠٠٩ دار الجامعة الجديدة ٢٠٠٧، ص ٤٠. الكعبي، محمد عبيد: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ٢٠٠٩، ص ١٤٥.

[٢٢] مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠ / ٠٩ / ٢٠٢١ نشر بتاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.

٦) الموقع الإلكتروني الحكومي:

وعُـرّف الموقـع الإلكترونـي: بانـه:" مكـان أو مجـال افتراضـي علـى الشـبكة المعلوماتيـة يعتمـد علـى بـرامج ذكيـة تمكـن مسـتخدميه مـن إتاحـة أو تبـادل أو نشـر أي محتـوى، سـواء كـان نصـي أو صـوتي أو مرئـي أو بيانـات، ويشـمل مواقـع وشـبكات ومنصـات التواصـل الاجتمـاعي، والصـفحات والحسـابات الشخصـية والمدونات والخدمات الإلكترونية وما في حكمها[٢٣]".

والموقـع الالكترونـي الحكـومي شـأنه شـأن بـاقي المواقـع الالكترونيـة العاديـة التـي تـتم مـن قبـل الأشـخاص، حيـث يعنـى بـالموقع هـو اتاحـة المعلومـات علـى الشـبكة المعلوماتيـة، فيـتم خلـق موقـع الكترونـي خـاص بالحكومـات والمؤسسـات والهيئـات يـتم مـن خلالهـا ادراج كـل مـا يتعلـق بهـذه المؤسسـة او الهيئـة او الحكوميـة سـواء مـن ناحيـة اخبـار او وظـائف او بـرامج ونـدوات ومـؤتمرات، مـن خـلال توضـيحها فـي المنصـة الالكترونيـة بطريقـة تسـهل للزائـر المتصـفح برؤيتها.

٧) نظام المعلومات الإلكتروني:

وعـرف نظـام المعلومـات الإلكترونـي": برنـامج معلومـاتي أو مجموعـة البـرامج المعلوماتيـة المعـدة لمعالجـة أو إدارة أو تخـزين المعلومـات الإلكترونيـة القابلـة لتنفيـذ التعليمـات، أو الأوامـر بوسـائل تقنيـة المعلومـات، ويشـمل التطبيقـات أو مـا في حكمها[٢٤]".

ومـن هـذا التعريـف فـإن المشـرع الإمـاراتي قـد وضـع معيـار قـانوني لتمييـز النظـام المعلومـاتي الإلكترونـي عـن غيـره مـن نظـم تقنيـة المعلومـات، وهـو معيـار قابـل للتخـزين واسـترجاع المعلومـات، كمـا ان هـذا المعيـار هـو الـذي يميـز الـنظم الإلكترونية الحكومية عن غيرها.

---

(٢٣) مرسـوم بقـانون اتحـادي رقـم ٣٤ لسـنة ٢٠٢١ الصـادر بتـاريخ ٢٠ / ٠٩ / ٢٠٢١ نشـر بتـاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.

(٢٤) مرسـوم بقـانون اتحـادي رقـم ٣٤ لسـنة ٢٠٢١ الصـادر بتـاريخ ٢٠ / ٠٩ / ٢٠٢١ نشـر بتـاريخ ٢٦ / ٠٩ / ٢٠٢١ فـي الجريـدة الرسـمية. عفيفـي كامـل عفيفـي: المرجـع السـابق، ص ١٩٧-٢٠٨؛ د. قـورة، نائلة عادل: جرائم الحاسب الآلي الاقتصادية، مرجع سابق، ص١٩٢

اما في الفقه: فقد تم تعريفه من قبل البعض بأنه:" كل مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، الأشخاص والتي يمكن بواسطتها تحقيق وظيفة او هدف محدد[٢٥]".

ومن هذا التعريف يتضح أنه حصر النظام المعلوماتي الحكومي بمكونات الحاسب الآلي فقط دون التطرق إلى غيره من المكونات الأخرى، وهو بطبيعة الحال يعتبر تعريف ضيق.

كما عرفه البعض الآخر بانه "هو النظام الذي يحتوي على معلومات آلية تقنية مسماة محمية بإجراء أمني[٢٦]".

ومن هذا التعريف نرى أنه يتخذ معيار للتعريف، وهو المعيار الخاص بالإجراءات الامنية لحماية النظام المعلوماتي دون التطرق لمكوناته وعناصره.

ويؤثر فريق ثالث، القول إن نظام المعالجة الآلية للمعطيات هو تعبير يخضع للتطور السريع الذي يلحق بالبيئة الرقمية[٢٧]

ومما سبق من تعريفات توصلنا إلى أن ما جاء به المشرع الإماراتي هو التعريف الواسع والأشمل، الذي يبين كافة عناصر وخصائص النظام المعلوماتي الحكومي كونه يتضمن ماهية النظام المعلوماتي الحكومي القائم على المعلومات الحكومية الخاصة بمؤسسات الدولة ولا يشمل المعلومات الخاصة بالأفراد.

٨) المحتوى المعلوماتي:

---

[٢٥] د. العريان، محمد علي: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، ٢٠٠٤، م ٥٦. رمضان، مدحت عبد الحليم: الحماية الجنائية للتجارة الإلكترونية دراسة مقارنة، دار النهضة العربية ٢٠٠١ص٥١.

[٢٦] Guillaume Champy, La fraude informatique, tome 1, () Presses Universitaires d Aix-Marseille, 51992, p. 88.

[٢٧] د. الرابحي، عزيزة: الأسرار المعلوماتية وحمايتها الجزائية، دار هومة، الجزائر، ٢٠١٩، ص٥٦. الجندي، حسني: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ١٣٠.

وعـــرف المحتـــوى بأنـــه:": المعلومـــات والبيانـــات والخـــدمات الإلكترونيـــة التـــي يمكـــن أن تـــوفر قيمـــة للمتلقـــي فـــي ســـياقات محـــددة." ويضـــم المحتـــوى المعلومـــاتي العديد من الأمور هي التالي[٢٩]:

١- المواقـــع الثابتـــة: عبـــارة عـــن صـــفحة أو عـــدة صـــفحات بســـيطة التركيـــب وســـهلة التصـــميم؛ فـــالمحتوى عـــادة ثابـــت لا يتغيـــر، ويعـــرض لنـــا معلومـــات عـــن جهـــة أو شـــركة أو شـــخص مـــع محدوديـــة التفاعـــل مـــع هـــذا المحتـــوى. وبعـــض المواقـــع الثابتـــة قصـــيرة العمـــر؛ إذ تســـتخدم للتعريـــف بمنـــتج أو نشـــاط فـــي فتـــرة محـــددة ثـــم يـــتم إهمالهـــا أو حتـــى الاســـتغناء عنهـــا بعـــدها، فتصـــبح كمـــا يقـــال عنهـــا (مواقع غير نشطة).

٢- المواقـــع التفاعليـــة أو المتغيـــرة: يمكـــن تحـــديث محتواهـــا باســـتمرار، بإضـــافة صـــور ونصـــوص وغيـــره مـــن قبـــل المالـــك نفســـه، عـــن طريـــق لوحـــة تحكـــم بســـيطة تتطلـــب ابســـط معرفـــة تقنيـــة ممكنـــة. (مثـــل: بلـــوجر وفليكـــر، وحتـــى الفيس بوك).

٣- مواقـــع إدارة المحتـــوى: وفيهـــا يمكـــن تغييـــر أي جـــزء مـــن الموقـــع، كبرمجـــة محتـــوى او واجهـــة الموقـــع، ويســـتخدم فـــي المشـــاريع الكبيـــرة ويقـــوم عليهـــا أعلـــى البـــرامج المتخصصـــة وقواعـــد البيانـــات، وهـــو الأفضـــل والأغلـــى ســـعرة بين أقرانه السابقين (مثل موقع ويبلي، ويشابهه ايضاً ووردبرس).

ومـمـــا ســـبق، المشـــرع الامـــاراتي جـــاء بمصـــطلحات ومفـــاهيم جديـــدة فـــي قـــانون مكافحـــة الشـــائعات والجـــرائم الالكترونيـــة لـــم تكـــن موجـــودة ســـابقا، وهـــو مـــا يعتبـــر نقلـــة نوعيـــة فـــي النظـــام القـــانوني لمكافحـــة جـــرائم تقنيـــة المعلومـــات ويعـــود الســـبب لـــذلك إلـــى اتجـــاه المشـــرع الامـــاراتي إلـــى اتبـــاع سياســـة جنائيـــة خاصـــة بمواجهـــة الجـــرائم المســـتحدثة التـــي تظهـــر علـــى الســـاحة القانونيـــة والتقنيـــة تقـــوم علـــى تـــوفير الحمايـــة القانونيـــة للمعلومـــات والبيانـــات الحكوميـــة مـــن الاختـــراق أو الاعتـــراض، كمـــا أن المشـــرع الامـــاراتي قـــد أحســـن فـــي تجريمـــه لأفعـــال الـــدخول غيـــر المشـــروع لمنظومـــة معلوماتيـــة حكوميـــة ، لمـــا لهـــذه الجريمـــة مـــن أثـــر ســـلبي علـــى تقـــديم الخـــدمات الحكوميـــة، وبالتـــالي التـــأثير علـــى جـــودة تلـــك الخـــدمات، حيـــث أن دولـــة الإمـــارات العربيـــة المتحـــدة مـــن الـــدول الســـباقة إلـــى تطـــوير التشـــريعات الجنائيـــة

---

[٢٩] د. فكري ايمن عبد الله: جرائم نظم المعلومات المرجع السابق، ص ١٧٦.

الخاصة ضمن منظومة تشريعية متميزة وحديثة تضمن حماية أمن المعلومات الحكومية حيث أن القانون الجديد يعتبر نقلة نوعية في مجال التشريعات الجنائية الخاصة ومكافحة جرائم تقنية المعلومات التي تعتمد على الهجوم السيبراني.

كما ان جميع التعريفات السابقة تتفق مع بعضها البعض في نقطة واحدة مهمة هي أن النظام المعلوماتي هو نظام قائم على البيانات والمعلومات التي يتم تخزينها بشكل الكتروني وتستخدم في معالجة البيانات أنظمة خاصة وفق برامج وقواعد تقنية المعلومات.

الفرع الثاني

الطبيعة الخاصة لمحل جريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة

إن محل الجريمة هو الأنظمة المعلوماتية لمؤسسات الدولة والمرافق الحيوية فيها، وعليه نبين في هذا المطلب محل الجريمة وفق ما جاء به المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ على النحو الآتي:

أولاً: تعريف المرافق الحيوية:

لم يعرف المشرع الإماراتي المرافق الحيوية في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، وإنما أشار إليها في نصوص بعض المواد منه حيث تنص المادة (٥) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ على أنه:" يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٥٠٠,٠٠٠) خمسمائة ألف درهم ولا تزيد على (٣,٠٠٠,٠٠٠) ثلاثة ملايين درهم، كل من تسبب عمدا في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية. فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفا مشددا."

ومنه يمكن تعريف المرافق الحيوية بانها: مرافق هامة وذات أهمية كبيرة بالنسبة للدولة مثل وزارة الدفاع ووزارة الداخلية والمنشآت الخاصة بالطاقة النووية، وهي مرافق لها خاصية سرية".

ومن نص هذه المادة نستنتج أن محل الجريمة هو الدخول عير المشروع إلى موقع إلكتروني، أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية.

ويتحقق السلوك أو النشاط الإجرامي المكون لجريمة الإتلاف المعلوماتي بجميع الأفعال التي تؤدي إلى إتلاف النظم المعلوماتية، كما يتحقق بأي نشاط يؤدي إلى إعدام صلاحية المحل المعلوماتي، وقد جاءت التشريعات بتعبيرات مختلفة للدلالة على هذا السلوك ومنها تعبير "الإتلاف" و"التدمير" و"التخريب" و "محو البرامج والبيانات" و"التشويه" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل البيانات أو المعلومات أو البرامج والمحررات المعلوماتية غير صالحة للاستعمال كلياً أو جزئياً.

المطلب الثاني

اركان جريمة اختراق الأنظمة المعلوماتية الأمنية الخاصة بمؤسسات الدولة

يتطلب المشرع الإماراتي توافر الركن المادي والركن المعنوي لتجريم اختراق الأنظمة الإلكترونية الحكومية، حيث أن الركن المادي يتمثل في السلوك الإجرامي والسببية والركن المعنوي يتمثل بتوافر القصد الجنائي القائم على العلم والإرادة وهنا نبين في هذا المطلب أركان جريمة اختراق الأنظمة المعلوماتية من خلال فرعين على النحو الآتي:

الفرع الأول

الركن المادي

أولاً: تعريف الاختراق.

عرف المشرع الإماراتي في المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية بأن **الاختراق**:" هو الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها."

وهنا يتبادر للذهن سؤال مهم: حول **طبيعة جريمة اختراق منظومة معلوماتية حكومية، وهل هي تختلف عن جريمة اختراق الحساب الالكتروني الشخصي؟** والجواب عن هذا السؤال، يكون من خلال النظر إلى عنصر الخطورة في كل نوع من أنواع هذه الجرائم، حيث أن خطورة الدخول إلى منظومة معلوماتية حكومية هي الأكثر خطرا على المجتمع، مما هو عليه الحال في جريمة الدخول غير المشروع على حساب شخصي.

يقصد بالاختراق الدخول غير المرخص به او المخالف الأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها[٣٠]

وعرف الاختراق في القانون العربي النموذجي الموحد في شان جرائم إساءة استخدام تقنية المعلومات بأنه الدخول غير المصرح به او غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية[٣١].

نلاحظ أن مؤدي مما تقدم بأن الشارع في بعض القوانين العربية لم يعرف المقصود بالدخول، ولا ينصرف المقصود بالتوصل إلى الدخول إلى الموقع او النظام المعلوماتي بالمعنى المادي، كما في الدخول إلى الغرفة التي يوجد بها جهاز الحاسب، وإنما ينصرف فعل التوصل إلى النشاط الذهني الذي يقوم به الجاني للوصول إلى موقع على الحاسب، أو إلى نظام معلوماتي به، ولذلك يكون هذا الدخول ذات طبيعة معنوية. وقد يرتكب الفعل المادي للتوصل عن طريقه إلى اختراق الإجراءات الأمنية التي تحمي الموقع أو النظام المعلوماتي.

حيث أن مفهوم ومدلول الاختراق ينصرف إلى اتباع مرتكب الجريمة لخاصية الهاكرز، بهدف الوصول إلى المنظومة المعلوماتية الحكومية بقصد ارتكاب العديد من الأفعال والجرائم التي تنطوي على التأثير على المنظومة الحكومية.

---

[٣٠] المادة (١) من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

[٣١] د. فكري، ايمن عبد الله:جرائم نظم المعلومات المرجع السابق، ص ١٧٨.

ثانياً: السلوك الإجرامي في جريمة الاختراق

الواقع أن الاختراق كسلوك فني لا يعني جريمة الدخول غير المصرح به للنظام المعلوماتي، كما يخلط بينهما البعض، ولكنه سلوك فني يترتب عليه الدخول غير المصرح به للنظام المعلوماتي، ومن هذه المادة يتضح أن الركن المادي للاختراق يقوم على فعل الدخول غير المرخص به، أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة، أو البقاء بصورة غير مشروعة في نظام معلوماتي حكومي[٣٢].

يتمثل السلوك او النشاط الإجرامي في دخول الجاني عمدا أو عن طريق الخطأ والبقاء بدون وجه حق، او تجاوز حدود الحق المخول له من حيث الزمان، أو مستوى الدخول او اختراقه موقع أو بريد الكتروني، أو حساب خاص، او نظام معلوماتي يدار بمعرفة أو لحساب الدولة او أحد الأشخاص الاعتبارية العامة، أو مملوكة لها او يخصها. ويشمل أفعال الدخول سواء عن طريق العمد أم عن طريق الخطأ، والبقاء بدون وجه حق او تجاوز حدود الحق المخول للشخص من حيث الزمان أو مستوى الدخول، وكذلك اختراق الموقع أو البريد الالكتروني. ومؤدى ذلك أن يتجسد النشاط الإجرامي في العناصر التالية:[٣٣]

١) فعل الدخول أو البقاء اور الاختراق على النحو المار بيانه.

٢) أن يكون هذا الدخول إلى موقع او بريد الكتروني أو حساب خاص، أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة او مملوكة لها أو يخصها.

٣) أن يكون الدخول أو البقاء بغير وجه حق.

٤) أن يحدث السلوك الإجرامي عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات[٣٤]

---

[٣٢] د. الشريف، محمد عبد العزيز: السلوك الإجرامي الإلكتروني، مركز الحضارة العربية، القاهرة، مصر، الطبعة الأولى، ٢٠١٦م، ص٣١٧.

[٣٣] د. الحسيني عمار عباس: جريمة الإتلاف المعلوماتي المرجع السابق، ص٤٩

[٣٤] د. الجندي حسني: المرجع السابق، ص ٢٤٤.

وتتم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد؛ بسبب التعقيد الذي تتصف به نظم تشغيل الحاسبة الالكترونية والشبكات المعلوماتية[٣٥]

ان عناصر السلوك الإجرامي في جريمة اختراق النظام المعلوماتي تتمثل في الأفعال التي يقوم بها مرتكب الجريمة، مثل فعل تحديد الموقع الحكومي المستهدف في الاختراق، وايضا فعل الدخول غير المشروع بقصد الاختراق، وهنا يمكن القول بأن جريمة اختراق الموقع الحكومي ليست من الجرائم الواضحة والتي بسهل تحديد لعناصر السلوك الإجرامي بها، ولكنها من الجرائم الغامضة التي يصعب اكتشافها في بدايتها، بل إنها تتم عبر مراحل في غالب الأحوال لا يمكن اكتشاف عناصر السلوك الإجرامي فيها إلا بعد وقوع نتيجة الجريمة.

فالاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاصة بالهدف، فالمخترق لديه القدرة على دخول أجهزة الأخرين عنوة دون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها، سواء بأجهزتهم الشخصية أو نفسياتهم فما الفرق بين مخترق الأجهزة الشخصية ومقتحم البيوت الآمنة[٣٦].

ويعتبر الاختراق أهم وسائل ارتكاب الجريمة المعلوماتية وقد يطال الأجهزة والوسائل الفنية المؤمنة لتلك الأجهزة وغيرها ويمكن إيجاز ذلك على النحو التالي[٣٧]:

---

[٣٥] الأستاذ الفيل، علي عدنان: الإجرام الالكتروني، بيروت، منشورات زين الحقوقية، الطبعة الأولي ٢٠١١، ص ٨٧.

[٣٦] د. بنيه، نسرين عبد الحميد: الجريمة المعلوماتية والمجرم المعلوماتي، منشاة المعارف الإسكندرية، ٢٠٠٨، ص١٩٣.

[٣٧] د. بنيه، نسرين عبد الحميد: مرجع سابق، ص١٤٥.

أ- اختراق المزودات "مزودات الخدمة أو الأجهزة الرئيسة للشركات أو المؤسسات او الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة ما توضع لحمايتها، وغالبا ما يتم ذلك باستخدام المحاكاة وهي مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام.

ب- التعرض للبيانات اثناء انتقالها والتعرف على شفرتها إن كانت مشفرة، وهذه الطريقة تستخدم في كشف بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية.

ت- اختراق الأجهزة الشخصية، وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من برامج الاختراق سهلة الاستخدام.

ويحتاج التسلل إلى جهاز الضحية دون علمه إلى مجموعة من الأدوات والوسائل الخاصة، فهذه الأخيرة قد تكون بعض البرامج الموجودة داخل نظام التشغيل نفسه أو بعض البرامج التي صممت خصيصا لتسهيل عمليات الاختراق وتجنب استخدام العديد من الأوامر المعقدة.

ان جريمة الاختراق الالكتروني للموقع الالكتروني الحكومي هي من الجرائم متعدية القصد الجنائي، اي أن القصد الجنائي فيها يتعدى المتوقع منه، بمعنى أنها من الجرائم التي تكون فيها النتيجة الإجرامية مؤثرة بشكل كبير على الجهات الحكومية.

حيث تتوافر سوء نية الجاني، إذا كان دخوله إلى النظام نتيجة اختراقه لجهاز الأمن الذي يحمي النظام أو معرفة الرقم السري أو الشيفرة بطريق غير مشروع ودخل بواسطتها إلى النظام، أما إذا كان الجاني قد سبق له الاشتراك في النظام، ولكن انتهت مدة الاشتراك ودخل إلى نظام معتقدا خطأ بأنه ما زال له الحق في الدخول إليه فإن ذلك يعد جهلا بالواقع مما ينفي القصد الجنائي لديه، أما إذا دخل شخص إلى النظام بطريق الخطأ وبحسن نية وخرج منه فورا عند علمه بأنه لا يحق له الدخول إلى هذا النظام، فإنه لا يسأل جنائيا

لانتفاء القصد الجنائي لديه، أما إذا دخل بطريق الخطأ ولكنه بقي يتجول داخل النظام مع علمه بذلك فإنه يقع تحت طائلة المسؤولية[٣٨].

وإن سوء النية يكون من خلال قيام مرتكب الجريمة بالبقاء في الموقع الإلكتروني الذي دخل إليه ومحاولته العبث به إما بالحذف او التهكير، وذلك باستخدام تقنيات حديثة بهدف التأثير على البيانات ومحاولة العبث بها، وهنا تنوه الباحثة إلى أمر في غاية الأهمية هو أن التثبت من حسن النية أو سوء النية هو أمر من الصعب تقديره وهنا يرجع الأمر إلى تقارير الخبراء الفنيين لأن هذا الأمر من الصعب التحقق منها في الفضاء السيبراني، وهنا تقدم تقدم الباحثة اقتراح بإضافة مادة غلى القانون الاماراتي تحدد المعيار الذي يفرق بين حسن النية وسوء النية في البقاء في الموقع الالكتروني الحكومي.

وبعد عرض الأفعال التي يتكون منها الركن المادي لجريمة الاختراق يتضح لنا أن جميع ما تم ذكره من أفعال يتكون منها الركن المادي للجريمة ليست أفعال حصرية، حيث أن هناك الكثير من الأفعال التي يرتكبها الجاني في البيئة التقنية؛ لان الجرائم الخاصة بالاختراق للأنظمة الحكومية تستخدم فيه أساليب حديثة لا يمكن حصرها، حيث أنها تعتمد على القدرة التقنية التي يتمتع بها الجاني كونه من ذوي الخبرة في مجال استخدام التقنيات الحديثة.

ثالثاً: أنواع السلوك الإجرامي في جريمة الاختراق

تتعدد وتتنوع أساليب الاختراق، ويمكن إجمالها فيما يلي:

١- الاختراق عن طريق استعمال نظم التشغيل:

لأن نظم التشغيل مليئة بالثغرات، فإنه يتم استغلالها في عمليات الاختراق، ولكن الأهم هو القيام بذلك عن طريق البروتوكولات التي يستخدمها النظام للتعامل مع شبكة الانترنت او الشبكات الداخلية بأنواعها. ويمر المتسلل بعدة مراحل حتى يتمكن من اختراق الحاسب الآلي لغيره وهي: يبحث المخترق أولا عن ضحيته، وذلك بمعرفة (iP الخاص به، والبحث عن هذا الرقم يتم بمجموعة من الخطوات يقوم بها المخترق على جهازه، لكن يجب كذلك أن

(٣٨) د. رابحي عزيزة: الأسرار المعلوماتية وحمايتها الجزائية اطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، مرجع سابق، ص ١٦٧-١٦٨.

يكون متصلا بجهاز الضحية عن طريق شبكة الانترنت أو شبكة داخلية، وذلك في لحظة معينة، لأن هذا الرقم يتغير دائما مع كل اتصال جديد بالإنترنت. بعد تحديد رقم IP يحدد المخترق إمكانية اختراق جهاز الضحية عن طريق مجموعة من الخطوات ورقم الآي بي "رقم ديناميكي متغير، فهو يتغير في كل مرة يدخل الشخص على شبكة الانترنت [٣٩] فالآي بي IP هو بمثابة البطاقة الشخصية للمستخدم على شبكة الانترنت، يمنحه مزود الخدمة للمشترك آليا بمجرد طلب الخدمة ليمكنه من الولوج إلى الشبكة العالمية ، وينتج عن الآي بي معرفة بعض المعلومات الشخصية عن المستخدم في عالم الانترنت، كنوع من البريد المرسل والمواقع التي قام بزيارتها وغرف المحادثة التي قام بالدخول إليها، وذلك في سجل خاص لدى مزود خدمة الانترنت وهو ذا أهمية بالغة؛ إذ أنه يعتبر من الأمور المهمة والمساعدة في عملية الاختراق، فهو يشبه إلى حد كبير رقم الهاتف المنزلي، فعندما يريد شخص الاتصال بأخر، يقوم بطلب رقم هاتفه المنزلي ليستطيع الاتصال به أو التحدث إليه، كذلك رقم الآي بي فعندما يريد شخص أن يخترق جهاز شخص آخر فلا بد له من معرفة رقم الأي بي، حتى يتسنى له إدخال إحدى البرامج المتخصصة في عملية الاختراق ليتمكن من الاتصال بجهازه[٤٠].

يتبين لدينا مما سبق بأن استخدام نظام تشغيل الحاسب الآلي في ارتكاب الجريمة هو السمة الأبرز في تلوين عناصر السلوك الإجرامي، ولا يعني البقاء لزوم أن يقوم المخترق بارتكاب جريمة أخرى، وإنما يكفي أن يستمر في حالة بقاء دون أن يقوم بأي نشاط أو حركة تقنية سواء إيجابية تفيد الحاسوب أم سلبية تضر به.

ويمكن التمييز بين البقاء بشكل إرادي والبقاء في شكل سلبي، فالبقاء بشكل إيجابي يعني لزوم أن يكون مستخدم الحاسوب على دراية مسبقة معلنة موافقته على هذا البقاء في وثيقة نظام الحاسوب، كنظام التشغيل مثلا إذ يكون من حق مروج نظام التشغيل في بعض الأحيان التدخل في نظام تشغيل

---

(٣٩) د.الرومي ، محمد امين ،جرائم الكمبيوتر والانترنت ،دار المطبوعات الجامعية ، ٢٠٠٣ ، ص ١٣٧.

(٤٠) د. الشقيري، محمد مصطفى: السرية المعلوماتية، ضوابطها واحكامها الشرعية، دار النشر الإسلامية، بيروت لبنان، ٢٠٠٨، ص ٣٤١-٣٤٢.

الحاسوب المستخدم لكي يعدل فيه بقصد تطويره. ولذا يكون من الضروري الحصول مسبقا على موافقة مستخدم الحاسوب، وهي موافقة ضرورية؛ لأنها تبرر الاختراق، ومن ثم يلزم موافقة المستخدم لإعلان مشروعية مثل هذا الاختراق. ومن ثم فإنه كلما كان هناك توافر الإرادة المستخدم في الاختراق والبقاء، فإن الجريمة لا تقوم حتى ولو كانت هذه الإرادة متوافرة، كشرط مسبق لتشغيل نظام الحاسوب، وإنما تقوم جريمة البقاء إذا انتفت إرادة مستخدم الحاسوب مطلقا، وفي هذه الحالة الأخيرة يقوم نشاط سلبي يدعو إلى التجريم.

وأساس ذلك من ناحية أن كون الاختراق جريمة شكلية لا يفيد لزوم البقاء في نظام الحاسوب دون سند من المشروعية، باعتبار أن البقاء تعد جريمة أخرى في القانون وفق نص المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ التي تنص على أنه:" الاختراق: الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها.". إذ يكتفي هذا القانون بمجرد البقاء للقول بتوافر جريمة بقاء في نظام المعالجة الآلية للبيانات. ومن ناحية أخرى، يلزم في جريمة البقاء ألا يقوم المخترق بارتكاب ما من شأنه أن يغير في وصف الجريمة فيحيلها إلى جريمة أخرى، كان يقوم بتخريب النظام المعلوماتي او تدميره او انتهاك الحق في خصوصية بعض الوثائق أو سرقة بيانات مخزنة أو وضع فيروسات. . . الخ[٤١].

٢- الاختراق باستخدام البرامج:

لابد لقيام الاختراق بهذه الطريقة من وجود برنامجين، أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم " serve"؛ لأنه بمثابة الخادم الذي يتأمر بأوامر المخترق، وينفذ المهام الموكلة إليه داخل جهاز الضحية، وثانيهما برنامج يوجد بجهاز المخترق ويسمى ببرنامج المستفيد clientالعميل وأشهر

---

(٤١) lol n 200 du mars 2004 jorf 10 more 2004 JUSX0300028L٢-١٢١
د. يونس، عمر محمد ابوبكر ، الجرائم الناشئة عن استخدام الانترنت ، مرجع سابق ، ص ٣٣٤ و٣٣٥ .

مثال على هذه البرامج واخطرها هو برنامج حصان طروادة، فهو، يتمتع بمجموعة من المميزات تجعل الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه[٤٢].

ان برنامج حصان طروادة في ابسط صوره، يقوم بتسجيل كل ما تقوم بكتابته على لوحة المفاتيح منذ أول لحظة للتشغيل، وتشمل كل البيانات السرية أو الحسابات المالية أو المحادثات الخاصة على الانترنت او رقم بطاقة الائتمان الخاصة أو حتى كلمات السر التي تستخدمها للولوج إلى الشبكة العنكبوتية، والتي قد يتم استخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية[٤٣].

ويتم إرسال هذا البرنامج إلى جهاز الضحية بعدة طرق، لعل أشهرها إرسال بالبريد الالكتروني، إذ يقوم المخترق بإرسال رسائل إلى الضحية يرفق بها ملفا يحمل حصان طروادة، ليقوم الضحية بفتحها وتحميل الملف المرفق على أنه أحد البرامج المفيدة، ليكتشف بعدها أنه لا يعمل، فيظن أنه به عطلا ليقوم بإهماله، فيحتل حصان طروادة مكانه داخل النظام ويبدأ مهامه التجسسية، وحتى لو قام الضحية بحذف البرنامج فلا فائدة من ذلك، إذ يكفي أن يعمل هذا البرنامج لمرة وحدة فقط حتى يقوم بمهامه. وهناك طرق أخرى لإرسال هذا الملف، كاستخدام برامج الدردشة مثل برنامج YAHO0و MSN أو icd أو MESSENGER[٤٤]

٣- جمع كلمات السر والتقاطها:

إذا كانت أنشطة الاعتداء التي تتم باستعمال كلمة السر تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها تشمع او التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها

---

[٤٢] د.خليفة، محمد: المرجع السابق، ص ٤٢.

[٤٣] الأستاذ أبو الحجاج، يوسف: أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، الطبعة الأولى، ٢٠١٠، ص١٣.

[٤٤] الزيدي، عيسى سليم داوود: جرائم القرصنة الإلكترونية، دار شتات للنشر، مصر والإمارات، ٢٠١٦م، ص١٢٣.

لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول ١٢٨ بايت أو أكثر مثلا من كل اتصال بالشبكة التي تجري مراقبتها تتبع حركة الاتصال عليها. وعندما يطبع المستخدم كلمة السر أو اسمه، فإن البرنامج (الشمام) يجمع هذه المعلومات وينسخه إضافة إلى أن أنواعا من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطه معاً، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها[٤٥] .

٤- المسح والنسخ:

هو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة، ويستخدم تحديثا بشأن احتمالات كلمة السر او رقم هاتف الموزع أو نحو ذلك، وأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى احدها الذي يستخدم موزع للاتصال بالإنترنت، أو إجراء مسح الاحتمالات عديدة لكلمة سر للوصول إلى الكلمة الصحيحة التي تمكن المخترق من الدخول للنظام، ومن جديد فإن هذا أسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من اعتماد على التخمين البشري[٤٦]

٥- استغلال المزايا الإضافية:

الأصل أن مستخدم النظام يحدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، ولكن في الواقع العملي يحدث أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصه ورغباته في هذه الحالة، فإن أي مخترق للنظام لن يكون قادرا فحسب على تدمير معطيات المستخدم أو التلاعب بها، من خلال اشتراكه أو عبر نقطة الدخول الخاصة به وبكل بساطة سيتمكن من تدمير مختلف ملفات النظام ، حتى تلك غير المتصلة بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله، وأعظم مثال على هذا الخطر في العالم المادي أنه يمكن شخص من دخول

---

[٤٥] PETER SWIFT: HACK MAN MENACE OF THE KEYBOARD CRIMINAL BRITICH TELECOM WORLD MAG, HALF OF SEPT 1989 P 13-14.

[٤٦] د. سويلم، محمد علي: شرح قانون جرائم تقنية المعلومات- القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة تقنية المعلومات، دار المطبوعات الجامعية، ط ١، ٢٠١٩ م. ص١١٢.

غرفة مدير فندق القصد سرقته فيجد في غرفته مفاتيح كافة قاصات الأمانات، أو مفتاح الماستر الذي يفتح غرفة الفندق جميعها ولهذا فتحديد الامتيازات والصلاحيات قد يمنع في حقيقته من حصول دمار شامل ويجعل الاختراقات غير ذات أثر[٤٧]

تتسم هذه الجريمة بالخصائص التالية[٤٨]:

١) تندرج هذه الجريمة ضمن طائفة جرائم الصفة المطلقة. فلا يشترط توافر صفة معينة في الفاعل، ومن ثم يمكن أن يقع السلوك الإجرامي من أي شخص، محترفة أم غير محترف، عاملا في الجهة التي حدث فيها اتلاف أو تعطيل أو ابطاء أو تشويه أو أخفاء أو تغيير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.
٢) ان السلوك ذات طبيعة الكترونية لكي يتلاءم استعماله مع شبكة المعلومات ووسائل تقنية المعلومات الأخرى، التي هي في ذات الوقت ذات طبيعة الكترونية.
٣) انه نشاط ايجابي ويتحقق بطريق الارتكاب أو بفعل إيجابي، ومن ثم لا يتحقق بسلوك سلبي أو بمجر الامتناع.
٤) أن هذه الصور تدخل ضمن طائفة الصور التبادلية، وبالأحرى الجرائم ذات السلوك التبادلي التي يكفي لقيام الركن المادي بارتكاب أحد الأفعال او الصور التجريمية، كما تقع الجريمة بارتكاب أحد الأفعال دون أن يعد ذلك تعدداً مادياً للجرائم.
٥) ان هذه الجريمة تضم افعال تندرج ضمن طائفة الجرائم الوقتية مما يترتب عليه تحديد بدء حساب مدة تقادم الدعوى الجنائية، من اليوم التالي لارتكاب الفعل وهو دخول الجاني عمدا أو عن طريق الخطأ أو تجاوز حدود الحق المخول له، أو اختراقه موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصه. كما تضم فعل

---

[٤٧] د. خليفة محمد، مرجع سابق، ص ٤٥.
[٤٨] د. سويلم، محمد علي: شرح قانون جرائم تقنية المعلومات- القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة تقنية المعلومات المرجع السابق، ص ١١٧.

مستمر وهو الدخول بخطأ غير عمدي والبقاء بدون وجه حق، ومن ثم يبدا تقادم الدعوى الجنائية من اليوم التالي الانتهاء حالة الاستمرار.

٦) تعتبر من جرائم الوسيلة المطلقة ذات القالب الحر؛ إذ لم يشترط ارتكاب الجريمة عن طريق وسيلة معينة[٤٩]

العنصر الثاني محل السلوك هو موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة، أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصها.

الفرع الثاني

الركن المعنوي

تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي، ويتألف القصد الجنائي من عنصرين، هما: العلم والإرادة، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي، وهو دخوله عمد أو عن طريق الخطأ والبقاء بدون وجه حق أو تجاوز حدود الحق المخول له من حيث الزمان، أو مستوى الدخول او اختراقه موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة، أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصها ويتعين أن يعلم الجاني بخطورة فعله على محل الجريمة الذي ينالله الاعتداء بارتكاب الجريمة، ومن ثم إذا أتي فعله وهو يعتقد أنه لم يدخل أو يتجاوز بغير وجه حق، والتزم حدوده، انتفى عنصر العلم ومعه القصد الجنائي[٥٠]

كما ينبغي أن تتجه إرادة الجاني إلى أحد الأفعال التبادلية الواردة بالنص، فإذا انتفت هذه الإرادة انتفى القصد الجنائي، كما لو حدث الفعل نتيجة خطأ أو رعونة أو إهمال، وخرج على الفور ولم يتحقق البقاء بدون وجه حق أو

---

[٤٩] د. الجندي، حسني: المرجع السابق، ص ٢٤٣-٢٤٤.

[٥٠] المرجع السابق، ص ٢٤٣-٢٤٤.

التجاوز [٥١] ولا أهمية للباعث على السلوك الإجرامي؛ إذ لا يعتد القانون باي منها [٥٢]

وتنفرد جريمة الدخول غير المشروع ببقاء بنيانها على أساس ثنائي على الرغم من أن الشارع المقارن اعتبرهما في أغلب الأحيان جريمة شكلية، فالشارع يعاقب على مجرد الاختراق ثم إنه في ذات الوقت يجل من هذه الجريمة شتائية الموضوع بشكل سيء. وبيان ذلك أن الاختراق كجريمة شكلية يتطلب النفاذ إلى نظام حاسوب عبر الانترنت، اي يقوم المخترق بنشاط الدخول دون أن يكون له صلاحية أو مشروعية في الدخول إليه. وتتحقق صورة علم المشروعية في عدم صلاحية الدخول إلى نظام الحاسوب وبصورة يبرز فيها المخترق كما لو كان ممن لا تتحقق فيهم شروط إلى نظام حاسوبي. فالأصل في الاختراق ليس كونه جريمة شكلية وإنما يعد جريمة ثنائية الطابع إذ يوجد الاختراق، ثم بعد ذلك جريمة او سلسلة الجرائم الأخرى التي يتم ارتكابها على أثر الاختراق، بمعنى أنه لا يمكن أن ينشأ عن الاختراق اي ارتباط بحسن النية، ولو كان المخترق من دعاة السلام؟؟؟ "هاكر" [٥٣].

ومفاد ذلك أن الدخول غير المشروع يعني اختراق حواسيب مختلفة لغاية ارتكاب جرائم أخرى غير جريمة الاختراق فالفرض ان هناك دخول غير مشروع إلى الانترنت، ثم يتم بعد ذلك جريمة انتهاك لنظم المعالجة الآلية البيانات محظور الدخول إليها كما لو كانت هذه النظم مشفرة أو يلزم الحصول على كلمات للولوج إليها، مما يعني ضرورة توافر صفة معينة وصلاحيات معينة أيضا. ولا يعني ذلك ضرورة تحقق نتيجة معينة فقد يكون المقصود من الدخول نسخ ملفات معينة، كان يستهدف المخترق نسخ كود المصدر البرمجيات معينة بحيث يمكنه تقليدها فيما بعد. فالمقصود ليس مجرد الدخول إلى الانترنت، وإنما يلزم أن يكون هناك اختراق محدد لنظام حاسوبي، بمعنى أن الجريمة تتشابه مع حالة ارتكاب شخص لجريمة الدخول

---

[٥١] د. الملط، احمد محمد خليفة: الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، ٢٠٠٤، ص ٥٢٩

[٥٢] د. الجندي، حسني: المرجع السابق، ص١٣٨.

[٥٣] د. يونس، عمر محمد أبو بكر: الجرائم الناشئة عن استخدام الانترنت، ص ٣٢٧، ٣٣٧.

إلى نظام حاسوبي خاص في حاسوب غير مملوك له وليس له عليه كلمة مرور، وإنما مباح له تشغيله لسبب خاص او عام، أو كما يطلق عليها جريمة الدخول إلى ملفات وبرمجيات مخزنة في حاسوب[٥٤]

يتبين لدينا أن الركن المعنوي في جريمة التعدي أو اختراق النظم المعلوماتية أو نظم معالجة البيانات هي جريمة عمدية في كل صور السلوك الإجرامي فيها، والتي سبق ذكرها في الركن المادي، وصورة الركن المعنوي منها هو القصد الجنائي بعنصريه العلم والإرادة، فيجب أن يعلم الجاني أن نشاطه غير مشروع، وأنه يعتدي على صاحب الحق إلى فعل الاختراق أو البقاء أو الدخول غير المشروعين أو أي فعل كالمحو أو التعديل أو التلاعب أو الإعاقة أو الإفساد وهذه كلها هي صور السلوك الإجرامي، رغماً عن إرادة صاحب الحق في المعطيات أو من له السيطرة عليها.

المبحث الثاني

الأحكام الخاصة بعقوبات جرائم الاختراق السيبراني

حتى نتمكن من الإحاطة بالأحكام الخاصة بالعقوبات على جريمة الهجوم السيبراني، لابد لنا في البداية أن نبين الأحكام الخاصة بالعقوبات بشكل عام، وفق ما جاء به المرسوم بقانون اتحادي رقم (٣١) لسنة ٢٠٢١ بشأن الجرائم والعقوبات، ومن ثم نتطرق للأحكام الخاصة بالعقوبات الواردة في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، وعليه نبين في هذا المبحث الأحكام الخاصة بعقوبات جرائم الاختراق السيبراني من خلال مطلبين على النحو التالي:

المطلب الأول

الاحكام الخاصة بالعقوبات في قانون مكافحة الشائعات والجرائم الالكترونية.

بين المشرع الإماراتي عقوبة اختراق الأنظمة المعلوماتية الحكومية في نص المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ على أنه[٥٥]:"

---

[٥٤] د.يونس، عمر محمد ابو بكر: الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص ٣٢٩.

[٥٥] مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠ / ٠٩ / ٢٠٢١ نشر بتاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.

١) يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.

٢) وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة

أولاً: انواع العقوبات.

ومن هذه المادة نرى أن المشرع الإماراتي قد تدرج في العقاب على جريمة اختراق المنظومة المعلوماتية الحكومية، حيث أن الفقرة الأولى من هذه المادة بينت العقوبة بأنها بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.

أما الفقرة الثانية فقد شددت العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو

نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

كما أن المشرع الإماراتي في نص الفقرة الثالثة من المادة شدد العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

كما عاقب المشرع المصري على هذه الجريمة بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدة، أو بخطأ غير عمدي وبقي بدون وجه حق، او تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول او اخترق موقعة أو بريدة إلكترونية أو حسابا خاصة أو نظام معلوماتية يدار بمعرفه او لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكة لها، او يخصها.

مما سبق نستنتج ان هذه العقوبة جاءت موفقة كونها تعتبر من العقوبات الشديدة التي يكون لها أثر كبير في الحد من الجريمة، ولكن على الرغم من ذلك لابد من تشديد العقوبة أكثر مما هو عليه لكي تكون رادعا للحد من الجريمة.

تنص المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ على أنه:"

١) يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.
٢) وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد

على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

من خلال ما ودر في نص المادة (٣) من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية، يتضح لنا أن المشرع الإماراتي جاء ببعض الأحكام الخاصة بجريمة اختراق الأنظمة المعلوماتية الإلكترونية، ومن سياق المادة الثالثة يتضح لنا أن الأحكام الخاصة تتمثل في الآتي:

١) الأحكام الخاصة بجريمة اختراق الموقع الإلكتروني أو نظام المعلومات الإلكتروني أو شبكة المعلومات أو أية وسيلة تقنية معلومات تعود لمؤسسات الدولية.

٢) الاحكام الخاصة بالاختراق بغرض إحداث الضرر أو التدمير أو الإيقاف عن العمل أو التعطيل للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

٣) الأحكام الخاصة بالاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

وهنا يمكن القول بأن المشرع الإماراتي في نص المادة (٣) من المرسوم بقانون اتحادي قد بين أحكام هذه الانواع الثلاثة من الجرائم وهي ما سوف نتناوله على النحو الآتي:

لقد بين المشرع الإماراتي في الفقرة الأولى من نص المادة (٣) من المرسوم بقانون اتحادي نوع السلوك الإجرامي الذي يمثل جريمة اختراق الموقع الإلكتروني أو نظام المعلومات الإلكتروني أو شبكة المعلومات أو أية وسيلة تقنية معلومات تعود لمؤسسات الدولية. وهو فعل الاختراق ذاته، ويعاقب المشرع الإماراتي على هذا النوع من الجرائم بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، وهنا يتضح لنا أن المشرع الإماراتي نص على عقبة السجن المؤقت وعقوبة الغرامة وحدد الحد الأدنى للغرامة والحد الأعلى لها،

أما النوع الثاني من جرائم الاختراق الواردة في الفقرة (٢) من المادة الثالثة من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ الخاصة بالاختراق بغرض إحداث الضرر أو التدمير أو الإيقاف عن العمل أو التعطيل للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية. نلاحظ هنا ان المشرع الإماراتي ربط مابين جريمة الاختراق وما بين النتيجة الإجرامية التي تنتج عنها حيث اعتبر أن النتيجة الإجرامية تتمثل في الأفعال التالية:

- إحداث الضرر للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات
- التدمير للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات
- الإيقاف عن العمل للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات

- التعطيل للمواقع الإلكترونية أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات
- إلغاء أي بيانات أو معلومات
- حذف أي بيانات أو معلومات
- تدمير أي بيانات أو معلومات
- إفشاء أي بيانات أو معلومات
- إتلاف أي بيانات أو معلومات
- تغيير أي بيانات أو معلومات
- نسخ أي بيانات أو معلومات
- نشر أي بيانات أو معلومات
- إعادة نشر أي بيانات أو معلومات
- خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

كما أن المشرع الإماراتي قد شدد العقوبة على هذه الأفعال عن العقوبة الواردة على جريمة الاختراق وحدها، حيث تكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، وهنا ترى الباحثة أن المشرع الإماراتي أخذ بمبدأ تشديد العقوبة على جريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية في حال نتج عنها أي من النتائج السابقة، وهنا يمكن القول بأن الأحكام الخاصة بجريمة اختراق الأنظمة المعلوماتية للمؤسسات الحكومية تميل إلى التشديد وفق النتيجة الإجرامية التي تنتج عن فعل الاختراق ذاته.

بينما في الفقرة الثالثة من المادة (٣) من المرسوم بقانون اتحادي رقم (٣) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية جاءت بحكم خاص بجريمة الاختراق، وذلك في حال أن الاختراق كان بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة الثالثة، وهنا يمكن القول بأن المشرع الإماراتي يعاقب على الدافع وراء ارتكاب جريمة الاختراق الأنظمة الخاصة بالمؤسسات الحكومية، وهو ما

يطلق عليه في فقه القانون الجنائي بالغرض من وراء ارتكاب الجريمة أو الدافع، هنا نلاحظ أن المشرع الإماراتي قد شدد عقوبة جريمة الاختراق في حالكان الغرض من الاختراق هو الحصول على البيانات الحكومية، ويعاقب المشرع عليها بعقوبة مشددة تختلف عن التشديد الوارد في الفقرة الثانية من المادة (٣) وتكون العقوبة السجن المؤقت مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

ومنه يمكن القول بأن الأحكام الخاصة بجريمة الاختراق للأنظمة المعلوماتية للمؤسسات الحكومية تندرج في ثلاث فئات من الجرائم وكل فئة لها عقوبة تختلف عن الأخرى وتكون مشددة أكثر من سابقتها، الفئة الأولى هي جريمة الاختراق نفسها، والفئة الثانية جريمة الاختراق التي ينتج عنها الضرر للأنظمة المعلوماتية الحكومية، والفئة الثالثة وهي الاختراق بغرض الحصول على البيانات والمعلومات.

ثانياً: الظروف المشددة:

١) الظرف الأول الدخول بقصد الاعتراض:

حيث رفع المشرع نوع ودرجة العقوبة إلى السجن والغرامة حيث نصت الفقرة الثانية من المادة السابقة على عقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، وكذلك فعل المشرع المصري في نصع على العقوبة التي التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، إذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية. وقد بينت المادة الأولى من القانون المصري رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات الاعتراض بانه مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق.

ان ما جاء به المشرع الاماراتي من عقوبات تعتبر كافية بحد ذاتها للحد من الجريمة كونها تحقق الردع العام والردع الخاص.

الظرف الثاني: البقاء دون وجه حق في البيانات.

تكون العقوبة السجن، والغرامة ، إذا ترتب على أي من الأفعال المشار إليها الدخول عمدا والبقاء بدون وجه حق او تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول او اختراق موقع أو بريد الكتروني) إتلاف تلك البيانات أو المعلومات أو تلك الموقع أو الحساب الخاص ، او النظام المعلوماتي او البريد الالكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها او إعادة نشرها، أو إلغائها كليا أو جزئيا، بأي وسيلة كانت ويتم ذلك بتصميم فيروس وإعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام المعلوماتي ، مما يتسبب في تدميره تماما. وتطبيقا لذلك قام مبرمج بزرع فيروس في النظام المعلوماتي للشركة التي يعمل بها، وتم برمجته على أن يبدا بالتدمير والتخريب في برامج ومعلومات الشركة بعد عامين من فصله من الشركة، وظل المفجر في البرنامج يعمل في حساب ساعة وسنة التنفيذ، وعندما وصل البرنامج إلى الوقت المحدد توقف العديد من طرفيات الاتصال بنظام الشركة[٥٦]

وتجدر التفرقة بين صورتين للتدمير: الأول يتعلق بمحو وإزالة المعلومات تماما، والثاني يتعلق بإخفاء المعلومات، بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تماما [٥٧]

والتغيير يقصد به إحداث تعديل في البيانات أو المعلومات أو الموقع أو الحساب الخاص او النظام المعلوماتي أو البريد الالكتروني، بحيث تفقد قيمتها وحقيقتها التي كانت عليها. كما يتحقق ايضاً بكل تعد مادي على البيانات أو المعلومات، وقد يأخذ صورة المحو أو التشويه، وكذلك كل عمل يؤدي إلى جعل البرنامج أو المعلومة غير صالحة لأداء ما أعدت له، أو يؤدي إلى

---

[٥٦] د. فكري، ايمن عبد الله: جرائم نظم المعلومات المرجع السابق، ص١٧٠.

[٥٧] د. الكعبي، محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت- دراسة مقارنة-، مرجع سابق، ص ٢٢٨.

تعديل مسار البيانات أو المعلومات على النحو الذي كان يتعين أن يسير فيه. وإعادة النشر يتحقق في الحالات التي يتم فيها استبعاد الموقع او المعلومة لعدم الحاجة إليها، فيقوم الجاني بإعادة النشر.[٥٨]

ويعد النسخ أو التسجيل غير المرخص به من أهم صور الاعتداء على برامج الحاسبات الآلية وأكثرها انتشارا، ويأخذ النسخ إحدى صورتين: تتمثل الأولى في النسخ الحرفي سواء كان نسخة كليا أم جزئيا، وتتمثل الثانية في النسخ غير الحرفي وفيه يتم استخدام ذات الأفكار للبرنامج المحمي في إنتاج برنامج جديد ليظهر وكأنه إنتاج فكري أصلي مستقل، كما يعد إجراء تعديلات على برامج الحاسبات الآلية المحمية من الأمور المحظورة[٥٩].

والإلغاء يعني حذف البرنامج أو إزالة البيانات الموجودة داخل النظام المعلوماتي بصفة نهائية أو تشغيل خاصية حذف البرامج وما يترتب ايضاً من نشر الفيروسات على الشبكة أو الحاسب. وتوصف هذه الصور التجريمية بأنها من ناحية النتيجة الإجرامية للسلوك الوارد في الفقرة الأولى من النص، ومن ناحية ثانية تعد بمثابة ظرف مشدد للجريمة المنصوص عليها في الفقرة الأولى[٦٠].

العقوبات التي جاء بها المشرع الاماراتي في قانون مكافحة الشائعات والجرائم الالكترونية تسهم بشكل فاعل في الحد من ارتكاب هذا النوع من الجرائم على المستقبل القريب، وقد أحسن المشرع الاماراتي صنعا في تشديد العقوبات وهو الأمر الذي يسهم في الحد منها وإيقاع أقصى العقوبات على مرتكبها.

المطلب الثاني

---

(٥٨) د. الجندي، حسني: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، مرجع سابق، ص ٨٣.

(٥٩) المستشار الحناوي علي فاروق: قانون البرمجيات دراسة معينة في الأحكام القانونية البرمجيات الكمبيوتر، الكتاب الأول، ٢٠٠١، ص٢١٧ - ٢٣٧.

(٦٠) د. الجندي، حسني: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، مرجع سابق، ص ٢٤٥.

الاحكام الخاصة بالتدابير المتعلقة بالعقوبات على جريمة الاختراق السيبراني في قانون مكافحة الشائعات والجرائم الالكترونية.

تعتبر التدابير التي يفرضها المشرع الإماراتي على من يرتكب جريمة الهجوم السيبراني ضد المواقع الحكومية من أهم ما يتم الحكم به، ولها دور هام ومحوري في الحد من ارتكاب الجريمة وتحقيق الردع العام والخاص، وعليه نتناول في هذا المطلب الأحكام الخاصة بالعقوبات الفرعية والتكميلية التي جاء بها المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية على النحو الآتي:

بينت المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ العديد من التدابير التي يتم الحكم بها لحماية البيانات الحكومية حيث تنص على أنه:"

١) أوامر التصحيح وإزالة البيانات الزائفة: الإشعارات التي تصدرها الجهات المختصة إلى شخص معين أو أكثر بتصحيح أو إزالة أو حذف المحتوى غير القانوني أو بتصحيح أو إزالة أو حذف المعلومات أو البيانات الزائفة بالشكل أو بالطريقة التي تراها تلك الجهات مناسبة خلال المدة المحددة في الإشعار.

٢) أوامر التعطيل: الإشعارات التي تصدرها الجهات المختصة إلى وسيط شبكة معلوماتية ينشر من خلاله محتوى غير قانوني أو بيانات زائفة، وتطلب منه تعطيل وصول المستخدمين إلى المحتوى أو البيانات المشار إليها، بالشكل أو بالطريقة التي تراها تلك الجهات مناسبة خلال المدة المحددة في الإشعار.

٣) أوامر حظر الوصول: الأوامر التي تصدرها الجهات المختصة إلى مزود الخدمة بالدولة عند عدم إمكانية تنفيذ التعليمات الأخرى المشار إليها بهذا المرسوم بقانون وذلك لاتخاذ تدابير تعطيل وصول المستخدمين في الدولة إلى الموقع أو الحساب الإلكتروني."

ومن هذه المادة يتضح أن المشرع الإماراتي استحدث ثلاثة أنواع من التدابير وهي:

١) أوامر التصحيح وإزالة البيانات الزائفة:
٢) أوامر التعطيل: ٣
٣) أوامر حظر الوصول:

ومن التدابير التي نص عليها المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن الشائعات والجرائم الإلكترونية ما نصت عليه المادة (٥٩) حيث تنص على أنه:" يجوز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بأي من التدابير الآتية:

١) الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.
٢) إغلاق الموقع المخالف إغلاقا كليا أو جزئيا متى أمكن ذلك فنيا
٣) حجب الموقع المخالف حجبا كليا أو جزئيا للمدة التي تقررها المحكمة.

يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على (٥٠٠٠) خمسة آلاف درهم، كل من خالف أي تدبير من التدابير المحكوم بها، وللمحكمة أن تأمر بإطالة التدبير مدة لا تزيد على نصف المدة المحكوم بها ولا تزيد في أية حال على (٣) ثلاث سنوات أو أن تستبدل به تدبيرا آخر مما ذكر."

وعليه وعلى ضوء ما جاءت به هذه المادة نبين مع التفصيل تلك التدابير على النحو التالي:

أولاً: تدبير الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

هنا بين المشرع الإماراتي في هذه الفقرة عدة تدابير متلازمة مع بعضها البعض، ونبينها على النحو الآتي:

أ- الوضع تحت المراقبة الإلكترونية.

عرفها الفقه القانوني بأنها: "طريقة مستحدثة، لتنفيذ العقوبات السالبة للحرية قصيرة المدة، خارج المؤسسة العقابية، وتتمثل بإلزام المتهم، أو المحكوم عليه، بالبقاء في مقر إقامته، أو في أي مكان آخر محدد، خلال مدة معينة تحددها الجهة القضائية المختصة، حيث يمكن للمحكوم عليه الالتحاق بعمله أو متابعة دراسته، أو الوفاء بمتطلبات أسرته، ويتم تطبيق هذا النظام، من خلال استخدام وسائل تكنولوجية حديثة، تتمثل بجهاز إرسال يوضع على يد المحكوم عليه، لمراقبة المحكوم عليه، من أجل تمكين المؤسسة العقابية من تنفيذ العقوبة"[٦١].

أقرَّ التشريع الإماراتي، والتشريعات المقارنة، الحديث عن المراقبة الإلكترونية، ووضع له تعريفاً محدداً للمراقبة الإلكترونية، في التشريع الإماراتي، نجد أنَّ المشرع الاتحادي، تناول الحديث عن المراقبة الإلكترونية، في قانون الإجراءات الجزائية، الصادر بالقانون الاتحادي رقم ٣٥ لسنة ١٩٩٢م، والمعدل بالمرسوم بقانون اتحادي رقم ١٧ لسنة ٢٠١٨م، حيث تناول في المادة (٣٥٥) منه، الوضع تحت المراقبة الإلكترونية، وعرَّفه بأنَّه: (حرمان المتهم، أو المحكوم عليه، من أن يتغيب في غير الأوقات الزمنية المحددة له، عن محل إقامته، أو أي مكان آخر يعينه الأمر الصادر من النيابة العامة، أو المحكمة المختصة بحسب الأحوال، ويتم تنفيذه، عن طريق وسائل إلكترونية، تسمح بالمراقبة عن بعد، وتلزم الخاضع أن يحمل جهاز إرسال إلكتروني مدمج، طوال فترة الوضع تحت المراقبة)[٦٢].

قررت المادة (٣٦٢) من المرسوم بقانون اتحادي رقم (١٧) لسنة ٢٠١٨ على أنه:" يجوز للنيابة العامة إذا اقتضت ضرورة إجراءات التحقيق ذلك أن تضمن الأمر بالوضع تحت المراقبة الإلكترونية إلزام المتهم الخاضع بعدم الاتصال بغيره من المتهمين أو الشركاء المساهمين معه في الجريمة، أو

---

[٦١] . د. عمر سالم، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، مرجع سبق ذكره، ص ١٠.

[٦٢] . المادة رقم ٣٥٥ من قانون الإجراءات الجزائية الصادر بالقانون الاتحادي رقم ٣٥ لسنة ١٩٩٢م المعدلة بالمرسوم بقانون اتحادي رقم ١٧ لسنة ٢٠١٨م.

بالمجني عليهم أو ذويهم، وذلك كله بدون الإخلال بحق المتهم في الاتصال دائمًا بالمدافع عنه، ويجوز أن يتضمن الأمر أيضاً إخضاع المتهم للالتزامات المنصوص عليها في الفقرة الأولى من المادة (٣٧٢) من هذا القانون".

استند أصحاب المذهب الذي يعتبر المراقبة الإلكترونية كتدبير، إلى أنَّ هذه المراقبة ما هي إلا تدبير احترازي، فأنصار هذا الاتجاه، يرون أنَّ الغرض منها فقط، هو محاولة منع الجاني من العودة للجريمة مرة أخرى، ويتم ذلك عن طريق تحجيم ومنع الخطورة الإجرامية لديه، عن طريق مراقبته إلكترونياً، ومحاولة إعادة دمجه في المجتمع، ليصبح عضواً صالحاً فيه، وكل ذلك يتم من خلال القيود والالتزامات التي تفرضها تلك المراقبة، على المحكوم عليه، من حلال التزامه بعدم مغادرته لمكان إقامته، إلا في حالات محددة يحددها قرار القاضي، كل ذلك بغرض تأهيل الجاني، ومساعدته لترك طريق الجريمة، ولكي يصبح فرداً نافعاً في المجتمع الذي يعيش في كنفه((٦٣).

ب- الحرمان من استخدام شبكة الإنترنت أو النظام المعلوماتي

ت- الوضع في مأوى علاجي.

ثانياً: إغلاق الموقع المخالف إغلاقا كليا أو جزئيا متى أمكن ذلك فنيا

بين المشرع الإماراتي في نص المادة (٥٩) من قانون مكافحة الشائعات والجرائم الإلكترونية إمكانية الحكم بإغلاق الموقع الإلكتروني الذي ترتكب من خلاله جريمة الهجوم السيبراني وهو إجراء يسهم في الحد من ارتكاب الجريمة وعدم تمكين الجاني من ارتكابها مرة أخرى.

ثالثاً: حجب الموقع المخالف حجبا كليا أو جزئيا للمدة التي تقررها المحكمة.

١- تعريف حجب المواقع

في اللغة: حجب الشيء ستره(٦٤). قال تعالى" (كَلا انهم عن ربهم يومئذ لمحجوبون)(٦٥)

---

(٦٣) . د. رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، مرجع سبق ذكره، ص ٢٩٠. وما بعدها

(٦٤) المعجم الوجيز مجمع اللغة العربية ، ١٤١٤ه ١٩٩٣ ص ١٣٥.

(٦٥) سورة المطففين: الاية رقم (١٥).

في الاصطلاح: يقصد بالحجب الستر أو المنع للموقع أو المواقع كمجال أو مكان افتراضي اله عنوان محمد على شبكة معلوماتية، من إتاحة البيانات والمعلومات العامة أو الخاصة[٦٦].

٢- شروط الحجب[٦٧]:

أ- قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو مور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون وبالأحرى ان ترصد جهات التحري والضبط المختصة قيام مواقع الكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو مور، أو أفلام، أو أية مواد دعائية، أو غيرها وهذا يعني أمران: الأول ان يتعلق الفعل بموقع الكتروني أو اكثر ، والثاني ان يشكل ما يبثه الموقع جريمة الكترونية والملاحظ ان ما أورده الشارع من عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها بما يشكل جريمة من الجرائم المؤثمة بقانون جرائم تقنية المعلومات جاء على سبيل المثال وليس على سبيل الحصر.

ب- ان يشكل الفعل تهديدا للأمن القومي أو يعرض امن البلاد أو اقتصادها القومي للخطر وبعبارة أخرى ان يكون من شان الفعل تهديد الأمن القومي، أو السلم الأهلي، أو النظام العام، أو الآداب العامة.

ت- ان يكون ذلك ممكنة، وهذا ما عبر عنه الشارع بان يكون تحقيق ذلك فنيا".

في جمهورية مصر العربية نصت المادة ٧ من القانون ١٧٥ لسنة ٢٠١٨ بشان مكافحة جرائم تقنية المعلومات على ان لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة او خارجها، بوضع اي عبارات او ارقام او صور او افلام او اي مواد دعائية او ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدا للامن القومي او يعرض امن البلاد او اقتصادها القومي للخطر، ان تامر بحجب الموقع او

---

[٦٦]Buffelan – Lanore: La Procédure Apllicable Aux Infraction Commises Par Les Personnes Morales Rev, Sociétés 1993. P. 315 ets.

[٦٧]Boizard(M):Amend,confiscation,affichage ou communication de la decision Revue des Sociétés,1993, p.332.

المواقع محل البث، كلما امكن تحقيق ذلك فنيا وعلى جهة التحقيق عرض امر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة خلال اربع وعشرين ساعة مشفوعة بمنكرة برايها، وتصدر المحكمة قرارها في الامر مسببة اما بالقبول او بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها ويجوز في حالة الاستعجال لوجود خطر حال، او ضرر وشيك الوقوع، ان تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع او المحتوى او المواقع او الروابط المذكورة في الفقرة الاولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الاخطار فور روده اليه. وعلى جهة التحري والضبط التي قامت بالإبلاغ ان تحرر محضرة تثبت فيه ما تم من اجراءات وفق احكام الفقرة السابقة يعرض على جهات التحقيق خلال ثمان واربعين ساعة من تاريخ الابلاغ الذي وجهته للجهاز، وتتبع في هذا المحضر ذات الاجراءات المبينة بالفترة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها في هذه الحالة اما بتاييد ما تم من اجراءات حجب، او بوقفها. فاذا لم يعرض المحضر المشار اليه في الفقرة السابقة في الموعد المحدد، يعد الحجب الذي تعم كان لم يكن ولمحكمة الموضوع اثناء نظر الدعوى، او بناء على طلب جهة التحقيق او الجهاز او ذوي الشأن ان تامر بإنهاء القرار الصادر بالحجب، او تعديل نطاقه وفي جميع الاحوال، يسقط القرار الصادر بالحجب بصدور امر بالا وجه لإقامة الدعوى الجنائية، او بصدور حكم نهائي فيها بالبراءة.

الخاتمة

تناولنا في البحث نوع محدد من الجرائم وهي جريمة الاختراق السيبراني للأنظمة المعلوماتية الحكومية، وتناولنا هذا النوع من الجرائم وفق مات جاء به المشرع الإماراتي في المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠١١ بشأن الشائعات والجرائم الإلكترونية والمرسوم بقانون اتحادي رقم (٣١) لسنة ٢٠٢١ بشأن الجرائم والعقوبات، وتوصلنا في نهاية البحث للعديد من النتائج والتوصيات على النحو الآتي:

أولاً: النتائج.

١) أن جريمة الاختراق وما يتبعها من جرائم الكترونية، لا يمكن أن تتم إلا عن طريق هذه الشبكة فالمعلومات المدونة في الحاسوب الخاص، الذي لم يرتبط بالإنترنت لا يمكن اختراقه.

٢) ما يميز جريمة الاختراق السيبراني هي أنها جرائم سريعة التنفيذ إذ أنه وفي أغلب الأحيان لا يكون الركن المادي سوى ضغط على مفتاح معين في الجهاز مع إمكان تنفيذ ذلك عن بعد دون اشتراط التواجد في مسرح الجريمة ولهذا فأن الجريمة الالكترونية ولسهولة ارتكابها شكلت عنصر إغراء للمجرمين وإذ أن ارتكابها لا يتعدى سوى توفر إمكانية استغلال التكنولوجيا والتقنية الحديثة خصوصا عندما يكون الجاني موظفا عاما أو في إحدى الشركات التي تعتمد على الحاسب الآلي في طبيعة عملها المتعلق بالمعلومات أو الأموال بحيث يكون لديها كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة وتحقيق أرباح طائلة. ولهذا نشأت الحاجة لوجود طرق حماية قوية للمعلومات المخزنة في أجهزة حاسوب أو وسائط نقل الكترونية ومثال ذلك ما يسمى بجدران الحماية أو الجدران النارية وهي عبرة عن برامج حماية تمنع الاختراق أو الدخول غير المصرح به.

٣) يتميز مرتكب جريمة الاختراق السيبراني بأنه يعود للجريمة دائما، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به

مـــرات ومـــرات. فهـــو قـــد لا يحقـــق جريمـــة الاختـــراق بهـــدف الإيـــذاء وإنمـــا نتيجة شعوره بقدرته ومهارته في الاختراق.

٤) لقـــد أحســـن المشـــرع الإمـــاراتي بنصـــه علـــى ظـــروف تشـــديد العقوبـــات علـــى جريمة اختراق الأنظمة الإلكترونية الحكومية وهي عقوبات رادعة.

ثانياً: التوصيات.

١) قيـــام المشـــرع الإمـــاراتي بتعريـــف الهجـــوم الســـيبراني والاختـــراق الســـيبراني فـــي نـــص المـــادة الأولـــى مـــن المرســـوم بقـــانون اتحـــادي رقـــم (٣٤) لسنة ٢٠١١.

٢) تعيـــب الباحثـــة بالمشـــرع الإمـــاراتي تخصـــيص مـــادة قانونيـــة فـــي قـــانون الشـــائعات والجـــرائم الإلكترونيـــة تجـــرم اســـتخدام أنظمـــة الاختـــراق فـــي ارتكاب الجريمة.

٣) اســـتحداث عقبـــة خاصـــة فـــي قـــانون الجـــرائم والعقوبـــات علـــى جريمـــة اختراق الأنظمة المعلوماتية الحكومية.

٤) قيـــام المشـــرع الإمـــاراتي بتحديـــد أنـــواع أنظمـــة الاختـــراق الســـيبراني للأنظمة المعلوماتية الحكومية.

قائمة المراجع:

أولاً: المرجع العامة

- إبـراهيم حسـن عبـد الـرحيم المـلا: الـذكاء الاصـطناعي والجريمـة الإلكترونيـة، مجلـة الأمـن والقـانون صـادرة عـن أكاديميـة شـرطة دبـي، السـنة السادسـة والعشرون، العدد الأول، يناير ٢٠١٨ م.
- أحمـد محمـد الشامسـي وحسـب اللـه سـيد: المعجـم الموسـوعي لمصـطلحات المكتبـات والمعلومات، دار المريخ، الرياض، ١٤٠٨- ١٩٨٨،
- احمـد محمـد خليفـة الملـط: الجـرائم المعلوماتيـة، دار الفكـر الجـامعي، الطبعـة الثانية، ٢٠٠٤
- أحمـد مختـار محمـد: معجـم اللغـة العربيـة المعاصـرة، المجلـد ٢، عـالم الكتـب، القاهرة، ٢٠١٦،
- احمـد هلالـي عبـد الـلاه: جـرائم الحاسـب والإنترنـت بـين التجـريم الجنـائي وآليـات المواجهة، دار النهضة العربية، القاهرة، ٢٠١٥ م – ٢٠١٦ م،
- أندريـه لوغـاريف،: المعجـم الموسـوعي فـي الكمبيـوتر والإلكترونيـك، ترجمـة د. عبـد الحسـيني، المؤسسـة الجامعيـة للدراسـات والنشـر والتوزيـع، بيـروت، الطبعـة ٢، ٢٠٠٩،
- حسـني الجنـدي: التشـريعات الجنائيـة الخاصـة فـي دولـة الإمـارات العربيـة المتحـدة، قـانون مكافحـة جـرائم تقنيـة المعلومـات، اكاديميـة العلـوم الشـرطية، الشـارقة، ٢٠٠٩.
- خالـد ممـدوح إبـراهيم: التقاضـي الإلكترونـي (الـدعاوى الإلكترونـي وإجراءاتهـا أمام المحاكم)، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م.
- سـليمان أحمـد فضـل: المواجهـة التشـريعية والأمنيـة للجـرائم الناشـئة عـن اسـتخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ١٤١٣ه/.
- شـعبان خليفـة: قـاموس البنهـاوي الموسـوعي فـي مصـطلحات المكتبـات والمعلومات، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٤ م.
- طـارق إبـراهيم أحمـد فيـاض العبداللـه: جـرائم الروبـوت وكيانـات الـذكاء الاصطناعي، دار النهضة العربية، القاهرة، ٢٠٢٢.

- عـزة محمـد محمـود: مشـكلات المسـئولية المدنيـة فـي مواجهـة فيـروس الحاسـب، دراسـة فـي القـانون المـدني والشـريعة الإسـلامية برسـالة دكتـوراه، كليـة الحقـوق جامعة القاهرة، ١٩٩٤.
- علـي فـاروق الحنـاوي: قـانون البرمجيـات دراسـة معينـة فـي الأحكـام القانونيـة البرمجيات الكمبيوتر، الكتاب الأول، ٢٠٠١
- علـي محمـد العريـان: الجـرائم المعلوماتيـة، دار الجامعـة الجديـدة، الإسـكندرية، ٢٠١١ م .
- عمـر الشـريف: التنظـيم التشـريعي لجـرائم الاتصـالات فـي مصـر، التشـريع، السـنة الأولى، العدد الثاني يوليو ٢٠٠٤.
- عمـر محمـد أبـو بكـر يـونس: الجـرائم الناشـئة عـن اسـتخدام الانترنـت، دار النهضـة العربية، القاهرة، ٢٠١٨.
- محمـد عبـد العزيـز الشـريف: السـلوك الإجرامـي الإلكترونـي، مركـز الحضـارة العربية، القاهرة، مصر، الطبعة الأولى، ٢٠١٦م.
- نائلـة عـادل قـوره: جـرائم الحاسـب الآلـي الاقتصـادية، دراسـة نظريـة وتطبيقيـة، منشورات الحلبي الحقوقية، الطبعة الأولى ٢٠٠٥.

ثانياً: المراجع المتخصصة

- اميـر فـرج يوسـف: جـرائم تقنيـة المعلومـات بـدول الخلـيج العربـي والجهـود الدوليـة والمحليـة لمكافحـة جـرائم الإنترنـت والحاسـوب الإلكترونيـة فـي دول الخلـيج العربي، دار الكتب والدراسات العربية، الطبعة الأولى، ٢٠١٧.
- حشـمت قاسـم : جريمـة الـدخول غيـر المشـرع لنظـام معلومـاتي، منشـورات أطلـس، دمشق، ٢٠٢١.
- العريـان، محمـد علـي العريـان: الجـرائم المعلوماتيـة، دار الجامعـة الجديـدة للنشـر، ٢٠٠٤.
- رمضـان، مـدحت عبـد الحلـيم: الحمايـة الجنائيـة للتجـارة الإلكترونيـة دراسـة مقارنة، دار النهضة العربية ٢٠٠١.
- علـي عـدنان الفيـل: الإجـرام الالكترونـي، بيـروت، منشـورات زيـن الحقوقيـة، الطبعة الأولي ٢٠١١.

- عيسى سليم داوود الزيدي: جرائم القرصنة الإلكترونية، دار شتات للنشر، مصر والإمارات، ٢٠١٦م.
- محمد امين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، ٢٠٠٣.
- محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ٢٠٠٩.
- محمد علي سويلم: شرح قانون جرائم تقنية المعلومات- القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة تقنية المعلومات، دار المطبوعات الجامعية، ط ١، ٢٠١٩ م.
- محمد مصطفى الشقيري: السرية المعلوماتية، ضوابطها واحكامها الشرعية، دار النشر الإسلامية، بيروت لبنان، ٢٠٠٨.
- نبيل محمّد عثمان عرعارة: الحماية الجنائيّة للحق في حرمة المراسلات عبر البريد الإلكتروني، (ماجستير في القانون الجنائي)، المصريّة للنشر والتوزيع، القاهرة، مصر، الطبعة الأولى ١٤٣٩ ه/ ٢٠١٨ مـ.
- نسرين عبد الحميد نبيه: الجريمة المعلوماتية والمجرم المعلوماتي، منشاة المعارف الإسكندرية، ٢٠٠٨.
- يوسف أبو الحجاج: أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، الطبعة الأولى، ٢٠١٠.

ثالثاً: الرسائل العلمية

- أيمن فكري: جرائم نظم المعلومات رسالة دكتوراه كلية الحقوق جامعة المنصورة ٢٠٠٩ دار الجامعة الجديدة ٢٠٠٧.

رابعاً: المقالات

- احمد علي: مفهوم المعلومات في إدارة المعرفة، مجلة جامعة دمشق، المجلد ١، العدد ١، ٢٠١٢ م.
- فتيحة رصاع: الحماية الجنائية للمعلومات على شبكة الإنترنت، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، ٢٠١١ – ٢٠١٢ م.

خامساً: القوانين

- مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ الصادر بتاريخ ٢٠ / ٠٩ / ٢٠٢١ نشر بتاريخ ٢٦ / ٠٩ / ٢٠٢١ في الجريدة الرسمية.
- قانون الإجراءات الجزائية الصادر بالقانون الاتحادي رقم ٣٥ لسنة ١٩٩٢م المعدلة بالمرسوم بقانون اتحادي رقم ١٧ لسنة ٢٠١٨م.

سادساً: المراجع الأجنبية

- *PETER SWIFT: HACK MAN MENACE OF THE KEYBOARD CRIMINAL BRITICH TELECOM WORLD MAG, HALF OF SEPT 1989 P 13-14.*
- *Buffelan - Lanore: La Procédure Apllicable Aux Infraction Commises Par Les Personnes Morales Rev, Sociétés 1993. P. 315 ets.*
- *[0]Boizard(M):Amend,confiscation,affichage ou communication de la decision Revue des Sociétés,1993, p.332.*
- *Guillaume Champy, La fraude informatique, tome 1, () Presses Universitaires d Aix-Marseille, 51992, p. 88.*