جرائم الاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية

عبدالله ذيب محمود [1]، مأمون مسلم أبو حلو[2]، وهيب عبدالرحمن ابو علبة[3]

[1] كلية القانون – جامعة خضوري، فلسطين

abdullahmahmmoud22@gmail.com [1]

[2،3] كلية القانون – جامعة الاستقلال، فلسطين

الملخص

أدى التطور والانتشار الكبيرين لتكنولوجيا المعلومات وأجهزة الاتصال وزيادة الاعتمادية على الشبكة العنكبوتية إلى استخدامها بشكل واسع في الحياة اليومية للمواطن الفلسطيني، وبالتالي؛ ظهور العديد من الجرائم الإلكترونية المتصلة بها.

وتدور هذه الدراسة حول الحديث عن جرائم الاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، والتي تتمثل بتعطيل أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية على اختلاف أنواعها، فمحل الحماية في جريمة الاعتداء على الأجهزة الإلكترونية والشبكة الإلكترونية هو البرامج المكونة أو الملحقة بالحواسيب والشبكات، بالإضافة إلى البيانات والمعلومات المخزنة، وأيضاً الخدمات التي تقدمها، وقد اتبع الباحثان المنهج الوصفي التحليلي في دراسة هذه الجرائم، وذلك بالرجوع إلى نصوص القرار بقانون رقم -10- لسنة 2018 بشأن الجرائم الإلكترونية، والمعدل بموجب القرار بقانون رقم -38- لسنة 2021 والذي أقرّته الحكومة الفلسطينية للحد من انتشار هذه الجرائم، ومحاولة لاستخلاص وتحليل ومناقشة إرادة المشرع الفلسطيني فيما يتعلق بالحماية القانونية التي وفرها للبرامج الإلكترونية، ومحاولة مزج الجانب التقني مع الجانب القانوني.

ويشير البحث إلى أن المشرع الفلسطيني حاول توفير حماية قانونية للبرامج الإلكترونية انطلاقاً من حق المستخدم في الوصول إلى الجهاز الإلكتروني الخاص به، واستخدام هذه البرامج على الوجه المشروع، وأن تعطيل أو إعاقة الوصول إلى الأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكّل اعتداء على هذا الحق.

الكلمات الدالة: الجرائم الإلكترونية؛ البرامج الإلكترونية؛ الحماية القانونية؛ الاعتداء الإلكتروني.

Crimes of assault on electronic programmes in Palestinian legislation

Abdullah Mahmoud [1], Mamoun Abu Helou [2], Waheeb Abu Ulbeh [3]

[1] College of Law – Kadoorie university, Palestine

[1] **abdullahmahmmoud22@gmail.como**

[2,3] College of Law – Al Istiqlal University, Palestine

Abstract

The development and great spread of information technology and communication devices and the increase in reliability of the Internet have led to its widespread use in the daily life of Palestinian citizens and thus the emergence of many related electronic crimes. This study revolves around talking about the crimes of assaulting electronic programs in Palestinian legislation, which are represented by obstructing or disrupting access to electronic services, devices, programs, or electronic information of all kinds. The object of protection in the crime of assaulting electronic devices and the electronic network is the programs that are configured or accessories to computers and networks, in addition to stored electronic data and information, as well as the services they provide, and researchers have followed the descriptive and analytical approach in studying these crimes by referring to the provisions of the Decree Law No. 10 of 2018 regarding electronic crimes, which was approved by the Palestinian government to limit the spread of these crimes, and trying to extract, analyze, and discuss the will of the Palestinian legislator with regard to protection It provided legal protection for electronic programs and an attempt to mix the technical side with the legal side, noting that the Palestinian legislator tried to provide legal protection for electronic programs based on the user's right to access his electronic device and to use this program in a legitimate manner, and that obstructing or disrupting access to electronic devices, the electronic network, and the accessory programs constitutes a violation of this right.

Keywords: Cybercrime; electronic programmers; legal protection; cyber assault.

Received 17/10/2022 Revised 07/12/2022 Accepted 05/01/2022

مقدمة

في ظل الانتشار الواسع لاستخدام وسائل تكنولوجيا المعلومات والاتصال (ITC- Information Tech-nology and Communication) في مختلف أنشطة الحياة سواء الاقتصادية أو الصحية أو التعليمية أو المالية أو الترفيهية أو الاجتماعية وغيرها؛ بغية تسهيل وسرعة إنجاز الأعمال من خلال إتاحة توفر القدرة إلى الوصول ومعالجة البيانات المخزنة على الأنظمة الحاسوبية الموجودة بأشكال مختلفة في كل مكان، والمتصلة فيما بينها من خلال شبكات الاتصال؛ فعلى سبيل المثال انتشار التطبيقات الذكية (Smart Applications) والأجهزة الذكية (Smart Devises) في مناحي مختلفة في حياتنا واتصالها بشبكات الاتصال لا سيما شبكة الإنترنت، والذي بات يعرف بإنترنت الأشياء(Internet of Thing -IoT)، وبناء عليه؛ كان لزاماً على المؤسسات والأفراد على حد سواء التنبه إلى حماية هذه الأنظمة وما تمثله من أصول قيّمة من معدات وبرمجيات وبيانات، بحيث يجب توفير بيئة آمنة لها (الحمامي،الحكيم،2017، ص91) (العريشي، الشلهوب، 2016، ص21) (سليمة، 32، ص 2017) (الحسيناوي،2008، ص 18)، فالإنترنت ليس فقط أن يتأذى الناس وهو المكان الذي يتعلم فيه الأطفال والشباب عن العالم المحيط بهم (رئيس الوزراء البريطاني السابق ديفيد كاميرون، في خطابه أمام الجمعية الوطنية لمنع القسوة ضد الأطفال (NSPCC) في عام 2013)

وقد تنبه المشرع الفلسطيني إلى مدى خطورة وقوع الجرائم الإلكترونية بشكل عام، ومنها جرائم الاعتداء على البرامج الإلكترونية بشكل خاص، وتقع هذه الجرائم نتيجة سوء استخدام وسائل تكنولوجيا المعلومات وشبكات الاتصال (الحسيناوي،2008، ص20) (باطلي، 2015، ص24).

وتوجد عدة تصنيفات للجرائم الإلكترونية، والتي تستهدف الأفراد والمؤسسات والجماعات والدول (دراية، 2022) ويمكن تصنيفها بشمولية إلى **أربعة أقسام**:

أولا: جرائم تستهدف الأفراد: وهي جرائم تستهدف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات مهمة واستغلالها في ابتزاز الضحايا بالقيام بأعمال غير مشروعة.

ثانيا: جرائم تستهدف المؤسسات: والتي تتسبب بخسائر مادية كبيرة للمؤسسات والشركات، وأخرى تتعلق باختراق الأنظمة والمواقع الإلكترونية.

ثالثا: جرائم تستهدف الأموال: كالاستيلاء على حسابات بنكية أو حقوق الملكية الفكرية.

رابعا: الجرائم التي تستهدف أمن الدولة: كالتجسس أو التحريض على الإرهاب.

وتصنف جرائم الاعتداء على البرامج الإلكترونية من ضمن هذه التصنيفات والتي تقع ضمن الجرائم التي تستهدف المؤسسات، وتتمثل هذه الجريمة بالاعتداء على برامج الحاسوب وفقاً للمشرع الفلسطيني سواء من خلال إعاقة أو تعطيل الوصول إلى البرامج أو ما تقدمه من خدمات، وأيضاً من خلال إنتاج أو إدخال عن طريق الشبكة الإلكترونية أو إحدى مساوئ لتكنولوجيا المعلومات ما من شأنه إيقاف هذه البرامج عن العمل أو تعطيلها أو اتلافها[1] أو حذفها أو تعديلها وما يترب على ذلك من الاعتداء من سرقة أو تعديل أو تزوير أو تعطيل على البيانات المرتبطة بها من تخزين أو وصول؛ ولذلك جاء القرار بقانون رقم -10- لسنة 2018 بشأن الجرائم الإلكترونية والمعدل بموجب القرار بقانون رقم -38- لسنة 2021 ليوفر الحماية القانونية لهذه البرامج.

1 نصت المادة الأولى من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية على تعريف الإتلاف، بأنه «تدمير البرامج الإلكترونية، سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال».

أهمية الدراسة:

تكمن أهمية الدراسة في تناولها لجرائم الاعتداء على البرامج الإلكترونية على اختلاف أشكالها، وعليه فإن أهمية الدراسة تنبع من كونها الدراسة الأولى التي تتناول جريمة تعطيل البرامج الإلكترونية طبقا للقرار بقانون رقم -10- لسنة 2018 بشأن الجرائم الإلكترونية، بالإضافة إلى محاولة استخلاص إرادة المشرع الفلسطيني من النصوص القانونية الناظمة لتجريم الاعتداء على البرامج الإلكترونية، وتوضيح ماهية هذا الجريمة والتي أصبحت منتشرة بشكل كبير على مستوى العالم لاسيما المجتمعات العربية.

إشكالية الدراسة:

تبرز مشكلة الدراسة في الإجابة عن السؤال الرئيسي وهو: ما الطبيعة القانونية للجرائم المتعلقة بالاعتداء على البرامج الإلكترونية، وما العقوبات المتعلقة بها؟

كما ستجيب الدراسة على مجموعة من الأسئلة، وهي على النحو الآتي:

- ما أركان جريمة تعطيل وإعاقة الوصول إلى البرامج الإلكترونية؟
- ما أركان جريمة إنتاج وإدخال البرمجيات الخبيثة بقصد إلحاق الضرر بالبرامج الإلكترونية؟

أهداف الدراسة:

تهدف الدراسة إلى التعرف على الطبيعة القانونية للجرائم المتعلقة بالاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، كذلك التعرف على العقوبات المنصوص عليها لهذه الجرائم، كما ستهدف الدراسة إلى محاولة تفسير وتحليل النصوص القانونية بجريمة تعطيل وإعاقة الوصول إلى البرامج الإلكترونية، والتعرف وتحليل النصوص المتعلقة بجريمة إنتاج البرمجيات الخبيثة وإدخالها بقصد تعطيل البرامج وحذفها.

منهجية الدراسة:

تقوم هذه الدراسة على المنهج الوصفي التحليلي، من خلال دراسة وتحليل النصوص القانونية المتعلقة بجرائم الاعتداء على البرامج الإلكترونية في التشريعات الفلسطينية، والواردة في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، واستخلاص إرادة المشرع من تلك النصوص.

خطة الدراسة:

قُسمت الدراسة إلى مطلبين؛ جاء المطلب الأول ليتناول جريمة إعاقة الوصول إلى البرامج الإلكترونية، بينما تناول المطلب الثاني جريمة إنتاج وإدخال برمجيات الخبيثة بقصد تعطيل البرامج وحذفها. وسيأتي تفصيلها من خلال تبيان الركن المادي والمعنوي لكل منها.

المطلب الأول:

جريمة إعاقة الوصول إلى البرامج الإلكترونية

تعد البرمجيات أو ما يعرف بالكيان غير المادي(software) أحد العناصر الأساسية والتي تشكل بالإضافة إلى المعدات (Hardware) والبيانات (data)والعنصر البشري/ المستخدمين (users) نظام الحاسوب، وتعتبر البرامج الإلكترونية (programs) وكل مكونات نظام الحاسوب التي لا نستطيع لمسها بأيدينا من البرمجيات، أي الكيان غير المادي (باسل مصطفى الخطيب وآخرون،2016، ص23), (مصابيح المعرفة, 2020) (Pfleeger, Margulie, 2015 ,p3)

وتعّرف البرامج الإلكترونية (الخطيب وآخرون،2016، ص83) على أنها «مجموعة من التعليمات المتسلسلة التي تخبر الحاسوب ماذا يفعل»، ويعرفها (السيد،2018، ص132) على أنها «مجموعة من التعليمات والأوامر (مكتوبة بلغة برمجة) توضح للحاسوب تسلسل الخطوات (الخوارزميات) التي ينبغي القيام بها لأداء مهام معينة لحل المشكلة المطروحة واستخراج النتائج، ويختزن البرنامج في الذاكرة الرئيسية للحاسب لتوجهه إلى إنجاز العمليات المطلوبة، وتمكنه أيضا، من إدارة ومراقبة وتنظيم مكوناته المادية لتحقيق المهمة المطلوبة».

هذا ولم يأتي المشرع الفلسطيني على تعريف البرامج الإلكترونية بشكل ضمني، حيث يندرج هذا الوصف للبرمجيات ضمن تعريف المشرع لمصطلح تكنولوجيا المعلومات بأنها «أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية **أم غير مادية**، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة»(المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية).

وقد عرّف المشرع الفلسطيني التطبيق الإلكتروني (Electronic Application) على أنه «برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال لوسائل تكنولوجيا المعلومات أو ما في حكمها»(المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية)، ومثال على هذه البرامج هو برنامج أداة التوقيع: ويعرفه المشرع على أنه «برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة»(المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية).

وتعد الجريمة الواقعة على البرمجيات من الجرائم الإلكترونية والتي تصنف كجنحة، حيث تتمثل بتعطيل الوصول أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية على اختلاف أنواعها، وهنا تقوم هذه الجريمة على ركنين هما: الركن المادي والركن المعنوي، (عبدالله محمود، أسامة دراج، الجرائم الإلكترونية، ص102)، وهو ما نص عليه المشرع الفلسطيني في القرار بقانون رقم 10 لسنة 2018 في المادة (5)، والتي جاءت على النحو التالي: « كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، 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 «.

الفرع الأول: الركن المادي لهذه الجريمة (Corpus Delicti)

تعتبر هذه الجريمة من الجرائم الحديثة التي لم تكن شائعة من قبل، فهذه الجريمة تقوم في جوهرها على التعطيل المتعمد للبرامج الإلكترونية أو شبكات الاتصالات الإلكترونية، هذا وتتنوع البرامج وتختلف حسب طبيعة المهام المسندة إليها، وتنقسم هذه البرامج إلى نوعين رئيسين من البرامج: الأول برمجيات النظم (system soft-ware)، والثاني البرمجيات التطبيقية (Application Software) (الخطيب وآخرون،2016، ص84)، حيث تعمل برمجيات النظم على التحكم والإشراف على منظومة عمل الحاسوب بأكمله من مكونات مادية وبرمجيات، وتعمل على التنسيق والتناغم بينهما لأداء وظائف الحاسوب، وتنقسم برمجيات النظم إلى ثلاثة أنواع رئيسية وهي: نظم التشغيل(operating system)، معالجة اللغات (language processer)، والبرامج المساعدة(utility software) (باسل مصطفى الخطيب وآخرون،2016،ص85)(الزعبي،الشرايعة،2009،ص43 - 45)(القاضي، 2007، ص14)، وفي ما يلي تبيان لكل منها:

1) برامج نظم التشغيل (Operating System (OS)

ينظر إلى نظام التشغيل على أنه مجموعة من البرامج التي تتحكم بشكل فعال بمكونات الحاسوب وتجعلها متوفرة بشكل مناسب للمستخدم، وتقوم هذه البرامج بشكل أساسي بإدارة مكونات الحاسوب من اجل تكاملها مع بعضها في تنفيذ المهام المطلوبة سواء بشكل مباشر من المستخدم أو من برنامج داخل النظام، و يتحقق ذلك من خلال مجموعة من الوظائف منها تنظيم المشاركة الزمنية لهذه المصادر وإدارة الملفات. (منال البلقاسي،2019، ص19) (فايز الحمودي، عدنان الهلالي،2009، ص15) (القاضي،2007، ص19) ويمكن اعتباره جسر لتشغيل برامج المستخدم فالحاسوب بدون نظام تشغيل مجرد قطعة مادة لا فائدة منها, ومن الأمثلة على أنظمة التشغيل: DOS, Windows, Mac, Android, Linux (مصابيح المعرفة, 2020)

2) معالجة اللغات (Language Processer)/ لغات البرمجة (Programming Languages)

تستخدم الحواسيب لغة الآلة أو ما يعرف باللغة الثنائية (Binary)، لذا يجب ترجمة البيانات والتعليمات الخاصة بالبرامج التي تكتب بلغات الأداء العالي إلى لغة الآلة في مرحلة الإدخال ومرحلة الإخراج، حيث يقوم برنامج المترجم أو المفسر (Compiler\interpreter) بعملية فك الشفرة الخاصة بالبيانات والتعليمات، وتحويلها إلى لغة الآلة تمهيداً لتمكين الحاسوب من القيام بمعالجة البيانات وتنفيذ التعليمات، والعكس صحيح عند إجراء عملية إخراج البيانات مثلاً على الشاشة أو الطابعة(الزعبي، الشرايعة، 2009،ص 45) أي أنها تصنف كبرامج تستخدم لعمل برامج مختلفة ويتم تحديثها من قبل المبرمجين لتحقيق أهداف معينة ومن الأمثلة على ذلك لغات عالية المستوى (قريبة من اللغة التي يفهمها البشر) مثل لغة جافا ولغة سي, ولغات منخفضة المستوى (قريبة من لغة الآلة) مثل لغة التجميع Assembly(مصابيح المعرفة, 2020)

3) البرامج المساعدة ((Utility Programs

تعرف البرامج المساعدة أو برامج الخدمة بأنها عبارة عن برامج تهدف إلى تحليل جهاز الحاسوب أو تكوينه أو المساعدة في صيانته، وعادة ما تكون الأداة المساعدة أصغر من البرنامج القياسي ويمكن تضمينها مع نظام التشغيل أو تثبيتها بشكل منفصل ومن أمثلتها: برنامج مضاد الفيروسات Antivirus أو برامج النسخ الاحتياطي Backup, أو مراقب النظام (System Monitor, (Computerhope, 2022

كذلك هناك نوع مهم من البرامج وهو البرامج التطبيقية، ويشار إليها أيضاً بالتطبيق وهي عبارة عن حزمة برامج حاسوبية تؤدي وظيفة محددة مباشرة للمستخدم النهائي أو في بعض الحالات لتطبيق آخر ويمكن

ان يكون التطبيق قائما بذاته أو كمجموعة من البرامج ومن الأمثلة على التطبيقات: برنامج معالج النصوص MS Word, ومتصفحات الانترنت (Techtarget, Web Browsers, 2021)

وتعد أيضاً من البرامج التي تعد خصيصاً لحل مشكلة أو مشاكل معينة يرغب المستفيد في استخدام الحاسوب في حلها، وتكتب هذه البرامج إما بواسطة المستفيد (أو ما يسمى مطور برمجي program developer) أو الحصول عليها من الشركات التقنية المتخصصة في هذا المجال. (الخطيب وآخرون،2016، ص88)

وتجدر الإشارة هنا إلى أنه حتى وإن لم يكن الغرض الأساسي للجهاز هو الحوسبة (معالجة البيانات[2])، يمكن أن يتعرض الحاسوب المضمن بالجهاز الإلكتروني لحوادث أمنية قد تلحق الضرر بأحد مكوناتها المادية (Hard-ware) او غير المادية (Software) (عيدي سليمة،2017، ص34)(Pfleeger, Margulie, 2015 ,p5).

فالمقصود من توفير الأمان هنا هو حماية جميع عناصر النظام (الأصول- Assets) التي تتوجب حمايتها من وجهة نظر المستخدم، وتشمل إمكانية الوصول إلى البيانات وتوفر الخدمة وجودتها وتوفرها والعمليات المتاحة للمستخدمين والاتصال بالشبكة.

فالهدف من أمان نظام الحاسوب هو حماية هذه الأصول، ويعرف أمان الحاسوب (Computer Securi-ty) على أنه حماية أنظمة الحوسبة والبيانات التي تخزنها أو تصل إليها(1.Pfleeger et al, 2015, P) من الأذى والسرقة والاستخدام غير المصرح به، والسبب الرئيسي لتعرض المستخدمين للهجوم بشكل متكرر هو افتقارهم إلى الدفاعات الكافية لإبعاد المتسللين، ويسرع مجرمو الإنترنت في استغلال نقاط الضعف، وبالتالي؛ يعزز أمان الحاسوب مبدأ سرية البيانات المخزنة وسلامتها وتوفرها (Simplilearn, 2022)

وتتمثل جريمة الاعتداء على أنظمة الحاسوب بمجموعة الأفعال تشكل السلوك المادي المفترض في الركن المادي، والذي يتكون من نشاط ونتيجة وعلاقة سببية، فالنشاط الجرمي يتمثل بسلوك ايجابي (المجالي، 2012، 236) كالاعتراض (interception)، والانقطاع (interruption)، والتعديل (modification)، والتزوير (fabrica-tion)(الحمامي،العاني،2007، ص29) (العريشي والدوسري:2018، ص177)(6.Pfleeger et al, 2015, p).

ويمكن تلخيص الأنشطة الجرمية الإيجابية في الركن المادي على النحو التالي:

- **الاعتراضات (Interceptions)** يعني أن طرفًا غير مصرح له قد حصل على حق الوصول إلى أحد الأصول، ويمكن أن يكون الطرف الخارجي شخصًا أو **برنامجًا** أو نظامًا حاسوبيًا، ومن الأمثلة على هذا النوع؛ النسخ غير المشروع **للبرنامج** أو ملفات البيانات، أو التنصت على عمليات الإرسال وإعادة توجيهها للاستخدام غير المصرح به في الشبكة، وعلى الرغم من إمكانية اكتشاف الخسارة بسرعة إلى حد ما، إلا أن المعترض الصامت قد لا يترك أي أثر يمكن من خلاله اكتشاف الاعتراض بسهولة.

2 نصت المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية على تعريف معالجة البيانات، وهي «إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات أو استلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها، أو إعادة نشر بيانات أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها».

- **الانقطاعات (Interruptions)** تعني أن أحد أصول النظام أصبح مفقودًا أو غير متوفر أو غير قابل للاستخدام، ويتسبب الانقطاع في انقطاع قناة الاتصال مما يحول دون إرسال البيانات (Kim & Solomon, 2018) ومن الأمثلة على ذلك التدمير الضار لجهاز، أو محو **برنامج** أو ملف بيانات، أو خلل في مدير ملفات نظام التشغيل بحيث يتعذر عليه العثور على ملف قرص معين.

- **التعديلات (Modifications)** تعني أن طرفًا غير مصرح له قد حصل على حق الوصول إلى أحد الأصول وعبث به، على سبيل المثال، قد يقوم شخص ما بتغيير القيم الموجودة في قاعدة بيانات، أو تغيير أحد **البرامج** بحيث يقوم بإجراء عملية حسابية إضافية ، أو تعديل البيانات التي يتم إرسالها إلكترونيًا، حيث يمكن الكشف عن بعض حالات التعديل بمقاييس بسيطة، لكن التغييرات الأخرى الأكثر دقة قد يكون من المستحيل تقريبًا اكتشافها.

- **التلفيقات(Fabrications)** يعني أن يقوم طرف غير مصرح له بإنشاء ملفق لأشياء مزيفة على نظام حوسبة، فقد يقوم الدخيل بإدخال معاملات زائفة إلى نظام اتصالات الشبكة أو إضافة سجلات إلى قاعدة بيانات موجودة، وفي بعض الأحيان يمكن اكتشاف هذه الإضافات على أنها مزيفة، ولكن إذا تم إجراؤها بمهارة، فلا يمكن تمييزها فعليًا عن الشيء الحقيقي، وتشمل أحيانا اختلاق بعض الخدع لخداع المستخدمين المطمئنين (غير المتشككين).

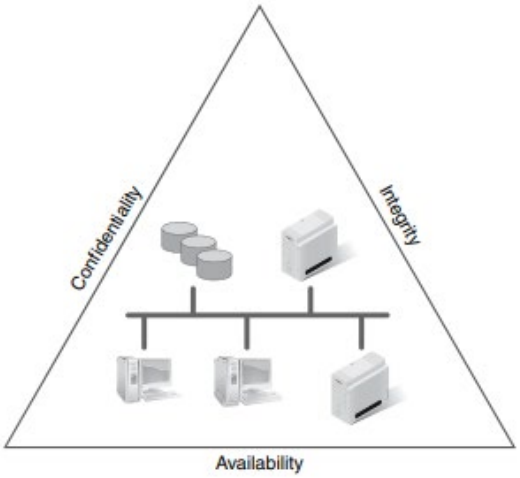
وعليه؛ فإن النتيجة الجرمية تتلخص في منع استخدام البرامج بسبب نشاط التعطيل للبرمجيات، أو منع الوصول إلى أجهز الحاسوب أو الأجهزة الإلكترونية الأخرى كأجهزة الاتصال الحديثة، أو تعطيل الدخول إلى مواقع معينة أو برامج معينة من خلال التعديلات أو التلفيقات، والتي أدت إلى تعطيل بعض البرامج، أو القيام بتغيير بعض البيانات والبرمجيات لأنظمة الحاسوب أو البرامج الإلكترونية بغية تعطيلها، وبالرجوع إلى نص المادة 5 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، والمعدل بموجب القرار بقانون رقم 38 لسنة 2021؛ نلاحظ أن المشرع الفلسطيني توسع في السلوك المادي لهذه الجريمة، حيث ذكر العديد من الأنشطة كإعاقة الوصول إلى الخدمات الإلكترونية أو تعطيل الوصول إلى هذه الخدمات أو الدخول إلى الأجهزة الإلكترونية على اختلاف أنواعها، وتشمل أي من وسائل تكنولوجيا المعلومات سواء أكانت أجهزة حاسوب، أو أجهزة اتصال حديثة، أو أجهزة تلفاز حديثة أو البرامج التي يمكن تحميلها أو المحملة من المصدر أو تعطيل الوصول إلى مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات.

وبالتالي؛ فإن السلوك الجرمي يجب أن يكون السبب المباشر لوجود النتيجة الجرمية، والتي تتلخص بمنع الوصول إلى البرامج من خلال مسح البيانات والمعلومات أو التعديل عليها وغيرها من الأنشطة الجرمية المحظورة.

ووفقاً للمختصين في مجال أمن المعلومات والأمن الإلكتروني؛ يتم منع الاعتداء على هذه الأصول وعدم تنفيذ التهديدات (threats)عليها من خلال العمل بالضوابط (control) المناسبة التي تتحكم في نقاط الضعف (weak-ness/vulnerability) وتمنع استغلالها لإحداث ضرر للأنظمة المحوسبة، ويتفق معظم الناس على أن المعلومات الخاصة يجب أن تكون آمنة، ولكن ماذا يعني أن تكون «المعلومات الآمنة»؟ المعلومات الآمنة يجب أن تستوفي ثلاثة مبادئ أو خصائص رئيسية، وإذا كان بإمكاننا ضمان هذه المبادئ الثلاثة، فنحن نفي بمتطلبات الأمان وهي كما يلي:

- **السرية** (Confidentiality)- يمكن للمستخدمين المصرح لهم فقط عرض المعلومات.

- **السلامة** (Integrity) - يمكن للمستخدمين المصرح لهم فقط تغيير المعلومات.
- **التوافر** (Availability)- المعلومات يمكن الوصول إليها من قبل المستخدمين المصرح لهم كلما طلبوا ذلك. ويوضح الشكل 1 المبادئ الثلاثة لأمن أنظمة المعلومات (Kim & Solomon, 2018).



الشكل 1- المبادئ الثلاثة لأمن أنظمة المعلومات (المصدر: Kim & Solomon, 2018).

إن فهم الأساسيات بتحديد الهوية(Identification) والمصادقة (Authentication) والتفويض (Authorization) والتدقيق (Auditing) والمساءلة (Accountability) وعدم التنصل أو الإنكار (Non - repudiation) سيقطع شوطًا طويلاً في فهم وتعزيز الأمان الإلكتروني. وتالياً نورد توضيحا لهذه المفاهيم.

تحديد الهوية Identification: هو القدرة على تحديد هوية المستخدم بشكل فريد (أو نظام أو تطبيق أو عملية)، ومثال ذلك: إدخال اسم المستخدم / معرف المستخدم / رقم الحساب في صفحة تسجيل الدخول / موقع الويب / التطبيق أو تقديم يدك على ماسح بصمة الإصبع (أو مواجهة الكاميرا للدخول إليها)

المصادقة Authentication : هي عملية التحقق من ادعاء الهوية (تحديد الهوية والتحقق) (Identification & Verification), ومثال ذلك: الهوية Identity (اسم المستخدم Username) و التحقق Verification (كلمة المرور Password) ، وتعتمد المصادقة Authentication على عاملين Two factor authentication أو أكثر (متعددة العوامل) multi-factor authentication، ومثال ذلك: استخدام كلمة مرور (شيء تعرفه) ورمزًا مميزًا (شيء لديك) لتسجيل الدخول.

التفويض Authorization : يقرر ما يمكن للهوية الوصول إليه (مستوى الوصول إلى مورد) أو تؤديه بمجرد المصادقة، أي أنه يعتبر وسيلة تقرير ما «تستطيع» الهوية «فعله» و «لا يمكنها» فعله على البرنامج أو الوصول إلى البيانات.

التعريف: يقوم المستخدم (الهوية) الذي يريد الوصول إلى كتاب إلكتروني، بإدخال اسم المستخدم وكلمة المرور الخاصة به في تطبيق ويب يقدم الخدمات.

المصادقة: يلتقط تطبيق الويب التفاصيل ويرسلها إلى خادم خلفية للتحقق من تركيبة اسم المستخدم وكلمة المرور. يتحقق الخادم من الإدخالات ويوافق (التعريف والتحقق) على الهوية إذا كانت المجموعة صحيحة، قائلاً «نعم، إنها

هوية صالحة» ولها حق الوصول إلى قاعدة بيانات الكتاب الإلكتروني.

التدقيق Auditing: هو فحص وتقييم موضوعي للوضع الأمني للمؤسسة يتم إجراؤه عادةً بواسطة طرف ثالث مستقل - داخلي (على سبيل المثال، قسم التدقيق الداخلي) أو خارجي (على سبيل المثال، الهيئات التنظيمية، إلخ)، تستخدم عمليات التدقيق للتحقق من صحة السياسات والإجراءات الأمنية للمؤسسة، والضوابط المعمول بها، والامتثال للوائح، ويساعد في كشف الاحتيال أو الأنشطة الخبيثة أو الأنشطة غير المصرح بها, حيث تساعد عمليات التدقيق في التحقق من الامتثال وتساعد في تحميل الموضوع المسؤولية عن أفعاله أو أنشطته.

المساءلة Accountability: وفقًا للمعهد الوطني للمعايير والتقنية NIST، فإن المساءلة هي «المبدأ القائل بأن الفرد مكلف بحماية ومراقبة المعدات ومواد المفاتيح والمعلومات وهو مسؤول أمام السلطة المناسبة عن فقدان أو إساءة استخدام تلك المعدات أو المعلومات.»

وهي القدرة على مساءلة الفرد (الشخص الذي يقوم بعمل ما) عن أفعاله على كائن ما (على سبيل المثال، قاعدة بيانات، أو ملف، أو نظام، أو تطبيق، وما إلى ذلك).

ونحتاج المساءلة لضمان أن كل أصل معلومات «مملوك» من قبل فرد في المنظمة يكون مسؤولاً بشكل أساسي عنه، ويمكن محاسبته في حالة وقوع حدث، ويساعد على ضمان واجبات ومسؤوليات جميع الموظفين للتعامل بعناية مع المعلومات التي يستخدمونها.

عدم التنصل/الإنكار Non - repudiation: هو عدم القدرة على إنكار المسؤولية عن أداء عمل معين، ويتعلق الأمر بالتقاط أدلة دامغة حول الأحداث أو الإجراءات التي قام بها فرد أو موضوع ، بحيث لا يمكن رفض تنفيذ هذا الإجراء، أي من قام بهذا الإجراء، وما الإجراء الذي تم تنفيذه، وإثبات منشأ الأحداث، والطابع الزمني، وما إلى ذلك، ومثال ذلك: في الاتصال الرقمي والهدف من عدم التنصل هو القدرة على إثبات أن رسالة معينة مرتبطة بهوية أو موضوع أو فرد أو مرسل معين، ومن الضوابط التي يمكن أن تساعد في إثبات عدم التنصل، سجل المتصفح ومعرفات الجلسة والسجلات وما إلى ذلك (Rajexh, 2021).

وبالنظر إلى معايير الأمان الأساسية، فإن سياسة أمن تكنولوجيا المعلومات تحتوي على أربعة مكونات رئيسية:

1. **السياسة Policy:** وهي عبارة عن بيان مكتوب قصير حدده المسؤولون عن المنظمة كمسار عمل أو اتجاه، وتأتي السياسة من الإدارة العليا وينطبق على المنظمة بأكملها.
2. **المعيار Standard**: وهو تعريف مكتوب مفصل للأجهزة والبرامج وكيف سيتم استخدامها، تضمن المعايير استخدام ضوابط أمنية متسقة في جميع أنحاء نظام تكنولوجيا المعلومات.
3. **الإجراءات Procedures**: هذه تعليمات مكتوبة حول كيفية استخدام السياسات والمعايير. قد تتضمن خطة عمل وتركيب واختبار وتدقيق ضوابط الأمان.
4. **المبادئ التوجيهية Guidelines:** وهي الدليل الإرشادي هو مسار عمل مقترح لاستخدام السياسة والمعايير أو الإجراءات، ويمكن أن تكون محددة أو مرنة فيما يتعلق بالاستخدام. (Kim & Solomon, 2018)

ويلاحظ مما سبق أن أهمية تطبيق معايير الأمان قد يساهم في منع ارتكاب هذه الجريمة، مع الإشارة إلى أن هناك تطوراً مستمراً في ابتكار أدوات ووسائل حديثة لارتكاب مثل تلك الجرائم إلا أن المشرع الفلسطيني حاول جاهداً توفير حماية كافية للبرامج الإلكترونية، حيث تعتبر تلك البرامج على اختلاف أشكالها محلاً لارتكاب مثل تلك الجرائم، وبالتالي قد تتواجد هذه البرامج على الأجهزة الإلكترونية والشبكة الإلكترونية، بالإضافة إلى البيانات والمعلومات الإلكترونية، أما بالنسبة للنتيجة الجرمية والتي تتمثل في عدم قدرة المجني عليه في الوصول إلى الخدمات الإلكترونية، بل وقد تتمثل النتيجة الجريمة في تعطل البرامج الإلكترونية وإعاقة عملها، مع الاشارة إلى أن إعاقة الوصول إلى الأجهزة الإلكترونية، لا تعني عدم الوصول بالمطلق من قبل المستخدم لهذه لجهاز الإلكتروني أو الشبكة الإلكترونية، بل يمكن الوصول من قبل المستخدم لجهازه الإلكتروني الخاص، ولكن بصعوبة نتيجة المعوقات التي صنعها أو أدخلها الجاني، من خلال التحريف والتعديل في البرمجيات الخاصة في الجهاز الالكتروني، أو إدخال برمجيات خبيثة أو غيرها من الوسائل، وهنا لا بد من الاشارة إلا أن المشرع توسع بذكر وسائل التعطيل والإعاقة للأجهزة الإلكترونية أو الشبكة الإلكترونية من أجل توفير أكبر قدر من الحماية لها.

ويلاحظ هنا أن المشرع الفلسطيني حاول توفير هذه الحماية انطلاقاً من حق المستخدم في الوصول إلى الجهاز الالكتروني الخاص به أو الخدمات الإلكترونية، (عبدالله محمود، أسامة دراج، الجرائم الإلكترونية، ص103)، وأن تعطيل أو إعاقة الوصول للأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكل اعتداء على هذا الحق.

الفرع الثاني: الركن المعنوي.

هذه الجريمة لا تقوم إلا عمدية، وهو ما يمكن أن يستخلص من نص المادة (5) من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية والتي جاءت على النحو التالي: « كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، 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؛ تقوم هذه الجريمة على القصد الجنائي العام (للمزيد حول القصد الجنائي أنظر المجالي، 2012، ص250) ، بحيث يكون التعطيل أو إعاقة الوصول إلى الخدمات الإلكترونية متعمداً سواء كان التعطيل مباشراً أو غير مباشر، أو من خلال برامج، أو إدخال برمجيات خبيثة من خلال إرسالها عبر شبكات الاتصال، وذلك لمنع الوصول إلى الخدمات (حجب الخدمة) أو الدخول إلى الأجهزة الإلكترونية على اختلاف أنواعها أو تعطيل الوصول إلى مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، هذا ويشترط أن يتوفر العلم لدى المجاني بأن ما يقوم به هو عمل غير مشروع، ولكن تتجه إرادته نحو القيام بهذا السلوك رغم معرفته بعدم مشروعيته.

لكن ماذا لو كان التعطيل بصورة غير مقصودة، نتيجة خطأ من قبل المستخدم، وذلك نتيجة استخدامه لجهاز مستخدم آخر، وعلى سبيل المثال: قام بتحميل برنامج أو إدخال بيانات على الجهاز بحسن نية وتبين فيما بعد أن البرنامج أو البيانات المحملة هي عبارة عن برمجيات خبيثة، فهنا لا محل لقيام جريمة، باعتبار أن هذا الفعل لم يكن مقصوداً، وهنا نثير التساؤل التالي:

ماذا لو أدى خطأ الفاعل إلى حدوث أضرار بجهاز الحاسوب الخاص بالمستخدم الآخر؟ وهنا نرى أنه يمكن للمستخدم صاحب جهاز الحاسوب الذي لحقه ضرر نتيجة خطأ الفاعل أن يعود عليه بالتعويض عن الأضرار التي لحقت به، ويعود تقدير الأضرار بناء على تقدير خبير يستعين به قاضي الموضوع (عبدالله محمود، أسامة دراج، الجرائم الإلكترونية، ص103). ويعاقب الجاني بالحبس حيث تكون مدته من أسبوع إلى ثلاث سنوات، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، بكلتا العقوبتين، كما وتضاعف العقوبة إلى الثلث في حال كان الجاني موظفاً عاماً، وهو ما أشارت إليه المادة (27) من القرار بقانون المتعلق بالجرائم الإلكترونية، ويعاقب المشترك والمحرض بنفس عقوبة الفاعل الأصلي وهو ما أشار إليه المشرع الفلسطيني في المادة (28) من القرار بقانون الخاص بالجرائم الإلكترونية، كما تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني وهو ما أشار إليه المشرع الفلسطيني في المادة (51) من القرار بقانون الخاص بالجرائم الإلكترونية.

كما وتضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية: 1. إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية. 2. ارتكاب الجاني الجريمة من خلال عصابة منظمة. 3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية. 4. إذا وقعت الجريمة على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية، وهو ما أشار إليه المشرع الفلسطيني في المادة (52) من القرار بقانون الخاص بالجرائم الإلكترونية.

ويلاحظ أن المشرع أعطى سلطة تقديرية واسعة لقاضي الموضوع، حيث تدخل هذه الجريمة ضمن اختصاص محكمة الصلح في النظام القضائي الفلسطيني.

المطلب الثاني:

جريمة إنتاج أو إدخال برمجيات خبيثة بقصد تعطيل البرامج وحذفها

يعرف البرنامج الضار/الخبيث (Malicious Software) وتكتب اختصارا Malware بأنه برنامج حاسوبي تم تطويره بشكل خبيث ليتم تثبيته على أجهزة الحاسوب دون موافقة المستخدمين

تهدف هذه البرمجيات إلى تعطيل الأجهزة الإلكترونية أو الحواسيب، كالاستحواذ على مساحة القرص الصلب أو على جزء من المعالج، أو تخريب البيانات، وإظهار رسائل مزعجة على شاشة المستخدم، أو رصد لوحة مفاتيح المستخدم ومعرفة ما يكتب (التجسس على المستخدمين)، كذلك إرسال رسائل بريدية غير مرغوب فيها لجهات اتصال المستخدم، وقد يشمل معرفة استراتيجيات العمل وتخريب النظام الحكومي وغيرها, (Thakur & Pathon, 2020)، ويستخدم أحياناً مصطلح الفيروسات (viruses) كمصطلح عام عوضاً عن البرمجيات الخبيثة (Malicious Software)، والنقطة الأساسية التي يجب التنبه لها في كيفية تحديد البرامج الخبيثة يكون بناءً على استخدامها الضار وليس على أساس تقنية معينة فعلى سبيل المثال: الشخص الذي يريد معرفة الفرق بين البرنامج الخبيث والفيروس ويستخدمها بالتناوب يخطئ قليلا، لأن الفيروس يعتبر نوعاً من أنواع البرامج الخبيثة، لذا؛ فإن كل

الفيروسات هي برامج خبيثة (ولكن ليس كل جزء من البرنامج الخبيث تعتبر فيروسات), (csoonline, 2022).

وقد تأتي البرمجيات الخبيثة بأشكال عديدة تحت أسماء متنوعة وأكثرها شيوعًا هي الفيروسات (viruses)، والديدان(worms)، وأحصنة طروادة (Pfleeger et al, 2015, P)(Trojan horses.196). والجذور الخفية (Root-kit)، وبرامج التجسس (Spyware), وبرامج الإعلانات المتسللة (Adware), والبرمجيات التخريبية (Scareware), وبرمجيات خاطفة المتصفح (Browser Hijacker). ويعد فيروس الحاسوب أحد أكثر المصطلحات المعروفة في عالم الأمن الإلكتروني مثل أي فيروس بيولوجي خطير ينذر العلماء، وأن المصطلح «فيروسات الحاسوب» يجلب الخوف للمسؤولين أو مستخدمي أي نظام حاسوبي، إذن من أين أتت الفيروسات؟ وأين ومتى بدأت؟ وكيف نشأت لتصبح خطيرة كما هي اليوم؟

يتمثل تاريخ البرمجيات الخبيثة بالفيروسات التي ظهرت كفكرة في بحث بعنوان «نظرية الجسم الآلي ذاتي النسخ» لعالم الرياضيات John von Neumann في نهاية أربعينيات القرن العشرين ونُشرت هذه الورقة البحثية في عام 1966 بعنوان نظرية الجسم الآلي ذاتي النسخ، وقد شكّلت الورقة البحثية تجربة فكرية، حيث تكهنت بأنه يمكن لكائن «آلي» تدمير أجهزة ونسخ نفسه وإصابة مضيفات جديدة (ولادة النسخ المتماثل الآلي)، تماماً مثل الفيروس البيولوجي[3].

ومع ظهور الحواسيب وشبكات الإنترنت ظهر ما يعتبر أول فيروس، في العام 1971، وما يطلق عليه الزاحف ((Creeper، وقد كان إنتاجه كاختبار أمني لمعرفة ما إذا كان إيجاد برنامج ذاتي النسخ أمرًا ممكنًا، فمع كل إصابة محرك أقراص جديد، كان برنامج Creeper يحاول حذف نفسه من المضيف السابق[4].

وفي العام 1974 تم تطوير فيروس Rabbit (أو Wabbit)، وقد كان له هدف خبيث وكان بإمكانه نسخ نفسه، فبمجرد تسلله إلى أحد الحواسيب، كان ينسخ نفسه عدة نسخ مقللاً بدرجة كبيرة من كفاءة أداء النظام ومؤديًا في نهاية المطاف إلى تعطل الجهاز، وكانت سرعة النسخ هي سبب تسمية الفيروس بهذا الاسم، أما في عام 1975، فقد تم إنشاء أول حصان طروادة[5]، عرف باسم ANIMAL، (رغم أنه أثار حوله الجدل ما إذا كان حصان طروادة أم مجرد فيروس آخر) من تصميم مبرمج الحاسوب John Walker في العام 1975.

وقد بدأ أول فيروس يصيب الحاسوب الشخصي، في إصابة الأقراص المرنة بحجم 5.2 بوصات في العام 1986، حيث يطلق على هذا الفيروس Brain Boot Virus، وكان هذا الفيروس من تصميم شخصين يديران متجراً لبيع

3 موقع شركة كاسبر العالمية لمكافحة الفيروسات
https://me.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
تاريخ الزيارة 5 / 2 / 2021
https://study.com/academy/lesson/the-history-of-computer-viruses.html#:~:text=In%201971%2C%20Bob%20Thomas%20of,was%20successful%20and%20it%20worked.
تاريخ الزيارة 20/6/2022

4 برنامج Creeper هدف خبيث، فكلما كان يحدثه هو إظهار رسالة بسيطة ألا وهي: «I'M THE CREEPER. CATCH ME IF YOU CAN!" (أنا CREEPER،أمسك بي إن استطعت».

5 انتشرت في بداية الثمانينات «برامج الحيوانات التي تحاول تخمين الحيوان الذي يفكر فيه المستخدم من خلال لعبة مؤلفة من 20 سؤالاً، وكان هناك إقبال شديد على الإصدار الذي صممه Walker.

الحواسيب في باكستان، وعندما سئما من العملاء الذين يقومون بالنسخ غير القانوني لبرامجهما، طورا فيروساً Brain، الذي يستبدل قطاع التمهيد في القرص المرن بفيروس، الذي كان أيضًا أول فيروس متسلل، على رسالة مخفية بحقوق النشر، لكنه في واقع الأمر لم يتلف أي بيانات.

وأدت زيادة انتشار الشبكة الإلكترونية على نطاق واسع في مطلع القرن 21 إلى تغيير طريقة انتقال البرامج الضارة، فلم يعد انتقالها مقتصرًا على الأقراص المرنة أو شبكات الشركات، لكنها أصبحت قادرة على الانتشار بسرعة كبيرة جدًا عبر البريد الإلكتروني أو عبر مواقع الويب الشائعة أو حتى عبر الإنترنت مباشرة، فمن هنا، بدأت البرامج الضارة الحديثة في التبلور، وأصبحت بيئة التهديد مختلطة؛ تتألف من الفيروسات والديدان وأحصنة طروادة، ومن ثمّ ظهر اسم «البرامج الخبيثة/الضارة» كمصطلح شامل للبرامج الخبيثة، كما سيأتي ذكره لاحقا خلال الحديث عن الركن المادي.

وقد أشار المشرع الفلسطيني في القرار بقانون رقم 10 لسنة 2018 في المادة (6) إلى جريمة إنتاج البرمجيات الخبيثة بصورة غير مباشرة، والتي جاءت على النحو التالي: « كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات (وتشمل البرمجيات)، 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»، وسنأتي على تبيان طبيعة تلك الجريمة من خلال الحديث عن الركن المادي لجريمة إنتاج الفيروسات بقصد تعطيل البرامج.

الفرع الأول:

الركن المادي لهذه الجريمة.

تعد هذه الجريمة من الجنايات، حيث يتمحور فيها الركن المادي حول إنتاج برمجيات خبيثة تؤدي إلى تعطيل البرامج الإلكترونية، ومن أبرز البرمجيات التي تؤدي إلى تعطيل البرامج وإتلافها الفيروسات، حيث تعرف على أنها تلك البرامج الضارة التي تقوم بعملية نسخ لنفسها على أجزاء الحاسوب المختلفة كالبرامج الأخرى أو حتى الملفات أو غيرها لتلحق به الضرر وتغير من طريقة عمله، وتنتشر هذه البرامج بين أجزاء الكمبيوتر بشكل غير مرئي، حيث يقوم الركن المادي لجريمة إنتاج الفيروسات بقصد تعطيل البرامج وحذفها على السلوك الجرمي والنتيجة الجرمية والعلاقة السببية بينهما(نجم، 2010، ص211)، والمقصود بالسلوك النشاط الذي يتبعه الجاني من خلال إنتاج الفيروسات الضارة بالحواسيب والشبكات بقصد تعطيلها.

ويتصور الركن المادي في النشاط الجرمي الإيجابي الذي يتمثل بتصنيع وإنتاج الفيروسات والتي لها من الخصائص ما يمكنها من التناسخ (التضاعف) والانتشار والتخفي إضافة إلى إلحاق الضرر بالبرامج الإلكترونية على اختلاف أشكالها (أبو العطا،2016، ص34)، كما أن كثير من الفيروسات تربط نفسها ببرنامج أخر يسمى المضيف host في جهاز الحاسوب، مع الإشارة إلى أن الفيروسات لا تنشأ من ذاتها، وإنما بحاجة إلى فاعل، وهو ما أشار إليه المشرع الفلسطيني في المادة السادسة من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية والذي تمت الإشارة إليه سابقاً، وبالتالي؛ تحتاج الفيروسات إلى شخص يقوم بإنتاجها أو إدخالها لأول مرة، ومن ثم تنتقل وتنسخ نفسها ذاتياً، حيث يمكن أن تنتقل من حاسوب مصاب لآخر سليم، كما يمكنها التخفي في عدّة ملفات.

وبالتالي يتصور النشاط المادي الإيجابي لهذه الجريمة من خلال نشر الفيروسات المؤثرة في جهاز الحاسوب من خلال عملية النقر على بعض الملفات أو عن طريق الإنترنت وذلك من خلال البريد الإلكتروني أو حتى تصفُح بعض المواقع وحتى مُشاهدة بعض الإعلانات وهو سلوك جرمي ايجابي، كما قد ينتقل الفيروس من خلال محركات الأقراص الصلبة مما قد يؤدي إلى حذف أو تشفير بعض البيانات الموجودة على الأجهزة، وقد تطورت هذه البرامج الخبيثة بأشكالها المختلفة حيث أصبحت عملية العثور على هذه الفيروسات واكتشافها أمراً أكثر صعوبة، حيث تتميز بعض برامج الفيروس بالقدرة على تجاوز وتخطي تلك البرامج المصممة لمكافحتها والتي تُعرف ببرامج مكافحة الفيروسات (أبو العطا،2016، ص37)، ويكمن الفيروس داخل البرامج التي تبدو شرعية وتنتشر من خلال البحث عن نقاط الضعف على أجهزة الحاسوب الأخرى والتي يمكنها الوصول اليها عبر الانترنت والشبكات المحلية, (csoonline, 2022).

كما يتصور النشاط الجرمي في كل ما يقوم بإنتاجه الفاعل من برمجيات خبيثة تهدف إلى تعطيل البرامج الإلكترونية والنظام المحوسب بشكل عام، كالملفات ذاتية التنفيذ مثل ملفات ذات امتداد (.EXE ,.DLL,.COM) ضمن أنظمة التشغيل (دوس وميكروسوفت ويندوز)، أو (ELF) في (أنظمة لينكس)، وسجلات الملفات والبيانات (VOL-UME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (0) في القرص الصلب MASTER BOOT، وكذلك ملفات الأغراض العامة مثل ملفات (الباتش والسكريبت في ويندوز) وملفات (الشل في يونيكس)، وملفات الاستخدام المكتبي في نظام تشغيل (مايكروسوفت ويندوز) التي تحتوي (ماكرو مثل مايكروسوفت وورد ومايكروسوفت إكسل ومايكروسوفت أكسس)، وقواعد البيانات وملفات (الأوتو لوك) لها دور كبير في الإصابة ونشر الإصابة لغيرها لما تحتويه من عناوين البريد الإلكتروني، والملفات من النوع (نسق المستندات المنقولة) وبعض نصوص لغة ترميز النص الفائق احتمال احتوائها على كود خبيث، والملفات المضغوطة مثل ((ZIP، وملفات (mp3) وغيرها من الملفات الملحقة. (المصري, 2011، ص9)

ولم يشر المشرع الفلسطيني إلى وسيلة انتقال هذه الفيروسات، بل ترك المجال مفتوحاً، وخصوصاً أن طبيعة هذه البرمجيات وتطورها تجعل إمكانية انتقالها سهلة وبسيطة عبر كثير وسائل تكنولوجيا المعلومات، ومن أهم طرق الانتقال الآن هي الشبكة الإلكترونية، حيث تكون وسيلة سهلة لانتقال الفيروسات من جهاز لآخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات وهو المنتج الأكثر شهرة في فئة منتجات الحماية من البرامج الضارة؛ على الرغم من وجود «الفيروس» في الاسم، فإن معظم العروض تتخذ جميع أشكال البرامج الضارة، في حين أن محترفي الأمان المتميزين يرفضون ذلك باعتباره عفا عليه الزمن، إلا أنه لا يزال العمود الفقري للدفاع الأساسي لمكافحة البرامج الضارة، ومن الأمثلة على هذه البرامج F-Secure و Kaspersky .(2022,Lab,(csoonline

وبالتالي؛ تتصور النتيجة الجرمية بمجرد وصول الفيروسات إلى آلاف الضحايا، وبالتالي؛ تعتبر الجريمة قائمة حتى لو وصل الفيروس إلى مستخدم في دولة أخرى، بحيث يكون الهدف من نشر الفيروسات هو تعطيل الأجهزة والبرامج الإلكترونية، أو حذفها أو تعديلها البيانات التي تحتويها، وهو ما أشار إليه المشرع الفلسطيني في المادة السادسة من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، حيث يمكن ملاحظة هذه الفيروسات من خلال أعراض تظهر على جهاز الحاسوب الخاص في المستخدم في بعض الأحيان، كتكرار رسائل الخطأ في أكثر من برنامج، وظهور رسالة تعذر الحفظ لعدم كفاية المساحة، وتكرار اختفاء بعض الملفات التنفيذية، بالإضافة إلى حدوث بطء شديد في بدء تشغيل (إقلاع نظام التشغيل) أو تنفيذ بعض التطبيقات، كذلك رفض بعض التطبيقات

الإلكترونية لأوامر التنفيذ.

فعند تشغيل البرنامج الإلكتروني المصاب بالفيروس، فإنه قد يصيب باقي الملفات الموجودة معه في القرص الصلب، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر في بعض الأحيان، بعد أن تم إدخاله إلى الجهاز عبر وسائل مختلفة منها البريد الإلكتروني أو الإنترنت أو عبر تحميل صورة أو تطبيق تحتوي على هذه البرمجيات الخبيثة، وبالتالي قد يساهم الضحية في اكتمال أركان هذه الجريمة دون أن يعلم بأن ما يقوم به من تشغيل او تنزيل برنامج ما عبر البريد الإلكتروني أو تحميله هو فيروس.

والفيروسات متنوعة، فمن حيث الإنتاج منها ما تقوم بصناعته الشركات الخاصة بإنتاج الفيروسات بغية إجبار جمهور المستهلكين على شراء مضاد الفيروسات الذي تنتجه هذه الشركة، ومنها ما يقوم بإنتاجها مجموعة من الهواء بهدف نشره عبر الفضاء الإلكتروني، وذلك لأغراض الانتقام أو التسلية.

وسنتحدث تاليا عن أبرز أنواع هذه البرمجيات الخبيثة من حيث طريقة الانتشار والتناسخ، فبالإضافة إلى الفيروسات التي تم التطرق إليها، هناك أنواع أخرى مثل: الديدان(worms)، وأحصنة طروادة (Trojan horses)، والجذور الخفية (Rootkit)، وبرامج التجسس (Spyware)، وبرامج الإعلانات المتسللة (Adware)، والبرمجيات التخريبية (Scareware), وبرمجيات خاطفة المتصفح (Browser Hijacker) وغيرها من البرمجيات الخبيثة. وتالياً نقدم لمحة عن هذه الأنواع:

الدودة (Worm): وهي برنامج خبيث ينشر نسخًا من نفسه عبر الشبكة، وتنتشر ديدان الحواسيب عبر الشبكات والإنترنت، فعلى سبيل المثال تنتشر الدودة عن طريق البريد الإلكتروني، فمثلاً عند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في العناوين ويرسل نفسه إلى كل شخص وهكذا، مما يؤدي إلى انتشاره بسرعة عبر الشبكة، ومع التطور الحاصل في ميدان تكنولوجيا المعلومات أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها، (مثلاً بعد الانتشار إلى عدد 50000 جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو أي شيء آخر (مثلاً في يوم معين أو ساعة أو تاريخ...الخ).

وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة، وتسمى هجمات حجب الخدمة (Denial of Service Attacks DoS)، حيث تنتشر الدودة على عدد كبير من الأجهزة، ثم توجه طلبات وهمية لجهاز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة)، فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا، مما يسبب توقفه عن العمل، وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية، أشهرها مايكروسوفت وغيرها الكثير(الخطيب وآخرون 2016، ص136).

فالاختلاف الأساسي بين الديدان والفيروس هو أن الدودة تعمل من خلال الشبكات، ويمكن للفيروس أن ينتشر عبر أي وسيط (ولكن عادةً ما يستخدم برنامجًا منسوخًا أو ملفات بيانات)، بالإضافة إلى ذلك تنشر الدودة نسخًا من نفسها كبرنامج مستقل، بينما ينشر الفيروس نسخًا منه كبرنامج يتم إرفاقه أو تضمينه في برامج أخرى(الخطيب وآخرون 2016، ص136) (الزعبي،الشرايعة، عبدالله،الزعبي، 2009، ص91).

حصان طروادة (Trojan Horse): المعروف أيضًا باسم حصان طروادة وهو برنامج ضار يتنكر كبرنامج مفيد، ويأتي اسمها من حصان طروادة الأسطوري في الملحمة الأسطورية The Aeneid)) حيث قام اليونانيون، الذين كانوا في حالة حرب مع طروادة لمدة 10 سنوات، ببناء حصان خشبي كبير وتقديمه «كهدية» لأحصنة طروادة والتي نظر إليها على أنها عرض سلام، وقد احضروا الحصان إلى المدينة، وفي تلك الليلة، وبينما كان جنود طروادة نائمون، كان الجنود اليونانيون المختبئون في بطن الحصان الأجوف يتسلقون وفتحوا أبواب المدينة للسماح لبقية الجيش اليوناني بدخول المدينة، وهزم الإغريق كما يروى في تلك الليلة.

وبالمثل، تستخدم برامج أحصنة طروادة مظهرها الخارجي لخداع المستخدمين لتشغيلها، حيث إنها تشبه البرامج التي تؤدي مهامًا مفيدة، لكنها في الواقع تخفي تعليمات برمجية ضارة، فبمجرد تشغيل البرنامج، يتم تنفيذ تعليمات الهجوم بأذونات وسلطة المستخدم.

وكان أول برنامج حصان طروادة معروفًا هو Animal، والذي تم إصداره في عام 1974، تنكر الحيوان على أنه لعبة اختبار بسيطة يفكر فيها المستخدم في حيوان ويطرح البرنامج أسئلة لمحاولة تخمينه، بالإضافة إلى طرح الأسئلة، قام البرنامج بنسخ نفسه في كل دليل كان للمستخدم حق الوصول للكتابة إليه.

وتقوم أحصنة طروادة اليوم بأكثر من مجرد حفظ نسخ من نفسها، إذ يمكن لأحصنة طروادة إخفاء البرامج التي تجمع معلومات حساسة، أو تفتح أبواب خلفية في أجهزة الحاسوب، أو تقوم بتحميل وتنزيل الملفات بشكل نشط.

الجذور الخفية (Rootkit): هو نوع من البرامج الضارة التي تحصل على امتيازات مستوى المسؤول على نظام تشغيل الحاسوب دون إظهار الميزة الرئيسية لـ rootkit هي أنه يتخفى عن الكشف بسهولة، ولكنه يحتفظ بالتحكم في نظام التشغيل لأداء المهام المحددة له على النظام. يتم تخريب السلوك الطبيعي لنظام التشغيل بواسطة البرامج الضارة للجذور الخفية.

ويعتبر الـ Rootkit أحد أكثر أشكال البرامج الضارة التي لا يمكن اكتشافها وإزالتها بسهولة من جهاز الحاسوب الخاص بك، فبمجرد إنشاء امتيازات الوصول إلى نظام التشغيل والتحكم فيه من خلال الثغرات الأمنية المتاحة في نظام التشغيل والتطبيقات الأخرى، إذا أظهر الحاسوب الأعراض التالية، فيجب أن تشك في إصابته بهجوم Rootkit.

(تعديلات في مواعيد ووقت الحاسب الآلي، تباطؤ أداء الحاسوب، رسائل خطأ غير متوقعة في النظام، فشل العديد من البرامج وخاصة البرامج المتعلقة بأمان الحاسوب عند بدء التشغيل، عمليات إعادة توجيه كبيرة على متصفحات الإنترنت، وغيرها من الأعراض).

برامج التجسس (Spyware): هو برنامج يتم تثبيته على أجهزة الحاسوب دون إعلام المستخدم به، والهدف الرئيسي منه هو مراقبة الأنشطة عبر الإنترنت، وعادات استخدام الحاسوب والاهتمامات الشخصية.

يتطفل برنامج التجسس على الطريقة التي يستخدم بها المستخدم الإنترنت، بحيث يمكن تنفيذ حملة تسويق رقمية مناسبة ومركزة من خلال رسائل البريد الإلكتروني وغيرها من المصادر عبر الإنترنت., وفي عالمنا الحديث اليوم، أصبحت أهمية الخصوصية بالغة الأهمية، من خلال إدخال قانون اللائحة العامة لحماية البيانات (GDPR) في دول الاتحاد الأوروبي، أصبحت أهمية الخصوصية جزءًا لا يتجزأ من أي خدمة عبر الإنترنت.

وقد تتضمن أعراض هجوم برامج التجسس على جهاز الحاسوب ما يلي: تباطؤ في أداء النظام, توقف برامج عن العمل بشكل صحيح, ظهور العديد من التغييرات في شريط أدوات المتصفح والمكونات الإضافية, ظهور الإعلانات على الشاشة باستمرار, اختناقات النطاق الترددي للإنترنت.

برامج الإعلانات المتسللة (Adware): هو برنامج يجبر مستخدمي الإنترنت على زيارة صفحة ويب معينة أو نافذة منبثقة أو إعلان على الصفحة لمشاهدته.

أصبح Adware أداة شائعة جدًا لفرق التسويق الرقمي لجذب انتباه المستخدمين إلى منتج أو خدمة معينة، تستخدم شفرة برامج الإعلانات المتسللة طرقًا مختلفة للنشر والعثور على الأهداف المناسبة بحيث يتم التعرف على الجمهور المركز لمنتج معين, لربما تكون قد صادفت بعض الروابط والصفحات المزعجة أثناء تصفح الإنترنت، وعند النقر فوق تلك الصفحات أو الروابط، تتم إعادة توجيهك إلى صفحة أخرى تروج لمنتج أو خدمة معينة، وفي بعض الحالات، تظهر النوافذ المنبثقة مع المحتوى الترويجي لمنتج معين، ويتم كل ذلك بمساعدة برامج الإعلانات المتسللة.

تتضمن بعض الأعراض الهامة جدًا لتأثر جهاز الحاسوب ببرنامج الإعلانات المتسللة ما يلي:

عمليات إعادة التوجيه المتكررة، عدد ضخم من رسائل البريد الإلكتروني العشوائية، نوافذ منبثقة متكررة للعروض، كثرة حركة المرور الصادرة والواردة، تباطؤ الاتصال بالإنترنت.

البرمجيات التخريبية (Scareware): هو نوع من البرامج الضارة، ينبثق في النافذة مع تحذير خطير بشأن أي تهديد فيروسي على جهاز الحاسوب، ولكن في الواقع لا يوجد تهديد أو فيروسات باستثناء تلك الخدعة التي ظهرت على الشاشة.

ويبدو التنبيه أصليًا جدًا من بعض المواقع ذات السمعة الطيبة، لكنها ليست مواقع ويب أصلية، هم فقط يبدون حقيقيين وعادة ما تطلب هذه الرسالة من المستخدمين تنزيل بعض الأرقام أو الاتصال بها للحصول على المساعدة, الهدف الرئيسي من Scareware هو بيع المنتجات المقلدة والمزيفة, وفي حالات معينة، يخدع المتسللون المستخدمين لإدخال معلومات بطاقة الائتمان والمعلومات الشخصية والمصرفية على موقع الويب الخاص بهم, بمجرد تقديم هذه المعلومات، يتم اختراق بياناتك لاستخدامات مالية ضارة.

كما يوجد استخدام آخر لخدعة Scareware وهو إجبار المستخدم على تنزيل بعض برامج مكافحة الفيروسات المجانية لتنظيف جهاز الحاسوب الخاص به من تلك الفيروسات التي اكتشفها موقع الويب, وفي الواقع، يعد برنامج مكافحة الفيروسات المجاني هذا بحد ذاته برنامجًا خطيرًا، إذ يمكنه التحكم في جهاز الحاسوب والبدء في إتلاف النظام أو سرقة البيانات لذلك، يمكن أن تكون أداة التخويف أساس العديد من الهجمات الإلكترونية الخطيرة.

برمجيات خاطفة المتصفح (Browser Hijacker): لربما واجهنا في بعض المواقف عندما تم تغيير الإعدادات الافتراضية لمتصفح الانترنت. على سبيل المثال، تم تغيير محرك البحث الافتراضي إلى محرك جديد دون الحصول على إذن.

وكما نعلم أن المتصفح هو أحد أدوات البرامج الأساسية المستخدمة للاتصال بمجموعة واسعة من برامج الحاسوب وتطبيقات الويب والمواقع الإلكترونية والعديد من الموارد الرقمية الأخرى الموجودة على الإنترنت أو حتى على الشبكات المحلية. في حالة حدوث أي اختراق في المتصفح، فإن جميع الموارد الرقمية بما في ذلك كلمات مرور الأمان معرضة للخطر. لذلك، يحاول المتسللون مهاجمة المتصفحات بشكل متكرر لإنشاء طريقة لمهاجمة أجهزة

الحاسوب والشبكات.

ويكمن السبب الرئيسي وراء هذه الأنواع من الأنشطة هو إنشاء برنامج خبيث معين يعرف باسم البرامج الضارة لخاطف المتصفح، ويستخدم هذا الرمز لتمهيد الطريق لأنواع مختلفة من الهجمات الإلكترونية على جهاز الحاسوب الخاص أو على أجهزة الحاسوب الأخرى على الشبكة.

Browser hijacker هو أيضًا برنامج حاسوب ضار يتم تنزيله عادةً على جهاز الحاسوب الخاص عبر بعض تطبيقات البرامج المجانية, حيث تقوم البرامج الضارة بتغيير إعدادات المتصفح على جهاز الحاسوب وذلك عندما نقوم بتثبيت هذا البرنامج المجاني على جهاز الحاسوب الخاص.

ويكمن الهدف الرئيسي من برنامج متصفح الخاطفين هو إجبار المستخدمين على زيارة مواقع ويب معينة لتحسين حجم حركة المرور على هذا الموقع المحدد، وبمجرد تحسن حركة المرور على موقع الويب، يحصل الموقع على عائد أعلى من الإعلان عبر الإنترنت. ويمكن أيضًا استخدام البرامج الضارة للمتصفح الخاطف لسرقة المعلومات الشخصية وحسابات المستخدمين وغيرها من المعلومات لتحقيق منافع مالية، وقد تتضمن أعراض البرامج الضارة لاختراق المتصفح وتأثيرها ما يلي: سرعة تصفح بطيئة، أشرطة أدوات متعددة على المتصفح، إعادة توجيه استعلامات البحث إلى مواقع الويب التي لم نقم بتعيينها كمواقع افتراضية، ظهور عدد كبير من النوافذ المنبثقة والإعلانات على المتصفح.

الفرع الثاني:

الركن المعنوي:

هذه الجريمة لا تقوم إلا عمدية، وهو ما أشار إليه المشرع الفلسطيني، حيث تقوم هذه الجريمة على القصدين العام والخاص (المجالي، 2012،ص 250 وما بعدها) ، حيث يتمثل القصد العام في توجه نية[6] وإرادة المستخدم لإنتاج مثل تلك الفيروسات وإدخالها عبر الشبكة الإلكترونية، أو أي وسيلة إلكترونية أخرى، مع علمه بضررها، أما القصد الخاص فيتمثل في هذه الجريمة بنية الفاعل أن تؤدي هذه البرمجيات إلى إيقاف أجهزة الحاسوب أو وسائل تكنولوجيا المعلومات عن العمل أو تعطيلها أو إتلاف البرامج الإلكترونية أو حذفها أو التعديل عليها[7].

وهنا يثار التساؤل التالي، ما مسؤولية الفاعل في حال تم إنشاء الفيروس وإرساله عبر الشبكة الإلكترونية، وقام هذا الفيروس بإصابة آلاف الأجهزة الحاسوبية سواء كانت أجهزة اتصالات محمولة أو أجهزة الحاسوب العادية؟

ونرى هنا أن الجريمة تقوم طالما قام الفاعل وهو على علم بأن ما يقوم به هو فيروس يشكل برمجيات خبيثة، وأن إدخاله لهذه الفيروسات عبر أجهزة الحاسوب أو من خلال الشبكة الإلكترونية تم عن علم وإرادة كاملة دون أي

6 وقد عرفت المادة (63) من قانون العقوبات الاردني رقم (16) لعام 1960 النية الاجرامية بأنها إرادة ارتكاب الجريمة على ما عرفها القانون.

7 للمزيد أنظر: فخري الحديثي، وخالد الزعبي: شرح قانون العقوبات (القسم العام)، الطبعة الثانية، دار الثقافة، الأردن، 2010، ص 173.

إكراه، وبالتالي فهو مسؤول جنائياً عن هذه الجريمة، حتى لو وصل الفيروس إلى شخص بالخطأ، حتى لو كان الفاعل يريد أن يصل الفيروس إلى شخص آخر.

وتضاعف العقوبة إلى الثلث في حال كان الجاني موظفاً عاماً، وهو ما أشارت إليه المادة (27) من القرار بقانون المتعلق بالجرائم الإلكترونية، ويعاقب المشترك والمحرض بنفس عقوبة الفاعل الأصلي وهو ما أشار إليه المشرع الفلسطيني في المادة (28) من القرار بقانون الخاص بالجرائم الإلكترونية، كما تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني وهو ما أشار إليه المشرع الفلسطيني في المادة (51) من القرار بقانون الخاص بالجرائم الإلكترونية. كما وتضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية:

1. إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية.

2. ارتكاب الجاني الجريمة من خلال عصابة منظمة.

3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية.

4. إذا وقعت الجريمة على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية، وهو ما أشار إليه المشرع الفلسطيني في المادة (52) من القرار بقانون الخاص بالجرائم الإلكترونية.

وتجدر الإشارة هنا إلى أن هذه الجريمة تعتبر من الجنايات التي تقع ضمن اختصاص محكمة البداية، حيث يعاقب الجاني بالسجن مدة لا تزيد على خمس سنوات، حيث أن الحد الأدنى هو ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، ويلاحظ أن المشرع جعل عقوبة هذه الجريمة مشددة بسبب الأضرار الكبيرة التي يمكن أن تصيب الأجهزة الإلكترونية والخسارات المالية أو الاقتصادية نتيجة تعطيل البرامج الإلكترونية، وخصوصا أن معظم التجارة أصبحت الكترونية. مع الإشارة إلى أن محل الحماية هو البرامج والأجهزة الإلكترونية والبيانات والمعلومات الموجودة عليها، كما يلاحظ أن المشرع الفلسطيني جعل عقوبة السجن ملازمة لعقوبة الغرامة.

النتائج والتوصيات

توصل الباحثان إلى مجموعة من النتائج والتوصيات التي تتعلق بموضوع الدراسة ومن أهم هذه النتائج ما يلي:

1. تعتبر جريمة إعاقة الوصول إلى الخدمات الإلكترونية من الجنح والتي تتمثل بتعطيل الوصول أو إعاقة الوصول إلى الخدمات الإلكترونية أو الأجهزة أو البرامج أو المعلومات الإلكترونية على اختلاف أنواعها.
2. إن محل الحماية في جريمة الاعتداء على البرامج الإلكترونية هو الأجهزة الإلكترونية والشبكة الإلكترونية

والبرامج الملحقة بها، بالإضافة إلى البيانات والمعلومات الإلكترونية المخزنة، وأيضا الخدمات التي تقدمها، وهنا حاول المشرع الفلسطيني توفير هذه الحماية انطلاقاً من حق المستخدم في الوصول إلى الجهاز الالكتروني الخاص به، وأن تعطيل أو إعاقة الوصول للأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكل اعتداء على هذا الحق.

3. هناك العديد من البرمجيات الخبيثة التي تستهدف تعطيل الأجهزة الإلكترونية أو الحواسيب، وجميع أشكالها وأنواعها تقع بها الجريمة.

4. جرائم الاعتداء على البرامج الإلكترونية لا تقوم إلا عمدية، وهو ما أشار إليه المشرع الفلسطيني، حيث تقوم على القصدين العام والخاص، حيث يتمثل القصد العام في توجه نية وإرادة المستخدم لإنتاج مثل تلك الفيروسات وإدخالها عبر الشبكة الإلكترونية، أو أي وسيلة إلكترونية أخرى، مع علمه بضررها، أما القصد الخاص فيتمثل في هذه الجريمة بنية الفاعل أن تؤدي هذه البرمجيات إلى إيقاف أو إتلاف البرامج الإلكترونية أو حذفها أو التعديل عليها.

5. حاول المشرع الفلسطيني توفير هذه الحماية للبرامج الإلكترونية انطلاق أمن حق المستخدم في الوصول إلى الجهاز الالكتروني الخاصة أو الخدمات الإلكترونية، وأنت عطيل أو إعاقة الوصول للأجهزة الإلكترونية والشبكة الإلكترونية والبرامج الملحقة يشكل اعتداء على هذا الحق.

التوصيات:

1. تعديل نص المادة الخامسة من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية والمعدل بموجب القرار بقانون رقم 38 لسنة 2021 لتكون على النحو التالي: « كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بصورة عمدية بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين».

2. حماية البرامج من البرمجيات الخبيثة لدى المستخدمين من خلال رفع مستويات الأمان في الحواسيب على اختلاف أنواعها، وتتمثل بتجنب زيارة المواقع الإلكترونية غير الآمنة، والتأكد من تحديثات برامج مضاد الفيروسات وأنظمة التشغيل، والتأكد من تشغيل الجدران النارية، وعدم فتح بريد الكتروني او مرفق من أشخاص غير معروفين، تفعيل أنظمة كشف التسلل IDS وأنظمة الحماية من التسلل IPS وذلك على مستوى الشبكات، وتفعيل تطبيقات مانع الإعلانات التجارية.

المصادروالمراجع :

- **القوانين والتشريعات:**

1. قانون العقوبات الأردني رقم 16 لسنة 1960 والساري بالضفة الغربية.
2. القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية.

- **الكتب القانونية:**

1. باسل مصطفى الخطيب وآخرون. (2016)، الحاسوب والبرمجيات الجاهزة، الطبعة الأولى، دار الاعصار العلمي، الأردن.
2. توفيق نظام المجالي. (2012)، شرح قانون العقوبات القسم العام، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن.
3. جبريل بن حسن العريشي، سلمى بنت عبد الرحمن محمد الدوسري. (2018)، الشبكات الاجتماعية والقيم، الطبعة الأولى، الدار المنهجية للنشر، الأردن.
4. جبريل بن حسن العريشي، محمد حسن الشلهوب. (2016)،أمن المعلومات، الطبعة الأولى، دار المنهجية للنشر والتوزيع، الأردن.
5. زياد القاضي. (2007)، انظمة التشغيل، الطبعة الخامسة، دار المسيره، الأردن.
6. عبدالله ذيب محمود، وأسامة اسماعيل دراج. (2022) الوجيز في الجرائم الإلكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن.
7. علاء حسين الحمامي، سعد عبد العزيز العاني. (2007)، تكنولوجيا امنية المعلومات وانظمة الحماية، الطبعة الأولى، دار وائل للنشر، الأردن.
8. علاء حسين الحمامي، مازن سمير الحكيم. (2017)، كل شيء عن إنترنت الاشياء وتطبيقات المدن الذكية: دار الراية للنشر والتوزيع, الطبعة الأولى، الأردن.
9. علي جبار الحسيناوي. (2009)، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية، الأردن.
10. عيدي سليمة. (2017)،أمن المعلومات وأنظمتها في العصر الرقمي، الطبعة الأولى، دار الفكر الجامعي، مصر.
11. غنية باطلي. (2015)، الجريمة الإلكترونية، الطبعة الأولى، منشورات الدار الجزائرية، الجزائر.
12. فايز مصطفى الحمودي، عدنان هادي الهلالي. (2009)، نظم التشغيل، الطبعة الأولى، دار صفاء, الأردن.
13. فخري الحديثي، وخالد الزعبي. (2010)، شرح قانون العقوبات(القسم العام)، الطبعة الثانية، دار الثقافة، الأردن.
14. مجدي أبو العطا. (2016)، أمن المعلومات والإنترنت، الطبعة الأولى، شركة علوم الحاسبة (كمبيوسانيس)، مصر.
15. محمد بلال الزعبي، احمد الشرايعة، سهير عبد الله، خالد محمد الزعبي. (2009)، الحاسوب والبرمجيات الجاهزة: مهارات الحاسوب الطبعة التاسعة، دار وائل، الأردن.
16. محمد صبحي نجم. (2010)، قانون العقوبات القسم العام، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن.

17. منـال البلقاسـي. (2019)، مفاهيـم مسـتحدثة فـي نظـام التشـغيل، الطبعـة الأولـى، دار القلـم الجامعـي، مصـر.

18. يوسـف المصـري. (2011)، الجرائـم المعلوماتيـة والرقميـة للحاسـوب والإنترنـت، الطبعـة الأولـى، دار العدالـة، مصـر.

19. Charles P. Pfleeger,(2015)Shari Lawrence Pfleeger, Jonathan Margulies, Securit-.yin Computing5th ed , Pearson Education, Inc

20. Kim, D., & Solomon, M. G. (2018). Fundamentals of information systems secu-.rity. Jones & Bartlett Publishers

21. Thakur, K., & Pathan, A. S. K. (2020). Cybersecurity Fundamentals: A Re-.al-World Perspective. CRC Press

- **المواقع الإلكترونية:**

1. موقع شركة كاسبر العالمية لمكافحة الفيروسات

https://me.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

تاريخ الزيارة 5 / 2 / 2021

2. موقع شركة ميكروسوفت

https://support.microsoft.com/ar-sa/windows/

تاريخ الزيارة 7/4/2021

3. واقع الجرائم الإلكترونية وتداعياتها على المجتمع المصري

https://draya-eg.org/2022/04/13/

تاريخ الزيارة 2022/6/17

4. Utility definitions: https://www.computerhope.com/

تاريخ الزيارة 2022/6/17

5. Application: https://www.techtarget.com/

تاريخ الزيارة 2022/6/18

6. What is computer security:

https://www.simplilearn.com/what-is-computer-security-article

تاريخ الزيارة: 2022/6/18

7. مصابيح المعرفة للعلوم التقنية وتقنية المعلومات

https://www.masabe7-almarefa.com/2020/05/Computer-system.html

تاريخ الزيارة: 2022/6/16

8. كل ما تريد معرفته حول الجرائم الإلكترونية او الجرائم المعلوماتية

https://www.alroeya.com/

تاريخ الزيارة: 2022/6/15

9. Cybersecurity

https://rajeshlaskary.medium.com/

تاريخ الزيارة: 2022/6/18

10. Malware explained: Definition, examples, detection and recovery

https://www.csoonline.com/

تاريخ الزيارة: 2022/6/19

Sources and references:

- **rules and regulations**:

1.Jordanian Penal Code No. 16 of 1960 in force in the West Bank.

2. Jordanian Cybercrime Law No. 27 of 2015 and its amendments for 2018.

3. Decree-Law No. 10 of 2018 regarding cybercrime.

• Legal books:

1. Basil Mustafa Al-Khatib et al. (2016), Computer and ready-made software, first edition, Dar Al-Assar Alami, Jordan.

2. Tawfiq Al-Majali System. (2012), Explanation of the Penal Code, General Section, third edition, House of Culture for Publishing and Distribution, Jordan.

3. Jibril bin Hassan Al-Areshi, Salma bint Abdul Rahman Muhammad Al-Dosari. (2018), Social Networks and Values, First Edition, Methodology House for Publishing, Jordan.

4. Jibril bin Hassan Al-Areshi, Mohammed Hassan Al-Shalhoub. (2016), Information Security, First Edition, House of Methodology for Publishing and Distribution, Jordan.

.Ziad Al-Qadi. (2007), Operating Systems, Fifth Edition, Dar Al Masirah, Jordan .5

Abdallah (Theeb Mahmoud, and Osama Ismail Darrag. (2022) Al-Wajeez in Electronic .6 .Crimes, first edition, House of Culture for Publishing and Distribution, Jordan

Alaa Hussein Al-Hamami, Saad Abdul Aziz Al-Ani. (2007), Information Security Technolo- .7 .gy and Protection Systems, First Edition, Wael Publishing House, Jordan

Alaa Hussein Al-Hamami, Mazen Samir Al-Hakim. (2017), All about the Internet of Things .8 .and smart city applications: Dar Al-Raya for Publishing and Distribution, first edition, Jordan

Ali Jabbar Al-Husseinawi. (2009), Computer and Internet Crimes, first edition, Al-Yazuri .9 .Scientific House, Jordan

Idi sound. (2017), Information security and systems in the digital age, first edition, Dar Al- .10 .Fikr Al-Jamii, Egypt

.Rich my void. (2015), Cybercrime, first edition, Algerian House Publications, Algeria .11

Fayez Mustafa Al-Hamoudi, Adnan Hadi Al-Hilali. (2009), Operating Systems, First Edi- .12 .tion, Dar Safaa, Jordan

Fakhri Al-Hadithi, and Khaled Al-Zoubi. (2010), Explanation of the Penal Code (General .13 .Section), second edition, House of Culture, Jordan

Magdy Abu Al-Atta. (2016), Information and Internet Security, first edition, Computer Sci- .14 .ence Company (CompuSanis), Egypt

Muhammad Bilal Al-Zoubi, Ahmed Al-Sharia, Suhair Abdullah, Khaled Muhammad .15 Al-Zoubi. (2009), Computer and Ready-made Software: Computer Skills, Ninth Edition, Dar .Wael, Jordan

Mohamed Sobhi Negm. (2010), Penal Code, General Section, third edition, House of Cul- .16 .ture for Publishing and Distribution, Jordan

17. Manal Belkassi. (2019), New concepts in the operating system, first edition, Dar Al-Qalam University, Egypt.

18. Youssef Al-Masry. (2011), Computer and Internet Information and Digital Crimes, First Edition, House of Justice, Egypt.

19. Charles P. Pfleeger, (2015)Shari Lawrence Pfleeger, Jonathan Margulies, Securityin Com- puting5th ed , Pearson Education, Inc.

20. Kim, D., & Solomon, M. G. (2018). Fundamentals of information systems security. Jones & Bartlett Publishers.

21. Thakur, K., & Pathan, A. S. K. (2020). Cybersecurity Fundamentals: A Real-World Perspec- tive. CRC Press.

• websites:

1. The site of the global Casper Anti-Virus Company

https://me.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Date of visit 5/2/2021

2. Microsoft website

https://support.microsoft.com/en-us/windows/

Visit date 7/4/2021

3. The reality of cybercrime and its repercussions on Egyptian society

https://draya-eg.org/2022/04/13/

Date of visit 17/6/2022

4. Utility definitions: https://www.computerhope.com/

Date of visit 17/6/2022

5. Application: https://www.techtarget.com/

Date of visit 18/6/2022

6. What is computer security:

https://www.simplelearn.com/what-is-computer-security-article

Date of visit: 18/6/2022

7. Knowledge lamps for technical sciences and information technology

https://www.masabe7-almaref.com/2020/05/Computer-system.html

Date of visit: 06/16/2022

8. All you need to know about cyber crimes or information crimes

https://www.alroeya.com/

Date of visit: 6/15/2022

9. Cybersecurity

https://rajeshlaskary.medium.com/

Date of visit: 18/6/2022

10. Malware explained: Definition, examples, detection and recovery

https://www.csoonline.com/

Date of visit: 6/19/2022