

جامعة القدس
عمادة الدراسات العليا

جريمة اختراق النظم والشبكات المعلوماتية

راشد حسن حسين عياش

رسالة ماجستير

القدس- فلسطين

1440هـ / 2019م

جريمة اختراق النظم والشبكات المعلوماتية

إعداد:-

راشد حسن حسين عياش

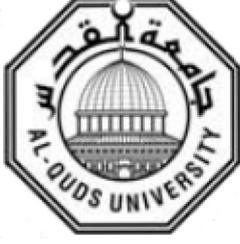
بكالوريوس حقوق من جامعة فلسطين الأهلية، بيت لحم / فلسطين

إشراف:-

أ.د. نبيه صالح

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في مسار القانون الجنائي / كلية الحقوق / جامعة القدس

2019 / هـ 1440



جامعة القدس
عمادة الدراسات العليا
برنامج القانون الجنائي

إجازة الرسالة

جريمة اختراق النظم والشبكات المعلوماتية

اسم الطالب: راشد حسن حسين عياش

الرقم الجامعي: ٢١٥٢٠٣٦٧

المشرف: أ.د. نبيه صالح

نوقشت هذه الرسالة وأجيزت بتاريخ: ٢٠١٩/٤/١٣ من أعضاء لجنة المناقشة المدرجة
أسمائهم وتوقيعهم:

١- رئيس لجنة المناقشة: أ.د. نبيه صالح التوقيع

٢- ممتحناً داخلياً: د. عبدالله النجاجة التوقيع

٣- ممتحناً خارجياً: د. رائد طه التوقيع

القدس- فلسطين

٢٠١٩ / ١٤٤٠ هـ / م

الإهداء

إلى الذي وهبني كل ما يملك حتى أحقق آماله وكان يدفعني قدماً نحو الأمام لنيل
المبتغى، إلى الذي يعيش قديسا للعلم

أبي الغالي على قلبي أطال الله في عمره.

إلى التي وهبت فلذة كبدها وصبرت على كل شيء

إلى نبع الحنان

أمي أعز ملاك على القلب والعين.

إلى زهرة العمر التي أحببتها

إلى خطيبي ياسمين.

إلى من رافقوني منذ أن حملنا حقائب صغيرة، ومعهم سرت الدرب خطوة بخطوة وما

زالوا يرافقوني حتى الآن

إخوتي كرم وعكرمة وأحمد

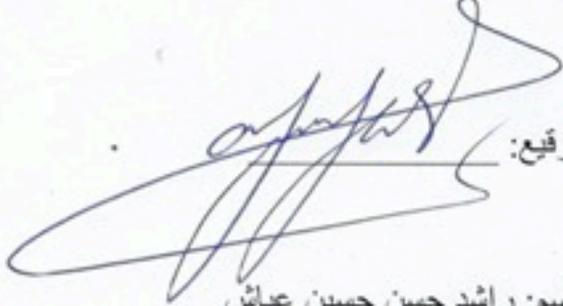
وأخيرا وليس آخرا؛ أهدي جهدي المتواضع

لكل من يؤمن بأنّ بذور نجاح التغيير هي في ذواتنا.

إليهم جميعاً أتقدّم بهذا الجهد المتواضع

إقرار:

أقر أنا معد الرسالة بأنها قدمت لجامعة القدس لنيل درجة الماجستير، وإنها نتيجة أبحاثي الخاصة، باستثناء ما تم الإشارة إليه حيثما ورد، وأن هذه الرسالة أو أي جزء منها، لم يقدم لنيل درجة عليا لأي جامعة أو معهد آخر.


التوقيع:

الاسم: راشد حسن حسين عياش

التاريخ: ٢٠١٩/٤/١٣.

شكر وتقدير

أتوجه بالشكر إلى من رعاني ووجهني في إعداد هذا البحث، أستاذي ومشرفي الأستاذ الدكتور: نبيه صالح، فله مني كل التقدير والعرفان. كما أتوجه بالشكر الجزيل إلى أساتذتي في كلية الحقوق بجامعة القدس/ أبو ديس. وفي هذا المقام أجد لزاماً علي الوقوف شاكراً لوالدي الدكتور حسن عياش الذي كان نعم القارئ والمصحح والمعين، والشكر موصول إلى المكتبات التي تزودت منها مادة هذا البحث ولاسيما مكتبة جامعة القدس ومكتبة الجامعة الأردنية.

وأقدم بشكري الجزيل إلى أساتذتي الأعزاء في لجنة المناقشة رئاسة وأعضاء لتفضلهم علي بقبول مناقشة هذه الرسالة، كما أشكر كل من وقف بجانبي وساندي علي إنجاز هذا البحث، فلهم كل الثناء والتقدير وإن لم يسعف المقام لذكركم، فهم أهل للفضل والخير والشكر.

الباحث

راشد حسن عياش

المخلص

توسع انتشار الجرائم الإلكترونية أصبح أمراً واقعياً في ظل الثورة المعلوماتية والتطور التكنولوجي الهائل على وسائل الاتصال المختلفة، إلا أن هناك مشكلة تثيرها الجرائم الإلكترونية وهو مدى كفاية القواعد التشريعية لمواجهة الجرائم الإلكترونية وسبل الوقاية منها.

تصدى المشرع الفلسطيني لهذا النوع من الجرائم بموجب قرار بقانون والخاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨) حيث جرم وعاقب على الجرائم التي ترتكب من خلال الحاسب الآلي. وقد توصل الباحث إلى أن جريمة الاختراق تتم بالولوج غير المشروع لنظام الحاسوب وللشبكات الإلكترونية، ويتم الوصول من خلالها للبيانات والمعلومات السرية الخاصة بكل من يتعامل معها. كما أن جريمة الاختراق يقوم بها المجرم المعلوماتي، وليس باستطاعة أي شخص أن يطلق على نفسه مخترقاً، فهو يتميز بصفات تميزه عن غيره من الخبراء كالكفاءة والمهارة التي تؤهله للتعامل مع الحاسوب ومكوناته.

خرج الباحث بعدد من النتائج ومن أهمها: اعتبار جريمة الاختراق جريمة قائمة بحد ذاتها، حتى ولو لم يتم بأي عمل تخريبي كتعطيل نظام الحاسب الآلي أو تدمير البيانات أو إتلافها وغيرها من الأعمال التخريبية التي قد يلجأ لها المجرم، فبمجرد دخوله للنظام بشكل غير مشروع وكان عالماً بذلك وبقي فيه

ولم يخرج ولم يرقم بأي عمل تخريبي يعتبر مرتكباً لجريمة الاختراق وفقاً للمادة (٤) الفقرة (١) من القرار

بقانون بشأن الجرائم الإلكترونية الفلسطينية رقم (١٠) لسنة (٢٠١٨)، وأما أهم توصيات هذه الدراسة فهي:

خلق بيئة معلوماتية حاسوبية فلسطينية آمنة وموثوقة ضمن أحدث وسائل التكنولوجيا المستخدمة وهو ما

تبنته المادة (٤) من القرار الصادر عن مجلس الوزراء رقم (١٦) لسنة (٢٠١٥) بالنظام الداخلي لعمل

الفريق الفلسطيني للاستجابة لطوارئ الحاسوب.

The Crime Of Penetrating Systems And Information Networks.

Prepared by : Rashed Hasan Husain Ayyash

Supervisor : Prof.Nabeh Saleh

Abstract:

expansion of the spread of cybercrime has become a reality in the light of the information revolution and the tremendous technological development on the various means of communication, but there is a problem raised by cybercrime is the adequacy of legislative rules to confront cybercrime and ways to prevent them.

Palestinian legislator has dealt with this type of crime in accordance with the Palestinian Law on Cybercrime No. (10) of 2018, which criminalizes and punishes crimes committed through the computer. The researcher concluded that the crime of penetration is the process that happened through the illegal entry of the computer system and the electronic networks, through which access to the data and confidential information of each dealing with it.

crime of penetration is carried out by the information criminal, and no one can call himself a hacker. He has certain characteristics that distinguish him from other experts such as competence and skill that qualify him to deal with the computer and its components. The researcher came out with a number of results,

the most important of which is: The crime of penetration is considered a crime in itself, even if it did not commit any destructive action such as disrupting the computer system, destroying the data or destroying it and other destructive acts that the criminal may resort to. According to the (4th)Paragraph of the article number (1) of the Palestinian Electronic Crimes Law No. 10 of 2018. The main recommendations of this study are: Creating a good information environment that saves safety and reliable Palestinian computer within the latest technological means Which was adopted by Article (4) of the Ministerial Resolution No. (16) for the year 2015 regarding the internal procedures of the Palestinian emergency response team.

فهرس المحتويات

أ.....	إقرار
ب.....	الشكر والتقدير
ج.....	المخلص
ه.....	Abstract
١.....	مقدمة
٣.....	أهمية الدراسة
٣.....	أهداف الدراسة
٤.....	إشكالية الدراسة
٤.....	منهجية الدراسة
٤.....	مصطلحات الدراسة
٧.....	الفصل الاول : الجانب الفني والتقني للحاسوب والإنترنت
٨.....	المبحث الاول : الجانب الفني والتقني للحاسوب
٩.....	المطلب الاول : ما هية جهاز الحاسوب وطبيعته وخصائصه
١٠.....	الفرع الأول:تعريف الحاسوب
٢٣.....	الفرع الثاني: الطبيعة القانونية لجرائم الحاسوب

- ٢٦.....الفرع الثالث: خصائص الحاسوب.
- ٢٨.....المطلب الثاني : مكونات الحاسوب الآلي.
- ٢٨.....الفرع الاول :مكونات مادية.
- ٣٠.....الفرع الثاني: مكونات معنوية.
- ٣٢.....المبحث الثاني :الجانب الفني والتقني للإنترنت.
- ٣٣.....المطلب الاول :ما هية الانترنت.
- ٣٥.....الفرع الاول :تعريف الإنترنت.
- ٣٧.....الفقرة الأولى: الإنترنت لغةً.
- ٣٧.....الفقرة الثانية: الإنترنت إصطلاحاً.
- ٤٣.....الفرع الثاني : نشأة الإنترنت.
- ٥٤.....المطلب الثاني : الانترنت ايجابياته وسلبياته.
- ٥٥.....الفرع الاول : ايجابيات شبكة الإنترنت.
- ٥٩.....الفرع الثاني :سلبيات شبكة الانترنت.
- ٦٤.....الفصل الثاني : جريمة اختراق أنظمة المعلومات والشبكات المعلوماتية.
- ٦٥.....المبحث الاول : التعريف بجريمة الاختراق.
- ٦٦.....المطلب الاول : ما هية جريمة الاختراق.

٦٧.....	الفرع الاول : الاختراق.....
٦٩.....	الفقرة الأولى: الاختراق لغةً.....
٧٠.....	الفقرة الثانية: الاختراق اصطلاحاً.....
٧٥.....	الفرع الثاني : أركان جريمة الاختراق.....
٨٤.....	الفرع الثالث: من هم مرتكبوا الجرائم المعلوماتية.....
٩٢.....	المطلب الثاني : أشكال ودوافع الإختراق وخصائصها.....
٩٣.....	الفرع الاول : أشكال جريمة الاختراق.....
٩٧.....	الفرع الثاني : دوافع جريمة الإختراق.....
١٠٥.....	الفرع الثالث: خصائص جريمة الاختراق.....
١٠٩.....	المبحث الثاني : نظم المعلومات وأمنها على الشبكة المعلوماتية.....
١١٠.....	المطلب الاول : نظم المعلومات وأمنها.....
١١١.....	الفرع الاول : تعريف نظم المعلومات.....
١١٦.....	الفرع الثاني :مكونات نظام المعلومات.....
١٢٠.....	المطلب الثاني : تعريف الأمن المعلوماتي.....
١٢١.....	الفرع الاول : تعريف الأمن المعلوماتي.....
١٢٥.....	الفرع الثاني :عناصر الأمن المعلوماتي.....

الخاتمة..... ١٣٠

النتائج..... ١٣٢

ثانياً: التوصيات..... ١٣٤

المقدمة

شَهِدَ عالمنا الحالي تطوراً كبيراً في مجالات الحياة كافة، وكان منها، التطور الكبير في المجال التكنولوجي، والذي جعل العالم قرية إلكترونية صغيرة، وأدى بدوره إلى وجود تحولات عدة على مختلف المفاهيم؛ بحيث تم تعديلها بما يتناسب مع هذا التطور من أجل مواكبة العصر وتقدمه، وفي غمرة التطور التكنولوجي السريع برزت جريمة الاختراق، إذ تعد جريمة إلكترونية، ولها دوافع عدة من بينها دوافع شخصية، أو انتقامية، أو بهدف كسب المال بطريقة غير مشروعة.

إضافة لما سبق، فإن عصرنا الراهن يشهد ثورة معلوماتية ضخمة، ومنافسة قوية حادة في هذا المجال، وبأساليب حديثة هدفها استغلال التكنولوجيا من أجل تحقيق غايات خاصة ببعض الأفراد والجماعات الإجرامية المنظمة، وهي بالتالي تهدد السلم والأمن الاجتماعيين.

لقد تميزت الشبكة العنكبوتية (الإنترنت) في مختلف أنحاء العالم، وجعلته قرية صغيرة؛ كما سبق الإشارة إليه، فأصبح مستخدموها من جميع الفئات العمرية وعلى مختلف مستويات تعليمهم، وبذلك فتحت الأبواب المغلقة، ودق ناقوس الخطر لا سيما، وأن هذه الشبكة بقيت بدون حراسة أو قيود أو حدود لردع الأعمال السيئة التي مصدرها دائماً البشر، وعليه فإن الانفتاح الكبير على التكنولوجيا والتقدم التقني كان عاملاً لظهور ما يسمى بالجرائم الإلكترونية التي أتت لتقرع أجراس الخطر، ولتنبه مجتمعات العصر الحالي من حجم المخاطر وهول الخسائر الناجمة عنها.

ولقد أسهمت هذه الشبكة في معرفة وسائل الاتصال المختلفة والبرامج بأنواعها كافة، والتي تمكّن من الدخول إلى الحاسوب وشبكات الإنترنت والبرامج التي تمكّن المجرمين من اختراق الأنظمة الحاسوبية، وهو بحد ذاته أسهم في تسهيل مهمة قرصنة المعلومات، ما جعل عمليات مكافحة التجسس والمحافظة على سرية المعلومات، وحمايتها من الإتلاف أو التدمير أو الاختراق أكثر صعوبة، ومن الأسباب التي تكون وراء عدم القدرة على حماية تلك المعلومات والبيانات، هو عدم وجود أجهزة مختصة لها الخبرة والقدرة على مكافحة الجرائم الإلكترونية بأنواعها المختلفة، وكذلك ندرة القوانين التي تحرّم وتعاقب على تلك الأفعال الإجرامية. ولقد أسهم التطور التكنولوجي إلى تحييد المجرمين عن استخدام الأساليب التقليدية في ارتكاب الجرائم، وهذا ساعد في إبراز أساليب حديثة تتماشى والتقدم الحاصل في تكنولوجيا المعلومات، لتصبح الجريمة الإلكترونية أكثر تنفيذاً باستعمال شبكة الإنترنت، وباستخدام الحاسوب كأداة في ارتكاب الجريمة، وهذا أوجد مخاوف للمؤسسات والجماعات والأفراد الذين يستخدمون الحاسوب وشبكة الإنترنت من الاعتداء عليهم من قبل المجرمين والمساس بالبيانات والمعلومات الخاصة بهم، وهو ما يهدد الأمن والسلم الدوليين بارتكاب جرائم متنوعة كالإرهاب والاحتيال والتزوير واختراق المواقع والتشهير بالأفراد والاعتداء على خصوصيتهم وسرقة الأموال.

إن الإختراق جريمة تتم بالخفاء، حيثُ يقوم بها مجرمون أذكيايمتكون قدرة على اختراق واكتشاف الثغرات الموجودة في المواقع الإلكترونية أو بجهاز الحاسوب، وبالتالي؛ فإن إدراك ماهية جريمة الاختراق وطبيعتها، ومعرفة أشكالها ودوافعها ومخاطرها وما يترتب عليها من خسائر إنما يتخذ أهمية استثنائية من أجل سلامة التعامل مع هذه الجريمة ونطاق مخاطرها الاقتصادية والاجتماعية والأمنية.

ويمكن تحديد أهمية الدراسة، أهداف الدراسة، إشكالية الدراسة، منهجية الدراسة، مصطلحات الدراسة.

أهمية الدراسة:-

رافق التطور الكبير الذي شهده العالم في المجال التكنولوجي إلى ظهور جرائم جديدة، أصبحت تعرف باسم "الجرائم الإلكترونية" حيث استغلها المخترقون من أجل الوصول إلى غايتهم وأهدافهم التي يسعون إلى تحقيقها، فمن خلال هذه الدراسة سوف نتعرف على جريمة الاختراق التي تعتبر من الجرائم التي ظهرت وتطورت مع التطور التكنولوجي، وتأتي أهمية الدراسة في قلة المصادر والمراجع التي تعالج هذا الموضوع ، وبالتالي هو ضروري لكل شخص يتعامل مع الحاسب الآلي، من أجل ضمان الامان وتحقيق السرية الخاصة للمعلومات، وكيفية الوقاية من تلك الجرائم الإلكترونية.

أهداف الدراسة:-

تهدف هذه الدراسة إلى التعرف على كيفية التعامل مع الحاسب الآلي، وكيفية الوقاية من الجرائم الإلكترونية وحماية المعلومات السرية الخاصة وزيادة الوعي لكل من يستخدم الحاسب الآلي ومن يعمل على شبكة الإنترنت، ومعرفة ما هي جريمة الاختراق وما أثرها على الشبكة الإلكترونية والنظم المعلوماتية. كما وتعتبر هذه الدراسة مرجعاً مهماً لطلبة العلم.

إشكالية الدراسة:-

تکمن إشکالية الدراسة في أن جريمة الإختراق تعتبر من الجرائم الخطرة التي تهدد كل من يستخدم الحاسب الآلي والشبكة العنكبوتية، كما وتتمثل مشكلة الدراسة في مدى كفاية القواعد التشريعية لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في النظم المعلوماتية.

منهجية الدراسة:-

أعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي؛ إذ سيعمل الباحث على تحليل النصوص القانونية التي لها صلة في الموضوع.

مصطلحات الدراسة:-

الحاسب الآلي:- هو أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو إستقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له^١.

الشبكة الإلكترونية:- ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت)^٢.

الاختراق:- هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية^٣.

١ قانون المعاملات الإلكترونية الفلسطيني رقم (٦) لسنة ٢٠١٣م الفصل الأول، تعاريف وأحكام عامة.

٢ قانون الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة ٢٠١٨م، المادة الأولى.

المجرم المعلوماتي: - هو كأي مجرم يقوم بارتكاب جريمة، لكنه يختلف عن المجرم التقليدي في أن المجرم المعلوماتي يتمتع بصفات خاصة تميزه عن المجرم التقليدي، كالخبرة والمهارة والذكاء في التعامل مع الحاسوب ومكوناته وبرامجه، ويرتكب جريمة معاقب عليها قانوناً^٤.

الهاكرز: - وهم الأشخاص الذين يشعرون بالفخر لاحتسابهم بمعرفتهم بأساليب عمل النظام أو الشبكات بحيث يسعون للدخول عليها بدون تصريح، وهؤلاء الأشخاص عادةً لا يتسببون بأي أضرار مادية، ولديهم قدرة بالغة على حل المشكلات كما يعتبروا أكثر الأشخاص علماً بخفيا وأسرار الحواسيب والإنترنت^٥.

البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها^٦.

نظم المعلومات: - مجموعة من الإجراءات والبرامج والأفراد والأجهزة والاتصالات وقاعدة البيانات التي تهدف إلى إنتاج معلومات محددة^٧.

^٢ راجع المادة (١) من قانون الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة ٢٠١٨.
^٤ العريان، محمد، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر، ٢٠٠٤، ص٦٢.
^٥ صادق، دلال، القتال، حميد، أمن المعلومات، دار اليازوري للنشر والتوزيع، عمان، الأردن، ٢٠١٣، ص١٤٢+١٤٣.
^٦ قانون الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة ٢٠١٨ م، المادة الأولى.
^٧ غراب، كامل، حجازي، فادية، نظم المعلومات الإدارية، مكتبة ومطبعة الأشعاع الفنية، ط٢، الإسكندرية، مصر، ٢٠٠٠، ص٩٠، ٣.

الأمن المعلوماتي: - هو حماية المعلومات المختلفة والأدوات التي تتعامل معها وتعالجها، من منظمة وغرف تشغيل أجهزة وأجهزة وسائط تخزين وأفراد من السرقة، أو التلف، أو الاختراق، أو الضياع، أو التزوير، وذلك من خلال اتباع إجراءات وسياسات وقائية^٨.

^٨ القحطاني، منصور، مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٨، ص ١٧.

الفصل الأول

الجانب الفني والتقني للحاسوب والانترنت

بالرغم من بعد القانون عن الأمور التقنية والتكنولوجية، إلا أنه من الجيد أن نتطرق إلى هذه الأمور والتعرف على الجانب الفني والتقني والتكنولوجي لكل من الحاسوب والانترنت، وذلك لارتباطهما ارتباطاً وثيقاً بموضوع الرسالة، حيث يتضمن هذا الفصل التعرف على الجانب الفني والتقني للحاسوب والانترنت، وذلك من خلال تعريف الحاسب الآلي أو (الحاسوب)، وبيان مكونات الحاسوب، ومعرفة مفهوم جرائم الحاسب الآلي وأنواعها وأنماطها، وتعريف الانترنت ونشأته، ثم التطرق إلى سلبيات وإيجابيات شبكة الإنترنت.

- **المبحث الأول:- الجانب الفني والتقني للحاسوب.**
- **المبحث الثاني:- الجانب الفني والتقني للانترنت.**

المبحث الأول

الجانب الفني والتقني للحاسوب

من الجدير ذكره أن الحاسب الآلي قد تطور بشكل كبير، وخاصة في هذا العصر التكنولوجي الذي أصبح فيه العالم قرية صغيرة، وتأتي بداية إنتاج الحواسيب الشخصية في أواخر السبعينات إلى أوائل الثمانينات، وقد كان إنتاج تلك الأجهزة محدوداً، فلم تنتشر بشكل واسع، ففي عام ١٩٥٠ كان عدد أجهزة الحاسوب لا تصل إلى مئة جهاز، وازدادت عام ١٩٧٠ إلى عشرة آلاف جهاز، وفي نهاية عام ١٩٩١ تم إنتاج أكثر من ٨٥ مليون جهاز، وهذا الرقم تزايد مع التطور التكنولوجي في الوقت الحالي^٩.

سنسلط الضوء في هذا المبحث على الجانب الفني والتقني للحاسوب، دون الدخول في تفاصيل الحاسوب بشكل واسع، حيث يقتصر هذا المبحث على ما يلي:-

- **المطلب الأول:- ماهية جهاز الحاسوب وطبيعة جرائمه وخصائصه.**
- **المطلب الثاني:- مكونات الحاسوب الآلي وذاتية جرائمه.**

^٩ المسند، صالح، المهيني، عبد الرحمن، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض مج١٥، ع٢٩٦، ٢٠٠٠، ص١٤٧-١٤٨.

المطلب الأول

ما هية جهاز الحاسوب وطبيعة جرائمه وخصائصه.

تطور جهاز الحاسوب من آلة حاسبة بسيطة إلى جهاز كهربائي يقوم بالعديد من العمليات، ويزداد يوماً بعد يوم أهمية الدور الذي يقوم به في المؤسسات سواء أكانت اقتصادية أو عسكرية أو غيرها، فأصبح لديه القدرة على أداء العمليات الحسابية والكتابية والقدرة الكبيرة على تخزين المعلومات والبيانات^{١٠} خشية الضياع وسهولة عرض هذه البيانات والمعلومات عند طلبها من قبل المستخدم، كما أن للحاسوب القدرة على تبادل البيانات والمعلومات مع أجهزة أخرى متوافقة، وهناك اختلاف كبير وواضح ما بين حواسيب العصر الماضي وحواسيب العصر الحاضر، وهي في قدرة الحواسيب الحديثة على إجراء البلايين من العمليات الحسابية والمنطقية في ثوانٍ معدودة.

ويعد جهاز الحاسوب جهازاً متنوع المهام، إذ أنه يساعد جميع مستخدميهم في حياتهم الشخصية أو المهنية بطرق متعددة، ويسهل عليهم إجراءات القيام بالمهام المطلوبة، ويوفر عليهم الوقت الكثير^{١١}.

لهذا قمنا بتقسيم هذا المطلب إلى ثلاثة فروع، حيث تناول في الفرع الأول تعريف الحاسوب، وفي الفرع الثاني الطبيعة القانونية لجرائم الحاسوب، وفي الفرع الثالث خصائص الحاسوب.

^{١٠} الحلبي، خالد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط١، دار الثقافة للنشر والتوزيع، ص٣٩.

^{١١} سقف الحيط، عادل، جرائم الهم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، ط٢، ٢٠١٥، عمان، ص٤١.

• الفرع الأول:- تعريف الحاسوب.

هناك تعريفات عدة لجهاز الحاسوب (الحاسب الآلي) منها^{١٢}:-

يمكن تعريف الحاسوب :- بأنه جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة، وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة^{١٣}.

كما يمكن تعريفه أيضاً بأنه مجموع متكاملة من الأجهزة التي تعمل مع بعضها البعض بهدف تشغيل (process) مجموعة البيانات الداخلة (input data) وذلك طبقاً لبرنامج (program) وتم وضعه مسبقاً من أجل الحصول على نتائج معينة^{١٤}.

كما عرفه جانب آخر من الفقه بأنه:- عبارة عن آلة إلكترونية تستخدم وفق نظام معين لمعالجة وإدارة البيانات والمعلومات الرقمية المدخلة فيه، وفق أوامر وتعليمات يختارها المشغل أو طالب الخدمة^{١٥}.

وهو أيضاً جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، ويكون ذلك من خلال تنفيذ عمليات عدة منها استقبال البيانات المدخلة، ومعالجة تلك البيانات إلى معلومات، وتحويل المعلومات إلى نتائج^{١٦}.

١٢ الحاسب الآلي هي التسمية العربية المتعارف عليها، وتقابلها باللغة الانجليزية لفظ (Computer)، نقلاً عن حسين عبد الرحمن، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة رسالة ماجستير في القانون العام غير منشورة، جامعة النجاح الوطنية، نابلس، ٢٠٠٨، ص٦.

١٣ الحلبي، خالد، مرجع سابق، ص٤٠.

١٤ عبدالله، محمود، سرقة المعلومات المخزنة في الحاسب الآلي أطروحة دكتوراه منشوره جامعة عين شمس، كلية الحقوق، ٢٠٠١، ص١٥+١٦.

١٥ المناعسة، أسامة، الزعبي، جلال، جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع، ط٣، عمان، ٢٠١٧، ص٢٧.

كما عرفه جانب آخر من الفقه بأنه:- نظام إلكتروني مصمم لكي يقوم بعدة مهام يطلبها طالب الخدمة بناءً على بيانات ومعطيات يتم تلقيها من أجل القيام بتلك المهام ويقوم بها في زمن قياسي^{١٧}.

وقد ورد تعريف الحاسوب أيضاً في موسوعة دلتا كمبيوتر والتي عنوانته باسم الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، وذلك لشموله على جميع الوظائف التي يقوم بها الحاسب الآلي في الحياة، ومن بين هذه التعريفات أنه جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال بيانات أو إخراج معلومات وإجراء العمليات الحسابية أو المنطقية^{١٨}.

وفي قانون المعاملات الإلكترونية الفلسطيني رقم (٦) لسنة ٢٠١٣م ورد تعريف الحاسب الآلي حسب المشرع الفلسطيني بأنه:- أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو استقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له^{١٩}. وهو أيضاً جهاز إلكتروني دقيق وسريع وقادر على معالجة البيانات، وصمم ونظم لقبول وتخزين ومعالجة البيانات أوتوماتيكياً لإنتاج مخرجات باستخدام برامج مطولة من التعليمات^{٢٠}.

١٦ المومني، نهلا، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط٢، ٢٠١٠، ص ٢٠.

١٧ واصل، محمد، بحث منشور بعنوان: الحماية القانونية لبرامج الحاسوب (المصنفات الإلكترونية)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج ٢٧، ع ٣، ٢٠١١، ص ٩.

١٨ عبدالله، أحمد، حجية المخرجات الكمبيوترية، في المواد الجنائية، ط١، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ١٩٩٧، ص ١٤.

١٩ قانون المعاملات الإلكترونية الفلسطيني رقم (٦) لسنة ٢٠١٣م الفصل الأول، تعاريف وأحكام عامة.

٢٠ الخليفة، محسن، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام رسالة ماجستير غير منشورة، أكاديمية نايف للعلوم الأمنية، قسم العدالة الجنائية، ٢٠٠٣م، ص ٢١.

وقد عرفه المشرع الأمريكي بأنه:- أداة إلكترونية مغناطيسية مرئية كهروكيميائية أو أية أداة ذات سرعة عالية في معالجة البيانات تؤدي عمليات منطقية رياضية أو عمليات تخزين وتتضمن أية تسهيلات لتخزين البيانات أو تسهيلات إتصالية ذات ارتباط مباشر بالتشغيل^{٢١}، وباختصار، فهو جهاز إلكتروني يمكن برمجته ليقبل مدخلات وبيانات ويحول هذه البيانات إلى معلومات مفيدة^{٢٢}.

وبالتالي فإننا نرى بأن الحاسوب عبارة عن:- جهاز إلكتروني يقوم بالعديد من المهام والوظائف خلال زمن قياسي، وذلك من خلال مستخدم الحاسوب (الإنسان) الذي يقوم بإعطائه تلك الأوامر.

من خلال تلك التعريفات السابقة عن الحاسوب يتضح لنا ما يلي:-

- ✓ أن الحاسوب فيه جهاز إلكتروني يتكون من وحدات مستقلة.
- ✓ يستقبل جميع البيانات المدخلة له.
- ✓ يحفظ تلك البيانات ويعمل على تخزينها من الضياع.
- ✓ يعمل على معالجة البيانات بطريقة سريعة ودقيقة.
- ✓ يحول البيانات المدخلة له إلى نتائج يمكن استخدامها بأغراض مختلفة.

٢١ الحسيناوي، علي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، ٢٠٠٩، ص٢٢.

٢٢ مهنا، عبد الوهاب، درجة توظيف الحاسوب في الإدارة المدرسية بمدارس وكالة الغوث في محافظات غزة وسبل تطويرها رسالة ماجستير غير منشورة، الجامعة الإسلامية، عمادة الدراسات العليا، كلية التربية، غزة، ٢٠٠٩، ص٢٩.

نود الإشارة في هذا المجال إلى تعريف جريمة الحاسب الآلي، فهي من الجرائم التي ظهرت وتطورت مع التطور التكنولوجي، وتشكل جرائم الحاسب الآلي تهديداً للأمن وللاقتصاد الوطني بشكل عام، كما تمثل انتهاكاً لحقوق الأفراد والجماعات والشركات^{٢٣}.

فقبل الإشارة إلى موضوع جريمة الحاسب الآلي، سوف نعطي نبذة تعريفية عن الجريمة بشكل عام، **فالجريمة لغةً**: - الجرم هو القطع، فيقال جرّمه يُجرّمه جرماً بمعنى قطعه، وشجرة جريمة: أي مقطوعة وجرّم النخل والتمر يُجرّمه جرماً وجرّاماً وجرّاماً واجترّمه: صرّمه. وجرمت صوف الشاة أي جزرته^{٢٤}، **والجريمة اصطلاحاً**: - عرفها أبو يعلى الفراء بأنها المحظورات بالشرع، زجر الله تعالى عنها بحد أو تعزير^{٢٥}، **والجريمة بشكل عام**: - هي فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبير احترازي^{٢٦}، وهذا ما أيده الدكتور محمود مصطفى في كتابه شرح قانون العقوبات القسم العام.

إن لقيام الجريمة بشكل عام ثلاثة أركان أساسية فلا جريمة دون وجود لأحد هذه الأركان.

١- **الركن القانوني** أي أن يكون هذا الفعل معاقب عليه قانوناً، وأن يكون المشرع قد ذكر تلك الجريمة في قانون العقوبات أو في قانون خاص بالجريمة إن لم يكن منصوصاً عليها في قانون العقوبات (**فلا جريمة ولا عقوبة إلا بنص**). ٢- **الركن المادي**: - يتمثل بالفعل أو النشاط الذي

^{٢٣} أحمد، هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، ط ١، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ١٩٩٧، ص ٢٢.

^{٢٤} ابن منظور، محمد بن مكرم (ت ٧١١هـ/١٣١١م) معجم لسان العرب، مج ١٢، ط ٣، دار صادر للنشر والتوزيع، لبنان، بيروت ١٩٩٠م، ص ٩٠.

^{٢٥} الحنبلي، أبي يعلى، الأحكام السلطانية، صححه وعلق عليه "محمد حامد الفقي"، دار الكتب العلمية، بيروت، لبنان، ٢٠٠٠، ص ٢٥٧.

^{٢٦} تنوري، سلام، جرائم الحاسوب والإنترنت، دراسة قدمت للجامعة اللبنانية، كلية الدراسات العليا، قانون الأعمال المحلي والدولي.

يقوم به الجاني ويتمثل بالاعتداء على حق أو مصلحة حماها القانون، وهو النشاط الخارجي للمجرم. ٣- **الركن المعنوي**: - يتمثل بعنصري العلم والإرادة وهو أن يكون الجاني عالماً بما يفعل ولديه علم كامل، والإرادة أي أن تتجه إلى حدوث النتيجة.

وقد عرف مكتب تقييم التقنية في الولايات المتحدة الأمريكية جريمة الحاسب الآلي بأنها: - الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيساً في ارتكاب الجريمة^{٢٧}. ويمكن أن نعرف جريمة الحاسب الآلي من الناحية الفنية على أنها: - " نشاط إجرامي يستخدم فيه الجاني الحاسوب من أجل القيام بجريمته وتنفيذها، سواء كانت قد تمت بطريقة مباشرة أو غير مباشرة^{٢٨}. وهناك من أشار إلى أن جرائم الحاسب الآلي لها مصطلحات عديدة منها: - الجرائم الإلكترونية، جرائم تقنية المعلومات، جرائم التقنية العالية، جرائم معلوماتية، كل هذه المصطلحات هي للدلالة على الجرائم التي تستخدم الحاسب الآلي في ارتكابها لجرائمها، او هي للدلالة على جرائم وقعت على جهاز الحاسوب واستهدفته^{٢٩}. وتعرف جريمة الحاسب الآلي بأنها: - هي الغش والسرقة والابتزاز وغيرها من أنواع الجريمة، وذلك بتسخير أو إساءة استخدام الحاسب الآلي^{٣٠}.

^{٢٧} الشدى، طارق، آلية البناء الأمني لنظم المعلومات، دار الوطن للنشر والتوزيع، ط١، الرياض، السعودية، ٢٠٠٠، ص١٩. أنظر أيضاً ل- الملط، أحمد، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٦، ص٨٤.

^{٢٨} البشرى، محمد، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض مج١٥، ع٣٠٤، ٢٠٠٠، ص٣٢١.

^{٢٩} البشرى، محمد، ندوة علمية بعنوان "الإنترنت والإرهاب"، عنوان المداخلة "تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، تاريخ انعقاد الندوة (١٥-١٩/١١/٢٠٠٨م)، ص٩.

^{٣٠} الخليفة، محسن، مرجع سابق، ص٤١.

واتجه جانب من الفقه الفرنسي ومنهم الأستاذ (Massa) إلى تعريف جرائم الحاسوب على أنها الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح. وعرف الفقيه الألماني تاديمان الجريمة المعلوماتية على أنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يتم ارتكابه باستخدام الحاسب الآلي^{٣١}. وعرفها خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية على أنها كل سلوك غير مشروع ومنافٍ للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها^{٣٢}. ويعرفها فريق من الفقهاء على أنها :- كل سلوك إجرامي يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية^{٣٣}. وقد عرفها الأستاذ جون فورستر بأنها:- فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية^{٣٤}.

وأرى بأن هناك قصور في إيجاد تعريف واضح وشامل لجريمة الحاسب الآلي يتفق عليه كافة المشرعين والمختصين بذلك الموضوع. لهذا نعرف بأن مصطلح جريمة الحاسوب:- هي تلك الجريمة التي يستخدم فيها الجاني الحاسوب بحيث تكون هي الأداة التي يتم من خلالها القيام بالعمل الإجرامي، وأن يكون لمرتكب الجريمة المعرفة الكاملة بالحاسوب، وأود الإشارة إلى أن مصطلح الجرائم المعلوماتية أدق وأشمل من جرائم الحاسوب، والسبب يكمن في أن الجرائم المعلوماتية تشمل الحاسوب وكل ما يتم ابتكاره من تقنيات تكنولوجية متسحدثة ومتطورة.

^{٣١} عباينة، محمود، الرازقي، محمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٥، ص ١٥.

^{٣٢} الشمري، غانم، الجرائم المعلوماتية ماهيتها. خصائصها. كيفية التصدي لها قانونياً، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط ١، ٢٠١٦، ص ٢٥.

^{٣٣} سفيان، سوير، جرائم المعلوماتية، مذكرة ماستر غير منشورة، جامعة أبو بكر بلقايد تلمسان، الجزائر، ٢٠١١، ص ١٤.

^{٣٤} الحلبي، خالد، مرجع سابق، ص ٢٩.

إن جرائم الحاسوب متنوعة وأشكالها متعددة، فهناك أنواع للجرائم التي يتم ارتكابها بواسطة الحاسب الآلي بأعتبره أداة لارتكاب الجرائم الإلكترونية ومنها:-

أولاً_ جريمة استنساخ برامج الحاسوب.

وهي الجريمة التي يقوم بها القرصنة، فالقرصان وظيفته قرصنة البرامج والألعاب، وأي أعمال إبداعية له حقوق محفوظة، وهو يقوم بتهكير تلك البرامج والألعاب وغيرها ليحصل عليها دون شراء من الشركة المنتجة لها ثم يبيع تلك البرامج والألعاب بأسعار منخفضة جداً، الأمر الذي يؤثر بشكل كبير على الشركات المنتجة لها، أي أن القرصنة عملية نسخ غير مشروعة واستخدام للبرامج دون أي إذن من جهة الاختصاص صاحبة الإنتاج^{٣٥}. والاستنساخ قد يكون حرفياً للبرنامج وقد يكون غير حرفي. حرفياً بمعنى أن يتم إعادة إنتاج البرنامج كما هو دون أن يتم إجراء أي تعديل أو حذف في خصوصية البرنامج، وهذا الاستنساخ يعد أشد أنواع النسخ خطورةً على الشركات المنتجة للبرامج، وغير حرفي أن يقوم به قرصنة محترفون بحيث يقومون بانتحال وأخذ نسخة مشابهة عن البرنامج، وتكون مطابقة للبرنامج الأصلي^{٣٦}.

هنالك جدل فقهي بين فقهاء الشريعة والقانون حول تجريم استنساخ البرامج أو عدم استنساخها، فيرى البعض جواز استنساخ البرامج طالما أن الاستنساخ كان بقصد الاستخدام

^{٣٥} كهينة، سليمان، ضاوية، زوازي، النظام القانوني لبرامج الحاسوب الآلي، مذكرة ماستر غير منشورة، جامعة عبد الرحمان ميرة-بجاية، الجزائر، ٢٠١٦، ص ٣٤+٣٥.

^{٣٦} حسين، عبد الرحمن، مرجع سابق، ص ١٣+١٤.

الشخصي، ويرى البعض الآخر بعدم جواز الاستساح باعتباره اعتداء على حق من حقوق الملكية، ومن الحقوق التي تتمتع بها الشركة المنتجة له فقط^{٣٧}.

ثانياً_ جريمة إنتاج فيروسات الحاسوب.

فيروسات الحاسب الآلي هي عبارة عن برنامج يقوم المجرم المعلوماتي بإنتاجه، وهي إحدى أنواع البرامج التي يتم إنتاجها بحيث ينتشر هذا البرنامج بسرعة كبيرة وبشكل سريع ويربط نفسه داخل البرامج الأخرى الموجودة بالجهاز، ويقوم بأعمال تخريبية تضر بالجهاز وبمحتوياته. فعند قيام صاحب الحاسوب بتشغيله وفتح البرنامج قد يكون هذا البرنامج مصاباً بالفايروس وبالتالي يمكن إلحاق الضرر بالحاسوب من خلال محو البيانات وتدميرها، وهذا بحد ذاته يشكل ضرراً كبيراً للحاسوب ولمحتوياته^{٣٨}.

ولقد ازداد الرعب من الفايروس بسبب التزايد الهائل في حجم استخدام الحاسوب، وينتقل الفايروس عندما يتم استخدام وسيط تخزيني ملوث بفايروس من الفيروسات، وعندما يتم إدخال الوسائط وتحميل البيانات على الحاسوب يتم تدمير تلك البيانات أو تعطيل استخدامها، فيتوجب ويفضل أن يتم تجربة هذه البيانات قبل تخزينها على الحاسوب الرئيسي^{٣٩}. فالفايروس والدودة هما مثالين على العمليات التخريبية التي تعمل على مهاجمة البرمجيات والبيانات، وقد يكون

^{٣٧} السرحاني، محمد، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، ٢٠٠٤، ص ٤٩.

^{٣٨} الصالح، صالح، دورة تدريبية بعنوان مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، تاريخ عقدها (١٠-١٤/٣/٢٠٠٧م)، ص ٢١.

^{٣٩} أبكر، سليمان مصطفى، جرائم الحاسب الآلي وطرق المواجهة، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، ٢٤٣ع، نشر بالمجلة بشهر (١٠/٢/٢٠٠٢)، ص ٥٠.

ذلك من خلال استخدام اقراص (CD) تحتوي على برامج خبيثة تدميرية بحيث تكون مخفية داخل البرامج المفيدة^{٤٠}، وهناك أنواع للفيروسات نذكر منها: - ١_ فيروسات الجزء التشغيلي للإسطوانة كفيروس براين ٢_ فيروس متطفل كفيروس (Cascad) ٣_ فيروسات متعددة الأنواع كفيروس (Spanish Telecom) وغيرها^{٤١}. نخلص للقول بأن الهدف من الفيروسات هو تدمير البيانات والبرامج مما يؤدي إلى تعطيلها وتخريبها وتلفها^{٤٢}.

للفيروسات سمات عديدة منها: - ١_ قدرتها على الاختفاء ٢_ سرعتها بالانتشار داخل الحاسب وشبكات الحاسب ٣_ قدرتها على التسلل واختراق حواجز الأمن ٤_ قدرتها على تدمير البيانات والمعلومات ٥_ قدرتها على تعطيل الحاسوب بشكل كامل^{٤٣}.

ثالثاً_ جريمة تدمير بيانات الحاسوب.

ويعني ذلك أن يتم تدمير نظم المعلومات بالمحو أو التعديل أو الإتلاف، بهدف إحداث ضرر واخل في النظام الحاسوبي، لكي لا يكون قادراً على القيام بمهامه، إذاً الهدف من تدمير نظم المعلومات هو إتلاف أو محو تعليمات البرنامج أو البيانات نفسها، فهو لا يريد تدمير بيانات الحاسوب من أجل الحصول على منفعة، بل هو بكل بساطة يرغب في تدمير النظام

^{٤٠} الطيطي، خضر، أساسيات أمن المعلومات والحاسوب، دار الحامد للنشر والتوزيع، عمان، الأردن، ٢٠١٠، ص١٣٦.

^{٤١} عمار، ماجد، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ١٩٨٩، ص٣٥.

^{٤٢} فكري، أيمن، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد للنشر والتوزيع، الرياض، السعودية، ٢٠١٥، ص١٧٣.

^{٤٣} الخليفة، محسن، مرجع سابق، ص٤٧.

وإعاقته عن القيام بوظائفه^{٤٤}. لقد ورد تعريف الإتلاف في القرار بقانون رقم (١٠) لسنة (٢٠١٨) والخاص بالجرائم الإلكترونية، وهو ما يعني في مدلوله التدمير، حيث عُرفَ على أنه: - تدمير البرامج الإلكترونية سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال^{٤٥}. وإذا أمعنا النظر في المادة (٦) من نفس القرار بالقانون، فإنها نصت على أنه: - " كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً"^{٤٦}. ونود أن نشير أيضاً إلى أن اتفاقية بودابست لمكافحة الجرائم المعلوماتية والتي وقعت سنة (٢٠٠١) قسمت جرائم الكمبيوتر والإنترنت إلى طوائف، وتناولت فيها الجرائم التي تستهدف سلامة وسرية المعلومات واعتراضها وتدميرها وإتلافها^{٤٧}. وتجدر الإشارة إلى أن إتلاف المعلومات وتدميرها يقوم على صور عدة ومنها:-

١. شطب البرنامج والمعلومات والبيانات والمعطيات التي تكون مخزنة على الحاسب

الآلي. ٢. تخريب البيانات والمعلومات والقيام بتغييرها أو تعديلها، وهذا ما يجعلها

غير صالحة للعمل^{٤٨}.

^{٤٤} الحلبي، خالد، مرجع سابق، ص ٦٨.

^{٤٥} أنظر المادة (١)، قرار بقانون بشأن الجرائم الإلكترونية رقم (١٠) لسنة (٢٠١٨م).

^{٤٦} أنظر المادة (٦)، قرار بقانون بشأن الجرائم الإلكترونية، رقم (١٠) لسنة (٢٠١٨م).

^{٤٧} شنين، صالح، الحماية الجزائية لبرامج الحاسب الآلي، مذكرة ماستر غير منشورة، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٠٧، ص ٢٠.

^{٤٨} قشقوش، هدى، جرائم الحاسب الإلكتروني، دار النهضة العربية للنشر والتوزيع، ط ١، ١٩٩٢، ص ٥٠.

رابعاً_ جريمة السرقة من خلال الحاسوب.

إن جريمة السرقة تعني أخذ مال الغير عنوةً ودون أخذ أذنه بذلك، والسرقة في الحاسب الآلي تتم من خلال قيام فرد باستخدام نظام مستخدم آخر أو جهة أخرى بحيث يتصرف في النظام دون إذن من مستخدم النظام الأصلي. ومع هذا التطور التكنولوجي أصبح من الممكن أن يقوم المجرم المعلوماتي بالسرقة، كسرقة البنوك أو المؤسسات والشركات التجارية وهو في منزله ومكان الجريمة في مكان آخر وقد تكون خارج حدود دولته. ولم يغفل المشرع الفلسطيني بالحديث عن جريمة السرقة التي تتم عبر الإنترنت، حيث نصت المادة (١٣) من القرار بقانون رقم (١٠) لسنة (٢٠١٨) بشأن الجرائم الإلكترونية على أنه: "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"^{٤٩}. يفهم من ذلك أن مشرعنا الفلسطيني قد عاقب على ذلك الفعل واعتبره عملاً إجرامياً بامتياز؛ لأنه يمس خصوصية الأفراد والمؤسسات والشركات.

خامساً_ جريمة التزوير والتزيف من خلال الحاسوب.

من الوهلة الأولى يبدو للقارئ بأن التزوير ما هو إلا تغيير للواقع وللحقيقة. فالمعلومات والبيانات التي تكون موجودة على ذاكرة الحاسب الآلي تمثل محرراً يصلح أن يكون محلاً لجريمة التزوير^{٥٠}.

^{٤٩} أنظر المادة (١٣)، قرار بقانون بشأن الجرائم الإلكترونية، رقم (١٠) لسنة (٢٠١٨م).
^{٥٠} المناعسة، أسامة، الزعبي، جلال، مرجع سابق، ص ١٦٤.

إن طريقة تزوير البيانات والمعلومات في الحاسب الآلي سهلة، إذ يقوم بعض المجرمين باستخدام الحاسوب كأداة لتزوير الوثائق والأسهم والسندات وغيرها من الأوراق المهمة، وقد أشرنا بأنها سهلة لأنها لا تحتاج إلا إلى حاسوب شخصي وبرامج خاصة بتغيير بعض الشعارات الرسمية أو تغيير نصوص كالفوتوشوب وبرنامج الرسام ذات الكفاءة العالية^{٥١}. ومن الأمثلة على التزوير والتزييف، "أنه في عام (١٩٩٢) تم إدانة مجرم يدعى "كابن كرنش" ومعه مجموعة من زملائه بتهمة تزييف تذاكر سفر لعبارة خليج سان فرانسيسكو، وكذلك إدانة عصابات في الولايات المتحدة الأمريكية في ولاية ميث بتهمة تزوير شيكات مصرفية منسوبة لأحد البنوك^{٥٢}.

لقد سهلت شبكة الإنترنت في انتشار الجريمة المعلوماتية بشكل كبير، حيث أصبح بإمكانهم القيام بعملهم الإجرامي، دون الحاجة للذهاب إلى مكان الجريمة ودون تكبد عناء التنقل من دولة لأخرى، فشبكة الإنترنت قربت البعيد وجعلت كل شيء متاحاً أمام شاشة الحاسوب، كذلك يمكن إضافة سبب آخر، وهو أن ضعف الوعي لدى مستخدمي الحاسوب وشبكة الإنترنت وعدم معرفتهم بالأساليب والطرق التي يتم فيها ارتكاب تلك الجرائم هذا كان سبباً أيضاً في انتشار تلك الجرائم بشكل كبير. أضف إلى ذلك أن إزدياد إقبال المستخدمين للحاسوب وشبكة الإنترنت بسبب سهولة استخدامها، شكّل فرصة كبيرة للمجرمين للقيام بجرائمهم دون وجود رقيب عليهم، فالمعرفة والخبرة التي يمتلكها هؤلاء المجرمون سهلت عليهم الكثير ووفرت لهم الفرص الكبيرة

^{٥١} الخليفة، محسن، مرجع سابق، ص ٤٩.

^{٥٢} داود، حسن، جرائم نظم المعلومات، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، ع ٢٤٣، نشر بالمجلة بشهر (٢٠٠١٥)، ص ٤٩.

من أجل تحقيق رغباتهم في اختراق الحواسيب والشبكات الإلكترونية. وهذا بحد ذاته ألقى عبئاً كبيراً على القائمين في مجال مكافحة الجريمة ضمن الأسس والقواعد المتبعة لإجراءات التحقيق والتحري والبحث، وهذا جعل من الضروري مراجعة الأحكام والقوانين التقليدية، لكي يتم ملائمتها مع الجرائم الجديدة ولمواكبة أي تطور جديد يظهر على التقنيات المعلوماتية^{٥٣}. ونرى بأن السبب الرئيس في انتشار جرائم الحاسوب بشكل سريع، هو أن هذا النوع من الجرائم لا يخلف أثراً كالجرائم التقليدية، فهو لا يحتاج إلى أسلحة بيضاء أو أسلحة نارية ولا يحتاج إلى استخدام العنف والقتل وأن يترك دماء في مسرح الجريمة وبالتالي فرار المجرم من العقاب غالباً، ففي الجريمة الإلكترونية لا يوجد شاهد على مسرح الجريمة ولا يترك المجرم في أغلب الأحيان أثراً يؤدي إلى وقوعه تحت حكم القضاء^{٥٤}. وإذا تم اكتشاف الجريمة الإلكترونية، فإنه يكون من باب الصدفة. إضافة لذلك عدم تعاون المجني عليه في الكشف عن الجرائم التي ترتكب ضده أدى إلى عدم وجود إحصائيات حقيقية تحدد نسبة الجرائم المرتكبة^{٥٥}. إذاً نخلص إلى القول بأن جريمة الحاسب الآلي جريمة يصعب كشفها وإثباتها بسبب ارتكابها بطريقة تقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها^{٥٦}. لهذا فإن المجرم المعلوماتي من خلال ارتكابه للجريمة المعلوماتية فهو غالباً يسعى إلى تحقيق مكاسب مادية من ورائها، ويوظف كل مهارته الفنية من أجل تحقيق الربح المادي. وفي استبانة أجزاها أحد الباحثين في الولايات

^{٥٣} عباس، طالب، عواد، عبد الجبار، بحث بعنوان جرائم تقنية المعلومات وإثباتها، موجود على <https://www.iasj.net/iasj?func=fulltext&ald=34155>، تاريخ الدخول (٢٠١٨/٧/٢٠)، ص ٢.

^{٥٤} الطائي، حعفر، جرائم تكنولوجيا المعلومات وآليات الحد منها، مجلة الفتح، جامعة ديالى، العراق، تاريخ النشر (٢٠١٥/١١/٤)، ص ٤١١_٤٢٧، ص ٤١٧.

^{٥٥} الشمري، غانم، مرجع سابق، ص ٤٠.

^{٥٦} نورة، طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماستر غير منشورة، جامعة الجزائر، كلية الحقوق، ٢٠١٢، ص ٥.

المتحدة الأمريكية تبين أن معدل الأرباح التي يحققها مرتكب جريمة الحاسوب وصلت إلى (٦٠٠) ألف دولار مقابل (٣٠٠) ألف دولار لمرتكب الجريمة التقليدية^{٥٧}.

• الفرع الثاني:- الطبيعة القانونية لجرائم الحاسوب.

تختلف الطبيعة القانونية للجريمة المعلوماتية (الإلكترونية) عن الطبيعة القانونية للجريمة العادية، فالاعتداء في الجريمة المعلوماتية يكون على البيانات والمعلومات والبرامج، في حين أن الاعتداء في الجريمة التقليدية (العادية) يكون على شيء مادي محسوس. فالمعطيات التي تشكل المكون المعنوي للحاسوب غير مادية وليست محسوسة لكنها تأخذ صفة المال، لأن برامج الحاسوب ذات قيمة مالية وتختلف قيمتها حسب طبيعة البرنامج والهدف منه، فالقوانين الجنائية وضعت حماية جنائية للأموال وبالتالي هي تشمل البيانات والمعلومات والبرامج^{٥٨}.

فجهاز الحاسوب يعتبر بمثابة أداة أساسية لقيام المجرم الإلكتروني بجريمته، فتطور الحاسب الآلي أدى إلى ظهور جرائم مستحدثة لم تكن معروفة من قبل، وأصبح من اللازم معرفة كيفية التعامل معها، والجرائم المعلوماتية تشكل طبيعة خاصة تدخل ضمن نطاق اختصاص القانون الجنائي المعلوماتي، على أساس أن معظم هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميع أو إدخالها إلى الحاسب الآلي

^{٥٧} الطائي، جعفر، مرجع سابق، ص ٤١٨.
^{٥٨} القهوجي، علي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر، ١٩٩٧، ص ١٣.

المرتبط بشبكة المعلومات^{٥٩}. حيث أن لهذه الجرائم طبيعة خاصة هي قدرة شبكة الإنترنت الفريدة على نقل وتبادل المعلومات ذات الطابع شخصي والعام في آن واحد، وخير مثال على ذلك الاعتداء على خصوصية كل من يتعامل مع الحاسب الآلي وشبكة الانترنت، والسبب بذلك يكمن في توسع بنوك المعلومات بأنواعها، نضف إلى ذلك توسع مستخدمي الحاسوب إلى ربط حواسيبهم بشبكة الانترنت^{٦٠}.

يتكون جهاز الحاسوب من عنصرين أساسيين وهما، عنصر مادي ويتمثل في الأثر الخارجي الملموس (كالشاشة، والطابعة، والفأرة، ولوحة المفاتيح)، والعنصر الثاني وهو المعنوي والمتمثل في البيانات من مخرجات ومدخلات والمعلومات والبرامج وهي ذات طبيعة غير ملموسة^{٦١}. فالعنصر المادي يخضع للمفهوم التقليدي والمتمثل في الحماية الجنائية التي بينها قانون العقوبات، بينما العنصر المعنوي والمتمثل في البيانات والبرامج فتأخذ صفة المال من خلال التعامل بها، فمثلاً السرقة في الجريمة التقليدية (العادية) تكون من خلال أخذ المال من صاحبه دون رضاه وهو ما يترتب عليه نقل الحيازة من شخص لآخر فهي تخضع بالتالي لقانون العقوبات، كذلك الأمر بالنسبة لسرقة البيانات والمعلومات المخزنة على الحاسوب فهي تتم دون رضاه صاحبها وهو ما يجعلها بنظرنا خاضعة أيضاً لقانون العقوبات^{٦٢}.

^{٥٩} الزعبي، علي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس، لبنان، ٢٠٠٦، ص ٢٤٩.

^{٦٠} عيسى، طوني، التنظيم القانوني لشبكة الانترنت، ط ١، دار صادر للمنشورات الحقوقية، بيروت، لبنان، ٢٠٠١، ص ٣٧٣.

^{٦١} عفيفي، عفيفي، جرائم الكمبيوتر، (د.ن)، القاهرة، مصر، ٢٠٠٠، ص ١١٠.

^{٦٢} شمس الدين، أشرف توفيق، الحماية الجنائية للمستند الإلكتروني (دراسة مقارنة)، ط ١، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ٢٠٠٦، ص ٣١.

وإذا نظرنا للقرار بقانون والمتعلق بالجرائم الإلكترونية الفلسطينية رقم (١٠) لسنة (٢٠١٨) نجد بأنه نص في بعض نصوصه على سرقة البيانات والأموال من خلال شبكة الانترنت وعاقب على تلك الأفعال الإجرامية فمثلاً المادة (١٣) نصت على أنه:- " كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكتا العقوبتين " والمادة (١٤) من نفس القانون نصت على أنه:- " كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكتا العقوبتين".

إذا نخلص للقول بأن الطبيعة القانونية لجرائم الحاسوب هي ذات طبيعة خاصة من حيث تكييفها القانوني، فالقوانين التقليدية (العادية) هي غير مخصصة لهذه الظواهر الاجرامية المستحدثة التي ظهرت مع التقدم والتطور التكنولوجي والتقني، فالنصوص التقليدية وضعت وفقاً لمعايير معينة، وبالتالي من الضروري إيجاد قوانين تتلائم مع هذا التطور وتبين الجرائم المعلوماتية والعقوبات التي تتوافق معها.

• الفرع الثالث:- خصائص الحاسوب

لقد أدى انتشار الحواسيب بشكل كبير وسريع، إلى دخولها في مختلف مجالات الحياة حيث أصبحت من العناصر الأساسية للإنسان، وبالتالي القيام بالعديد من العمليات والوظائف، وهي بذلك وفرت الوقت الكافي على الإنسان وسهلت عليه الكثير من الأمور، فلا وجود لمجتمع متطور وقوي إذا لم يكن لديه الخبرة والقدرة على التعامل مع الحاسوب، ويتبين لنا بناءً على ذلك بأن جهاز الحاسوب يتميز بالعديد من الخصائص التي تميزه وتفضله على أجهزة التكنولوجيا المختلفة. حيث أن من أهم خصائص الحاسب الآلي ما يلي:-

أولاً_ السرعة.

يتصف جهاز الحاسوب بالسرعة العالية، وهو ما جعله كثير الاستخدام في الوقت الحالي، إذ ينفذ العديد من العمليات الحساب والمنطقية المختلفة بسرعة فائقة جداً، ويكمن السبب في ذلك إلى تطور التكنولوجيا المستخدمة فيه ونوعية البرامج التشغيلية التي تعمل داخل جهاز الحاسوب، فسرعة البرامج التي يتم إنتاجها أثر كبير في ازدياد نقل المعلومات والبيانات ومعالجتها وتداولها بشكل كبير، وللسرعة ميزة في كسب رضى مستخدمي الحواسيب وازدياد الإقبال عليها.

ثانياً_ الدقة.

يمتاز جهاز الحاسوب بالدقة العالية، والقدرة على العمل لفترات طويلة دون أن يصاب بملل إذا ما قورنَ بالإنسان الذي يمل إذا عمل لفترات طويلة متواصلة^{٦٣}، تتعلق الدقة بجودة المهام

٦٣ خاطر، منتصر عبدالله، وآخرون، الحاسوب، مقرر تأسيسي لجامعة القدس المفتوحة، دون ناشر، ٢٠٠٨، ص١٧.

وحسن تطبيق الجهاز لما يعطيه من أوامر، ومن أجل تحقيق فعالية الدقة وتطويرها تعتبر البرامج التطبيقية الوسيلة الأكثر فعالية للحصول على دقة ذات أثر ونتيجة يمكن الاعتماد عليها في المهام الخاصة^{٦٤}.

ثالثاً_ قدرة التخزين.

لجهاز الحاسوب قدرة تخزينية فائقة، حيث باستطاعته استيعاب وتخزين البيانات والبرامج في الذاكرة الرئيسية بصورة مؤقتة في أثناء تنفيذ البرامج، وله القدرة على إمكانية إعادة استرجاعها وتحويلها إلى قوالب وإشارات مفهومة سواء كانت كتابية أو رقمية أو سمعية، فيعتبر الحاسوب من أهم الابتكارات التي أوجدها الإنسان على وجه الأرض^{٦٥}.

رابعاً_ سهولة الاستعمال.

يمتاز جهاز الحاسوب بسهولة استعماله من قبل المستخدم دون الحاجة إلى مختصين للعمل على جهاز الحاسوب، حيث أدى وجود البرامج التطبيقية والتشغيلية إلى تسهيل عمل الحاسوب وسهولة التعامل معه حيث أدى ذلك إلى انتشاره بشكل كبير وواسع بالمجتمعات والفئات العمرية المختلفة كافة، ومن خلال كبسة زر واحدة قد يحقق الإنسان النتيجة التي يرغب في تحقيقها.

٦٤ المناعسة، أسامة، الزعبي، جلال، مرجع سابق، ص ٣٢.

٦٥ المرجع نفسه، ص ٣٢+٣٣.

خامساً_ القدرة على الاتصال والتواصل.

بفضل وسائل الاتصال الحديثة والمتطورة، أصبح من الممكن وليس من الصعب أن يتم الاتصال والتواصل بين جهاز الحاسوب وآخر وأن يتم تبادل المعلومات والبيانات فيما بينهما دون وجود أي صعوبات^{٦٦}.

سادساً_ مواكبة التطور التكنولوجي.

يتميز جهاز الحاسوب بمواكبته للتطور التكنولوجي وموافقته للتطورات العلمية والتكنولوجية التي تهدف إلى تقدم البشرية وخدمتها.

المطلب الثاني

مكونات الحاسوب الآلي وذاتية جرائمه.

يتكون جهاز الحاسوب (الحاسب الآلي) من أجزاء محسوسة ولموسة، ومن أجزاء غير محسوسة وغير ملموسة، سوف يتم الحديث عن كل منهما بشكل منفرد (مكونات مادية واخرى معنوية).

^{٦٦} الفيومي، محمد، مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، المكتب الجامعي الحديث للنشر والتوزيع، الإسكندرية، مصر، ١٩٩٨، ص٦+٧.

المعدات:- وهي الأجزاء المحسوسة والملموسة التي يلمسها ويراهما الشخص المستخدم للحاسوب في الحاسب الآلي، وهي الأجزاء التي تجعل الحاسوب قادراً على القيام بعمله وأداء الواجبات وذلك عند إعطائه الأوامر لكي يقوم بتنفيذها وتحقيق النتيجة المطلوبة.

وحدات الإدخال:- وهي الوحدات المسؤولة عن إدخال المعلومات والبيانات إلى الحاسوب^{٦٧}، وذلك من أجل التمهيد للقيام بالمهام المعطاة له، ومن هذه الوحدات، لوحة المفاتيح ويطلق عليه باللغة الإنجليزية مصطلح (Keyboard) وتستخدم هذا اللوحة من أجل إدخال وكتابة الأوامر على شكل نصوص، ومن هذه الوحدات أيضاً الفأرة ويطلق عليها باللغة الإنجليزية مصطلح (Mouse) وتستخدم من خلال النقر أو التأشير على واجهة الحاسوب، وكذلك من وحدات الإدخال "الماسح الضوئي" ويطلق عليه باللغة الانجليزية (Scanner) والذي يقوم بإدخال الصور والملفات إلى الحاسوب كما هي في طبيعتها^{٦٨}، ومن وحدات الإدخال الأخرى للحاسوب المايكروفون والكاميرا والقلم الضوئي وغيرها من الوحدات التي قد يتوصل إليها العلم بهدف تغذية الحاسب الآلي بالبيانات والمعلومات كافة^{٦٩}.

^{٦٧} العزة، فراس، وآخرون، مهارات الحاسوب والبرمجيات الجاهزة التطبيقات البرمجية والاستخدامات العملية، ط١، دار اليازوري للنشر والتوزيع، عمان، الأردن، ٢٠٠٣، ص ١٤.
^{٦٨} المسند، صالح، مرجع سابق، ص ١٦٠_١٦١.
^{٦٩} المناعسة، أسامة، الزعبي، جلال، مرجع سابق، ص ٢٩.

وحدات المعالجة أو التشغيل:- تعتبر المحرك المتحكم بالحاسب الآلي وفيها يتم معالجة

المدخلات وإنتاج معلومات^{٧٠} ويسمى أيضاً بعقل الحاسوب^{٧١} ومن هذه الوحدات:-

وحدة التحكم:- وهي الوحدة التي يتم من خلالها التحكم في جميع البيانات والمعلومات من

خلال أجهزة تحكم معينة، وتعمل على تنظيم علاقة وحدة المعالجة المركزية مع الوحدات

الآخري من أجل استلام البيانات وإرسال النتائج بعد المعالجة^{٧٢}.

وحدة الحساب والمنطق:- وهي الوحدة التي تكون مسؤولة عن جميع العمليات الحسابية

التي تتم داخل الحاسب الآلي، وتتكون من مجموعة من الدوائر الحسابية والمنطقية ومجموعة

من المسجلات اللازمة لتنفيذ العمليات المطلوبة^{٧٣}.

وحدة التخزين أو الذاكرة الرئيسية:- وهي التي تستخدم من أجل حفظ وتخزين المعلومات

والبيانات داخل الحاسب الآلي^{٧٤}. والذاكرة قد تكون ذاكرة القراءة والكتابة فقط ونسميها بالذاكرة

العشوائية أو الرئيسية وهذه الذاكرة قابلة للتعديل والحذف والإضافة وذاكرة القراءة فقط التي

٧٠. عمار، زكريا، حماية الشبكات الرئيسية من الاختراق والبرامج الضارة (رسالة ماجستير غير منشورة)، جامعة النيلين، كلية الدراسات العليا، السودان، ٢٠١١، ص ٢١.

٧١. عبدالله، محمود، مرجع سابق، ص ١٨.

٧٢. العزة، فراس، مرجع سابق، ص ١٤.

٧٣. فكيرين، محمد، أساسيات الحاسب الآلي، دار الراتب الجامعية للنشر والتوزيع، بيروت، لبنان، ١٩٩٣، ص ٥١.

٧٤. المسند، صالح، مرجع سابق، ص ١٦١.

تستخدم للقراءة فقط ولا تضيع البيانات المخزنة بإنقطاع التيار الكهربائي^{٧٥}، ووحدة التخزين يمكن أن نقسمها إلى قسمين هما:-

التخزين الداخلي:- ويكون ذلك بتخزين البيانات والمعلومات داخل جهاز الحاسوب وله صورتان:- الأولى ويطلق عليها الحفظ الدائم بحيث يتم تخزين المعلومات والبيانات داخل الحاسوب بصورة دائمة وقد يكون الحفظ على القرص الصلب ويسمى (Hard Disk) أو قد يتم الحفظ على (Ram) على هيئة نبضات كهربائية، والصورة الثانية يطلق عليها بالحفظ المؤقت، وتعتمد على الذاكرة الدائمة للحاسوب ويمكن حذفها وإلغاؤها بمجرد إنقطاع التيار الكهربائي عن الجهاز.

التخزين الخارجي:- يختلف عن التخزين الداخلي في الوسيلة، فأدوات التخزين منفصلة عن جهاز الحاسب الآلي مثل القرص المرن والإسطوانات^{٧٦}.

وحدات الإخراج:- وهي الوحدة التي تكون مسؤولة عن إظهار ما يحتاجه المستخدم للتفاعل مع الحاسوب وإيصال نتائج المعالجة للمستخدم^{٧٧}، ويتم فيها إخراج البيانات والمعلومات ألياً داخل الحاسب الآلي، ومن أجهزة الإخراج الشاشة والتي من خلالها يستطيع الشخص مشاهدة ما يقوم به، والطابعة التي يتم من خلالها طباعة النصوص التي كتبت على جهاز الحاسوب والسماعة التي تقوم بإخراج الأصوات بشكل يمكن سماعه.

^{٧٥} عبدالله، محمود، مرجع سابق، ص ١٨+١٩. كذلك. أنظر: طوالبه، علي، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث للنشر والتوزيع، إربد، عمان، ٢٠٠٤، ص ١٨.

^{٧٦} المناعسة، أسامة، الزعبي، جلال، مرجع سابق، ص ٣٠.

^{٧٧} القاضي، زياد، الكمبيوتر وتطبيقاته، دار المستقبل للنشر والتوزيع، عمان، الأردن، ١٩٩٠، ص ٦٢.

البرمجيات:- وهي الكيان المنطقي للحاسوب وتتمثل في مجموعة التعليمات التي تهدف إلى إنجاز أعمال بواسطة نظام لمعالجة المعلومات يدعى الحاسوب بالإضافة للتوثيق الملحق به وأدواته التحضيرية^{٧٨}. وهي تلك البرامج التي لا يمكن لمسها ورؤيتها، لأنها غير مرئية، وهي المكمل الأساسي للمعدات حيث أنه لا قيمة للمعدات دون البرمجيات، فهي التي تشرف على المعدات وتكمله ومن خلالها يتم إدارة الحاسوب والبرمجيات نوعان: برامج التشغيل، وبرامج التطبيق فبرامج التشغيل هي التي تعتمد عليها برامج الحاسب الآلي وذلك لاحتوائها على آليات العمل والتشغيل، وبرامج التطبيق هي تلك التي تعمل من خلال القيام بوظائف معينة تخدم من خلالها الإنسان الذي يستخدم تلك البرامج من أجل الوصول إلى تحقيق هدف معين، ويسمى مصطلح المبرمج على ذلك الشخص الذي يقوم بتصميم البرنامج^{٧٩}، وتعرف البرمجيات بأنها مجموعة البرامج والأساليب والقواعد المتعلقة بتشغيل وحدة معالجة البيانات^{٨٠}.

المبحث الثاني

الجانب الفني والتقني لشبكة الإنترنت

لا يخفى على أحد أن شبكة الإنترنت أو ما تسمى بالشبكة (العنكبوتية)، تعتبر من أهم الإنجازات التي أوجدها الإنسان ضمن التطور التكنولوجي والتقني الذي شهده العالم في القرن

^{٧٨} بن يونس، عمر، الجرائم الناشئة عن استخدام الانترنت، أطروحة دكتوراه منشورة في القانون الجنائي، كلية الحقوق، جامعة عين شمس، ٢٠٠٤، ص٥٨.

^{٧٩} حسين، عبد الرحمن، الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة (رسالة ماجستير غير منشورة)، جامعة النجاح الوطنية، كلية الدراسات العليا، نابلس، ٢٠٠٨، ص٩.

^{٨٠} الحسيناوي، علي، مرجع سابق، ص٢٥.

العشرين. ولا شك في أن انتشار الشبكة بسرعة هائلة وما تتصف به بسهولة الاستخدام والتعامل معها ليصبح استخدامها في مجالات عسكرية واقتصادية وسياسية وتعليمية واجتماعية غيرها من المجالات.

وتعد شبكة الإنترنت إحدى وسائل الاتصال بين البشر، فهي تحتل المرتبة الثانية من حيث عدد المستخدمين لها بعد الهاتف الخليوي أو يمكن أن نطلق عليه مصطلح (الموبايل) ففي عام ٢٠١٢ تجاوز عدد مستخدمي الإنترنت ملياري مستخدم حول العالم، وتزايد عدد مستخدمي الهاتف الخليوي (الموبايل) لخمس مليارات نسمة، وكانت هذه الإحصائية بناءً على موقع Internet World Stats^{٨١}.

وهنا نركز في هذا المبحث على الجانب الفني والتقني للإنترنت، دون الدخول في تفاصيلها بشكل واسع، حيث يقتصر هذا المبحث على ما يلي:-

- **المطلب الأول:- ما هية الإنترنت.**
- **المطلب الثاني:- الإنترنت إيجابياته وسلبياته.**

المطلب الأول

ماهية الإنترنت.

لم يرَ العالم في العصر الحديث تطوراً مثلما حدث مع تطور الشبكة العنكبوتية، وهناك طريقتان لكي يستطيع مستخدمو الحواسيب من الاتصال بالإنترنت، فيكون عادةً إما عن طريق

٨١ موقع إحصائيات الإنترنت العالمية، <https://www.internetworldstats.com>، تاريخ الدخول (٢٠١٨\٥\٢٩)

الاتصال الهاتفي الأرضي بمزود خدمة الإنترنت (ISP_Internet Service Provider) عبر جهاز مودم، وهناك طريقة أخرى يمكن من خلالها الوصول إلى الإنترنت، وذلك عن طريق ربط خط مؤجر، ونقصد به وسيلة اتصال رقمية بين موقعين (عادة بين عميل يريد الاتصال بالإنترنت و مقدم الخدمة ISP) و ليس له رقم كالتليفون العادي، وهي متعددة الاستخدامات (تليفون، بيانات، انترنت) ٨٢،

ويستخدم هذه الطريقة المؤسسات أو الشركات الكبيرة التي تمتلك عقدة Node خاصة بها على الإنترنت أو تكون مرتبطة بخدمة مزود الإنترنت^{٨٣} ويعتبر الإنترنت جزءاً من ثورة الاتصالات، ويعرف البعض الإنترنت بأنه شبكة من الشبكات في حين يعرفها بعضهم بأنها شبكة طرق المواصلات السريعة^{٨٤}

لقد تطورت هذه الشبكة ليصل ربع سكان العالم ممن يستخدمها^{٨٥}، ولم تعد ملكاً لأحد كما كانت في بداية تأسيسها من قبل وزارة الدفاع الأمريكية، ففي الوقت الحاضر أصبحت للجميع ولا يملكها أحد، فانتهى مصطلح التملك وتحولت إلى شبكة مجتمعية يستخدمها الجميع دون أن تكون حكراً لأحد ويرجع السبب في ذلك إلى بساطتها وسهولة العمل فيها.

٨٢ الخطوط المؤجرة، موقع فودافون، -<https://www.vodafone.qa/ar/internet/enterprise-internet-services/leased-lines>، تاريخ الدخول (٢٠١٨/١١/٢٥).

٨٣ سقف الحيط، عادل، مرجع سابق، ص ٥٣.

٨٤ سارة، عياط، جريمة القذف على شبكة الإنترنت، مذكرة ماستر غير منشورة، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٤، ص ٨.

٨٥ مصطفى، سمير، وآخرون، الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها بحث غير منشور، ص ٢.

ويتبين لنا بأن شبكة الإنترنت تتمتع برواج وانتشار كبيرين يعكس نظيراتها من وسائل الاتصال المختلفة، فقد أدى انتشار الشبكة بشكل سريع إلى ظهور الآثار السلبية لها كونها أصبحت مكاناً ملائماً ووسيلة يستخدمها مخترقو الحواسيب من أجل ارتكاب الجرائم الإلكترونية وبالتالي الوصول للخصوصيات والبيانات الخاصة بالمستخدمين بكل سهولة وبطريقة غير مشروعة، وقد أطلق على هذه الجرائم في مؤتمر جرائم الإنترنت المنعقد بأستراليا في الفترة الواقعة من (١٦-١٧ فبراير ١٩٩٨) مصطلح (جرائم الإنترنت Crimes Internet)^{٨٦}.

لهذا قمنا بتقسيم هذا المطلب إلى فرعين، حيث تناولنا في الفرع الأول تعريف شبكة الإنترنت، وفي الفرع الثاني الإنترنت إيجابياته وسلبياته.

الفرع الأول:- تعريف شبكة الإنترنت. هي شبكة عالمية وهي اختصار (Network International)، وهو اسم بديل عن شبكة (ARRANET)، ويقصد الإنترنت بذلك مجموعة لا متناهية من الحواسيب الآلية المرتبطة معاً بوسيلة إلكترونية عبر العالم من أجل تبادل البيانات والمعلومات بأشكالها المختلفة^{٨٧}.

ويمكن أن يطلق عليها أيضاً بأنها مجموعة من الأجهزة المرتبطة مع بعضها البعض بواسطة كوابل أو قد يكون اتصالاً لا سلكياً من أجل نقل المعلومات فيما بينها على أساس

٨٦ بحر، عبدالرحمن، معوقات التحقيق في جرائم الإنترنت دراسة مسحية على ضباط الشرطة في دولة البحرين، أكاديمية نايف العربية للعلوم الأمنية، رسالة ماجستير غير منشورة معهد الدراسات العليا، ١٩٩٩، ص ٢.

٨٧ المناعسة، أسامة، الزعبي، جلال، مرجع سابق، ص ٣٦.

بروتوكول عمل^{٨٨}، ويمكن أن نعرف الشبكة بأنها مجموعة من الأنظمة المعلوماتية تهدف إلى الوصول إلى البيانات وبالتالي الحصول على المعلومات.

ولم يغفل المشرع الفلسطيني عن ذكر تعريف للشبكة الإلكترونية فقد أورد تعريفها في المادة (١) من قرار بقانون الخاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨) حيث عرفها بأنها: - " ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت)^{٨٩}، وعند قراءة نصوص مواد هذا القرار نجد بأن أغلبها تتحدث عن كل من يقوم بإساءة استخدام الشبكة الإلكترونية، وذلك من أجل تحقيق الهدف من هذه الإساءة، وهو الوصول إلى النتيجة الجرمية، ويتبين لنا أيضاً من نصوص المواد بأن الشبكة الإلكترونية هي أداة سهلت في ارتكاب الجريمة، وأصبح باستطاعة المخترقين الوصول للبيانات بدون مشقة ولعدم وجود رقابة من قبل الأجهزة المختصة أيضاً على هذه الشبكة أصبح بالسهولة ارتكاب الجريمة ودون أن يكون هناك أي أثر لمرتكب الجريمة الإلكترونية.

والإنترنت أيضاً شبكة عالمية تربط آلاف الشبكات وملايين أجهزة الكمبيوتر المختلفة في العالم، وتظهر أهمية الإنترنت في كونها وسيلة يستخدمها الأفراد والمؤسسات من أجل التواصل وتبادل المعلومات^{٩٠}.

لهذا قمنا بتقسيم هذا الفرع إلى فترتين الأولى الإنترنت لغةً والثانية الإنترنت اصطلاحاً.

٨٨ خاطر، منتصر عبدالله، مرجع سابق، ص ٥٠٦.

٨٩ أنظر المادة (١)، قرار بقانون الخاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨م).

٩٠ سارة، عياط، مرجع سابق، ص ٨.

• الفقرة الأولى: الإنترنت لغةً.

الإنترنت لغةً كما وردت في معجم اللغة العربية المعاصرة: - شبكة معلومات عالمية تهدف إلى ربط العالم وجعله كقرية صغيرة، ويمكن الدخول إليها من خلال جهاز الحاسوب "انتشرت الأخبار سريعاً عبر الإنترنت"^{٩١}.

والإنترنت لغةً أيضاً هي كلمة جديدة في القاموس اللغوي لمختلف لغات العالم وهي كلمة انجليزية ومختصرة من مقطعين Inter وهي اختصار لمصطلح International وتعني دولي وNet تعني شبكة وهي اختصار Network وعند جمع الكلمتين مع بعضهما International Network تصبح معناها الشبكة الدولية^{٩٢}.

• الفقرة الثانية: الإنترنت اصطلاحاً.

ويمكن أن نطلق على الإنترنت بأنه نظام عالمي يعمل على دمج شبكات الحواسيب المتصلة به مع بعضها البعض، ويتم مبادلة المعلومات والبيانات بين تلك الحواسيب وشبكات الحاسوب من خلال بروتوكولات خاصة بها، ويمكن أن نقول عنها بأنها عبارة عن خطوط اتصال تلف الكرة الأرضية وتحقق الاتصال بين الملايين من أجهزة الحاسب الآلي.

يقول العالمان الأمريكيان جلي هاري (GLEE HARA) وزميله بات ماكروجر (PAT MCREGALR) بأنه لا يوجد تعريف محدد للإنترنت فقد عرّفها بعدة تعريفات نذكر بعضها:-

٩١ عمر، أحمد مختار، معجم اللغة العربية المعاصرة، عالم الكتب، مج ١، ط ١، ٢٠٠٨، ص ١٢٧.
٩٢ فتحية، رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت مذكرة ماستر غير منشورة، جامعة أبي بكر بلقايد، تلمسان، الجزائر، ٢٠١٢، ص ٧+٨.

أنها مجموع من الحواسيب الآلية تتحدث عبر الألياف الضوئية وخطوط التليفون ومحطات الأقمار الصناعية.

✓ هي مئات المكتبات والأرشيف التي تفتح بمجرد أن تلمسها.

✓ هي تكنولوجيا المستقبل التي ستجعل حياتنا وحياء الأجيال اللاحقة أكثر إشراقاً.

✓ هي فرص تجارية غير محدودة.

وغيرها من التعريفات الأخرى التي ذكرها المذكوران أعلاه^{٩٣}.

والإنترنت أيضاً هو مجموعة من الأجهزة الحاسوبية متصلة ببعضها البعض، وهذه الأجهزة

تتخاطب باستخدام لغة معينة مثلنا بني البشر، إلا أن هذه اللغة تسمى بروتوكولات^{٩٤}.

وهي أيضاً عبارة عن شبكة عالمية، وهذه الشبكة العالمية تعود ملكية معظم أجهزتها إلى

شركات وجامعات ودوائر حكومية، إضافة إلى أشخاص متحمسين يمتلكون حواسيب شخصية

موصولة على الإنترنت^{٩٥}.

ويمكن أن نطلق على شبكة الإنترنت بأنها بنك للمعلومات، فمن خلال الدخول لهذه الشبكة

ويربطها بجهاز الحاسوب عبر بروتوكولات خاصة يستطيع مستخدم تلك الشبكة أن يصل للكثير

من المعلومات والبيانات.

٩٣ سارة، عياط، مرجع سابق، ص ٩.

٩٤ الحربي، خالد، الأمن والحماية في الإنترنت، ط ١، دار الفلاح للنشر والتوزيع، الرياض، السعودية، ٢٠٠٦، ص ١٨.

٩٥ الخوري، هاني، تكنولوجيا المعلومات على أعتاب القرن الحادي والعشرين، ج ١، دار السلام للنشر والتوزيع، مصر، ١٩٩٨، ص ١٠٥.

كلمة الإنترنت (Internet) تعني شبكة تتكون من مجموعة شبكات وهي اختصار لـ (Interconnected network) وتعتبر شبكة الإنترنت شبكة عملاقة مكونة من مجموعات من شبكات الحاسب المرتبطة ببعضها البعض على نطاق عالمي^{٩٦}

يشير المجلس الفيدرالي الأمريكي لشبكات الحاسوب The Federal Networking Council إلى أن مصطلح الإنترنت هو:-

✓ مرتبط علمياً بعنوان مميز مبني على مواصفات خاصة بالإنترنت والأنظمة المشتقة منه والمتفرعة عنه.

✓ يمكن من خلاله دعم الاتصالات عن طريق استخدام مواصفات النظام أو مواصفات أخرى مطابقة.

✓ يوفّر ويستخدم أو يسمح باستخدام خدمات عالية في مجال الاتصالات بوساطة القطاع الخاص أو العام^{٩٧}.

يتبين لنا من هذا التعريف بأن الإنترنت شامل لكافة الجوانب المتعلقة بشبكة الإنترنت من حيث المقومات والخدمات المقدمة منه، لكن تكمن صعوبة في فهم بعض المصطلحات العلمية بسبب غموض تلك المصطلحات لغير المختصين في مجال الحاسوب، إلا أن هناك تعريفاً سهلاً وهو أن الشبكة عبارة عن مجموعة من الشبكات المرتبطة مع بعضها البعض عن طريق أجهزة الحاسوب التي تقوم بتبادل المعلومات وإرسالها للطرف الآخر.

٩٦ خاطر، منتصر عبدالله، مرجع سابق، ص ٥٠٧.
٩٧ السرحاني، محمد، مرجع سابق، ص ٨.

ويمكن تعريف الشبكة المعلوماتية بأنها ارتباط أكثر من نظام معلومات للحصول على المعلومات والبيانات وتبادلها^{٩٨}.

ومما لا شك فيه بأنه لا يوجد تعريف واضح ومحدد لشبكة الإنترنت، حيث ظهرت اجتهادات فقهية وقضائية من أجل محاولة وضع تعريف واضح ودقيق لشبكة الإنترنت سنورد لكم بعض هذه التعريفات الفقهية والقضائية.

❖ المحاولات الفقهية لوضع تعريف لشبكة الإنترنت.

يرى هذا الاتجاه بأن شبكة الإنترنت هي شبكة تسمح بانتظام شبكات معلوماتية مختلفة إليها عن طريق استخدام بروتوكول TCP/IP، والبريد الإلكتروني e-mail، ومجموعات الأخبار News groups، والصفحات FTP، وبنوك المعلومات les banques de donnees .^{٩٩}

ويرى هذا الاتجاه أن الإنترنت ظاهرة تقنية وفنية، لها صفات تميزها من حيث عدم ملكيتها لأحد في العالم، بالإضافة إلى أنها مفتوحة للجميع فهي مجال ليس لأحد سلطان عليه، ومن خلالها نستطيع فعل ما نريد، ومن هنا تظهر لنا سلبيات تلك الشبكة من خلال عدم وجود رقابة من قبل الأجهزة المختصة عليها، حيث أصبح باستطاعة المخترقين والمحترفين القيام بكل أعمالهم بدون أن يكون هناك أي حسيب أو رقيب عليهم، ولكن مع التطور التكنولوجي الكبير

٩٨ العجمي، عبدالله، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، ٢٠١٤، ص٦.
٩٩ فتحية، رصاع، مرجع سابق، ص٩.

أصبحت أغلب دول العالم تعمل على إيجاد القوانين الخاصة بمكافحة الجريمة الإلكترونية من أجل وقف هذا النزيف ولأن الجرائم الإلكترونية تكلف الدول ملايين الدولارات.

وقد عرفها البعض الآخر من الناحية التقنية أيضاً كما ورد في موقع ويكيبيديا الموسوعة الحرة بأنها: "شبكة عالمية من الحواسيب التي تعتمد على بروتوكول TCP/IP، والبروتوكولات الأخرى للاتصالات فائقة السرعة بين الآلاف من النقاط والملايين من المستخدمين"^{١٠٠}.

ويرى البعض بأن شبكة الإنترنت هي شبكة المعلومات الدولية أو كما أشرنا سابقاً بأنها بنك المعلومات الدولية المتصلة بمراكز الحاسوب ومراكز البحث العلمي، ومن خلالها يتمكن المشتركين بشبكة الإنترنت من الوصول إلى المعلومات وذلك عن طريق الاشتراك بشبكة الإنترنت من خلال بريد إلكتروني وكلمة سرية مخصصة لكل مشترك.

كما عرفها أحد الاساتذة بجامعة "بركلي" بالولايات المتحدة الأمريكية بأنها: "شبكة الشبكات"^{١٠١}. نجد أن أغلب المحاولات الفقهية وضحت الجانب الفني لشبكة الإنترنت ووضحت طريقة مل تلك الشبكة، في حين أن جانباً آخر ذهب إلى محاولة إيضاح الجانب التقني لشبكة الإنترنت وذلك بتبيان أسلوب الاتصال والأدوات المستخدمة في الاتصال بالشبكة من خلال بروتوكولات التي ذكرناها سابقاً (TCP/IP). وتكمن وظيفة البروتوكول في أنه يهتم بأمور شبكة الاتصال حتى يؤمن التواصل بين الموقع والمستخدم عبر الشبكة"^{١٠٢}.

<https://ar.wikipedia.org/wiki> ١٠٠

١٠١ فتحية، رصاع، مرجع سابق، ص ١٠٠.

١٠٢ أغلال، الزهراء بوكرمة، مقال عن الشبكة العنكبوتية العالمية وسيلة للتعلم الذاتي وتطوير البحث العلمي، مجلة العلوم الإنسانية والاجتماعية، عدد خاص الحاسوب وتكنولوجيا المعلومات في التعليم العالي، الجزائر، ٢٠١١، ص ٢٤٢.

❖ المحاولات القضائية لوضع تعريف لشبكة الإنترنت.

لقد ذهبت أغلب المحاكم إلى وضع أحكام خاصة بشبكة الإنترنت، وذلك بتبيان وظائف تلك الشبكة وتبيان جانبها التقني والفني. ووصفت المحكمة العليا في الولايات المتحدة الأمريكية، وهي أعلى هيئة قضائية هناك شبكة الإنترنت بأنها: "شبكة دولية من الحواسيب المرتبطة والمتصلة وتعد أهم وسائل الاتصال الحديثة ولا يوجد لها أي حدود إقليمية"^{١٠٣}.

كذلك ذهبت المحكمة الابتدائية لشرق ولاية فرجينيا إلى تعريف شبكة الإنترنت بأنها: "الطريق الدولي للمعلومات، فهي عبارة عن شبكة اتصالات معقدة يرتبط بها مجموعة من شبكات الحاسوب العامة والخاصة، سواء أكانت أنظمة أم أفراد وهي تتكون من حاسبات وقواعد بياناتها متصلة من خلال خطوط هاتف"^{١٠٤}.

وضمن المحاولات الدولية من أجل وضع تعريف لشبكة الإنترنت نرى أن الاتفاقية الأوروبية الافتراضية المنعقدة في بودابست بتاريخ (٢٠٠١/١١/٢٣) قد وضعت تعريف للإنترنت بأنها شبكة عالمية تتكون من العديد من الشبكات المتصلة، والجميع يستخدم ذات البروتوكول"^{١٠٥}.

بعد الإطلاع على هذه الاتفاقية نجد بأنها جاءت من أجل تنظيم شبكات الكمبيوتر والاتصال، ومن أجل ردع الأعمال الإجرامية التي قد تقع من خلال شبكة الإنترنت، والصادرة عن إساءة استخدام هذه الشبكات والبيانات وتجرى هذا الفعل (السلوك) يكون من خلال معاقبة كل من يقوم بارتكاب جرائم إلكترونية، عن طريق الكشف والتحقيق والملاحقة القضائية على

١٠٣ فتحية، رصاع، مرجع سابق، ص ١١.

١٠٤ المرجع نفسه، ص ١١.

105 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

المستويين المحلي والدولي، وأن يكون هناك تعاون دولي في ملاحقة مرتكبي الجرائم الإلكترونية.

نرى أن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين، وضع تعريفاً جامعاً لجرائم الانترنت وشبكاتة حيث عرف جريمة الانترنت (الجريمة المعلوماتية) بأنها: - "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتشمل هذه الجريمة من حيث المبدأ جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية". يعد هذا التعريف أفضل تعريف للجريمة المعلوماتية لأنه يشمل كلاً من الجانب المادي والجانب المعنوي للحاسب الآلي ومنها شبكة الانترنت وهنا يكون الحاسب الآلي وشبكاتة محلاً للاعتداء كما أنه وسيلة للاعتداء وارتكاب الجرائم.

ونرى هنا أن أفضل تعريف للجريمة المعلوماتية (الانترنت) إنما يتمثل "في أن هذه الجريمة هي كل اعتداء يقع على نظم الحاسب الآلي وشبكاتة أو بواسطتها" حيث نجد أن مثل هذا التعريف إنما يشمل الاعتداء على كلا من الجانب المادي للحاسب الآلي وشبكاتة المحلية والجانب المعنوي معاً، وذلك لأن نُظْم الحاسب الآلي تشمل كلاً من مكونات الحاسب المادية والمعنوية^{١٠٦}.

• الفرع الثاني:- نشأة الإنترنت.

كانت فكرة إنشاء شبكة الإنترنت من صنع الخيال، حيثُ تخيل خبراء أمريكيان يعملون في وزارة الدفاع الأمريكية من وقوع كارثة تؤدي إلى تدمير كافة البيانات والمعلومات الخاصة بين

^{١٠٦} الشوابكة، محمد، جرائم الحاسوب والانترنت الجريمة المعلوماتية، ط١، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٤، ص ١١٠.

المراكز العسكرية، فكان السؤال ما هو مصير تلك البيانات والمراكز؟ وكيف سيتم حفظها من الدمار؟.

كما هو متعارف عليه بأن الحاجة أم الاختراع أصبح لدى هؤلاء الخبراء حاجة ملحة من أجل إيجاد طريقة يتم من خلالها حفظ البيانات والمعلومات الهامة في المراكز العسكرية، فكانت نواة إنشاء شبكة الإنترنت من ذلك الخيال.

من هنا بدأت فكرة إنشاء شبكة اتصالات غير مركزية تجيب عن كل التساؤلات ويتم من خلالها التواصل مع المراكز العسكرية الأخرى وتبادل البيانات والمعلومات، فقد كانت أولى محاولات الربط بين أجهزة الحاسوب في الظهور كمشروع حكومي تُشرف عليه وزارة الدفاع الأمريكية، وذلك خلال فترة الحرب الباردة والتنافس مع الاتحاد السوفيتي السابق، قامت الإدارة الأمريكية بإنشاء وكالة مشاريع البحث المتقدم (The Advanced Research Projects Agency) في عام ١٩٥٧م، واختصارها (ARPA).

كان الهدف من هذا المشروع هو تطوير تقنية الشبكة بحيث يكون باستطاعتها الصمود أمام أي هجوم عسكري، تم تصميم شبكة (ARPA) عن طريق خاصية إعادة التوجيه الديناميكي، وتعمل هذه الطريقة على تشغيل الشبكة بشكل مستمر حتى وفي حالة انقطاع إحدى الوصلات أو تعطلها عن العمل، بحيث أنه يتم تحويل الحركة إلى وصلات^{١٠٧}.

١٠٧ عبد الجبار، عبدالله، مقال عن الإنترنت والتاريخ التطور والتطبيقات، شبكة الألوكة الثقافية، <http://www.alukah.net/culture/0/28516>، تاريخ الدخول (٢٠١٨/٦/٣).

١٠٨ نورية، العاج، استخدام الشبكة العنكبوتية (الإنترنت) في الدراسة وعلاقتها بالدفاعية للتعلم لدى المراهق من (١٢_١٤ سنة)، مذكرة ماستر غير منشورة، كلية العلوم الاجتماعية والانسانية، الجزائر، ٢٠١٣، ص ٥١.

لقد واجهت شبكة أربانت (ARPA) مشاكل عديدة، بسبب اقبال الجامعات عليها بشكل كبير جداً مما أدى ذلك إلى ازدحام تلك الشبكة ووجود مشاكل عديدة كالبطء وصعوبة إدارة تلك الشبكة، بعد ذلك انقسمت الشبكة إلى جزئيين (MILNET) وهو مختص بالمواقع العسكرية و(ARPANET) وهو مختص بالمجالات الأخرى غير العسكرية^{١٠٩}. لهذا سوف نقوم بالتتابع التدريجي والتاريخي لتأسيس شبكة الإنترنت.

فترة الخمسينات.

في أواخر الخمسينات، وكما هو معلوم بالحرب الباردة بين الإتحاد السوفيتي السابق والولايات المتحدة الأمريكية وضمن حالة التنافس والصراع والتوتر الذي كان يسود تلك الفترة، قام الإتحاد السوفيتي عام ١٩٥٧ بإطلاق أول قمر صناعي حمل اسم (Suptnik١) سبوتنيك ١، وتعني بالروسية صاحب^{١١٠}، ردت الولايات المتحدة الأمريكية على إطلاق القمر الصناعي بإنشاء وكالة مشروع الأبحاث المتطورة (Advanced Research Projects Agency) واختصارها (ARPA) وكانت بتمويل من وزارة الدفاع الأمريكية^{١١١}.

فترة الستينات.

كما هو معروف سابقاً بأن الحاسوب كان كبيراً، ويقوم كل حاسوب بعمل عمليات حسابية معقدة وكل واحد يقوم بعمل عملية واحدة، كانت الفكرة تقوم على ربط مجموعة حواسيب

١٠٩ بوهلال، أحلام، تأثير استخدام شبكة الإنترنت على العلاقات الأسرية الجزائرية، مذكرة ماستر غير منشورة، كلية العلوم الإنسانية والاجتماعية، جامعة العربي التبسي، الجزائر، ٢٠١٦، ص ٢٣.
١١٠ لماذا سارع السوفييت لإطلاق أول قمر اصطناعي قبل ٦٠ عاماً؟، <https://arabic.rt.com/>، تاريخ الدخول (٢٠١٨/٦/١١).

١١١ نورية، العاج، مرجع سابق، ص ٥٢.

ببعضها البعض لكي تقوم جميعها بحل نفس المشكلة وأطلق على تلك النظرية باسم (TIM SHARING).

لم تكن وزارة الدفاع الأمريكية وحدها طرفاً في فكرة إنشاء شبكة الإنترنت، ففي أغسطس عام (١٩٦٢) كان أول وصف مسجل للتفاعلات الاجتماعية التي يمكن تمكينها من خلال الربط الشبكي سلسلة من المذكرات التي قام بكتابتها (J.C.R. Licklider) من معهد ماساتشوستس للتكنولوجيا، حيث قام بمناقشة مفهومه الذي سماه "بشبكة المجرة". لقد كانت فكرته تتصور مجموعة من أجهزة الكمبيوتر المترابطة عالمياً والتي من خلالها يمكن للجميع الوصول بسرعة إلى البيانات والبرامج من أي موقع كان^{١١٢}.

قامت مؤسسة راند (Rand corporation) وهي المؤسسة المسئولة عن إعداد الأفكار لمواجهة الحرب الباردة والتي كانت بين الولايات المتحدة الأمريكية والإتحاد السوفيتي، فكرة تلك المؤسسة كانت تقوم على أساس ضرورة إعداد مقترحات وبدائل من أجل استمرار الاتصال والتواصل بين سلطات الولايات المتحدة الأمريكية، وذلك في حال تعرضت الولايات المتحدة لهجوم نووي من الإتحاد السوفيتي أو في حال تعرضت لكارثة طبيعية، انتهت فكرتهم إلى إنشاء شبكة اتصال تعمل في كل الظروف وليست سلطة مركزية بمعنى أنه لن يكون عليها سلطة من قبل أي دولة في العالم^{١١٣}.

Leiner, Barry,(And Others), Brief History of the Internet,^{١١٢}
<https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f1>,
internet/ تاريخ الدخول (٢٠١٨\٦\٣)
^{١١٣} فتحية، رصاع، مرجع سابق، ص١٢.

كما أشرنا سابقاً بأن الولايات المتحدة أنشأت شبكة (ARAPNET). ثم بدأت بعد ذلك في عام (١٩٦٩) بتطويرها من أجل تحويلها لشبكة الحزم، ثم بعد ذلك قامت وكالة مشروعات البحوث المتطورة (DARPA). والتي تتبع لوزارة الدفاع الأمريكية بربط الباحثين والجامعات بمراكز الحاسب الآلي في الولايات المتحدة من إتاحة الفرصة لهم بالمشاركة في البرامج التي تقدمها الأجهزة كقواعد البيانات، ومن خلال ذلك تم ربط العديد من الشبكات التي كانت تحت التجربة والتي تستخدم حزم الراديو والأقمار الصناعية^{١١٤}.

إذا يتبين لنا بأن مشروع (ARPANER). كان الهدف منه هو مساعدة سلطات الولايات المتحدة الأمريكية وعلى رأسها الجيش الأمريكي في حال تعرضت لهجوم أو كارثة طبيعية، وذلك من خلال ربط شبكات ومراكز الحواسيب مع الجامعات ومراكز البحث العلمي من أجل استغلال الإمكانيات الحاسوبية.

فترة السبعينات

بدأت في عام (١٩٧٣) وكالة مشاريع الأبحاث الدفاعية الامريكية المتقدمة (DARPA) برنامجاً للبحث عن تقنيات الربط بين الشبكات وأنواع مختلفة منها، وكان الهدف الرئيسي هو تطوير بروتوكولات الاتصال التي تسمح لأجهزة الكمبيوتر المتصلة بالشبكة بالاتصال بشفافية عبر شبكات حزم متعددة مرتبطة ببعضها البعض وقد أطلق على هذا المشروع (انترنتنج)
Interneting project ، وكان نظام الشبكات الذي نشأ من البحث معروفاً باسم الإنترنت وقد

^{١١٤} المسند، صالح، مرجع سابق، ص ١٦٥.

كان اسم نظام البروتوكولات (TCP/IP) وهناك بروتوكولات أولية تم تطويرها: - بروتوكول التحكم في الإرسال (TCP) وبروتوكول الإنترنت (IP)^{١١٥} .

بروتوكول TCP/IP هو في الواقع عبارة عن بروتوكولين مختلفين ولكنهما يعملان معا دوما في نظام الإنترنت، ولهذا السبب فإنهما أصبحا مقبولين لأن يوصفان بأنهما وكأنهما نظام واحد^{١١٦} .

فترة الثمانينات

في تلك الفترة قررت الولايات المتحدة الأمريكية وبالتحديد وزارة الدفاع، بسبب الضعف الكبير الذي أصبح على الشبكة و بسبب ضغط الجامعات ومراكز البحث العلمي وغيرهما على الشبكة فصل الجزء العسكري من الشبكة حيث انقسمت الشبكة إلى جزئين (MILNET) وهو مختص بالمواقع العسكرية و(ARPANET) وهو مختص بالمجالات الأخرى غير العسكرية^{١١٧} .

وفي أواسط الثمانينات بدأت مؤسسة العلوم الوطنية الأمريكية NSIS في تطوير خدمة اتصالات أساسية رئيسية للإنترنت مرافقها البالغة ٤٥ ميغابايت في الثانية، وتحتل NSFNET ترتيب ١٢ مليار رزمة شهريا بين الشبكات التي تربطها (NSFNET)^{١١٨}، وهي كلمة مختصرة

^{١١٥} Kahn, Robert, Cerf, Vinton, (Study What Is The Internet and What Makes It Work), 1999, page8, <http://www.policyscience.net/cerf.pdf>

^{١١٦} عالم الكمبيوتر - ما هو الـ TCP/IP ؟، موقع ثقاف نفسك، <https://www.thaqafnafsak.com/2012/05/tcpip.html>، تاريخ الدخول (٢٠١٨\٦\٤).

^{١١٧} أحلام، بوهلال، مرجع سابق، ص ٢٤.

^{١١٨} Leiner, Barry,(And Others), Brief History of the Internet, <https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f1>، تاريخ الدخول (٢٠١٨\٦\٨).

من (National Scienc Foundation). وهذه الشبكة مختصة بالأمرور المدنية والأبحاث العلمية^{١١٩}.

فترة التسعينات

إن التطور السريع الذي حدث في بداية التسعينيات، يعود إلى قيام الحكومة الأمريكية بالسماح للشركات باستخدام الإنترنت تجارياً لأول مرة بعد أن كان استخدامها كما ذكرنا سابقاً مقصوراً فقط على القطاعات الحكومية والتعليم ومراكز الأبحاث^{١٢٠}، وتعد شركة THE WORLD COMES ONTIME أول شركة عملت على توفير خدمة الإنترنت التجارية^{١٢١}.

في عام ١٩٩٥ بدأ تواجد خدمة الانترنت في الأقطار العربية بشكل تجاري، وفي ١٩٩٦ انعقد أول معرض دولي للإنترنت^{١٢٢}، سوف يضع الباحث نبذة عن دخول الإنترنت للوطن العربي، ففي عام ١٩٩١ تعتبر تونس أول دولة عربية ترتبط بشبكة الإنترنت، وفي عام ١٩٩٢ ارتبطت الكويت بشبكة الإنترنت، وفي ١٩٩٣ الإمارات ومصر ترتبطان بالانترنت، وفي ١٩٩٤ الجزائر والمغرب والأردن ولبنان، في ١٩٩٥ ارتبطت فلسطين بالإنترنت، في ١٩٩٦ ارتبطت كل من قطر وسوريا واليمن وعمان، في ١٩٩٧ ارتبطت بشبكة الإنترنت كل من ليبيا

^{١١٩} ردمان، عبدالله، الإنترنت وتطبيقاتها الدعوية للمبتدئين، (د.ن)، (د.م)، المصدر موقع منزل الاسلام، <https://islamhouse.com/ar/books/53292/>، تاريخ الدخول (٢٠١٨/١٨)، ص ١٥.

^{١٢٠} عبد الجبار، عبدالله، مقال عن الإنترنت والتاريخ التطور والتطبيقات، شبكة الألوكة الثقافية، <http://www.alukah.net/culture/0/28516/>، تاريخ الدخول (٢٠١٨/١٣).

^{١٢١} سارة، عياط، مرجع سابق، ص ٩.

^{١٢٢} أمينة، صافة، آثار استعمال التكنولوجيات الحديثة على أفراد الأسرة الجزائرية دراسة للتأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الإنترنت على أبناء الأسرة الجزائرية نموذجاً، أطروحة دكتوراة، جامعة وهران، ٢٠١٦، ص ٣٧.

والسودان والعراق والصومال، في ١٩٩٩ ارتبطت السعودية لشبكة الإنترنت^{١٢٣}. وفي مرجع آخر يظهر بأن الإنترنت دخل للعراق في عام ٢٠٠٠^{١٢٤}.

هكذا كانت بداية التسعينات، حيث تطورت شبكة الإنترنت تطوراً كبيراً، وأصبحت تغطي رقعة واسعة من العالم، وانضم لها آلاف الشبكات، ويعود الفضل في ذلك إلى تطبيق نظام البروتوكول (TCP/IP)، وقد وصلت حينها إلى حوالي خمسة آلاف شبكة في أكثر من (٣٦) دولة، وارتبط بها أكثر من سبعة آلاف حاسوب، وأصبحت تقدم كافة الخدمات لكل شخص لديه جهاز حاسوب ومودم متصل بخط نفاذ^{١٢٥}.

لهذا سوف نتناول في هذه الفترة دخول الإنترنت للأراضي الفلسطينية المحتلة، فكما هو متعارف للجميع بأن السلطة الوطنية الفلسطينية دخلت إلى الأراضي الفلسطينية بموجب اتفاقية أوسلو عام ١٩٩٣، حيث تسلمت إدارة المدن في الضفة الغربية وقطاع غزة بدءاً من عام ١٩٩٤، كانت إسرائيل تدير الأراضي الفلسطينية المحتلة من حيث البنية التحتية للاتصالات عبر شركة إسرائيلية تدعى "بيزك"، وكانت السلطة الفلسطينية بعد دخولها للأراضي الفلسطينية مقيدة، وحتى هذه اللحظة من قبل الإسرائيليين بسبب تدخلاتهم وسيطرتهم على البنية التحتية الفلسطينية.

^{١٢٣} ردمان، عبدالله، الإنترنت وتطبيقاتها الدعوية للمتدئين، (د.ن)، (د.م)، المصدر موقع منزل الاسلام، <https://islamhouse.com/ar/books/53292>، تاريخ الدخول (٢٠١٨/٦/٨)، ص ١٧..

^{١٢٤} نورية، العاج، مرجع سابق، ص ٥٤.

^{١٢٥} أمينة، صافة، مرجع سابق، ص ٣٧.

ففي عام ١٩٩٥، أنشئت أول شركة فلسطينية توفر خدمة الإنترنت في فلسطين وقد عرفت باسم "بال نت" حيث وفرت خدمات الوصول للإنترنت والاستضافة لكل المناطق الخاضعة للسيطرة الفلسطينية^{١٢٦}.

في الوقت الحالي انتشرت شبكة الإنترنت بشكل كبير جداً، وأصبحت تغطي تقريباً ١٧٠ دولة، وتقدم خدمات عديدة^{١٢٧}، وقبل الانتقال للمطلب الثاني والذي أتحدث فيه عن سلبيات وإيجابيات الإنترنت سوف نتحدث بشكل بسيط عن الخدمات التي تقدمها شبكة الإنترنت لمستخدمي تلك الشبكة.

أولاً_ خدمة البريد الإلكتروني (E-mail).

يعتبر البريد الإلكتروني أحد أدوات الاتصال في العالم الحديث، وأصبح يعتمد عليه الكثير من الشركات والأفراد، ووظيفته استقبال وإرسال الرسائل مع أي شخص لديه بريد إلكتروني، من مميزاته أنه سهل الاستخدام، ليس له كلفة مالية لمن يقوم بإنشاء بريد إلكتروني، ويتميز أيضاً بالسرعة، وكذلك الأمر أنه لا حاجة أن يكون متصل الطرف الآخر المستقبل لرسالة البريد الإلكتروني.

^{١٢٦} تاريخ الإنترنت في فلسطين، موقع بعـال نت،
https://web.archive.org/web/20030608075650/http://www.palnet.com:80/about_us/about_us.php
(٢٠١٨\٦\٩) تاريخ الدخول
^{١٢٧} سقف الحيط، عادل، مرجع سابق، ص ٥٤.

ثانياً_ خدمة شبكة الويب (WORLD WIDE WEB).

واختصارها (WWW) وهي من أهم الخدمات التي قدمتها شبكة الإنترنت حيث تحتوي على كم هائل من المعلومات وقد تكون تلك المعلومات على شكل صورة أو صوت أو نص أو أي نوع آخر من البيانات^{١٢٨}.

ثالثاً_ خدمة نقل الملفات.

هذه الخدمة تسمح بنقل الملفات من جهاز حاسوب لآخر بحيث يكون ذلك الحاسوب بعيد إلى حاسوب المستخدم الشخصي، وتسمى هذه العملية بالتنزيل (Downloading) وقد تكون العملية عكسية بحيث تتم من الحاسوب الشخصي للمستخدم إلى حاسوب آخر، وتسمى هنا تحميل (Uploading) وتسمح هذه الخدمة كذلك بنقل الملفات من حاسوب بعيد إلى حاسوب بعيد آخر^{١٢٩}.

رابعاً_ خدمة الدردشة.

ويطلق عليها باللغة الإنجليزية مصطلح (Chat) تقوم هذه الخدمة على عملية إجراء محادثة جماعية أو فردية مع مستخدمي تلك الدردشة ومن مختلف أنحاء العالم، بحيث أنه قد تتم

^{١٢٨}العشقي، مصطفى، دورة إنترنت. مركز الأيمن الدولي للمعلوماتية،
الدخول (٢٠١٨/٦/٩)، ص ٦
file:///C:/Users/Rashed%20Ayyash/Downloads/elebda3.net-7720.pdf، تاريخ

^{١٢٩}قنيطرة، أحمد، الآثار السلبية لاستخدام الإنترنت من وجهة نظر طلبة الجامعة الإسلامية بغزة ودور التربية الإسلامية في علاجها، الجامعة الإسلامية غزة، كلية التربية، رسالة ماجستير غير منشورة، ٢٠١١، ص ١١.

المحادثة إما على شكل نصوص أو صور أو صوت أو فيديو، وهذه الدردشة تكون بجميع اللغات دون أن تكون حكراً على دولة دون الأخرى.

خامساً_ خدمة البحث.

وفر الإنترنت خدمة البحث حيث باستطاعة كل مستخدم أن يصل لأي معلومة يريدتها من خلال خاصية البحث التي وفرتها شبكة الإنترنت.

سادساً_ خدمة الدخول أو الاتصال عن بُعد.

حيث يكون باستطاعة مستخدم تلك الخدمة أن يستخدم برامج وتطبيقات موجودة في حاسب آلي إلى حاسب آلي آخر.

سابعاً_ خدمة التجارة الإلكترونية.

حيث أنه باستطاعة أي شخص ومن خلال تلك الخدمة أن يقوم بعمليات شراء سواء كان كتب أو أجهزة إلكترونية أو ملابس وغيرها، ويكون ذلك من خلال مواقع تجارية موجودة على شبكة الإنترنت وتتم عملية الشراء بوساطة بطاقات الائتمان الخاصة بالشخص مثل بطاقة Visa Card وغيرها^{١٣٠}.

^{١٣٠} شريف، عبد العزيز، الاعلام الإلكتروني، موقع <http://k-tab.net>، تاريخ الدخول (٢٠١٨/٦/١٠).

كما أن هناك العديد من الخدمات الأخرى التي تقدمها شبكة الإنترنت، لم نتطرق لها جميعها، كخدمة راديو الإنترنت وعرض شرائط الفيديو والألعاب ومشاركة الملفات (P2P Filc sharing) وتلفزيون الإنترنت وخدمة القوائم البريدية والاستعلامات وخدمة البحث عن الكتب وغيرها الكثير من الخدمات التي تقدمها تلك الشبكة،^{١٣١} وهذا ما جعلها سبباً في إقبال المستخدمين عليها بكثرة.

المطلب الثاني

الإنترنت ايجابياته وسلبياته.

أنشأت شبكة الإنترنت عالماً افتراضياً موازياً للعالم الحقيقي، وجعلت العالم قرية صغيرة وقربت كل ما هو بعيد، ووفرت الشبكة الكثير من الخدمات لمستخدمي تلك الشبكة وسهلت الوصول إلى كثير من المعلومات التي يحتاجها المستخدمون.

لقد أصبح الإنترنت أداة في غاية الأهمية بالنسبة للكثيرين، فالشركات التجارية والدوائر الحكومية والمؤسسات الرسمية وغير الرسمية أصبحت تحتاجه بكثرة من أجل تسيير أعمالها وتسهيل عملية الاتصال مع المستفيدين وغيرهم، كما أن الأفراد أصبحوا يحتاجون الإنترنت للتواصل مع غيرهم من خلال البريد الإلكتروني وشبكات التواصل الاجتماعي، وكذلك أصبحت

^{١٣١} كيروز، حيمس، وروس، كيث، شبكات الحاسب والإنترنت أسس ومبادئ الشبكات والإنترنت، (ترجمة السيد الألفي، ورضوان عبد العال)، دار العبيكان للنشر، السعودية، ٢٠١١، ص ٩.

الشبكة مكاناً يلهو ويلعب فيه الأطفال. يتبين لنا بأن للإنترنت إيجابيات كما أن له سلبيات، وهذا ما سنوضحه في هذا المطلب ؟ فما هي إيجابيات الإنترنت وما هي سلبياته؟

لقد قسمنا هذا المطلب إلى فرعين حيث تناول الفرع الأول ايجابيات شبكة الإنترنت، وتناول الفرع الثاني سلبيات شبكة الإنترنت.

• الفرع الأول:- ايجابيات شبكة الإنترنت.

كان لوجود شبكة الإنترنت في الوقت الحالي أثر كبير في تقدم كثير من المجتمعات، حيث ساهمت الشبكة في تقديم أغلب الخدمات التي يحتاجها الإنسان كخدمات البحث العلمي، والتجارة وغيرها. إن الإنترنت يعد من أهم مكتشفات القرن العشرين وهي كغيرها من المكتشفات سلاح ذو حدين، فالسلاح بكافة أنواعه وأشكاله وغيره من الصناعات والاكتشافات التي أوجدها الإنسان يمكن أن يتم استخدامها في الخير، ويمكن أن يتم استخدامها في الشر.

نحن هنا لسنا بمناظرة، ولسنا في معرض دفاع عن الإنترنت، ولا نقلل من شأن الأضرار التي تنتجها شبكة الإنترنت والتي تغلب على ايجابياتها، ولكن من باب إيراد محاسن تلك الشبكة ومن باب العلم بالشيء رأينا أنه من الواجب أن نتحدث عن فوائد الإنترنت.

أولاً_ سرعة نقل المعلومات.

تميزت شبكة الإنترنت بسرعتها في نقل المعلومات، وضمان انتشارها بشكل سريع، فأصبح من الممكن أن تصل إلى أي معلومة في دقائق معدودة بنقرة واحدة من خلال البريد الالكتروني أو مواقع التواصل الاجتماعي.

لهذا فإن هناك مثلاً يؤكد إيجابيات الشبكة في سرعة نقل وتمرير المعلومات هو بروتوكول نقل الملفات (FTP: File Transfer Protocol) بين الحواسيب المختلفة في الشبكة حواسيب (FTP) تحتوي على ملفات، يمكن نسخها إلى الحاسوب الشخصي، تدعمه العملية بإنزال الملفات (Download)، كذلك يمكن نسخ ملفات من الحاسوب الشخصي إلى الحاسوب (FTP) أي بالاتجاه الآخر (Upload). هذه العمليات تتم بسرعة كبيرة جداً، حيث يمكن نسخ كميات كبيرة من الملفات بوقت قصير جداً^{١٣٢}.

ثانياً_ استخدام الإنترنت في التجارة.

سهلت شبكة الإنترنت التجارة الإلكترونية، حيث عملت على إلتقاء البائع والمشتري من خلال شبكة الإنترنت، وقد كانت عمليات التجارة تتم من خلال مواقع إلكترونية خاصة بالتجارة وبالتسويق بحيث يستطيع المشتري الدخول إلى تلك المواقع وطلب السلعة التي يريدها ويكون تسديد قيمة تلك السلعة من خلال بطاقات إئتمان خاصة به كالفيزا كارد وغيرها، وهذا ما نتج عنه شيء يمكن أن نطلق عليه اسم عقد البيع الإلكتروني، فهي من أكثر العقود انتشاراً وتداولاً على شبكة الإنترنت، وهذا يدل على ارتباط هذا الموضوع بالقانون المدني وبفروع القانون الخاص سواء أكان داخلياً أم دولياً.

يُستنتج لنا أيضاً أن التجارة على شبكة الإنترنت وفرت عناء ومشقة السفر حيث أصبح بإمكان المشتري والبائع أن يقوم بعملية البيع والشراء دون أن يكون هنالك أي مشقة أو تعب

^{١٣٢} هاشم، مصطفى، إيجابيات وسلبات شبكات الحاسوب في التجارة الإلكترونية،

<https://kenanaonline.com/users/mhae2016/posts/398674>

عليه، وكذلك أصبح أصحاب المهن يستطيعون أن يطوروا من أنفسهم وأعمالهم وأن يحصلوا على كل ما يرغبون به من أجل تطوير صناعتهم، وهذا بدوره يؤدي بنا إلى القول بأن جرائم الإنترنت شديدة الصلة بالقانون التجاري كما لها صلة بحركة التجارة العالمية الحديثة، وهذه من الإيجابيات المهمة التي وفرتها شبكة الإنترنت^{١٣٣}.

ثالثاً_ سهولة الاستخدام.

تميزت شبكة الإنترنت بسهولة استخدامها وهذا ما جعلها سبباً في انتشارها بشكل سريع، حيث أنها لا تحتاج إلى خبراء ومختصين لكي يعملون على تلك الشبكة، لقد كان لسهولة عمل تلك الشبكة أثر كبير في انتشارها في مختلف أنحاء العالم وبالتالي إقبال ملايين المستخدمين لها.

ويلاحظ أن سهولة استخدام هذه الشبكة العالمية العديد من المزايا التي مكنت الطلبة والباحثين والتجار وعمامة الناس من مستخدمي هذه الشبكة من الحصول على السلع التجارية والأبحاث بسرعة وبأقل التكاليف وبدون عناء السفر والانتقال من مكان إلى آخر.

رابعاً_ الإنترنت نظام مفتوح.

تتميز شبكة الإنترنت بأنها نظام مفتوح للجميع، بحيث أنه باستطاعة أي شخص في مختلف أنحاء العالم من الدخول لها والاستفادة من الخدمات التي تقدمها، والوصول إلى أي موقع

^{١٣٣} الجريدلي، جمال، البيع الإلكتروني للسلع المقلدة عبر شبكة الإنترنت دراسة فقهية مقارنة، ط١، دار الفكر الجامعي، الاسكندرية، مصر، ٢٠٠٨، ص٧٩+٨٠.

موجود على تلك الشبكة وفي أي مجال يريده، المهم أن يكون لديه جهاز حاسوب وخط هاتف
واشتراك لدى إحدى الشركات التي تقدم خدمة الإنترنت^{١٣٤}.

خامساً_ الشمولية والعمومية.

كما تتميز شبكة الإنترنت بصفة العمومية والشمولية، ويقصد بالعمومية أنها تشمل كل
أجهزة الحاسوب المرتبطة بشبكة الإنترنت والمنتشرة في مختلف أنحاء العالم، ويقصد بالشمولية
أن قواعد المعلومات المتوفرة على الإنترنت تغطي معلومات أشمل حيث إنه في حالة الاتصال
بالإنترنت فإن مراجع البحث ستكون على مستوى العالم بأسره بدلاً من أن تكون مراجع البحث
هي المكتبات فقط^{١٣٥}.

سادساً_ حرية الشبكة.

من ايجابيات شبكة الإنترنت أيضاً أنها ليست حكراً لأحد، بحيث أنها لا تخضع لسيطرة أو
لهيمنة من أحد على تلك الشبكة، أما في الوقت الحالي فأوجدت الدول التي تستخدم تلك الشبكة
صلاحية المراقبة والكشف والإشراف عليها بحيث يكون تحت سيطرتها وضمن حدود دولتها،
وذلك حتى لا تتم أي اعمال تخطيط ارهابية ضد الدولة^{١٣٦}.

^{١٣٤} زهران، مضر، جرائم الدعاية على الإنترنت، دار زهران للنشر والتوزيع، الأردن، عمان، ٢٠٠٣،
ص ١٤.

^{١٣٥} الحلبي، خالد، مرجع سابق، ص ٥٢.

^{١٣٦} الزعبي، جلال، وآخرون، جرائم الحاسوب والإنترنت، دار وائل للنشر والتوزيع، الأردن، عمان، ٢٠٠١،
ص ٦٣.

لهذا نشير إلى أن هنالك ايجابيات أخرى لشبكة الإنترنت، ولكن لم نتحدث عنها لأنها ليست متعلقة بموضوع البحث بشكل مباشر.

• الفرع الثاني:- سلبيات شبكة الإنترنت.

بالرغم من الايجابيات التي قدمتها شبكة الإنترنت، إلا أنه نتج عنها أيضاً سلبيات سوف نتحدث عن بعض تلك السلبيات.

أولاً_ الإدمان.

لقد كان لسهولة استخدام شبكة الإنترنت أثر كبير في ازدياد عدد مستخدمي تلك الشبكة، وهذا ما جعلها سبباً في ادمان الكثير من الشباب، فكما يوجد أشخاص مدمنون على التلفاز يوجد أيضاً أشخاص مدمنين على شبكة الإنترنت، هناك دراسات عديدة تؤكد على أن للإنترنت طبيعة ادمانية خطيرة، وعندما نجد أشخاص مدمنون على شبكة الإنترنت لساعات طويلة دون راحة فمن الواجب أن ندق ناقوس الخطر، لأن هذا الادمان سينتج عنه اضطرابات جسمية ونفسية تنعكس سلباً على حياة الشخص المدمن^{١٣٧}.

لهذا نطرح مثلاً بسيطاً على الادمان، وهو ما حدث في جمهورية مصر العربية حيث أصدرت محكمة الأحوال الشخصية حكماً بالطلاق لمصلحة زوجة مصرية تقدمت بشكوى للمحكمة ضد زوجها الذي يعاني من ادمان بشكل غير طبيعي على شبكة الإنترنت، حيث قالت

^{١٣٧} توم، مجذوب، تكنولوجيا الإتصال وتأثيرها على الجمهور العربي (بالتركيز على فئة الشباب)، <http://repository.sustech.edu/handle/123456789/4736>، تاريخ الدخول (٢٠١٨\٦\١٧)

زوجته بأنه يقضي يوماً ما يقارب (١٤ ساعة) وهذا ما جعل حياتها الزوجية في وضع لا يطاق فأصبحت حياتها كالجحيم بعد أن فشلت كل محاولات وقف ادمانه من أجل إصلاحه^{١٣٨}.

ثانياً_ الخطر الثقافي.

تميزت شبكة الإنترنت بأنها ذات طابع حر، بمعنى أنها ليست حكراً لأحد، وهذا ما أدى إلى وجود مواقع تعمل على تدمير الثقافة والدين، فأصبحت وسيلة من وسائل الغزو الثقافي الغربي كالتبشير قديماً^{١٣٩}.

ثالثاً_ الخطر الأخلاقي.

ساهم انتشار شبكة الإنترنت بشكل كبير إلى انتشار المواقع الإباحية التي تعمل على تدمير الأخلاق، وذلك من خلال إنشاء مواقع تعمل على نشر أفلام وصور غير أخلاقية، وهذا بحد ذاته يؤدي إلى تدمير الأخلاق وبالتالي فساد المجتمع، إن كل مستخدم للإنترنت معرض للإسقاط والتأثر بما يتم عرضه على الإنترنت من مشاهد إباحية، وهذا بحد ذاته يشكل خطراً حقيقياً على الشباب، لأن الشباب خلال فترة المراهقة يكونون بحاجة لإشباع رغباتهم فمن خلال تلك المواقع الإباحية يعتقد الشباب بأنهم أشبعوا رغباتهم^{١٤٠}. وقد قدر عدد المواقع الإباحية في الإنترنت عام (١٩٩٧) بنحو (٧٢٠٠٠) موقعاً مع نشوء (٢٦٦) موقعاً إباحياً جديداً كل يوم،

^{١٣٨} الداھري، صالح، الإدمان على الإنترنت كثقافة تواصل اجتماعي وأبعاده النفسية والاجتماعية على الأسرة العربية، مجلة كلية التربية الأساسية، جامعة المستنصرية، مج ٢١، عدد ٨٧، ٢٠١٥، ص ٦٣٧.

^{١٣٩} الجريدلي، جمال، مرجع سابق، ص ٨٣.

^{١٤٠} قنيطرة، أحمد، مرجع سابق، ص ٢١.

كما قدر حجم الدخل الإجمالي للمواقع الإباحية في الإنترنت بمليار دولار سنوياً على الأقل منذ عام (١٩٩٧)١٤١.

رابعاً_ العزلة.

إن الجلوس المستمر على شاشة الحاسوب وحيداً، والدخول إلى شبكة الإنترنت وتصفح المواقع بمختلف أنواعها سواء كانت إخبارية أم اقتصادية أم اجتماعية وغيرها، تؤدي إلى العزلة وبالتالي انقطاع النسيج الاجتماعي بين الناس، وحدوث المشاكل الأسرية وغيرها، فمن الواجب على الأهل أن ينتبهوا لأولادهم خوفاً عليهم من الضياع والادمان.

خامساً_ تدمير المواقع.

إن المواقع الإلكترونية على شبكة الإنترنت معرضة غالباً وفي أي وقت إلى هجمات إلكترونية يمكن أن نطلق عليها اسم عمليات الاختراق أو التخريب سواء كان هذا التخريب كلي أو جزئي، وتكون عملية التخريب أو الاختراق أما عن طريق زرع فيروسات في أنظمة أجهزة الحاسوب أو من خلال ظهور تلك الفيروسات عن طريق برامج خاصة تنزل تلقائياً على جهاز الحاسوب بعد أن يقوم مستخدم الحاسوب بفتح برامج معينة فتأتي الفيروسات من خلال نوافذ منبثقة بشكل مفاجئ وتؤدي إلى تدميره ، مما يسبب ذلك خلافاً في برامج نظام التشغيل أو المعالجة، والفايروس هو برنامج من صنع خبراء مختصين بهذه البرامج حيث يتم إقحام

^{١٤١} القدهي، مشعل، الإباحية وتبعاتها ظاهرة نقشي المواد الإباحية في الإعلام و الاتصالات و الإنترنت وأثرها على الفرد و المجتمع و أمن الشعوب، د.ن، ٢٠٠٥، ص٣٨.

الفايروس داخل برامج معينة بحيث أنه عندما يقوم مستخدم الحاسوب بفتح برنامج معين فإن ذلك يؤدي لدخول الفايروس إلى الحاسوب بطريقة خبيثة حيث أنه ينزل لجهاز المستخدم بشكل تلقائي دون أن يأمر بفتح ذلك البرنامج، ويمكن أن نطلق على الفايروس بأنه كمرض السرطان الخبيث فهو لديه قدرة على مضاعفة نفسه، وعلى أن ينسخ نفسه في برامج أخرى عند تشغيله في الحواسيب.

لهذا سوف نتطرق لتدمير المواقع في الفصل الثاني من هذا البحث وسنتحدث بشكل مفصل عن الإختراق وكيف يتم ومن هو المخترق وهل باستطاعة أي شخص أن يقوم بالإختراق أم أنها تقتصر على أشخاص ذوي خبرة في هذا المجال.

سادساً_ الإباحة وعدم السرية.

بالرغم من الايجابيات التي قدمتها شبكة الإنترنت، إلا انها لم تكن في موضع رقابة من قبل أجهزة معينة، ولعدم وجود هيمنة ولأنها لم تكن حكراً لأحد هذا ما جعلها سبباً في عدم سرية المعلومات، حيث أنه وباستطاعة كل شخص أن يقوم بنشر ما يريد على مواقع الإنترنت، ودون أن يكون هناك رقيب على تلك المواقع، كالمواقع الإباحية والمواقع التي تحض على الفساد والعنف، والمواقع التي تبث الكراهية الدينية والطائفية وغيرها.

نخلص للقول أنه من الواجب على كل دولة أن تقوم بتوفير أجهزة مراقبة مختصة لمراقبة تلك المواقع التي تحض على الكراهية أو المواقع التي تعمل على نشر الفكر الإرهابي الذي يهدف لفساد الدولة وتدميرها.

وفي فلسطين يمكن القول بأنها أوجدت رقابة على شبكة الإنترنت من خلال إنشاء قسم مختص داخل النيابة العامة، وهو قسم مختص بالجرائم الإلكترونية، وقد تم إقرار قرار بقانون الخاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨) حيث تناول فيه بعض المواد التي تعاقب على كل من يقوم بإنشاء مواقع تحريضية أو ينشر أخباراً كاذبة أو يكون الهدف منها تدمير أو تخريب الدولة، وهذا بدوره يؤدي إلى زيادة انتهاك الحقوق الأساسية والحريات الفردية للأشخاص التي كفلها القانون الأساسي، وهذا يدل على ارتباط جرائم الانترنت بالقانون الدستوري^{١٤٢}.

سابعاً_ الابتزاز.

من السلبيات التي ظهرت حديثاً على شبكة الإنترنت وهي ظاهرة الابتزاز، وتتم غالباً عملية الابتزاز على الفتيات وذلك لسهولة استدراجهن بالكلام الجميل والوعود الخيالية الكاذبة، حيث يمكن أن نعرف الابتزاز بأنه قيام شخص (شاب) بابتزاز (فتاة) سواء كان بصور خاصة بها أو بمقطع صوتي لها أو بفيديو بحيث أن هذا الشخص الذي يقوم بابتزاز الفتاة يعرض عليها عرضاً ما من أجل عدم نشر صورها وفضحها، ويكون ذلك عن طريق طلب مبلغاً مالياً معيناً أو قطع من المجوهرات، وقد حدثت حالات كثيرة في فلسطين لهذا النوع من الابتزاز، نشير للحصر إلى قضية فتاة من نابلس حيث تم ابتزازها بنشر صورها على مواقع التواصل

^{١٤٢} الشوابكة، محمد، مرجع سابق، ص ١١.

الاجتماعي بعد أن أوهمها بالزواج وأنه تاجر عقارات، وقد وصلت قيمة الأموال التي دفعتها الفتاة لذلك الشخص الذي هددها بمبلغ يقدر حوالي ١٨٥ ألف شيكل^{١٤٣}.

الفصل الثاني

جريمة اختراق أنظمة المعلومات والشبكات المعلوماتية

لقد كان لسهولة التعامل مع شبكة الإنترنت أن مهدت طريقاً ليس صعباً للمجرمين من أجل تحقيق مصالحهم والقيام بأعمالهم الإجرامية، ومن هنا بدأت تظهر سلبيات شبكة الإنترنت التي تحدثنا عنها في نهاية الفصل الأول.

وساعدت شبكة الإنترنت المجرمين كافة، ومن لديهم خبرة في الحاسوب بأن يقوموا بارتكاب أنواع عديدة من الجرائم الإلكترونية، هذه الجرائم أثرت بشكل كبير على مختلف المجتمعات حيث سببت خسائر مالية فادحة بلغت ملايين الدولارات.

في هذا الفصل سوف نتحدث عن جريمة الاختراق من حيث تعريفها وبيان أركانها، والتعرف على من هم المخترقون؟ وهل هم أشخاص ذوي خبرة معينة؟ سنتعرف في هذا الفصل على أشكال ودوافع جريمة الإختراق، ومن ثم بعد ذلك التعرف على نظم المعلومات من حيث بيان تعريفها ومكوناتها، وكذلك التعرف على الأمن المعلوماتي وعناصره وسيتم تقسيم هذا الفصل كالتالي:

^{١٤٣} خبر نشر على وكالة معا الإخبارية، كشف قضية إبتزاز فتاة ب١٨٥ ألف شيكل في نابلس، <https://www.maannnews.net/Content.aspx?id=950163>، تاريخ الدخول (٢٠١٨\٦\١٨).

- **المبحث الأول:-** التعريف بجريمة اختراق.
- **المبحث الثاني:-** نظم المعلومات وأمنها على الشبكة المعلوماتية.

المبحث الأول

التعريف بجريمة الاختراق

تعتبر جريمة الاختراق من الجرائم الإلكترونية التي ظهرت مع تطور شبكة الإنترنت، حيث أسهم تطور الشبكة إلى بروز جرائم إلكترونية لم تكن تعرفها البشرية من قبل، ومع بروز تلك الجرائم ونموها بشكل مستمر أصبح من الضروري على الدول التي تتعامل مع شبكة الإنترنت أن تقوم بإيجاد الحلول وتوفير الحماية ضد تلك الهجمات الإلكترونية التي تكلف الدول خسائر مالية فادحة.

لهذا سوف نركز في هذا المبحث على جريمة الاختراق من حيث تعريفها لغةً، واصطلاحاً، والتطرق إلى أشكال الاختراق والدوافع التي تدفع المجرم أو المخترق إلى القيام بذلك الهجوم الإلكتروني، حيث يقتصر هذا المبحث على ما يلي:-

- **المطلب الأول:-** ماهية جريمة الاختراق.
- **المطلب الثاني:-** أشكال ودوافع الإختراق وخصائصها.

المطلب الأول

ماهية جريمة الاختراق

أصبح من الضروري والمهم على الدول التي تعمل على شبكة الإنترنت وتستخدمها بشكل أساسي في كافة مجالاتها، أن توفر الحماية لمستخدمي الشبكة من الهجمات الإلكترونية، لأن قضية أمن الشبكات تمثل النواة الأولى في بناء أي منظومة شبكية آمنة.

ويمكن الإشارة إلى أن جريمة الاختراق في حد ذاتها هي جريمة إلكترونية عابرة لحدود الدول، فهي جريمة لا تسأل عن سياق أمني فاصل بين الدول ولا تسأل عن جنود يقفون على حراسة حدود دولهم، حيث يمكن أن نسميها بأنها جريمة صامتة ترتكب دون أن يشعر أحد بذلك إلا بعد حدوث النتيجة وهي اختراق المواقع وتدميرها. لهذا سميت الجريمة الإلكترونية بهذا الاسم لأنها تتم من خلال الحاسوب وشبكة الإنترنت.

وهناك واجب يقع على عاتق الدول لمكافحة الجريمة والجرائم الإلكترونية الأخرى وهو مواكبة التطور التكنولوجي والمستمر يومياً، وذلك من أجل إيجاد الحل الأمثل لحماية الشبكة من خطر الهجمات الإلكترونية.

لقد قمنا بتقسيم هذا المطلب إلى ثلاثة فروع، حيث تناول في الفرع الأول تعريف جريمة الاختراق، وفي الفرع الثاني أركان جريمة الاختراق وفي الفرع الثالث من هم مرتكبوا الجرائم الإلكترونية.

• الفرع الأول:- الاختراق.

ذهب بعض الفقهاء إلى اعتبار جريمة الاختراق وتصنيفها على أساس أنها ضمن عائلة الجرائم المعلوماتية التي يتم ارتكابها بوساطة النظام المعلوماتي^{١٤٤}، في حين ذهب البعض الآخر من الفقهاء إلى أنها تنتمي للسلوك الإجرامي بجرائم الاعتداء على نظم المعالجة الآلية، أو بجرائم السلوك التي تتصل بنظام المعالجة الآلية للمعلومات^{١٤٥}. وهذا ما يدفعنا للقول بأن الهجوم على المواقع واختراقها على شبكة الانترنت، إنما يعد من الجرائم الشائعة في العالم.

لهذا فإن التطور التكنولوجي السريع في وسائل الاتصال المختلفة، وزيادة الإقبال على شبكات الإنترنت قد أدى إلى انتشار ظاهرة جريمة الاختراق بشكل غير متوقع من قبل أشخاص غير مصرح لهم بالدخول إلى تلك المواقع أو غير مصرح لهم بالبقاء لفترات داخل هذا الموقع.

ويمكن القول بأن جريمة الاختراق هي جريمة إلكترونية تتم من خلال الدخول إلى جهاز حاسوب الضحية عن طريق فايروسات أو عن طريق برامج أخرى يتم تلغيمها بحيث أنه عندما يقوم الضحية بفتح موقع ما فتظهر له شاشة (نافذة منبثقة) بشكل عشوائي، وعادةً ما تكون هذه النوافذ ملغومة بفايروسات أو ببرامج اختراق، حيث يعتبر جهاز الحاسوب الأداة التي تستخدم في ارتكاب جريمة الاختراق ومن خلال شبكة الإنترنت يقوم المجرم المعلوماتي بالدخول إلى موقع ما، ويبدأ بالتخريب بذاك الموقع بناءً على مهارته العبقرية في مجال

^{١٤٤} عفون، حمزة، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماستر غير منشورة، جامعة الحاج لخضر باتنة، الجزائر، ٢٠١٢، ص ١١٧.

^{١٤٥} حجازي، عبد الفتاح، الدليل الجنائي والتزوير في جرائم الكمبيوتر، دار الفكر الجامعي، الأسكندرية، مصر، ط ١، ٢٠٠٢، ص ٢٣٥.

الحاسوب. إذا يُفهم من ذلك بأن الحاسوب هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم الإلكترونية على شبكة الإنترنت. إذ تتألف الجريمة الإلكترونية من مقطعين الأول (الجريمة) والثاني (الإلكترونية) وبالتالي يستخدم مصطلح الإلكترونية من أجل وصف هذه الجريمة بأنها تمت من خلال الحاسب وشبكة المعلومات فكما أشرت سابقاً فالحاسوب هو الأداة التي تستخدم لارتكاب الجريمة، أما الجريمة فهي تعبر عن السلوك السلبي للشخص فكما هو متعارف عليه فإن الإنسان يولد وهو على الفطرة الصحيحة الخالية من السلوكيات السلبية، لكن قد يتأثر الإنسان من البيئة المحيطة به فيكتسب منها السلوك السلبي. وبالتالي نخلص إلى القول بأن الجريمة هي انحراف الإنسان عن طبيعته الإيجابية وانتقالها إلى طبيعة سلبية فقد يصبح هذا الشخص عدوانياً ويقوم بارتكاب الأفعال غير القانونية ومنها الجرائم الإلكترونية بمختلف أنواعها. والجرائم الإلكترونية هي التي ترتكب ضد أفراد أو مجموعة من الأفراد بهدف ارتكاب جريمة ما ويقصد تحقيق النتيجة المتمثلة في الإساءة للضحية أو إجباره على دفع مبالغ مالية مقابل التراجع عن الهجوم الإلكتروني. وسواء أكان هذا الهجوم بطريقة مباشرة أو غير مباشرة، حيث يكون الهجوم من خلال الحاسوب وعن طريق شبكات الاتصالات المختلفة كالإنترنت والبريد الإلكتروني (Email)^{١٤٦}. ونرى أن الشخص المهاجم قد يستخدم في هجومه ما يُعرف بالقنبلة المنطقية، وهي عبارة عن برنامج يدمر البيانات أو يستخدم حصان طروادة، وهو عبارة عن برنامج صمم لاقتحام أمن النظام بحيث يتكرر فيه بشكل بريء حتى يصل إلى هذا النظام ومن ثم افساده.

^{١٤٦} البداينة، ذياب، ورقة بحث بعنوان "الجرائم الإلكترونية المفهوم والأسباب" الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحويلات الإقليمية والدولية" الواقع من (٢_١٤\٩\٢٠١٤)، عمان، الأردن، ص ١.

ونشير هنا إلى أن أوائل عمليات الاختراق تعود لسنة (١٩٨٥ - ١٩٨٦) حيث قام بها الألمان والأمريكان، وتعتبر أشهر جريمة اختراق قيام طفل أمريكي لم يتجاوز (١٤) عاماً من عمره في سنة (١٩٩٢) باختراق شبكة البنتاغون حيث سُمح له بإكمال عملية الاختراق من أجل تحديد مكانه عن طريق مزود خدمة الإنترنت، وقد ضم هذا الطفل إلى البنتاغون وأصبح عضواً فعالاً فيها^{١٤٧}. لهذا قمنا بتقسيم هذا الفرع إلى فئتين الأولى الاختراق لغةً والثانية الاختراق اصطلاحاً.

• الفقرة الأولى: الاختراق لغةً.

الاختراق:- الخَرْق:- **الخَرْقَة**، وجمعه خُرُوق ؛ خَزَقَهُ يَخْرِقُهُ خَرْقاً وخَزَقَهُ واخْتَزَقَهُ فَتَخَرَّقَ وانخَرَقَ واخْرُورِقَ ، يكون ذلك في الثوب وغيره التهذيب الخرق الشَّقُّ في الحائط والثوب ونحوه يقال : في ثوبه خَرْق وهو في الأصل مصدر والخَرْقَة: القِطْعَة من خِرَقِ الثوب، والخَرْقَة المِرْقَة منه وخَرْقَتِ الثوب إذا شَقَّتْهُ ويقال للرجل المْتَمَرِّقِ الثياب : مُتَخَرِّقِ السَّرْبَالِ^{١٤٨}. وقد ورد في قوله تعالى: "إِنَّكَ لَنْ تَخْرِقَ الْأَرْضَ"^{١٤٩} يقصد بخرق الأرض يخرقها: قطعها حتى بلغ أقصاها، وخرقت الأرض أي جبهته^{١٥٠}. وقوله تعالى: "وَحَرَّقُوا لَهُ بُنْيَانَ وَبَنَاتٍ بِغَيْرِ عِلْمٍ"^{١٥١} يقصد بالآية أنهم افتعلوا ذلك كذباً وكفراً^{١٥٢}.

^{١٤٧} العنزري، سليمان، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠٣، ص ٤.
^{١٤٨} ابن منظور، محمد، مرجع سابق، ص ٧٣.
^{١٤٩} أنظر سورة الإسراء، الآية (٣٧).
^{١٥٠} ابن منظور، محمد، مرجع سابق، ص ٧٥.
^{١٥١} أنظر سورة الأنعام، الآية (١٠٠).
^{١٥٢} ابن منظور، المرجع نفسه، ص ٧٥.

إذاً نذهب للقول بأن الاختراق في اللغة قد ورد بمعانٍ عديدة تدور معظمها على التجاوز بالحق وغير الحق.

والاختراق كما ورد في معجم مالية هو دخول غير مصرّح به إلى نظام إلكتروني لمعالجة البيانات (ب) الحصول على حصّة في السوق ويكون ذلك عادة من خلال تخفيض الأسعار، وتعني بالانجليزية (penetration) ١٥٣.

والاختراق كما ورد في معجم اللغة العربية المعاصر خَرَّقَ يَخْرُقُ، خَرَقاً، فهو خارق، والمفعول مَخْرُوق، واختراق (مفرد) مصدر (اخترق) ويمكن القول بأنها تجاوز معيق أو حاجز وتغلب عليه أو يقال هو هجوم يخترق مناطق العدو أو جبهة عسكرية^{١٥٤}.

• الفقرة الثانية: الاختراق اصطلاحاً.

أدركت دولة فلسطين الخطر الحقيقي للجرائم الإلكترونية، وتأثيره الكبير على مرافق الدولة عامةً، حيث تسبب الهجمات الإلكترونية خسائر مالية باهظة تكلف الدولة كثيراً، فرأت أنه ومن الضروري أن يكون هناك قانون يتعلق بالجرائم الإلكترونية ويعاقب عليها، فقد أصدر الرئيس الفلسطيني محمود عباس قراراً بقانون رقم (١٠) لسنة (٢٠١٨) والمتعلق بالجرائم الإلكترونية حيث ورد تعريف الاختراق في المادة الأولى منه، فالاختراق:- هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية^{١٥٥}.

^{١٥٣} معنى كلمة اختراق، موقع معجم المعاني، <https://www.almaany.com/>، تاريخ الدخول (٢٠١٨/٦/١٩).

^{١٥٤} عمر، أحمد مختار، معجم اللغة العربية المعاصر، مرجع سابق، ص ٦٣٤+٦٣٥.
^{١٥٥} راجع المادة (١) من قرار بقانون والمتعلق بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨م).

إذا أمعنا النظر في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة في القاهرة بمقر جامعة الدول العربية عام (٢٠١٠) نجد بأن المادة السادسة تتحدث عن جريمة الدخول غير المشروع، ويمكن أن نفهم من تلك المادة بأنه يقصد بها جريمة الاختراق ولكن دون أن يشار إليها بمعنى مباشر، فكما أشرنا سابقاً بأن جريمة الاختراق هو الدخول إلى جهاز الضحية دون إذن، بحيث يقوم خلال تلك الفترة التي يتواجد فيها داخل الموقع بتخريبه وتدميره وسرقة البيانات المهمة، فقد نصت المادة السادسة على ما يلي:-

١. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

٢. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
ب- الحصول على معلومات حكومية سرية^{١٥٦}.

بعد النظر في المادة السادسة نرى بأن هذه الجريمة هي جريمة خطيرة جداً ومعاقب عليها في حال قام (المجرم) بالبقاء لفترة طويلة داخل الموقع، وتشدد العقوبة بشكل أكبر في حال قام بتدمير الموقع أو الجهاز ويكون ذلك من خلال تشطيب أو تغيير في البيانات، أو في حال قام

^{١٥٦} انظر إلى المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية لسنة (٢٠١٠م) حيث تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

بالدخول لمواقع حكومية رسمية وحصل على معلومات سرية تهدد الدولة (الضحية)، وهذا ما أكدته المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الإماراتي بأنه: "كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين". في حين نصت (ف٢١) من هذه المادة: "إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين". أما (ف٣١) من نفس المادة: "إذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين". يتبين لنا من هذه النصوص التشريعية المتقدمة أن شبكة المعلومات قد تكون موضوعاً لبعض الجرائم الواقعة على المال مثل السرقة والاحتيال والنصب وخيانة الأمانة والاتلاف العمدي، حيث نرى أن هذه الشبكات قد تكون وسيلة لارتكاب الجرائم كما هو الحال في جريمة الدخول أو النفاذ غير المشروع في النظام المعلوماتي، أو نظم معالجة البيانات كما هو الحال في حالة لو تم اختراق موقع جهة حكومية في الدولة عمداً وذلك بدون تصريح أو اختراق موقع لأحد الأشخاص بدون إذن منه^{١٥٧}.

^{١٥٧} تمام، أحمد حسام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ٢٠٠٠، ص ٢٦٠.

لهذا تعرف جريمة الاختراق بأنها الدخول أو التوصل غير المصرح به وبالتالي يمكن القول بأنها القدرة على الوصول لهدف معين بطريقة غير مشروعة، ويكون ذلك من خلال ثغرات في نظام الحماية الخاص بالهدف^{١٥٨}.

ويمكن أن نطلق على الاختراق بأنه الدخول أو الولوج إلى النظام إما بقيام الجاني بالدخول إلى الحاسوب كله أو إلى جزء منه، حيث تكون عملية الاختراق غالباً في حال كان للجاني القدرة على الدخول للحاسب، ويشبه جانب من الفقه الجنائي الفرنسي عملية الدخول غير المشروع أو الاختراق إلى نظام الحاسوب أو الموقع الإلكتروني كالدخول أو اختراق ذاكرة الانسان^{١٥٩}. ونرى أنه لكي تتم عملية الاختراق يجب توافر برنامج يتم تصميمه حتى يتيح للمخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أن تتم عملية الاختراق بكل سهولة وقد صممت العديد من تلك البرامج التي تتيح عملية الاختراق وتجعلها سهلة.

والاختراق يطلق عليه باللغة الإنجليزية مصطلح (hacking) وهو محاولة الدخول لجهاز المشترك في شبكة الإنترنت من قبل شخص آخر لا يحق له الدخول إلى ذلك الجهاز أو تلك الشبكة، وذلك بهدف الاطلاع على البيانات والمعلومات وتدميرها أو زرع فيروسات^{١٦٠}.

^{١٥٨} الحلبي، خالد، مرجع سابق، ص ٨٩.
^{١٥٩} خلف، سامية، بحث بعنوان "جريمة اختراق أنظمة المعلومات دراسة مقارنة"، مجلة العلوم القانونية، جامعة بغداد، ٢٠١٠، ص ١٨.
^{١٦٠} عمار، زكريا، مرجع سابق، ص ١٨.

ولهذا فإن الاختراق يختلف عن القرصنة بأمر معين مع أن كلاهما يتم من خلال الدخول غير المصرح به ، فالقرصنة هي عبارة عن عملية سرقة الملكية والحقوق وتتم من خلال دخول غير مصرح به إلى شبكة الإنترنت، وأكثر عرضة لهؤلاء القرصنة هم الشركات، فالشركات عادةً تقوم بإنتاج برامج خاصة للحواسيب وتكون هذه البرامج فقط حكر للشركة المنتجة من حيث حرية التصرف به وإلخ.. وتقوم ببيعها بأسعار معينة فيأتي القرصان ويدخل الى موقع تلك الشركة ويبدأ بتغيير إعدادات البرنامج ونطلق على تلك العملية اسم "التهكير" حتى يستطيع العمل عليه دون شراء، فالقرصان هو خطير غالباً على الشركات التي تنتج البرامج والألعاب، بينما المخترق هو خطير على الجميع، **فالاختراق** هي كسر لحاجز الأمان التي تمنع الشخص العادي من الوصول للبيانات والمعلومات، والمخترق يقصد تدمير النظام من خلال المساس بسريته ومعلوماته، والقرصنة هي عملية دخول غير مشروعة تتم من خلال ثغرات موجودة داخل الحاسوب أو شبكة الإنترنت التي يستخدمها^{١٦١}. **والقرصنة** هي النسخ غير المشروع لنظام الحاسب الآلي أو لبرنامج معين من برامج الحاسب الآلي المختلفة وقد بلغت الخسائر التي سببتها القرصنة عام (١٩٨٨) حوالي (١١) مليار دولار أمريكي في مجال البرمجيات^{١٦٢}. لذلك نرى أن معظم هذه البرامج بها نقطة ضعف أساسية وبالتالي تقلل من امكانيات هذه البرامج، وهي امكانية الشعور بتلك البرامج على الجهاز الذي تم اختراقه وعليه يجب متابعة هذه البرامج والقضاء عليها فيما عدا برنامج واحد، فقد تمكن مصمموه من التغلب على هذا العيب الموجود في كافة برامج الاختراق الأخرى حيث أطلق على هذا

^{١٦١} فتحية، ليتيم، نادية، ليتيم، بحث منشور بعنوان " الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، ١٢٤، جامعة بسكرة، الجزائر، ٢٠١٥، ص٢٤٢.

^{١٦٢} الشمري، غانم، مرجع سابق، ص٨٤+٨٥.

البرنامج "حصان طروادة" حيث يعتبر هذا البرنامج من البرامج الخطرة والتي تستخدم في عمليات اختراق أجهزة الحاسب الآلي.

لهذا نرى أن الاختراق هي عبارة عن جريمة يستطيع من خلالها المخترق (المجرم) من الدخول إلى جهاز شخص ما (الضحية) بحيث يقوم من خلال هذا الهجوم بتحقيق النتيجة (الغاية) وهو حدوث ضرر وبصرف النظر عن قيمة الأضرار التي تحدث للضحية.

• الفرع الثاني :- أركان جريمة الاختراق.

إن جريمة الاختراق كغيرها من الجرائم التي ترتكب في الغالب ضد الشخص الطبيعي أو الشخص الاعتباري، وكما أشرنا سابقاً فإن جريمة الاختراق تعني الدخول غير المصرح به لجهاز نظام الحاسوب أو للشبكات والمواقع الإلكترونية، فالاختراق جريمة قائمة بحد ذاتها ولها أركان كالجرائم الأخرى. وبالتالي فإن السلوك الإجرامي في هذه الجريمة يتمثل في الدخول غير المشروع عمداً على نظم معالجة البيانات ومن ثم إعادة تحريف أو تشغيل نظم معالجة البيانات، وكذلك التلاعب في بيانات نظم معالجة البيانات وهي صورة الجريمة عامة والتي تسمى بجريمة الاعتداء على نظم المعالجة الآلية للبيانات.

لهذا تقوم جريمة الاختراق على ركنين أساسيين، ركن مادي وآخر معنوي، ويمكن أن نضيف أيضاً لها ركن ثالث وهو الركن القانوني. فالركن المادي يتمثل بالفعل أو النشاط الذي يقوم به الجاني ويتمثل بالاعتداء على حق حماية القانون، والركن المعنوي يتمثل بعنصري العلم

والإرادة وهو أن يكون الجاني عالماً بما يفعل ولديه علم كامل بمعنى آخر أي أن لا يكون مكره " مجبر على ذلك" أو أن تكون إرادته سليمة، ويقصد بالإرادة وهي أن تتجه إرادة الجاني إلى حدوث النتيجة وإرادتها بغض النظر عن خطورة النتيجة التي حدثت أو ستحدث، والركن القانوني أي أن يكون هذا الفعل معاقب عليه بالقانون وأن يكون المشرع قد ذكر تلك الجريمة في قانون العقوبات أو في قانون خاص " بالجرائم الإلكترونية" لهذا نقوم بإلقاء الضوء بشكل مفصل على أركان جريمة الاختراق وهي:-

أولاً_ الركن المادي.

هو الوجود الخارجي للنشاط الإجرامي، ويقصد به الفعل أو النشاط الذي يقوم به الجاني من خلال الاعتداء على حق يحميه القانون، والركن المادي في جريمة الاختراق يتمثل في الدخول إلى نظام جهاز الحاسوب وإتلاف برامج وبيانات أو الوصول إلى معلومات سرية هامة.

لهذا يقوم الركن المادي على ثلاثة عناصر أساسية وهي:-

١_الفعل.

وهو النشاط أو السلوك الإجرامي للجاني. والسلوك قد يكون إيجابي وقد يكون سلبي. فالسلوك الإيجابي:- هو عبارة عن حركة عضوية إرادية نهى القانون عن القيام بها لأنها ستؤدي إلى وقوع النتيجة، ويشترط أن تكون الحركة إرادية أي صادرة عن إرادة الإنسان وأنه

غير مكره على فعله. بينما السلوك السلبي:- هو عبارة عن الامتناع عن القيام بفعل أوجب القانون على القيام به رعاية لمصالح وحقوق الأفراد^{١١٣}.

٢_ النتيجة.

وهي ما يترتب من أضرار على النشاط الذي قام به الجاني، والنتيجة الإجرامية يكون لها مفهومان هما ١- المفهوم المادي للنتيجة ٢- المفهوم المعنوي للنتيجة.

٣_ العلاقة السببية.

وهي أن يكون هناك علاقة أو رابطة سببية بين الفعل والنتيجة، حيث يكون السلوك هو السبب الطبيعي لإحداث هذه النتيجة، وأن تكون النتيجة هي الأثر الطبيعي الناجم أو المترتب على السلوك الإجرامي.

إن جريمة الاختراق هي الدخول غير المصرح به للجاني لجهاز شخص آخر، والركن المادي فيها يقوم من خلال الدخول لجهاز نظام الحاسوب أو المواقع الإلكترونية أو شبكات الانترنت. فقد يكون الدخول للحاسوب عن طريق وسائل معينة منها الغش وهي تعتبر إحدى

^{١١٣} نجم، محمد، قانون العقوبات القسم العام النظرية العامة للجريمة، ط٤، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٢، ص٢٠٩+٢١٠.

الوسائل المتاحة للدخول لنظام الحاسوب، ولكن يبقى المعيار الأساسي هو عدم أحقيته في
الدخول لنظام الحاسوب^{١٦٤}.

وقد يتحقق الركن المادي لجريمة الاختراق ببعض من الصور منها: - **الدخول غير
المشروع لنظام المعالجة الآلية للمعطيات**، حيث نصت المادة الرابعة الفقرة الأولى من القرار
بقانون الصادر عن رئيس دولة فلسطين محمود عباس والخاص بالجرائم الإلكترونية رقم (١٠)
لسنة (٢٠١٨) بالقول " كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو
نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول
المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن
مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً،
أو بكلتا العقوبتين".

وبالتالي فإن هذا الشكل من الاعتداء على نظام المعالجة الآلية للمعطيات يتكون من
صورتين بسيطة وأخرى مشددة. فالصورة البسيطة تكمن فيها بالدخول للنظام أو البقاء غير
المشروع.

يقصد **بفعل الدخول**، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية
للمعطيات، ولم يحدد المشرع طريقة الدخول أو الوسيلة التي تتم بها عملية الدخول، المهم أن
تكون عملية الدخول قد تحققت.

^{١٦٤} الحسيني، عمر، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية : دراسة تحليلية
نقدية لنصوص التشريع المصري مقارنة بالتشريع الفرنسي، (د.ن)، ط٢، ١٩٩٥، ص١٢٧.

بينما يقصد **بفعل البقاء** وهو الاستمرار في الوجود غير المشروع داخل النظام ضد إرادة صاحب النظام. نرى أن الهدف من تجريم فعل البقاء غير المشروع في النظام المعلوماتي، هو تجريم فعل البقاء، فالجاني مثلاً لم يكن يقصد الدخول إلى هذا المكان، ولكن عندما تبين له أنه دخل هذا المكان، كان من الواجب عليه مغادرته، ومع ذلك بقي هذا الجاني داخل النظام المعلوماتي، حيث تتصرف إرادته حينئذ إلى جريمة اختراق هذا النظام، وبالتالي يعاقب هذا الجاني عن جريمة قصدية، وذلك لأن إرادته انصرفت إلى البقاء داخل هذا النظام، بالرغم من أنه يعلم أن دخوله غير مشروع، كما يكون الدخول غير مشروع في حالة دخول الجاني إلى جزء في النظام المعلوماتي مسموح له الدخول إليه، ثم يدخل إلى جزء آخر في النظام المعلوماتي غير مسموح له الدخول فيه^{١٦٥}. إذاً نستنتج أنه قد يجتمع البقاء غير المشروع والدخول غير المشروع في نفس الوقت، ويكون ذلك في حالة قيام الجاني بالدخول لنظام الحاسوب وهو لا يحق له ذلك، ولكنه يدخل بالرغم من إرادة الضحية أو إرادة صاحب حق الدخول، ويتحقق البقاء غير المشروع من خلال بقاء الجاني داخل نظام الحاسوب بالرغم من علمه بمخالفته لذلك^{١٦٦}. والصورة المشددة تكمن نتيجة حصول الدخول أو البقاء غير المشروع ويكون ذلك من خلال المحو أو اللعب في المعطيات الموجودة في النظام أو تخريبه. وهذا ما دفع الفقه الفرنسي للقول بأن الدخول غير المشروع (العمدي) له مفهومان ١- مفهوم معنوي ويقصد به أن الدخول إلى نظام معالجة البيانات أو النظام المعلوماتي أو الإلكتروني، إنما يشبه الدخول إلى ذاكرة الانسان ٢- مفهوم مادي يتمثل في أن هذا الشخص يكون قد حاول

^{١٦٥} تمام، أحمد حسام، مرجع سابق، ص ٢٩٩.

^{١٦٦} فريال، لعائل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر غير منشورة، جامعة محند أولحاج، الجزائر، ٢٠١٥، ص ٣٣.

الدخول أو دخل فعلاً إلى النظام المعلوماتي أو الإلكتروني^{١٦٧}. لهذا نرى أن الدخول إلى النظام المعلوماتي قد يتم بأية وسيلة تقنية، سواء أكان ذلك عن طريق استعمال كلمة السر الحقيقية متى كان الجاني غير مسموح له استخدامها، أو عن طريق استخدام برامج أو شيفرة خاصة^{١٦٨}. ونجد أن هناك جانب من الفقه يرى أن هذه الجريمة قد تقوم بسلوك سلبي، وذلك لأن الجاني يدخل النظام المعلوماتي بإرادته وبالرغم من علمه بذلك إلى أنه يرفض الخروج من هذا النظام^{١٦٩}. وقد عالج المشرع الفلسطيني والمشرع الإماراتي جريمة الدخول غير المشروع إلى النظام المعلوماتي بشكل واضح وصريح في نص المادة (٤) من قانون الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨)، ونص المادة (٢) من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

وهناك جانب من الفقه يرى أن فعل البقاء غير المشروع داخل النظام المعلوماتي هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام^{١٧٠}.

وهناك جانب من الفقه من يرى أن هناك تعدد معنوي ما بين فعل الدخول غير المشروع وفعل البقاء غير المشروع، ومنهم من يرى بعدم التعدد المعنوي في هذه الحالة^{١٧١}، وهناك جانب آخر من الفقه يرى بأن هناك تعدداً مادياً سببه أن الدخول غير المشروع هو صورة

^{١٦٧} حجازي، عبدالفتاح، الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ط١، ٢٠٠٨، ص٨١.

^{١٦٨} رمضان، مدحت، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر، ٢٠٠١، ص٥١.

^{١٦٩} حجازي، عبدالفتاح، مرجع سابق، ص٨١.

^{١٧٠} القهوجي، علي، بحث بعنوان "جرائم التعدي على نظم معالجة المعطيات"، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، ٢٠٠٠، ص٥٢.

^{١٧١} تمام، أحمد، مرجع سابق، ص٣٠.

للسلوك الإجرامي لجريمة الاختراق وهو مختلف عن جريمة البقاء غير المشروع وكلاهما غير مرتبط بالآخر وبالتالي فهو تعدد مادي وليس تعدد معنوي بين فعلي الدخول غير المشروع والبقاء غير المشروع^{١٧٢}.

نخلص للقول بأن جريمة الاختراق تعتبر جريمة قائمة بحد ذاتها، وذلك بمجرد إتيان الجاني النشاط أو السلوك الإجرامي، فلا يلزم تحقق نتيجة معينة فجريمة الاختراق قائمة بمجرد الدخول غير المشروع، حتى ولو لم يرغب الجاني في تحقيق نتيجة ما، فهي من حيث المكان عبارة عن التسلل داخل النظام المعلوماتي، ومن حيث زمان الدخول فإنه يتمثل في تجاوز حدود التصريح أو الترخيص داخل هذا النظام والذي هو عبارة عن فترة زمنية محددة^{١٧٣}.

ثانياً_ الركن المعنوي.

هو الوجه الداخلي للإنسان أو الباطني، ويقوم الركن المعنوي على عنصرين هما: - العلم + الإرادة. وصورة الركن المعنوي تقوم على "القصد الجنائي المباشر" بالتالي لا يمكن أن تتحقق هذه الجريمة عن طريق الخطأ، وتعتبر جريمة الاختراق من الجرائم القصدية لأن الجاني يكون على علم بأن الفعل الذي يقوم به هو فعل غير مشروع، وإذا أمعنا النظر في المادة الرابعة الفقرة الأولى من القرار بقانون الخاص بالجرائم الإلكترونية الفلسطيني " كل من دخل

^{١٧٢} حجازي، عبدالفتاح، مرجع سابق، ص ٣٣.

^{١٧٣} تمام، أحمد، مرجع سابق، ص ٣٠٥.

عمداً وبدون وجه حق بأية وسيلة... إلخ" يفهم من هذا النص بأن الجاني يكون على علم بما يقوم به وبغض النظر عن الوسيلة التي دخل فيها الجاني إلى النظام.

إذاً يمكن أن يفهم بأن جريمة الاختراق أو جريمة الدخول غير المشروع يتطلب القصد فيها علم الجاني بأنه يقوم بعملية دخول غير مشروعة إلى النظام الخاص بالضحية "المجني عليه" وأن تتجه إرادته إلى ارتكاب الجريمة بغض النظر تحققت النتيجة أم لم تتحقق، بمعنى يجب أن يعلم الجاني أنه ليس له الحق في دخول النظام المعلوماتي أو البقاء فيه، أو أن يعلم بأنه يخالف إرادة ورضى صاحب هذا النظام المعلوماتي، وبالرغم من ذلك تتصرف إرادة الجاني إلى ارتكاب سلوك الدخول مخالفاً بذلك القانون، ومخالفاً لإرادة صاحب النظام المعلوماتي^{١٧٤}. لهذا يرى جانب من الفقه إلى أن الدخول إلى هذا النظام يكون مشروعاً إذا كان دخوله بمحض الصدفة أو الخطأ، فإذا دخل الشخص لمكان فجأةً عليه أن يخرج رأساً وهو ما نطلق عليه مصطلح "حسن النية"، وإذا لم يفعل ذلك يكون قد توافر بحقه القصد الجنائي العام الذي تقوم به هذه الجريمة وهو ما نطلق عليه مصطلح "سيء النية"، فالسطو والخطأ ينفي عدم المشروعية ومن ثم تنتفي إرادة القصد من سلوكه، فإذا دخل الجاني أو بقي داخل النظام المعلوماتي ووقع في خطأ من حيث حقه في الدخول للنظام أو البقاء فيه فالقصد الجنائي لا يقوم في هذه الحالة^{١٧٥}.

^{١٧٤} الصغير، جميل، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، مصر، القاهرة، ١٩٩٢، ص ١٥٢.
^{١٧٥} رمضان، مدحت، مرجع سابق، ص ٥٢.

ثالثاً_ الركن القانوني.

يسميه البعض بالركن الشرعي، فكما هو معروف نرى أن مبدأ الشرعية الجنائية "لا جريمة ولا عقوبة إلا بنص" يفهم من ذلك أن القواعد الجنائية هي التي تحدد الأفعال التي تعتبر جريمة أم لا وهي التي تقرر العقوبة المناسبة لها، والجهة المختصة بتحديد تلك العقوبات وتحديد تلك الجرائم هي السلطة التشريعية لأنها هي من تقوم بإصدار القوانين والسلطة القضائية تقوم بتطبيق تلك القوانين على المجرمين والفصل في الجرائم التي ترتكب^{١٧٦}.

وتعتبر الشريعة الاسلامية هي أول من نادى بمبدأ الشرعية حيث قال تعالى في كتابه العزيز "وَمَا كُنَّا مُعَذِّبِينَ حَتَّىٰ نَبْعَثَ رَسُولًا"^{١٧٧}. وقوله تعالى "وَمَا أَرْسَلْنَاكَ إِلَّا رَحْمَةً لِّلْعَالَمِينَ"^{١٧٨}. يفهم من هذه الآيات الكريمة أن الله سبحانه وتعالى حرم معاقبة أي شخص قبل أن يبعث الرسل وآخرهم نبينا محمد عليه الصلاة والسلام، فقد جاء الرسل جميعهم لبيان الحلال والحرام وما هو محظور وما هو واجب، يفهم من ذلك أن الدولة أيضا لا تقوم بإيقاع العقوبة على الشخص إلا إذا ارتكب عملاً إجرامياً معاقب عليه قانوناً. وإذا نظرنا للمادة الحادية عشرة من القانون الأساسي الفلسطيني لسنة (٢٠٠٣م) نجد بأنها كفلت حق المواطن الفلسطيني في حريته وكرامته وأكدت على أنه لا يجوز معاقبة أي شخص ما لم يكن قد ارتكب جنائية أو جنحة أو مخالفة.

١٧٦ نجم، محمد، مرجع سابق، ص ١٣٧.
١٧٧ أنظر سورة الإسراء، الآية رقم (١٥).
١٧٨ أنظر سورة الأنبياء، الآية رقم (١٠٧).

وفي الركن القانوني "الشرعي" نرى أنه لا يجوز لسلطات الدولة أن تقوم بإيقاع العقوبة على الشخص الذي ارتكب جريمة ما إذا لم تكن تلك العقوبة محددة سلفاً في قانون العقوبات بنص خاص وصريح، وإذا كان هناك نص يجب أن يكون قد صدر قبل ارتكاب الجريمة ويجب أن يكون معلوماً للجميع بحيث لا يحتج أحد بعدم علمه بالقانون أو جهله به، وكما هو معروف فإن أي قانون جديد في فلسطين يتم نشره في الجريدة الرسمية لدولة فلسطين وهي جريدة الوقائع الفلسطينية بحيث يكون مدة نشره ٣٠ يوماً لكي يتسنى للجميع معرفة ذلك القانون والعلم به. إذاً الركن القانوني وجد لخدمة الناس ولحماية حقوقهم ومصالحهم وتأمين كرامتهم وعدم المساس بها^{١٧٩}.

• الفرع الثالث:- من هم مرتكبوا الجرائم المعلوماتية.

في العالم الإلكتروني لا يوجد صديق، فصديقك قد يكون عدوك ببعض الأحيان من خلال اطلاعه على بعض خصوصياتك الخاصة بك، ولضمان أمن المعلومات وضمان سريتها وعدم التعرض للمسؤوليات يتوجب معاملة الجميع على أنهم مصدر للخطر، لسنا هنا في مناظرة لنبين حسن النية من سيء النية، وإنما هي ضمانة للحماية من مصادر الخطر. من المعروف أن أعمار منفذي الجرائم الإلكترونية مختلفة باختلاف دوافعهم، فهناك من منفذي الهجمات الأطفال والمراهقين، الذين تكون في الغالب دوافعهم لمجرد التسلية غير مدركين

^{١٧٩} نجم، محمد، مرجع سابق، ص ١٣٩+١٤٠.

بحجم الأضرار التي يقومون بها، وهناك من هم محترفين ومختصين، الذين من الممكن ان تحطم أعمالهم شركات ضخمة وتضر بدول كبيرة^{١٨٠}.

فيمكن تصنيف مرتكبوا الجرائم المعلوماتية إلى ما يلي:-

أولاً_ المازحون بهدف التسلية.

وهم الأشخاص الذين يرتكبون الجرائم الإلكترونية بهدف هدر الوقت والتسلية والمزاح مع الآخرين، ودون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم^{١٨١}، فهؤلاء الأشخاص عندما يقومون بتلك الأعمال فإنهم يقومون بها من باب الفضول والاستمتاع وليس من باب الإضرار بالمجني عليهم، ولكنهم قد يتسببون بإلحاق الأضرار بالمجني عليهم ويكون ذلك نتيجة الجهل الذي يقعون به أو لعدم معرفتهم في كيفية إخفاء آثارهم، وذلك من أجل التضليل على الجهات المختصة التي تطارد كل من تسول له نفسه ارتكاب أي جريمة إلكترونية^{١٨٢}. وهناك مجموعة اشتهرت بأمريكا، حيث قامت بارتكاب أكثر من (٦٠) هجوم وأدت إلى تكلفة مبالغ طائلة، وكان عمل تلك المجموعة فقط الإطلاع على البيانات ونشر ما تراها من معلومات وبيانات سرية على شبكة الإنترنت، وفي الغالب تكون تلك الفئة "المازحون" هم حسن النية لأنهم يعتقدون أنهم يقومون بعمل غير معاقب عليه وفي الحقيقة يكون عكس ذلك، أغلب

^{١٨٠} جواد، أشرف، الجريمة المعلوماتية أو الإلكترونية أنواعها وخصائصها وطرق الوقاية منها، مجلة الدراسات المالية والمصرفية - المعهد العربي للدراسات المالية والمصرفية- الأردن، مج ٢٣، ع ١٤، ٢٠١٥، ص ٣٠.

^{١٨١} سليم، مزيود، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، ع ١، ٢٠١٤، ص ٩٩.

^{١٨٢} حجازي، عبدالفتاح، مرجع سابق، ص ١٤٠+١٤١.

جرائم الإنترنت بحاجة لذكاء عقلي كبير وليست بحاجة إلى عضلات^{١٨٣}. وهؤلاء قد يتحولون إلى قراصنة في وقتٍ لاحق.

ثانياً_ المتطفلون.

ويطلق عليهم لقب (الهاكرز) وهم الأشخاص الذين يشعرون بالفخر لاحساسهم بمعرفتهم بأساليب عمل النظام أو الشبكات بحيث يسعون للدخول عليها بدون تصريح، وهؤلاء الأشخاص عادةً لا يتسببون بأي أضرار مادية. يكون الهدف من هذا الدخول هو من أجل محاولة إثبات قدرتهم على الدخول للنظام، وليس من أجل تحقيق أي مردود مادي وغالباً ما يقوم بعمليات الدخول هم الشباب وقد يكون السبب حسب توقعنا الشخصي هو أنهم في فترة مراهقة فيقومون بالتسالي ومضيعة الوقت من خلال استغلال موهبتهم بنفس الوقت. **وخير مثال على المتطفلون، هو قيام شابان في مرحلة الثانوية بإيقاف الحاسبة الإلكترونية في الجامعة عن العمل لمدة يومين، وبعدما سئل الشابان عن سبب قيامهما بهذا العمل قالوا أنه مجرد تحدي فقط^{١٨٤}. وتتعرض المواقع الإلكترونية لأربعة أنواع من المتطفلين:-** متطفل قد يكون الهدف من دخوله هو فقط من أجل معرفة تفاصيل موقعك لأشباع فضوله، ومتطفل آخر يهدف لمعرفة مكنون موقعك ولكن يقوم بتغيير المعلومات من أجل التصرف بها كبيعها للآخرين، ومتطفل آخر يريد أن يستخدم موقعك كأداة من أجل استخدامه في الهجوم ضد مواقع أخرى بحيث يكون موقعك هو الأداة وبالتالي تحمل العواقب التي ستتجم عن تدمير

^{١٨٣} الحلبي، خالد، مرجع سابق، ٣٥.

^{١٨٤} صادق، دلال، القتال، حميد، أمن المعلومات، دار اليازوري للنشر والتوزيع، عمان، الأردن، ٢٠١٣، ص١٤٣.

الموقع الآخر، ومتطفل آخر يريد أن يستخدم موقعك من أجل أن يقوم بالنشر عليه ما هو ممنوع في القانون كبيانات سرية أو لنشر صفحات تدعم جنس الأطفال أو لبيع المخدرات أو لنشر مواقع غير أخلاقية "إباحية"^{١٨٥}.

ثالثاً_ المحترفون.

تتميز هذه الفئة بقدرتهم الفائقة في مجال الحاسوب وخبرتهم الواسعة في تقنياته، فهم يمتلكون المعرفة والعلم الكافي من أجل استطاعتهم التلاعب بنظام الحاسوب^{١٨٦}. وقد يكون الجاني في بعض جرائم الحاسوب مستخدماً فقط وهؤلاء هم من يتوافر لديهم الإلمام الكامل والتام بنظام الحاسوب وبعض برامجه وآلية عمله^{١٨٧}. يهدف هؤلاء المحترفون إلى سرقة المعلومات والبيانات الحساسة الخاصة بالدوائر الحكومية الرسمية وغير الرسمية والعسكرية، وذلك لاحتواء تلك الدوائر على مراكز خاصة بحفظ المعلومات والبيانات الرسمية والسرية^{١٨٨}. وميزة جرائم الحاسوب أنه من الصعب اكتشافها وفي حال تم اكتشافها فإنه يكون من باب الصدفة ويقع على الأجهزة المختصة صعوبة الإثبات، ولو أردنا أن نعمل مقارنة بين اكتشاف الجرائم التقليدية والجرائم الإلكترونية سنجد أن الجرائم التقليدية أكثر اكتشافاً مقارنةً بالجرائم الإلكترونية والسبب يكمن في أن الجريمة الإلكترونية لا تترك أي أثر خارجي ظاهر، ويمكن

^{١٨٥} المسند، صالح، المهيني، عبد الرحمن، مرجع سابق، ص ١٨١.

^{١٨٦} الشمري، غانم، مرجع سابق، ص ٣١.

^{١٨٧} الحلبي، خالد، مرجع سابق، ص ٣٤.

^{١٨٨} صادق، دلال، الفتال، حميد، مرجع سابق، ص ١٤٤.

للجاني أن يقوم بارتكاب الجريمة الإلكترونية في دول مختلفة من العالم وهذا ما يميز الجريمة الإلكترونية بأنها جريمة عابرة للدول ومختربة للحدود^{١٨٩}.

رابعاً_ محبو المال.

وهذه الفئة من مرتكبي الجرائم الإلكترونية يكون دافعهم من وراء الاختراق هو فقط من أجل تحقيق مردود مادي. وأغلبهم من الأذكى والمبرمجين الذين يعرفون كيف يتعاملون مع البرامج بنكاه أو يقومون باستخدام وسائل احتيالية من أجل الحصول على المال^{١٩٠}. فهذه الفئة خطر كبير على القطاع التجاري والاقتصاد بشكل عام فهي بتلك الهجمات الإلكترونية تشل الاقتصاد الوطني وتسبب خسائر كبيرة للشركات ولرجال الأعمال، فهذه الفئة تتألف من مجموعة من ذوي الخبرة والكفاءة الذين يوظفون مهاراتهم في سرقة المعلومات أو البيانات وبالتالي التسبب في خسائر مالية فادحة.

خامساً_ المجرمون العاملون في الجريمة المنظمة.

الجريمة المنظمة هي: مؤسسة إجرامية ذات تنظيم هيكلي متدرج، تمارس نشاطات غير مشروعة، بهدف تحقيق أرباح مالية، مستخدمة الطرائق المتاحة كلها لتمويل مشروعها الإجرامي وتحقيق هذا الهدف، وذلك في سرية تامة لتأمين وحمايتها^{١٩١}. ولكي تكون

^{١٨٩} ثنيان، ثنيان، إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١٢، ص ٢٤.
^{١٩٠} صادق، دلال، القتال، حميد، مرجع سابق، ص ١٤٣.
^{١٩١} القحطاني، محمد، الجريمة المنظمة، دار العرب للنشر والتوزيع، ط٢، الرياض، السعودية، ٢٠١١، ص ٥٧.

الجريمة منظمة يجب أن يكون السلوك الإجرامي على درجة عالية من التعقيد أو التشعب، وأن يكون على درجة عالية من التنظيم والتخطيط الدقيق، وأن يكون تنفيذه قد تم على نطاقٍ واسع، وأن تنطوي وسيلة تنفيذه على درجةٍ من العنف، أو على نوع من الحيلة بحيث يتم تجاوز ما هو مألوف في الجريمة العادية، وهذا يشكل خطر على المجتمع ككل سواء كان من الناحية الاقتصادية أو السياسية^{١٩٢}. إذا نخلص للقول بأن الجريمة المنظمة هي جريمة يتم ارتكابها بواسطة جماعات ومنظمات إجرامية لديها التخطيط الدقيق والقدرة على ممارسة العمل الإجرامي بهدف توسعة نشاطها الإجرامي والحصول على المال والتأثير على الاقتصاد الوطني واستغلال الأشخاص.

سادساً_ المخترقون.

وهؤلاء أشخاص قد يكونوا على شكل جماعات أو أفراد، بحيث أنهم يقومون باختراق الحاسوب أو شبكات الإنترنت، من أجل تدمير نظام الضحية أو الموقع الخاص به وإتلاف البيانات والمعلومات الخاصة به وهؤلاء المجرمون لديهم خبرة واسعة في مجال الحاسوب وبرامجه ولديهم نكاه كبير، وتكون ميولهم إجرامية هدفها الإضرار بالمجني عليهم وتحقيق مكسب مادي.

وفي دراسة للمعاهد المتخصصة في الجرائم المعلوماتية تبين أن مرتكبي الجرائم المعلوماتية هم غالباً من الشباب الذين تتراوح أعمارهم ما بين العشرينات إلى الأربعينات،

^{١٩٢} خاطر، مايا، الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، مج ٢٧، ع ٣٤، ٢٠١١، ص ٥١٢.

وتبين أيضاً أن (٢٥%) من الجرائم المعلوماتية يتم ارتكابها من قبل المحلل، و(١٨%) يرتكبها المبرمج، و(١٧%) يرتكبها المستخدم للنظام، و(١٢%) يرتكبها أجنبي عن المكان والنظام، و(١١%) ترتكب في مرحلة التشغيل^{١٩٣}.

وهنا نود الإشارة إلى أن هنالك مخترقون أخلاقيون بحيث أنهم يعملون للمصلحة العامة، كالمخترقين الذين يقومون باختراق المواقع الإباحية وتدميرها، والمواقع التي تقوم بنشر الطائفية والعنصرية فهؤلاء مخترقين هم بالفعل يخدمون الصالح العام، وكذلك الأمر هناك مخترقين تقوم بتوظيفهم الشركات الكبيرة من أجل كشف الثغرات الموجودة داخل موقع الشركة وذلك بهدف إغلاق تلك الثغرات حمايةً من المخترقين أصحاب النوايا السيئة والذين يطالبون الشركات من خلال استغلالهم لتلك الثغرات بمبالغ مالية طائلة^{١٩٤}.

نود أن نشير أيضاً بصورة سريعة إلى من هو المجرم المعلوماتي وما هي الخصائص التي يتميز بها عن غيره من المجرمين التقليديين. يمكن القول بأن المجرم المعلوماتي:- هو كأي مجرم يقوم بارتكاب جريمة، لكنه يختلف عن المجرم التقليدي في أن المجرم المعلوماتي يتمتع بصفات خاصة تميزه عن المجرم التقليدي، ويرتكب جريمة معاقب عليها قانوناً، كما أنه هو الذي يمارس وظيفته الإجرامية في مجال الحاسب الآلي، حيث يكون انساناً

^{١٩٣} البلوي، شيخة، المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية للدولة في النظام السعودي مقارنة بالقانون الإماراتي رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ٢٠١٦، ص ٣٢+٣٣.

^{١٩٤} عفون، حمزة، مرجع سابق، ص ٣٩.

اجتماعياً يعيش داخل المجتمع ويقوم بممارسة حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية، كما أنه شخص محترف يتمتع بقدر كبير من الحنكة والذكاء^{١٩٥}.

يتمتع المجرم المعلوماتي بسمات وخصائص تميزه عن المجرم التقليدي وهي كالآتي:-

أ_ المهارة.

تعتبر سمة خاصة يتميز بها المجرم المعلوماتي عن المجرم التقليدي، فهي صفة قد يكتسبها من خلال دراسته الجامعية في هذا المجال أو من خلال هواية مكتسبة ولا يشترط أن يكون المجرم المعلوماتي قد تلقى المهارة من خلال الدراسة أو الخبرة، لكن قد يكون تفاعله مع الآخرين ممن لديهم خبرة في هذا المجال أثر كبير في تقوية مهارته التقنية. نخلص للقول بأن المجرم المعلوماتي يتمتع باحترافية ومهارة عالية في تنفيذ جريمته، فهو يرتكب هذه الجرائم عن طريق جهاز الحاسوب وهذا يتطلب منه الكثير من الدقة والتخصص والاحترافية في هذا المجال للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسوب^{١٩٦}.

ب_ المعرفة.

بمعنى أنه يجب أن يكون لدى المجرم المعلوماتي المعرفة الكافية بجهاز الحاسوب، وأن يكون على علم بكافة الظروف التي تحيط بالجريمة المعلوماتية من حيث احتمالية نجاحها أو

^{١٩٥} العريان، محمد، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر، ٢٠٠٤، ص٦٢.

^{١٩٦} قطب، محمد، بحث بعنوان "الجرائم المعلوماتية وطرق مواجهتها"، الأكاديمية الملكية للشرطة، البحرين، ٢٠١٠، ص٨.

فشلها، فقد يقوم المجرم بتطبيق تلك الجريمة مسبقاً على نظام حاسوب آخر لكي يتأكد من نجاح أو فشل تلك الجريمة.

ج_ الذكاء.

يتمتع المجرم المعلوماتي بذكاء يميزه عن المجرم التقليدي، فهو يمتلك مهارات تؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية، ونرى أن المجرم المعلوماتي يتميز بالذكاء بجريمته الإلكترونية، ذلك أنه لا يترك أي أثر مادي في مسرح الجريمة بحيث يمحو كل دليل يوقعه بالفخ. وهذا ما دفع بعض القانونيين إلى وصف المجرمين المعلوماتيين بإجرام الأنكباء مقارنةً بالمجرمين التقليديين الذين يميلون للعنف في أغلب الجرائم التي يرتكبوها^{١٩٧}.

المطلب الثاني

أشكال ودوافع الإختراق وخصائصها.

إن فئات مرتكبي الجرائم التقليدية تختلف عن فئات مرتكبي الجرائم الإلكترونية، فكما هو معروف فإن لكل جريمة شكلها الخاص وخصائصها الخاصة بها، فإنه ومن الطبيعي أن نرى بأن دوافع الجرائم الإلكترونية تختلف عن دوافع الجرائم التقليدية.

^{١٩٧} البلوي، شيخة، مرجع سابق، ص ٤٤.

في هذا المطلب سوف نتحدث عن أشكال ودوافع جريمة الاختراق والخصائص التي تتميز بها جريمة الاختراق عن الجرائم الأخرى.

• الفرع الأول:- أشكال جريمة الاختراق.

تحدثنا سابقاً عن جريمة الاختراق، واستتجنا في نهاية المطاف بأن جريمة الاختراق هي عملية دخول غير مشروعة لأجهزة الحاسوب ولشبكات الإنترنت المختلفة، وذلك بهدف إحداث ضرر في جهاز الضحية أو في الموقع الخاص بالمجني عليه، وذكرونا أيضاً أنه ليس باستطاعة أي شخص أن يكون مخترقاً، فالمخترق هو انسان طبيعي ولكن عقلية الانسان وذكائه يختلف من انسان لآخر، فالمخترق يتمتع بذكاء عالي ولديه الدراية الكاملة في برامج الحاسوب. لجريمة الاختراق اشكال عديدة سوف نتحدث عنها على النحو الآتي:-

أولاً_ اختراق البريد الإلكتروني.

يعتبر البريد الإلكتروني وسيلة من وسائل الاتصال والتواصل بين الشركات والأفراد، وتعود بدايات ظهور البريد الإلكتروني إلى فترة تطور وظهور شبكة (ARPANET)، كان لسهولة استخدام البريد سبباً في الإقبال الكبير عليه من قبل المجتمع والشركات التجارية والمؤسسات الحكومية وهو ما جعله عرضة لأن يكون محل اختراق من قبل المجرمين ذوي الخبرة والكفاءة العالية في مجال الاختراق. لقد أصبح البريد الإلكتروني وسيلة لحفظ المعلومات والبيانات وتبادلها بين الأفراد والشركات والمؤسسات، وهذا ما جعله عرضةً لأن يتم اختراقه من قبل مخترقين وهدفهم بذلك هو الحصول على تلك البيانات والمعلومات السرية الخاصة

بمستخدم البريد الإلكتروني، وعند حصولهم على تلك المعلومات والبيانات يقومون إما بتهديد صاحبها أو (ابتزازها) بنشر تلك المعلومات إن لم يقد بدفع مبلغ معين من المال أو أن يقوموا بنشرها على الإنترنت من أجل فضح صاحب تلك المعلومات. أذكر مثلاً على ذلك ما حدث مع الرئيس السوري بشار الأسد عندما قام مجموعة مخترقين باختراق بريده الشخصي وتسريب رسائل خاصة به^{١٩٨}. وكان أول حكم قضائي لجرائم الإنترنت في الوطن العربي بتاريخ (٢٠٠٨١١٢١٢٣) حيث أصدرت محكمة الإحصاء شمال شرق السعودية بسجن شاب سعودي وقلده وتغريمه بعد أن تبين أنه قام باختراق بريد إلكتروني يعود لفتاة سعودية حيث قام بسحب صورها وابتزازها بتلك الصور^{١٩٩}.

ثانياً_ اختراق الهاتف.

كان للتطور العلمي الكبير، ونتيجة لانتشار الهواتف الذكية بشكل كبير جداً في مختلف أنحاء العالم ونتيجة لاتصال تلك الهواتف بشبكة الإنترنت، فقد أصبح كل شخص يستخدم الهاتف عُرضة للاختراق من قبل المجرمين بدءاً من التنصت على مكالماته ومحادثاته مروراً بسرقة الصور أو الفيديوهات أو المراسلات أو حتى تعطيله عن العمل وضربه بالفايروسات، وقد يتم اختراق الهاتف من خلال إرسال رسائل تكون ملغمة بفايروسات ويكون لها القدرة على تدمير الهاتف بالكامل.

^{١٩٨} الغفيلي، فهد، دورة تدريبية حول توظيف التقنيات الحديثة في العمل الأمني، مداخلة بعنوان "استخدام الحاسب الآلي في الوقاية من الجريمة (جرائم الاختراق نموذجاً)"، جامعة نايف العربية للعلوم الأمنية، تاريخ الانعقاد (٦-٢٠١٣/٣١٢-٢٠١٣). ص ٤.
^{١٩٩} فتحية، رصاع، مرجع سابق، ص ١٨٣.

ثالثاً_ اختراق الحواسيب الشخصية.

تعتبر هذه الجريمة الأكثر انتشاراً على مستوى العالم، وذلك لأسباب عديدة منها:- سهولة اختراق الحاسوب بسبب ضعف استخدام المستخدم للحاسوب، أو قد يكون بسبب دخوله إلى مواقع على شبكة الإنترنت بحيث تنبثق نوافذ وقد تكون تلك النوافذ ملغمة بفايروسات تؤدي إلى تدمير الحاسوب أو تعطيله بالكامل، سبب آخر لسهولة اختراق الحاسوب هو أن مستخدم الحاسوب قد يستخدم كلمة مرور ضعيفة، أو أنه دخل إلى مواقع غير موثوقة وروابط غير آمنة، كذلك عدم وجود أنظمة حماية ضد برامج الاختراق وضد الفايروسات هذا كله يجعل الحاسوب عرضة للاختراق بشكل قوي.

رابعاً_ اختراق الشبكات.

تعتبر الشبكات وسيلة من وسائل نقل البيانات والمعلومات لذلك فمن الواجب أن يتم ضمان أمنها من الاختراق لكي تصل المعلومات والبيانات بسلامة ودون أي اعتراض، والشبكات لها أنواع عديدة:- فقد تكون شبكة محلية "منزلية" وهي شبكة تربط عدة حاسبات داخل منطقة معينة، ويتم اختراقها من أجل تحقيق أهداف خاصة، فقد يكون اختراق تلك الشبكة من أجل تدميرها وتعطيلها أو من أجل سرقة بيانات خاصة بتلك الشبكة، وقد تكون شبكة تخص عمل مؤسسة حكومية أو شركة، بحيث يكون الهدف من ذلك الاختراق هو تعطيل عمل المؤسسة أو من أجل الوصول إلى البيانات الخاصة بها من أجل ابتزاز تلك الشركة إما بنشرها أو بدفع مبلغ مالي معين مقابل عدم نشر تلك البيانات والمعلومات، وقد يصل الاختراق إلى شبكات

ضخمة جداً كشبكات الكهرباء، وشبكات المياه، بحيث يستطيع المخترق أن يسيطر على الشبكة، وبالتالي يكون له القدرة بالتحكم في إدارتها وتغيير إعداداتها أو قد يقوم بالوصول للبيانات والمعلومات من أجل الحصول على نسخة منها لأغراض قد تكون سياسية أو استخباراتية أو ما شابه من هذا القبيل، وقد يقوم بإتلاف البيانات وتدميرها. ويذكر الباحث مثلاً لقائد قيادة الإنترنت في البنتاغون الجنرال كيث ألكسندر حيث أنه حذر من هجوم إلكتروني يشل واشنطن، وقال إنه تقدم بطلب إلى الرئيس الأمريكي السابق باراك أوباما لمنحه سلطات إدارة شبكات الإنترنت في واشنطن، وذلك خوفاً من وقوع هجوم إلكتروني، ولضمان حماية أنظمة الحاسب في البلاد في حالة وقوع هجوم كبير، مضيفاً إلى أنه إذا استطاع العدو اختراق شبكة الكهرباء في واشنطن وفي بقية أنحاء الولايات المتحدة، أو غيرها من المؤسسات الحيوية، فإنه سيصدر على الأرجح أمر إغلاق، ويضيف:- إن الموضوع ليس حماية شبكات الحاسب العسكرية فقط، ولكن حماية الأمة كلها^{٢٠٠}.

خامساً_ اختراق مواقع الإنترنت.

لقد ساهم تطور الإنترنت وانتشاره بشكل كبير إلى انتشار مواقع الإنترنت وقد أدى ذلك التطور إلى ظهور ثغرات أمنية، وهذه الثغرات تشكل تهديداً على إدارة الموقع ليس وحدهم فقط، وإنما تهدد أيضاً كافة مستخدمي تلك المواقع، وهذا يشكل خطر على اقتصاد وأمن

^{٢٠٠} خبر منشور على جريدة الشرق الأوسط تحت عنوان "قائد قيادة الإنترنت في البنتاغون يحذر من هجوم إلكتروني يشل واشنطن، تاريخ النشر (٢٥/١٠/٢٠١٠م)، تاريخ الدخول (١٧/١١/٢٠١٠م).

<http://archive.aawsat.com/details.asp?issueno=11700&article=588253#.Wz8vf9LXI>

dU

الدول. نخلص للقول أن اختراق مواقع الإنترنت من الاختراقات التي تحدث بشكل كبير جدا في الوقت الحالي، لسهولة اختراق تلك المواقع والسبب في ذلك هو أن مواقع الإنترنت قد تكون الحماية فيها ليست قوية لوجود ثغرات غير ظاهرة لأدارة الموقع، بحيث يستغل المخترقين تلك الثغرات ويقومون بهجارتهم الإلكترونية ضد تلك المواقع.

• الفرع الثاني :- دوافع جريمة الإختراق.

مما لا شك فيه أن الجريمة هي ظاهرة اجتماعية، حيث أنه لا يوجد مجتمع على وجه الأرض يخلو من الجريمة مهما بلغ من التطور والتقدم والرقي، إن لتنازع المصالح أثر كبير في ظهور الجريمة وارتكابها وبالتالي مخالفة القانون والإضرار بالمصالح التي حماها القانون وتحقيق الأهداف بطريقة غير مشروعة. عُرف المجرم المعلوماتي بأنه:- هو الشخص الذي يتمتع بمهارة ومعرفة عالية وعند ارتكابه للجريمة يبررها بمبررات مختلفة لأنه يخاف من كشف جريمته^{٢٠١}. إذا قارنا من بين الجريمة التقليدية والجريمة الإلكترونية سنجد بأن المجرم في كلتا الجريمتين يكون له دوافع وغايات يسعى لتحقيقها من خلال ارتكابه للجريمة سواء كانت تقليدية أم إلكترونية وهذا ما سنتحدث عنه في هذا الفرع.

الباعث(الدافع):- عرفها د. مصطفى زيدان بأنه:- حالة فسيولوجية وسيكولوجية داخل نفسية الفرد، بحيث تجعله يقوم بأنواع معينة من السلوك الإجرامي... إلخ^{٢٠٢}. أما نحن فنعرّف الدافع

^{٢٠١} سعيدة، بكرة، الجريمة الإلكترونية في التشريع الجزائري دراسة مقارنة، مذكرة ماستر غير منشورة، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٦، ص٩.
^{٢٠٢} الوهاب، سرور، الدافع والباعث على الجريمة وأثرهما في العقوبات التعزيرية، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم والأمنية، ٢٠٠٤، ص٢٠.

بأنه: - عبارة عن قوة داخلية كامنة في نفس المجرم تجبره على القيام بسلوك خارجي يؤدي إلى ارتكاب الجريمة. ويعتبر الدافع أو "الباعث" كمحرك المركبة الذي يجعلها تعمل بناءً على حركة إرادية صادرة عن سائق المركبة، فالدافع في الجريمة هو محرك لإرادة المجرم فهو الذي يوجه السلوك الإجرامي إلى القيام بارتكاب الجريمة بناءً على حركة عضوية إرادية. إن لمعرفة الدافع أو الباعث على ارتكاب الجريمة أثر كبير في دراسة وتحليل شخصية المجرم وبالتالي معرفة الأسباب الكامنة وراء قيامه بارتكاب الجريمة ومن خلالها الوصول إلى إيقاع العقوبة المناسبة للمجرم بما يتوافق مع الجريمة المرتكبة وهذا يسهم بشكل رئيسي في تحقيق العدالة والحفاظ على مصالح الأفراد والمجتمع. إذاً الدافع في الجرائم المعلوماتية لا يختلف عن الدافع في الجريمة التقليدية، حيث أن الدافع أو الباعث ليس عنصراً من عناصر الجريمة، فالجريمة موجودة سواءً توافر الباعث أو انتفى، كل ما هنالك أن للباعث أثر في تشديد العقوبة أو تخفيفها فقط، وقد يكون دافع ارتكاب الجريمة شخصي وقد يكون دافع خارجي كل مصدر هذه الدوافع هو الرغبة الإجرامية، ما هو معروف أن الحاجات تسبق عادةً الدوافع، فحاجة الإنسان المجرم تنشأ نتيجة شعوره بنقص ما أو شعوره بأنه محروم من شيء كفله القانون للفرد، وهذا بعد ذاته يؤدي إلى التأثير بشكل كبير على نفسيته الداخلية وبالتالي يتشكل لديه دافع قوي لأن يقوم بممارسة عمل إجرامي نهى عنه القانون، وذلك من أجل إشباع حاجته ولكي يسد الفراغ أو النقص الذي يشعر به من خلال حالة الرضاء النفسي لديه، إن دوافع القيام بارتكاب الجريمة الإلكترونية هو مختلف باختلاف منفيها، وتبعاً لخبرته في مجال المعلومات والإنترنت، حيث يمكن تصنيف هذه الدوافع إلى صنفين دوافع شخصية ودوافع خارجية، وهو ما سنتحدث عنه بشكل تفصيلي.

أولاً_ الدوافع الشخصية.

يمكن إجمال الدوافع الشخصية لدى مرتكب الجريمة المعلوماتية إلى دوافع مالية، وأخرى دوافع ذهنية.

أ_ الدوافع المالية (تحقيق الربح والكسب المالي).

تعتبر الدوافع المالية من أكثر الدوافع تحفيزاً للمجرم لكي يقوم بارتكاب جريمته، حيث يشعر أنه ومن خلال ارتكابه للجريمة سوف يحصل على المال الكثير والربح الكبير وهذا يشجع المجرم المعلوماتي على مواكبة التطور والتقدم التكنولوجي في مجال الحاسوب والإنترنت لكي يكون باستطاعته إيجاد كافة الثغرات من أجل الإستفادة منها لكي يحصل على المال. ويكون تحقيق الدافع المالي عن طريق اختلاس المعلومات ثم المساومة عليها، أو استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية^{٢٠٣}. وقد أشارت مجلة الأمن المعلوماتي (Securite informatique) أن (٤٣%) من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و (٢٣%) من أجل سرقة معلومات و (١٩%) أفعال إتلاف و (١٥%) الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية^{٢٠٤}. إذا نفهم بأن الإنسان لديه حب كبير للمال وهذا ما أكده الله سبحانه وتعالى في كتابه العزيز " **وَتُحِبُّونَ الْمَالَ حُبًّا جَمًّا**"^{٢٠٥} فحب المجرم للمال هو ما يشجعه على ارتكاب الجرائم بمختلف أنواعها. مما نخلص

^{٢٠٣} سندالي، عبد الرازق، مداخلة بعنوان "التشريع المغربي في مجال الجرائم المعلوماتية"، قدمت لندوة تحت عنوان الجرائم المتصلة بالكمبيوتر، المملكة المغربية، تاريخ الإنعقاد (٢٠١٩\٤\٢٠٠٧).

^{٢٠٤} المومني، نهلا، مرجع سابق، ص ٩٠.

^{٢٠٥} أنظر سورة الفجر، الآية رقم (٢٠).

للقول بأنه في حال نجاح المجرم المعلوماتي في ارتكاب جريمته المعلوماتية فإن ذلك سيدر عليه أرباحا كبيرة وفي زمن قياسي^{٢٠٦}. إذا أراد الإنسان العادي أن يصبح ثرياً في الوقت الحالي فإنه سيواجه صعوبات بالغة لكي يستطيع تحقيقها بالطرق القانونية والمقبولة اجتماعياً، لكنه قد يلجأ إلى الجرائم الإلكترونية وهي طريقة غير قانونية نهى القانون عن القيام بها وعاقب عليها، وذلك لسهولة تنفيذها وإمكانية محو الدليل والمستهدف فيها مجتمع بأكمله وليس أفراد أو مؤسسات معينة، ففي الجرائم الإلكترونية كل شخص يستخدم الحاسوب والإنترنت هو معرض للاختراق في أي لحظة^{٢٠٧}.

ب_ الدوافع الذهنية.

في الواقع نرى أن المجرم المعلوماتي يقوم عادة بارتكاب الجريمة الإلكترونية، وذلك من باب إحساسه وشعوره بأنه له القدرة على القيام بذلك الفعل، ومن باب أيضاً إثباتهم للذات ووضع بصماتهم ومن أجل مواجهة التطور والتقدم التقني في الحاسوب والإنترنت، ولكي يظهروا قدراتهم بالتفوق على ذلك التقدم، ولا يكون لديهم أي ميول سلبية إتجاه تلك الأفعال وإنما وكما أشرنا هو من أجل إثبات قدرتهم على الاختراق والدخول للنظام في أي لحظة يشاؤون، فهم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه في حال ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف في قهر النظام أكثر من شهوة تحقق

^{٢٠٦} سعيداني، نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر غير منشورة، جامعة الحاج باتنة، الجزائر، ٢٠١٣، ص ٦١.
^{٢٠٧} ياسمين، بونغارة، الجريمة الإلكترونية، مذكرة ماستر منشورة، جامعة الأمير عبد القادر للعلوم الإسلامية، الجزائر، ٢٠١٥، ص ١١.

النتيجة، فيحاولون جاهدين لإيجاد الوسيلة التي يستطيعون من خلالها تحطيمها والتفوق عليها^{٢٠٨}. نخلص للقول أن مجرموا الجرائم المعلوماتية لديهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، ففي بعض الأحيان نجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي^{٢٠٩}. وقد بلغت نسبة ارتكاب الجريمة الإلكترونية بسبب الحب بالرغبة في إثبات الذات إلى (٣٠%) موزعة كالاتي (٣١.٠%) للذكور في مقابل (٢٩.٠%) للإناث^{٢١٠}.

ثانياً_ الدوافع الخارجية.

قد يتأثر المجرم المعلوماتي ببعض المواقف التي تكون سبباً في القيام بالفعل الإجرامي، فهو بتلك الأسباب لا يكون جاهداً لحصوله على المال ولا يقوم بهذا الفعل الإجرامي من باب التسلية ولا من باب إثبات قدرته على خرق كل تطور يظهر على التقنيات، وإنما يقوم بذلك الفعل من باب دوافع خارجية كالانتقام من شخص ما أو من مؤسسة ما وقد يكون دافع سياسي. وكما هو معروف فإن المجرم يتأثر بالعوامل الاجتماعية المحيطة به والتي تكون سبباً في حدوث وارتكاب الجريمة^{٢١١}.

^{٢٠٨} غايب، محروس، الجريمة المعلوماتية، بحث منشور في مجلة التقني بجامعة هيئة التعليم التقني، مج ٢٤، ٩٤، ٢٠١١، الأنبار، العراق، ص ١٠٥.
^{٢٠٩} فتحية، رصاع، مرجع سابق، ص ٦٦.
^{٢١٠} نصار، غادة، الإرهاب والجريمة الإلكترونية، دار العربي للنشر والتوزيع، القاهرة، مصر، ٢٠١٧م، ص ١٦٢.
^{٢١١} عبدالله، نوري، بحث منشور بعنوان "العوامل الاجتماعية المؤثرة في ارتكاب الجريمة"، مجلة الأنبار للعلوم الإنسانية، ١٤، ٢٠١١، ص ١٣٢.

أ_ الإنتقام.

يعد دافع الإنتقام من أخطر الدوافع التي تجبر المجرم على القيام بعمله الإجرامي، فقد يكون دافع الإنتقام من باب الثأر أو أن يكون من باب الصاع بالصاع، وقد يتعرض موظف ما في شركة أو مؤسسة إلى الفصل التعسفي من وظيفته مع العلم أن لديه الخبرة والكفاءة العالية بالعمل فيقوم ذلك الموظف بالرد على الفصل التعسفي بقيامه بالإنتقام من تلك الشركة أو المؤسسة من خلال اختراق موقعها وتدمير ملفاتها وتعطيلها بحيث تتكبد الشركة أو المؤسسة خسائر مالية فادحة، حيث يشعر حينها ذلك الموظف الذي فصل من عمله بالرضى على العمل الذي قام به.

يفهم بأن الموظفين الذي يعملون في المؤسسات أو الشركات يتعرضون لضغوطات في العمل ولمشاكل نفسية يترتب عليها لدى الموظف رغبة في الإنتقام من تلك المؤسسة أو الشركة التي يعمل بها بحيث يقوم بتدمير ملفاتها وهذا يكبدها خسائر مالية كبيرة. وخير مثال على ذلك، قيام موظف يعمل لدى إحدى شركات التأمين بعد أن فصل منها بحجز وحدة التخزين المركزية الخاصة بالشركة كرهينة ووسيلة لكي يقوم رئيسه بإرجاعه للعمل، حيث قام بتدمير البيانات الخاصة بحسابات شركة التأمين وهو ما حصل بالفعل بعد رحيله عن العمل بعدة أشهر^{٢١٢}.

^{٢١٢} مزغيش، سمية، جرائم المساس بالأنظمة المعلوماتية، مذكرة ماستر غير منشورة، جامعة محمد خيضر بسكرة، ٢٠١٤، ص ١١.

ب_ دافع سياسي.

يعتبر الدافع السياسي من أهم الدوافع الخارجية التي تحفز المجرم على ارتكاب الجرائم الإلكترونية، فالخلافات السياسية بين الدول أو بين المعارضة والدولة نفسها أو بين الأحزاب نفسها يؤدي إلى انتهاك القانون وارتكاب الجرائم في ظل غياب الوعي وعدم تقبل وإدراك معنى الديمقراطية كوسيلة من وسائل التطور والتقدم. ويذكر الباحث مثلاً على قيام بعض القراصنة المتواجدين على الأراضي الروسية باختراق نظام الحاسبات الإلكترونية الحكومية في الولايات المتحدة الأمريكية لمدة سنة كاملة، فقاموا بسرقة معلومات غير سرية من أجهزة الحواسيب الخاصة بالعسكرية^{٢١٣}. كذلك الأمر ما قام به مجموعة مخترقين من اختراقهم لوكالة الأنباء القطرية بتاريخ ٢٠١٧/٥/٢٤، حيث اتهمت قطر الإمارات بأن المخترقين ينتمون لها، وأشارت الحكومة القطرية بأن المخترقين قاموا بنشر أخبار مفبركة عن أمير قطر الشيخ تميم بن حمد آل ثاني في الموقع الرئيسي لوكالة "قنا" وحسابات مواقع التواصل الخاصة بها، كما نشر فيديو ملفق على يوتيوب وقاموا أيضاً باختراق الحسابات الخاصة بوكالة قنا وسرقة كل حساباتها، وأشار المسؤول القطري إلى أن جريمة اختراق وكالة الأنباء القطرية تنقسم إلى ثلاثة أقسام:- أولاً_ جريمة الاختراق الوكالة والسيطرة على الشبكة وزرع الفايروسات الخبيثة، وثانياً_ قيام المخترقين بنشر الأخبار المفبركة لأمير قطر، وثالثاً_ الجهة المستفيدة من الاختراق والأخبار المفبركة هو من كان ينتظر نشر تلك الأخبار المفبركة^{٢١٤}.

^{٢١٣} فتحية، رصاع، مرجع سابق، ص ٦٧+٦٨.

^{٢١٤} خبر نشر على موقع الجزيرة، اختراق وكالة الأنباء القطرية تم من الإمارات، <http://www.aljazeera.net/portal>، تاريخ الدخول (٢٠١٨/٧/١٠)

جـ دوافع دينية (طائفية).

يعتبر الدافع الديني (الطائفي) أحد الدوافع التي ظهرت مؤخراً وبشكل كبير في العالم العربي، والسبب في ذلك هو غياب الديمقراطية وانتشار الظلم وعدم وجود القوانين التي تكفل احترام المواطن وتحقيق مصالحه، فقد ظهرت الحركات التكفيرية والتي تدعم العنصرية الطائفية. وهذا ما دفع كثير من الشباب والمراهقين للجوء إلى العنف للتعبير عن آرائهم وأفكارهم^{٢١٥}.

دـ دافع لفت الإنتباه.

وهذا الدافع قد يستخدمه بعض المخترقين من أجل توجيه الأنظار عليهم ولفت الإنتباه إليهم، فمركبوا الجرائم المعلوماتية لديهم شعور بالبحث عن القوة ولديهم الحب في إظهار التفوق على التطورات التي تحدث على تقنيات التكنولوجيا والحاسوب. وخير مثال للفت الإنتباه وهو ما قام به شاب إيراني يدعى (فرهد) حيث قام باختراق صفحة المغنية اللبنانية نانسي عجرم وقد كتب اسمه على صفحتها بأنه هو من قام باختراقها وأضاف إلى أنه معجب كثيراً بها هو وعدد كبير من الجمهور الإيراني، مطالباً منها بأن تقوم بإنتاج أغنية لإيران كما فعلت للكويت ولمصر^{٢١٦}.

^{٢١٥} إسماعيل، أيمن، خبر بعنوان دوافع الجريمة في المجتمع الفلسطيني، موقع دنيا الوطن، تاريخ النشر (٢٠١٧\١٢\٢٧م)، تاريخ الدخول (٢٠١٨\٢\١٠م).

^{٢١٦} الغفيلي، فهد، مرجع سابق، ص ٥.

• الفرع الثالث:- خصائص جريمة الاختراق.

تتميز جريمة الاختراق بخصائص مميزة باعتبارها أحد أنواع الجرائم الإلكترونية، وبما أن جريمة الاختراق تتم من خلال شبكة الإنترنت وجهاز الحاسوب فإنها تتمتع بخصائص تتميز بها عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة التنفيذ، كما تتميز أيضاً جريمة الاختراق بطابعها الدولي في أغلب الأحيان حيث تجتاز كل الحدود المرسومة بين الدول.

أولاً_ صعوبة إكتشافها وإثباتها.

تتميز جريمة الاختراق باعتبارها أحد انواع الجرائم الإلكترونية إلا أنها جريمة يصعب الكشف عنها وعدم وجود أثر لها، وهذا يرجع بطبيعة الحال إلى نكاء المخترق فهو انسان طبيعي ولكن قدراته العقلية والذهنية تختلف عن الانسان الطبيعي، فالجرائم المعلوماتية لا تحتاج إلى أي شكل من أشكال العنف ولا تحتاج إلى نزول أي قطرة من الدماء، ولا تحتاج إلى طرق لاقتحام منزل أو شركة أو بنك من أجل سرقة الأموال وإنما جريمة الاختراق تحتاج فقط لأرقام وبيانات يتم تغييرها والتلاعب بها. علاوة على صعوبة الإحتفاظ الفني بأثارها إن وجدت^{٢١٧}. فجريمة الاختراق لا تترك أي بصمة أو أثر مادي، بالإضافة إلى سهولة محو الدليل وإزالته في ثوانٍ معدودة وهذا بحد ذاته يشكل صعوبة في إقامة الدعوى أمام المحاكم النظامية الجنائية المختصة، نشير إلى أنه تم إنشاء محاكم إلكترونية ببعض الدول، وهي مختصة للنظر في

^{٢١٧} سليم، مزبود، مرجع سابق، ٩٧.

الجرائم الإلكترونية بشكل خاص، مثل المحكمة (الإلكترونية) بإمارة دبي^{٢١٨}. نخلص للقول بان الجرائم المعلوماتية لها طبيعة خاصة، ويعد التطور التكنولوجي سبباً في ذلك، الجدير بالذكر أنه انتشر حديثاً على شبكة الإنترنت مواقع مختصة بأعمال السرقة المعلوماتية واستتجار القرصنة المحترفين من أجل القيام بأعمال غير مشروعة قانونياً، مقابل الحصول على مبالغ مالية، ومما يزيد الأمر تعقيداً وسوءاً، هو أن المخترقين قد يقومون بعمليات الاختراق من خلال شبكات حواسيب ليست خاصة بهم وإنما تكون لأفراد ليس لهم أي علاقة بعمليات الاختراق^{٢١٩}.

ثانياً_ جريمة الاختراق جريمة دولية عابرة للحدود.

تتميز جريمة الاختراق بأنها جريمة دولية عابرة للحدود، بمعنى أنها جريمة غير وطنية فهي لا تعرف الحدود الفاصلة بين الدول، إذ يمكن القول بأن جريمة الاختراق هي جريمة تتم بالكتمان دون أن يكون هنالك أي أثر مادي ملموس على أرض الواقع. لقد ساهم وجود شبكة الإنترنت وانتشارها بشكل سريع إلى عدم وجود حدود بين الدول، وأصبح هناك قدرة لتبادل المعلومات والبيانات بين مختلف أنحاء العالم وأصبح من الممكن أن تتم عملية الاختراق للعديد من الدول في آن واحد^{٢٢٠}. إذا يفهم من ذلك أنه لا يوجد مساحة محددة لمسرح الجريمة الإلكترونية، لأنها لا تعترف بالحدود الجغرافية بين الدول وإنما مسرحها أصبح عالمي، وهذا بحد ذاته أدى إلى وجود مشاكل عديدة تتمثل في من هي الدولة صاحبة النظر والاختصاص

^{٢١٨} الجنبيهي، منير، ممدوح، الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٠٤، ص ١٩.

^{٢١٩} فرام، كوثر، بحث نهاية تدريب بعنوان "الجريمة المعلوماتية على ضوء العمل القضائي المغربي"، وزارة العدل، المعهد العالي للقضاء، المغرب، فترة التدريب (٢٠٠٧-٢٠٠٩)، ص ١٤.

^{٢٢٠} فريال، لعافل، مرجع سابق، ص ١٨.

القضائي بتلك الجريمة؟ وهل للدولة التي وقعت عليها جريمة الاختراق حق الاختصاص؟ وما هو القانون الواجب التطبيق؟ وهناك العديد من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام وجريمة الاختراق بوجه الخصوص^{٢٢١}. إذا أمعنا بالنظر في الاتفاقية العربية لمكافحة الجرائم الإلكترونية والتي حررت بتاريخ (٢٠١٠/١١/٢١) نرى بأن الهدف منها هو إيجاد سبل تعاون مشترك بين الدول العربية من أجل المحافظة على مصالح وسلامة أمن الدول العربية، كذلك الأمر إذا نظرنا للمادة الثالثة منها والمتعلقة بتطبيق هذه الاتفاقية نجد بأنها تنطبق على كافة الجرائم المعلوماتية ما لم ينص على خلاف ذلك، وذلك بهدف منع وقوعها والتحقيق فيها وملاحقة مرتكبيها في حالات معينة وهي:- في حالة ارتكبت في أكثر من دولة، وفي حال ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى، وفي حال ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة، وفي حال ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى. نرى بأن نصوص هذه المادة تتوافق وملائمة لكون جريمة الاختراق جريمة دولية عابرة للحدود الجغرافية، وهذه المادة تحدد الدولة صاحبة الاختصاص القضائي ومن لها الحق في النظر في تلك الجريمة بوصفها أحد انواع الجرائم الإلكترونية^{٢٢٢}..

ثالثاً_ جريمة الاختراق جريمة مستحدثة.

جريمة الاختراق جريمة مستحدثة باعتبارها إحدى أنواع الجرائم الإلكترونية المنتشرة بشكل كبير في العالم، فليس بالغريب أن نطلق على الجرائم الإلكترونية بأنها من الجرائم

^{٢٢١} فتحية، رصاع، مرجع سابق، ص ٤٣.
^{٢٢٢} مناعسة، اسامة، وآخرون، جرائم الحاسب الآلي والانترنت، دار وائل للنشر والتوزيع، ط١، عمان، الأردن، ٢٠٠١، ص ١٠٥.

المتسحثة، والسبب بذلك يرجع إلى التطور والتقدم التكنولوجي الكبير الذي شهده هذا العالم أجمع، بحيث أنه جعل العالم قرية إلكترونية صغيرة، حيث أدى هذا التقدم إلى عدم قدرة الدولة على مواكبة التطور التكنولوجي وبالتالي عدم وجود أجهزة لها القدرة على الرقابة الإلكترونية وهذا بحد ذاته شكل خطر كبير على العالم بشكل عام، فعدم وجود رقابة من قبل أجهزة مختصة وعدم وجود قوانين خاصة بتلك الجرائم من أجل ردعها ساهم بشكل كبير في تهديد مصالح وسلامة أمن الدولة وأمن المواطنين الذي يقطنون على أراضي تلك الدولة.

رابعاً_ جريمة الاختراق لا تتم إلا بجهاز حاسوب.

الهدف من ذلك هو أن جريمة الاختراق لا تتم إلا إذا تم الاتصال بجهاز الحاسوب، فهو الأداة التي يتم من خلالها ارتكاب وتنفيذ عملية الاختراق، فالمطلوب من المخترق أو المجرم المعلوماتي أن يكون على دراية كاملة بمكونات الحاسوب وإجراءات التعامل معه وأن يكون لديه الخبرة الكافية في مجاله.

خامساً_ جريمة الاختراق جريمة ترتكب بواسطة شبكة الإنترنت.

تعتبر شبكة الانترنت حلقة الوصل بين جريمة الاختراق وجهاز الحاسوب، فكما أشرنا سابقاً فالحاسوب هو الأداة التي يستطيع من خلالها المخترق البدء بالشروع للقيام بجريمته^{٢٣}.

^{٢٣} شيرين، دابنة، مقال بعنوان "الجرائم الإلكترونية القرصنة الإلكترونية"، مجلة الدراسات المالية والمصرفية- المعهد العربي للدراسات المالية والمصرفية، مج ٢٣، ع ١٤، ٢٠١٥، الأردن، ص ١٩.

وشبكة الإنترنت هي المكان الذي تتم فيها جريمة الاختراق، فمن خلال شبكة الإنترنت يتمكن المخترق من الوصول لمواقع ذات أهمية كبيرة عسكرية أو حكومية أو إلى مواقع خاصة بالبنوك والشركات وغيرها.

المبحث الثاني

نظم المعلومات والشبكة المعلوماتية

يزداد يوماً بعد يوم التطور والتقدم العلمي بمختلف مجالات الحياة، وقد ظهرت أهمية الدور الذي لعبه التطور التكنولوجي من خلال تخزينه ومعالجته للبيانات والمعلومات ذات الأهمية الكبيرة. وأصبح من الممكن الوصول إلى تلك البيانات والمعلومات في حال عدم وجود أنظمة حماية قادرة على ضمان سرية وأمن المعلومات والبيانات.

إن لنظم المعلومات أهمية كبيرة نظراً لما تحتويه من برامج وبيانات تهدف إلى إنتاج معلومات محددة، فنظم المعلومات هي مستهدفة في ارتكاب جرائم نظم المعلومات وهو ما يتطلب في التحقيق بالإطلاع على أجزاء النظام المعلوماتي سواء كانت قاعدة بيانات أو شبكات أو غيرها، فقد أسهم تطور الشبكة إلى بروز جرائم إلكترونية لم تكن تعرفها البشرية من قبل، ومع بروز تلك الجرائم أصبح من الضروري على جميع الدول أن تقوم بتوفير الأمن والحماية للمعلومات والبيانات المتوفرة على الشبكة. لقد قمنا بتقسيم هذا المبحث إلى مطلبين إثنين وهما كالتالي:-

- **المطلب الأول:- نظم المعلومات وأمنها.**
- **المطلب الثاني:- تعريف الأمن المعلوماتي.**

المطلب الأول

نظم المعلومات

إن دراسة ومعرفة نظم المعلومات يحظى بأهمية خاصة في ظل ثورة المعلومات والإتصالات، فقد أصبحت المعلومات عنصراً هاماً وأساسياً ومورداً حيويّاً تعتمد عليه المنظمات في النهوض والتقدم. حيث يعتبر موضوع نظم المعلومات من المواضيع التي ازداد الاهتمام فيها، كونه موضوع يتماشى مع متطلبات العصر الحديث، والذي يمكن أن نطلق عليه باسم (العصر الإلكتروني) والذي جعل العالم قرية صغيرة، فقرب البعيد وأصبح من السهل تبادل المعلومات والبيانات وأنت في بيتك إلى شخص آخر في دولة خارج حدود دولتك، ساهم هذا التطور إلى الحاجة الملحة لجمع البيانات و المعلومات و معالجتها و استخدامها بفعالية، فهو بمثابة المطلب الأساسي للنجاح في عصرنا الحالي والذي يتميز بالتغيرات البيئية المستمرة و المعقدة.

أنه وفي ظل التطور التكنولوجي الكبير، ازدادت أهمية نظام المعلومات فأصبحت طريقة جمع المعلومات والمعرفة تتم بطرق ومواصفات عملية وموضوعية، وأصبح من الضروري حماية تلك المعلومات والبيانات من المخترقين من خلال تشكيل أجهزة مختصة تقوم

برقابة المواقع والشبكات المهمة. لقد قسمنا هذا المطلب إلى فرعين، حيث تناولنا في الفرع الأول:- تعريف نظم المعلومات، وفي الفرع الثاني تناول الباحث مكونات نظام المعلومات.

• الفرع الأول:- تعريف نظم المعلومات.

قبل أن نُعرف نظم المعلومات سوف نوضح ما هو النظام وما هي المعلومات، وبعد ذلك نوضح ما هو المقصود بنظم المعلومات.

إن كلمة **نظام** متداولة في حياتنا اليومية بشكل كبير بين أفراد المجتمع، ويُفهم من الوهلة الأولى لكلمة نظام بأنها تعني الانضباط وعدم مخالفة القوانين والأنظمة، ومصطلح نظام نستعمله في مصطلحات عديدة كالنظام السياسي، النظام الغذائي، والنظام الاقتصادي وغيرها من الأنظمة المتعددة والمختلفة.

النظام:- يطلق عليه باللغة الإنجليزية مصطلح (Systems) وهو عبارة عن مجموعة من الأجزاء والمكونات التي تتفاعل مع بعضها البعض لتحقيق هدف معين^{٢٢٤}. و يجب أن تكون المكونات والأجزاء كلاً واحداً، فالعلاقة بين عناصر النظام هي الرابطة التي تربطها معاً من أجل تحقيق الهدف المشترك، و للنظام مدخلات وآلية لتحويل المدخلات إلى مخرجات^{٢٢٥}. ويُعرف أيضاً بأنه مجموعة من الإجراءات من أجل اتخاذ القرارات ودعم التحكم بالأعمال^{٢٢٦}.

^{٢٢٤} السديري، محمد، نظم المعلومات الإدارية، الفصل الأول مدخل إلى نظم المعلومات مفاهيم وأساسيات، جامعة الملك سعود، السعودية، ٢٠١٠، ص ٤.

^{٢٢٥} بلقاسم، مرغني، نظام المعلومات ودوره في اتخاذ القرار، مذكرة ماستر غير منشورة، جامعة قاصدي مرباح، الجزائر، ٢٠١٤، ص ٣.

^{٢٢٦} العنزي، سليمان، مرجع سابق، ص ١٣.

كما عُرفَ أيضاً بأنه عبارة عن مجموعة من الحقائق أو المبادئ أو الأجزاء المرتبطة

في أي حقل من حقول المعرفة^{٢٢٧}.

أما بالنسبة لمصطلح النظام فيعود للأصل اليوناني للكلمة (System) وتعني معاً

يكون^{٢٢٨}.

نخلص للقول أن تعريف النظام يجب أن يكون مشتملاً على عناصر منها^{٢٢٩}:-

١_ أن النظام يتكون من مجموعة من الأجزاء.

٢_ أن تكون الأجزاء على علاقة متبادلة أو متداخلة.

٣_ أن تكون الأجزاء معتمدة على بعضها البعض.

٤_ أنها تعمل معاً في سبيل تحقيق الهدف المشترك

فالنظام يقوم بتحويل المدخلات إلى مخرجات، ويمكن معرفة قيمة النظام إذا فهمنا

قيمة المدخلات وبالتالي يمكن تقدير قيمة المخرجات

المعلومات:- يطلق عليها باللغة الإنجليزية مصطلح (Information) وهي عبارة عن

بيانات وحقائق وأرقام وأوصاف تساعد الإدارة على تصور ما يحدث من ظواهر وأحداث وصولاً

إلى التنبؤ الدقيق بما يمكن أن يحدث في المستقبل ومن يكون في إمكان الإدارة تعظيم قدراتها

^{٢٢٧} الصيرفي، محمد، نظم المعلومات الإدارية، دار الفكر الجامعي للنشر والتوزيع، الإسكندرية، مصر، ٢٠٠٥، ص٢٥.

^{٢٢٨} هاشم، غسان، أثر كفاءة نظم المعلومات في تحسين فاعلية عملية صنع اتخاذ القرارات، أطروحة دكتوراة غير منشورة، جامعة سانت كليمينتس العالمية (المكلا، اليمن، ٢٠١٣، ص٤٠.

^{٢٢٩} بلقاسم، مرغني، مرجع سابق، ص٤.

على إجراء الاتصالات الإدارية واتخاذ القرارات ورسم الخطط الملائمة والرقابة على أوجه النشاط^{٢٣٠}.

وعُرفت أيضاً المعلومات بأنها:- نتاج لمجموعة من البيانات المنظمة بطريقة هادفة بما يجعل لها قيمة إضافية على قيمة البيانات نفسها، وهي مخرجات ناتجة من معالجة البيانات تسهل في اتخاذ قرار أو إصدار حكم بشكل أفضل^{٢٣١}. كما وتعرف أيضاً المعلومات بأنها بيانات قد تم تحويلها ومعالجتها بحيث يكون لها معنى وقيمة حقيقية أو مدركة بالنسبة لمتخذ القرار^{٢٣٢}.

بعد توضيح الفرق بين النظام والمعلومات سوف نتحدث الآن عن تعريف نظم المعلومات.

نظم المعلومات.

لقد ظهر مفهوم نظم المعلومات وازدادت أهميته بعد التطور الذي شهده العالم في وسائل الاتصال، وبعد ظهور الحاسب الآلي وتطوره. وقد تنوعت التعريفات التي تحدثت عن نظم المعلومات. فقد ازداد إهتمام العالم بنظم المعلومات لما فيها من أهمية في صنع القرار.

يقصد **بنظم المعلومات**:- بأنه مجموعة من الإجراءات التي تقوم بجمع واسترجاع وتشغيل وتخزين المعلومات من أجل دعم اتخاذ القرارات والرقابة بالتنظيم، كذلك تهدف لتدعيم

^{٢٣٠} المصري، أحمد، الإتصالات والقرارات وفعاليتها في الإدارة، دار القلم للنشر والتوزيع، الكويت، ١٩٨٩، ص٢٠٢.

^{٢٣١} عمار، زكريا، مرجع سابق، ص١٥.

^{٢٣٢} السديري، محمد، مرجع سابق، ص٤.

اتخاذ القرارات والتنسيق والرقابة، ويمكن لنظم المعلومات أن تساعد المدراء والعاملين في تحليل المشاكل وخلق المنتجات الجديدة^{٢٣٣}.

وتُعرف أيضاً **نظم المعلومات بأنها**: - مجموعة من الإجراءات والبرامج والأفراد والأجهزة والاتصالات وقاعدة البيانات التي تهدف إلى إنتاج معلومات محددة^{٢٣٤}.

وهي أيضاً مجموعة منظمة من الموارد التي تتكون من مواد وبرامج وأفراد وإجراءات مساعدة على الاكتساب، وتخزين وتواصل معلومات على شكل بيانات، ونصوص وصور وأصوات. وهو ما يعني أن نظام المعلومات عبارة عن مجموعة من العناصر المتداخلة أو المتفاعلة بعضها مع البعض والتي تعمل على جمع مختلف البيانات و المعلومات و تخزينها و بثها و توزيعها على المستخدمين بغرض دعم القرارات، وتأمين التنسيق والسيطرة على المنظمة، أو الجهة المستفيدة. ويمكن الإضافة إلى أن نظام المعلومات يقوم بتحليل المشكلات وتأمين النظرة المتفحصة على الموضوعات المعقدة^{٢٣٥}.

وقد عُرفَ نظام المعلومات (Information System) بأنه مجموعة من العناصر والمكونات المترابطة مع بعضها البعض تجمع البيانات وتعالجها وتخزنها وتخرج المعلومات حسب الطلب. نفهم من ذلك أن نظام المعلومات عبارة عن مجموعة من القواعد والإجراءات

^{٢٣٣} البكري، سونيا، نظم المعلومات الإدارية والمفاهيم الأساسية، الدار الجامعية للنشر والتوزيع، الإسكندرية، مصر، ٢٠٠٠، ص ١٤.

^{٢٣٤} غراب، كامل، حجازي، فادية، نظم المعلومات الإدارية، مكتبة ومطبعة الأشعاع الفنية، ط ٢، الإسكندرية، مصر، ٢٠٠٠، ص ٩٠.

^{٢٣٥} قنديلجي، عامر، الجنابي، علاء الدين، نظم المعلومات الإدارية، دار الميسرة للنشر والتوزيع، عمان، الأردن، ٢٠١٨، ط ٩، ص ٢٧.

المحددة والتي صممت من أجل القيام بتلك الإجراءات ويتم استخدامها بمساعدة تجهيزات المعلومات، فهي تلعب دور الشبكة التي تقوم من خلالها بعمل النظم الأخرى^{٢٣٦}.

نشير إلى ضرورة توضيح المقصود بنظام المعلومات المحوسبة (الحاسوبي)

(Computerize Information System) فهو ذلك النظام الذي يعتمد على المكونات

المادية (Hardware) والمكونات البرمجية (Software) للحاسوب في معالجة البيانات وبث

واسترجاع المعلومات^{٢٣٧}. يفهم من ذلك أن الحاسوب يتم تغذيته بالبيانات لكي يتم معالجتها

وتحويلها إلى مخرجات حيث يتم تغذية الحاسوب بالمدخلات وهي البيانات ويتم معالجتها

وتحويلها إلى مخرجات تعرض على شاشة الحاسوب بناءً على طلب المستخدم.

وتعتبر وحدة المعالجة إحدى وحدات المكونات المادية، ونقصد بالمعالجة أي معالجة

البيانات (المدخلات) وتحويلها إلى (مخرجات) وتقوم فكرتها على معالجة البيانات حسب

التعليمات التي تكون موجودة بالبرنامج، بحيث تقوم بإرسالها إلى وحدة الذاكرة أو إلى وحدة

الإخراج^{٢٣٨}. فهي تعتبر بمثابة الجهاز العصبي للحاسوب أو العقل المشغل والمسيطر على

عمل باقي الوحدات، وتتكون وحدة المعالجة المركزية من وحدة الحساب والمنطق، ووحدة

التحكم، والمسجلات^{٢٣٩}.

^{٢٣٦} عمار، زكريا، مرجع سابق، ص ١٥.

^{٢٣٧} تم جمع هذه المعلومات من محاضرة عن نظم المعلومات في جامعة الأندلس الخاصة للعلوم الطبية،
طرطوس، سوريا، ص ١٤٩، http://au.edu.sy/images/courses/pharmacy/1-2/153_computer-skills.pdf، تاريخ الدخول (٢٠١٨\١٣\١٣).

^{٢٣٨} مهنا، عبد الوهاب، مرجع سابق، ص ٣٠.

^{٢٣٩} العريان، محمد، مرجع سابق، ص ٥٦+٥٧.

لقد أشرنا لتوضيح البرمجيات بالفصل الأول من الرسالة، ولكن من باب الإستزادة قمنا بالمرور إليها بشكل سريع. فتعتبر البرمجة أو البرمجيات إحدى المكونات الرئيسية لجهاز الحاسوب. فالبرمجيات هي التي تعمل على تشغيل المكونات الفيزيائية للحاسب الآلي، وهي مجموعة البرامج التي تستخدم لتشغيل جهاز الحاسوب والاستفادة من إمكانياته المختلفة في إدخال البيانات والبرامج وتخزينها والاستفادة منها^{٢٤٠}.

نخلص للقول بأن نظم المعلومات المحوسب (الحاسوبي) هو ذلك النظام الذي يتكون من مكونات الحاسوب المادية (Hardware) والمكونات البرمجية (Software) حيث تكمل هذه المكونات بعضها البعض في إدخال البيانات (المدخلات) ومعالجتها وتحويلها إلى (مخرجات) بحيث يتم عرض هذه المخرجات على شاشة الحاسوب بناءً على أوامر من قبل المستخدم.

• الفرع الثاني :- مكونات نظام المعلومات.

يتشكل نظام المعلومات من مجموعة من المكونات التي يقال عنها بأنها الأساس المكون لنظم المعلومات، حيث تترابط جميع هذه المكونات من أجل ادخال ومعالجة البيانات والمعلومات، ويتشكل نظام المعلومات من حواسيب آلية، وقاعدة بيانات، وبرامج، وشبكات، وأفراد يكونوا مختصين بكيفية التعامل مع النظام، بحيث أنهم يهدفون إلى إنتاج معلومات جديدة يتم عن طريقها تنفيذ وتوفير المعلومات المطلوبة من أجل دعم عملية القرار.

^{٢٤٠} حسين، عبد الرحمن، مرجع سابق، ص ٩.

أولاً_ الأفراد.

يعتبر الأفراد هم حجر الأساس، فنجاح وتقدم المؤسسات والأنظمة وغيرها يعتمد على وجود أفراد لديهم خبرة وكفاءة عالية في الإدارة والتنظيم، فالعمل الأساسي لنجاح أو فشل نظم المعلومات يتمثل في كوادر من الأفراد ممن لديهم الخبرة والكفاءة.

حيث يمكن تقسيم الأفراد إلى مختصون بنظم المعلومات وهم الأفراد الذين يقومون بتطوير وتشغيل وإدارة وصيانة نظام المعلومات، ويشكلون وضعاً إدارياً كبيراً في إدارة نظم المعلومات، ووظيفتهم هي تطوير النظم وتطوير البرامج وإدارة كافة العمليات الحسابية والبيانات.

هناك أنواع من الأفراد المختصين في نظام المعلومات، فهناك محللو النظام بحيث تكون وظيفتهم في بناء نظم جديدة وإحداث تطورات على النظام فهم مختصون في المجال التكنولوجي. كما ويتعاونوا مع المبرمجين والمستخدمين في بناء نظم المعلومات^{٢٤١}، أيضاً يوجد المبرمجين وهم مختصين بالمجال التكنولوجي حيث تكون وظيفتهم اعداد البرامج من أجل تحويل البيانات إلى معلومات^{٢٤٢}، وهناك مختصين في الشبكات بحيث تكون وظيفتهم إنشاء شبكات على الإنترنت وإدارتها^{٢٤٣}، ويوجد أيضاً فئة يمكن أن نطلق عليها اسم المستفيدون من النظام وهؤلاء ليسوا مختصين بشيء وإنما يستفيد هؤلاء من المعلومات الموجودة بالنظام سواء كانت داخله أو خارجه^{٢٤٤}.

^{٢٤١} العنزي، سليمان، مرجع سابق، ص ٣٩.
^{٢٤٢} الدنف، أيمن، الدنف، أيمن، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير غير منشورة، الجامعة الإسلامية/غزة، كلية التجارة، ٢٠١٣، ص ٢٧.
^{٢٤٣} العنزي، المرجع السابق، ص ٣٩+٤٠.
^{٢٤٤} الدنف، المرجع السابق، ص ٢٧.

ثانياً_ المكونات التقنية.

حيث تشمل المكونات الملموسة وغير الملموسة، حيث تضم المكونات المادية للحاسوب (Hardware) وتشمل كل أنواع الحاسوب وما يتبعه من معدات خارجية كالطابعة والفأرة والكييبورد وأي شيء تستحدثه التكنولوجيا الحديثة^{٢٤٥}، وهناك المكونات البرمجية للحاسوب (Software) وتشمل على المكونات غير الملموسة كالبرامج والتطبيقات ونظم التشغيل المختلفة^{٢٤٦}.

ثالثاً_ الشبكات.

للشبكات أنواع فمنها الشبكات المحلية، والشبكات الواسعة، والشبكات الخارجية، وتشتمل أيضاً الشبكات على تكنولوجيا الاتصالات ، والتي أصبحت مهمة في إدارة الأعمال الإلكترونية والأعمال التجارية بكل أنواعها عبر نظام معلوماتي موجود بالمنظمة. وتتشكل شبكة الحاسوب من خلال ربط مجموعة أجهزة حاسوب ببعضها البعض، وذلك باستخدام وسائط الاتصال لكي يتم تكوين شبكة يتم من خلالها تبادل البيانات والمعلومات عليها بين نظم الحاسوب المرتبطة بالشبكة^{٢٤٧}. وتظهر أهمية الشبكات في أنه لا يوجد فائدة لجهاز حاسوب دون أن يكون متصلاً بالشبكة، وتظهر أهميتها أيضاً في أنها ساهمت في انتقال البيانات بين شبكات العالم المختلفة الموجودة على الحواسيب بسرعة كبيرة جداً

Principles of Information Systems A Managerial ، George، Reynolds، Ralph، Stair^{٢٤٥}
Page86، part2، USA: Cengage Learning، Approach
^{٢٤٦} تم جمع هذه المعلومات من محاضرة عن نظم المعلومات في جامعة الأندلس الخاصة للعلوم الطبية،
طرطوس، سوريا، ص١٦٠، 1-<http://au.edu.sy/images/courses/pharmacy/>
2/153_computer-skills.pdf، تاريخ الدخول(٢٠١٨\٧\١٤).
^{٢٤٧} الدنف، أيمن، مرجع سابق، ص٢٦.

رابعاً_ البرامج.

يستخدم مصطلح البرامج للإشارة إلى كل أنواع الأوامر والتعليمات التي توجه وتراقب وتجعل أجهزة الحاسب تقوم بأداء مهام المعالجة والمهام الأخرى كافة المتعلقة بنظام الحاسب، وتقسّم برامج الحاسب إلى برامج النظم ومنها نظم التشغيل والبرامج التطبيقية ومنها البرامج المكتبية وبرامج الحسابات و برامج تحليل المبيعات ولغات البرمجة ومنها لغة (جافا)، ويتم اختيار الطريقة المناسبة للحصول على البرمجيات المطلوبة من خلال توافر مبرمجين مختصين مع إمكانية قيام هؤلاء المبرمجين بتطوير البرامج المطلوبة ضمن الحدود التي تكون مناسبة مع الزمن والتكلفة^{٢٤٨}.

خامساً_ البيانات.

تعتبر البيانات ذات أهمية قيمة في النظام، وبالتالي فإنه ومن الواجب أن يتم إدارتها بشكل فعال بحيث يتم استثمارها لكي تجلب الفائدة لمستخدمها، وهذه البيانات قد تكون بأشكال عديدة ومنوعة^{٢٤٩}، فقد تكون البيانات على شكل نصوص وقد تكون على شكل أرقام، وحينئذٍ يمكن تعريف البيانات أيضاً على أنها حروف وجمل وعبارات وأرقام ورموز غير منظمة وغير مرتبطة بموضوع واحد، فالبيانات تمثل المواد الأولية للحصول على المعلومات^{٢٥٠}.

^{٢٤٨} العنزي، أيمن، مرجع سابق، ص ٢٨.

^{٢٤٩} هاشم، غسان، مرجع سابق، ص ٣٩.

^{٢٥٠} عياد، سامي، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي للنشر والتوزيع، الإسكندرية، مصر، ٢٠٠٧، ص ٢٣+٢٤.

المطلب الثاني

تعريف الأمن المعلوماتي

إن موضوع الأمن المعلوماتي يعتبر موضوعاً ذا أهمية وارتباطه في الدرجة الأولى يتعلق بأمن الحاسوب، ولكن عبر التطورات المتسارعة في العالم، فإنه لا بد من توفير الأمن والحماية للمعلومات والبيانات؛ وإلا ستكون عُرضةً للهجمات الإلكترونية سواء كان ذلك عن طريق، السرقة أو تدمير المعلومات أو تعطيل أنظمة الحاسوب، فكان لا بد من أن يتم التفكير بشكل جدي من أجل تحديد إجراءات الدفاع والوقاية لحماية البيانات والمعلومات من أي اختراق أو تخريب أو تعطيل لها أو لنظام الحاسوب.

لقد لعب الحاسوب دوراً مهماً في زيادة الإقبال عليه، سواء كان من قبل المؤسسات، الاقتصادية أو العسكرية وغيرها، من أجل تخزين ومعالجة البيانات ذات الطابع المهم، إضافة إلى أن المعلومات التي تكون على الحاسوب قد تكون معلومات خاصة (شخصية) وهذا يمس من خصوصية وحرية الفرد في المجتمع، حيث يعد هذا أكبر سبب لكي يتم توفير الأمن والحماية للمعلومات وضمانة سلامتها دون أي عيوب. كذلك الأمر نشير إلى أن المعلومات يتم الحصول عليها بشكل كبير من خلال وسائل الاتصال والتواصل وأحياناً ما تكون هذه الوسائل عُرضةً لأن يتم اختراقها بسبب ضعف الحماية فيها وهذا بحد ذاته يهدد أمن تلك البيانات والمعلومات التي يتم تبادلها عبر الشبكات بين الحواسيب بمختلف أنحاء العالم. لهذا أصبح من الضرورة القول بأن توفير الأمن المعلوماتي يُعدُّ فريضةً على إدارة الأنظمة من أجل ضمان

خلق أجواء آمنة للمعلومات بهدف الحفاظ عليها من أي هجوم إلكتروني قد يسبب ضياع أو سرقة أو تزوير أو تدمير للنظام وللمعلومات والبيانات.

• الفرع الأول :- تعريف الأمن المعلوماتي.

وقبل أن ندخل في تعريف الأمن المعلوماتي، ودور الأمن في حماية المعلومات من التعرض لأي هجوم إلكتروني كالاختراق مثلاً، سوف نتحدث عن مفهوم جريمة نظم المعلومات وبعدها ننقل إلى تعريف الأمن المعلوماتي.

أولاً_ جريمة نظم المعلومات:- يمكن القول بأن جريمة نظم المعلومات هي التي تكون فيها جميع نظم المعلومات مستهدفة، والتي يتم ارتكابها بواسطة نظم المعلومات كالبيانات والبرامج والمعلومات وغيرها، ويكون ذلك إما عن طريق أفراد يعملون داخل المؤسسة أو عن طريق أفراد لا ينتمون للمؤسسة بحيث أنهم يقومون بالتلاعب بأنظمة المعلومات وبالبيانات الموجودة على الحاسب الآلي، ويكون ذلك العمل بهدف التخريب وسرقة المعلومات أو لممارسة أي عمل آخر غير مشروع وهذا بحد ذاته يتسبب في إلحاق الضرر الكبير بالنظام المعلوماتي بشكل كامل أو بشكل جزئي^{٢٥١}.

لقد أدى التطور الكبير في التقنيات التي تهتم بمعالجة البيانات إلى كثرة تلك المعلومات وتفرعها، وهذا بحد ذاته شكل عبء كبير على الأجهزة المختصة أن تقوم بتوفير الأمن للحفاظ على تلك المعلومات عن طريق تنظيمها وحفظها وتحديثها بشكل مستمر، فقد ساهم هذا التطور

^{٢٥١} العريان، محمد، مرجع سابق، ص ١٠٧.

إلى وجود طفرة نوعية حيث انتقل الناس من عصر الصناعة إلى عصر العالم الإلكتروني، وهذا بحد ذاته ساهم بشكل قوي وفعال في ضرورة حماية تلك المعلومات من أي هجوم إلكتروني، ففي هذا المجتمع التكنولوجي الحالي أصبح من يملك المعلومة يملك القوة، وفي هذا العصر أصبح تبادل المعلومات يتم بشكل فعال وسريع وهذا بحد ذاته أيضاً يعتبر سبباً لزيادة الإهتمام وأهمية الحفاظ على المعلومات^{٢٥٢}.

ثانياً_ الأمن المعلوماتي:- هو حماية المعلومات المختلفة والأدوات التي تتعامل معها وتعالجها، من منظمة وغرف تشغيل أجهزة وأجهزة وسائط تخزين وأفراد من السرقة، أو التلف، أو الاختراق، أو الضياع، أو التزوير، وذلك من خلال اتباع إجراءات وسياسات وقائية^{٢٥٣}.

وقد عرفها السالمي :- أنها مجموعة من الإجراءات و التدابير الوقائية التي تستخدم سواء في المجال التقني او الوقائي للحفاظ على المعلومات والأجهزة و البرمجيات إضافة الى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال^{٢٥٤}.

^{٢٥٢} الزهراني، راشد، تقنيات المعلومات بين التبنّي والابتكار، مطبوعات مكتبة الملك فهد الوطنية، الرياض، السعودية، ٢٠٠٤، ص٢٤.

^{٢٥٣} الفحطاني، منصور، مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٨، ص١٧.

^{٢٥٤} السالمي، علاء عبدالرازق، تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، ط٢، عمان، الأردن، ٢٠٠٢، ص٤٢٣.

فيما عرفها المشهداني بأنها:- الحفاظ على المعلومات المتواجدة في اي فضاء معلوماتي من مخاطر الضياع و التلف او من مخاطر الاستخدام غير الصحيح سواء المتعمد او العفوي او من مخاطر الكوارث الطبيعية^{٢٥٥}.

وعرفتها أمل بأنها:- مجموعة المعايير والمقاييس والاجراءات والتدابير الوقائية والدفاعية التي تستخدم لحماية انظمة المعلومات بكل مكوناته وتحقيق التكامل على كافة المستويات لضمان سرية المعلومات، وتوافرها وسلامة محتواها، وتحديد مسؤولية المتصرف بها^{٢٥٦}.

لقد ورد في كتاب "مبادئ أمن المعلومات" للمؤلفان (Whitman) و (Mattord) بأن الحفاظ على سرية وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل يتحقق من خلال التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعليم والتدريب. ويرى الكاتبان بأن أمن أي مؤسسة يهدف لتحقيق إدارة ناجحة لأمن نظم المعلومات فإنه يجب أن يكون شاملاً^{٢٥٧}:-

أ- أمن مادي يشمل المصادر والممتلكات لمنع الوصول غير المشروع.

ب-أمن أفراد من أجل حماية الأفراد والجماعات التي لها حق الوصول للمعلومة.

ت-أمن العمليات من أجل حماية الأنشطة والعمليات.

^{٢٥٥} الدنف، أيمن، مرجع سابق، ص ٤٣.
^{٢٥٦} علي، أمل، نظام أمن المعلومات في منظمات الأعمال مع نموذج مقترح لمواجهة تهديدات النظام، المجلة العراقية للعلوم الادارية، مج ٦، ع ٢٣، ٢٠٠٩، كربلاء، العراق، ص ٢٥٧.
^{٢٥٧} ' PRINCIPLES OF INFORMATION SECURITY، Herbert، Mattord، Michael، Whitman
. Page8، Chapter1،Fourth Edition, USA: Cengage Learning

ث- أمن اتصالات لحماية الوسائط والتكنولوجيا التي يتم استخدامها.

ج- أمن شبكات لحماية مكونات الشبكة من الاختراق.

ح- أمن البيانات من أجل حماية سرية وسلامة المعلومات.

في حين عرفها صادق والفتال على أن أمن المعلومات:- هو مصطلح يتسع ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني من أجل حماية المصادر البيانية، من أجهزة وبيانات وبرمجيات وأفراد من التجاوزات والتدخلات غير المشروعة والتي تقع عن طريق الصدفة أو بطريق العمد، وذلك عن طريق التسلل، أو قد يكون نتيجة إجراءات خاطئة متبعة^{٢٥٨}.

من كل ما تقدم نرى أن هذه التعريفات التي تم ذكرها أنها تهدف إلى حماية المعلومات والبيانات من التلف أو الضياع أو السرقة أو التزوير أو الاختراق من خلال الدخول غير المصرح به للنظام، وأن أمن المعلومات يقوم على (السرية وسلامة المعلومات وأن تكون تلك المعلومات متوافرة). وبناءً على ذلك يمكن أن نتوصل إلى تعريفاً للأمن المعلوماتي على أنه **عبارة عن:-** مجموعة من الاجراءات الوقائية، وهذه الإجراءات قد تكون إدارية وقد تكون فنية ويتم اتخاذها من أجل حماية الحاسوب بكافة مكوناته ووسائل الاتصال الخاصة به والبيانات والمعلومات والبرامج والتطبيقات التي يستخدمها الحاسوب من الضياع أو السرقة أو التلف أو الاختراق أو الدخول لنظام الحاسوب دون أن يكون هنالك إذن بذلك.

^{٢٥٨} صادق، دلال، الفتال، حميد، مرجع سابق، ص ١١+١٢.

• الفرع الثاني :- عناصر الأمن المعلوماتي.

إن المحافظة على أمن المعلومات، إنما يعتبر أمر ضروري ومهم للأفراد وللجماعات، فهو مصدر ثقة لكي يستمر الفرد والمؤسسات في تبادل المعلومات والبيانات فيما بينهم، وبالتالي فإنه ومن الضروري أن يتم توفير عناصر الحماية والأمن للمعلومات والبيانات.

لهذا يُعدُّ الكيان الاقتصادي ممثلاً في الشركات والبنوك من أهم الركائز التي يقوم عليها اقتصاد أية دولة، وبالتالي فإن حماية الأمن الإلكتروني لهذا الكيان يعد من أهم ما يجب تحقيقه على وجه السرعة، وذلك خوفاً من أن يؤدي ذلك إلى اختراق مثل هذا الكيان وبالتالي يؤدي إلى خسائر مادية ومعنوية مما يؤثر على مستوى سمعة هذه المنشآت من الثقة والأمان، لهذا فإن تحقيق الأمن المعلوماتي في مثل هذه المنشآت يتمثل في جود نظام على قدر من الكفاءة لإدارة مثل هذه المعلومات ومن ثم تحقيق الأمن المعلوماتي.

وتُعرف عناصر الأمن المعلوماتي:- على أنها مجموعة من العناصر التي يجب أن تتوفر لكي يتم حماية المعلومات الموجودة عليها، سواء كانت هذه المعلومات ثابتة أو منقولة، بحيث يقوم كل عنصر بتغطية أي جانب من الجوانب المطلوبة للحماية، حيث يفهم من ذلك أن العناصر يجب أن تتكامل كلها مع بعضها البعض لتوفير الحماية وذلك في حالة وقوع خلل في أحد العناصر^{٢٥٩}.

وقد تم الإشارة إلى أنه إذا أرادت المنظمات تحقيق أمن نظم المعلومات فإنه يجب تحقيق الثالوث والذي يطلق عليه مصطلح (CIA Triangle) وهو ما يعني السرية والسلامة

^{٢٥٩} القحطاني، ذيب، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية KACST، فهرس مكتبة الملك فهد الوطنية أثناء النشر، الرياض، السعودية، ٢٠١٥، ص ٧٨.

والتوفر^{٢٦٠}، حيث نرى أن الإتحاد العالمي للاتصالات في توصيته x800، قام بتحديد سبعة عناصر للأمن المعلوماتي ويمكن نكرها كآلاتي:- ١_ التحقق من الهوية، ٢_ التحكم بالوصول، ٣_ سلامة المعلومة وتكاملها، ٤_ السرية، ٥_ المتابعة، ٦_ التدقيق، ٧_ توافر المعلومة^{٢٦١}.

لهذا عندما يتم ذكر أمن المعلومات فإن أول ما يتبادر للذهن هو كشف لمعلومات كان من الواجب أن تبقى سرراً، فالحقيقة إن الحفاظ على سرية المعلومات لا يشترط أن يكون جانباً واحداً من جوانب الأمن، بينما يرى المتخصصون أن لأمن نظم المعلومات مكونات ثلاثة على درجة واحدة من الأهمية، وهو ما سنتناوله في هذا الفرع بشكل مفصل.

العنصر الأول:- سرية المعلومات.

إن الحفاظ على المعلومات سواء كانت منقولة أو مخزنة من السرقة أو التزوير أو الاختراق وغيرها إنما يعتبر أمر ضروري وهام يقع على الجهات المختصة، فالسرية تعني ضمان حفظ تلك المعلومات الموجودة على الشبكة وعدم الاطلاع عليها إلا إذا كان هناك قرار أو إذن يسمح بالاطلاع على تلك المعلومات.

إن النظام الأمن هو ذلك النظام الذي يضمن سرية وخصوصية البيانات المخزنة فيه، والنظام الأمن هو ذلك النظام الذي يتيح إظهار البيانات فقط لمن له الحق بذلك، بالإضافة إلى

^{٢٦٠} الدنف، أيمن، مرجع سابق، ص ٤٥.

^{٢٦١} القحطاني، ذيب، مرجع سابق، ص ٧٧.

ضمان تأمين نقل المعلومات والبيانات عبر الشبكة بدرجة عالية من الحماية والأمان، ويتحقق ذلك من خلال إتباع طرق الحماية والأمن التي تكون منصوص عليها من قبل الجهة المختصة^{٢٦٢}. والسرية باللغة الإنجليزية تعني (Confidentiality) وتعني أيضاً أن المعلومات والبيانات لا يتم كشفها إلا لصاحبها ولا يمكن أن يطلع عليها أحد غير مخول بذلك^{٢٦٣}. كما أن خطر كشف المعلومات السرية قد يؤدي إلى اطلاع من يقوم بعملية الدخول غير المشروعة إلى معلومات لا يحق له الاطلاع عليها وليس له الإذن بذلك، وهذا بحد ذاته يشكل تهديداً لأصحاب هذه المعلومات والبيانات من عدم رغبتهم في اطلاع أي شخص آخر على تلك المعلومات والبيانات، وقد يؤدي ذلك الدخول غير المشروع إلى حرمان الشخص الأصلي صاحب تلك المعلومات والبيانات من الوصول إليها عند حاجته لها، وذلك في حال عدم وجود نسخة أخرى للمعلومات أو البيانات^{٢٦٤}.

نود الإشارة إلى أن هناك طرق عديدة لضمان سرية المعلومات والبيانات فقد تكون عن طريق:- حجب المعلومة أو عدم تسليمها إلا للشخص المصرح له بذلك، أو عن طريق التشفير الحديث بإستخدام خوارزميات رياضية معقدة بحيث لا يستطيع فهمها أحد سوى ذاك الشخص المصرح له بالاطلاع عليها، إذاً نستطيع القول أنه يمكن توفير الأمن والحماية (السرية) من

^{٢٦٢} الدنف، أيمن، مرجع سابق، ص٤٦.

^{٢٦٣} الحصري، أحمد، درس بعنوان "مقدمة أمن المعلومات"، منتدى الرياض الاجتماعي الثالث، وزارة الشؤون الاجتماعية، السعودية، موقع يوتيوب، https://www.youtube.com/watch?v=Q_M5q_aFK7Y، ص٢٠١٥، ص٤.

^{٢٦٤} الغنبر، خالد، القحطاني، محمد، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، فهرس مكتبة الملك فهد الوطنية، ط١، الرياض، السعودية، ٢٠٠٩، ص١٢.

خلال تشفير البيانات بغض النظر عن نوع تلك البيانات ثابتة أو منقولة، أو عن طريق بصمات للعين أو للإصبع أو للوجه بشكل، ومن خلال إيجاد فريق يختص بالحماية والأمن، عن طريق تدريبهم من قبل مختصين بالحماية والأمن وممن لديهم الخبرة بهذا المجال^{٢٦٥}.

العنصر الثاني:- سلامة المعلومات.

ويعني ذلك أن يتم التأكد من سلامة المحتوى، هل هو صحيح، وهل تم إجراء تعديل عليه أو لا، أو هل تم العبث به. وسلامة المعلومات يعني تكاملية البيانات المخزنة فيه، ونقصد بالتكاملية حماية البيانات من أي عملية حذف أو تخريب أو تغيير، حيث يتم تأمين ذلك من خلال مجموعة من الأساليب التي تقوم بتوفيرها نظم قواعد البيانات.

إذا نظرنا للمادة (٣٥) من القرار بقانون الخاص بالجرائم الإلكترونية الفلسطينية رقم (١٠) لسنة (٢٠١٨) والتي نصت على أنه " على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها"^{٢٦٦} يتبين لنا من هذه المادة أهمية سلامة المعلومات والبيانات وكل الأدوات التي يتم حفظها عليها، وهذا بحد ذاته دليل قاطع على أن المشرع الفلسطيني على دراية كاملة بأهمية تلك المعلومات والبيانات. ونرى بأن الأهم من الحفاظ على سرية المعلومات، هو أن يتم اتخاذ التدابير اللازمة من أجل حماية المعلومات من

^{٢٦٥} القحطاني، ذيب، مرجع سابق، ص ٩٢.
^{٢٦٦} راجع المادة (٣٥) من القرار بقانون الخاص بالجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨م).

التغيير أو التعديل أو الحذف، فهو أمر ضروري ومهم من أجل خلق الثقة والراحة النفسية للفرد وللجماعات وللمؤسسات التي تقوم بمبادلة المعلومات والبيانات فيما بينها، فطالما أن المعلومة تتم عبر الشبكات الإلكترونية فهي بالتالي مرشحة بشكل قوي لأن يتم اختراقها وتغيير مضمون تلك المعلومة.

وسلامة المعلومة يطلق عليها باللغة الإنجليزية (Data Integrity) وهي تعني أنه تم تلقي المعلومة كما أرسلت دون إجراء أي تعديل أو تغيير عليها وأنها صحيحة بالمضمون والمحتوى، وأنه تم معالجتها أثناء تنقلها بالطرق الصحيحة دون حدوث أي تغيير متعمد أو غير متعمد^{٢٦٧}.

العنصر الثالث:- توافر المعلومات.

يطلق عليها باللغة الإنجليزية مصطلح (Availability). بمعنى إن النظام الآمن والذي يأخذ بكافة تدابير الحماية والأمن، هو ذلك النظام الذي يمكن أن نقول عنه بأنه يوفر المعلومة في كل الأوقات عندما يطلبها من يحق له الإطلاع عليها.

فتوافر المعلومة هي خدمة تحمي النظام بحيث تكون المعلومة متاحة لكل من يحق له الإستفادة، وهذا ما يعني بديمومة توافر المعلومة أي أنها (دائمة)، فالنظام الآمن هو الذي يضمن استمرار وصول المستخدمين إلى المعلومات التي يحق لهم الاطلاع عليها دون أن يكون هناك أي عقبات أمامهم، كشطب أو تعديل أو تغيير أو اختراق لتلك المعلومات.

^{٢٦٧} القحطاني، ذيب، مرجع سابق، ص ٩٤.

لهذا فإن توفر المعلومة لها خصائص عديدة منها^{٢٦٨}:-

١. المقاومة وهي قدرة النظام على الحفاظ على نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه، (على سبيل المثال أن يكون النظام قادرا على منع تنفيذ استعلامات تتطلب حجز حيز كبير من ذاكرة المخدم).
٢. المقدرة على التوسع لسد الحاجات المستقبلية.
٣. المرونة والتمثلة في توفر الامكانيات والأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك إلى توقفه.
٤. سهولة الاستخدام.

الخاتمة

بعد دراستنا لجريمة اختراق النظم والشبكات المعلوماتية، نود الإشارة إلى أنه يجب علينا أن نسلم بالثورة المعلوماتية، التي أدت إلى تحطيم الحدود الجغرافية والسياسية استناداً إلى التقدم العلمي والتقني المتعلق بجرائم المعلوماتية والانترنت، حيث أصبح العالم عبارة عن قرية معلوماتية صغيرة واحدة.

^{٢٦٨} جامعة الدول العربية، المركز العربي للبحوث القانونية (٢٠١٢م)، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات المنعقد في (٥-٧/٠٣/٢٠١٢) بيروت، الجمهورية اللبنانية، ص٦+٧، متاح على الرابط التالي <https://carjj.org/node/1242>، تاريخ الدخول (١٧/١١/٢٠١٨م).

ونظراً لهذا التطور والتقدم التقني والتكنولوجي الهائل، نرى أن هناك مزايا وحسنات قد نجمت عن الثورة المعلوماتية، وإلى جانب ذلك نجمت عدة مساوئ عن إساءة استخدام شبكة الانترنت والمعلوماتية وتطويرها لصالح المجرم المعلوماتي، مما أدى إلى ظهور جرائم جديدة يطلق عليها الجرائم المستحدثة، حيث نرى أن الشبكة المعلوماتية وشبكة الانترنت إنما هي عبارة عن أداة لارتكاب الجريمة، وبالتالي قد تكون أداة إيجابية وقد تكون أداة سلبية للمجرم المعلوماتي فتكون أداة إيجابية لأنها تسهل للمجرم المعلوماتي ارتكاب جرائم عديدة، تشكل أغلب جرائم الاعتداء على الأشخاص مثل جرائم الاعتداء على حق الانسان في شرفه وسمعته واعتباره وحقه في انتهاك حرمة حياته الخاصة. كما أن هناك جرائم الاعتداء على حق الانسان في حياته والمتمثل بإعدام حق الانسان في الحياة، أما الصورة السلبية لجرائم المعلوماتية فإن هدف الجاني منها هو الحصول على المعلومات والبيانات وغيرها من المعلومات المنقولة بصورة غير مشروعة لهذا نرى أن هناك بعض الملاحظات التي تثيرها جرائم المعلوماتية والانترنت أهمها:-

١. أن جرائم المعلوماتية لها خاصية معينة أهمها صعوبة اكتشافها، حيث أن مثل هذه الجرائم لا عنف فيها، ولا يترتب عليها أي أثر مادي، مما لا يدعونا إلى أن نطلق على هذه الجريمة مصطلح (الجرائم النظيفة) حيث لا يترتب عليها أي أثر له وجود خارجي يراه الناس.

٢. نرى أن الجرائم المعلوماتية جرائم ترتكب في داخل الوطن وفي الدول والقارات، وذلك بواسطة شبكات الاتصال ودون أن نتحمل عناء السفر والتنقل من دولة لأخرى، وبالتالي

فإن القانون يجرم هذه الجرائم استناداً إلى المعاهدات الدولية.

٣. نود الإشارة إلى أن المجرم المعلوماتي إنما هو مجرم نكي واجتماعي بطبعه، وبالتالي عالجا في قانون الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨).

أولاً: - النتائج.

١. أن التطور التكنولوجي ساهم بشكل كبير في حدوث نقلة نوعية فقد أصبح من السهل الحصول والوصول إلى المعلومات بكافة أنواعها.
٢. أفرز التقدم الهائل في تكنولوجيا المعلومات جرائم لم تكن معروفة منذ القدم، حيث أصبحنا نسمع بجرائم جديدة مستحدثة كالجرائم المعلوماتية.
٣. لا يوجد مفهوم عام متفق عليه بين الدول بخصوص نموذج النشاط المكون للجريمة المعلوماتية أو جريمة الانترنت.
٤. نقص الخبرة لدى رجال الضابطة العدلية والنيابة العامة، وكذلك القضاء في مجال كشف عناصر الجريمة في حال وجودها، وكذلك في حال جمع المعلومات والأدلة اللازمة التي يجب توافرها لإدانة المجرم المعلوماتي.
٥. بالرغم من الايجابيات التي نتجت عن هذا التقدم التكنولوجي في سهولة الوصول للمعلومات والبيانات والتبادل التجاري وتنشيط الاقتصاد بين الدول إلا أنها ساهمت في انتشار الجرائم التي أصبحت تهدد سلامة وأمن الدول.
٦. الإقبال الكبير من قبل الأفراد والجماعات والشركات والمؤسسات على شبكة الإنترنت والحاسب الآلي نتيجة لسهولة التعامل معها.

٧. عدم أخذ الاحتياطات اللازمة وقلة الوعي للأفراد ساهم بشكل كبير لجعلهم عرضة للاختراق أو لأي جريمة إلكترونية أخرى.

٨. عدم التناسب بين قوانين الإجراءات الجزائية للدول خاصة فيما يتعلق بالتحري والبحث عن جرائم المعلوماتية والانترنت.

٩. إن جريمة الاختراق تعتبر جريمة عابرة للدول، فهي لا تعرف حدود ولا تعرف اتفاقيات ومعاهدات بين الدول، وهي جريمة صامته تتم بالخفاء.

١٠. كل مستخدم لشبكة الإنترنت وللحاسب الآلي هو معرض لجريمة الاختراق أو لأي جريمة من الجرائم الإلكترونية.

١١. نشير إلى أن التكنولوجيا الحديثة إنما هي مورد قادر على خلق ثروة جديدة، حيث أنها تتيح لمالكها أن يمارس السيطرة الاجتماعية، وبالتالي تصبح هذه التكنولوجيا عامل مؤثر وفعال وهي أسلوب من أساليب صنع القرار في الدولة.

١٢. أن المجرم في الجريمة الإلكترونية يختلف كلياً عن المجرم في الجرائم التقليدية، فالمجرم الإلكتروني يتميز بخبرته وكفاءته وذكاءه في التعامل مع الحاسب الآلي وشبكة الإنترنت.

١٣. في الجريمة الإلكترونية يعتبر جهاز الحاسوب هو الأداة، وشبكة الإنترنت مسرح الجريمة، بينما في الجريمة التقليدية قد تكون سلاحاً أبيضاً كالسكين، وقد تكون سلاحاً نارياً، ومسرح الجريمة في الجريمة التقليدية قد يكون مكان عام وقد يكون داخل شقة في عمارة وقد يكون داخل إحدى غرف المنزل.

١٤. أن الجريمة الإلكترونية بشكل عام لا تترك أي أثر مادي يوقع بمرتكبها للعقاب، وإن وجد أثر مادي فيكون من باب الصدفة، فكما أشرنا المجرم المعلوماتي خبير وذكي في التعامل مع الحاسب الآلي وشبكة الإنترنت.

١٥. تعتبر جريمة الاختراق جريمة قائمة بحد ذاتها، حتى ولو لم يقم بأي عمل تخريبي كتعطيل نظام الحاسب الآلي أو تدمير البيانات أو إتلافها وغيرها من الأعمال التخريبية التي قد يلجأ لها المجرم، فبمجرد دخوله للنظام بشكل غير مشروع وكان عالماً بذلك وبقي فيه ولم يخرج ولم يقم بأي عمل تخريبي يعتبر مرتكباً لجريمة الاختراق وفقاً للمادة (٤) الفقرة (١) من القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني رقم (١٠) لسنة (٢٠١٨).

ثانياً: - التوصيات.

١. ضرورة تكثيف الجهود الوطنية والدولية من أجل مواجهة الجرائم الإلكترونية وذلك لما تشكله من مخاطر كبيرة على سلامة وأمن الدول، وأن يكون هناك تعاون تكنولوجي وتقني بين الدول المتقدمة والدول النامية، فهذا قد يؤدي إلى عدم استفادة الدول النامية من هذا التقدم التقني والتكنولوجي الذي يعيشه العالم اليوم.

٢. توفير الحماية لبرامج الحاسب الآلي، ومن خلال العمل على وضع سياسة وطنية ملائمة للقوانين والاتفاقيات الدولية المختصة بمكافحة الجرائم الإلكترونية.

٣. نود الإشارة إلى أنه يجب النص على تقنين الاستخدام الإلكتروني، مثل قانون التجارة الإلكترونية، وقانون التوقيع الإلكتروني، حيث أن التجارة الدولية من شأنها أن تعمل على سرعة انتقال المعاملات التجارية ورؤوس الاموال بين الدول.
٤. إيجاد أجهزة مختصة لملاحقة مرتكبي الجرائم الإلكترونية، حيث تعتبر دولة فلسطين إحدى الدول التي أوجدت نيابة لمكافحة الجرائم المعلوماتية.
٥. عقد الدورات التدريبية لرجال الشرطة وأعضاء النيابة العامة والقضاء ، وللأجهزة المختصة من أجل معرفة كيفية مكافحة الجريمة الإلكترونية.
٦. عقد ندوات توعوية لأفراد المجتمع وخاصة الشباب والشابات لأنهم بمرحلة المراهقة فهم عرضة للكثير من الابتزازات والتهديدات وغيرها من الوسائل التي قد يلجأ إليها المجرمين المعلوماتيين، فمن الواجب توعيتهم للوقاية من المجرمين ومن مخاطر تلك الجرائم الإلكترونية، ونشر منشورات توعوية في المدارس والجامعات.
٧. أن يكون هناك مراقبة من قبل الأسرة على أولادهم لكي لا يدخلوا إلى المواقع الإباحية والمواقع التحريضية والطائفية.
٨. أن تقوم جهات الاختصاص بمتابعة قضايا الاختراق والابتزاز التي تتعرض لها الفتيات على وجه الخصوص، وأن يكون ذلك بسرية تامة، لكي لا يُصبن الفتيات بالمرض النفسي والقلق والتوتر.
٩. أن أهم ما يواجهه الدول بالنسبة للجرائم المعلوماتية إنما يتمثل في الحفاظ على السرية والخصوصية، وهذا بدوره مشكلة تواجه التجارة الإلكترونية في جميع دول العالم.

١٠. أن يتم إيقاع أقصى العقوبات لكل من تسول له نفسه القيام بجرائم تهدد سلامة اقتصاد وأمن الدولة.

١١. أن يتم التعاون والتواصل بشكل فعال مع الشرطة الدولية (الإنتربول) لكي يتم التعرف أكثر على طرق الحماية والأمن، ومن أجل ضرورة تسليم المجرمين وملاحقتهم، وأن يتم تبادل الخبرات الفنية والتقنية بينهم.

١٢. يجب إنشاء إدارة جديدة في وزارة الداخلية في جميع دول العالم مهمتها تكون مسؤولة عن الجرائم المعلوماتية، خاصةً بعد الإقبال الكبير من مستخدمي شبكة الانترنت والجرائم المعلوماتية، حيث أصبح الدخول إلى الشبكة المعلوماتية سهل جداً فلا يحتاج لأي تعقيدات، فمن الممكن الدخول إلى شبكة الانترنت بواسطة خط تليفون وجهاز كمبيوتر فقط.

١٣. خلق بيئة معلوماتية حاسوبية فلسطينية آمنة وموثوقة ضمن أحدث وسائل التكنولوجيا المستخدمة وهو ما تبنته المادة (٤) من القرار الصادر عن مجلس الوزراء رقم (١٦) لسنة (٢٠١٥) بالنظام الداخلي لعمل الفريق الفلسطيني للاستجابة لطوارئ الحاسوب.

قائمة المصادر والمراجع.

أولاً: - المصادر.

١. القرآن الكريم.

٢. ابن منظور، محمد بن مكرم. (١٩٩٠): (ت ٧١١هـ / ١٣١١م)، معجم لسان العرب، مج ١٢، ط ٣، دار صادر للنشر والتوزيع، بيروت، لبنان.

٣. عمر، أحمد مختار. (٢٠٠٨): معجم اللغة العربية المعاصرة، مج ١، ط ١، عالم الكتب، القاهرة، مصر.

أ_ القوانين.

١. قانون المعاملات الإلكترونية الفلسطينية رقم (٦) لسنة (٢٠١٣)، الفصل الأول، تعاريف وأحكام عامة.

٢. قرار بقانون بشأن الجرائم الإلكترونية، رقم (١٠) لسنة (٢٠١٨).

ب_ الاتفاقيات.

١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة عن جامعة الدول العربية لسنة (٢٠١٠).

٢. اتفاقية بودابست للجرائم الإلكترونية لسنة (٢٠٠١).

ثانياً:- المراجع.

١. أحمد، هلال. (١٩٩٧): تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.

٢. البكري، سونيا. (٢٠٠٠): نظم المعلومات الإدارية والمفاهيم الأساسية، الدار الجامعية للنشر والتوزيع، الإسكندرية، مصر.
٣. تمام، أحمد حسام. (٢٠٠٠): الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.
٤. الجريدلي، جمال. (٢٠٠٨): البيع الإلكتروني للسلع المقلدة عبر شبكة الإنترنت دراسة فقهية مقارنة، ط١، دار الفكر الجامعي، الإسكندرية، مصر.
٥. الجنيهي، منير، ممدوح، الجنيهي. (٢٠٠٤): جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر.
٦. حجازي، عبد الفتاح. (٢٠٠٢): الدليل الجنائي والتزوير في جرائم الكمبيوتر، ط١، دار الفكر الجامعي، الإسكندرية، مصر.
٧. حجازي، عبدالفتاح. (٢٠٠٨): الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، مصر.
٨. الحربي، خالد. (٢٠٠٦): الأمن والحماية في الإنترنت، ط١، دار الفلاح للنشر والتوزيع، الرياض، السعودية.
٩. الحسيناوي، علي. (٢٠٠٩): جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن.
١٠. الحسيني، عمر. (١٩٩٥): المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، ط٢، (د.ن.).

١١. الحلبي، خالد. (٢٠١١): إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط١، دار الثقافة للنشر والتوزيع، عمان، الأردن.
١٢. الحلبي، أبي يعلى. (٢٠٠٠): الأحكام السلطانية، صححه وعلق عليه "محمد حامد الفقي"، دار الكتب العلمية، بيروت، لبنان.
١٣. خاطر، منتصر عبدالله، وآخرون. (٢٠٠٨): الحاسوب، مقرر تأسيسي لجامعة القدس المفتوحة، (د.ن).
١٤. الخوري، هاني. (١٩٩٨): تكنولوجيا المعلومات على أعتاب القرن الحادي والعشرين، ج١، دار السلام للنشر والتوزيع، مصر.
١٥. رمضان، مدحت. (٢٠٠١): الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، مصر.
١٦. الزعبي، جلال، وآخرون. (٢٠٠١): جرائم الحاسوب والإنترنت، دار وائل للنشر والتوزيع، عمان، الأردن.
١٧. الزعبي، علي. (٢٠٠٦): حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس، لبنان.
١٨. زهران، مضر. (٢٠٠٣): جرائم الدعارة على الإنترنت، دار زهران للنشر والتوزيع، عمان، الأردن.
١٩. الزهراني، راشد. (٢٠٠٤): تقنيات المعلومات بين التبرني والابتكار، مطبوعات مكتبة الملك فهد الوطنية، الرياض، السعودية.

٢٠. السالمي، علاء عبدالرازق. (٢٠٠٢) تكنولوجيا المعلومات، ط٢، دار المناهج للنشر والتوزيع، عمان، الأردن.
٢١. سقف الحيط، عادل. (٢٠١٥): جرائم الدم والقذح والتحقيق المرتكبة عبر الوسائط الإلكترونية دراسة قانونية مقارنة، ط٢، دار الثقافة للنشر والتوزيع، عمان، الأردن.
٢٢. الشدى، طارق. (٢٠٠٠): آلية البناء الأمني لنظم المعلومات، دار الوطن للنشر والتوزيع، ط١، الرياض، السعودية.
٢٣. الشمري، غانم. (٢٠١٦): الجرائم المعلوماتية ماهيتها. خصائصها. كيفية التصدي لها قانونياً، ط١، دار الثقافة للنشر والتوزيع، عمان، الأردن.
٢٤. شمس الدين، أشرف توفيق. (٢٠٠٦): الحماية الجنائية للمستند الإلكتروني (دراسة مقارنة)، ط١، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.
٢٥. الشوابكة، محمد. (٢٠٠٤): جرائم الحاسوب والانترنت الجريمة المعلوماتية، ط١، دار الثقافة للنشر والتوزيع، عمان، الأردن.
٢٦. صادق، دلال، الفتح، حميد. (٢٠١٣) أمن المعلومات، دار اليازوري للنشر والتوزيع، عمان، الأردن.
٢٧. الصغير، جميل. (١٩٩٢): القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر.
٢٨. الصيرفي، محمد. (٢٠٠٥): نظم المعلومات الإدارية، دار الفكر الجامعي للنشر والتوزيع، الإسكندرية، مصر.

٢٩. طوالبة، علي. (٢٠٠٤): التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتب الحديث للنشر والتوزيع، إربد، عمان.
٣٠. الطيطي، خضر. (٢٠١٠): أساسيات أمن المعلومات والحاسوب، دار الحامد للنشر والتوزيع، عمان، الأردن.
٣١. عبابنة، محمود، الرازقي، محمد. (٢٠٠٥) جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن.
٣٢. عبدالله، أحمد. (١٩٩٧): حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.
٣٣. العريان، محمد. (٢٠٠٤): الجرائم المعلوماتية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر.
٣٤. العزة، فراس، وآخرون. (٢٠٠٣): مهارات الحاسوب والبرمجيات الجاهزة التطبيقات البرمجية والاستخدامات العملية، ط١، دار اليازوري للنشر والتوزيع، عمان، الأردن.
٣٥. عفيفي، عفيفي. (٢٠٠٠): جرائم الكمبيوتر، (د.ن)، القاهرة، مصر.
٣٦. عمار، ماجد. (١٩٨٩): المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.
٣٧. عياد، سامي. (٢٠٠٧): الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي للنشر والتوزيع، الإسكندرية، مصر.

٣٨. عيسى، طوني. (٢٠٠١): التنظيم القانوني لشبكة الانترنت، ط١، دار صادر للمنشورات الحقوقية، بيروت، لبنان.
٣٩. الغنبر، خالد، القحطاني، محمد. (٢٠٠٩): أمن المعلومات بلغة ميسرة، ط١، مركز التميز لأمن المعلومات، فهرس مكتبة الملك فهد الوطنية، الرياض، السعودية.
٤٠. غراب، كامل، حجازي، فادية. (٢٠٠٠): نظم المعلومات الإدارية، ط٢، مكتبة ومطبعة الأشعاع الفنية، الإسكندرية، مصر.
٤١. فكري، أيمن. (٢٠١٥): الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد للنشر والتوزيع، الرياض، السعودية.
٤٢. فكيرين، محمد. (١٩٩٣): أساسيات الحاسب الآلي، دار الراتب الجامعية للنشر والتوزيع، بيروت، لبنان.
٤٣. الفيومي، محمد. (١٩٩٨): مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، المكتب الجامعي الحديث للنشر والتوزيع، الإسكندرية، مصر.
٤٤. القاضي، زياد. (١٩٩٠): الكمبيوتر وتطبيقاته، دار المستقبل للنشر والتوزيع، عمان، الأردن.
٤٥. القحطاني، ذيب. (٢٠١٥): أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية KACST، فهرس مكتبة الملك فهد الوطنية أثناء النشر، الرياض، السعودية.
٤٦. القحطاني، محمد. (٢٠١١) الجريمة المنظمة، ط٢، دار العرب للنشر والتوزيع، الرياض، السعودية.
٤٧. القدهي، مشعل. (٢٠٠٥): الإباحية وتبعاتها ظاهرة تفشي المواد الإباحية في الإعلام و الاتصالات و الإنترنت وأثرها على الفرد و المجتمع و أمن الشعوب، (د.ن).

٤٨ . قشقوش، هدى. (١٩٩٢): جرائم الحاسب الإلكتروني، ط١، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر.

٤٩ . القهوجي، علي. (١٩٩٧): الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر.

٥٠ . قنديلجي، عامر، الجنابي، علاء الدين. (٢٠١٨): نظم المعلومات الإدارية، دار الميسرة للنشر والتوزيع، عمان، الأردن.

٥١ . كيروز، حيمس، وروس، كيث. (٢٠١١): شبكات الحاسب والإنترنت أسس ومبادئ الشبكات والإنترنت، (ترجمة السيد الألفي، ورضوان عبد العال)، دار العبيكان للنشر، السعودية.

٥٢ . المصري، أحمد. (١٩٨٩): الإتصالات والقرارات وفعاليتها في الإدارة، دار القلم للنشر والتوزيع، الكويت.

٥٣ . الملط، أحمد. (٢٠٠٦): الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر.

٥٤ . المناعسة، أسامة، وآخرون. (٢٠٠١): جرائم الحاسب الآلي والإنترنت، دار وائل للنشر والتوزيع، ط١، عمان، الأردن.

٥٥ . المناعسة، أسامة، الزعبي، جلال. (٢٠١٧): جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة، ط٣، دار الثقافة للنشر والتوزيع، عمان، الأردن.

٥٦ . المومني، نهلا. (٢٠١٠): الجرائم المعلوماتية، ط٢، دار الثقافة للنشر والتوزيع، عمان، الأردن.

٥٧ . نجم، محمد. (٢٠١٢): قانون العقوبات القسم العام النظرية العامة للجريمة، ط٤، دار الثقافة للنشر والتوزيع، عمان، الأردن.

٥٨. نصار، غادة. (٢٠١٧): الإرهاب والجريمة الإلكترونية، دار العربي للنشر والتوزيع، القاهرة، مصر.

أطروحات الدكتوراة.

١. أمينة، صافة. (٢٠١٦): آثار إستعمال التكنولوجيات الحديثة على أفراد الأسرة الجزائرية دراسة للتأثيرات النفسية والاجتماعية والأخلاقية والصحية لاستعمال الإنترنت على أبناء الأسرة الجزائرية نموذجاً، أطروحة دكتوراة، جامعة وهران.
٢. عبدالله، محمود. (٢٠٠١): سرقة المعلومات المخزنة في الحاسب الآلي، أطروحة دكتوراه منشوره، كلية الحقوق، جامعة عين شمس، مصر.
٣. هاشم، غسان. (٢٠١٣): أثر كفاءة نظم المعلومات في تحسين فاعلية عملية صنع اتخاذ القرار، أطروحة دكتوراة غير منشورة، جامعة سانت كليمنتس العالمية المكلا، اليمن.
٤. بن يونس، عمر. (٢٠٠٤): الجرائم الناشئة عن استخدام الانترنت، أطروحة دكتوراه منشورة في القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر.

الرسائل الجامعية

٥. بحر، عبدالرحمن. (١٩٩٩): معوقات التحقيق في جرائم الإنترنت دراسة مسحية على ضباط

الشرطة في دولة البحرين، أكاديمية نايف العربية للعلوم الأمنية، رسالة ماجستير غير

منشورة معهد الدراسات العليا.

٦. بلقاسم، مرغني. (٢٠١٤): نظام المعلومات ودوره في اتخاذ القرار، مذكرة ماستر غير

منشورة، جامعة قاصدي مرباح، الجزائر.

٧. البلوي، شيخة. (٢٠١٦): المسؤولية الجنائية عن اختراق المواقع الإلكترونية الرسمية

للدولة في النظام السعودي مقارنة بالقانون الإماراتي، رسالة ماجستير غير منشورة، جامعة

نايف العربية للعلوم الأمنية، الرياض، السعودية.

٨. بوهلال، أحلام. (٢٠١٦): تأثير استخدام شبكة الإنترنت على العلاقات الأسرية الجزائرية،

مذكرة ماستر غير منشورة، كلية العلوم الإنسانية والاجتماعية، جامعة العربي التبسي،

الجزائر.

٩. ثنيان، ثنيان. (٢٠١٢): إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، رسالة

ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

١٠. حسين، عبد الرحمن. (٢٠٠٨): الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، كلية الدراسات العليا، نابلس، فلسطين.
١١. الخليفة، محسن. (٢٠٠٣): جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، رسالة ماجستير غير منشورة، أكاديمية نايف للعلوم الأمنية، قسم العدالة الجنائية.
١٢. الدنف، أيمن. (٢٠١٣): واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، رسالة ماجستير غير منشورة، الجامعة الإسلامية، كلية التجارة ، غزة، فلسطين.
١٣. سارة، عياط. (٢٠١٤): جريمة القذف على شبكة الإنترنت، مذكرة ماستر غير منشورة، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، الجزائر.
١٤. السرحاني، محمد. (٢٠٠٤): مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا.
١٥. سعيداني، نعيم. (٢٠١٣): آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر غير منشورة، جامعة الحاج لخضر باتنة، الجزائر.

١٦. سعيدة، بكرة. (٢٠١٦): الجريمة الإلكترونية في التشريع الجزائري دراسة مقارنة، مذكرة

ماستر غير منشورة، جامعة محمد خيضر بسكرة، الجزائر.

١٧. سفيان، سوير. (٢٠١١): جرائم المعلوماتية، مذكرة ماستر غير منشورة، جامعة أبو

بكر بلقايد تلمسان، الجزائر.

١٨. شنين، صالح. (٢٠٠٧): الحماية الجزائرية لبرامج الحاسب الآلي، مذكرة ماستر غير

منشورة، جامعة محمد خيضر بسكرة، الجزائر.

١٩. العجمي، عبدالله. (٢٠١٤): المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة،

رسالة ماجستير غير منشورة، جامعة الشرق الأوسط.

٢٠. عفون، حمزة. (٢٠١٢): السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماستر غير منشورة،

جامعة الحاج لخضر باتنة، الجزائر.

٢١. عمار، زكريا. (٢٠١١): حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، رسالة

ماجستير غير منشورة، جامعة النيلين، كلية الدراسات العليا، السودان.

٢٢. العنزي، سليمان. (٢٠٠٣): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير

غير منشورة، أكاديمية نايف العربية للعلوم الأمنية.

٢٣. فتحية، رصاع. (٢٠١٢): الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة ماستر

غير منشورة، جامعة أبي بكر بلقايد، تلمسان، الجزائر.

٢٤. فريال، لعاقل. (٢٠١٥): الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر غير منشورة، جامعة محند أولحاج، الجزائر.

٢٥. القحطاني، منصور. (٢٠٠٨) مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية.

٢٦. قنيطة، أحمد. (٢٠١١): الآثار السلبية لاستخدام الإنترنت من وجهة نظر طلبة الجامعة الإسلامية بغزة ودور التربية الإسلامية في علاجها، الجامعة الإسلامية، كلية التربية، غزة، رسالة ماجستير غير منشورة.

٢٧. كهينة، سليمان، ضاوية، زوازي. (٢٠١٦): النظام القانوني لبرامج الحاسوب الآلي، مذكرة ماستر غير منشورة، جامعة عبد الرحمان ميرة-بجاية، الجزائر.

٢٨. مزغيش، سمية. (٢٠١٤): جرائم المساس بالأنظمة المعلوماتية، مذكرة ماستر غير منشورة، جامعة محمد خيضر بسكرة.

٢٩. مهنا، عبد الوهاب. (٢٠٠٩): درجة توظيف الحاسوب في الإدارة المدرسية بمدارس وكالة الغوث في محافظات غزة وسبل تطويرها، رسالة ماجستير غير منشورة، الجامعة الإسلامية، عمادة الدراسات العليا، كلية التربية، غزة، فلسطين.

٣٠. نورة، طرشي. (٢٠١٢): مكافحة الجريمة المعلوماتية، مذكرة ماستر غير منشورة، جامعة الجزائر، كلية الحقوق، الجزائر.

٣١. نورية، العاج. (٢٠١٣): استخدام الشبكة العنكبوتية (الإنترنت) في الدراسة وعلاقتها

بالدافعية للتعلم لدى المراهق من (١٢_١٤ سنة)، مذكرة ماستر غير منشورة، كلية العلوم

الاجتماعية والانسانية، الجزائر.

٣٢. الوهاب، سرور. (٢٠٠٤): الدافع والباعث على الجريمة وأثرهما في العقوبات التعزيرية،

رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم والأمنية.

٣٣. ياسمين، بونقارة. (٢٠١٥): الجريمة الإلكترونية، مذكرة ماستر منشورة، جامعة الأمير

عبد القادر للعلوم الإسلامية، الجزائر.

المجلات.

١. أبكر، سليمان مصطفى. (٢٠٠٢): جرائم الحاسب الآلي وطرق المواجهة، مجلة الأمن والحياة،

أكاديمية نايف العربية للعلوم الأمنية، ع٢٤٣، نشر بالمجلة بشهر (١٠).

٢. أغلال، الزهراء بوكريمة. (٢٠١١): مقال عن الشبكة العنكبوتية العالمية وسيلة للتعلم الذاتي

وتطوير البحث العلمي، مجلة العلوم الإنسانية والاجتماعية، عدد خاص الحاسوب وتكنولوجيا

المعلومات في التعليم العالي، الجزائر.

٣. البشرى، محمد. (٢٠٠٠): التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات

الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض مج١٥، ع٣٠.

٤. جواد، أشرف. (٢٠١٥): الجريمة المعلوماتية أو الإلكترونية أنواعها وخصائصها وطرق الوقاية منها، مجلة الدراسات المالية والمصرفية - المعهد العربي للدراسات المالية والمصرفية. - الأردن، مج ٢٣، ١٤.
٥. خاطر، مايا. (٢٠١١): الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، سوريا، مج ٢٧، ٣٤.
٦. خلف، سامية. (٢٠١٠): بحث بعنوان "جريمة اختراق أنظمة المعلومات دراسة مقارنة"، مجلة العلوم القانونية، جامعة بغداد.
٧. الداهري، صالح. (٢٠١٥): الإدمان على الإنترنت كثقافة تواصل اجتماعي وأبعاده النفسية والاجتماعية على الأسرة العربية، مجلة كلية التربية الأساسية، جامعة المستنصرية، مج ٢١، عدد ٨٧.
٨. داود، حسن. (٢٠٠٠): جرائم نظم المعلومات، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، ع ٢٤٣، نشر بالمجلة بشهر (٥).
٩. سليم، مزيود. (٢٠١٤): الجرائم المعلوماتية واقعا في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، ع ١٤.
١٠. شيرين، دبابنة. (٢٠١٥): مقال بعنوان "الجرائم الإلكترونية القرصنة الإلكترونية"، مجلة الدراسات المالية والمصرفية - المعهد العربي للدراسات المالية والمصرفية، مج ٢٣، ع ١٤.
١١. الطائي، حعفر. (٢٠١٥): جرائم تكنولوجيا المعلومات وآليات الحد منها، مجلة الفتح، جامعة ديالى، العراق، نُشر (١١).

١٢. عبدالله، نوري. (٢٠١١): بحث منشور بعنوان "العوامل الإجتماعية المؤثرة في ارتكاب الجريمة"، مجلة الأنبار للعلوم الإنسانية، ع١٤.
١٣. علي، أمل، "نظام أمن المعلومات في منظمات الأعمال مع نموذج مقترح لمواجهة تهديدات النظام"، المجلة العراقية للعلوم الادارية، ع٦٤.
١٤. غايب، محروس. (٢٠١١): الجريمة المعلوماتية، بحث منشور في مجلة التقني، هيئة التعليم التقني، مج٢٤، ع٩٤، الأنبار، العراق.
١٥. فتحية، لتيتم، نادية، لتيتم. (٢٠١٥): بحث منشور بعنوان " الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، ع١٢، جامعة بسكرة، الجزائر.
١٦. قطب، محمد. (٢٠١٠): بحث بعنوان "الجرائم المعلوماتية وطرق مواجهتها"، الأكاديمية الملكية للشرطة، مركز الإعلام الأمني التابع للشرطة البحرينية.
١٧. المسند، صالح، المهيني، عبد الرحمن. (٢٠٠٠): جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض مج١٥، ع٢٩٤.
١٨. مصطفى، سمير، وآخرون. (٢٠١١): الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها، بحث منشور في مجلة التقني، هيئة التعليم التقني، مج٢٤، ع٩٤، الأنبار، العراق.
١٩. واصل، محمد. (٢٠١١): بحث منشور بعنوان: الحماية القانونية لبرامج الحاسوب (المصنفات الإلكترونية)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج٢٧، ع٣٤.

المؤتمرات والندوات والدورات

١. البداينة، ذياب، ورقة بحث بعنوان "الجرائم الإلكترونية المفهوم والأسباب" الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية" الواقع من (٢_١٩١٤/٢٠١٤)، عمان، الأردن.
٢. البشرى، محمد، ندوة علمية بعنوان "الإنترنت والإرهاب"، عنوان المداخلة "تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، تاريخ انعقاد الندوة (١٥-١٩/١١/٢٠٠٨).
٣. تتوري، سلام، جرائم الحاسوب والإنترنت، دراسة قدمت للجامعة اللبنانية، كلية الدراسات العليا، قانون الأعمال المحلي والدولي.
٤. جامعة الدول العربية، المركز العربي للبحوث القانونية (٢٠١٢)، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات المنعقد في (٥-٧/٣/٢٠١٢) بيروت، الجمهورية اللبنانية، ص ٦-٧، متاح على الرابط التالي <https://carjj.org/node/1242>.
٥. الحصري، أحمد، درس بعنوان "مقدمة أمن المعلومات"، منتدى الرياض الاجتماعي الثالث، وزارة الشؤون الاجتماعية، السبوعودية، موقع يوتيوب، https://www.youtube.com/watch?v=Q_M5q_aFK7Y، ٢٠١٥.
٦. سندالي، عبد الرازق، مداخلة بعنوان "التشريع المغربي في مجال الجرائم المعلوماتية"، قدمت لندوة تحت عنوان الجرائم المتصلة بالكمبيوتر، المملكة المغربية، تاريخ الإنعقاد (١٩/١٢/٢٠٠٧).

٧. الصالح، صالح، دورة تدريبية بعنوان مكافحة الجرائم الاقتصادية التي ترتكب بواسطة الحاسب الآلي، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، تاريخ عقدها (١٠-٢٠٠٧/٣/١٤م).
٨. الغفيلي، فهد، دورة تدريبية حول توظيف التقنيات الحديثة في العمل الأمني، مداخلة بعنوان "استخدام الحاسب الآلي في الوقاية من الجريمة (جرائم الاختراق نموذجاً)"، جامعة نايف العربية للعلوم الأمنية، تاريخ الانعقاد (٦-٢٠١٣/٣/١٢م).
٩. فرام، كوثر، بحث نهاية تدريب بعنوان "الجريمة المعلوماتية على ضوء العمل القضائي المغربي"، وزارة العدل، المعهد العالي للقضاء، المغرب، فترة التدريب (٢٠٠٧-٢٠٠٩م).
١٠. القهوجي، علي، بحث بعنوان "جرائم التعدي على نظم معالجة المعطيات"، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، ٢٠٠٠.
١١. محاضرة عن نظم المعلومات في جامعة الأندلس الخاصة للعلوم الطبية، طرطوس، سوريا، ص١٤٩، http://au.edu.sy/images/courses/pharmacy/1-2/153_computer-skills.pdf.

المراجع الأجنبية

١. Kahn, Robert, Cerf, Vinton, (Study What Is The Internet and What Makes It Work), 1999, <http://www.policyscience.net/cerf.pdf>

Leiner, Barry,(And Others), **Brief History of the Internet**, .٢

<https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f1>

Principles of Information Systems A ، George، Reynolds، Ralph،Stair .٣

. part2، USA: Cengage Learning،**Managerial Approach**

PRINCIPLES OF ، Herbert،Mattord، Michael،Whitman .٤

، Fourth Edition, USA: Cengage Learning،**INFORMATION SECURITY**

Chapter1

المواقع الإلكترونية

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/d .١

[v/7_conv_budapest_/7_conv_budapest_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<https://ar.wikipedia.org/wiki> .٢

٣. إسماعيل، أيمن،خبر بعنوان دوافع الجريمة في المجتمع الفلسطيني، موقع دنيا الوطن، تاريخ

النشر(٢٠١٧\١٢\٢٧م).

٤. تاريخ الإنترنت في فلسطين، موقع بال ننت،

<https://web.archive.org/web/20030608075650/http://www.palne>

[.t.com:80/about_us/about_us.php](http://www.palne.com:80/about_us/about_us.php)

٥. توم، مجذوب، تكنولوجيا الإتصال وتأثيرها على الجمهور العربي (بالتركيز على فئة الشباب)،

[.http://repository.sustech.edu/handle/123456789/4736](http://repository.sustech.edu/handle/123456789/4736)

٦. خبر منشور على جريدة الشرق الأوسط تحت عنوان "قائد قيادة الإنترنت في البنتاغون يحذر من

هجوم إلكتروني يشعل واشنطن، تاريخ النشر (٢٠١٠\١٩\٢٥م).

<http://archive.aawsat.com/details.asp?issueno=11700&article=588253#>

Wz8vf9LXIdU

٧. خبر نشر على موقع الجزيرة، اختراق وكالة الأنباء القطرية تم من الإمارات،

<http://www.aljazeera.net/portal>

٨. خبر نشر على وكالة معا الإخبارية، كشف قضية إبتزاز فتاة ب١٨٥ ألف شيكل في نابلس،

<https://www.maannews.net/Content.aspx?id=950163>

٩. ردمان، عبدالله، الإنترنت وتطبيقاتها الدعوية للمبتدئين، (د.ن)، (د.م)، المصدر موقع منزل

الاسلام، <https://islamhouse.com/ar/books/53292>

١٠. شريف، عبد العزيز، الاعلام الإلكتروني، موقع <http://k-tab.net>

١١. عالم الكمبيوتر - ما هو الـ TCP/IP ؟، موقع ثقّف نفسك،

<https://www.thaqafnafsak.com/2012/05/tcpip.html>

١٢. عباس، طالب، عواد، عبد الجبار، بحث بعنوان جرائم تقنية المعلومات وإثباتها، موجود على

<https://www.iasj.net/iasj?func=fulltext&ald=34155>

١٣. عبد الجبار، عبدالله، مقال عن الإنترنت والتاريخ التطور والتطبيقات، شبكة الألوكة الثقافية،

<http://www.alukah.net/culture/0/28516>

١٤. عبد الجبار، عبدالله، مقال عن الإنترنت والتاريخ التطور والتطبيقات، شبكة الألوكة الثقافية،

<http://www.alukah.net/culture/0/28516>

١٥. العشي، مصطفى، دورة إنترنت. مركز الأيمن الدولي للمعلوماتية

<files.books.elebda3.net/elebda3.net-7720.pdf>

١٦. لماذا سارع السوفييت لإطلاق أول قمر اصطناعي قبل ٦٠ عاماً؟، <https://arabic.rt.com>

١٧. موقع معجم المعاني، <https://www.almaany.com>

١٨. موقع إحصائيات الإنترنت العالمية، <https://www.internetworldstats.com>،

هاشم، مصطفى، إيجابيات وسلبيات شبكة الإنترنت،

<https://kenanaonline.com/users/mhae2016/posts/398674>