جريمة إتلاف البيانات الحكومية الإلكترونية

الباحث / مصطفى حسون عبيد هجول

(ISSN: 2537 - 0758)

جريمة إتلاف البيانات الحكومية الإلكترونية

الباحث / مصطفى حسون عبيد هجول

ملخص البحث:

أن التقدم العلمي والتكنلوجي الذي تشهده البشرية في العصر الحديث يلقي بظلالة ونتائجه على كافة جوانب الحياة والعلاقات بين الأفراد والحكومات ، ولا سيما على حقوق الأفراد وحرياتهم وبياناتهم الموجودة لدى الجهات الحكومية.

وفي ضوء عالم التقنية وثورة المعلومات وما صاحب ذلك من استخدام تلك التقنيات سواء على مستوى الأفراد أو الجهات أو المؤسسات الحكومية أو الخاصة في شتى التعاملات، وتبلور ذلك بوضوح بصدد بصدد ثورة المعلومات والاتصالات، وانعكاساتها الهائلة على سرعة وسهولة التواصل وتداول البيانات الحكومية الالكترونية، وازدهار المعاملات والتجارة الالكترونية؛ معلنة سقوط الحواجز التقليدية بين الدول وبين المواطنين والحكومات، وصيرورة العالم بمثابة بلدة واحدة من خلال شبكة الانترنيت.

حيث تم بيان أن الجرائم المتعلقة بإتلاف البيانات الحكومية الالكترونية ذات طبيعة خاصة من حيث أساليب وطرق ارتكابها وفق المهارات والخبرات الفنية لمرتكبيها، وأمام هذا الواقع ظهرت بذور الخير للاستفادة من ثمار التواصل والمعرفة، كما تكشفت في الوقت ذاته نوازع الشر لاستغلال ذلك التقدم التقني في ارتكاب الجريمة التقليدية والمستحدثة على حد سواء ، سعيا وراء تحقيق غايات شخصية على حساب قيم وأخلاقيات وحقوق وخصوصيات الأفراد وأمن وسلامة المجتمع .

ولأجل معالجة الموضوع بأفضل الصيغ والحلول القانونية فقد بين هذه البحث في المبحث الأول تعريف الإتلاف في المجال الإلكتروني، وفي المبحث الثاني تناولنا إلى الوسائل الفنية لإتلاف البيانات الحكومية الالكترونية، وتم تقسيم هذه المبحث إلى مطلبين، في المطلب الأول منه قد بينا برامج الفايروسات الخبيثة أما المطلب الثاني منه تناولنا فيه برنامج الدودة.

Abstract:

The scientific and technological progress that humanity is witnessing in the modern era casts a shadow and its consequences on all aspects of life and the relations between individuals and governments, especially on the rights and freedoms of individuals and their data held by government agencies

.And in the light of the world of technology and the information revolution and the accompanying use of these technologies, whether

at the level of individuals, agencies, or governmental or private institutions in various transactions, and this was clearly crystallized in connection with the information and communication revolution, and its tremendous repercussions on the speed and ease of communication and circulation of electronic government data, and the prosperity of transactions electronic commerce; Announcing the fall of traditional barriers between countries and between citizens and governments, and the world becoming like a single town through the Internet.

Where it was shown that the crimes related to the destruction of electronic government data are of a special nature in terms of the methods and methods of committing them according to the technical skills and expertise of the perpetrators, and in the face of this reality, the seeds of good appeared to take advantage of the fruits of communication and knowledge, and at the same time evil motives were revealed to exploit that technical progress in committing the crime Both traditional and modern, in pursuit of personal goals at the expense of the values, ethics, rights and privacy of individuals and the security and safety of society.

In order to address the issue with the best formulas and legal solutions, this research has shown in the first section the definition of destruction in the electronic field, and in the second section we have dealt with the technical means to destroy electronic government data, and this section has been divided into two requirements, in the first requirement of it we have shown malicious virus programs. The second of which we dealt with the worm program .

مقدمة

بسم الله الرحمن الرحيم والصلاة والسلام على أفضل الخلق أجمعين سيدنا محمد وعلى اله وصحبه أجمعين..... ان الله سبحانه وتعالى كرم الانسان ورزقه من الطيبات وفضله على كثير من مخلوقاته، وقد سخر عز وجل له الكنوز والعلوم ليجتهد في استخراج مكنوناتها خدمة لبني جنسه.

قد لا يكتفي المجرم الولوج أو الدخول غير المشروع والبقاء غدرا في الانظمة الالية لمعالجة المعلومات، ويتلصص ويتجسس على البيانات المشتهى فيها والمخزنة داخل الانظمة المعلوماتية، وانما يتجاوز بفعله لغرض اجرامي كإتلاف البيانات المسجلة الكترونيا والمخزنة بداخل هذه الانظمة.

(ISSN: 2537 - 0758)

ومن السهل تصور الاتلاف التقليدي الذي يميل للعنف أو الذي يقع على المكونات المادية للأنظمة الالية لمعالجة البيانات ، كإتلاف شاشة الحاسب الالي بتكسيرها مثلا ، أما الاتلاف المعني في بحثنا هذا فهو الذي يقع باستخدام تقنيات التدمير الناعمة كالفايروسات والقنابل المنطقية والزمنية لإتلاف المكونات المعنوية أو المنطقية للأنظمة الالية لمعالجة البيانات ، مثل البرامج المعلوماتية والبيانات المسجلة بهذه الانظمة . شهد العالم منذ منتصف القرن الحالي ثورة جديدة اصطلح على تسميتها (بالثورة المعلوماتية)، وبالنظر الى ما تقدمه هذه الثورة من خدمات وفوائد جليلة للأفراد والمؤسسات الحكومية في الوقت الراهن ، فقد أمست قوة لا يستهان بها .

أولا : **أهمية البحث** :

تظهر أهمية هذا البحث في الدور الذي تلعبه تقنية المعلومات الحديثة في حياتنا اليومية ، وتأثيره على مظاهر الحياة في جميع مجالاتها ، ومدى الحاجة لبحث ظاهرة جرائم الاعتداء على البيانات الحكومية الإلكترونية والعمل على خلق اطار قانوني لها ، يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية المواطنين والحكومات من تأثيرها وحماية النشاطات بكافة انواعها ، حيث تبرز أهمية هذا البحث في الوقوف على هذه الظاهرة الجرمية التي نمت بنماء تقنية المعلومات وتطورت بتطورها فظهرت على السطح جرائم لم تكن موجودة في السابق.

ثانياً: **اشكالية البحث** :

يثير موضوع جريمة إتلاف البيانات الحكومية الالكترونية اشكاليات عديدة ، لعل من ابرزها غياب النص القانوني الذي من شأنه الحد من الاعتداءات التي تقع على البيانات الحكومية الالكترونية ، فضلا عن ذلك فقد ادى التطور العلمي والتكنلوجي الحالي الى تزايد صور تلك الاعتداءات وتعددها ، والتي تنال من اهم ما يجب ان يبقى مستورا ومحجوبا عن الاخرين ، زيادة على ذلك فان غياب ملاكات التحري والتحقيق او قلة معرفتهم بالأمور الفنية والوسائل المرتكبة بها هكذا جرائم قد يزيد من تعقد مكافحتها بل وحتى مكافحة جزء منها .

ثالثاً: **منهجية البحث** :

من اجل الوقوف على أهم النقاط المهمة في هذا البحث ومعالجتها معالجة وافية، فقد اعتمدنا في هذا البحث المنهج التحليلي ، من خلال تحليل النصوص التشريعية ذات العلاقة بالموضوع والوصول بها الى النتائج المطلوبة .

رابعاً : **خطة البحث** :

بغية تحقيق النتائج العلمية المرجوة من هذه الدراسة ومن ثم التوصل الى نتائج محددة، فقد تم تقسيم البحث إلى مبحثين ، في المبحث الأول تطرقنا إلى تعريف الإتلاف في المجال الإلكتروني، وفي المبحث الثاني تناولنا إلى الوسائل الفنية لإتلاف البيانات الحكومية الالكترونية، وتم تقسيم هذه المبحث إلى مطلبين ، في المطلب الأول منه قد بينا برامج الفايروسات الخبيثة أما المطلب الثاني منه تناولنا فيه برنامج الدودة ، وخير ما اختتمنا به بحثنا هذه خاتمة بينا فيها أهم الاستنتاجات والمقترحات التي توصلنا اليها ، اسأل الله عز وجل أن يوفقني في ما أسعى اليه والله ولي التوفيق .

المبحث الأول
تعريف الاتلاف في المجال الالكتروني

يعرف الاتلاف لغة ، بانه الهلاك والقطب[١] ، وهو من الجذر اللغوي تلف ، ويقال ذهبت نفسه تلفا، اي هدرا[٢] ويقال رجل متلاف اي كثير الاتلاف لماله[٣]، وفي الاصطلاح الشرعي يعرف الاتلاف بانه اخراج الشيء من ان يكون منتفعا به منفعة مطلوبة في العادة ، ولعل تحريم الاتلاف في الفقه الاسلامي يستند الى العديد من الأدلة الشرعية التي تؤسس لحرمة الاضرار بأموال الغير وعدم جواز الاعتداء عليها بغير حق، ومنه قوله تعالى في محكم كتابة المجيد (يأيها الذين امنو لا تأكلو اموالكم بينكم بالباطل....)[٤].

ولذا تصدى الفقه الى تعريفها ، ومن هذه التعريفات التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الانقاص من كفاءته للاستعمال المعد له[٥]، وعرفت ايضا بانها جعل الشيء غير صالح للاستعمال كليا أو جزئيا بإعدام صلاحيته أو تعطيله بصورة كلية او جزئية[٦]، أو هو كل ما من شأنه انقاص قيمة الشيء أو زوالها اتلافا وتخريبا ويعاقب عليه القانون بوصفه قد قلل من اهمية وقيمة

(١) ينظر : لسان العرب لابن منظور ابي الفضل جمال الدين بن محمد بن منظور بن مكرم الافريقي ، دار احياء التراث العربي ، بيروت ، الجزء التاسع ، ص ١٨ .
(٢) ينظر : المعجم الوسيط لإبراهيم مصطفى واخرون، ج١، ط٦، مؤسسة الصادق (ع) للطباعة والنشر، ص٨٧ .
(٣) ينظر: مختار الصحاح للرازي، محمد بن ابي بكر بن عبد القادر، دار الرسالة، الكويت، ١٩٨٢، ص٧٨.
(٤) ينظر : سورة النساء / الآية -٢٩ .
(٥) د. عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، دراسة مقارنة ، منشرات الحلبي الحقوقية ، بيروت ، الطبعة الأولى، ٢٠٠٣، ص ٢٠١ .
(٦) د. عمار عباس الحسيني ، جرائم الحاسوب والانترنيت (الجرائم المعلوماتية) ، الطبعة الاولى ، منشورات زين الحقوقية ، بيروت ، ٢٠١٧ ، ص ١٣٧ .

(ISSN: 2537 - 0758)

الشيء بالنبة لمالكه[٧]، وبعد التطرق الى تعريف جريمة الاتلاف في صورتها التقليدية نأتي على بيان تعريف هذه الجريمة في صورتها الالكترونية وبهذا الصدد طرح الفقه عددا من هذه التعريفات .

كما عرف الإتلاف بأنه الاعتداء الالكتروني الموجه للمعلوماتية مما تحتويه من بيانات أو برامج تستخدم فيه الانترنيت لتنفيذه، وهذا الاعتداء يتناول المكونات المنطقية غير المادية للكمبيوتر[٨]، ويبدو أن الفقه لم يكن له قول واحد بشأن مدلولي الاتلاف والتخريب، ان سبب ذلك يعود الى استخدام المشرع المصري للمفردتين معا.

فذهب بعضهم الى المقصود بالإتلاف تعطيل منفعة شيء معين بذاته اما التخريب هو اتلاف للشيء بصورة عشوائية ، وقيل ان الاتلاف هلاك الشيء اما التخريب فهو عدم صلاحية الشيء للاستعمال ، وهو بخلاف التعطيل الذي يقصد به توقف عن القيام بوظيفة لفترة مؤقته[٩]، وبدورنا نرى ان الاتلاف الالكتروني هو المحو أو التشوية الالكتروني للبرامج أو البيانات أو المعلومات أو المحررات المعلوماتية –كليا أو جزئيا على نحو يجعلها غير صالحة للاستعمال .

المبحث الثاني
(الوسائل الفنية لإتلاف البيانات الحكومية الالكترونية)

لاختلاف الوسائل الفنية والتقنية المستخدمة البيانات والمعلومات والبرامج التي تشكل في مجملها المكونات المنطقية لأجهزة وانظمة الحاسب الالي إلا أن أخطرها على الاطلاق استخدام الشفرة الخبيثة Malicious Software وهي برمجيات ضارة[١٠]، HARMFUL ROGRAMS تعد من اخطر العناصر التي تهدد امن البيانات والمعلومات لأنها تؤدي الى اتلاف البرامج وضياع البيانات والمعلومات ، وايضا انها تؤثر على كفاءة ادائه او فقد النظام او فقد تكامله ، وهي تعمل على اجراء تعديلات في انظمة الحاسوب كونها تنتقل من شبكة الى اخرى ومن حاسب الى اخر .

---

(٧) د. محمود محمود مصطفى ، شرح قانون العقوبات ، القسم الخاص ، ط ٨ ، دار النهضة العربية ، القاهرة ، ١٩٨٤ ، ص ٦٤٦.

(٨) د. محمد حسين الغول ، جرائم شبكة الانترنيت والمسؤولية الجزائية الناشئة عنها ، دراسة مقارنة ، ط ١ ، مكتبة بدران الحقوقية ، ٢٠١٧ ، ص ٢٢٤.

(٩) د. محمد حسين الغول ، المرجع سابق ، ص ٢٢٥ ، وبالمعنى نفسه ينظر: د. محمد حماد مرهج الهيتي ، الجريمة المعلوماتية – نماذج من تطبيقاتها ، دراسة مقارنة في التشريع الاماراتي والسعودي والبحريني والقطري والعماني ، دار الكتب القانونية ، دار شتات للنشر والبرمجيات ، ٢٠١٤ ، ص ٣٨٦ - ٣٨٧ ، د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت ، دراسة مقارنة ، ط ٢ ، دار النهضة العربية ، القاهرة ، ٢٠٠٩ ، ص ٢٦٦ .

(١٠) ينظر : د يوسف بن سعيد الكلباني ، مرجع سابق، ص ١٥٢ .

لا بد من الاشارة الى ان مصطلح البرامج الخبيثة MALL WARE هو اختصار لكلمتي MALICIOUS SOFTWARE التي تعني البرامج الماكرة او الخبيثة ، مما جعل المهتمين بالمعلوماتية يدرجون تحت هذا المسمى كافة الوسائل المعلوماتية التي تؤدي الى افساد النظام وتعطيله(١١)، وعلى العموم فان ابرز هذه الوسائل التي سنتناولها في هذا المطلب هي الفايروسات البرامج الخبيثة وبرنامج الدودة ، ويمكن تقسيم هذه البرمجيات إلى عدة فئات على النحو التالي :

المطلب الأول
(برامج الفايروسات الخبيثة)

الفايروس Virus ، في المجال الفني المعلوماتي برنامج يصممه بعض المخترقين لأهداف تخريبية ، مع اعطائه القدرة على ربط نفسه ببرامج اخرى ثم يتكاثر وينتشر داخل النظام المعلوماتي حتى يتسبب في تدميره تماما(١٢).

والفيروسات هي عبارة برمجيات مشفرة للحاسب الالي مثل اي برمجيات اخرى يتم تصميمها بهدف محدد وهو احداث اكبر ضرر ممكن بالأنظمة الالكترونية ، والتي تتميز بإعادة انشاء نفسها حتى تبدو وكأنها تتكاثر وتتولد ذاتيا ، وفي تعبير اخر هو بمثابة المرض الذي يصيب الحاسب الالي ، وهو عبارة عن برنامج صغير يتم تسجيله او زرعه على الاقراص او الاسطوانات الخاصة بالحاسب ويظل هذا الفايروس خاملا لفترة محددة ثم ينشط فجأة في وقت محدد ليدمر البيانات والبرامج المسجلة والمخزنة في داخل الحاسب الالي ، كما يشمل اثره التخريبي الاتلاف والحذف والتعديل(١٣)، كما يمثل النشاط التدميري لها حيث انها تقوم بمسح البيانات والمعلومات المخزنة على وسائط التخزين واتلافها لذا يطلق على هذه العملية اسم مسح البيانات وتحويلها الى صفر ZEROING (١٤).

كما عرف هذا الفايروس أيضاً بأنه (برنامج حاسب الي مصمم عمدا ليقترن ببرنامج اخر ، بحيث يعمل الفايروس عندما يعمل ذلك البرنامج ، ومن ثم يعيد انتاج نفسه باقترانه ببرامج اخرى، ويقترن الفايروس بالبرنامج الاصلي بإلصاق نفسه به او

---

(١١) دلخار صلاح بوتاني ، الحماية الجنائية الموضوعية للمعلوماتية ، دار الفكر الجامعي ، الاسكندرية ، ٢٠١٦ ، ص ٢٣٤ .

(١٢) د . ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالأنترنيت والمعلوماتية (دراسة تطبيقية مقارنة)، الطبعة الاولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، ٢٠١٧، ص٣٩٧.

(١٣) د. هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، ١٩٩٢ ، ص ١١٦.

(١٤) د . عبادة احمد عبادة ، التدمير المتعمد لأنظمة المعلومات الالكترونية ، بحث منشور لدى مركز البحوث والدراسات ، الادارة العامة لشرطة دبي ، مارس ، ١٩٩٩ ، ص ٢١.

(ISSN: 2537 - 0758)

استبداله احيانا ، وقد يغير الفايروس نفسه عند اعادة الانتاج فيظهر نسخة معدلة عن النسخة التي قبلها كلما كرر العملية[١٥].

كما أن هناك اختلاف جوهري بين فيروسات الحاسب الالي وفيروسات الشبكة المعلوماتية على الرغم من اتفاقهما من حيث التقنية ، وذلك من حيث امكانية الانتشار الواسع فهي كبيرة جدا في مجال الانترنيت ومقيدة بالصدفة بالنسبة لفيروسات الحاسب الالي ، هذا من جهة ومن جهة اخرى نجد ان امكانيات فيروس الشبكة المعلوماتية تفوق تلك المقررة لفيروس الحاسب الالي ، فالأول طالما ان الشبكة تعمل فإرساله مستمر على النحو الموضوع له حتى ولو تم اغلاق الاجهزة الالكترونية او الشبكات او الخوادم ، في حين ان النوع الثاني يكمن في الجهاز المصاب به ولا ينتقل الى الجهاز الاخر الا عن طريق انتقال ملف او برنامج من الجهاز التالف الى جهاز اخر[١٦]، أو عن طريق القرص الصلب او القرص المرن او الممغنط .

ويقال أن مصطلح (فيروس) من المصطلحات الواسعة التي تشمل انواعا مختلفة وكثيرة ومتعددة، تؤدي احيانا مهاما مفيدة او غير ضارة ، ويطلق عليها الفايروسات الامنة واحيانا منها الفيروسات الخبيثة والتي تؤدي الى التخريب والاتلاف والاعطاب ، ويطلق على النوع الاول بالفيروسات الامنة اذ لا تتم برمجة القوة المضافة فيها على اساس القيام بأعمال تخريبية وتدميرية ، بل ان برمجتها تتم على اساس القيام بتحركات مفيدة في بعض الاحيان وان كانت تبدو مزعجة احيانا اخرى ، ولهذا اشار البعض ان الفيروسات في مجال المعلوماتية ، غرضان اولهما الغرض الحمائي ، ويراد به ان الفيروس هنا يكون الغرض منه حماية النظام المعلوماتي من مخاطر النسخ غير المشروع ، اذ ينشط الفايروس بمجرد النسخ ليقوم بتدمير نظام الحاسب الالي الذي يعمل عليه، اما الغرض الثاني هو غرض تخريبي حيث يهدف واضع الفيروس منه الى التخريب والاتلاف المعلوماتي ، بهدف الحصول على منافع شخصية.

أما من حيث الاضرار التي تحدثها الانظمة والاجهزة الالكترونية فهي تنقسم الى قسمين:

القسم الأول : الفيروسات التي تصيب الملفات التنفيذية :

(١٥) د. عمار عباس الحسيني ، جريمة الاتلاف المعلوماتي ، دراسة قانونية مقارنة ، منشورات زين الحقوقية ، بيروت ، الطبعة الاولى ، ٢٠١٩ ، ص ٩٠.

(١٦) د . عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنيت، دار النهضة العربية، القاهرة، ص٣٦٥.

ويقصد بالملفات التنفيذية تلك الملفات المسؤولة عن تشغيل البرامج الموجودة في النظام الإلكتروني ، ومن ثم فان اصابة هذه الملفات سيؤدي الى تعطيل البرنامج بالكامل ، وبرنامج الفايروس عندما يصيب هذه الملفات فانه امات ان يقوم بحذف الجزء الاول من الملف التنفيذي وكتابة نفسه في هذا المكان ، الأمر الذي يؤدي الى توقف عمل الملف التنفيذي بشكل جزئي ويعرف هذا النوع من الفيروسات باسم (فايروسات الكتابة الفوقية) Over Writing viruses ، أو أنه يقوم بنسخ نفسه في الجزء الاخير من الملف التنفيذي ومن ثم فان هذا الاخير يظل يعمل بشكل طبيعي حتى ينشط الفيروس ويقوم بمهامه التخريبية ، ويعرف هذا النوع باسم (فايروسات الكتابة غير الفوقية) .

القسم الثاني : فيروسات الكتابة فوق المباشرة :

هذه الصورة من الفيروسات لا تقوم بنسخ نفسها في ملف عادي كما في النوع الأول، وانما تقوم بكتابة نفسها على القرص الصلب مباشرة، وهذا النوع من الفيروسات عندما يصيب النظام الالكتروني فانه يؤدي الى عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من ان هذه الملفات لا زالت موجودة على القرص الصلب ولم يتم حذفها[١٧]، ولأننا بصدد جريمة الاتلاف الالكتروني، فلا بد من الإشارة إلى أن الدمار الذي تحدثه هذه الفيروسات يقع على مستويات متعددة كالاتي:

أولا – الدمار الخطير :هو الذي يحدث عندما يقوم الفايروس عقب وصوله للحاسب الالي بإحداث تغييرات متوالية في الملفات ونظام التشغيل ، كما لا يستطيع المستخدم ادراكها والفايروس هنا يكون غير مرئي ولا يتم رصده ، وعندما يحدث تغييرات في الملفات والبيانات على الحاسب الالي وفي الوقت نفسه لا يدرك المستخدم التغيير الذي حدث، كما انه يتعامل مع البيانات بانها صحيحة .

ثانياً – الدمار المعتدل : وهو الدمار الذي يحدث اذا قام الفايروس بتهيئة القرص الصلب او بشطبه كاملا، وهنا يكون حجم الدمار بسيطا ، ويمكن اعادة تثبيت نظام التشغيل مرة اخرى وتحميل النسخ الاحتياطية .

ثالثا – الدمار التافه : هو الذي يترتب على بعض انواع الفيروسات ، كما يتمثل في صدور صوت لوحة المفاتيح في وقت معين عند الضغط على ازرار اللوحة ، والتخلص منه يكون بسيطا .

(١٧) د . علي عبود جعفر ، جرائم تكنلوجيا المعلومات الواقعة على الاشخاص والحكومة ، الطبعة الأولى ، مكتبة زين الحقوقية والأدبية، بيروت ، ٢٠١٣، ص ٥٥٤ .

(ISSN: 2537 - 0758)

المطلب الثاني
برنامج الدودة

هي عبارة عن برامج تقوم باستغلال اية فجوة في انظمة التشغيل لكي تنتقل من حاسب لأخر ، مغطيا الشبكة بأكملها ليحدث في النهاية اثارة التخريبية ، وقد ينتقل من شبكة لأخرى عبر الوصلات link التي تربط بينها ، وهذا هو الاختلاف بينه وبين برنامج حصان طروادة الذي دائما ما يعتمد على التدخل الانساني لمباشرة نشاطه، واثناء عملية انتقاله فانه يتكاثر كالبكتريا بإنتاج نسخة منه، ومن اهم اهداف تلك البرامج شغل اكبر قدر ممكن من سعة الشبكة ومن ثم تقليل او خفض كفاءتها، وقد تتعدى اهدافها لتبدأ بعد التكاثر والانتشار بالتخريب الفعلي للملفات والبرامج ونظم التشغيل(١٨).

وقد سمي هذا البرنامج بالدودة لان انتشاره من الناحية الفنية يتلاءم مع طرق انتشار الديدان في الوقت الحاضر ، حيث نجد ان برنامج الدودة يتكون من اجزاء (رأس وجسم كما في الدودة الطبيعية) لتعمل في اجهزة الحاسب متفرقة تواصل فيما بينها عبر الشبكة، فيمكن ان نجد رأس البرنامج في جهاز وذيله في جهز اخر بعيد، ولعل ابرز الطرق انتشارا لهذه الديدان هي مرفقات البريد الالكتروني المصابة والتحميل التلقائي عند زيارة بعض مواقع الانترنيت والتسلل عبر الثغرات الامنية في انظمة التشغيل او برامج الحماية، ومن جهة اخرى تتجلى اضرار هذه الديدان في انها تتيح للمهاجم ان يستخدم الحاسب الالي المصاب لمهاجمة مواقع انترنيت او ارسال بريد الكتروني او تحميل برامج ضارة اليه، وكذلك من خلال الدودة فتح باب خلفي في الجهاز المصاب حيث يمكن التحكم به من خلال ذلك الباب، كما يمكن للديدان ان تقوم بنسخ نفسها وارسال نسخة الى كل بريد الكتروني في عناوين البريد المخزنة في جهاز الحاسب الالي المصاب(١٩).

كما عبر عنها البعض بأنها فيروس مخادع يعيش في الشبكات حين بثه ، ثم أنه يقوم بحركات كشفية بحثا عن ابواب غير مؤمنة لكي يدخل منها الى نظام الحواسيب ، وبمجرد انه يدرك انه اصاب نظاما حاسوبيا معينا ، فانه لا يتوقف وانما تقوم بتكرار ذاته في صور استنساخ ، مما يتسبب في تحميل الذاكرة بأكثر مما يجب في فترة زمنية قصيرة ، بما يؤدي الى عجز النظام الحاسوبي عن الحركة ، ومن ناحية اخرى تستخدم

(١٨) د . هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط ، ١٩٩٢، ص ١٦١ .

(١٩) د . ذيب بن عايض القحطاني ، المدخل الى امن المعلومات، الطبعة الاولى ، مكتبة الحميضي ، الرياض ، ٢٠١٠ ، ص ١٢٩ .

هذا النظام الحاسوبي في استنساخ ذاتها لكي تقوم بتفعيل قوتها في الانطلاق لحاسوب اخر وتستمر على هذا الحال الى حين القضاء عليها[٢٠].

الخاتمة

لقد بينا في مقدمة هذه الرسالة بأن موضوع "جريمة إتلاف البيانات الحكومية الالكترونية" من المواضيع المهمة، التي تعالج الجريمة وتسهم في الحد منها، وفيما يأتي نجمل أهم ما توصلنا اليه في متن هذه الرسالة من استنتاجات وتوصيات سوف نقوم باستعراضها بالتفصيل:

أولاً _ النتائج :

١_ ان اغلب التشريعات التي تناولت البيانات والمعلومات بالحماية الجزائية استخدمتها باعتبارها مصطلحات مترادفة ، أما الفرق بينها هو فقط من الناحية النظرية ولا أثر لها في مجال القانون الجنائي .

٢_ لا يوجد تعريف مانع جامع للجرائم المتعلقة بإتلاف لبيانات الحكومية الالكترونية، يتلائم والطبيعة الخاصة لها وفكرة عالمية البيانات والاتصالات والتطور السريع الذي يلحق بهما.

٣- عدم وجود تعاون دولي فعال لمواجهة الجرائم المتعلقة بإتلاف البيانات الحكومية الإلكترونية وهي من الظواهر الاجرامية المستحدثة وخاصة من الناحية الإجرائية.

٤_ تلاحظ ان الجرائم المتعلقة بإتلاف البيانات الحكومية الالكترونية تتميز عن الجرائم التقليدية بطبيعة خاصة ، ومرد ذلك عدة عوامل اهمها انها ترتكب في بيئة تقنية وتكنلوجيا المعلومات مما اضفى عليها وعلى مرتكبيها سمات خاصة وسمي المجرم فيها بالمجرم المعلوماتي الذي تميز بانه ذو مهارات فنية وتقنية عالية، وايضا فضلا عن كونها جريمة عابرة للحدود ومحل الاعتداء فيها غالبا هي البيانات الحكومية.

٥- عدم وجود محكمة أو قضاء متخصص للنظر بالجرائم المعلوماتية بشكل عام وبالجرائم المتعلقة بإتلاف البيانات الحكومية الالكترونية على وجه الخصوص.

ثانيا _ التوصيات :

من خلال استعراض النتائج السالفة الذكر تم التوصل للتوصيات التالية :

(٢٠) د . ربيع محمود الصغير ، مرجع سابق ، ص ٤٠٤ .

(ISSN: 2537 - 0758)

١_ يجب وضع برامج متخصصة وحديثة للحفاظ على البيانات الحكومية الالكترونية من الانتهاكات المستحدثة للحفاظ على البيانات الحكومية وبيانات الافراد الموجودة لدى الجهات الحكومية لسلامة وحرية حق الخصوصية لديهم .

٢_ ندعوا المشرع العراقي الى المسارعة على المصادقة على مشروع الجرائم المعلوماتية اسوة بالدول العربية الاخرى ، لان مثل هكذا جرائم موجودة في الواقع العراقي بكثرة ، خصوصا جرائم (الهواتف النقالة وجرائم الانترنيت) .

٣_ نوصي المشرع المصري بضرورة انشاء جهات تحقيق متخصصة وقضاء متخصص يعنى بالجرائم المعلوماتية بشكل عام والجرائم المتعلقة بإتلاف البيانات الحكومية الالكترونية بشكل خاص وصولا الى عدالة حقيقية ، وقد يكون لحداثة هذا النوع من الجرائم وقلة المستكشف منها سبب وراء عدم اكتساب تلك الاجهزة خبرة التعامل معها ، ناهيك عن الانتشار الواسع للكمبيوتر وتنوع انظمته وبرامجه.

٤_ السعي الى جعل التشريعات القانونية مواكبة لما يشهده العالم من تطور تقني سريع في مجال المعلومات والاتصالات بما يمهد اليه بوضع الاطر القانونية التي تلتزم بمبدأ الشرعية الجزائية لتنوع الجرائم المرتكبة في المجال المعلوماتي وتجددها ولتغيير الوسائل التي ترتكب فيها هذه الجرائم .

٥_ ضرورة الاستفادة من نظام عمل أجهزة امن الانترنيت في الدول المتقدمة ووسائل التعاون بينها وبين الجهات المحلية واستخدام وسائل التعاون الدولي التي توفرها المنظمات الدولية وفقا للاتفاقيات والمعاهدات المبرمة لمكافحة جرائم الانترنيت بشكل عام والجرائم المتعلقة بإتلاف البيانات الحكومية الالكترونية بشكل خاص.

قائمة المصادر

- **القران الكريم**

أولاً: الكتب :

أ_ كتب اللغة :

١. لسان العرب لابن منظور ابي الفضل جمال الدين بن محمد بن منظور بن مكرم الافريقي، دار احياء التراث العربي، بيروت، الجزء التاسع.

٢. المعجم الوسيط لإبراهيم مصطفى واخرون، ج١، ط٦، مؤسسة الصادق (ع) للطباعة والنشر.

٣. مختار الصحاح للرازي، محمد بن ابي بكر بن عبد القادر، دار الرسالة، الكويت، ١٩٨٢.

ب_ كتب القانون :

١. د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشرات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠٠٣.

٢. د. عمار عباس الحسيني، جرائم الحاسوب والانترنيت (الجرائم المعلوماتية)، الطبعة الاولى ، منشورات زين الحقوقية ، بيروت ، ٢٠١٧ ، ص ١٣٧.

٣. د. محمود محمود مصطفى ، شرح قانون العقوبات ، القسم الخاص ، ط ٨، دار النهضة العربية ، القاهرة ، ١٩٨٤.

٤. د. محمد حسين الغول ، جرائم شبكة الانترنيت والمسؤولية الجزائية الناشئة عنها ، دراسة مقارنة ، ط ١ ، مكتبة بدران الحقوقية ، ٢٠١٧.

٥. د. محمد حماد مرهج الهيتي، الجريمة المعلوماتية – نماذج من تطبيقاتها، دراسة مقارنة في التشريع الاماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، دار شتات للنشر والبرمجيات، ٢٠١٤.

٦. د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت ، دراسة مقارنة ، ط ٢ ، دار النهضة العربية ، القاهرة ، ٢٠٠٩.

٧. دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية ، دار الفكر الجامعي، الاسكندرية ، ٢٠١٦.

٨. د . ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالأنترنيت والمعلوماتية (دراسة تطبيقية مقارنة)، الطبعة الاولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، ٢٠١٧.

٩. د. هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، ١٩٩٢.

١٠. د . عبادة احمد عبادة، التدمير المتعمد لأنظمة المعلومات الالكترونية، بحث منشور لدى مركز البحوث والدراسات، الادارة العامة لشرطة دبي، مارس، ١٩٩٩.

١١. د. عمار عباس الحسيني، جريمة الاتلاف المعلوماتي، دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت، الطبعة الاولى، ٢٠١٩.

(ISSN: 2537 - 0758)

١٢. د . عمر محمد ابو بكر بن يونس ، الجرائم الناشئة عن استخدام الأنترنيت، دار النهضة العربية، القاهرة.
١٣. د . علي عبود جعفر، جرائم تكنلوجيا المعلومات الواقعة على الاشخاص والحكومة، الطبعة الأولى، مكتبة زين الحقوقية والأدبية، بيروت، ٢٠١٣، ص ٥٥٤ .
١٤. د . هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة، أسيوط ، ١٩٩٢.
١٥. د . ذيب بن عايض القحطاني ، المدخل الى امن المعلومات، الطبعة الاولى، مكتبة الحميضي، الرياض، ٢٠١٠.
١٦. د. جميل عبد الباقي الصغير ، القانون الجنائي والتكنلوجيا الحديثة ، دار النهضة العربية ، القاهرة ، ١٩٩٢.
١٧. أمير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي لها (دراسة مقارنه بالتشريعات العربية والأجنبية)، مكتبة الوفاء القانونية، الاسكندرية، ٢٠١٦.
١٨. د. عمار عباس الحسيني، جريمة الاتلاف المعلوماتي، دراسة قانونية مقارنه، منشورات زين الحقوقية، بيروت، لبنان، ٢٠١٩.
١٩. د. خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، ٢٠٠٩.
٢٠. محمد محمود الحوتي، الوجيز في الحماية الجنائية من جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، ط١، ٢٠٢١.

ثانياً_ القوانين :

١. قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤.
٢. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.
٣. قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧.
٤. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

ثالثاً_ التطبيقات القضائية :

١. الطعن رقم (١١١٠ للسنة الثالثة) مجموعة عمر، السنة الثالثة.
٢. الطعن رقم (١٧٩٣ لسنة ١٦ ق) في (١٩٤٦/١١/١١) مجموعة عمر، السنة (٧).
٣. الطعن رقم (٤١٤) لسنة ٤٣) المكتب الفني (٢٤).
٤. الطعن رقم (٩٤٧ لسنة ٥٢) المكتب الفني، السنة ٤٣.