جامعة محمد خيضر – بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق

عنوان المذكرة:

جريمة الإتلاف المعلوماتي

(قانون مقارن)

مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

إعداد الطالبة:

حوحو وفاء

إشراف الأستاذ:

شبري عزيزة

الموسم الجامعي:

2017/2016

شكر و عرفان

الحمد لله والصلاة والسلام على نبي محمد صلى الله عليه وسلم.

اتقدم بجزيل الشكر و الاحترام و التقدير الى استاذتي التي ادين لها بالنجاح "شبري عزيزة" التي تشرفت بمساندتي علميا, ولم تبخل علي بتوجيهاتها السليمة و المستمرة, ونصائحها القيمة والخالصة لوجه الله, كما اشكر كل من ساهم في دعمي و تكويني لوصولي الى هذه المرحلة والحمد لله.

الطالبة: حوحو وفاء

مقدمة

ارتبط ظهور الجريمة بظهور الإنسان ارتباطا قويا, وحازت تطورا كبيرا ومذهلا في العصر الحديث, وكان من المتصور إن تظهر إشكال جديدة من الجرائم لم تكن متوقعة في السابق.
فشهد العالم منذ منتصف القرن العشرين ثورة جديدة, وسميت بالثورة المعلوماتية .وذلك وفقا للمكانة البارزة التي احتلتها المعلومات في الوقت الحالي.

وان التقدم والتطور الحاصل في التكنولوجيا وظهور الشبكة العالمية والانترنت بكل ما حملته من تقدم وخدمات, لم يترك العالم يمر بسلام, لأنه بقدر ما كان يحدث اثأر ايجابية وغير حياة ونمط المجتمعات ومارس في تطورها وتقدمها, فهو لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة في إساءة واستخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع حيث تضر بمصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع كله, حيث أدى هذا التطور إلى ولادة أنماط وصور مستحدثة والتي سميت بالجرائم المعلوماتية.

وباعتبار الطبيعة المعنوية للحاسوب والتي هي المعطيات (المعلومات, البيانات, البرامج) ينطبق عليها صفة المال في القانون وتتمتع بالحماية الجزائية. وبما أن العنصر المعنوي كذلك ,فحتى العنصر المادي تنطبق عليه صفة المال, وتقع عليه الجرائم ومن هذه الجرائم جريمة الإتلاف ألمعلوماتي.

وتعد جريمة الإتلاف ألمعلوماتي صورة من صور الجريمة المعلوماتية التي تقع على الأجهزة الالكترونية أو ما تكون أحيانا في المال المنقول ويكون هذا الإتلاف أيضا مادي بحيث يقع على المكونات المادية المتصلة بالحاسب الآلي وملحقاته بهدف إحداث تغيرات عليه وطمس معالم الجريمة.

وبما أن جريمة الإتلاف ألمعلوماتي تعد سلوك غير مشروع وأنها ترتبط بالحاسبات الالكترونية فهي جريمة عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها .غير أن تطبيق النصوص التقليدية على هذه الصور المستحدثة من الجرائم أدىإلى اختلاف في أراء الفقهاء بشان تطبيق النصوص التقليدية عليها. وقد تصادمت مبادئ وأحكام القضاء في البلد الواحد, فصدرت أحكام تطبق النصوص التقليدية على أي جريمة تقع على نظم معالجة المعلومات, أو أي سلوك يتعلق بالحاسبات الالكترونية .

أهمية الموضوع :

1. يكتسب الموضوع أهمية كبيرة متزايدة بسبب استغلال وسائل الاتصال الحديثة كالانترنت وسائر صور الاتصال الالكتروني عبر الأقمار الصناعية التي استغلها المجرمون المعلوماتيون في إتلافهم للبيانات والأنظمة وتخريبها وتدميرها وذلك لتسهيل ارتكابهم لجرائمهم .
2. وتبرز أهمية الموضوع أيضا من الناحية النظرية والعلمية لكونه يمس كثيرا من مصالح المجتمع وعلى وجه الخصوص الدخول إلى برامج لإتلافها وإحداث تغيير فيها من شانها تمس بالحياة الخاصة للأفراد وبأموالهم وذلك باستخدام المجرم ألمعلوماتي لأساليب وطرق فنية غير مشروعة في أنظمة الغير وتدميرها بما يعرف بالفيروسات المعلوماتية.
3. أن أهمية الموضوع أيضا تتمثل في الاهتمام الكبير من قبل الفقه والتشريعات المختلفة, لمناداتهم بضرورة توفير الحماية اللازمة لمكونات الحاسب الآلي من الإتلاف ألمعلوماتي والقضاء على كياناته المادية والمعنوية .
4. يعتبر الإتلاف فعل خطير في حياة المعلوماتية, مما يؤدي إلى انتشار الاعتداء على البيانات والمعلومات والبرامج داخل المنظومة المعلوماتية, والتي بدورها تعيق سير عمل النظام ألمعلوماتي

أسباب اختيار الموضوع :

_ من أسباب اختيار موضوع الإتلاف ألمعلوماتي كونه جريمة حديثة, وكذلك زيادة أهمية المحافظة والحماية من هذه الجريمة, حيث قامت مختلف الدول والتشريعات بإصدار القوانين التي تحمي بها المعلوماتية من هذه الجريمة الخطيرة والحفاظ على ممتلكات الحاسب الآلي كونه مال منقول مملوك للغير.

_ وبالنظر إلى القانون الجزائري والقوانين المقارنة بعد وضعهم لقوانين تحمي المعلوماتية من جريمة الإتلاف ألمعلوماتي, ودور الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية, أعطوا لنا العديد من المفاهيم الجديدة التي تتعلق بجريمة الإتلاف ألمعلوماتي والقوانين والنصوص التي تحمي ذلك.

أهداف الدراسة :

تهدف دراسة هذا الموضوع إلى :

_ البحث والتعرف على جريمة الإتلاف ألمعلوماتي في مختلف التشريعات الجزائية .

_ تحديد المظاهر التي يقوم عليها الإتلاف ألمعلوماتي, وكيفية سيطرته على الجهاز الآلي, والتحكم فيه بتخريبه وجعله غير صالح للاستعمال .

_ توعية التشريعات الجزائية من هذه الجريمة, وضرورة حماية المعلوماتية من هذا الاعتداء الخطير.

الإشكاليةالرئيسية :

هل تسري الأحكام التقليدية الواردة في قانون العقوبات على جريمة الإتلاف ألمعلوماتي ؟

التساؤلات الفرعية :

1 _ ما مفهوم الإتلاف ألمعلوماتي ؟

2 _ وما هي مظاهره ؟

3 _ كيف تقوم جريمة الإتلاف ألمعلوماتي ؟

4 _ ما موقف التشريعات الجزائية من جريمة الإتلاف ألمعلوماتي ؟

5 –ما هو دور الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية منجريمة الإتلاف ألمعلوماتي؟

المنهج المتبع :

اعتمدنا في بحثنا هذا على **المنهج الوصفي** : وذلك من اجل وصف وتعريف وتبيان مفهوم الإتلاف ألمعلوماتي ومظاهره والأركان التي تقوم عليها الجريمة والجزاءات المقررة التي تهدف إلى حماية المال المنقول من جريمة الإتلاف ألمعلوماتي .

هيكل الدراسة :

من اجل الإجابة على الإشكالية المطروحة رأينا تقسيم هذه الدراسة إلى فصلين :

حيث تطرقنا في الفصل الأول إلى الإطار ألمفاهيمي لجريمة الإتلاف ألمعلوماتي, وذلك من خلال تقسيم الفصل إلى مبحثين, يتناول الأول مفهوم الإتلاف ألمعلوماتي, والثاني ذكرنا فيه مظاهر الإتلاف ألمعلوماتي.

إما الفصل الثاني سنتناول فيه الحماية الجزائية الموضوعية لجريمة الإتلاف ألمعلوماتي في مبحثين مستقلين, سنتطرق في المبحث الأول إلى أركان جريمة الإتلاف ألمعلوماتي والمبحث الثاني سندرس فيه الجزاءات المقررة لجريمة الإتلاف ألمعلوماتي .

الفصل الأول : الإطار ألمفاهيمي لجريمة الإتلاف ألمعلوماتي .

تمهيد:

يعد الإتلاف ألمعلوماتي جريمة من الجرائم ألمعلوماتية التي تقع على الأموال المملوكة للغير, سواء كانت منقولات أو عقارات. وقد يقع فعل الإتلاف المكونات المادية لأنظمة المعالجة الآلية للمعلومات, أو على المعلومات ذاتها .

ويتخذ الإتلاف صورة الاعتداء على المعلومات والبرامج والبيانات المخزنة في أنظمة الحاسب الآلي والمتبادلة بين الحواسيب, بما يؤدي ذلك إلى إعاقة سير عمل النظام الآلي بصورة مختلفة .

لذلك حاولت مختلف التشريعات أن تحمي تلك المعلومات من هذه الجريمة الخطيرة.

و ذلك كان من الضروري التعرف على مفهوم الإتلاف ألمعلوماتي في (المبحث الأول), و أهم مظاهره في (المبحث الثاني).

المبحث الأول: مفهوم الإتلاف ألمعلوماتي .

نظرا للجرائم التي تقع على الحاسب الآلي و تؤثر على منتوجاته وثرواته المعلوماتية. نجد أن جريمة الإتلاف ألمعلوماتي تقع بدورها على الأموال المملوكة للغير, و بذلك تمس الحاسب الآلي بذاته سواء على مكوناته المادية لأنظمة المعالجة الآلية للمعلومات, أو على المعلومات أو البرامج أو البيانات ذاتها.

و لهذا كان من الضروري أن نتناول تعريف الإتلاف ألمعلوماتي في (المطلب الأول) , ثم خصائص الإتلاف ألمعلوماتي في (المطلب الثاني) , لننتهي عند صوره في (المطلب الثالث).

المطلب الأول: تعريف الإتلاف المعلومات .

نظرا للدور الذي يلعبه الإتلاف في مجال المعلوماتية والتكنولوجيا بمختلف صوره كان لابد من التوسع في تفسير الإتلاف ألمعلوماتي .وبصرف النظر نجد أن معظم التشريعات أشارت إلى الإتلاف ألمعلوماتي في مواد قانونية ولم تعرفه قانونيا. وفي هذا الصدد سنتناول في هذا المطلب تعريف الإتلاف ألمعلوماتي وسنحاول إعطاء معنى الإتلاف بصفة عامة في (الفرع الأول) والمقصود بالإتلاف في إطار المعلوماتية في (الفرع الثاني)

الفرع الأول : تعريف الفقه القانوني لمعنى الإتلاف.

تناول كل من المشرع المصري هذه الجريمة في المادة 361 من قانون العقوبات المعدلة بالقانون رقم 97 لسنة 1992 [1].والمشرع الجزائري في المادتين 407 و412 من قانون العقوبات .[2] وأيضا في المادة 322 فقرة 1 من قانون العقوبات

[1]- تنص المادة 361 من قانون العقوبات المصري على انه :" كل من خرب أو اتلف عمدا أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر و بغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين."

[2]- تنص المادة 407 من قانون العقوبات الجزائري على انه :" كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى يعاقب بالحبس منن 3 أشهر إلى 3 سنوات و بغرامة من 500 إلى 5000 " و تنص المادة 412 من نفس القانون :"كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة و ذلك بواسطة مواد من شانها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات و بغرامة من 500 إلى 5000 ".

الفرنسي .[1]والمادة719 من قانون العقوبات السوري .[2] ففي هذه المواد جرمت فعل الإتلاف لكن لم تعطي تعريفا أو معنى للإتلاف لا بصفة عامة أو بصفة خاصة . فذهب الفقه بتعريفه إلى :

"هو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له . فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي اعد من اجله."[3]

وعرف أيضا بأنه:

"لا يخرج عن كونه التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية من طريق الإنقاص من كفاءته للاستعمال , فالإتلاف إذن يرد على كل المال أو على جزء منه بشرط أن يكون الإتلاف في الحالة الأخيرة من شانه أن يجعل المال غير صالح للاستعمال كما انه لا يشترط أن يتم بواسطة وسيلة معينة بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي أخر."[4]

ويقصد به أيضا:

"انه تعيب الشيء بما يجعله غير صالح لما اعد له مع بقاء أصله."[5]

Art 322 -1 du C-P-E dispose que:" la destruction ;la dégradation ou la détérioration d'un bien [1]aparten outruit est punie de deux ans d'emprisonnement et de 30000 d'amende ;sauf s'il est résulté qu'un --dommage léger..."

[2]- تنص المادة 719 من قانون العقوبات السوري على انه :

"1- كل من هدم أو خرب قصدا شيئا يخص غيره مما لم يعين في هذا الباب يعاقب بغرامة لا تتجاوز قيمة الضرر على أن تنقص عن مائة ليرة

2- و إذا كانت قيمة الشيء المتلف أو الضرر الناجم يجاوز المائة ليرة فيمكن علاوة على الغرامة أن يحبس الفاعل مدة لا تفوق الستة أشهر ."

[3]-نهلا عبد القادر المومني , الجرائم المعلوماتية , دار الثقافة للنشر و التوزيع , الأردن , 2008 ,ص 123 .

[4]- أمال قارة , الحماية الجزائية للمعلوماتية في التشريع الجزائري , دار هومة للطباعة و النشر و التوزيع , ط1 , الجزائر , 2006 ,ص 58 .

[5]- سليمان احمد فضل , المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) , دار النهضة العربية , ب ط , القاهرة , 2007 , ص 93 .

فـالملاحظ هنـا مـن هـذه التعـاريف أن الفقهـاء لـم يختلفـوا فـي تعريـف الإتـلاف ولـم يخرجـوا عـن تعريفـه بأنـه يـؤثر علـى مـادة الشـيء و يقلـل قيمتـه الاقتصـادية وينقص مـن كفاءتـه للاسـتعمال بـأي وسـيلة كانـت. ففـي هـذه الجريمـة المشـرع لـم يجـرم فعـل الإتـلاف فقـط وإنمـا جـرم فعـل التخريـب والإتـلاف وعـدم صـلاحية الاسـتعمال, و ذلـك بغاية حماية المال المتلف لقيمته الاقتصادية.

ونلاحـظ أيضـا أن التشـريعات لـم تقيـد النشـاط الإجرامـي فـي هـذه الجريمـة بوسـيلة معينة و إنما أطلق أو قام بذكر الوسيلة التي تقع بها الجريمة.

الفرع الثاني: المقصود بالإتلاف الماس بأنظمة المعلومات.

يقصد بالإتلاف ألمعلوماتي بأنه:

"إتـلاف أو محـو تعليمـات البـرامج أو البيانـات ذاتهـا, ولا يهـدف التـدمير إلـى مجـرد الحصـول علـى منفعـة مـن الحاسـب الآلـي أيـا كـان شـكلها سـواء اسـتيلاء علـى أمـوال أو اطـلاع علـى معلومـات و لكـن إحـداث الضـرر بالنظـام ألمعلومـاتي و إعاقتـه عـن أداء وظيفته."[1]

واتجاه أخر يعرفه بأنه :

"محـو المعلومـات أو البـرامج كليـا أو تـدميرها الكترونيـا أو أن يـتم تشـويه المعلومـات أو البرامج على نحو فيه إتلاف بها يجعلها غير صالحة للاستعمال."[2]

[1]– أيمن عبد الله فكرى, جرائم نظم المعلومات (دراسة مقارنة), دار الجامعة الجديدة للنشر والتوزيع, ط1 , مصر, 2015, ص 47.

[2]– محمد نصر محمد, الوسيط في الجرائم المعلوماتية, مركز الدراسات العربية للنشر و التوزيع , ط 1 , مصر, 2015, ص 47.

ويقصد بفعل الإتلاف في مجال المعلوماتية بأنه:

"قد يقع على المكونات المادية للنظام ألمعلوماتي, وقد يقع على المكونات المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي."[1]

وعرف بمصطلح إتلاف البرامج:

"يعني تدمير البرامج الكترونيا سواء كان كليا أو جزئيا, أو إتلافها على نحو يجعلها غير صالحة للاستعمال."[2]

فنظرا لتعاريف الإتلاف ألمعلوماتي السابق ذكرها أن المشرع بتجريمه فعل الإتلاف فهو يحمي حق الملكية العقارية أو المنقولة من الأفعال التي تنقص مادته أو قيمته في صورة كلية أو جزئية , فتنقضي من منفعة الشيء الذي يتعين أن يكون ذات كيان مادي ملموس ومحسوس وإلا لن يكون محلا لجريمة الإتلاف.

[1]– نهلا عبد القادر المومني, نفس المرجع السابق, ص 123.

[2]– عبد الفتاح بيومي حجازي, نحو صياغة نظرية عامة في علم الجريمة والمجرم ألمعلوماتي, ب د ن, ط 1 , الإسكندرية , 2008, ص 67

الفرع الثالث: المقصود بالمال ألمعلوماتي.

يقصد بالمال ألمعلوماتي:

"الحاسوب بكل مكوناته وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات و معالجتها وتخزينها واسترجاعها عند الطلب. ويتكون من كيانين: كيان مادي و كيان معنوي.[1]

فالكيان المادي يضم الأجهزة المادية المختلفة و هي جهاز الإدخال وجهاز الإخراج ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات و تخزينها وإخراجها. أما **الكيان المعنوي** يشمل البرامج المختلفة التي يتم التحقق من خلالها قيام الحاسب بوظائفه المختلفة وبالإضافة إلى المعلومات المطلوب معالجتها."[2]

[1]- سوير سوفيان , جرائم المعلوماتية, مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام , كلية الحقوق والعلوم السياسية , جامعة أبو بكر بلقايد تلمسان, 2010 – 2011, ص 50 .

[2]- علي عبد القادر القهوجي, الحماية الجنائية لبرامج الحاسب, دار الجامعة الجديدة للنشر, الإسكندرية, 1997, ص 3.

المطلب الثاني: خصائص الإتلاف ألمعلوماتي.

من خلال تعريفنا لجريمة الإتلاف ألمعلوماتي بأنها تتمثل في إعاقة سير العمل في نظام المعالجة الآلية للبيانات وأنها من الجرائم التي افرزها التطور التكنولوجي وهو الأمر الذي أضفى عليها طابعا خاصا يميزها عن جريمة الإتلاف التقليدية.

و نظرا للتعاريف التي تناولناها سنوضح خصائص الإتلاف ألمعلوماتي في النقاط التالية :

1.ترتكب جريمة الإتلاف ألمعلوماتي من طرف شخص متخصص ومحترف على قدر كبير من الكفاءة والثقافة الفنية بعالم المعلوماتية, و يملك الذكاء الذي يسمح له باختراق نظام المعالجة الآلية للمعطيات وإتلاف البرامج والمعطيات والبيانات ثم التخفي.

2.تتم جريمة الإتلاف ألمعلوماتي في بيئة رقمية, و غالبا ما تكون عابرة للحدود الأمر الذي يصعب تعقب مرتكبيها, لا سيما في حالة عدم وجود اتفاقيات دولية في هذا الإطار.

3.تتميز جريمة الإتلاف ألمعلوماتي بعدم وضوحها, إذ يصعب تعقبها في حال حصولها لأن أنماط هذه الجريمة تكون مخفية, و تتطلب جهودا جبارة و خبرة فنية كبيرة من اجل المتابعة والتدقيق.[1]

4.غالبا ما يتعلق محل جريمة الإتلاف الالكتروني بالمال ألمعلوماتي المعنوي الأمر الذي يتطلب تغطية تشريعية خاصة تعالجها وتضبطها.[2]

---

[1]- محسن بن سليمان الخليفة, جرائم المعلوماتية وعقوباتها في الفقه والنظام, مذكرة مقدمة لنيل درجة ماجستير في القانون الجنائي,اكادمية نايف العربية للعلوم الأمنية, قسم الدراسات العليا, 1463 -1464, ص 44 .

[2]- يعيش تمام شوقي, "محل الحماية الجنائية عن جريمة الإتلاف ألمعلوماتي " (مقاربة تحليلية), ملتقى الجريمة المعلوماتية بين الوقاية والمكافحة, كلية الحقوق والعلوم السياسية, جامعة بسكرة, يومي 17- 18 نوفمبر2015, ص 3 .

نستخلص من هذه الخصائص أن جريمة الإتلاف ألمعلوماتي فعلا عمديا غير مشروع بحيث تكون أنماط هذه الجريمة مخفية وتتطلب خبرة فنية كبيرة بحيث تؤدي إلى إعاقة سير العمل في نظام المعالجة الآلية للبيانات والمعلومات والبرامج داخل النظام مما يؤدي إلى إلحاق الضرر بملحقات الحاسوب أو يتسبب في تدمير أجهزته.

المطلب الثالث: صور الإتلاف ألمعلوماتي.

قد يتخذ الإتلاف ألمعلوماتي عدة صور يتم عن طريقها إتلاف المعلومات المخزنة بالنظام ألمعلوماتي إما بواسطة طرق الإتلاف العادية كالحريق أو الضرب أو السرقة وإما عن طريق استبدال أو محو المعلومات أو تخريبها جزئيا أو كليا.

الفرع الأول: استبدال المعلومات.

ويشكل استبدال المعلومات نوع من جرائم الغش أو التزوير ألمعلوماتي[1], وبعد من الأنماط السهلة للإجرام ألمعلوماتي كاستبدال رقم بأخر أو تاريخ معين بتاريخ آخر وهذا النوع من الجرائم على قدر كبير من الخطورة ذلك أنه في حال نجاح التزوير فإن الجريمة قد تستمر لفترة طويلة من الزمن إلى أن يتم الكشف عنها, فهناك على سبيل المثال مجموعة من المستخدمين الإداريين استطاعوا خلال عدة سنوات مضاعفة رواتبهم وأجورهم عن طريق الحاسب الآلي, حتى لحظة الكشف عن هذا العمل الآثم بمحض الصدفة.[2]

[1]- سوير سوفيان, مرجع سابق, ص 39 .

[2]- www.damascusbar.org يوم الزيارة 27 – 02 – 2017

الفرع الثاني: محو المعلومات.

إن يتم شطب البرامج والمعلومات والبيانات المخزنة على الحاسوب[1], ومحوها كليا و تدميرها الكترونيا,[2] فمحو المعلومات هو من أسهل طرق الإتلاف كون انه من خصائص الجرائم المعلوماتية قدرة الجاني على محو آثار جريمته في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفارة, فمثلا قام شخصان باختلاس مبلغ يقدر ب 000. 61 دولار مرسلة من شركات التامين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام ألمعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل[3].

الفرع الثالث: تخريب البيانات.

نصت عليها المادة 407 من قانون العقوبات الجزائري أنه:"كل من خرب أو أتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب عليها بالحبس من سنتين إلى خمس سنوات وبغرامة من 500 إلى 5000 دج ..."[4]

و التخريب:"يقصد به أن المال أصبح غير قابل للإصلاح, أي فقد صلاحيته للاستعمال ."[5]

و يقصد به أيضا:"تخريب البيانات والمعلومات و تغييرها وتعديلها بحيث يتم تشويهها وجعلها غير صالحة للاستعمال."[1]

---

[1] -خالد عياد الحلبي, إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت, دار الثقافة للنشر والتوزيع, ط 1, عمان, 2011, ص 69 .

[2] - هدى حامد قشقوش, جرائم الحاسب الالكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, ب س ن, ص43

[3] -سوير سوفيان, مرجع سابق, ص 40

[4] - المادة 407 قانون العقوبات من الأمر 66-156 المؤرخ في 8 يونيو 1966 , المتضمن قانون العقوبات , المعدل و المتمم , جريدة رسمية العدد08.

[5] - سليمان احمد فضل, المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت), دار النهضة العربية, القاهرة , 2007, ص 93 .

و عـرف بأنـه:"أن يـتم تشـويه المعلومـة أو البرنـامج علـى نحـو فيـه إتـلاف بهـا يجعلهـا غير صالحة للاستعمال."[2]

فيعـد التخريـب صـورة مـن صـور الإتـلاف ألمعلومـاتي بحيـث يشـوه المعلومـة ويغيرهـا ويجعلها غير صالحة للاستعمال.

[1]- خالد عياد الحلبي, مرجع سابق, ص 69 .

[2]- هدى حامد قشقوش, مرجع سابق, ص 43 .

المبحث الثاني: مظاهر الإتلاف ألمعلوماتي.

للإتلاف ألمعلوماتي طرق وأساليب متعددة. فمنها ما يؤثر على ماديات النظام ألمعلوماتي بتعطيلها وإيقافها عن العمل, ومن ما يتعلق بالبرامج المعلوماتية ويؤثر على النظام ألمعلوماتي, ومنها ما يتصل بالمعلومات دون باقي عناصر النظام ألمعلوماتي بحيث يخرج من نطاق البحث تلك الحالة التي يكون فيها الإتلاف بالطرق المادية بالكسر والتخريب وغير ذلك من الطرق. واقتصر ذلك في البحث عن استخدام الطرق التقنية في الإتلاف ألمعلوماتي.

قد قسمنا هذا البحث إلى ثلاثة مطالب :

المطلب الأول: الإتلاف عن طريق الإعاقة والاعتداء .

المطلب الثاني: الإتلاف عن طريق الإضافة والتعديل في المعطيات.

المطلب الثالث: الطرق الفنية لإتلاف المال ألمعلوماتي.

المطلب الأول:الإتلاف عن طريق الإعاقة و الاعتداء.

للإتلاف ألمعلوماتي عدة أشكال مختلفة منها ما يتعلق بالبرامج المعلوماتية ويؤثر على النظام ألمعلوماتي, ومنها ما يؤثر على ماديات النظام ألمعلوماتي بتعطيلها و إيقافها عن العمل, ومنها ما يتصل بالمعلومات دون باقي عناصر النظام ألمعلوماتي. ويخرج من نطاق البحث تلك الحالة التي يكون فيها الإتلاف بطرق المادية بالكسر والتخريب إلى غير ذلك من الطرق ونقصر البحث على استخدام الطرق التقنية في الإتلاف ألمعلوماتي[1]:

الفرع الأول: إعاقة سير العمل في نظام المعالجة الآلية للبيانات.

وينجم عن فعل يتسبب في تباطؤ أو ارتباك عمل النظام, ويسوي بعضهم بين عرقلة النظام عن العمل ومحو أو تعديل أو إلغاء المعلومات[2], وحتى يمكن أن تتحقق الفاعلية في الإتلاف ينبغي أن يوجه لبرامج تشغيل النظام ألمعلوماتي وليس على المعلومات بالمعنى الضيق سواء كان نظام التشغيل يتعامل سواء أكانت مالية و اقتصادية آو شخصية[3].

وتتمثل أساليب الإعاقة في تعديل البرامج في نظام المعالجة أو عمل برنامج احتيالي (كبرنامج salami), أو من خلال إجراء التحويلات الالكترونية كإغراق موقع (site) على الشبكة بالرسائل الالكترونية مما يؤدي إلى شله[4].

---

[1]- أيمن عبد الله فكرى, مرجع سابق, ص 166 .

[2]- نفس المرجع السابق, ص 166 .

[3]- محمد نصر محمد, مرجع سابق , ص 53 .

[4]- محمد أمين احمد الشوابكة, جرائم الحاسوب والانترنت (الجريمة المعلوماتية), دار الثقافة للنشر والتوزيع , ط 1, عمان, 2004, ص 223.

الفرع الثاني: الاعتداء على المعلومات المخزنة داخل النظام ألمعلوماتي.

تقع صورة الإتلاف ألمعلوماتي بتدمير وإتلاف وتخريب المعلومات المخزنة بالنظام ألمعلوماتي[1], بحيث تصير بلا معنى ولا يمكن الاستفادة منها أيا كان نوعها دون أن يترتب على هذا الفعل إلحاق ضرر بالنظام ألمعلوماتي أو برامجه حيث يستمران في العمل بنفس الكفاءة التي كانت قبل وقوع الإتلاف ألمعلوماتي على المعلومات.[2]

الفرع الثالث: تضخيم البريد الالكتروني.

أن يتم إرسال نسخ مكررة بعدد كبير من الرسائل بما يترتب عليه من إعاقة سير النظام التقني ألمعلوماتي بشكل منضبط و يؤدي ذلك الأمر إلى إعاقة استخدام تلك الخدمة أو توقفها وفي الغالب يتم هذا الأمر من خلال فيروسات معلوماتية يتم بثها و نشرها عن طريق الانترنت[3].

الفرع الرابع: بث الفيروسات المعلوماتية عبر شبكة المعلومات لتعطيل الاتصالات.

تعد جريمة بث الفيروسات من اخطر التهديدات التي تمارس ضد شبكة المعلومات فهنا الجريمة لا تقع ضد المعلومات أو البرامج بل تتم قصد تعطيل أو إيقاف شبكة الاتصالات من خلال تدمير أو إتلاف وتخريب برامج الاتصال, وتتحقق صورة الإتلاف ألمعلوماتي تلك من خلال القيام بالإدخال أو التعديل أو المحو للمعلومات

---

[1]- محمد نصر مجمد, مرجع سابق , ص 53 .

[2]- أيمن عبد الله فكرى, مرجع سابق , ص167

[3]- محمد نصر محمد, مرجع سابق , ص 54 .

أو البـرامج[1], كمـا يتحقـق الاعتـداء عـن طريـق التـدخل فـي طـرق معالجـة المعلومـات مـن خـلال الكيانـات المنطقيـة (البـرامج), أو مـن خـلال نقـل المعلومـات بواسـطة بـرامج الاتصال الأمر الذي يؤدي إلى تعطيل أو إيقاف النظام ألمعلوماتي عن العمل[2].

[1]- نصر محمد نصر, مرجع سابق , ص 54 .

[2]- أيمن عبد الله فكرى , مرجع سابق , ص ص 167, 168 .

المطلب الثاني: الإتلاف عن طريق الإضافة و التعديل في المعطيات.

قد تتنوع صور إتلاف البيانات و البرامج بحسب ما إذا اتخذت صورة التدخل في المعطيات أو إذا اتخذت صورة التدخل في الكيان المنطقي.[1]

الفرع الأول: التدخل في المعطيات.

حيث يعتبر التعديل غير المشروع للمعطيات من ابرز صور الإتلاف ألمعلوماتي وأخطرها, إذ يؤدي إلى إحداث تغيير غير مشروع في المعلومات والمعطيات والبيانات بمحوها أو إدخال معلومات وهمية أو مزورة.[2]

أولا: إدخال معلومات وهمية .

و يقصد بذلك إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة من قبل, وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة.

ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولا سيما في المنشات ذات الأموال, حيث يعد المسؤول عن القسم ألمعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب, و الذي قد يكون بضم مستخدمين غير موجودين بالفعل أو الإبقاء على مستخدمين تركوا العمل.[3]

---

[1]– محمد أمين احمد الشوابكة , المرجع السابق , ص 231 .

[2]– يعيش تمام شوقي , المرجع السابق , ص 5 .

[3]– محمد أمين احمد الشوابكة , المرجع السابق , ص 232 .

ثانيا: إدخال معلومات مزورة.

وتعني تزوير المستندات والبيانات المختزنة على الكمبيوتر, وتزوير المعلومات بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية, و تزييف المخرجات وتستهدف جريمة تزوير المستندات والبيانات الممثلة للمستحقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات وأوامر الدفع وقوائم المبيعات وأنظمة التحويل الالكترونية للأموال والودائع المصرفية[1].

الفرع الثاني: التدخل في الكيان المنطقي.

ويتمثل في مجموعة البرمجيات المخصصة لقيام بالمعالجة ويتم ذلك إما بتعديل برنامج معين أو التلاعب داخله أو خلق برنامج جديد وهميا مصطنع يهدف للغش ألمعلوماتي[2].

ويتم أيضا من خلال تعديل برامج الحاسوب, أو دس برامج خبيثة ويطلق عليها تسمية "فيروسات" قد تؤدي إلى تدمير البرامج الأصلية[3].

أولا : تعديل البرنامج.

يعد البرنامج كيانا ماديا له أصل مولد صادر عنه يمكن رؤيته على شاشة الحاسب كترجمة إلى أفكار, كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسب ويأخذ هذا الفرض احد الصور الآتية:

1. التلاعب في البرامج: ويتم ذلك ببرمجة الجهاز الآلي والنظام ألمعلوماتي بشكل يؤدي إلى اختفاء البيانات بشكل كلي أو جزئي.
2. اختلاس نتائج الحساب أو الإدارة: ويتم ذلك عن طريق إعادة نسخ المعطيات عن بعد أو عن طريق عملية النقل الالكتروني للبيانات, وذلك بإتباع أسلوب

---

[1]-محمد أمين احمد الشوابكة, مرجع سابق, ص 232.

[2]-www.djelfa.infoيوم الزيارة : 26-02-2017 .

[3]- يعيش تمام شوقي, المرجع السابق, ص 5.

التجسس ألمعلوماتي عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر شبكة الانترنت.

3. تغيير نظام التشغيل : ويكون ذلك بتزويد برنامج نظام التشغيل بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة كلمة السر Word passe أو مفتاح الشفرة وأداة الربط connections بحيث تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسب الآلي.[1]

ثانيا: خلق برنامج جديد.

وفي هذه الحالة إما أن يكون البرنامج المصطنع وهميا, أو أن يكون برنامجا ناقصا من الناحية الفنية.

1. خلق برنامج وهمي: أي اصطناع برنامج كامل و مخصص فقط لارتكاب فعل الغش ألمعلوماتي.
2. إعداد برنامج ناقص من الناحية الفنية: و في هذا الفرض يقوم الجاني وهو غالبا المبرمج بإدخال فجوات في برنامج الحاسب الآلي حتى يتمكن من تنفيذ التعديلات الضرورية بإدخال كودات (code) إضافية أو إحداث مخارج وسيطة وإذا كان يفترض في المبرمج نزع هذه الفجوات عند الانتهاء من البرمجة, إلا أن سوء النية من المبرمجين قد يتغاضون عن استبعاد هذه الفجوات لممارسة أفعال الغش والاستمرار في استغلال البرنامج المعيب من الناحية الفنية, أو أنها قد تنسى بطريقة الخطأ, بسبب عيب في التصميم, مما يتيح للجاني فرصة الدخول من خلالها[2].

وعادة ما يؤدي التدخل في المعطيات أو الكيان المنطقي للحاسوب إلى إعاقة سير العمل في نظام المعالجة الآلية للمعطيات أو الاعتداء على البيانات الموجودة[3].

---

[1]- محمد أمين احمد الشوابكة, المرجع السابق , ص 236 .

[2]- نفس المرجع السابق, ص 237 .

[3]- يعيش تمام شوقي ,مرجع سابق , ص 5 .

المطلب الثالث: الطرق الفنية لإتلاف المال ألمعلوماتي.

قد تتعدد وسائل الإتلاف ألمعلوماتي أو المكونات المنطقية لأنظمة المعالجة الآلية كما أنها تهدف بإلحاق الضرر لأنظمة الحاسب الآلي وتقوم بإتلافه, كما تقوم بتدميره الكترونيا و تشويهه أو تعديل طرق معالجته وذلك باستخدام الطرق الفنية والتقنية كالفيروسات وبرامج الدودة والقنابل المنطقية والزمنية.

الفرع الأول : فيروسات الحاسب الآلي .

تعد فيروسات الحاسب الآلي طريقة من الطرق الفنية والتقنية لإتلاف البيانات والأموال اللامادية تهدف إلى محوها أو تدميرها الكترونيا أو تشويهها أو تعديل طرق معالجتها[1].

أولا : تعريف الفيروس ألمعلوماتي.

"برنامج حاسب مثل أي برنامج تطبيقي آخر, ولكن يتم تصميمه بواسطة احد المجرمين بهدف محدد وهو إحداث اكبر ضرر ممكن بنظام الحاسب , ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى, وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر, ويتوالد ذاتيا وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة."[2]

[1]- www.Djelfa.info يوم الزيارة : 25-02-2017 .

[2]- نسرين عبد الحميد نبيه, الجريمة المعلوماتية والمجرم ألمعلوماتي, منشاة المعارف, الإسكندرية, 2008, ص 185.

و تعرف أيضا: "أنها عبارة عن برنامج للحاسب الآلي يهدف إلى إحداث اكبر ضرر بنظام الحاسب وله القدرة على ربط نفسه بالبرامج الأخرى, وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيا, ويقوم الفيروس بالانتشار بين برامج الحاسب المختلفة وبين مواقع مختلفة في الذاكرة."[1]

ويقصد بالفيروسات أيضا: "هي برامج مشفرة مصممة يقدر على التكاثر والانتشار من نظام إلى أخر, إما بواسطة قرص ممغنط أو عبر شبكة للاتصالات بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم, وهو ما يسمى عادة باسم أول مكان اكتشف فيه."[2]

ثانيا: خصائص الفيروسات المعلوماتية .

تتمثل خصائص الفيروسات المعلوماتية وفقا للتعريفات المتقدمة في القدرة على الاختراق, والقدرة على الاختفاء, والقدرة على الانتشار, والقدرة على التدمير ألمعلوماتي. ونتناولها فيما يلي:[3]

1. القدرة على الاختراق: تزود البرامج الفيروسية بما يمكنها من اختراق النظم المعلوماتية والمواقع الالكترونية المحاطة بنظم أمنية, ولا يتوقف إيداع المخربين في ذلك عند حد معين بل يتم استخدام كل الوسائل الممكنة التي يتم تزويد الفيروس بها حتى يحقق أهدافه التخريبية والتدميرية للمواقع الالكترونية وأشهر مثال على ذلك فيروس حصان طروادة.

---

[1]- عبد الفتاح بيومي حجازي, الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة, دار النهضة العربية للنشر والتوزيع, ط 1, الإسكندرية , 2009, ص 192.

[2]- نائلة عادل محمد فريد قورة, جرائم الحاسب الآلي الاقتصادية (دراسة نظرية و تطبيقية), ب د ن , منشورات الحلبي الحقوقية, ط 1, لبنان, 2005, ص 192.

[3]- أيمن عبد الله فكرى, مرجع سابق, ص 156.

2. القدرة على الاختفاء: يتم تزويد الفيروس ألمعلوماتي بما يمكنه من التخفي والتمويه حتى لا يتم اكتشافه من قبل المواقع المستهدفة, فهناك فيروسات تدخل للنظام ألمعلوماتي في صورة ملفات مختلفة, وابرز مثال على ذلك الفيروسات المنطقية والزمنية[1].
3. القدرة على الانتشار: إن سرعة انتقال الفيروسات تفوق التصور فهو يستطيع أن ينتقل من قارة إلى أخرى في ثوان معدودة بسبب التكاثر اللانهائي, وقد ساعد على هذا الانتشار توافق في البرامج المستخدمة على نطاق واسع عبر دول العالم, و شبكات المعلومات.
4. القدرة على التدمير: الهدف الأساسي للفيروس ألمعلوماتي هو تدمير وتخريب المعلومات والبرامج بما يؤدي في النهاية إلى تعطيل أو توقف النظم المعلوماتية فإن الفيروس يتجه إلى مكان ما في الذاكرة ويظل كامنا حتى يتحقق الأمر أو الزمن الذي تم برمجة المفجر في الفيروس عليها, ثم أن يقوم بنشاطه في تدمير المعلومات.

من خصائص هذا الفيروس انه معدي: فهو عبارة عن مجموعة من التعليمات والأوامر المتعارضة والممنوعة والغير مشروعة[2] وتوجد برامج حماية ضد ذلك الفيروس تسمى Anti-virus , وهي برامج معلوماتية توقف انتشارها وغالبا ما تقضي عليه[3].

[1]- محمد نصر محمد, مرجع سابق, ص 52 .

[2]- عبد الفتاح بيومي حجازي, النظام القانوني لحماية الحكومة الالكترونية, دار الفكر الجامعي, ط 1, الإسكندرية, 2003 ص 287.

[3]- عبد الفتاح بيومي حجازي, مرجع سابق, ص 506.

ثالثا:أنواع الفيروسات.

الفيروسات كثيرة جدا لا يمكن عدها, وإن كان يمكن حصرها في الفئات التالية:[1]

1. فيروسات الكتابة: وتشترك هذه المجموعة بينها في المكان الذي تصيبه من الحاسب و تنقسم إلى قسمين, الأول يصيب الملفات التنفيذية والثاني ينسخ نفسه داخل ملف خفي على احد وحدات التخزين أو ينسخ نفسه على الاسطوانة مباشرة دون الحاجة إلى ملف.
2. الفيروسات المقيمة: وتتخذ من الذاكرة المؤقتة مكانا دائما لها, وتعمل على كتابة بيانات وهمية داخل الذاكرة المؤقتة مما يؤدي إلى عدم وجود مساحة كافية لتشغيل التطبيقات الأخرى على الحاسب.
3. فيروسات ألمكرو:[2]وتصيب بشكل أساسي الملفات التي تعمل على مجموعة برامج office والملفات الخاصة ببرنامج Microsoft Word فتجعل التعامل معها غير متاح. ويسفر دائما عن ظهور رسائل الخطأ.
4. الفيروسات النائمة: تكتفي هذه بإصابة الحاسب ثم تنتظر لحين تحقق شرط معين دون أن تظهر أثار تخريبية, لتقوم بذلك بعد تحققه من أمثالها فيروس الجمعة الإسرائيلي.

---

[1]- محمد خليفة, الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, دار الجامعة الجديدة, الإسكندرية 2007, ص53.

[2]- جلال محمد الزعبي وأسامة احمد المناعسة , جرائم تقنية نظم المعلومات الالكترونية, دار الثقافة للنشر والتوزيع, ط 1 , عمان , 2010, ص 128.

كما يوجد تقسيم آخر للفيروسات المعلوماتية بحسب وضيفتها:[1]

1. فيروسات في شكل برامج "programmes virus": وهي فيروسات صممت لإصابة المعطيات المطبقة. مثلا هذه الفيروسات تضيف رموز في المعطيات المطبقة وبالتالي بمجرد تشغيل هذه المعطيات المصابة فان الفيروس يبدأ في العمل أي التدفق إلى الذاكرة المركزية بهدف إصابة برامج أخرى ويجعل هذه البرامج غير قابلة للاستعمال .

2.فيروسات إشعال "virus-d'amorçage": هذه الفيروسات تحتل مختلف المواقع في القرص المرن التي تحتوي على البرامج المهمة لتشغيل النظام ألمعلوماتي وضمان سيره الجيد وتصيبها بخلل مهم بحيث لا تفتح الفرصة لاستعمال القرص المرن من جديد في المستقبل.

3. فيروس الكريسماس "christmascard": ينشر عبر البريد الالكتروني :

فبعد أن يتمثل للقارئ بطاقة تهنئة بمناسبة العيد على الشاشة في خلال هذا الوقت يقرا الملفات التي تحتوي على عناوين المشتركين في الشبكة ويرسل نسخ من نفسه إلى هؤلاء المشتركين مما يترتب عليه توقيف النظام كله حتى يتم عزله والقضاء عليه[2].

وكذلك فيروس مايكل أنجلو (MichalAnglo) الذي تم ابتكاره في 6 مارس 1992 م, ومنذ ذلك التاريخ و حتى الآن فان هذا الفيروس ينشط في ذلك اليوم من كل سنة[3].

[1]– دردور نسيم ,جرائم المعلوماتية على ضوء القانون الجزائري والمقارن, مذكرة لنيل شهادة الماجستير في القانون الجنائي, كلية الحقوق والعلوم السياسية, جامعة منتوري قسنطينة , 2012-2013, ص 49.

[2]– محمود احمد عبابنة, جرائم الحاسوب وأبعدها الدولية, دار الثقافة للنشر والتوزيع , ط 1, عمان, 2009, ص 102.

[3]- نفس المرجع السابق, ص 102 .

وهناك تقسيمات أخرى للفيروسات المعلومات بحسب نوعها, أي الفيروسات الخفية الفيروسات المتعددة الإشكال وأخيرا الفيروسات المحمية برموز .[1]

و فيروس حصان طروادة : وهو عبارة عن برنامج يتمتع بقدرته الفائقة على الاختفاء داخل البرنامج الأصلي ليعمل أثناء التشغيل بحيث يؤدي إلى تعديل البرنامج آو تغييره ومحو المعلومات وتدميرها.[2]

رابعا: الحماية الفنية من الفيروسات .

لقد أدى الانتشار الواسع لاستخدام الحاسب الآلي إلى انتشار الفيروسات, والشأن هنا شان السلاح, كلما أنتج نوع أنتج النوع المضاد له وهكذا, فإثر الانتشار الواسع للفيروسات أنتجت العديد من الشركات برامج كمنع الإصابة بالفيروس, ثم ظهرت فيروسات جديدة محصنة ضد هذه البرامج[3].

الفرع الثاني : برامج الدودة .

أطلق في سنة 1988 عبر شبكة الانترنيت في الولايات المتحدة الأمريكية برنامجا يعرف بالدودة والذي سبب لأجهزة الحاسوب خلال الشبكة انهيارا في قيادة وتوجيه الجامعات والمعدات العسكرية ومنشات الأبحاث الطبية.[4]

---

[1]– فيروسات متعددة الأشكال: هذه الفيروسات تتميز بالعبقرية إذ يتغير شكلها في كل عملية إصابة.

فيروسات خفية: هذه الفيروسات نقلت من الرقابة بواسطة قدرتها على التنكر مما يجعل اكتشافها صعب.

فيروسات محمية برموز مشفرة: هذه الفيروسات تحمي نفسها برموز أو شفرة متغيرة مما يجعل من الصعب العثور عليها.

انظر إلى رسالة دردور نسيم, جرائم المعلوماتية على ضوء القانون الجزائري والمقارن, مذكرة لنيل شهادة الماجستير في القانون الجنائي, كلية الحقوق والعلوم السياسية, جامعة منتوري قسنطينة, 2012–2013 , ص 10.

[2]– محمود احمد عبابنة, مرجع سابق , ص 101 .

[3]– محمد خليفة, مرجع سابق , ص 55.

[4]-www.droite entreprise.org يوم الزيارة : 25–02–2017 .

وبـرامج الـدودة: هـي عبـارة عـن بـرامج تسـتغل أيـة فجـوات فـي نظـم التشـغيل كـي تنتقـل مـن حاسـب إلـى آخـر و مـن شـبكة إلـى أخـرى عبـر الوصـلات التـي تـربط بينهـا وتتكاثر أثناء عملية انتقالها كالبكتيريا بإنتاج نسخ منها[1].

و الـدودة المعلوماتيـة: هـي عبـارة عـن برنـامج لـه القـدرة علـى تعطيـل أو إيقـاف نظـام الحاسـب الآلـي بصـورة كاملـة وهـو يستنسـخ نفسـه عـدة مـرات, وينتشـر مـن خـلال الوصـلات الالكترونيـة يظهـر معلومـات غيـر صـحيحة, تـؤدي فـي النهايـة إلـى إغـلاق النظام ومن ثم تلفه.[2]

و تهـدف بـرامج الـدودة إلـى شـغل اكبـر حيـز ممكـن مـن سـعة الشـبكة ومـن ثـم العمـل علـى تقليـل أو خفـض كفاءتهـا, وأحيانـا تتعـدى هـذا الهـدف لتبـدأ بعـدها بالتكـاثر والانتشار في التخريب الفعلي للملفات والبرامج ولنظم التشغيل[3].

[1]- محمود احمد عبابنة, مرجع سابق, ص 103 .

[2]- عبد الفتاح بيومي حجازي, مرجع سابق , ص 509 .

[3]- عن نهلا عبد القادر المومني, مرجع سابق , ص 131 .

ونشير إلى بعض الأمثلة لاستخدام برامج الدودة في إتلاف المعلومات وتدميرها منها :

- ✓ قيام طالب دراسات عليا أمريكي يدعى (روبرت موريس) بإعداد برنامج عرف باسم (warm-internet) تمكن من خلاله من تدمير وإلحاق إضرار ب 16 ألف شبكة حاسبات واسعة الانتشار في الولايات المتحدة الأمريكية, الأمر الذي أسفر عن خسائر مالية قدرت بعدة ملايين من الدولارات.
- ✓ قيام بعض الأشخاص بصنع برامج دودة سميث "بالبرامج الدودية ضد القتلة مستخدمين الذرة " وذلك احتجاجا منهم على قيام الولايات المتحدة الأمريكية بإطلاق مكوك فضائي يحمل مجسا فضائيا مغطى ببودرة نووية, حيث استهدفت هذه البرامج شبكة حاسوب علوم الأرض والفضاء في الولايات المتحدة الأمريكية[1]

[1]- نهلا عبد القادر المومني, مرجع سابق, ص 132 .

الفرع الثالث: القنبلة المعلوماتية.

هو اصطلاح يطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف. وهي بدورها تنقسم إلى قسمين:

أولا: القنبلة المنطقية .

"هي عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منظمة, بحيث تعمل على مبدأ التوقيت فتحدث تدميرا وتغييرا في المعلومات والبرامج عند انجاز أمر معين في الحاسوب أو برنامج معين."[1]

و تعرف أيضا:"بأنها برنامج أو جزء من برنامج ينفذ في لحظة محددة, أو كل فترة زمنية منتظمة, يوضع على شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع."[2]

والقنبلة المنطقية: هي التي تنشط بمجرد لحصول واقعة معينة قبل بدا تشغيل الجهاز. مثالها الفيروس الباكستاني.[3]

ومن الأمثلة الواقعية على وضع قنابل منطقية في النظام ألمعلوماتي من اجل تدمير المعلومات و إتلافها :

- ✓ قيام احد المبرمجين في ولاية تكساس الأمريكية سنة 1985 بوضع قنبلة منطقية في حاسوب الشركة التي كان يعمل بها بعد فصله منها مستغلا عدم تغيير الشركة كلمة السر التي كان يعرفها, مما أدى إلى تدمير سجلات عمولة المبيعات مرة كل شهر.

---

[1]- www.droitetentreprise.org يوم الزيارة : 25-02-2017 .

[2]- محمود احمد عبابنة, مرجع سابق , ص ص 103, 104 .

[3]- عبد الفتاح بيومي حجازي, مرجع سابق , ص 508 .

- ✓ تمكن خبير في نظم المعلومات في الدنمارك من وضع قنبلة منطقية في نظام احد الحواسيب أدت إلى محو أكثر من مائة برنامج, وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال اثر القنبلة إليها[1].
- ✓ زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف, بحيث تنفجر لتتمو سجلات الموظفين الموجودة أصلا في المنشاة , ففي الولايات المتحدة الأمريكية ,في ولاية لوس أنجلس تمكن احد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسوب الخاص بها, مما أدى إلى تخريب هذا النظام عدة مرات.[2]

ثانيا: القنبلة الزمنية.

هي على نقيض من القنبلة المنطقية, فهي تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة, ويتم إدخالها في برنامج, وتنفذ في جزء من الثانية أو في بضع ثوان أو دقائق وفقا للتحديد اللازم.[3] فبتالي هنا الفيروس فيها ينشط في تاريخ معين.[4]

وسميت كذلك لقيامها بالعمل التخريبي في وقت يحدد سلفا ,فعلى سبيل المثال :

يمكن للمخرب كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين وبياناتهم اللازمة لدفع رواتبهم قبل استلام رواتبهم بساعة, مما يؤدي إلى تأخير عملية الدفع وإرباك أعمال الشركة وإساءة سمعتها.[5]

---

[1]- نهلا عبد القادر المومني, مرجع سابق , ص 133 .

[2]-www.droitetentreprise.org يوم الزيارة : 25-02-2017.

[3]- خالد عياد الحلبي, مرجع سابق , ص 87 .

[4]- عبد الفتاح بيومي حجازي , النظام القانوني لحماية التجارة الالكترونية, دار الفكر الجامعي, الإسكندرية, 2002 , ص 93 .

[5]- محمد أمين احمد الشوابكة, مرجع سابق , ص 241 .

ومن احد أمثلة القنبلة الزمنية في أنظمة الحاسوب :

- ❖ قيام احد المبرمجين الفرنسيين بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالجهة التي كان يعمل بها, تتضمن أمرا بتفجيرها بعد ستة أشهر من تاريخ فصله مما ترتب عليه تدمير كافة بياناتها.[1]

ويلاحظ أن أثاره لا تقف فقط عند حد التدمير أو الإتلاف ولكن يمكن الاستفادة منه من قبل المجرمين أيضا في مجال التجسس على بيانات الآخرين.[2]

[1]- خالد عياد الحلبي, مرجع سابق, ص 87 .

[2]- أيمن عبد الحفيظ, الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية, ب د ن , ب ب ن , 2005, ص 73 .

خلاصة الفصل الأول :

لقد تعرضنا في هذا الفصل إلى بيان أهم النقاط التي تمثل جريمة الإتلاف ألمعلوماتي بصفة عامة و خاصة بإبرازنا مفهوم الإتلاف ألمعلوماتي والذي بدوره وضحنا تعريف الإتلاف بصفة عامة و تعريفه في إطار المعلوماتية وكذلك توضيح المقصود بالمال ألمعلوماتي كون أن الإتلاف يقوم على المكونات المادية للحاسب الآلي وهو بدوره من الأموال المادية المعلوماتية.ومن خلال ذلك عرفنا خصائص الإتلاف ألمعلوماتي وصوره. وكذلك عرفنا أن للإتلاف ألمعلوماتي مظاهر يقتصر عليها عن طريق الإعاقة والاعتداء وعن طريق الإضافة والتعديل في المعطيات وفي الأخير الطرق الفنية للإتلاف ألمعلوماتي التي من خلالها إلحاق الضرر بأنظمة الحاسب الآلي.

الفصل الثاني : الحماية الجزائية الموضوعية للإتلاف ألمعلوماتي .

حرصت بعض التشريعات الجزائية الإبقاء على الاهتمام بالحماية الجزائية من الإتلاف ألمعلوماتي بأشكاله المختلفة, ونظرا لنسبية الحماية الجزائية المقررة للمعلوماتية من خلال النصوص التقليدية, توجه رجال القضاء لوضع الأطر القانونية لهذه الحماية لبرامج الحاسب الآلي.

في حين أصبحت المعلومات محلا للإتلاف والتدمير والذي اثَر ووضع حد للاستفادة منها وأهدر قيمتها. فمع ذلك اتجهت مختلف التشريعات إلى حماية تلك المعلومات من الإتلاف والتدمير والحفاظ عليها من الخطر والتعدي عليها.

و لمواجهة هذه الجريمة من الخطر الواقع على المعلومات من الإتلاف والتدمير من اجل الحفاظ على سلامة المعلومات وفقا للأحكام القانونية التي تطبق على المكونات المادية للحاسب الآلي. وكان لابد التطرق في هذا الفصل إلى مبحثين نبين ذلك في:

المبحث الأول: أركان الإتلاف ألمعلوماتي.

المبحث الثاني: الجزاءات الناتجة عن جريمة الإتلاف ألمعلوماتي.

المبحث الأول : أركان الإتلاف ألمعلوماتي .

أن جريمة الإتلاف ألمعلوماتي من الجرائم التي تمس المعلوماتية وتلحق الضرر بها و لقيام هذه الجريمة يجب توافر فيها الركنين المادي والمعنوي حتى يمكن لرجال القضاء وضع الحماية الجزائية لهذه الجريمة وتوقيع عليها الجزاء المناسب وذلك لحماية المعلومات من هذا الفعل.

و نجد أن جريمة الإتلاف ألمعلوماتي تقوم على ركنين أساسيين سنوضَحهما من خلال المطلبين المواليين:

المطلب الأول: الركن المادي لجريمة الإتلاف ألمعلوماتي .

المطلب الثاني: الركن المعنوي لجريمة الإتلاف ألمعلوماتي .

المطلب الأول : الركن المادي لجريمة الإتلاف ألمعلوماتي .

لقد ورد في علم الإجرام لقيام جريمة ما يجب توافر فيها ركنين وهما الركن المادي والركن المعنوي, ولقيام جريمة الإتلاف ألمعلوماتي يجب توافر هذين الركنين.
وقد يتمثل الركن المادي لجريمة الإتلاف ألمعلوماتي في النشاط الإجرامي وهو فعل الإتلاف وأيضا محل الجريمة والمتمثل في مال ثابت أو منقول مملوك للغير.
وسنتحدث عن ذلك في الفروع التالية:

الفرع الأول : النشاط الإجرامي.

النشاط الإجرامي وهو الإتلاف ويتم تعريفه في الفقه بأنه : " كل فعل من شانه يؤثر في مادة الشيء أو في قيامه بوظائفه المختلفة على نحو يذهب من قيمته على النحو غير المعتاد لقيمة الشيء مع مرور الزمن مع قصد الإضرار بالغير ."[1]
والنشاط الإجرامي في جريمة الإتلاف: يتخذ أربع صور كما هو منصوص عليها في المادة 361 قانون العقوبات المصري على النحو التالي:[2]

1. التخريب : ويقصد به أن المال أصبح غير قابل للإصلاح, أي فقد صلاحيته للاستعمال.
2. الإتلاف : ويقصد به تعييب الشيء بما يجعله غير صالح لما اعد مع بقاء أصله.
3. جعل الشيء غير صالح للاستعمال أي إعدام صلاحيته ويلحق بالتخريب .
4. تعطيل الشيء أي إعاقته عن العمل كليا أو جزئيا .

[1] - محمد نصر محمد, مرجع سابق ,ص 58 .
[2] – سليمان احمد فضل , مرجع سابق , ص 93 .

فنلاحظ هنا من النص القانوني عدم تقييد المشرع للنشاط الإجرامي بوسيلة , مما يعني أن هذه الجريمة تدخل ضمن نطاق الجرائم ذات القالب الحر كما أن النص اتسم بتعدد النتائج التي جرمها المشرع وهي الإتلاف أو التخريب أو التعييب أو التعطيل.[1]

ونجد المشرع الجزائري أيضا لم يقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة إذ هي من الجرائم ذات الطابع الحر ولهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج الحاسب الآلي خاصة وأن المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة وحيدة محددة لقيامها.[2]

الفرع الثاني : محل الجريمة .

محل جريمة الإتلاف هو مكونات الحاسوب المادية والمعنوية.[3] ويكون محل المنقولات المادية المعلوماتية كأجهزة الحاسب الآلي وملحقاته مثل شاشات العرض والطابعات والاسطوانات والكابلات والمفاتيح والأقراص الممغنطة وغيرها من المكونات المادية سواء كانت تحتوي بيانات أو برامج أو مجرد أوعية خالية بشرط أن يؤدي الإتلاف أو التخريب إلى الإقلال من قيمتها الاقتصادية.[4]

أما المكونات الغير مادية ويطلق على هذه الحالة للإتلاف تدمير نظم المعلومات ويقصد به إتلاف أو محو تعليمات البرامج أو البيانات ذاتها, ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة الحاسب الآلي أيا كان شكلها. استيلاء على نقود أو

[1] – محمد نصر محمد, مرجع سابق , ص 58 .

[2] – فشار عطاء الله, مواجهة الجريمة المعلوماتية في التشريع الجزائري, بحث مقدم إلى الملتقى ألمغاربي حول القانون والمعلوماتية, عقده باكادمية الدراسات العليا بليبيا في أكتوبر, 2009, ص 10 .

[3] – خالد عياد الحلبي , مرجع سابق , ص 71 .

[4] – سليمان احمد فضل, مرجع سابق , ص 93 .

اطلاع على معلومات. ولكن يبقى ببساطة إحداث الضرر بنظام المعلومات وإعاقته عن أداء وظيفته.[1]

الفرع الثالث : صور تحقق الركن المادي .

يتحقق الركن المادي في جريمة الإتلاف التقني بإحدى هاتين صورتين:

الصورة الأولى :الإتلاف المباشر.

وصورته أن يتوسل الفاعل بصورة مشروعة أو غير مشروعة, و بأية طريقة كانت للوصول إلى جهاز الحاسب الآلي ذاته, أو إحدى مداخلات أو النهايات الطرفية لنظام معلوماتي ما, بصورة مباشرة بوصوله إلى لوحة المفاتيح مثلا, أو بوصوله إلى احد منافذ الدخول وبوابات العبور للنظام, ثم هو يقدم على سلوك تقني الكتروني مباشر ويحقق به الإتلاف المقصود.[2]

الصورة الثانية: الإتلاف الغير مباشر.

وصورته الوصول إلى نظام الحاسب الآلي أو نظم المعلومات عبر نافذة غير مباشرة فالفاعل سواء كان ذا علاقة بالنظام ألمعلوماتي محل الجريمة, أم كان غريبا عنه فانه لا يصل إلى لوحة المفاتيح الخاصة بالنظام بصورة مباشرة, كما هو الفرض السابق ولكنه يستخدم إحدى النهايات الطرفية للنظام, فيستغل وجود اتصال به لأية غاية, أو يستعين بأحد نظم وبرامج الاختراق ألمعلوماتي.[3]

---

[1] – المرجع نفسه , ص 54 .

[2] – جلال محمد الزعبي و أسامة احمد المناعسة, مرجع سابق, ص 124 .

[3] – المرجع نفسه , ص 130 .

المطلب الثاني : الركن المعنوي لجريمة الإتلاف ألمعلوماتي .

أن جريمة الإتلاف من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة فيتعين أن يعلم الجاني انه يعتدي على أموال معلوماتية مملوكة للغير وأن من شان فعله أن يتلف الشيء أو يعطله أو أن ينتقص من منفعته بشكل يجعله غير صالح للاستعمال بما يؤدي إلى إلحاق الضرر به.[1]

و هذه الجريمة لا تتطلب قصدا خاصا, وإنما يكتفي بشأنها القصد العام بعنصرية العلم والإرادة .[2]

و ينتفي القصد إذا اعتقد الشخص أن المال المملوك له, و بأن كان نتيجة غلط مادي كخلطه بينه وبين مال مماثل يملكه, وكذلك ينتفي القصد الجنائي لدى الشخص, الذي يقوم بإدخال إحدى الأقراص الخاصة به, والتي كانت مصابة بفيروس في الجهاز الخاص بإحدى المشروعات من اجل طباعته والتي لها خصائص الطابعة.[3]

و يشترط أيضا لتوافر القصد الجنائي أن تتجه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل أو عدم الصلاحية للاستعمال, فإذا انتفت هذه الإرادة ينتفي بالتبعية القصد الجنائي ومن ثم الجريمة.[4]

---

[1]– محمد أمين احمد الشوابكة , مرجع سابق , ص 221 .

[2]– سليمان احمد فضل , مرجع سابق , ص 106 .

[3]– خالد عياد الحلبي, مرجع سابق, ص 73 .

[4]– المرجع نفسه , ص 106 .

فـالإتلاف جريمـة مقصـودة سـواء بصـورتها الماديـة التقليديـة أو بصـورتها المعنويـة المسـتحدثة ولا يتصـور وقـوع فعـل الإتـلاف جزائيـا بغيـر قصـد. وهـذا القصـد يقـوم علـى عنصـرين العلـم والإرادة, العلـم بالفعـل ونتائجـه ثـم إرادة هـذا الفعـل وإرادة نتائجـه بغـض النظر عن طبيعة وماهية السلوك أو حجم وطبيعة الضرر الناشئ عنه.[1]

[1] - جلال محمد زعبي وأسامة احمد المناعسة , مرجع سابق , ص 130 .

المبحث الثاني: الجزاءات الناتجة عن جريمة الإتلاف ألمعلوماتي.

لقد اختلفت التشريعات حول مسالة حماية المعلومات التي يشملها نظام المعالجة الآلية وذلك بموجب نصوص جريمة الإتلاف, وقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة تحمي من هذه الاعتداءات. وقد قامت عدة دول للاستجابة لهذا الغرض, منها الولايات المتحدة الأمريكية وكندا وفرنسا ومصر و... وغيرها من الدول الأخرى.

أما المشرع الجزائري تدارك مؤخرا هذا الفراغ ولو نسبيا في مجال الجريمة المعلوماتية و ذلك بوضع نصوص قانونية تجرم الاعتداءات الواقعة على المعلوماتية وذلك بموجب القانون رقم 05/04 المتضمن تعديل قانون العقوبات.[1]

و نرى أن المشرع الجزائري قد اغفل عن بعض الاعتداءات لكنه ركز على الاعتداءات الماسة بالأنظمة المعلوماتية. وسنركز ذلك في المطالب التالية :

المطلب الأول : العقوبات المقررة لجريمة الإتلاف ألمعلوماتي .

المطلب الثاني : موقف التشريعات الجزائية من الإتلاف ألمعلوماتي .

المطلب الثالث : دور الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية من الإتلاف ألمعلوماتي.

[1] – القانون رقم 04 – 05 المؤرخ في 10 نوفمبر 2004, المتضمن قانون العقوبات, ج ر , العدد 71 .

المطلب الأول : العقوبات المقررة لجريمة الإتلاف ألمعلوماتي .

لقد وضعت بعض التشريعات الجزائية نصوص قانونية تحمي المعلوماتية من الإتلاف ألمعلوماتي. وقد ورد في قانون العقوبات الأردني نص على جريمة الإتلاف في المادة 445 الفقرة1(كل من الحق باختياره ضررا بمال غيره المنقول يعاقب بناء على شكوى المتضرر)[1]و قانون العقوبات المصري نص في المادة 361 على جريمة الإتلاف (يعاقب كل من خرب أو اتلف أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر و بغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين).[2]

أما الوضع في القانون الجزائري نص على جريمة الإتلاف في المادة 407 من قانون العقوبات "كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500 إلى 5000 دج"

ونصت المادة 412 أيضا من نفس القانون "كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة وذلك بواسطة مواد من شانها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات و بغرامة من 500 إلى 5000 دج .[3]

[1] – خالد عياد الحلبي , مرجع سابق , ص 68 .

[2] – محمد نصر محمد , مرجع سابق , ص 55 .

[3] – المادة 407 و المادة 412 من قانون العقوبات الجزائري .من القانون رقم 04 – 05 المتضمن قانون العقوبات , المؤرخ في 10 نوفمبر 2004 ,ج ر , العدد 71 .

و نرى الأمر الذي اقتصر في القانون الجزائري هو عدم وجود جريمة إتلاف مستقلة و إنما هناك ظرف مشدد فقط لجريمة الدخول أو البقاء غير المصرح بهما , و هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات . وسنتطرق إليها بتفصيل في الفروع الآتية :

الفرع الأول: الدخول و البقاء الغير مشروع في نظام المعالجة الآلية للمعطيات.

نصت عليه المادة 394 مكرر من قانون العقوبات الجزائري : " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 40000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ".[1]

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة " تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 5000 إلى 150000 دج ."[2]

أما في التشريع الفرنسي :

الحبس لمدة سنتين و غرامة مالية تقدر ب (30000) يورو.

لم تكن العقوبة في وقت ليس بالبعيد كما هي عليه الحال ألآن , ذلك أن المشرع الفرنسي عندما سَن أول قانون تناول فيه بالتجريم جرائم الاعتداء على نظم المعالجة الآلية. وهو القانون رقم 88-19 المؤرخ في 5 جانفي 1988 المتعلق بالغش

[1] – المادة 394 مكرر قانون العقوبات الجزائري .

[2] – فشار عطاء الله , مرجع سابق , ص 25 .

ألمعلوماتي , كان الحد الأدنى وكذا الأقصى منخفضا, وهو بهذا يقترب كثيرا من العقوبة التي قررها المشرع الجزائري.[1]

كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي. فالصورة البسيطة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة, تتحقق بتوافر الظرف المشدد لها, و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.[2]

أما الصورة المشددة :

نصت المادة 394 مكرر 2/ 3 من قانون العقوبات الجزائري :" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج ".[3]

كما هو ملاحظ أن المشرع الجزائري قد جعل من النتيجة المترتبة ظرفا مشددا للعقوبة في جريمة الدخول أو البقاء غير المصرح بهما[4], ومن نص المادة 394 مكرر 3/2 قانون العقوبات تحقق ظرفين مشددين وهذان الظرفان ينتجان عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وأما عدم صلاحية النظام لأداء وظائفه و يكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء الغير مشروع وتلك النتيجة الضارة مقصودة, لان تطلب مثل هذا الشرط يكون

[1]– رشيدة بوكر , جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن , منشورات الحلبي الحقوقية , ط1, ب ب ن , 2012 , ص 318 .

[2] – فشار عطاء الله , مرجع سابق , ص 25 .

[3] – المادة 394 مكرر 2 – 3 قانون العقوبات الجزائري .

[4]– رشيدة بوكر , مرجع سابق , ص 325 .

غير معقول ,حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة, أي على سبيل الخطأ الغير ألعمدي.[1]

فنرى أن المشرع اخضع الجاني لعقوبة بسيطة في جريمة الدخول أو البقاء تتراوح من 3 أشهر إلى سنة وغرامة من (50000 إلى 2000000 دج). فان العقوبة تشدد وهذا في الحالتين هما:[2]

الحالة الأولى : إذا نجم عن هذا الدخول أو البقاء حذف أو تغيير المعلومات المنظومة .

فترفع العقوبة إلى ضعف تلك المقررة للجريمة المجردة أو البسيطة سواء في حدها الأدنى الذي يضاعف إلى ستة أشهر, أو في حدها الأقصى الذي يضاعف إلى سنتين, أما الغرامة فترفع للضعف أي تتراوح من مائة ألف (100000) إلى أربعمائة ألف (400000) دينار جزائري .

الحالة الثانية : إذا نجم عن الدخول أو البقاء تخريب لنظام اشتغال المنظومة .

فترفع عقوبة الحبس من ستة (6) أشهر إلى سنتين (2), أما الغرامة فيثبت حدها الأدنى عند خمسين ألف (50000) دينار في حين يرتفع حدها الأقصى عند ثلاثمائة ألف (300000) دينار جزائري .

[1] – فشار عطاء الله , مرجع سابق , ص 27 .

[2] – رشيدة بوكر , مرجع سابق , ص 326 .

والى جانب المشرع الجزائري نجد المشرع الفرنسي الذي بدوره جعل من جسامة النتيجة ظرفا مشددا لعقوبة جريمة الدخول أو البقاء غير المشروع , إذ ترتفع العقوبة متى نجم عن الدخول أو البقاء حذف أو تغيير أو تخريب اشتغال المنظومة .

وهذا ما نصت عليه المادة (323 فقرة 2) كما يلي : "... إذا ترتب على الأفعال المذكورة حذف أو تغيير لمعطيات المنظومة أو تخريب اشتغال هذا النظام تصل العقوبة إلى 3 سنوات حبس و 45000 يورو غرامة.

أما في ظل قانون 1988 رفع المشرع عقوبة الحبس في حدها الأقصى من سنة إلى سنتين بينما ترك الحد الأدنى كما كان عليه و هو شهرين. كما رفع الغرامة في حديها الأدنى و الأقصى.[1]

الفرع الثاني: الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات.

الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان الا إذا تما عمدا .

المادة 2 من الاتفاقية الدولية للإجرام ألمعلوماتي تسمح للدولة العضو أن تشترط بان ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله وجريمة الدخول آو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة.[2]

[1] –رشيدة بوكر,مرجع سابق , ص 326 .

[2] – فشار عطاء الله , مرجع سابق , ص 31 .

الفرع الثالث: الجزاءات المقررة على جريمة الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات .

سنتناول فيها الجزاءات التي قررها المشرع الجزائري لهذه الجريمة الحديثة .

أولا: العقوبات المطبقة على الشخص الطبيعي .

1 _ العقوبات الأصلية:

أ/ الدخول و البقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة (المادة 394 مكرر)

ب / الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال الحذف أو تغيير لمعطيات المنظومة , وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة المادة 394 مكرر 02 -03 .[1]

_ العقوبات التكميلية :

نصت المادة 394 مكرر3 قانون العقوبات الجزائري على العقوبات التكميلية الى جانب العقوبات الأصلية والمتمثلة في:[2]

أ/المصادرة : وهي عقوبة تكميلية تشمل الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية .

[1]–فشار عطاء الله, مرجع سابق , ص 33 .

[2] – المادة 394 مكرر3 قانون العقوبات الجزائري .بموجب الأمر 66 –156 المؤرخ في 8 يونيو 1966 , المتضمن قانون العقوبات , ج ر , ص 158 .

ب / إغلاق الموقع: والأمر يتعلق بالموقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية .

ج / إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها.

الظروف المشددة :

أ / نصت المادة 394 مكرر2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء الغير مشروع داخل النظام , و يتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة. ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر, وفي الحالة الثانية. تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج فهذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه و بين الجريمة الأساسية وهي جريمة الدخول والبقاء غير المشروع علاقة سببية .

ب / نصت المادة 394 مكرر3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية و ذلك إذا استهدفت الجريمة الدفاع الوطني و الهيئات والمؤسسات الخاضعة للقانون العام.[1]

[1] - فشار عطاء الله , مرجع سابق , ص 34 .

ثانيا: العقوبات المطبقة على الشخص المعنوي .

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من الاتفاقية الدولية للإجرام ألمعلوماتي , بحيث يسال الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها, كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة احد أعضائه أو ممثله .

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبعين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة .[1]

كما أشار المشرع الجزائري المسؤولية الجزائية للشخص المعنوي و ذلك في نص المادة 18 مكرر من القانون 04 / 15 المتضمن قانون العقوبات الذي ينص على: العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي:[2]

أ/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة .

ب/ واحدة أو أكثر من العقوبات الآتية .

- حل الشخص المعنوي .
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات .
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات .
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر او غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات .
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها .
- نشر أو تعليق حكم الإدانة .
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات, و تنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته .

[1] – فشار عطاء الله , مرجع سابق , ص 34 .

[2] – المادة 18 مكرر من القانون 04 –15 المتضمن قانون العقوبات , المؤرخ في 10 نوفمبر 2004 , ج ر , العدد 71 .

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه احد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[1]

[1] – فشار عطاء الله , مرجع سابق , ص 34 .

المطلب الثاني: موقف التشريعات الجزائية من الإتلاف ألمعلوماتي.

فقد احتدم الخلاف الفقهي حول مدى صلاحية انطباق نصوص الإتلاف التقليدية على جرائم الإتلاف الالكتروني و جاء ذلك في اتجاهين:[1]

الاتجاه الأول: يرى صلاحية النصوص التقليدية لاستيعاب القوالب الجرمية المستحدثة الناشئة عن استغلال تقنية نظم المعلومات في إيقاع الإتلاف, وذلك اعتمادا على أن المشرع لم يحدد وسيلة لفعل الإتلاف, كما لم يبحث في طبيعة فعل الإتلاف, ولم يشترط فيه شوطا خاصة سوى تحقيقه لآثاره وهي وقوع الضرر الذي لم يحدد هو أيضا لطبيعة معينة, فهم لم يرون أي مانع من تطبيق أحكام نصوص الإتلاف التقليدية على الإتلاف التقني .

_ فأنصار هذا الاتجاه يتجاهلون حديث النصوص التجريمية التقليدية عن المال وصوره باعتبارها أموالا مادية ذات خصائص مادية .

الاتجاه الثاني: هذا الاتجاه أكثر انفتاحا وتفهما للطبيعة الخاصة لفعل الإتلاف التقني وإدراكا أكثر لمعطيات الجريمة وبيئتها إذ أن أنصار هذا الاتجاه لا يرون في النصوص التقليدية ما يستفاد منه في تجريم هذا السلوك المستحدث نظرا لان نصوص التقليدية مغرقة بالمادية, وهي تتحدث عن مال مادي, في حين أن محل جرائم الإتلاف التقنية مال معلوماتي لا يحمى صفات مادية كالمطلوبة بنصوص التجريم التقليدية.

[1] – جمال محمد الزعبي و أسامة احمد لمناعسة, مرجع سابق , ص ص 131 , 132 .

وبشكل عام يمكن ملاحظة أن التشريعات المختلفة ميزت بين إتلاف المعلومات من ناحية وإعاقة أنظمة الحاسبات الآلية من ناحية أخرى. بينما اتجهت بعض الدول كفرنسا, لكسمبورغ, ألمانيا, البرتغال, هولندا, ايطاليا واليابان إلى تجريم كل من الفعلين بنصوص منفصلة واتجهت دول أخرى تعديل النصوص التقليدية الخاصة بجريمة الإتلاف وإدراج الفعلين معا في هذه النصوص كاستراليا, كندا وتركيا واكتفت تشريعات دول أخرى كفنلندا, المملكة المتحدة, والنمسا, والسويد, هولندا واسبانيا وسويسرا إلى تجريم الإتلاف الذي يكون محله المعلومات والبرامج , واختلفت هذه التشريعات في مدى قابلية نصوصها لتطبيق في حالة إعاقة نظام الحاسب الآلي وأخيرا اتجهت تشريعات دول أخرى إلى الاكتفاء بتجريم إعاقة أنظمة الحاسبات الآلية[1].

ويلاحظ على هذه التشريعات ملاحظتين :

الملاحظة الأولى: أن اغلب التشريعات التي تناولت جريمة الإتلاف ألمعلوماتي لم تشر إلى استخدام البرامج الفيروسية لإتلاف المكونات المنطقية أو إعاقتها عن أداء وظائفها , إلا أن جميعها يمكن تطبيقها على حالات الإتلاف ألمعلوماتي الذي يتم بواسطة استخدام البرامج الفيروسية .[2]

الملاحظة الثانية : تختلف النصوص التي تناولت جريمة الإتلاف ألمعلوماتي فيما بينها من حيث تناولها لأعمال الإتلاف التي يمكن أن تقع على المعلومات أثناء نقلها. فإذا كان الإتلاف يقع عادة على معلومات تم تخزينها,فقد يقع أحيانا على معلومات يتم نقلها من مكان إلى آخر حيث يمكن اعتراض عملية نقل المعلومات وإجراء تعديل أو إضافة لها.[3]

---

[1]– نائلة عادل محمد فريد قورة , مرجع سابق , ص 204 .

[2] – أيمن عبد الله فكرى , مرجع سابق , ص ص 303, 304 .

[3] – نائلة عادل مجمد فريد قورة , مرجع سابق , ص 205 .

ومن بيان الملاحظتين السابقتين ,سوف نتناول في ما يلي كل من النصوص بالتشريعات الجنائية في فرنسا والولايات المتحدة الأمريكية والتشريع الكندي, التي تختلف في تجريم إتلاف المعلومات وإعاقة أنظمة الحاسبات الآلية.

1 _ التشريع الفرنسي:

تم تعديل قانون العقوبات الفرنسي وإدخال مواد ذات علاقة بالجريمة المستحدثة منها ما يتعلق بجريمة الإتلاف التقني ,حيث نظمت هذه الجريمة بثلاث نصوص هي:[1]

- ✓ نص المادة 462 / 3 من قانون 19 لسنة 1988 والتي تجرم الدخول في نظام معلوماتي بصفة غير مشروعة وإلحاق الضرر أو تدمير أو إتلاف بمشتملاته من معلومات و بيانات.
- ✓ نص المادة462/ 4 من ذات القانون التي عالجت إلحاق أضرار بحقوق الغير في النظام ألمعلوماتي .
- ✓ نص المادة 462 / 5 من ذات القانون والتي عالجت الدخول الغير مشروع في نطاق معالجة آلية للمعلومات والبيانات وإلغاء بثها أو تعطيلها.

أما في قانون العقوبات الفرنسي الصادر عام 1993 م نظم هذه المسألة في نص المادة 323/ 3 " كل من يدخل بطريقة مخادعة لمعطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام, فإنه يعاقب بالسجن لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك فرنسي ".[2]

[1] – جلال محمد الزعبي و أسامة احمد لمناعسة , مرجع سابق , ص 132 .

[2] – محمود احمد عبابنة , مرجع سابق , ص 214 .

2_ الولايات المتحدة الأمريكية :

لم يحتوي التشريع الفدرالي للولايات المتحدة الأمريكية قبل عام 1986 على تجريم الإتلاف المعلومات والبرامج , وإنما اقتصر التجريم على إعاقة أنظمة الحاسبات الآلية. فقد جرمت الفقرة الثالثة من المادة 1030 (أ) من القانون الفيدرالي لجرائم الحاسبات الآلية الصادر عام 1984 إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية وفي عام 1986, ونتيجة لكثير من الانتقادات التي وجهت إلى القانون الصادر وعام 1984, تم تعديله وأصبحت الفقرة الثالثة من المادة 1030 (أ) تتناول فقط الدخول غير المصرح إلى حاسب آلي تستعمله الحكومة من أعاق الدخول هذا الاستعمال , وأضيفت فقرة خامسة إلى المادة 1030 (أ) تتناول جريمة الإتلاف ألعمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع لحكومة الولايات المتحدة وإدارتها أو حاسب آلي غير تابع للحكومة إلا أنه يتم استخدامه من قبلها أو لصالحها.[1]

وتطبيقا لذلك فلقد أدانت محكمة ولاية نيوجيرسي في الولايات المتحدة المتهم ديفيد سميث . حيث أسند إليه تهمة إنتاج فيروس ميلسيا الذي أجتاح الولايات المتحدة عام 1999 م تسبب في عطل أكثر من مليون جهاز حاسب آلي, وخسارة مالية بحوالي ثمانية مليون دولار, وتم الحكم عليه وفقا الفقرة 1030 (A) البند الخامس من المرسوم رقم (18) الذي يعاقب على إتلاف البرامج و التسبب في الإضرار إلى أجهزة الحاسب الآلي المحمية و التي عرفها ذلك القانون بأنها أجهزة الحاسب الآلي العاملة لدى الحكومة أو لدى المؤسسات المالية والتجارية .[2]

[1]– نائلة عادل محمد فريد قورة , مرجع سابق , ص 214 .

[2] – محمود احمد عبابنة , مرجع سابق , ص 106 .

3 _ التشريع الكندي :

عالجت المادة (387) من قانون العقوبات الكندي كافة أشكال الإتلاف المعنوي أو صور الجريمة التقنية من خلال تجريم كافة أشكال الإعاقة والتعطيل غير المشروع نظم المعلومات وتعديل محتويات البرامج .[1]

[1] – جلال محمد الزعبي , أسامة احمد المناعسة , مرجع سابق , ص ص 132 , 133 .

المطلب الثالث: دور الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية من الإتلاف ألمعلوماتي.

لقد حاولت مختلف التشريعات حماية المعلوماتية من الإتلاف ألمعلوماتي ,وليس ذلك فحسب حتى أن هناك اتفاقية قامت بمكافحة هذه الجريمة, وأبرمت هذه الاتفاقية في مدينة بودابست في سبتمبر 2001 ووقعت عليها العديد من الدول وهي اتفاقية مفتوحة لأي من الدول التي ترغب في الانضمام إليها وهي خاصة بمكافحة الجريمة المعلوماتية وتضم العديد من النصوص التجريمية والإجرائية الخاصة بمكافحة الجريمة المعلوماتية و تقسم دراسة هذه الاتفاقية إلى التجريم الغير مباشر للإتلاف ألمعلوماتي وإلى الحماية الجنائية من الإتلاف ألمعلوماتي.[1]

الفرع الأول: التجريم الغير مباشر من الإتلاف ألمعلوماتي.

أولا: تجريم الولوج غير المشروع للنظام ألمعلوماتي .

تم النص على تجريم الولوج غير القانوني بالمادة الثانية من الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية, والتي تنص على انه:" يجب على كل طرف أن يتبنى التدابير التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل اعتبارها جريمة جنائية, وفقا لقانونه الداخلي, الولوج ألعمدي لكل أو لجزء من جهاز الحاسب بدون حق, كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن

[1] – هلالي عبد اللاه احمد, الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 , دار النهضة العربية , ط1 , ب ب ن ,2003 , ص 29 و ما بعدها .

بنيـة الحصـول علـى بيانـات الحاسـب أو أيـة نيـة إجراميـة أخـرى أو أن ترتكـب الجريمـة في حاسب إلي يكون متصلا عن بعد بحاسب أخر."[1]

فالتعليقـات الـواردة علـى تلـك المـادة وفقـا لمـا جـاء بالمـذكرة التفسـيرية أن الولـوج غيـر القـانوني يعـد الجريمـة الرئيسـية التـي تنطـوي علـى تهديـد والتعـدي علـى امـن النظـام ألمعلومـاتي بمعنـى السـرية والسـلامة والإتاحـة للـنظم و البيانـات المعلوماتيـة, إذ أن هنـاك ضـرورة لتـوفير حمايـة ملائمـة لمصـالح المنظمـات[2], والتـدخل غيـر المصـرح بـه يعنـي القرصـنة أو السـطو أو الـدخول غيـر المشـروع فـي النظـام ألمعلومـاتي كـل أولئـك يجـب أن يعتبـر غيـر قـانوني فـي حـد ذاتـه كمبـدأ عـام , وذلـك علـى أسـاس أن هـذه الأفعـال يمكـــن أن تخلـــق عقبـــات أمـــام المســـتخدمين الشـــرعيين للـــنظم و البيانـات , كمـا يمكـن أن تـؤدي إلـى إتـلاف أو تـدمير بـاهظ التكلفـة فـي حالـة إعـادة البنـاء كمـا أن هـذا التـدخل يمكـن أن يترتـب عليـه الوصـول إلـى بيانـات سـرية, مثـال: ذلـك كلمات المرور أو معلومات عن النظام الهدف وأسرار تسمح باستخدام النظام مجانا.[3]

---

[1] – انظر نص المادة بالفرنسية :

titre 1- infraction contre la confidentialité; l'intègrité et la disponibilité des données et systémesinformatiques Article 2 _ Accés illégal

chaque partie adapte les mesures législatives et autres qui se révélentmécessaires pour ériger en infraction pénale; conformément a sont droit interne ; l'accés intentionnel et sans droit a tout ou partie d'un systém informatique - une partie peut exiger que l'infraction soit commise en violation des mesures de sécurité ; dans l'intention d'obtenir des données informatiques ou dans une outre intention délictueuse ; ou soit en relation avec un systéme informatique connecté à un outre systéme informatique .

انظر :أيمن عبد الله فكرى , مرجع سابق , ص ص 287 .

[2] –أيمن عبد الله فكرى ,مرجع سابق ,ص ص 287 , 288 .

[3] – المرجع نفسه , ص 288 .

ثانيا: الاعتراض غير القانوني بالمادة الثالثة من الاتفاقية .

يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل اعتبارها جريمة جنائية, وفقا لقانونها الداخلي, واقعة الاعتراض ألعمدي و بدون حق من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول, في المنشأ, أو في داخل النظام ألمعلوماتي, بما في ذلك الانبعاث الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات,كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش) أو أن ترتكب الجريمة في حاسب إلي يكون متصلا عن بعد بحاسب آخر.

أن الهدف من نص المادة الثالثة هو حماية الحق في احترام نقل البيانات وأن هذه الجريمة تمثل انتهاك للحق في احترام الاتصالات مثل التصنت والتسجيل التقليدي للمحادثات التليفونية بين الأشخاص. و جريمة الاعتراض غير القانوني تنطبق على وسائل النقل غير العلنية لبيانات الحاسب و يلاحظ أن مصطلح غير العلنية صفة تتبع طبيعة وسائل النقل والاتصال, وليس طبيعة البيانات المرسلة.[1]

الفرع الثاني: الحماية الجنائية من الإتلاف ألمعلوماتي .

أولا: الاعتداء على سلامة البيانات بالمادة الرابعة من الاتفاقية الأوروبية .[2]

1. يجب على كل عضو أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم, تبعا لتشريعية الداخلي, إذا حدث ذلك عمدا, ودون حق, أي إضرار, أو محو, أو تعديل, أو إتلاف, أو طمس للبيانات الحاسب.
2. يمكن لأي طرف أن يحتفظ بحق, اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة.

[1] – أيمن عبد الله فكرى , مرجع سابق , ص ص 292 , 293 .

[2] –المرجع نفسه , ص ص 295 , 296 .

أن الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج الحاسب المكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمدا, وقد ورد بالفقرة الأولى من المادة الرابعة مصطلح الأضرار, ومصطلح التعطيل, وهي من الأفعال المركبة التي تتصل على وجه الخصوص بالإتلاف السلبي لسلامة أو محتوى معلومات البيانات والبرامج, كما ورد بالفقرة أيضا مصطلح محو البيانات, وهذا المصطلح يعادل مصطلح تدمير الأشياء في مجال تدمير الأشياء المادية, فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها.

ثانيا: الاعتداء على سلامة النظام بالمادة الخامسة من الاتفاقية الأوروبية .

يجب على كل عضو أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم, تبعا لتشريعه الداخلي, الإعاقة الخطيرة, إذا حدث ذلك عمدا, ودون حق , لوظيفة نظام الحاسب, عن طريق إدخال, أو نقل, أو إضرار, أو محو, أو تعطيل ,أو إتلاف أو طمس البيانات المعلوماتية.[1]

[1] - Article 5 _ Atteite à l' intégritè du systéme .
chaque partie aopte les mesures législatives et outer qui se révéleutnècessaires pour ériger en infraction pénal ; conformément à sont droit interne ; l'entrave grave ; intentionnelle et sans droit ou fonctionnement d'un systéme informatique ; par l'introduction ; la transmission ; l'endommagement ; l'effacement ; la détérioration ; l'altération et la suppression de données informatiques .

ويهدف هذا النص إلى تجريم الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الاتصالات باستخدام أو التأثير على بيانات الحاسب.

ومصطلح الإعاقة يرتبط بالأفعال التي تمثل اعتداء على حسن تشغيل النظام, وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال, أو النقل, أو الإضرار,أو المحو, أو الإتلاف, أو طمس البيانات المعلوماتية, و يجب أن تكون الإعاقة جسيمة حتى يترتب عليها جزاءا جنائيا, ويجب على دولة أن تحدد الشروط الواجب توافرها حتى تتحقق الإعاقة المجرمة بنص قانوني.[1]

[1]– أيمن عبد الله فكرى , مرجع سابق , ص ص 298 , 299.

خلاصة الفصل الثاني :

لقد وضعت مختلف التشريعات الجزائية الحماية القانونية من جريمة الإتلاف ألمعلوماتي و ذلك من خلال توفر هذه الجريمة لركنيها المادي والمعنوي وذلك لقيام الجريمة لفعل الإتلاف وتتحقق بتوافر القصد الجنائي العام الذي يقوم على عنصري العلم والإرادة , وقد لا تتطلب هذه الجريمة للقصد الخاص. كما اختلفت هذه التشريعات في مسالة حماية المعلومات من خلال توقيع العقوبات أو النصوص التي وضعتها.

كما وضحنا موقف التشريعات الجزائية من هذه الجريمة و صلاحية انطباق نصوص الإتلاف التقليدية على جرائم الإتلاف الالكتروني . وكذلك عرفنا دور الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية , وحمايتها للمعلومات من الإتلاف ألمعلوماتي.

الخـــاتمة

الخاتمة

بعد دراسة موضوع الإتلاف ألمعلوماتي في التشريعات المقارنة, اتضح لنا أن الإتلاف ألمعلوماتي يؤدي إلى محو وطمس تعليمات البرامج والبيانات المخزنة في الحاسب الآلي.

وقد يقع الإتلاف على كل مكونات الحاسب. وذلك بواسطة مجموعة من الكيانات منها المادية والمعنوية, وأن جريمة الإتلاف ألمعلوماتي هي فعل عمدي غير مشروع بحيث تكون أنماط هذه الجريمة مخفية وتتطلب خبرة فنية كبيرة.

و ما يلاحظ أيضا أن الإتلاف ألمعلوماتي صورة من صور الجريمة المعلوماتية بحيث يقوم المجرم ألمعلوماتي ببث فيروسات مختلفة تدخل في البرامج أو البيانات أو المعلومات, و تقوم بالانتشار بحث تخرب أو تتلف المعلومات الموجودة داخلها. أو يقوم الإتلاف ألمعلوماتي بعدة طرق أو أساليب تؤدي إلى هدم وطمس كيانات الحاسب أللآلي.

و على ذلك قامت مختلف التشريعات بوضع نصوص قانونية تقوم بحماية المعلوماتية أو الحاسبات الآلية من هذا الاعتداء الخطير.

و قد قامت أيضا الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية بوضع نصوص قانونية تحمي المعلومات من جريمة الإتلاف ألمعلوماتي.

نتائج الدراسة :

1. أن جريمة الإتلاف ألمعلوماتي جريمة حديثة ازداد تفاعلها كثيرا في الآونة الأخيرة .
2. أن مختلف التشريعات الجزائية لم تعطي تعريفا لجريمة الإتلاف ألمعلوماتي بحيث عرفها الفقهاء وإعطائها مفهوما واسعا .
3. أن المشرع الجزائري وضع نصين جزائيين فقط يعاقب فيهما عن جريمة الإتلاف ألمعلوماتي.
4. أن لجريمة الإتلاف ألمعلوماتي صور و مظاهر منها: المحو والتخريب والاستبدال ومنها الطرق الفنية لإتلاف المال ألمعلوماتي ومنها الاعتداءات الواردة على البيانات والبرامج داخل نظام المعالجة الآلية للبيانات .
5. أن جريمة الإتلاف ألمعلوماتي تقوم على ركنين أساسيين وهما الركن المادي والركن المعنوي, بحيث تقوم هذه الجريمة بتوفر عنصري العلم والإرادة وتوفر القصد الجنائي.
6. أن مختلف التشريعات الجزائية وضعت نصوص قانونية تحمي بها المعلوماتية من جريمة الإتلاف ألمعلوماتي, كما قامت الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية بتوقيع عقوبات على من يقوم بجريمة الإتلاف ألمعلوماتي .

قائمة المصادر

والمراجع

أولا : المصادر.

I. القوانين و الأوامر.

1 _ القانون رقم 04 -15 المؤرخ في 15 نوفمبر 2004 , المتضمن قانون العقوبات , جريدة رسمية, العدد 71 .

2 _ الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 ,المتضمن قانون العقوبات, جريدة رسمية , العدد 08 .

ثانيا : المراجع .

II. الكتب :

1 _ أمال قارة, الحماية الجزائية للمعلوماتية في التشريع الجزائري, دار هومة للطباعة و النشر و التوزيع, الطبعة الأولى, الجزائر, 2006 .

2 _ أيمن عبد الحفيظ, الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية , بدون دار النشر, 2005 .

3 _ أيمن عبد الله فكرى, جرائم نظم المعلومات (دراسة مقارنة), دار الجامعة الجديدة للنشر و التوزيع, الإسكندرية, 2007 .

4 _ جلال محمد الزعبي و أسامة احمد لمناعسة , جرائم تقنية نظم المعلومات الالكترونية, دار الثقافة للنشر و التوزيع, الطبعة الأولى , عمان, 2010 .

5 _ خالد عياد الحلبي, إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت, دار الثقافة للنشر و التوزيع, الطبعة الأولى, عمان, 2011 .

6 _ رشيدة بوكر, جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن , منشورات الحلبي الحقوقية, الطبعة الأولى, 2012 .

7 _ سليمان احمد فضل, المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت), دار النهضة العربية, القاهرة, 2007 .

8 _ عبد الفتاح بيومي حجازي, نحو صياغة نظرية عامة في علم الجريمة و المجرم ألمعلوماتي ,بدون دار النشر, الطبعة الأولى, الإسكندرية, 2008 .

9 _ عبد الفتاح بيومي حجازي, الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة, دار النهضة العربية للنشر و التوزيع, الطبعة الأولى, الإسكندرية, 2009 .

10 _ عبد الفتاح بيومي حجازي, النظام القانوني لحماية الحكومة الالكترونية, دار الفكر الجامعي, الطبعة الأولى, الإسكندرية, 2003 .

11 _ عبد الفتاح بيومي حجازي, النظام القانوني لحماية التجارة الالكترونية, دار الفكر الجامعي, الإسكندرية, 2002 .

12 _ عبد القادر القهوجي, الحماية الجنائية لبرامج الحاسب, دار الجامعة الجديدة للنشر, الإسكندرية, 1997 .

13 _ محمود احمد عبابنة , جرائم الحاسوب و أبعادها الدولية, دار الثقافة للنشر و التوزيع, الطبعة الأولى, عمان, 2009 .

14 _ محمد أمين احمد الشوابكة, جرائم الحاسوب و الانترنت (الجريمة المعلوماتية), دار الثقافة للنشر و التوزيع, الطبعة الأولى, عمان, 2004 .

15 _ محمد خليفة , الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن, دار الجامعة الجديدة, الإسكندرية, 2007 .

16 _ محمد نصر محمد, الوسيط في الجرائم المعلوماتية , مركز الدراسات العربية للنشر و التوزيع, الطبعة الأولى, مصر, 2015 .

17 _ نائلة عادل محمد فريد قورة, جرائم الحاسب الآلي الاقتصادية (دراسة نظرية و تطبيقية), بدون دار نشر, منشورات الحلبي الحقوقية, الطبعة الأولى, لبنان, 2005 .

18 _ نسرين عبد الحميد نبيه, الجريمة المعلوماتية و المجرم ألمعلوماتي, منشأ المعارف, الإسكندرية , 2008 .

19 _ نهلا عبد القادر المومني, الجرائم المعلوماتية, دار الثقافة للنشر و التوزيع, بدون دار نشر, الأردن, 2008 .

20 _ هدى حامد قشقوش, جرائم الحاسب الالكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, بدون سنة النشر.

21 _ هلالي عبد ألاه احمد, الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 , دار النهضة العربية, طبعة الأولى, 2003 .

III. المذكرات .

1 ـ دردور نسيم, جرائم المعلوماتية على ضوء القانون الجزائري و المقارن, مذكرة لنيل شهادة الماجستير في القانون الجنائي, كلية الحقوق و العلوم السياسية, جامعة متنوري قسنطينة, 2012 , 2013 .

2 _ سوير سوفيان, جرائم المعلوماتية, مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام, كلية الحقوق و العلوم السياسية, جامعة أبو بكر بلقايد تلمسان, 2010 _ 2011 .

3 _ محسن بن سليمان الخليفة, جرائم المعلوماتية وعقوباتها في الفقه و النظام, مذكرة مقدمة لنيل درجة ماجستير في القانون الجنائي, اكاديمية نايف العربية للعلوم الأمنية, قسم الدراسات العليا , 1463 _ 1464 .

IV. المداخلات .

1 ـ فشار عطاء الله, مواجهة الجريمة المعلوماتية في التشريع الجزائري, بحث مقدم الى الملتقى ألمغاربي حول القانون و المعلوماتية, عقده باكاديمية الدراسات العليا بليبيا في أكتوبر, 2009 .

2 _ يعيش تمام شوقي, محل الحماية الجنائية عن جريمة الإتلاف ألمعلوماتي (مقاربة تحليلية), ملتقى الجريمة المعلوماتية بين الوقاية و المكافحة, كلية الحقوق و العلوم السياسية, جامعة بسكرة, يومي 17 / 18 نوفمبر 2015 .

V. المواقع الالكترونية :

1 _ www.djelfa.info يوم الزيارة: 22 / 12 / 2016 .

2 _ www.accronline.com يوم الزيارة: 22 / 12 / 2016 .

3 _ www.droitetentreprise.org يوم الزيارة: 22 / 12 / 2016 .

الفهرس