وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

القرصنة الإلكترونية و مكافحتها في التشريع الجزائري

ميدان الحقوق والعلوم السياسية

الشعبة:حقوق

التخصص:قانون قضائي

من إعداد الطالب(ة):

بن عمارة مروة

تحت إشراف الأستاذ(ة):

جلطي منصور

أعضاء لجنة المناقشة

الأستاذ(ة) محمد كريم نور الدين .رئيسا

الأستاذ(ة) جلطي منصور مشرفا مقررا

الأستاذ(ة) زواتين خالد مناقشا

السنة الجامعية: 2024/2023

نوقشت في : 19/ 06 /2024

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

كلية الحقوق و العلوم السياسية
مصلحة التربصات
الرقم :.....م.ت/

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

السيد: بن عمارة مروة الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 410554865 والصادرة بتاريخ: 2024/03/15

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون الخاص

والمكلف بإنجاز مذكرة ماستر بعنوان:

الحوسبة الإلكترونية ومدى خضوعها للتشريع الجبائي

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

تصادق على صحة الإمضاء
بن عمارة مروة
410554865
06 فيفري 2025
المجلس الشعبي البلدي

التاريخ: 06 فيفري 2025

إمضاء المعني

رئيس المجلس الشعبي البلدي
وبالتفويض منه
عون إدارة إقليمية
إمضاء: بوبكر سليمان

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

الإهداء

إلى والديّ العزيزين ,

دعمكم و حبكم كانا النور الذي يضيء دربي

إلى أخي و أختي ,

إلى كل من ساندني في كل خطوة ,

إلى كل هؤلاء ,

أهدي ثمرة عملي المتواضع ,

شكر و تقدير

و شكرا من كل أعماق قلبي

لكل من ساهم في تحقيق هذا العمل ,

لكل من قدم لي الدعم و النصيحة ,

و لكل من كان جزءا من رحلتي

هذا الإنجاز ثمرة تعاونكم و محبتكم

قائمة المختصرات :

ج.ر : الجريدة الرسمية

ط: الطبعة

ق: قانون

ق.ع : قانون العقوبات

م: مجلد

ص: صفحة

دج: دينار جزائري

إ.ج : إجراءات جزائية

V : volume

P : page

مقدمة

تعد التكنولوجيا الحديثة، وخاصة الإنترنت، من أعظم الابتكارات التي شهدها القرن الحادي والعشرون، إذ أحدثت تحولًا جذريًا في كل جانب من جوانب الحياة اليومية. بدءًا من التعليم الذي أصبح أكثر تفاعلاً وسهولة في الوصول إلى المعلومات، وصولًا إلى عالم الأعمال الذي تطور ليصبح أكثر كفاءة واتصالاً عالميًا. كما شملت تأثيرات الإنترنت مجالات الترفيه والحكومة، حيث أصبحت وسائل الإعلام الرقمية والخدمات الحكومية الإلكترونية جزءًا لا يتجزأ من بنيتنا التحتية العالمية .

ومع هذا الانتشار الواسع للتكنولوجيا، برزت تحديات جديدة ومعقدة. من بين هذه التحديات، تبرز مشكلة القرصنة الإلكترونية كواحدة من أخطر التهديدات التي تواجه الأمن السيبراني اليوم. تتعرض الأفراد والمؤسسات والدول لخطر متزايد من الهجمات الإلكترونية التي يمكن أن تؤدي إلى خسائر مالية فادحة وتسريب معلومات حساسة. إن التهديدات الإلكترونية المتنامية تتطلب استجابة فعالة ومستمرة لحماية البيانات وضمان سلامة الأنظمة التكنولوجية .

وهكذا، بينما تواصل التكنولوجيا تشكيل مستقبلنا بطرق لا تعد ولا تحصى، يبقى التحدي الأكبر هو كيفية الاستفادة من هذه الابتكارات مع تأمين الحماية اللازمة ضد التهديدات المرافقة لها.

و كباقي دول العالم لم تكن الجزائر بعيدة عن هذه الظاهرة فقد شهدت في السنوات الأخيرة عدة حوادث تتعلق بالقرصنة الإلكترونية استهدفت مؤسسات حكومية و خاصة منها التعليمية مما دف السلطات إلى اتخاذ اجراءات صارمة لمكافحة هذه الظاهرة و حماية البنية التحتية المعلوماتية , و قد أدرك المشرع الجزائري أهمية وضع إطار تنظيمي و قانوني لمواجهة التحديات التي تفرضها الجرائم المعلوماتية و أصدر العديد من التشريعات و القوانين التي تهدف إلى تعزيز الأمن السيبراني و الحد من عمليات القرصنة .

أهمية الدراسة :

تكمن أهمية هذا البحث في التحديات الكبيرة التي تفرضها القرصنة الإلكترونية على المجتمعات من بينها المجتمع الجزائري خاصة مع التقدم السريع في التكنولوجيا و زيادة الاعتماد على الأنظمة الرقمية في كافة مجالات الحياة , و قد تزايدت الجرائم المعلوماتية في الجزائر بشكل ملحوظ , و لذلك تعد هذه الدراسة ضرورية لفهم مدى فعالية هذه التشريعات في مواجهة التهديدات الإلكترونية و تحليل نقاط القوة و الضعف فيها و تقديم توصيات لتحسين الإطار القانوني لضمان أمان المعلومات و حماية الخصوصية و الإسهام في رفع الوعي بأهمية الأمن السيبراني و تشجيع المؤسسات و الأفراد على تبني ممارسات آمنة في استخدام التكنولوجيا .

أهداف الدراسة :

الهدف من هذا البحث هو تسليط الأضواء على أحد أخطر الجرائم المعلوماتية و هي جريمة القرصنة الإلكترونية فمن خلال دراستنا نسعى لتحليل و دراسة القوانين التي وضعها المشرع بهدف التصدي لهذه الجريمة و الحد من انتشارها.

أسباب اختيار الموضوع :

الأسباب الذاتية: منذ صغري كنت مهتمة بالتكنولوجيا و مع تقدم الزمن أدركت الأهمية الكبيرة للأمن السيبراني في حماية البيانات و المعلومات الشخصية ,هذا الاهتمام الشخصي بالتكنولوجيا حفزني على اختيار موضوع يركز على جوانب الحماية من التهديدات الإلكترونية.

الأسباب الموضوعية :

قلة الأبحاث التفصيلية:

- بالرغم من وجود العديد من الأبحاث في مجال الأمن السيبراني، إلا أن هناك نقصاً في الدراسات التي تتناول موضوع القرصنة الإلكترونية بشكل مفصل. هذا يمنح فرصة لإضافة قيمة علمية حقيقية من خلال تقديم بحث شامل وعميق في هذا المجال.

زيادة جرائم القرصنة:

- تزايد حالات القرصنة الإلكترونية وتنوع أساليبها يشكلان تهديداً متزايداً على الأفراد والمؤسسات. البحث في هذا الموضوع يساعد في فهم كيفية تطور هذه الجرائم وتحديد الطرق الأكثر فعالية لمواجهتها.

الحاجة لتطوير استراتيجيات مكافحة القرصنة:

- أحد الدوافع الرئيسية لاختيار هذا الموضوع هو الحاجة لتطوير استراتيجيات فعالة لمكافحة تأثيرات القرصنة الإلكترونية. البحث في هذا المجال يمكن أن يسهم في تقديم حلول مبتكرة تساعد في حماية المجتمع من هذه الجرائم.

التوعية:

- رفع مستوى الوعي حول مخاطر القرصنة الإلكترونية وكيفية التصدي لها يعتبر من الأمور الضرورية. اختيار هذا الموضوع يمكن أن يسهم في نشر المعرفة وتوعية الجمهور والمجتمعات بمخاطر هذه الجرائم وأساليب الحماية منها.

الدراسات السابقة :

و من بين الدراسات السابقة لموضوع القرصنة الإلكترونية قمت بالاستعانة ب بدراسة الباحثتان دحو نجاة و أولاد حمو فاطمة حيث كان موضوعها " جريمة القرصنة في التشريع الجزائري " في مذكرة الماستر الخاصة بهما حيث تناولتا الإطار المفاهيمي لجريمة القرصنة الإلكترونية وطرق مكافحتها . و الدراسة الثانية كانت أطروحة دكتوراه للباحث عمر يوسف عبد الله موضوعها " الإطار القانوني و المؤسساتي لمكافحة التقليد و القرصنة الإلكترونية " حيث تطرق في الباب الأول إلى النظام القانوني و المؤسساتي لجماية الملكية الفكرية من جرائم التقليد , و في الباب الثاني تناول الآليات القانونية لمكافحة جرائم القرصنة الإلكترونية .

الصعوبات :

من بين الصعوبات التي واجهتني أثناء دراسة هذا الموضوع هو قلة المراجع القانونية التي تحدثت عن جريمة القرصنة الإلكترونية بشكل مفصل و شامل , على الرغم من وجود العديد من المقالات إلا أنها في الغالب تتحدث عن الجريمة المعلوماتية بشكل عام .

المنهج المتبع:

و من طبيعة الموضوع الذي اخترت , ارتأيت أن المناهج التي تلائمه هي المنهج التحليلي و الوصفي , حيث قمت بوصف و تحليل القرصنة الإلكترونية من خلال تبيان مفهومها و خصائها.. و جمع المراجع و تحليل المادة العلمية فيها و إعادة شرحها .

الإشكالية :

و عليه مما سبق يمكن طرح الإشكالية التالية :

_ ماهو الدور الذي يلعبه المشرع الجزائري في مكافحة القرصنة الإلكترونية ؟

و للإجابة على هذه الإشكالية اتبعت الخطة التالية:

خطة الدراسة :

في هذه الدراسة اتبعت الخطة الثنائية حيث خصصت الفصل الأول إلى ماهية القرصنة الإلكترونية بالتطرق إلى مفهومها في المبحث الأول و المبحث الثاني إلى خصائصها و أسباب ارتكابها , أما الفصل الثاني فقد خصصته إلى اجراءات مكافحة القرصنة الإلكترونية في التشريع الجزائري و ذلك بتخصيص المبحث الأول للحماية الموضوعية للأنظمة المعلوماتية من القرصنة , و المبحث الثاني للحماية الإجرائية للانظمة المعلوماتية من القرصنة المعلوماتية .

الفصل

الأول

تمهيد :

بفضل ثروة التكنولوجيا يمكننا ملاحظة كيف تطورت حياة المجتمعات الانسانية حيث أصبحت جزءا لا يتجزأ من حياتنا اليومية ، وتطبيقها في جميع في جميع جوانب الحياة بداية من الإتصالات وانتهاءا بالمعاملات الصناعية والمالية، ولكن صاحب كل هذه الميزات مشاكل أخرى وتسبب في تفاقم الكثير منها بدلا من حلها.

فقد بدأت تكنولوجيا المعلومات تستخدم بشكل غير مشروع ومخرب في بعض الاحيان حيث تم اختراق الأنظمة والشبكات بطرق متطورة.

مما أدى الى انتشار ظاهرة الجرائم الالكترونية بشكل كبير من بينها جريمة القرصنة الإلكترونية التي تهدد الأمن المعلوماتي والاقتصادي والسياسي للدول ، وهي لا تهدد المال والممتلكات فقط بل تهدد أيضا الخصوصيات والحقوق المدنية للأفراد مما يجعلها تشكل تحديا كبيرا للاستقرار والأمن الاجتماعي ولذلك فن فهم هذه الظاهرة الاجرامية وتطوير استراتيجيات فعالة لمكافحتها يعد أمرا ضروريا لضمان سلامة وأمان المجتمعات الحديثة فما هو مفهوم جريمة القرصنة الالكترونية وما هي مظاهرها وأسبابها وماهي الخصائص التي تميزها هذا ما سنتطرق إليه في هذا الفصل.

المبحث الأول : مفهوم جريمة القرصنة المعلوماتية

إن القرصنة الإلكترونية ظاهرة إجرامية متطورة تشكل بذلك تهديدا للأمن و الاستقرارفي مختلف المجالات ,ينبغي أن تعي المجتمعات بخطورته , فهي ليست مقتصرة على البيانات و المعلومات التقنية , بل تستهدف البرامج بجميع اشكالها و لفهم خطورة هذه الجريمة و الإلمام الشامل بها ينبغي أن نمر على تعريفها في المطلب الأول و أنواعها في المطلب الثاني .

المطلب الأول : تعريف جريمة القرصنة المعلوماتية

تعددت التعريفات التي تناولت جريمة القرصنة الالكترونية و سأحاول التطرق إليها كالآتي:

أولا: التعريف اللغوي:

مصدرها " قرصن" و هي السطو على شيء ما كالسفن و البحار.[1]

ثانيا: التعريفات الاصطلاحية:

يعرف قاموس كامبيردج مصطلح "القرصنة "بأنه الاستخدام الغير مشروع لتقنيات الحاسبات الآلية للوصول إلى المعلومات المخزنة على أجهزة الحاسبات الأخرى ,أو لنشر الفيروسات و القرصان "hacker" هو أي شخص يحاول اختراق أنظمة الحاسوب و الوصول إليها دون حق مشروع.[2]

و قد عرفها الفقيه الألماني تديمان بأنها :شكل من أشكال السلوك الإجرامي الغير مشروع أو الضار بالمجتمع باسخدام الحاسب الآلي.[3]

---

[1] https://www.almaany.com/ ,تاريخ01|05|2024,الساعة 15:12

[2] هبة صلاح الدين النموري ,القرصنة الاكترونية على مواقع الانترنت ,المجلة المصرية لعلوم المعلومات ,مصر, م10, ع02 , 01|10|2023,ص38

[3] عبد الفتاح بيومي حجازي , مكافحة جرائم الكمبيوتر في القاون العربي النموذجي, بدون ط , دار الفكر العربي , الاسكندرية ,2006 ,ص22

و يعرفها معاذ عبد الرزاق أحمد بأنها "استخدام نظم المعلومات و الشبكات بطريقة غير مشروعة " , و يصنفها كأحد الجرائم الإلكترونية . و تجدر الإشارة إلى مصطلح آخرو هو piracy و يعني النسخ أو إعادة انتاج غير مصرح به للبرمجيات و المصنفات الفنية و حقوق الطبع و النشر و التأليف بهدف بيعها .[1]

وقد تم تعريفها كذلك على أنها عملية تتعلق باختراق أجهزة الحاسوب عبر شبكة الانترنت و يتسم هذا النوع من الهجمات بالدقة العالية و التي تتيح للمخترقين الوصول إلى معلومات حساسة و هامة, ومع توافر الانترنت عالميا و ارتباط أغلب أجهزة الكمبيوتر به تصبح الأنظمة و البيانات عرضة للخطر و يقوم القراصنة بتنفيذ هذه العمليات باستغلال مهاراتهم في برمجيات الحاسوب و مختلف التقنيات السيبرانية , و يمكن أن يتمثل أحد اهدافهم الرئيسية في اختراق أجهزة مخصصة لذلك و فقط من خلال هذه الاختراقات يستطيع المهاجمون الوصول إلى أجهزة أخرى مرتبطة في نفس الشبكة .[2]

ثالثا: التعريفات القانونية:

عرفتها اتفاقية بودابست في المادة 04 منها تحت مصطلح التدخل البيانات حيث جاء في نصها:" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى لتجريم الأفعال التالية في قانونها الوطني , إذا ما ارتكب عمدا , و بغير حق إتلافا , محو أو إفساد أو تعديل , أو تدمير بيانات موجودة على كمبيوتر ".

وأضافت مصطلح التدخل الغير مشروع في المنظومة و ذلك في المادة الخامسة منها .[3]

و قد عرفتها الاتفاقية العربية لمكافحة جرائم تقنية الانترنت في المادة السادسة منها : "و هي الدخول أو البقاء و كل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو

[1] هبة صلاح الدين النموري, المرجع نفسه ,ص38 وص39

[2] سامي علي حامد عياد , الجريمة المعلوماتية و اجرام الانترنت , بدون ط , دار الفكر الجامعي , الاسكندرية , 2007, ص78

[3] مجلس أوروبا ,الاتفاقية الاوروبية لمكافحة الجريمة المعلوماتية , 2001/11/23

الاستمراربه و في المادة الثامنة كذلك ب " تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا أو بغير وجه حق ".[1]

و قد عرفها المشرع الجزائري في تعديله لقانون العقوبات 15/04 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع مكرر و خصصه للاعتداءات الماسة بانظمة المعالجة للمعطيات حيث وصفها و حدد العقوبات في المادة 394 مكرر (3) [2]"يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة من 1000000 إلى 5000000 دج كل من يقوم عمدا أو عن طريق الغش ما يأتي :

تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أومرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذ القسم.

حيازة أو إفشاء أو نشر أو الاستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.[3]

وعليه كل من يستخدم البرامج المخزنة بطرق غير مشروعة و لأجل منفعة شخصية يعد مرتكبا لهذه الجريمة . [4]

و من خلال هذه التعريفات و بإختصار فإن القرصنة الإلكترونية هي استخدام غير قانوني أو غير مصرح به للوصول إلى أنظمة الكمبيوتر أو الشبكات الإلكترونية لأهداف أو منفعة شخصية من بينها السرقة , التجسس أو التأثير على البيانات و تخريبها أو تعطيل الخدمات.

[1] جامعة الدول العربية , الاتفاقية العربية لمكافحة جرائم تقنية الانترنت , ديسمبر2010 , رقم 185

[2] مريم بالطة ,أسيا برغيث , الأمن المعلوماتي في مواجهة القرصنة الإلكترونية ,دراسات في حقوق الإنسان , جامعة 20 أوت 1955 سكيكدة (الجزائر) , م 06,ع 01 ,2022/06/30 , ص 19.

[3] الأمر رقم 15/04 , المؤرخ في 2004/11/10 , المعدل المتمم للأمر رقم 150/66 الصادر في 1966/06/08 , المتضمن ق .ع , ج ر العدد 71

[4] مريم بالطة , المرجع نفسه ,ص 20

المطلب الثاني : أنواع القرصنة المعلوماتية و مرتكبيها

أولا: أنواع القرصنة:

تصنف الجريمة التقليدية بحسب خطورتها في التشريع الجزائري إلى جنايات و جنح و مخالفات [1]و يختلف هذا التصنيف بالنسبة للجريمة الالكترونية و بصفة خاصة القرصنة المعلوماتية ,حيث تنقسم حسب عدة عوامل منها:

الأساليب أو الطرق المستخدمة في ارتكابها أو بناءا على الدوافع التي تحفز على ارتكابها ,أما بالنسبة للمشرع الجزائري فإنه صنفها إلى جرائم تتم عبر النظام المعلوماتي و تشمل كل الجرائم التي يتم ارتكابها عن طريق تكنولوجيا المعلومات و الصنف الثاني إلى الجرائم التي وقعت على النظام المعلوماتي نفسه.[2]

و نظرا لكثرة هذه التقسيمات سأحاول تقسيمها بشكل عام بحيث تكون شاملة لأهم أنواع القرصنة الالكترونية و هي كالتالي:

سرقة البيانات: تتعرض البيانات للعديد من المخاطر أبرزها السرقة من خلال الانترنت حيث يتمتع المجرمون الالكترونيون بصفة خاصة الهاكرز بمستوى عال من الذكاء و المهارة في التحكم في برامج الحاسوب و تقنياته ,جاعلا إياهم قادرين على استخدام أحدث التقنيات و الأساليب لسرقة المعلومات بكفاءة عالية مما يشكل تحديا كبيرا لأمان المعلومات .[3]

و مع تقدم التكنولوجيا في مجال المعلومات ووجود أمظمة حوسبة تتطور باستمرار متضمنة مجموعة من البرامج التي تسهل للمستخدين الوصول إلى البيانات كمثال على ذلك تسجيلها و تخزينها في بطاقات الذاكرة أو أقراص مضغوطة يصبح تعرضها للسرقة أمرا ممكنا ,و بما أن هذه المعلومات ملك للآخرين تغتبر جريمة الاستيلاء عليها أو التلاعب بها من الجرائم الالكترونية و هذا يدفع بالمشرعين أينما كانوا إلى معاقبة مرتكبي هذه الأفعال بشكل

[1] راحراح شهرزاد, جريمة القرصنة في التشريع الجزائري ,تخصص قانون جنائي و علوم جنائية ,جامعة عبد الحميد بن باديس مستغانم ,2022,ص69

[2] رضاع فتيحة ,الحماية الجنائية للمعلومات على شبكة الانترنت ,رسالة ماجيستر في القانون العام ,جامعة أبي بكر بلقايد ,وهران ,ص69

[3] عبد الله حسين علي محمود ,سرقة المعلومات المخزنة في الحاسب الآلي ,ط04,دار النهضة العربية ,القاهرة ,ص283

صارم [1] . و لكن المرع الجزائري لم يذكر جريمة سرقة المعطيات بشكل خاص بل أشار إليها في المادة 350 من قانون العقوبات و المادة 350 مكرر1في التعديل الأخير لقانون العقوبات بموجب القانون رقم 01/09 المؤرخ في 2009/02/25 ,فالمادة 350 منه تنص على:

"... كل من اختلس شيئا غير مملوك له يعد سارقا..." و تنص المادة 350 مكرر 1 على "... كل من سرق أو حاول سرقة ممتلك ثقافي منقول محمي أو معرف .."

و المشرع الجزائري لم يخالف باقي التشريعات الاخرى فقانون العقوبات المصري نص في المادة 311 منه في تعريفه لجريمة السرقة كالآتي:" كل من اختلس منقولا مملوكا لغيره فهو سارق" . و في القانون الفرنسي لسنة 1994 و في المادة 311 أورد تعريفا للسرقة على أنها "اختلاس الشيء المملوك للغير".[2]

التجسس الإلكتروني:

التجسس الإلكتروني بمثابة عملية سرية تهدف إلى استخراج المعلومات من الأفراد ,المؤسسات ,المنظمات ...الخ دون موافقتهم , و قد تطورت هذه الجريمة لتشمل العديد من الأهداف من معلومات اقتصادية إلى سياسية و عسكرية و شخصية ... و يتميز التجسس الالكتروني عن التقليدي بكونه يعتمد على تكنولوجيا المعلومات مما يمنح للجواسيس الالكترونيين حرية و سهولة أكبر في جمع المعلومات دون أن يلاحظ أحد , لذلك يعد انتهاكا لخصوصية الأفراد و الجماعات.

و بناءا على ذلك تشمل جرائم التجسس الاكتروني على عدة أنشطة مثل اختراق المواقع و الصفحات الاكترونية للتجسس على البيانات الحساسة , سواء كانت نصية أو صوتية أو مرئية , و تشمل هذه الجرائم أيضا ارسال رسائل بريد الكتروني تحتوي على ملفات برمجية قادرة

[1] أحمد محمود مصطفى ,جرائم الحاسبات الآلية في التشريع المصري دراسة مقارنة ,ط01, دار النهضة العربية للنشر و التوزيع ,القاهرة ,2010,ص283

[2] زيبحة زيدان , الجريمة المعلوماتية في التشريع الجزائري و الدولي , بدون ط , دار الهدى , عين مليلة الجزائر , 2011, ص 85

على جمع المعلومات من جهاز المستخدم بشكل آلي بالإضافة إلى استخدام برامج متخصصة لاختراق أجهزة الحاسوب المتصلة بالانترنت بهدف استخلاص البيانات منها.[1]

الإحتيال الإلكتروني:

عرف المشرع الجزائري جريمة الإحتيال الإلكتروني في قانون العقوبات في نص المادة 372 على أنها " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من إلتزامات أو إلى الحصول منها على أي منها أو شرع في ذلك و كان ذلك بالاحتيال و لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأصل على الفور لأي شيء أو في وقوع حادث أو أي واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر و بغرامة من 500 إلى 20000 دج."

و قد ربطها أيضا بانتحال الوظائف و الألقاب أو الأسماء بإساءة استعمالهال و اعتبرها احتيالا .

و عليه فإن جريمة الاحتيال الإلكتروني هي جريمة ناشئة عن استخدام غير مشروع لشبكة الانترنت , فهي كل نشاط غير قانوني تستخدم فيه تقنيات الحاسب الآلي و شبكة الانترنت بغية الحصول على امتياز ما أو التلاعب عمدا ببيانات تشكل قيمة مادية هامة أو الإدخال الغير مصرح به لمعلومات و بيانات صحيحة أو التلاعب في أي تعليمات أو أوامر قد تحكم عملية البرمجة .[2]

و يعتمد ارتكاب هذه الجريمة بشكل خاص على رسائل البريد الإلكتروني التسويقية.[3]

[1] سامية بوشوشة, حياة سليماني , التجسس الالكتروني و طرق مكافحته , مجلة العلوم الاجتماعية و الانسانية , جامعة باجي مختار عنابة الجزائر ,م16, ع 01 , 2023/06/08 ,ص52,53

[2] بولحية شهيرة ,سويح دنيا زاد ,الاحتيال الإلكتروني, مجلة الدراسات القانونية , المركز الجامعي سي حواس بريكة , ع 04, ص38,39

[3] GABRIEL Hudson nkotago , internet fraud ,information for teachers and students ,Journal of international students ,vol 01 , issue 02 , nove;ber 2011, p 71 .

استخدام البرامج الضارة:

في مجال القرصنة الالكترونية يستعين كل من الهاكرز و الكراكرزبعدة برامج خبيثة تساعدهم في تنفيذ جرائمهم منها:

الفيروسات: (virus)

و الفيروس المشار إليه في هذا السياق ليس ذلك النوع من الفيروسات الذي يؤثر على الصحة الجسدية , بل هو فيروس يستهدف أنظمة الحواسيب و يعتبر الفيروس في مجال القرصنة المعلوماتية و جرائم الحاسوب عبارة عن برنامج ضار يتسلل إلى أنظمة الكمبيوتر و بقوم بإتلاف البيانات و المعلومات الموجودة فيها , سواء بمسحها أو إزالتها أو حتى إفسادها بشكل لا يمكن استخدامها بعد ذلك و بالتالي فهو يهدد سلامة المستخدمين و يعرض ملفاتهم للخطر.[1]

برامج الدودة : (warm software)

أطلق هذا النوع من البرامج في الولايات المتحدة الأمريكية عام 1918 مسببا لأجهزة الكمبيوتر من خلال شبكة الانترنت انهيارا في قيادة و توجيه الجامعات و القواعد العسكرية و منشآت الأبحاث العلمية .

فهذا البرنامج يستغل أي فجوة في أنظمة التشغيل متنقلا من حاسوب إلى آخر أو من شبكة إلى أخرى عبر الوصلات التي تربط بينها . و تتناقل أثناء هذا الإنتقال و هي تعمل على تخفيض كفاءة الشبكة أو تخريب الملفات و نظم التشغيل .[2]

[1] محمد علي العريان , الجرائم المعلوماتية , بدون ط,دار الجامعة الجديدة للنشر , الاسكندرية ,2004,ص84

[2] محمد أمين الشوابكة , جرائم الحاسوب و الانترنيت ,ط01 , دار الثقافة للنشر و التوزيع , عمان الاردن , 2009 , ص 240, 239

القنبلة المعلوماتية : (logic bomb) :

و هي بدورها تنقسم إلى قسمين :

*القنبلة المنطقية : و هي عبارة عن برامج صغيرة يتم إدخالها بطرق غير شرعية و مخفية مع برامج أخرى تهدف إلى تدمير برامج و معلومات النظام محدثة تغييرات في لحظة محدودة , بحيث تعمل على مبدأ التوقيت فتسبب دمارا و تغييرا في المعلومات و البرامج عند إنجاز أمر معين في الحاسب الآلي أو أي برنامج آخر .

*القنبلة الزمنية : و أتت هذه التسمية نظرا لكونها تقوم بالعمل التخريبي في وقت يحدد مسبقا فعلى سبيل المثال يمكن للكراكر كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين و بياناتهم الازمة لدفع رواتبهم قبل استلامها بساعة و على خلاف القنبلة المنطقية فإن الزمنية تحدث تأثيرا في لحظة زمنية محددة و بدقة .

حصان طروادة : (trojan horse) **:**

يعد برنامج حصان طروادة [1] من أخطر البرامج التي تستخدم في اختراق الأنظمة المعلوماتية بما يتميز به من قدرة على التخفي و التمويه مما يصعب عملية كشفه و هو ما أكسبه شهرة عالية ، فكما اعتمد حصان طروادة في القصة القديمة على التمويه باستغلال مظهره الخارجي المسالم و غير المسلح عل عكس داخله كان يحوي أسلحة فتاكة و الجنود , و هذا هو المبدأ الذي يرتكز عليه هذا البرنامج فبرامج أحصنة طروادة يبدو مظهرها بريئا , و لكن عندا يشغل أحد المستخدمين هذه البرامج ينشط الجزء الخبيث المستتر و يقوم بالعمل الذي برمج لأجله , و لكن في الأصل صمم هذا البرنامج لأهداف نبيلة كمراقبة الآباء لأبنائهم و أو مراقبة انشطة الموظفين على أجهزة الحواسيب و لكن تم استغلال هذا البرناج لأغراض إجرامية كالقرصنة و التجسس على بيانات المستخدمين , و لكن ما يجعل برنامج حصان طروادة خبيثا أنه يمكن

[1] سمي هذا البرنامج بحصان طروادة لأنه يشبه القصة الشهيرة لحصان طروادة حيث اختبئ الجنود اليونان داخله و استطاعوا اقتحام مدينة طروادة و التغلب على جيشها.

للمخترق قرصنة و اقتحام الحاسب الآلي دون أن يكون على علم بكلمة السر , و هذا ما يجعل المستخدم لا ينتبه لاختراق جهازه .[1]

برامج الإنزال: (droppers)

صممت لمراوغة برامج مكافحة الفيروسات و تعتمد على التشفير غالبا لمنع اكتشافها , و دورها هو تركيب و نقل الفيروسات فهي تنتظر حدوث نشاط على الحاسوب لتقوم بعدها بتلويثه بالفيروسات.[2]

الأبواب الخلفية : (Backdoors)

هي ثغرة تترك عن عمد من الشخص الذي صمم البرنامج لكي يستطيع الدخول للبرنامج عند الحاجة إلى ذلك , و قد شاع استعمال ذلك في البرامج التي تنتجها الولايات المتحدة الأمريكية و التي توج فيها برامج خلفية تسمح لها بالدخول إلى أي نظام يستعمل هذا البرنامج , ففي سنة 2008 تحديدا في شهر أكتوبر قامت شركة مايكروسوفت بنشر تحذير يتضمن وجود ثغرة تسمح بتنفيذ أحد الرموز على عدد من أنظمة التشغيل لديها دون المرور من عملية التحقق منه عبر استخدام عدة تعليمات و تقنيات المضللة لنظام الحماية على الجهاز و تعطيل برامج مكافحة الفيروسات , و قد أضافت تحذيرا آخر عن إمكانية استغلال هذه الثغرة لتحويل الجهاز إلى بوابة للاعتداء على باقي الجهزة المتصلة به. [3]

[1] عميمر عبد القادر , التحديات القانونية لإثبات الجريمة المعلوماتية , بدون ط, دار النشر الجامعي الجديد, 2021, ص40
[2] دلال صادق و حميد ناصر الفتال,أمن المعلومات , دار اليازوري العلمية للنشر و التوزيع ,الأردن ,2008, ص74
[3] عميمر عبد القادر, المرجع السابق , ص40

ثانيا : أنواع القراصنة :

و بما أننا تطرقنا إللى أنواع جريمة القرصنة المعلوماتية فلابد كذلك من التطرق إلى أنواع القراصنة الذين يرتكبون هذه الجرائم فكل نوع من الجريمة المعلوماتية أو القرصنة يقوم بارتكابها شخص متخصص فيها فالشخص الذي يقوم باختراق القاعدة الأمنية لأي مؤسسة اقتصادية كبرى ليس كمن يقوم باختراق حسابات التواصل الإجتماعي على سبيل التسلية فهي تختلف من قرصان إلى آخر حسب الأهداف و المهارة ...إلخ و عليه يتم تصنيفهم كالتالي:

القراصنة الهواة: (hackers)

الهاكر أو المخترق مصطلح عام يطلق على كل شخص يستطيع التلاعب بأجهزة الحاسب الآلي و شبكاته, عللى الرغم من اعتقاد الأغلبية أن هذا المصطلح يطلق على الأطفال الصغار النوابغ الذين يسهرون مع حواسيبهم في الليل , فالهاكرز هم الناس الشغوفة لفهم هذه التقنيات و لديهم ميول كبيرة لها و يطلق عليهم كذلك بالأشخاص الذين يلجون إلى المواقع على شبكة الأنترنت دون استعمال العنف[1].

و كذلك يعرفون على أنهم الشباب المفتون بالتقنيات المعلوماتية و أهم أهدافهم اللهو و المتعة باستعمال هذه التقنيات لإثبات قدراتهم أمام الآخرين , و ذلك عن طريق كشف نقاط الضعف في البرامج و الأجهزة دون إلحاق الضرر بها .[2]

و قد اختلف الفقهاء في تصنيف هذا النوع من الناس على أساس انهم مجرمون حيث أن هدفهم هو المتعة و الاستكشاف و التحدي و هم لا يقومون بأعمال غير أخلاقية و تخريبية عكس نوع آخر سأتطرق إليه تاليا .

[1] عمر يوسف عبد الله, الإطار القانوني و المؤسساتي لمكافحة التقليد و القرصنة الإلكترونية , أطروحة دكتوراه في القانون الخاص , جامعة وهران2 , كلية الحقوق و العلوم السياسية ,2022 , ص207

[2] عبد الفتاح بيومي حجازي , مبادئ الاجراءات الجنائية في جرائم الكمبيوتر و الانترنت , ط01, دار الفكر الجامعي , الاسكندرية , 2006, ص46

و البعض الآخر من الفقهاء رأى أنه يجب تصنيفهم على أنهم مجرمين نظرا لإمكانية أن ينتقل هذا النوع من القراصنة إلى نوع آخر يحترف الإجرام او إنضمامهم إلى منظمات تخريبية أخرى .[1]

القراصنة المحترفون : (crackers)

تعرف هذه المجموعة من الأفراد بالمجرمين المحترفين أو المخربين، ويُشار إليهم أحياناً بـ"كراكرز".

تتراوح أعمارهم عادة بين 25 و45 عاماً، ويتمتعون بمكانة اجتماعية معتبرة. هؤلاء الأفراد غالباً ما يكونون خبراء في مجال التكنولوجيا الإلكترونية، حيث يقومون بتطوير برامج متقدمة جداً لاختراق أنظمة الحماية الخاصة بأجهزة الكمبيوتر والوصول إلى المعلومات المخزنة بداخلها.

على الرغم من قدراتهم العالية في تصميم البرامج، إلا أنهم يوجهون مهاراتهم نحو اختراق الأنظمة الإلكترونية والمعلوماتية بهدف السيطرة الكاملة على بيئة معالجة المعلومات، ومن ثم تدمير البيانات الموجودة فيها بدافع التخريب .[2]

و تتميز هذه الفئة من القراصنة بنزعات إجرامية خطيرة تنم عن رغبتهم العارمة في إحداث التخريب و الفوضى و يمتلكوم مهارات عالية و خبرات واسعة في أنظمة الحاسوب و الشبكات , مما يجعلهم أكثر خطورة من فئة الهاكرز حيث أنه يمكنهم إلحاق أضرار جسيمة لضحاياهم و عادة ما يعود المجرم المحترف إلى ارتكاب الجرائم بشكل متكرر مما يزيد من سجله الإجرامي يعيش هذا النوع من القراصنة من العائدات التي يجنونها من أنشطتهم الغير قانونية و التي تكون غالبا مدفوعة بالربح الشخصي بدلا من الدوافع الإيديولوجية , و هذا ايجعلهم أكثر تهديدا , حيث تكون أضرارهم على الضحايا كبيرة .[3]

[1] عمر يوسف عبد الله , المرجع السابق , ص208
[2] أشرف السعيد أحمدي , القرصنة الإلكترونية , بدون ط , دار الفكر العربي, القاهرة , 2010 , ص28
[3] عمر يوسف عبد الله, نفس المرجع , ص208

القراصنة الحاقدون:

غالبًا ما يُطلق على هذه الفئة تسمية "المنتقمون"، بسبب الطابع الانتقامي الذي يميزهم عن غيرهم. إن مشاعر الانتقام وردود الفعل العاطفية هي التي تحرك سلوكهم، حيث تتوجه تصرفاتهم ضد أصحاب العمل والمنشآت التي كانوا يعملون بها. يدفعهم إلى ذلك الشعور بالظلم وسوء التقدير الذي عانوا منه في أماكن عملهم السابقة، مما يولد لديهم رغبة قوية في الانتقام من أصحاب العمل كرد فعل على ما يعتبرونه معاملة غير عادلة. هذه التصرفات هي تعبير عن إحباطاتهم العميقة وسعيهم لاستعادة كرامتهم والاعتراف بقيمتهم المهنية.[1]

يسعى هؤلاء الأفراد إلى إثبات مهاراتهم التقنية والفنية، ويهدفون إلى تحقيق مكاسب مادية أو سياسية دون أن يتباهوا أو يروجوا لأنشطتهم. بل على العكس، يعمدون إلى إخفاء وإنكار أفعالهم بشكل دقيق. ليس هناك فئة عمرية محددة تميزهم، وأغلب أنشطتهم تتم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة لتخريب الأنظمة المعلوماتية، أو إتلاف كامل أو جزء من البيانات أو المواقع المستهدفة على الإنترنت .

ورغم تصنيفهم ضمن الفئات الأقل خطورة بين مجرمي التقنية المعلوماتية، إلا أن هذا لا يمنع أن تؤدي بعض أنشطتهم إلى خسائر فادحة للمؤسسات التي يستهدفونها.[2]

القراصنة المتطرفين فكريا:

لعب التباين بين الشرق والغرب، والشمال والجنوب، وكذلك بين الاشتراكيين والرأسماليين، أو حتى بين الأديان والمذاهب المختلفة لنفس الدين، دورًا بارزًا في تسليط الضوء على هذه الطائفة. بمعنى أن كل طائفة تجد نفسها في خضم تأجيج الأفكار والآراء حول مواضيع الخلاف مع الطوائف الأخرى، مما يلفت الانتباه بعيدًا عن طبيعة هذه الخلافات، سواء كانت دينية أو سياسية أو اقتصادية. هذا التأجيج المستمر يسهم في تعزيز الهوية الخاصة بكل طائفة

[1] عمر يوسف عبد الله, المرجع السابق , ص209

[2] أيمن عبد الحفيظ , الاتجاهات الفقية لمواجهة الجرائم المعلوماتية, بدون ط , دار النهضة العربية , القاهرة , 2005, ص209

ويدفعها إلى الدفاع عن مواقفها، مما يجعل الصراعات والتباينات أكثر وضوحًا وتأثيرًا في المجتمع .

و يُعرف التطرف في هذا السياق بأنه مجموعة من الأنشطة التي تستغل شبكة الإنترنت لنشر وتوزيع واستقبال وإنشاء المواقع والخدمات التي تساهم في انتقال وترويج الأفكار المتطرفة. يتم ذلك من خلال المواد الفكرية التي تغذي التطرف الفكري، لا سيما تلك التي تشجع على العنف بغض النظر عن التيار أو الشخص أو الجماعة التي تتبنى أو تشجع أو تمول مثل هذه الأنشطة. تعتبر هذه الجهود المتطرفة خطيرة لأنها تهدف إلى توسيع دائرة انتشار هذه الأفكار عبر الإنترنت، مما يجعل من الصعب التحكم في تأثيرها على الأفراد والمجتمعات. يلجأ المتطرفون إلى استغلال مختلف المواقع الإلكترونية لتحقيق أغراضهم الدعائية، حيث يستخدمون حتى المواقع الإخبارية التي تتابع نشاطاتهم وتنشر بياناتهم وتصريحاتهم حول موضوعات متعددة تطرحها الجماعة، بما في ذلك الدعوة إلى التطرف الفكري بلغات أجنبية.

بالإضافة إلى ذلك، يعتمد المتطرفون على خدمات البريد الإلكتروني المجانية للتواصل مع أي مكان في العالم. وغالبًا ما يتم هذا الاتصال من خلال مقاهي الإنترنت والمكاتب العامة، وذلك لأن الحصول على بريد إلكتروني مجاني يتطلب فقط إدخال بعض البيانات الشخصية البسيطة، التي تكون غالبًا غير صحيحة.

تتجلى خصائص هذه الجماعة في أن المتطرف لا يسعى لتحقيق مكاسب شخصية أو مادية، بل يهدف إلى تغيير المجتمع ليوافق معتقداته وأفكاره التي يؤمن بصحتها. هذه السمات تبرز أن الهدف الرئيسي للمتطرف هو فرض رؤيته الخاصة على المجتمع، بغض النظر عن الوسائل المستخدمة لتحقيق ذلك[1].

[1] عمر يوسف عبد الله , المرجع السابق , ص210

القراصنة المتجسسين:

طائفة المتجسسين هي مجموعة من الأفراد الذين يسعون إلى التلاعب أو تخريب المحتويات الموجودة على الشبكة العنكبوتية. يشكل هؤلاء الأشخاص خطراً كبيراً، حيث يمكن أن تتضمن أنشطتهم إرسال أسرار العمل الخاصة بشركة ما عبر الإنترنت ومواقع التواصل الاجتماعي إلى الشركات المنافسة. يهدف المتجسسون في المقام الأول إلى الحصول على قاعدة بيانات معلوماتية عن الأعداء والأصدقاء على حد سواء، مما يتيح لهم ميزة تنافسية غير عادلة ويعرض سلامة وأمن البيانات للخطر. إنهم يتلاعبون بالمعلومات لتحقيق مكاسبهم الخاصة أو لتحقيق أهداف تلك الجهات التي يعملون لصالحها، مما يجعلهم مصدر تهديد حقيقي للأمن المعلوماتي.

القراصنة مخترقو الأنظمة:

يشمل هذا النوع القراصنة الذين يتبادلون المعلومات فيما بينهم بهدف اكتشاف نقاط الضعف في الأنظمة المعلوماتية التي يستهدفونها , و يعتمدون في ذلك على النشرات الإعلامية الإلكترونية كوسيلة أساسية لتبادل المعلومات و يقومون كذلك بعقد مؤتمرات دورية بهدف التشاور, تضم هذه المؤتمرات جميع مخترقي الأنظمة المعلوماتية. و ذلك بهدف التشاور حول آليات ووسائل الإختراق .[1]

[1] e3arabi.com , بتاريخ 2024/05/18 , 18:06

المبحث الثاني: خصائص جريمة القرصنة المعلوماتية و أسبابها.

بعدما تعرفنا في المبحث السابق على تعريف القرصنة المعلوماتية و أنواعها سنتطرق في المبحث الثاني إلى أهم خصائصها في المطلب الأول من هذا المبحث و أسباب ارتكابها في المطلب الثاني .

المطلب الأول: خصائص جريمة القرصنة المعلوماتية:

إن الطريقة أو الأسلوب المتبع لارتكاب الجريمة المعلوماتية يختلف تماما عن تلك الأساليب التي تتبع في ارتكاب الجرائم التقليدية كالقتل مثلا , فهي تمتاز بوجود خصائص تختلف بها عن باقي الجرائم, لكونها جرائم تتم عن طريق الحاسبات الاليات و عن طريق الشبكة المعلوماتية فهما الوسيلتان الأساسيتان لارتكاب الجريمة المعلوماتية بما فيها القرصنة [1] , و عليه يمكن تصنيف المميزات و الخصائص المتعلقة بجريمة القرصنة إلى :

_ خصائص جريمة القرصنة .

_ خصائص الجاني الإلكتروني (القرصان الإلكتروني)

أولا: خصائص القرصنة الإلكترونية :

تعد القرصنة الإلكترونية أحد أنواع الجريمة المعلوماتية و بذلك هي تحمل نفس الخصائص و المميزات الموجودة في هذه الأخيرة و هذا ماسنقوم بدراسته كما يلي :

جريمة القرصنة محلها شبكة الانترنت :

شبكة الانترنت , التي يطلق عليها أحيانا " الشبكة العالمية العنكبوتية " أو "الفضاء السيبراني", فهي ليست فقط مجرد وسيلة لتبادل المعلومات و الاتصال , بل هي بيئة مواتية لتنامي جرائم الانترنت . تعتبر هذه البيئة مكانا مثاليا لمرتكبي الجرائم المعلوماتية لأنها تسهل الوصول إلى

[1] لينا محمد الأسدي , مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة , ط01 , دار الجامد للنشر و التوزيع ,عمان الاردن , 2015 , ص24

مجموعة من الأشخاص سواء كانو طبيعيين أو معنويين سواء كانوا أفراد أو مؤسسات مالية أو صناعية , و تشمل الجريمة المعلوماتية بما فيها القرصنة مهاجمة الشبكات بواسطة الفيروسات أو القنابل الإلكترونية و التلاعب بالبيانات و التشويش و التفخيخ .

و مع ذلك , فإن هذه الأساليب الخبيثة أصبحت أدوات يستخدمها المجرمون لتحقيق أهدافهم غير القانونية بما في ذلك جرائم الاعتداء الجنسي و الاحتيال المالي و اختراق الأمن السيبراني(القرصنة).

جريمة القرصنة أداة ارتكابها الحاسب الآلي:

من المتعارف عليه في القانون الجنائي أنه في أي جريمة لابد من وجود سلاح لارتكابها و يسمى سلاح الجريمة , و تختلف الأسلحة من جريمة إلى أخرى حسب نوعها و في الجرائم التقنية "الحاسوب " هو الوسيلة التي تستعمل لارتكاب هذا النوع من الجرم , و تعد هذه الخاصية من أهم الميزات التي تميز الجريمة الالكترونية عن التقليدية . نظرا لأن الانترنت هي إحدى التقنيات الحديثة التي استحدثتها أنظمة الحوسبة و لذلك فإن ارتباطها بالحاسبات الآلية أمر لا مفر منه باعتباره الباب النافذ للشبكة المعلوماتية فهو أداة استخدام الانترنت .[1]

جريمة صعبة الإكتشاف و الإثبات:

جرائم الانترنت تمثل ظاهرة إجرامية فريدة من نوعها في العصر الحديث , حيث تشكل تحديا لمجتمعاتنا المتقدمة نظرا لحجم المخاطرالتي تنطوي عليها وخسائرها الهائلة . يعود السبب في هذه الظاهرة إلى طابعها الخاص الذي يميزها عن الجرائم التقليدية و الذي يتمثل في صعوبة اكتشافها و إثباتها فبينما تترك الجرائم التقليدية أثرا واضحا مثل الجثث أو الأدلة المادية

تكون جرائم الانترنت غالبا مستترة و مخفية حيث لا يلاحظها المجني عليه أو يعرف بوقوعها بسبب عدم ترك أي أثر خارجي ملموس بعد ارتكابها , مما يجعل من الصعب تحديد مرتكبها.

و يمكن تلخيص صعوبة اكتشافها و إثباتها في ما يلي:

[1] هروال هبة نبيلة , جرائم الانترنت دراسة مقارنة, أطروحة دكتوراه , جامعة أبي بكر بلقايد كلية الحقوق و العلوم السياسية , تلمسان , 2014, ص37, 38

1. صعوبة الإحتفاظ الفني بآثار الجريمة : و ذلك فقط إن وجدت , فالأدلة فيها الكترونية و غير ملموسة تنساب عبر الشبكات و أجهزة الحواسيب كما تنساب الكهرباء عبر الأسلاك.
2. إحجام المجني عليه عن الإبلاغ في مجتمع الأعمال : فغالبا ما يتم اكتشاف هذه الجرائم بصورة عرضية , حيث يظهر الدليل غير المرئي المشفر , كاستخدام المجرمين كلمات مرور أو ترميز العلامات بشكل لايمكن لا يمكن لهم من فك رموزه بسهولة مما يصعب على الشرطة تتبع المجرمين و التحقيق في هذا النوع من الجرائم . لافتقار معظم القائمين على جهاز العدالة إلى الخبرة الفنية في هذا المجال و هذا يخلق صعوبة كبيرة في التعامل مع الجريمة الالكترونية و مع وجود إمكانية تدمير الدليل الإلكتروني أثناء تجميعه أو جراء أي خطأ فني أثناء التحقيقات لذلك يستوجب وجود خبراء فنيين في سلك العدالة لمكافحة هذا النوع من الجريمة .

لذلك فإن تأسيس و إنشاء شرطة تختص في هذا النوع من الجرائم يعد أمرا ضروريا و حتميا , و يمكن حتى تسميتها بشرطة الانترنت . [1]

عالمية جريمة القرصنة :

بمعنى أنها لا تعترف بالحدود الجغرافية للدول و لا حتى بين القارات , لأنه مع الانتشار الواسع لشبكة الانترنت أمكن ربط أعداد ضخمة و هائلة لا حصر لها من الحواسيب و الهواتف الذكيو و كل جهاز آخر متصل بهذه الشبكة , حيث يمكن أن يكون الجاني في بلد و المجني عليه في بلد آخر , أو يكون كلاهما من قارتين مختلفتين , و لهذا السبب تقع الجرائم الإلكترونية بين حدود دول كثيرة [2] , و بالتالي يمكن لأي شخص ارتكاب جريمة عبر حاسبه الآلي موقعا بذلك أضرارا لشخص في دولة أخرى .[3]

[1] هروال هبة نبيلة , المرجع السابق , ص39 , 40
[2] عبد الصبور عبد القوي علي مصري , المحكمة الرقمية و الجريمة المعلوماتية ,ط 01 , مكتبة القانون و الاقتصاد ,الرياض , 2012 , ص50
[3] عبد الله عبد الكريم عبد الله , جرائم المعلوماتية و الانترنت , ط01 , منشورات الحلبي الحقوقية , بيروت , 2007 ,ص32

ثانيا : خصائص القرصان

لكي نستطيع فهم الجاني في الجرائم المعلوماتية و خصوصا القرصان الالكتروني لا بد أن يوضع في الحسبان شخصية المجرم و الذي يستوجب إعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا و بالتالي يمكن شرح هاتين النقطتين كالتالي:

تمتمع القرصان المعلوماتي بالذكاء :

بانتماء الجاني المعلوماتي من الناحية الوظيفية إلى التخصصات المتصلة بعلومه , يتمتع هذا النوع من الجناة بنظرة ليست بالتقليدية أو العادية على اعتبار أنه يوصف غالبا بدرجة عالية من الذكاء المعلوماتي و المهارة , تجعل من الصعب تصنيفه حسب التصنيفات المعتادة و التقليدية للإجرام لذلك يستعمل معيار محدد في تحديد أنواع الجناة المعلوماتيين و هو الهدف من ارتكابهم لهذه الجرائم .

القرصان الإلكتروني كإنسان اجتماعي:

الجاني في الجرائم الاكترونية إنسان متوافق مع المجتمع حيث أنه شديد الذكاء و ذلك يساعده على عملية التكيف مع هذا المجتمع و لكنه يقترف عذا النوع من الجرائم غالبا بدافغ اللهو أو مجرد استعراض لمهارات تحكمه في الحاسبات الآلية أو البرامج التي يتم تشغيلها بها .[1]

القرصان المعلوماتي مجرم عائد إلى الإجرام:

يتميز بعودة رجوعه لاقتراف الجريمة بهدف سد الفجوات و الثغرات التي كانت سبب فشله في أول تجربة و إعادة تصحيح ما أغفله سابقا مستفيدا بذلك من أخطائه السابقة من أجل تطوير قدراته الفنية و التقنية .

مجرم متخصص:

من خلال بعض القضايا السابقة تم اكتشاف و التوصل أن المجرمين المعلوماتيين متخصصين في الإجرام المعلوماتي دون غبره من الجرائم التقليدية .

[1] عبد الصبور عبد القوي علي مصري , المرجع السابق, ص52

القرصان المعلوماتي يبرر لجريمته:

يبرر ارتكاب جريمته بأنها أفعال مشروعة و أنها كانت بدافع التسلية و هو أمر عادي و لا يمكن تكييفه على أنه جريمة.[1]

فادحة الأضرار:

كثرة الاعتماد على الحاسبات الآلية في إدارة معظم الأعمال في كل المجالات أدى إلى مضاعفة الأضرار و الخسائر التي تخلفها الهجمات الإلكترونية على هذه الحاسبات , خصوصا إذا كانت تمثل قيما مالية , فالمؤسسات المالية و البنوك و معظم الشركات في وقتنا الحالي تعتمد على الحاسبات الالية في تسييرها , فالجرائم الماسة بالأنظمة الآلية لمعالجة المعطيات تفوق عدد الجرائم التقليدية .[2]

المطلب الثاني: أسباب جريمة القرصنة المعلوماتية :

كون القرصنة المعلوماتية جزءا من الجريمة المعلوماتية ككل فإن أسباب ارتكابهما لا تختلف عن بعض و تتعدد الأسباب التي يمكن حصرها , على عدة مستويات منها ماهو شخصي و منها ماهواجتماعي و منها ماهو كوني (عالمي) ... الخ و تختلف الأسباب كذلك وفق نوعها ونوع المستهدفين و نوع الجاني نفسه و فجرائم الهاوين تختلف عن المحترفين وتختلف كذلك وفق هدفها .

على المستوى الشخصي:

1) البحث عن الاهتمام و التقدير

هناك بعض الأشخاص من يرتكب الجرائم الإلكترونية من بينهم الشباب الطائشون و رغبة في التحدي و الظهور في وسائل الإعلام بحثا عن الشهرة و أغلبهم يتوقفون بعد بلوغ سن معين كالعشرينات .

[1] الحاج علي بدر الدين , القرصنة الرقمية كعائق تقني لنظام التقاضي المعلوماتي , مجلة البصائر للدراسات القانونية و الإقتصادية , المركز الجامعي مغنية الجزائر , العدد الخاص, 2021 , ص315

[2] محمد خليفة ,خصوصية الجريمة الإلكترونية و جهود المشرع الجزائري في مواجهتها , جامعة 08ماي1945 كلية الحقوق و الآداب الإجتماعية , قالمة , م 01 , ع01 , 09/15 / 2009, ص 376

2) كثرة الفرص :

توافرت فرص غير مسبوقة وفرتها الانترنت و التقنيات الحديثة لانتشار الجريمة السيبرانية ,كما ان الفرصة هي المنتجة للجريمة كما تلعب البيئة دورا كبيرا في ذلك و خاصة الخروج عن القواعد و الأساس الإجتماعي فمع عدم وجود رقابة تصاحبها عدم الامتثال للقواعد في أي وقت يزيد من احتمالية ارتكاب الجريمة المعلوماتية , فقد تشكل البيانات الآلية هدفا سهل المنال و يمكن أن يحقق منفعة شخصية و بالتالي فهي فرصة قليلة المخاطر و مربحة و احتمالية اكتشافها ضئيلة .[1]

3) عدم ضبط النفس :" تنطلق هذه الدراسة من النظرية العامة في السلوكات الطائشة و تؤكد ان احتمالية تورط و انضمام الأفراد إلى هذه الفعال الإجرامية تحدث بسبب كثرة الفرص مع توفر سمة شخصية من سمات الضبط النفسي المنخفض و قد عرف كل من هيرشي و جتفردسون السلوك الطائش بانه :" كل فعل يقوم على القوة و الخداع لتحقيق الرغبات الذاتية" , و بناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش أنه من خصائص الأشخاص , فهو يعد مظهرا من مظاهر الضبط النفسي المنخفض و كما في نظرية الضبط الإجتماعي لهيرشي فالدوافع لارتكاب هذا السلوك ليست متغيرة . و ذلك لأن كل فرد قد يندفع لتحقيق مصالحه الخاصة , فالسلوك الطائش يعد عملا سهلا و قد يحقق المصالح الخاصة بسرعة كالرشوة و السرقة ...

إن توفر صفة الضبط النفسي مع وجود فرصة لارتكاب السلوك الطائش يعدان عاملان مهمان في ارتكاب هذا السلوك الطائش .[2]

[1] ذياب موسى البداينة , الجرائم الإلكترونية المفهوم و الأسباب , ملتقى الجرائم المستحدثة في ظل التغيرات و التحولات الإقليمية و الدولية , كلية العلوم الاستراتيجية , عمان الاردن ,2014 , ص10

[2] عبد السلام محمد المايل و عادل محمد الشريجي وعلي قابوسة , الجريمة الإلكترونية في الفضاء الإلكتروني , مجلة آفاق للبحوث و الدراسات , م02 , ع02 , 2019/07/31 , ص249

4) الضغوط العامة :

ترجع نظرية الضغوط العامة الانحراف و خرق القانون إلى دوافع ناجمة عن قوى البناء الاجتماعي أو استجابات النفس الاجتماعية للحوادث و الظروف و التي تعمل كظغوطات أو مقلقات خاصة عندما تسد الطريق لتحقيق هدف ما.

5) النشاط الروتيني:

مع التقدم التكنولوجي الي نشهده حاليا فإننا نلاحظ تطورا كبيرا في حياتنا اليومية كذلك , حيث أصبحت وسائل التواصل الاجتماعي جزءا لا يتجزأ من روتيننا اليومي , هذا التحول الجذري في طريقة تعاملنا مع بعضنا البعض و كيفية إدارتنا لحياتنا اليومية أدى بدوره إلى تغيرات أخرى جذرية في عالم الجريمة .

بدأت حالات مثل القرصنة و الانتحال الالكتروني و غيرها من الجرائم تتزايد بشكل ملحوظ حيث يستغل المجرمون التقنيات و البرامج الحديثة للوصول إالى البيانات الشخصية و كذلك تلك التي تتعلق بالأموال و الشركات و غيرها ...

إن تحليل مختلف الجرائم الاكترونية يستوجب النظر إلى الدافع و الفرصة و البيئة , فعندما برى المجرم أن سيحقق ربحا من ارتكابه الجريمة مع سهولة وصوله إلى هدفه دون خطر الكشف أو الملاحقة تتزايد رغبته في ارتكابها .

لذلك و لمواجهة هذا النوع من التحديات يستوجب علينا التفكير الشامل بتطوير استراتيجيات الأمن السيبراني و تعزيز التوعية بأهمية الحماية الششخصية للمعطيات على شبكة الانترنت , بالإضافة إلى الحث على تكاثف الجهود الدولية للحث على الحرص على عدم تأثيرها الكبير على حياتنا اليومية. [1]

6) الرغبة في الانتقام:

[1] اسراء جبريل رشاد مرعي , الجرائم الإلكترونية "الأسباب الأهداف طرق الجريمة و معالجتها" , مجلة الدراسات الإعلامية , المركز الديموقراطي العربي , ع01 , يناير 2018, ص434

يعد الانتقام من بين الدوافع لارتكاب الجرائم بصفة عامة سواء كانت تقليدية أو حديثة كالقرصنة الاكترونية فتصفية الحسابات مع الخصوم يؤدي إلى القيام بتصرفات و أعمال غير مشروعة من شأنها الإضرار بالخصوم , ففي الجرائم التقليدية يقوم المجرمون بالترصد لضحاياهم و القيام بالإعتداء عليهم , أو حتى خطفهم انتقاما من عائلاتهم التي قامو بأشياء ضدهم أو انتقاما منهم بحد ذاتهم و هو نفس الشيء الذي يقام عن طريق وسائل التكنولوجيا الحديثة [1] من طرف أشخاص يملكون معلومات عن خصومهم و التي في الغالب تكون مؤسسات تعامل الجاني معها سواء تم فصله منها أو وقع خصام بينهما , و تتعدد الاسباب في هذا الشأن فيقوم هذا الجاني باستغلال المعلومات التي تحصل عليها أثناء تعامله مع هذه المؤسسة كاستعمال كلمة المرور الخاصة بالشبكة و الولوج إليها و تحقيق مراده بالإنتقام.[2]

على المستوى الإجتماعي:

1) التحضر:

عموما يعتبر التحضر من أهم الأسباب التي تساهم في زيادة الجريمة المعلوماتية , خصوصا لانتشار ظاهر النزوح الريفي بكثرة و أغلب الشباب المهاجرين غير مستعدين للصعوبات الاقتصادية التي من الممكن أن تعترضهم في الحياة الحضرية التي انتقلو لها , كتكاليف المعيشة من طعام و شراب و مسكن و مصاريف اخرى ... مما يشكل مجموعة كبيرة منهم غير قادرة على تحمل كل هذه التكاليف , و نتيجة لكل هذه الظروف يجدون أنفسهم في وضع لا يستطيعون التعايش معه , مما قد يدفع بفئة منهم إللى اللجوء للجريمة الإلكترونية كوسيلة لسد حاجياتهم كونها لا تتطلب رؤوس أموال كبيرة و تكون مربحة في نفس الوقت و كما يرى ميك فإن التحضر سبب رئيسي للجرائم الإلكترونية و خاصة في

[1] عميمر عبد القادر , المرجع السابق , ص 50
[2] غادة النصار, الإرهاب و الجريمة الإلكترونية , بدون ط , دار العربي للطبع و النشر , القاهرة , مصر , 2017, ص54

نيجيريا حيث يصبح الاستثمار فيها فرصة مغرية بالنسبة للأفراد في ظل غياب فرص العمل و ظروف الحياة الصعبة .[1]

2) تحقيق مكاسب مادية (الثروة):

تعد الرغبة في تحقيق المكاسب المادية من أبرز الدوافع لارتكاب الجريمة المعلوماتية , و أصحاب هذه الرغبة من المجرمين الذين يمتلكون قدرا عاليا من المهارة و هم الراكرز بصفة كبيرة , فهم على علم كبير بتكنولوجيا الإعلام و الإتصال التي يستخدمونها في صرصنة الأنظمة و الشبكات الخاصة بالشركات و البنوك العالمية و غيرها من الهيئات التي تمتلك معطيات تود استرجاعها من هؤلاء القراصنة بعد المساومة عليها , أو التحويل المباشر للأموال عن طريق استغلال ثغرات موجودة في هذه الأنظمة , أو عن طريق تعطيل الخدمة عن بعض المؤسسات و مطالبتها بمبالغ مالية مقابل إعادتها لهم و هي أكثر الطرق شيوعا. [2]

3) البطالة :

و كذلك من الدوافع الإجتماعية البطالة شأنها شأن الجريمة التقليدية و الظروف الإقتصادية الصعبة و تتركز البطالة بين قطاعات كبيرة بين الشباب , و لذلك هناك الفئة من الشباب التي تملك المعرفة و يعانون م البطالة فيلجؤون الأنشطة الإجرامية الإلكترونية .

4) الضغوطات الإجتماعية :

تعد كل من الفقر و البطالة و الأمية و الظروف الإقتصادية الصعبة عوامل ضاغطة على المجتمع و بشكل خاص الشباب مما يولد مشاعر سلبية عند العديد من الناس ضد الظروف و ضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها التجارة الإلكترونية بأعضاء البشر .

[1] ذياب موسى البداينة , المرجع السابق , ص14

[2] أحمد خليفة الملط , الجرائم المعلوماتية ,ط02 , دار الفكر الجامعي , الإسكندرية , مصر , 2006, ص 89

على المستوى العقائدي:

من أقوى الدوافع التي تحرك الأفراد هو عقيدتهم حيث أن الإنسان مستعد للتضحية بكل ما لديه من أجل معتقداته الخاصة و يستغل القراصنة هذا النوع لتبريربعض محاولاتهم لاختراق أجهزة الآخرين مدعومة بتفسيرات ملتوية و بحجج كانتماء الأجهزة التي اخترقوها إلى طائفة دينية معادية لهم , مبررين ذلك بتكفيرها أو بنية الكشف عن عن أسرارها لتشويه سمعتها و التشهير بها , و يمكن لهذه السلوكات أن تهدد السلم الإجتماعي و المعلوماتي و يعرضهم للخطر .

على المستوى الإيديولوجي و السياسي:

في العصر الحالي، تعتبر الدوافع السياسية والإيديولوجية من أبرز العوامل التي تدفع ببعض المنظمات إلى ارتكاب أعمال إجرامية ضد معارضيها. يتم ذلك عبر استخدام شبكات المعلومات للتشهير بهم ونشر أفكارها وآرائها.

فالإرهاب في العصر الحديث يتميز بتوظيف شبكة الإنترنت كأداة رئيسية لنقل الأفكار والتنسيق بين الأفراد، مما يعكس تكامله مع التكنولوجيا الحديثة.الإرهاب الإلكتروني يعتمد على استخدام التكنولوجيا والوسائل الإلكترونية لتنفيذ أعماله، ويستهدف هذا النوع من الإرهاب بنية التحتية المعلوماتية والأنظمة الإلكترونية، مثل أنظمة القيادة والاتصالات والشبكات المصرفية والمرافق الحيوية.

وبالتالي، فإن خطورة الإرهاب الإلكتروني تتزايد في الدول المتقدمة التي تعتمد بشكل كبير على الحواسيب والشبكات المعلوماتية في بنيتها التحتية، مما يجعلها أهدافًا سهلة للهجمات.

بدلاً من استخدام التفجيرات التقليدية، يمكن للجماعات الإرهابية تنفيذ أعمال تخريبية من خلال الهجمات الإلكترونية، مثل تعطيل خدمات الاتصالات أو تعطيل أنظمة الدفاع أو حتى شل البنية التحتية للطاقة والموارد. هذا يبرز التطور المستمر للتهديدات الأمنية والحاجة الملحة لتعزيز الأمن السيبراني والتصدي للتهديدات الإلكترونية المتطورة[1].

[1] بن مالك اسمهان, خصائص الجريمة المعلوماتية و أسباب ارتكابها , مجلة البيبان للدراسات القانونية و السياسية , كلية الحقوق و العلوم السياسية سطيف, م04 ,ع 01 , 2019/06/15 , ص118

على المستوى الكوني:

1) التحول للمجتمع الرقمي :

هناك ثلاث سمات مهمة في عصر المعلومات و هي : تغيرات كمية في نوعية المعلومات و دقتها كمثال على ذلك نجد في المواصلات و أجهزة الإتصال عددا كبيرا من الصور تختلف حسب دقتها و عددها من جهاز إلى آخر, إرسال عدد هائل من المعلومات إلى عدة أماكن و في نفس الوقت فالمعلومات توجه الصواريخ و الصحفي يرسل التقرير و البث المباشر من مكان الحدث, وجود الشبكات و اهمها شبكة الانترنت ففيها تتم أغلب المعاملات من اتصالات و رسائل .

دخلنا عصر المعلوماتية الجديد، حيث يمضي الناس جزءًا من حياتهم اليومية في الفضاء الإلكتروني، حيث ينشئون الشبكات والمواقع ويستمتعون بأنواع جديدة من العلاقات الاجتماعية، ويكونون على اطلاع بما يحدث في العالم الخارجي ويقومون ببعض الأعمال. تلك الأنشطة جعلت من الممكن للجميع المشاركة بوجود جهاز كمبيوتر أو مودم وبمعرفة تقنية بسيطة.

بعبارة أخرى، فإن شبكة الإنترنت هي التي خلقت ما يُعرف الآن بالفضاء الإلكتروني أو العالم الافتراضي. يحتاج المجتمع لضمان أمن وسلامة العمليات في هذا العالم الجديد، بما في ذلك النظام والاستمرارية، وذلك لأن توفير الأمن والسلامة لم يعد مقتصرًا على العالم المادي فحسب، بل امتد ليشمل العالم الافتراضي أيضًا .[1].

2) العولمة :

" عندما نتحدث عن الفضاء الإلكتروني، نجد أنه يُعَدّ مجالاً جديداً يختلف عن الأنظمة التقليدية للكمبيوتر. هناك فرص مباشرة للجريمة تنشأ مع تطور التكنولوجيا، فالأشخاص قد يظهرون سلوكيات مختلفة في الفضاء الإلكتروني مقارنة بالواقع، قد يقترفون أفعالاً غير

[1] ذياب موسى البداينة, المرجع السابق, ص16

قانونية بسبب الإختلافات في البيئة والهوية. هذه المرونة في تغيير الهوية وضعف عوامل الردع يمكن أن تحفز السلوك الإجرامي في هذا العالم الافتراضي، كما أشارت إليه الأمم المتحدة في عام 2013[1]".

على مستوى الخصائص:

الإزالة: ليست دائمًا هناك حاجة لإزالة المعلومات في الجرائم الإلكترونية، فقد يكفي نسخها.

التوافر: المعلومات متاحة في كل مكان، مما يجعلها عرضة للجريمة.القيمة: تشمل المعلومات قيمة مثل بيانات بطاقات الائتمان ومعلومات المصرفية.

المتعة: بعض الجرائم الإلكترونية، مثل سرقة الموسيقى والأموال، يمكن أن تكون ممتعة للمرتكبين.

الديمومة: المعدات والبرامج المسروقة قد تستخدم لفترة طويلة.سرعة التنفيذ: الجرائم الإلكترونية يمكن أن تنفذ بسرعة، ولكن ليست دائمًا بدون استعداد مسبق.

بالإضافة كذلك إلى سرعة تنفيذها و جاذبيتها و ميزتها أنها عن بعد كل هذه الخصائص تعد من أهم أسباب ارتكاب الجريمة المعلوماتية من بينها القرصنة.

[1] ذياب موسى البداينة , المرجع السابق , ص17

خلاصة الفصل الأول:

كخلاصة لهذا الفصل نلاحظ أن القرصنة الإلكترونية من أخطر الجرائم المعلوماتية , و لذلك كان لا بد من التطرق في المبحث الأول إلى مفهوم القرصنة الإلكترونية حيث وجدنا أنها تعرف بالإستخدام الغير قانوني لأجهزة الحاسب الآلي للوصول إلى أنظمتها أو الشبكات الإلكترونية و برامجها لتحقيق أهداف خاصة ووجدنا أنها تنقسم إلى عدة أنواع تتمثل في: سرقة البيانات , التجسس و الإحتيال الإلكرتوني , و في المبحث الثاني تطرقنا إلى الخصائص و الأسباب التي تحرض على ارتكابها و من بين هذه الخصائص التي تعرضنا لها في المطلب الأول أنها جريمة محلها شبكة الأنترنت , و يستعمل الحاسب الآلي في ارتكابها , و أنها صعبة الإكتشاف و عابرة للحدود الدولية , كما أن مرتكبها يعرف بما يسمى المخترق أو الهكرز أو الكراكر حيث يتمتعون بالذكاء و المهارة العالية في استخدام أجهزة الكمبيوتر .

أما بالنسبة للمطلب الثاني فقد خصصته للدوافع التي تؤدي إلى ارتكاب هذه الجريمة و هي : البحث عن الاهتمام و التقدير , عدم ضبط النفس سهولة ارتكابها , الضغوطات الإقتصادية و الاجتماعية المحيطة بمرتكبها , الرغبة في تحقيق الشهرة , الإنتقام و غيرها من الأسباب الأخرى.

الفصل

الثاني

تمهيد :

بعدما تطرقت إلى ماهية القرصنة الإلكترونية في الفصل الأول من خلال تعريفها و ذكر أنواعها و أسباب ارتكابها و خصائصها , سأتطرق في الفصل الثاني إلى أهم الإجراءات التي اتخذها المشرع الجزائري للتصدي لها و ذل من خلال المبحثين الآتين :

1_ المبحث الأول: الحماية الموضوعية للأنظمة المعلوماتية من القرصنة .

2_ المبحث الثاني: الحماية الإجرائية للأنظمة المعلوماتية من القرصنة.

المبحث الأول: الحماية الموضوعية للأنظمة المعلوماتية من القرصنة .

بما أن المعلومات أصبحت تُعتبر ثروة اقتصادية كبيرة، صار من الضروري توفير حماية جنائية خاصة لها. لقد أصبحت المعلومات ذات قيمة مالية، مما يضعها ضمن الأصول الاقتصادية. كما يمكن أن تكون المعلومات شخصية، وإفشاؤها قد يهدد الخصوصية بطرق متعددة . ومع التطور السريع في التكنولوجيا وتقنيات المعلومات، اكتشفت الدراسات الجنائية أن القوانين التقليدية لم تعد كافية للتعامل مع الجرائم الجديدة التي نتجت عن هذا التطور الهائل في نظم معالجة المعلومات ونقلها عبر الشبكات. لذلك، أصبح من الضروري وضع قوانين جديدة لمواجهة هذه الجرائم وضمان حماية المعلومات بفعالية[1].

المطلب الأول : أركان جريمة القرصنة المعلوماتية :

الركن المادي:

يتألف الركن المادي في الجرائم التقليدية من 3 عناصر أساسية و هي السلوك الإجرامي , النتيجة الضارة و العلاقة السببية بينهما . و في الجرائم الإلكترونية نجد أن الركن المادي يتألف من نفس العناصر و هي السلوك الإجرامي و النتيجة و العلاقة السببية بينهما , و مع ذلك يمكن تحقيق الركن المادي للجريمة المعلوماتية دون وقوع النتيجة النهائية , على سبيل المثال إذا قام شخص ما بإنشاء موقع إلكتروني بهدف التشهير بشخص آخر و لكن لم يتم نشر الموقع على الانترنت بعد , فإن الفعل نفسه يستوفي متطلبات الركن المادي , و من ثم يستحق مرتكبه العقاب , بمعنى آخر , حتى و لو لم تتحقق النتيجة النهائية الضارة بعد فإن مجرد الشروع في الفعل الإجرامي يمكن أن يكون كافيا لاعتبار أن الجريمة وقعت و بالتالي يصبح الجاني مستحقا للمسائلة القانونية .[2]

[1] رضاع فتيحة , المرجع السابق , ص88

[2] أحسن بوسقيعة , الوجيز في القانون الجزائي العام ,ط10, دار هومة الجزائر , 2011 , ص27

تتميز الجرائم الإلكترونية بوجود حاسب آلي و شبكة الانترنت حيث لا يمكننا تخيل وجود جريمة معلوماتبة دون وجود شبكة أو جهاز كمبيوتر أو حتى الهواتف الذكية , يعتبر استخدام هذه الوسائل أمرا طبيعيا في حياتنا اليومية , إلا أن الاختلاف يظهر عندما تستخدم هذه الوسائل لأغراض غير قانونية لهذا السبب تعد الوسيلة الإلكترونية عاملا اساسيا في تشكيل السلوك الإجرامي في الجرائم المعلوماتية, تعتمد هذه الجرائم بشكل اساسي على استغلال التكنولوجيا لتحقيق اهداف غير مشروعة مما يجعل فهم و استخدام التقنيات الحديثة جزءا لا يتجزأ من ارتكاب الجرائم الإلكترونية . و هذا النوع من الجرائم يتطلب تطوير آليات و تقنيات جديدة لمكافحة هذا النوع من الجرائم و حماية المعلومات و الشبكات من أي تهديد محتمل. [1]

و بما أن هذه الجريمة تعتمد على على سلوك إجرامي يتخذ أحد الشكلين إما الخول أو البقاء الغير مصرح بهما , و يمكن فهم الدخول غير المصرح به بأنه الوصول إلى المعلومات و البيانات المخزنة داخل نظام الحاسب الآلي دون موافقة المسؤول عن النظام . بعض التعريفات تشير إلى أن هذا النوع من الدخول يمثل إساءة لاستخدام الحاسب الآلي و نظامه من قبل شخص غير مخول له باستخدامه و يتم ذلك بهدف الوصول و الدخول إلى المعلومات المخزنة في الداخل سواء كان بدافع الاطلاع عليها او التسلية أو لإشباع شعور النجاح في اختراق النظام. [2]

الركن المعنوي:

ذكر في نص المادة 394 مكرر من قانون العقوبات الجزائري بوضوح أن جريمة الدخول أو البقاء الغير مصرح بهما يجب ان تكون جريمة عمدية , يمكن استنتاج هذا الأمر من الشرط الذي يقول " كل من يبقى أو يدخل عن طريق الغش " . هذا يعني أن الفعل لا يعتبر جريمة إلا إذا تم ارتكابه بنية مسبقة للغش أو التحايل . يتطلب القانون هنا أن يكون لدى الجاني قصد جنائي واضح و محدد عند دخوله أو بقائه في المكان بشكل غير قانوني , مما يعني أن التواجدغير المصرح به يجب أن يكون ناتجا عن نية متعمدة للتحايل على القوانين و اللوائح المتصلة بهذا

[1] الحسيناوي علي جبار , جرائم الحاسوب و الانترنت , بدون ط , دار الباروزي للنشر و التوزيع , عمان , الاردن , ص31
[2] محمد خليفة , خصوصية الجريمة الالكترونية و جهود المشرع الجزائري في مواجهتها , دراسات و ابحاث , جامعة 8ماي 1945 كلية الحقوق و الاداب و العلوم الاجتماعية قالمة , م 01 ,ع01 , 09/15/ 2009 , ص379

الشأن .هذه الدقة في تحديد النية تؤكد على أهمية التمييز بين الأفعال غير المقصودة و بين تلك التي تتم بوعي كامل و رغبة في خرق القانون .

و لكن في الحقيقة المنطق يفرض أن تكون جريمة القرصنة أو الدخول أو البقاء في أنظمة الحواسيب جريمة عمدية , فعمليات الدخول إلى هذه الأنظمة و البقاء فيها تحدث بشكل مذهل و متكرر يوميا من قبل عدد كبير من الأشخاص خاصة مع الارتفاع الكبير لأعداد مستخدمي شبكة الانترنت و في ظل هذا النشاط الكبير و الدائم يمكن أن تحدث حالات دخول أو بقاء غير مصرح به دون أن تكون نية الغش و التحايل موجودة . لهذا السبب من الضروري أن تكون هذه الجريمة عمدية , حتى لا يعاقب أشخاص يدخلون دون قصد إجرامي .

هذا الشرط يساعد على التوازن بين حماية خصوصية الأنظمة المعلوماتية من جهة و ضمان حرية الأفراد من جهة اخرى و لذلك وجب التمييز بين الأفعال العمدية التي يقصد أصحابها انتهاك القوانين أو التحايل عليها , و بين الأخطاء غير المقصودة التي قد تحدث نتيجة سوء الفهم أو قلة الخبرة . بهذا الشكل يمكن الحفاظ على نظام قانوني عادل لا يعاقب سوى من لديه نية واضحة لارتكاب الجريمة.

و فيما يتعلق بالظروف المتشددة المرتبطة بهذه الجريمة . أو النتائج المترتبة عنها , فيجب أن تكون تلك الظروف غير مقصودة و السبب في ذلك هو أنه اذا كانت مقصودة فسيؤدي ذلك إلى نشوء جريمة جديدة تماما و هي جريمة التلاعب بالمعطيات .[1]

[1] محمد خليفة , المرجع السابق, ص378

الركن الشرعي:

يشير الركن الشرعي للجريمة إلى ضرورة وجود نص قانوني يجرّم الفعل ويحدد العقوبة المناسبة له. فلا يمكن اعتبار أي فعل جرماً إلا إذا كان هناك نص قانوني واضح يصفه كجريمة ويضع عقوبة محددة له. هذا يعني أنه بدون نص قانوني لا يمكن تحميل أي شخص مسؤولية جنائية أو تطبيق أي تدابير أمنية بحقه.

الجريمة هي نتيجة الأفعال المادية التي يقوم بها الإنسان، وهذه الأفعال تتنوع وفقاً لنشاطات الأفراد المختلفة. لذلك، تدخل المشرع لتجريم بعض الأفعال التي تُعتبر ضارة بالمجتمع، وذلك من خلال وضع قوانين تحدد بوضوح الأفعال المحظورة والعقوبات المترتبة عليها.

على سبيل المثال، القانون رقم 15-261 الذي ينص على تشكيل وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. هذا القانون يهدف إلى حماية المجتمع من الجرائم الإلكترونية التي تتزايد مع تقدم التكنولوجيا، من خلال وضع إطار قانوني يعاقب على هذه الأفعال ويوفر وسائل لمكافحتها بفعالية .
وهذا ما دفع المشرعين إلى التدخل لتجريم هذه الأفعال الضارة من خلال وضع نصوص قانونية تحدد ماهية الفعل الضار وتفرض العقوبات المناسبة لارتكابه. فيما يخص الجرائم المعلوماتية، سعت معظم التشريعات إلى تنظيم قوانين ومعاهدات تهدف إلى حماية الحقوق الشخصية للأفراد ومكافحة الجريمة المعلوماتية على الصعيدين الدولي والمحلي. من أبرز المعاهدات الدولية التي تناولت مكافحة الجرائم المعلوماتية، نجد الاتفاقية الدولية حول الجرائم المعلوماتية المنعقدة في بودابست في 23 نوفمبر 2001، بالإضافة إلى جهود منظمة التعاون الاقتصادي والتنمية وغيرها من القوانين والمعاهدات التي اهتمت بهذه الظاهرة[1].

[1] دحو نجاة و أولاد علي فاطمة , جريمة القرصنة الإلكترونية في التشريع الجزائري , مذكرة ماستر تخصص قانون جنائي جامعة غرداية , كلية الحقوق و العلوم و السياسية , 2022 , ص 37

أما على المستوى الوطني، فقد اتخذ المشرع الجزائري خطوات جادة في التصدي للجرائم المعلوماتية من الناحيتين الموضوعية والإجرائية. من الناحية الموضوعية، جاء قانون العقوبات الجزائري المعدل ليشمل الجرائم المعلوماتية، حيث تم إدراجها في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات". هذا القانون يمثل وسيلة ردعية تهدف إلى منع ارتكاب الجرائم بشكل عام .

ومن الناحية الإجرائية، نجد أن قانون الإجراءات الجزائية الجزائري تطرق إلى وسائل اعتراض المراسلات وتسجيل الأصوات والصور، وذلك في المواد من 65 مكرر إلى 505 مكرر 10، بالإضافة إلى العديد من التعديلات الأخرى التي تتعلق بالجرائم المعلوماتية. على سبيل المثال، قانون رقم 09-04 جاء بعدة وسائل لمحاولة مكافحة الجرائم المعلوماتية، من بينها تفتيش المنظومة المعلوماتية، إلى جانب قانون رقم 2000/03[1].

الهدف من جميع هذه الجهود، سواء على المستوى الدولي أو الوطني، هو حصر مصادر التجريم والعقاب ضمن إطار قانوني واضح ودقيق. يسعى المشرعون إلى التأكد من أن كل فعل ضار يمكن تصنيفه كجريمة يتم تغطيته بنصوص قانونية محددة، وذلك لتجنب الوقوع في حالة يتم فيها ارتكاب جرائم جديدة ذات أضرار جسيمة دون وجود قوانين تجرمها بشكل صريح.

هذه العملية تضمن أن المشرعين يكونون على دراية بالتطورات الاجتماعية والتكنولوجية التي قد تخلق أنواعاً جديدة من الجرائم. فمع التقدم التكنولوجي المستمر، تظهر تهديدات جديدة مثل الجرائم الإلكترونية التي تتطلب تدخلات تشريعية فورية لتجريمها وتحديد العقوبات المناسبة لها .

[1] دحو نجاة و أولاد حمو فاطمة , المرجع السابق , ص38

على سبيل المثال، قوانين مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تأتي كاستجابة ضرورية للتطورات في هذا المجال. فبدون هذه النصوص القانونية، قد يجد المشرعون أنفسهم في موقف صعب حيث تكون هناك أفعال ضارة ولكن لا يمكن معاقبتها بسبب غياب النص القانوني المناسب.

من هنا، نجد أن جهود حصر التجريم والعقاب تسهم في تحقيق العدالة والحفاظ على النظام العام، حيث يتم توفير الأطر القانونية اللازمة لمواجهة أي نوع من الجرائم الجديدة والتعامل معها بفعالية. هذه العملية تعزز ثقة المواطنين في النظام القانوني وتضمن أن كل فرد يعرف حقوقه وواجباته وحدود الأفعال المسموح بها[1].

المطلب الثاني: العقوبات المقررة لجريمة القرصنة المعلوماتية في التشريع الجزائري :

أكدت اتفاقية بودابست في المادة 13 منها على ضرورة اتخاذ الدول التدابير الازمة و الفعالة لضمان أن الجرائم المنصوص عليها في الاتفاقية تعاقب بعقوبات مناسبة . و تؤكد المادة كذلك على أهمية أن تكون هذه العقوبات و تدابير المسائلة ملائمة لطبيعة الجرائم المرتكبة , بما في ذلك تقييد الحريات و توقيع العقوبات المالية على الأشخاص الاعتباريين و تشدد الاتفاقية على ضرورة أن تكون التدابير الجنائية المتخذة رادعة و فعالة بما يكفي لتحقيق العدالة و منع تكرار هذه الجرائم و ضمان التزام الدول بمكافحتها.

و قد نص المشرع الجزائري على العقوبات الخاصة بجريمة القرصنة الالكترونية و الجريمة المعلومايتة بصفة عامة بعقويات أصلية و أخرى تكميلية :

العقوبات الأصلية :

في سياق دراستنا للأنظمة المعلوماتية لاحظنا وجود حاجة ماسة لتسليط الضوء على على

[1] دحو نجاة و أولاد حمو فاطمة , المرجع السابق , ص39

العقوبات الماسة بالجرائم المعلوماتية و يعود السبب في ذلك أن العقوبات في هذه الجرائم تكون اشد بكثير من العقوبات على الجرائم التقليدية .

1/عقوبة الأشخاص الطبيعية :

يعاقب كل من يدخل أو يبقى عن طريق الغش في كل جزء من المنظومة المعلوماتية أو يحاول ذلك بالحبس من من ثلاث أشهر إلى سنة واحدة و بغرامة من 50000 إلى 100000 دج , و تضاعف العقوبة إذا ترتب عن ذلك تغيير للمعطيات أو حذفها.

و إذا ترتب عن هذا الدخول و التخريب و التغيير تخريب لنظام التشغيل الخاص بالمنظومة المعلوماتية تكون العقوبة الحبس من 6 أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج .[1]

وتكون العقوبة بالحبس من 6 أشهر إلى 3 سنوات و بغرامة من 500000 إلى 2000000 دج على كل شخص قام بإدخال معطيات في نظم المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها .[2]

2/ عقوبة الأشخاص المعنوية :

هناك شروط يجب توفرها لقيام الجريمة التي يرتكبها الشخص العنوي و ذلك حسب المادة 51 مكرر من قانون العقوبات و هي ثلاثة :

<u>أن ترتكب إحدى الجرائم المنصوص عليها حصرا:</u>

بالنظر إلى المادة 51 مكرر من قانون العقوبات الجزائري، نجد أن المشرع قد قيد مسؤولية الشخص المعنوي جنائياً بنطاق محدد من الجرائم. تتضمن هذه الجرائم تلك التي نص عليها قانون العقوبات على وجه الحصر، وذلك احتراماً لمبدأ شرعية الجرائم والعقوبات. يتطلب هذا المبدأ أن يشير النص الجنائي بشكل صريح إلى إمكانية محاسبة الشخص المعنوي.

[1] المادة 394 مكرر , قانون العقوبات الجزائري
[2] المادة 394مكرر 1, قانون العقوبات الجزائري

غالباً ما تتعلق الجرائم التي يمكن أن يسأل عنها الشخص المعنوي بالاعتداء على الأملاك وجرائم الأعمال. وعليه، فإن الشخص المعنوي لا يمكن مساءلته جنائياً في حال ارتكاب أحد أعضائه أو ممثليه جرائم لم ينص القانون على إمكانية مسائلته عنها. من الأمثلة على هذه الجرائم التي لا تُسأل عنها الأشخاص المعنوية هي الجرائم الماسة بالآداب العامة، نشر الأخبار الكاذبة، والإهانة، والسب والقذف. لذا، تظل المسؤولية الجنائية للشخص المعنوي في إطار الجرائم المحددة بوضوح في القانون، مما يعزز مبدأ الشرعية القانونية.

أن يتم ارتكاب الجريمة بواسطة شخص تابع للشخص المعنوي أو ممثله :

اختار المشرع الجزائري، بموجب المادة 51 مكرر في فقرتها الأولى، تحديد المسؤولية القانونية للشخص المعنوي من خلال أفعال الأشخاص الطبيعيين المرتبطين به قانوناً. وبموجب هذا النص، فإن مسؤولية الشخص المعنوي لا تتحقق إلا عبر الأفراد الذين يُحددهم القانون بشكل صريح. هؤلاء الأفراد، الذين يُشار إليهم عادةً بأجهزة الشخص المعنوي، يلعبون دوراً حاسماً في المؤسسة نظرًا للمناصب الحيوية التي يشغلونها، والتي تمنحهم صلاحيات إدارة شؤون المؤسسة والتصرف والتعاقد باسمها ولحسابها. تعتمد استمرارية المؤسسة على إرادة هؤلاء الأشخاص الذين قد يكونون شركاء أو أعضاء مجلس الإدارة أو الجمعية العامة.

وفي هذا السياق، يجب أن تكون الجريمة المرتكبة من قبل شخص يملك سلطة اتخاذ القرارات داخل الشخص المعنوي حتى يتحمل الأخير المسؤولية القانونية. وبالتالي، لا يمكن محاسبة الشخص المعنوي عن الأفعال الإجرامية التي يرتكبها أشخاص لا يمتلكون هذه الصفة أو السلطة، حتى لو كانت تلك الأفعال محددة قانوناً كجرائم[1].

أن ترتكب الجريمة لفائدة الشخص المعنوي:

نصت المادة 51 مكرر/1 بوضوح على هذا الشرط، وينتج عن هذا الشرط بمفهوم المخالفة عدم مساءلة الشخص المعنوي عن الجريمة التي يرتكبها ممثله إذا قام بها لحسابه الشخصي أو

[1] مزاولي محمد , المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري , محاضرا من كلية الحقوق و العلوم السياسية جامعة بشار , بدون سنة , ص276

لحساب شخص آخر، أو إذا تسببت في ضرر بمصالح الشخص المعنوي. في هذه الحالة، يؤاخذ الشخص الطبيعي عن الجريمة، استنادًا إلى جريمة التعسف في استعمال السلطة أو الإفلاس.
وفي جميع الأحوال، تُعد هذه المسألة ضمن السلطة التقديرية للقاضي الذي يقيم ويميز بين المصالح المختلفة لتحديد أيهما كان له الغلبة في نفس ممثل الشخص المعنوي.

وتشير عبارة "الحساب الشخصي" الواردة في المادة 51 مكرر/1 من قانون العقوبات إلى المنافع والأرباح أو المصالح التي يمكن أن يجنيها الشخص المعنوي من وراء ارتكاب الجريمة.
وليس من الضروري أن يجني الشخص المعنوي فائدة مادية من الجريمة؛ بل يكفي أن يكون الفعل المكون للجريمة قد وقع بمناسبة ممارسة ممثله لوظيفته، على أمل تحقيق هذا الهدف، سواء كان هذا الهدف مادياً أو معنويا.
تبرز أهمية تحميل المسؤولية مباشرة للشخص المعنوي في تسهيل عملية الادعاء، حيث لا يحتاج المدعي إلى إثبات مسؤولية الفرد الطبيعي. يكفي عدم الامتثال للواجبات القانونية أو اللوائح لقيام المسؤولية، مع مراعاة طبيعة الجرائم المرتكبة.

وتقتصر مسؤولية المسير على الحالات التي يثبت فيها ارتكابه لخطأ شخصي أو إهمال. ووفقًا للمادة 51 مكرر / 1 من قانون العقوبات، تتطلب المسؤولية الجنائية للشخص المعنوي ارتكاب خطأ من قبل أجهزته أو أعضائه الممثلين. ولتحديد المسؤولية، يجب التحقق من هوية الشخص الذي ارتكب الجريمة. هذا المبدأ يوضح أن المسؤولية الجنائية للشخص المعنوي محدودة بمدى أفعال ممثليه أو أعضائه، ولا تُحمّل لكل من ينتمي إلى أجهزة الشخص المعنوي. على سبيل المثال، يُستثنى العمال الأجراء من هذه المسؤولية، إلا إذا تم تفويض أحدهم بسلطة قانونية. وبذلك، يمكن من خلال تحديد مفهوم "الجهاز" أو "العضو" فهم نطاق المسؤولية بشكل أدق[1].

[1] مزاولي محمد , المرجع السابق , ص 277

3/ عقوبة المشاركة في الجريمة:

خصص المشرع الجزائري لجريمة الإشتراك في المساس بأنظمة المعالجة للمعطيات عقوبة و ذكرت المادة 394 مكرر منه أهم الشروط الواجب توافرها في الجريمة ليتم المعاقبة عليها و هي كالتالي:

1- يجب أن تكون الجريمة قد وقعت ضمن إطار مجموعة أو اتفاق بين عدة أطراف
2- يجب أن يكون الهدف و الغاية من تكوين هذه المجموعة هو ارتكاب أحد الجرائم المنصوص عليها في قسم الجرائم المعلوماتية .
3- يجب أن يتجسد التحضير لهذا النوع من الجرائم من خلال أفعال مادية ملموسة .

و يعاقب المشرع الجزائري على الاشتراك في الاتفاق على ارتكاب الجريمة بعقوبة تعادل عقوبة الجريمة التي تم التحضير لها مع فرض العقوبة الأشد لهذه النوع من الجرائم , و هناك رأي آخر يعتقد أن مجرد الاتفاق الجنائي يشكل جريمة بحد ذاته , حيث يظهر العزم الجماعي الإجرامي من خلال إعلان كل عضو عزمه لبقية الأعضاء مما يؤدي إلى توحيد إرادتهم لارتكاب الجريمة .

و من جهة أخرى يعتبر الاتفاق الجنائي ظاهرة خطيرة لأنها تقوم على التقاء الإرادات الإجرامية لتنفيذ عمل إجرامي يهدد المصالح المحروسة بموجب النصوص القانونية . هذه الخطورة الناتجة عن التهديد تدعو إلى الاتفاق على تجريم الاشتراك في الجرائم .[1]

4/ عقوبة الشروع في الجريمة:

الشروع هو البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب

[1] آمال قارة , الحماية الجزائية للمعلوماتية في التشريع الجزائري, بدون ط , دار الهومة للطباعة و النشر , الجزائر , 2006, ص131

لا دخل لإرادة الفاعل فيها .[1]في المادة 30 من قانون العقوبات نجد أنها تتحدث عن المحاولات لارتكاب الجرائم حيث تنص على أن أي محاولة لارتكاب أي جناية تعتبر و كأنها جناية تامة و ذلك إذا لم تتوقف هذه الأفعال أو لم يعاق أثرها نتيجة لظروف خارجة عن إرادة الفاعل,

تنص المادة 11 من اتفاقية بودابست على ضرورة معاقبة الشروع في الجرائم التي تمس الأنظمة المعلوماتية. وقد تبنى المشرع الجزائري هذا المبدأ في المادة 394 مكرر 7 من قانون العقوبات، حيث ينص على معاقبة الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بنفس العقوبة المقررة للجريمة التامة. هذا النص الصريح يتماشى مع ما جاء في المادة 31 من قانون العقوبات الجزائري.

يعكس هذا التشريع رغبة واضحة لدى المشرع في توسيع نطاق العقوبات لتشمل أكبر عدد ممكن من الأفعال التي تهدد الأنظمة المعلوماتية. من خلال مساواة الشروع في ارتكاب هذه الجرائم مع الجريمة التامة من حيث العقوبة، يؤكد القانون على أهمية حماية الأنظمة المعلوماتية من أي محاولة اختراق أو اعتداء، مهما كانت صغيرة أو لم تكتمل. ويهدف هذا الإجراء إلى تعزيز الردع والحماية القانونية في مواجهة التهديدات السيبرانية[2].

و من خلال استقراء نص المادة 394 مكرر 5 من قانون العقوبات نجد أن المشرع الجزائري قد تبنى فكرة الشروع في الجريمة وهذا يعني أن حتى محاولات الإجلرام التي لم تكتمل تعتبر جرائم قائمة بحد ذاتها وكمثال على ذلك إذا قام الجاني بمحاولة الدخول إلى نظام معلوماتي و تم إيقافه نشاطه من قبل شخص آخر , أو انهى نشاطه و لكن لم يحقق النتيجة المرجوة منه بسبب خلل لم يكن على علم به ,فإن هذه المحاولات الفاشلة تعتبر جرائم , و كمثال على ذلك استخدام برنامج للدخول للنظام المعلوماتي و التعلاعب ببياناته . قد يتمكن الجاني من الدخول إلى النظام و لكنه فشل في التلاعب ببياناته بسبب خلل في البرنامج , في هذه الحالة تتحقق

[1] أحمد عوض بلال , مبادئ قانون العقوبات المصري , بدون ط, دار النهضة العربية , القاهرة , 2012 , ص324
[2] دحو نجاة و أولاد حمو فاطمة , المرجع السابق , ص 46

جريمة الدخول إلى النظام بالإضافة إلى جريمة الشروع في التلاعب بالبيانات , و بالتالي تسمى في هذه الحالة بال"الجريمة الخائبة" لأنها لم تكتمل لأسباب خارجة عن إرادة مرتكبها.[1]

العقوبات التكميلية :

المصادرة :

تعني الاستيلاء على الأجهزة والبرامج والوسائل التي تم استخدامها في ارتكاب الجرائم التي تهدد النظام العام. يشمل ذلك بيع هذه الأدوات أو حجزها، مع الحرص على مراعاة حقوق الأطراف الثالثة الذين قد يكونون قد حصلوا عليها بحسن نية. تهدف هذه الإجراءات إلى منع استخدام هذه الوسائل في المستقبل لأي أغراض غير قانونية وضمان تحقيق العدالة بدون الإضرار بحقوق الأفراد الذين لم يكونوا على علم باستخداماتها غير المشروعة.

إغلاق المواقع الإلكترونية:

يعني تعطيل الوصول إلى مواقع الإنترنت التي كانت تستخدم كأداة لارتكاب الجرائم أو ساهمت في تنفيذها. تشمل هذه الإجراءات إيقاف نشاط المواقع التي تروج لمحتويات غير قانونية أو تساعد في تسهيل الأنشطة الإجرامية. الهدف من هذه التدابير هو حماية المجتمع من التأثيرات السلبية لهذه المواقع وضمان عدم استمرارها في تقديم منصات للأنشطة غير

المشروعة. كما يتطلب ذلك التنسيق مع الجهات المعنية لضمان فعالية الإغلاق وحماية حقوق المستخدمين الذين قد يكونون تضرروا بشكل غير مباشر.

إغلاق المحل (مقاهي الانترنت):

يتم إغلاق المقهى الإلكتروني في الحالات التي يكون فيها صاحب المقهى متواطئًا في الجريمة، سواء كان ذلك بعلمه بها وعدم تبليغه السلطات عنها، أو بعدم اتخاذه الإجراءات اللازمة لمنع الجناة من استخدام محله لارتكاب هذه الجرائم. ويلاحظ أن هذه العقوبات مصممة لتكون رادعة، حيث يمكن تشديدها عند الضرورة لتشمل عقوبات إضافية وأخرى موجهة ضد

[1] فايز محمد راجح غلاب , الجرائم المعلوماتية في القانون الجزائري و اليمني, أطروحة دكتوراه جامعة الجزائر 1, كلية الحقوق , 2010ص146

الشخص المعنوي. هذه الإجراءات تهدف إلى ضمان عدم تكرار مثل هذه الجرائم وتحقيق العدالة من خلال محاسبة كل من يساهم في تسهيل الأنشطة الإجرامية[1].

المبحث الثاني: الحماية الإجرائية للأنظمة المعلوماتية من القرصنة

على عكس الجرائم التقليدية فإن عمليات مكافحة الجرائم المعلوماتية شكلت تحديات كبيرة نظرا لكونها لا تترك أثرا ماديا و يمكن لمرتكبيها اتلاف الأدلة وقت ما يشاؤون و في هذا النوع من الجرائم يتم التفتيش عبر اجهزة الكمبيوتر و أحيانا يتم تفتيش كذلك كل الأجهزة و الشبكات المرتبطة بجهاز المشتبه به سواء كان خارج الوطن أو داخله و التفتيش خارج الوطن يشكل في حد ذاته صعوبة و تحدي و عليه نحن بصدد معرفة الاجراءات التي اتخذها المشرع الجزائري للتصدي لهذا النوع من الجرائم .

المطلب الأول: المكافحة الإجرائية في القانون الجزائري

من حيث معالجة الجريمة المعلوماتية أثناء التحقيق:

أولا : التفتيش .

يرى بعض الفقهاء أن الهدف من التفتيش هو ضبط الأدلة المادية لكشف الحقيقة , لذا يعتبر تفتيش مكونات الحاسوب بحثا عن أدلة الجريمة المعلوماتية قانونيا إذا تم وفق الإجراءات المنصوص عليها قانونا مع مراعاة حساسية هذه الأجهزة و يختلف حكم التفتيش حسب مكان وجود هذه المكونات , حيث تخضع الماكن التي يتواجد فيها الحاسوب كمنزل المتهم أحكاما خاصة .[2]

و عليه يجب توافر عدة ضوابط لصحة تفتيش نظم الحاسوب و هي:

الضوابط الموضوعية : المقصود بهذه الضوابط الشروط الازمة لصحة التفتيش و يمكن حصرها في ثلاث نقاط و هي السبب , المحل و السلطة المخولة لها للقيام بذلك.

[1] ختير مسعود , الحماية الجنائية لبرامج الكمبيوتر , بدون ط, دار الهدى للنشر و التوزيع, 2010, ص103
[2] عبد الفتاح بيومي حجازي , المرجع السابق , ص77

1- السبب: الهدف الأساسي من إجراء التفتيش بشكل عام هو جمع الدلة في سياق تحقيق جار من أجل الوصول إلى الحقيقة الكاملة حول الجريمة و يكون ذلك غالبا عند وقوع الجريمة سواء كانت جناية أو جنحة حيث يتطلب الأمر اتهام شخص أو عدة أشخاص محددين بارتكاب الجريمة يعتمد التفتيش على وجود دلائل أو مؤشرات قوية تشير إلى أن هناك مواد أو أدلة قد تسهم في كشف الحقيقة موجودة لدى أحد المشتبه فيهم سواء في مسكنه أو بحوزته أو لدى شخص آخر على صلة به أو في مسكن ذلك الشخص , و هذا الأمر ينطبق كذلك على الجرائم الإلكترونية , حيث يتطلب الكشف عن الأدلة المتعلقة بها نفس الدقة و الحرص إذ تتواجد الأدلة الرقمية على أجهوة الحواسيب أو الهواتف المحمولة أو حسابات المشتبه فيهم الإلكترونية .[1]

2- محل التفتيش:

يقصد بمحل التفتيش المكان الذي يحتفظ به الشخص بالأشياء المادية التي تحمل أسراره أو دلائل تورطه في جريمة ما ففي الجرائم التقليدية , يتوجه التفتيش نحو شخص المتهم أو أي

شخص آخر مرتبط بالقضية و كذلك نحو مسكن المتهم أو مسكن أي شخص آخر يحتمل أن تكون له علاقة بالقضية بما يشمل ملحقاتها , أما في الجرائم المعلوماتية فإن محل التفتيش يتعلق بالكمبيوتر سواء كانت مكوناته المادية مثل الأجهزة و الملحقات أو مكونات معنوية مثل البيانات و المعلومات المخزنة فيه بالإضافة إلى ذلك يمكن أن تمتد عمليات التفتيش لتشمل الشبكات المتصلة بالحاسوب . و ليتم إجراء التفتيش بشكل صحيح , يجب الإشارة إلى أن هذه الأجهزة لا تكون مستقلة بذاتها بل في أغلب الأحيان تكون في أماكن مثل المنازل أو المكاتب أو مقاهي الانترنت ... أو تكون في حوزة مالكيها كالهواتف المحمولة .و تتطلب هذه العمليات فهما عميقا و خبرة عالية لكيفية التعامل مع المكونات المادية و المعنوية لأجهزة الحاسب الآلي و شبكات الاتصال نظرا لتعقيد الطبيعة الرقمية لهذه الأدلة و إمكانية تخزينها في مواقع عديدة

[1] ليندا بن طالب , التفتيش في الجريمة المعلوماتية , مجلة العلوم القانونية و السياسية , تيزي وزو الجزائر , م08, ع16, 2017, ص492

لا يمكن الوصول إليها دون خبرة تقنية عالية و هذا ما يجعل عملية التفتيش في الجرائم المعلوماتية تتطلب مهارات غير الموجودة في الجرائم التقليدية .[1]

3- السلطة المختصة بالتفتيش:

إن التفتيش يعد من اجراءات التحقيق التي تنتهك تنتهك الحرية الشخصية للأفراد و لذلك حرصت التشريعات على إسناد هذا الإجراء إلى جهات قضائية تكفل حماية الحقوق و الحريات و مع ذلك لم يتبعو منهجا موحدا فيما يخص تحديد الجهة المسؤولة عن التحقيق و التي تملك صلاحية التفتيش . و كمثال على ذلك اتبعت بعض التشريعات منها القانون المصري نهج منح هذه السلطة للنيابة العامة عند صدور قانون الاجراءات الجنائية بموجب القانون رقم 150 سنة 1950 , أعاد النظام الجمع بين سلطتي التحقيق و الاتهام في يد النيابة العامة باستثناء بعض الجرائم التي يختص بها قاضي التحقيق و على العكس من ذلك نجد أن كل من المشرع الجزائري و الفرنسي قد اتبعا نظام الفصل بين سلطتي الاتهام و التحقيق , حيث اوكلت هذه المهمة في فرنسا إلى قاضي التحقيق , في حين أسندت في الجزائر إلى النيابة العامة . و يتضح من كل هذا أن هناك تباينا في كيفية توزيع السلطات بين الجهات القضائية المختلفة لضمان التوازن بين تحقيق العدالة و حماية حقوق الأفراد .[2]

4- الإذن بالتفتيش :

غالبًا ما يُصدر الإذن بتفتيش مسكن المتهم، ويشمل هذا الإذن كل ما هو موجود داخل المسكن. ولكن يبقى السؤال: هل يتيح هذا الإذن لضباط الشرطة القضائية حق الدخول إلى البيئة الرقمية للمتهم والتغلغل في المنظومة المعلوماتية بحثًا عن أدلة يمكن استخدامها في التحقيق؟

[1] قدري عبد الفتاح الشهاوي , ضوابط التفتيش في التشريع المصري , بدون ط, منشأة المعارف, الاسكندرية , 2005 ,ص112

[1] عائشة بن قارة مصطفى , حجية الدليل الالكتروني في مجال الاثبات الجنائي , بدون ط , دار الجامعة الجديدة الاسكندرية , 2009, ص55

يرى معظم الفقهاء أن إذن التفتيش يجب أن يحدد بوضوح المكان المراد تفتيشه والأشياء أو الأشخاص المطلوب تفتيشهم وضبطهم، مثل أجهزة الحاسوب، الصور الجنسية الإلكترونية الخاصة بالأطفال، أو المصنفات الإلكترونية المقلدة. هذا التحديد في الإذن ضروري لتجنب ما يُعرف بالتفتيش الاستكشافي، حيث لا ينبغي للمأذون بالتفتيش أن يتمتع بسلطة تقديرية واسعة. إلا أن تطبيق هذا الشرط في الواقع العملي عند تفتيش أجهزة الكمبيوتر يواجه صعوبات كبيرة.

تعقيد المسألة يعود إلى الطبيعة الخاصة لأجهزة الكمبيوتر، حيث تحتوي على عدد كبير من الملفات التي قد لا تعكس أسماؤها محتوياتها الفعلية. هذا يثير تساؤلاً حول ما إذا كان يجب اعتبار كل ملف "صندوقًا مغلقًا" يتطلب إذنًا قضائيًا مستقلاً لفتحه، خصوصًا وأن المتهم قد يستخدم أسماء مستعارة للملفات التي تحتوي على مواد غير مشروعة. هذه المسألة المعقدة تبرز الحاجة إلى توازن دقيق بين حقوق المتهم ومتطلبات العدالة الجنائية.

فيما يخص المشرع الجزائري، لم يحدد قانون رقم 09/04 شرط تحديد المكان والأشياء المراد تفتيشها وضبطها عند إجراء التفتيش المعلوماتي. بدلاً من ذلك، يقتصر القانون على ضرورة إبلاغ جهات التحقيق للسلطة القضائية المختصة عند تمديد التفتيش إلى منظومة

معلوماتية أخرى. هذا يهدف لضمان مراقبة القضاء ومنع تجاوزات حقوق الأفراد. ومع ذلك، يظل غياب التفصيل بشأن هذا الشرط نقطة ضعف قد تؤدي إلى جدل قانوني، خاصة في الجرائم الرقمية التي تتطلب تفتيش مساحات واسعة من البيانات[1].

الضوابط الشكلية : إن هذه الضوابط الشكلية تهدف إلى ضمان الحقوق و الحريات للأفراد إلى جانب ضمان السير الحسن للتحقيق:

1- إجراء التفتيش بالحضور الضروري للأشخاص المعنيين قانونا:

[1] عائشة بن قارة , المرجع السابق , ص63

يُعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية لضمان سلامة الإجراءات. التفتيش ينطوي على الاطلاع على أسرار الغير، ولذلك تختلف متطلباته بين تفتيش الأشخاص وتفتيش المساكن. بالنسبة لتفتيش الأشخاص، لا تشترط التشريعات الإجرائية حضور شهود. أما في حالة تفتيش المساكن، ينص القانون الجزائري على ضرورة حضور المشتبه فيه أو المتهم أثناء التفتيش، سواء قام به قاضي التحقيق أو ضابط الشرطة القضائية. إذا تعذر حضور المشتبه فيه، يتم التفتيش بحضور شاهدين غير تابعين للسلطة القائمة بالتفتيش.

تجدر الإشارة إلى أن التعديل الذي أدخله المشرع الجزائري بموجب القانون رقم 06-22 على المادة 45 من قانون الإجراءات الجزائية، استغنى عن ضمانة حضور الأشخاص المحددين في الفقرة الأولى في بعض الجرائم، مثل الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات. الهدف من ذلك هو الحفاظ على سرية جمع الأدلة الإلكترونية نظراً لطبيعتها الخاصة وسهولة التلاعب بها عن بعد. هذه الضمانة بدأت تفقد أهميتها في الدول التي تعتمد نظام التفتيش عن بعد، أو ما يسمى في الفقه الفرنسي "التفتيش المباشر[1]."

2- وقت إجراء التفتيش في الجرائم المعلوماتية :

يشير شرط الميعاد الزمني في عمليات التفتيش إلى أن التفتيش يجب أن يتم خلال فترة زمنية محددة عادةً من قبل القانون، وذلك للحد من انتهاكات الحرية الفردية وحرمة المسكن. يحظر القانون الجزائري تفتيش المنازل في أوقات معينة، حيث تنص المادة 47 من قانون الإجراءات الجزائية على أن التفتيش يمكن أن يتم فقط من الساعة الخامسة صباحًا حتى الساعة الثامنة مساءً. ومع ذلك، توجد استثناءات يمكن فيها إجراء التفتيش في أي وقت من النهار أو الليل بناءً على إذن مسبق من وكيل الجمهورية المختص، وذلك في حالات محددة مثل الجرائم الخطيرة التي تمس أنظمة المعالجة الآلية للمعطيات.

تسمح المادة 64/3 من قانون الإجراءات الجنائية، فيما يتعلق بتحقيقات الجرائم المنصوص عليها في المادة 47/3، بإجراء التفتيش في أي ساعة من ساعات النهار أو الليل بشرط

[1] ليندا بن طالب , المرجع السابق , ص493

الحصول على إذن مسبق. يُلاحظ أن المشرع الجزائري في هذه الحالات يفضل مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حماية حرمة مسكنهم، خاصة في الجرائم الإلكترونية التي يمكن فيها محو الأدلة بسرعة كبيرة.

أما بالنسبة للأماكن العامة، فإذا وجد شخص يحمل مكونات حاسوب معينة أو كان مسيطرًا عليها، فإنه يجوز تفتيشها فقط في الحالات التي يُسمح فيها بتفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في القانون.

3- محضر التفتيش في الجريمة المعلوماتية:

يُعتبر التفتيش من أعمال التحقيق الأساسية، ويتعين تحرير محضر يُثبت فيه ما نتج عن التفتيش من أدلة. على الرغم من أن القانون لم يتطلب شكلاً خاصًا لمحضر التفتيش، إلا أن هناك بعض القواعد العامة التي يجب الالتزام بها لضمان صحة المحضر. يجب أن يكون المحضر مكتوبًا باللغة الرسمية، مؤرخًا، وموقعًا عليه[1].

علاوة على ذلك، ينبغي أن يتضمن المحضر كافة الإجراءات التي تم اتخاذها خلال عملية التفتيش، وذلك بما يشمل التفاصيل المتعلقة بالشخص المتخصص في الحاسوب والإنترنت

الذي تمت الاستعانة به لإجراء الخبرة الفنية الضرورية. هذا التوثيق الدقيق يضمن أن جميع الخطوات والإجراءات تم تنفيذها وفقًا للقانون، مما يساهم في الحفاظ على نزاهة التحقيقات وضمان قبول الأدلة المستخلصة في المحاكم.

ثانيا : اعتراض المراسلات و التقاط الصور و تسجيل الأصوات:

في 20 ديسمبر 2006، تم تعديل قانون الإجراءات الجزائية الجزائري بالقانون رقم 06-22، ليشمل فصلاً جديداً بعنوان "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور". يحتوي هذا الفصل على المواد من 65 مكرر 5 إلى 65 مكرر 10، ويحدد الشروط

[1] ليندا بن طالب , المرجع السابق , ص494

التي يجب أن يلتزم بها رجال الشرطة القضائية عند القيام بهذه الإجراءات في إطار التحقيقات الجنائية.

أولاً، يحق لرجال الشرطة القضائية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ولكن فقط في حالات محددة تتعلق بجرائم مثل المخدرات، الجرائم المنظمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الإرهاب، التشريع الخاص بالصرف، والفساد. يعتبر هذا التحديد مهمًا بسبب خطورة هذه الجرائم وتأثيرها على السياسة العامة والاقتصاد الوطني.

ثانياً، يجب أن يصدر الإذن للقيام بهذه الإجراءات من وكيل الجمهورية أو قاضي التحقيق المختص، ويتضمن الإذن اعتراض المراسلات عبر وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات التقنية اللازمة لالتقاط وتسجيل الكلام والصور في أماكن خاصة أو عامة[1].

ثالثاً، يجب أن تتم هذه العمليات تحت المراقبة المباشرة لوكيل الجمهورية أو قاضي التحقيق، وفي حالة اكتشاف جرائم أخرى أثناء التنفيذ، فإن ذلك لا يبطل الإجراءات المتخذة.

رابعاً، يتعين أن يحتوي الإذن على كافة التفاصيل التي تسمح بالتعرف على الاتصالات المطلوب اعتراضها، مثل رقم الهاتف واسم المشترك، وتحديد الأماكن المعنية، والجريمة التي تبرر هذه التدابير.

خامساً، يكون الإذن ساريًا لمدة أقصاها أربعة أشهر قابلة للتجديد وفق نفس الشروط.

سادساً، يجوز لوكيل الجمهورية أو قاضي التحقيق تسخير عون مؤهل من وحدة أو هيئة مكلفة بالمواصلات السلكية واللاسلكية لتولي الجوانب التقنية للعمليات.

[1] شرف الدين وردة و بلجراف سامية , الجوانب الموضوعية و الاجرائية لمكافحة الجرائم المعلوماتية في التشريع الجزائري , مجلة المنار للبحوث و الدراسات القانونية و السياسية , م02, ع03 , ديسمبر 2017, ص 43 ص44

سابعاً، يحرر ضابط الشرطة القضائية المأذون له محضرًا عن كل عملية اعتراض وتسجيل، يوضح فيه تاريخ وساعة بدء وانتهاء العمليات.

ثامناً، يتم نسخ وترجمة المحادثات التي تتم بلغات أجنبية بمساعدة مترجم مختص عند الضرورة[1].

ثالثا : التسرب

في قانون الإجراءات الجزائية الجزائري، تم إضافة اختصاصين جديدين وهما اعتراض المراسلات والتسجيل والتقاط الصور، والتسرب. المادة 65 مكرر 12 تُعرّف التسرب بأنه قيام ضابط أو عون الشرطة القضائية بمراقبة المشتبه في ارتكابهم جريمة تحت غطاء أنه شريك أو متعاون معهم، وذلك تحت إشراف ضابط شرطة قضائية مسؤول عن التنسيق.

لتنفيذ هذه الإجراءات، يجب مراعاة شروط محددة:

-يجب أن تكون الجريمة تتعلق بالإرهاب، المخدرات، الجريمة المنظمة عبر الحدود، الجرائم المعلوماتية، تبييض الأموال، قضايا الصرف، الفساد أو التهريب وفقاً للقوانين ذات الصلة.

-يجب الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق، ويكون هذا الإذن كتابياً ومسبباً، مع تحديد الجريمة وهوية ضابط الشرطة القضائية المسؤول. مدة الإذن لا تتجاوز أربعة أشهر ويمكن تجديدها عند الضرورة.

-لا يُفصح عن الهوية الحقيقية لضباط الشرطة الذين يقومون بعملية التسرب، ومن يكشف عن هويتهم يُعاقب بالسجن من سنتين إلى خمس سنوات وغرامة تتراوح بين 50,000 و200,000 دينار. إذا نتج عن الكشف أعمال عنف، تزيد العقوبة إلى السجن من خمس إلى عشر سنوات وغرامة من 200,000 إلى 500,000 دينار. وإذا تسبب في وفاة، تكون العقوبة من عشر إلى عشرين سنة سجناً وغرامة من 500,000 إلى 1,000,000 دينار.

[1] شرف الدين وردة و بلجراف سامية , المرجع نفسه , ص45

-عند انتهاء مدة التسرب أو إيقافه، يمكن للعون المتسرب مواصلة العمل لفترة كافية تضمن أمانه، وذلك لمدة لا تتجاوز أربعة أشهر إضافية بعد إبلاغ القاضي. وإذا لم يتمكن العون من إنهاء المهمة بأمان خلال هذه الفترة، يمكن للقاضي تمديدها لأربعة أشهر أخرى كحد أقصى.

-يمكن الاستماع لضابط الشرطة المسؤول عن عملية التسرب كشاهد في الإجراءات المتعلقة بالعملية[1].

من حيث الوقاية من الجرائم المعلوماتية:

1/ مراقبة الاتصالات :

وفقا للمادة الثانية من قانون 09_04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها , يعرف الاتصال الالكتروني على انه أي تبادل لعلامات أو إشارات أو كتابات او صور او أصوات أو اي معلومات بواسطة وسائل إلكترونية و تنص المادة الرابعة من نفس القانون على إمكانية مراقبة الإتصالات الإلكترونية في ثلاث حالات:

- تهديد للنظام العام أو الدفاع الوطني .
- صعوبة في التحقيقات الجارية .
- تنفيذ طلبات مساعدة قضائية دولية.

و يتطلب إجراء المراقبة موافقة قضائية و في الحالة الاولى يمنح ضباط الشرطة القضائية إذنا بمدة سنة قابلة للتتجديد لجمع و تسجيل المعلومات ذات الصلة بالأمن القومي و مكافحة الارهاب و قد كلف المشرع الجزائري هيئة الوقاية من من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها بمراقبة الاتصالات الالكترونية بتوجيه من القاضي المختص.

2/ في حالة التفتيش:

[1] قانون رقم 06-22 , المؤرخ في 2006/12/20,المعدل و المتمم للأمر رقم 66-155المؤرخ في 1966/06/08 و المتضمن قانون إج ,ج ر, ع45

في المادة 5 من قانون الوقاية من الجرائم التقنية، يشير النص إلى ضرورة توفير حالات تسمح للسلطات القضائية بتفتيش الأنظمة الإلكترونية في إطار القانون الجنائي. هذه الحالات تشمل الوقاية من جرائم الإرهاب والتخريب والتهديدات لأمن الدولة، وكذلك لحماية النظام العام والدفاع الوطني والاقتصاد الوطني. تتضمن أيضًا حالات البحث والتحقيق الصعبة، وتنفيذ طلبات المساعدة القضائية الدولية[1].

عندما يتعلق الأمر بالوقاية من جرائم الإرهاب والتخريب والتهديدات لأمن الدولة، يتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها حصرياً إجراءات التفتيش. يمكن أيضًا للقضاة وضباط الشرطة القضائية التابعين للهيئة أن يقوموا بعمليات التفتيش بناءً على الشروط والأسس المحددة في التشريع الساري، خاصة قانون الإجراءات الجزائية، لفحص أي مكان أو هيكل أو جهاز يُشتبه في استخدامه لوسائل المراقبة في

الاتصالات الإلكترونية. في تلك الحالات، يُسمح بالدخول لأغراض التفتيش، بما في ذلك الوصول عن بُعد، إلى أنظمة المعلومات أو جزء منها، وكذلك إلى نظم التخزين الإلكتروني.

قبل التوجه إلى فحص المعلومات في نظام معلوماتي آخر، يُعتبر من الضروري إبلاغ السلطة القضائية بالخطوة المقترحة مسبقًا، بناءً على الاعتبارات التي تشير إلى وجود المعلومات هناك وإمكانية الوصول إليها. وفي الحالة التي تظهر فيها مؤشرات تدل على أن المعطيات المبحوث عنها مخزنة خارج البلاد، يجب أن يتم الحصول عليها بالتعاون مع السلطات الأجنبية ذات الاختصاص، بموجب الاتفاقيات الدولية المعمول بها ووفقًا لمبدأ المعاملة بالمثل.

3/ حجز المعطيات المعلوماتية :

وضع المشرع تنظيما دقيقا للحماية من الجرائم المعلوماتية في المادتين 6 و 7 من القانون السابق الذكر:

[1] شرف الدين وردة و بلجراف سامية , المرجع السابق, ص50

يجب على الجهات المعنية بمكافحة الجريمة الرقمية أن تتخذ إجراءات لحماية البيانات وضمان سلامتها أثناء التحقيقات، وذلك عبر نسخ المعلومات الضرورية وتخزينها بطريقة آمنة ومناسبة للحجز. ينبغي أن يتولى الجهاز المشارك في التفتيش والتحقيق العناية بحماية هذه البيانات وتأمينها من أي اختراق أو تلاعب. وفي حال الحاجة إلى تعديل أو إعادة تشكيل البيانات لغايات التحقيق، ينبغي أن تتخذ الجهة المعنية بذلك الإجراءات الفنية اللازمة دون المساس بسرية المعلومات[1].

يبدو من الضروري تطوير السياسات والإجراءات التقنية المناسبة للتأكد من عدم إمكانية الوصول غير المصرح به إلى المعلومات خلال عمليات التفتيش والحجز. ينبغي للسلطة التي تقوم بالتفتيش أن تضع في اعتبارها تكنولوجيا الأمان اللازمة لمنع الوصول غير المشروع إلى البيانات المخزنة في الأنظمة الرقمية .

وعليها أيضًا توجيه الإجراءات اللازمة لحماية البيانات التي قد تحتوي على معلومات جرمية، ويمكنها تكليف أشخاص مؤهلين لاستخدام التقنيات اللازمة لضمان سرية هذه المعلومات وتأمينها. يجب على الجهات المعنية أن تلتزم بالقوانين المعمول بها وعدم استخدام المعلومات المتحصل عليها بطرق غير قانونية، مع مراعاة حقوق الأفراد والحفاظ على خصوصيتهم.

وفي سياق مكافحة الجرائم المتعلقة بالإعلام والاتصالات والتخطيط لها، يتولى الجهاز المختص حصريًا إجراءات الحجز وفقًا للتشريعات المعمول بها، بما يتيح الحفاظ على أمن الدولة ومكافحة الجريمة بفعالية[2].

4/ تسجيل و جمع المعطيات المتعلقة بالاتصال في الحين :

حدد المشرع الجزائري في قانون 09-04 مجموعة من الإجراءات المتعلقة بجمع وتسجيل البيانات الخاصة بمحتوى الاتصالات في الوقت الفعلي، وجعل ذلك من ضمن الالتزامات

[1] مجدوب نوال , الآليات الإجرائية للكشف عن الجريمة المعلوماتية , مجلة البحوث القانونية و الاقتصادية , المركز لجامعي مغنية الجزائر , م 06, ع03 , 2022/11/09 , ص204

[2] مجدوب نوال , المرجع السابق , ص205

المفروضة على مقدمي الخدمات لدعم السلطات القضائية في تحرياتها. تنص المادة 10 على ضرورة تقديم مقدمي الخدمات المساعدة اللازمة للسلطات المكلفة بالتحقيقات القضائية، من خلال جمع وتسجيل البيانات المتعلقة بمحتوى الاتصالات فور طلبها. ويجب على مقدمي الخدمات الحفاظ على سرية هذه العمليات والمعلومات ذات الصلة، وذلك تحت طائلة العقوبات المقررة في حال إفشاء أسرار التحري والتحقيق.

كما أضافت المادة 12، إلى جانب الالتزامات المنصوص عليها في المادة 11 من قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التزامات أخرى على مقدمي خدمات الإنترنت. تتضمن هذه الالتزامات ضرورة اتخاذ الإجراءات المناسبة لضمان تنفيذ القانون بكفاءة، وتقديم الدعم المطلوب للسلطات لمواجهة الجرائم الإلكترونية وضمان سرية المعلومات المتعلقة بالتحقيقات. بهذه الطريقة، يسعى المشرع إلى تعزيز بيئة قانونية صارمة تحمي البيانات وتحافظ على النظام العام.

بمجرد اكتشاف أن المحتويات المنشورة تخالف القوانين السارية، يجب اتخاذ إجراءات فورية لسحبها ومنع الوصول إليها. يمكن تحقيق ذلك من خلال وضع ترتيبات تقنية تسهم في حصر الوصول إلى تلك الموزعات التي تحتوي على معلومات تتعارض مع النظام العام أو الآداب العامة. بالإضافة إلى ذلك، يجب إخطار المشتركين بوجود مثل هذه المحتويات المخالفة لضمان توعيتهم والتحذير من الوصول إليها. إن هذا التدخل السريع لا يساهم فقط في الامتثال للقوانين، بل يعزز أيضا بيئة رقمية آمنة ومسؤولة[1].

5/ التحفظ بالبيانات المخزنة:

نظم المشرع الجزائري عملية التحفظ العاجل للبيانات المعلوماتية المخزنة في إطار قانون رقم 09-04، الذي يحدد القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويُلزم هذا القانون مقدمي خدمات الإنترنت بمساعدة السلطات المكلفة بالتحقيقات القضائية بحفظ المعطيات اللازمة. بالإضافة إلى ذلك، تم تنظيم هذه العملية أيضًا

[1] القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من جرائم الاعلام و الاتصال و مكافحتها , ج ر, ع44

في مرسوم رئاسي رقم 15-261، الذي يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مما يجعل من التحفظ العاجل للبيانات مهمة أساسية لهذه الهيئة.

أولا: الحفظ العاجل للبيانات المعلوماتية المخزنة ضمن قانون 09-04:

في الفصل الرابع من قانون 09-04، تناولت المادتين 10 و11 التزامات مقدمي الخدمات بمساعدة السلطات القضائية في حفظ البيانات. تنص المادة 10 على أنه في سياق تطبيق هذا القانون، يجب على مقدمي الخدمات تقديم الدعم للسلطات المكلفة بالتحقيقات القضائية، والحفاظ على المعطيات المتعلقة بحركة السير ووضعها تحت تصرف هذه السلطات وفقًا للمادة 11. وتشمل البيانات التي يجب حفظها معلومات تساعد في التعرف على مستخدمي الخدمة، والمعطيات المتعلقة بالأجهزة الطرفية المستخدمة للاتصال، والخصائص التقنية

للاتصال، وتاريخ ووقت ومدة كل اتصال، والخدمات التكميلية المستعملة، وكذلك البيانات التي تساعد في التعرف على المرسل أو المرسلين وعناوين المواقع التي تم الاطلاع عليها. يتعين على مقدمي الخدمات الحفاظ على سرية العمليات والمعلومات المرتبطة بها، تحت طائلة العقوبات المقررة في حال إفشاء أسرار التحري والتحقيق. تُحفظ هذه البيانات لمدة سنة واحدة ابتداءً من تاريخ تسجيلها. وتترتب مسؤولية جزائية على الأفراد والكيانات في حال عدم الامتثال لهذه الالتزامات، مما قد يؤدي إلى عرقلة سير التحقيقات القضائية. يُعاقب الأفراد بالحبس من ستة أشهر إلى خمس سنوات، وبغرامة تتراوح بين 50,000 إلى 500,000 دينار جزائري، بينما تُعاقب الكيانات بالغرامة وفقًا لقانون العقوبات.

ثانيا: الحفظ العاجل للبيانات المعلوماتية المخزنة ضمن مرسوم رئاسي رقم 15-261:

نص المشرع الجزائري في المادة 4 من مرسوم رئاسي رقم 15-261، المؤرخ في 8 أكتوبر 2015، على أن من بين المهام الموكلة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حفظ البيانات الرقمية وتحديد مصدرها ومسارها لاستعمالها في الإجراءات القضائية. إلا أن المرسوم لم يحدد مدة قصوى لحفظ هذه البيانات،

على عكس ما هو منصوص عليه في المادة 11 من قانون 09-04 بالنسبة لمقدمي خدمات الإنترنت.

بهذا الشكل، يظهر التنظيم الجزائري حرصًا واضحًا على ضمان حفظ البيانات المعلوماتية وتسهيل مهام السلطات القضائية في مكافحة الجرائم المرتبطة بالتكنولوجيا، مما يبرز دور مقدمي الخدمات والهيئة الوطنية في تحقيق هذا الهدف الحيوي[1].

[1] شرف الدين وردة و بلجراف سامية , المرجع السابق , ص53 و ص54

خلاصة الفصل الثاني:

وختاما لهذا الفصل نستنتج من دراستنا له أن المشرع الجزائري قد اتخذ الإجراءات الازمة لمكافحة جرائم القرصنة الإلكترونية و الجريمة المعلوماتية بشكل عام و ذلك عن طريق تعديله للقوانين الحالية و استحداث أخرى جديدة لتجريم جميع أنواع و أشكال الاعتداءات على النظم المعلوماتية , و قد منح هذا النوع من الجرائم إجراءات خاصة و استثنائية للتحقيق و لكيفية تجميع الأدلة و الحفاظ عليها , و تسخير كل الأجهزة الأمنية لمكافحة هذا النوع من الجرائم و التقليل منه.

خاتمة

ومن هنا نستخلص أن جريمة القرصنة المعلوماتية تعد من أبرز التحديات التي تواجه العالم الرقمي في عصرنا الحالي. تتزايد هذه التحديات مع تطور التكنولوجيا واعتمادنا المتزايد على الأنظمة الإلكترونية في كافة مناحي الحياة اليومية، مما يجعل مسألة الأمان الرقمي أكثر أهمية من أي وقت مضى.

في دراستي هذه، قمت بمعالجة موضوع القرصنة المعلوماتية عبر فصلين رئيسيين. خصصت الفصل الأول لتناول ماهية القرصنة الإلكترونية بشكل موسع، حيث تطرقت إلى تعريف القرصنة الإلكترونية من منظور قانوني وتقني، واستعرضت الأنواع المختلفة للقرصنة مثل القرصنة الأخلاقية، القرصنة الخبيثة، والهجمات الإلكترونية المستهدفة. كما تناولت خصائص القرصان الإلكتروني، موضحة السمات والمهارات التي تميز هؤلاء الأفراد عن غيرهم، بالإضافة إلى الخصائص المتعلقة بالقرصنة كعملية، مثل الأساليب المستخدمة والتقنيات المتطورة في هذا المجال.

أما في الفصل الثاني، فقد ركزت على الإجراءات التي اتخذها المشرع الجزائري لمكافحة جريمة القرصنة المعلوماتية. درست الأطر القانونية التي تحدد أركان هذه الجريمة، والعقوبات المقررة لها بموجب القوانين الجزائرية. كما تناولت أساليب المكافحة الإجرائية المتبعة أثناء وقوع الجريمة، مثل تتبع الأدلة الرقمية والتحقيقات الإلكترونية، بالإضافة إلى الإجراءات الوقائية التي تهدف إلى منع وقوع الجرائم المعلوماتية من خلال تعزيز الأمان السيبراني والتوعية بالمخاطر.

من خلال هذه الدراسة، توصلت إلى مجموعة من النتائج الهامة التي تسلط الضوء على فعالية الجهود المبذولة في مكافحة القرصنة المعلوماتية، وأوجه القصور التي تحتاج إلى معالجة. بناءً على هذه النتائج، قدمت عدة اقتراحات لحلول من شأنها تعزيز الأمان الرقمي، مثل تحسين

التشريعات القانونية، وتعزيز التعاون الدولي، وتطوير برامج توعية للمستخدمين حول كيفية حماية معلوماتهم الشخصية والتعامل الآمن مع التكنولوجيا.

النتائج:

- نقص التوعية والتدريب:

تبين أن هناك نقصاً كبيراً في التوعية حول مخاطر القرصنة الإلكترونية وأهمية الأمن السيبراني. الكثير من الأفراد والمؤسسات يفتقرون إلى المعرفة اللازمة لحماية بياناتهم وأنظمتهم من الهجمات الإلكترونية، مما يجعلهم عرضة للقرصنة بشكل أكبر. هذا النقص في الوعي يؤدي إلى ثغرات أمنية يمكن استغلالها بسهولة من قبل القراصنة. ينبغي على الجهات المعنية تنظيم حملات توعوية مكثفة وتقديم برامج تدريبية وورش عمل تستهدف جميع فئات المجتمع لتعزيز الوعي بأهمية الأمن السيبراني وطرق الحماية الفعّالة.

- صعوبة اكتشاف الجريمة المعلوماتية:

واحدة من أكبر التحديات التي تواجه مكافحة الجرائم الإلكترونية هي صعوبة اكتشافها. تتميز الجرائم المعلوماتية بقدرتها على عدم ترك أي أثر ملموس، مما يجعل تعقب مرتكبيها أمراً بالغ الصعوبة. القراصنة يستخدمون تقنيات متطورة لإخفاء هوياتهم وتضليل التحقيقات، مما يستدعي استخدام أدوات متقدمة وتقنيات حديثة لتحليل البيانات وتحديد الأنشطة المشبوهة بدقة. هذا يتطلب استثمارات كبيرة في تطوير الموارد البشرية والتقنية لمواجهة هذه التحديات بفعالية.

- قلة التبليغ وتقديم الشكاوى:

تواجه السلطات الأمنية تحدياً إضافياً يتمثل في قلة التبليغ عن الجرائم الإلكترونية. يتردد العديد من الضحايا في تقديم شكاوى رسمية إما بسبب الخوف من التعرض لمزيد من الهجمات أو بسبب اعتقادهم بعدم جدوى التبليغ. هذا التردد يمكن أن يؤدي إلى تفاقم المشكلة وانتشار الجرائم الإلكترونية دون رادع. يجب تعزيز الثقة بين الضحايا والجهات المعنية وتقديم دعم

قانوني وتقني للمساعدة في تتبع الجناة ومحاسبتهم. كما ينبغي تشجيع الضحايا على التبليغ عن الحوادث الإلكترونية من خلال حملات توعية تثقيفية وتوفير قنوات آمنة وميسرة للتبليغ.

- ضعف البنية التحتية التقنية:

على الرغم من الجهود المبذولة لتحسين الرقمنة، إلا أن الجزائر لا زالت تواجه تحديات كبيرة في تطوير البنية التحتية اللازمة لرصد ومكافحة القرصنة الإلكترونية بشكل فعال. تحتاج البلاد إلى استثمارات أكبر في مجال التكنولوجيا والبنية التحتية الرقمية لضمان قدرة المؤسسات على التصدي للتهديدات الإلكترونية المتزايدة وتعزيز الأمان السيبراني على مستوى وطني. تطوير البنية التحتية التقنية يتطلب تعاوناً وثيقاً بين القطاعين العام والخاص، بالإضافة إلى تحديث السياسات والإجراءات لمواكبة التطورات السريعة في مجال الأمن السيبراني. تعزيز التعاون الإقليمي والدولي في تبادل المعلومات والخبرات يمكن أن يسهم بشكل كبير في تعزيز قدرات الجزائر على مواجهة التحديات الإلكترونية بفعالية أكبر.

الإقتراحات:

تحتاج المجتمعات الحديثة إلى تعزيز التشريعات وتحديثها باستمرار لمواكبة التطورات التكنولوجية السريعة. من الضروري أن تكون هذه التشريعات شاملة لكل أنواع الجرائم الإلكترونية، مما يضمن حماية فعالة للمجتمع من التهديدات المتزايدة والمعقدة. يجب أن تتماشى القوانين مع الابتكارات الجديدة وتحديات العصر الرقمي، وهو أمر حيوي في ظل التطور المستمر في وسائل وتقنيات الجرائم الإلكترونية.

- التعاون الدولي :

لا يمكن التغاضي عن أهمية التعاون الدولي في هذا المجال. نظرًا للطبيعة العابرة للحدود للجرائم الإلكترونية، يصبح تعزيز التعاون بين الدول والمنظمات الدولية أمرًا لا بد منه. تبادل الخبرات والمعلومات بين البلدان يسهم بشكل كبير في مواجهة التهديدات المشتركة بفعالية

أكبر. من خلال هذا التعاون، يمكن تطوير استراتيجيات منسقة وشاملة للتصدي للجريمة الإلكترونية على مستوى عالمي، مما يساهم في تقوية الشبكة العالمية للأمن السيبراني.

- تجديد المناهج التعليمية باستمرار :

يجب تحديث المناهج التعليمية بشكل مستمر لتشمل مفاهيم الأمن السيبراني والوعي بالجرائم الإلكترونية. إدراج هذه المفاهيم ضمن المقررات الدراسية في المدارس والجامعات يهدف إلى إعداد جيل واعٍ ومدرب على مواجهة التهديدات الإلكترونية. التعليم المبكر حول هذه القضايا يعزز من قدرة الأفراد على حماية أنفسهم، ويساهم في بناء مجتمع أكثر أمانًا ووعيًا بالتحديات الإلكترونية التي قد يواجهها.

- تطوير الأنظمة :

يجب الاستثمار في تطوير أنظمة لكشف التهديدات والاستجابة السريعة لها. التقنية المتقدمة التي تكشف مبكرًا عن التهديدات الإلكترونية مثل الهجمات والفيروسات وتستجيب لها بسرعة، تقلل من الأضرار المحتملة بشكل كبير. هذا التطوير المستمر في الأنظمة الأمنية يعد خط الدفاع الأول ضد الجرائم الإلكترونية. إن امتلاك تقنيات حديثة ومتطورة يمكنها الكشف عن التهديدات بسرعة واستجابتها الفورية يعد أمرًا ضروريًا لحماية البنية التحتية الرقمية.

أخيرًا، نشر ثقافة الإبلاغ عن الجرائم الإلكترونية هو عنصر أساسي في مكافحة هذه الجرائم. يجب إنشاء منصات آمنة وسهلة الاستخدام للإبلاغ عن حوادث القرصنة والجرائم الإلكترونية، وتشجيع الأفراد على استخدامها لضمان تتبع هذه الجرائم بفعالية. بث الوعي بأهمية الإبلاغ يمكن أن يساعد في جمع البيانات اللازمة لتحليل الجرائم وتحسين أساليب المكافحة المستقبلية.

إن تشجيع الأفراد على الإبلاغ عن الجرائم الإلكترونية يعزز من قدرة السلطات على مواجهة التحديات الأمنية بفعالية أكبر، ويضمن مجتمعًا أكثر أمانًا ووعيًا بأهمية التعاون في مكافحة الجريمة الإلكترونية.

قائمة المراجع

المراجع و المصادر باللغة العربية :

الكتب:

1. الكتب العامة :

1)أحسن بوسقيعة , الوجيز في القانون الجزائي العام , ط10 , دار هومة , الجزائر , 2011.

2)أحمد عوض بلال , مبادئ قانون العقوبات المصري , دون ط , دار النهضة العربية , القاهرة , 2012 .

2. الكتب المتخصصة:

1) أحمد خليفة الملط , الجرائم المعلوماتية , ط 02, دار الفكر الجامعي, الاسكندرية , مصر,2006.

2)أحمد عوض بلال , مبادئ قانون العقوبات المصري , دون ط , دار النهضة العربية , القاهرة , 2012 .

3)أحمد محمود مصطفى , جرائم الحاسبات الآلية في التشريع المصري , دراسة مقارنة , ط01 , دار النهضة العربية للنشر و التوزيع , القاهرة , 2010.

4)أشرف السعيد أحمدي , القرصنة الالكترونية , دون ط , دار الفكر العربي , القاهرة 2010.

5)الحسيناوي علي جبار, جرائم الحاسوب و الانترنت , دون ط , دار اليازوري للنشر و التوزيع , عمان , الاردن , 2008.

6)آمال قارة , الحماية الجزائية للمعلوماتية في التشريع الجزائري , دون ط , دار الهومة للطباعة و النشر , 2006.

7)أيمن عبد الحفيظ , الإتجاهات الفقية لمواجهة الجرائم المعلوماتية , دون ط , دار النهضة العربية , القاهرة , 2005.

8) ختير مسعود , الحماية الجنائية لبرامج الكمبيوتر , دون ط , دار الهدى للنشر و التوزيع , 2010.

9)دلال صادق و حميد ناصر الفتال , أمن المعلومات دار اليازوري للنشر و التوزيع , الأردن , 2008.

10) سامي علي حامد عياد , الجريمة المعلوماتية و إجرام الانترنت , دون ط , دار الفكر الجامعي الاسكندرية ,2007.

11) عائشة بن قارة مصطفى , حجية الدليل الالكتروني, في مجال الاثبات الجنائي , دون ط , دار الجامعة الجديدة الاسكندرية , 2009.

12) عبد الصبور عبد القوي علي المصري, المحكمة الرقمية و الجريمة المعلوماتية , ط 01, مكتبة القانون و الاقتصاد , الرياض , 2012.

13) عبد الفتاح بيومي حجازي, مبادئ الاجراءات الجنائية في جرائم الكمبيوتر و الانترنت , ط01, دار الفكر الجامعي , الاسكندرية , 2006.

14) عبد الفتاح بيومي حجازي , مكافحة جرائم الكمبيوتر في القانون العربي النموذجي , دون ط , دار الفكر العربي , الاسكندرية , 2006.

15) عبد الله حسين علي محمود , سرقة المعلومات المخزنة في الحاسب الآلي , ط04, دار النهضة العربية للنشر و التوزيع, القاهرة 2010.

16) عبد الله عبد الكريم عبد الله , جرائم المعلوماتية و الانترنت ,ط 01, منشورات الحلبي الحقوقية , بيروت , 2017.

17) عميمر عبد القادر , التحديات القانونية لاثبات الجريمة المعلوماتية , دون ط , دار النشر الجامعي الجديد , 2021.

18) غادة النصار , الإرهاب و الجريمة الالكترونية , دار العربي للطبع و النشر , القاهرة مصر , 2017.

19) قدري عبد الفتاح الشهاوي , ضوابط التفتيش في التشريع المصري, دون ط , منشأة المعارف , الاسكندرية , 2005.

20) لينا محمد الأسدي , مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية , دراسة مقارنة , ط01, دار الجامد للنشر و التوزيع , عمان ,الاردن , 2015.

21) محمد أمين الشوابكة , جرائم الحاسوب و الانترنت , ط01, دار الثقافة للنشر و التوزيع , عمان , الأردن , 2009.

22) محمد علي العريان , الجرائم المعلوماتية , دون ط , دار الجامعة الجديدة للنشر و التوزيع , الاسكندرية , 2004.

23) زيبحة زيدان , الجريمة المعلوماتية في التشريع الجزائري و الدولي , دون ط , دار الهدى , عين مليلة , الجزائر , 2011.

القوانين و الأوامر :

1) الأمر رقم 04_150 المؤرخ في 2004/11/04 المعدل و المتمم للأمر رقم 66-150 الصادر في 08/ 1966/06 المتضمن ق.ع الجزائري ,ج.ر , العدد 71.

2) قانون رقم 06_22 المؤرخ في 2006/12/20 ,المعدل و المتمم للأمر 66_155 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية .

3) القانون رقم 09_04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام و الاتصال و مكافحتها , ج.ر, ع44.

الرسائل و الأطروحات:

1) عمر يوسف عبد الله , الإطار القانوني و المؤسساتي لمكافحة التقليد و القرصنة الإلكترونية , أطروحة دكتوراه في القانون الخاص , جامعة وهران 2 كلية الحقوق و العلوم السياسية و 2022.

2) فايز محمد راجح غلاب , الجرائم المعلوماتية في القانون الجزائري و اليمني, أطروحة دكتوراه , جامعة الجزائر 1, كلية الحقوق ,2010.

3) رصاع فتيحة , الحماية الجنائية للمعلومات على شبكة الانترنت و رسالة ماجستير في القانون العام , جامعة أبي بكر بلقايد ,وهران ,2012 .

المجلات و المقالات:

1. إسراء جبريل رشاد مرعي , الجرائم الاكترونية "الأسباب , الأهداف, طرق الحماية و معالجتها" , مجلة الدراسات الإعلامية , المركز الديموقراطي العربي ,ع01, يناير2018.
2. الحاج علي بدر الدين , القرصنة الرقمية كعائق تقني لنظام التقاضي المعلوماتي , مجلة البصائر للدراسات القانونية, و الاقتصادية , المركز الجامعي , مغنية الجزائر , العدد الخاص ,2021.
3. بولحية شهيرة و سويح ليندا , الاحتيال الالكتروني , مجلة الدراسات القانونية , المركز الجامعي سي حواس بريكة , ع04.
4. بن مالك اسمهان , خصائص الجريمة المعلوماتية و أسباب ارتكابها , مجلة البيان للدراسات القانونية و السياسية , كلية الحقوق و العلوم السياسية ,سطيف,م04,ع01, 2019/06/15.
5. سامية بوشوشة و حياة سليماني, التجسس الالكتروني و طرق مكافحته, مجلة العلوم الاجتماعية و الانسانية , جامعة باجي مختار عنابة , الجزائر ,م16, ع01, 2023/06/08.
6. شرف الدين وردة و بلجراف سامية , الجوانب الموضوعية و الاجرائية لمكافحة الجرائم المعلوماتية في التشريع الجزائري , مجلة المنار للبحوث و الدراسات القانونية و السياسية , م 02, ع03 ,ديسمبر 2017.
7. عبد السلام محمد و عادل محمد الشريجي و علي قابوسة , الجريمة الاكترونية في الفضاء الالكتروني , مجلة آفاق للبحوث و الدراسات ,م02, ع 02, 2019/07/31.
8. ليندا بن طالب , التفتيش في الجريمة المعلوماتية, مجلة العلوم القانونية و السياسية ,تيزي وزو , الجزائر , م08 , ع16, 2017.
9. مجدوب نوال , الآليات الإجرائية للكشف عن الجريمة المعلوماتية , مجلة البحوث القانونية و الاقتصادية , المركز الجامعي مغنية الجزائر , م06, ع03, 2022/11/09.

10. محمد خليفة , خصوصية الجريمة الإلكترونية و جهود المشرع الجزائري في مواجهتها, جامعة 08 ماي 1945, كلية الحقوق والآداب الاجتماعية , قالمة , م01, ع01, 2009/09/15.

11. مريم بالطة و آسيا برغيث , الأمن المعلوماتي في مواجهة القرصنة الإلكترونية , دراسات في حقوق الإنسان , جامعة 20أوت 1955, سكيكدة الجزائر , م06,ع01, 2022/06/30.

12. هبة صلاح الدين النموري , القرصنة الإلكترونية على مواقع الانترنت ,المجلة المصرية لعلوم المعلومات , مصر , م10,ع02, 2013/10/01.

الملتقيات والإتفاقيات :

1. ذياب موسى البداينة , الجرائم الإلكترونية (المفهوم و الأسباب), ملتقى الجرائم المستحدثة , في ظل التغيرات و التحولات الإقليمية و الدولية , كلية العلوم الاستراتيجية , عمان , الأردن , 2014.

2. جامعة الدول العربية , الاتفاقية العربية لمكافحة جرائم تقنية الانترنت ,ديسمبر 2010, رقم 185.

3. مجلس أوروبا , الافاقية الاوروبية لمكافحة الجريمة المعلوماتية ,23.

مذكرات الماستر:

1. راحراح شهرزاد ,جريمة القرصنة في التشريع الجزائري ,مذكرة ماستر تخصص قانوني جنائي و علوم جنائية , جامعة عبد الحميد بن باديس ,مستغانم , 2022.

المواقع الإلكترونية :

1) https://www.almaany.com/ ,تاريخ01|05|2024,الساعة 15:12

2) e3arabi.com , بتاريخ 2024/05/18 , 18:06

المراجع باللغة الأجنبية :

1) GABRIEL Hudson nkotago , internet fraud ,information for teachers and students ,Journal of international students ,vol 01 , issue 02 , nove;ber 2011, p 71 .

الفهرس

الفهرس

مـلخص مذكرة الماستر

يهدف هذا البحث إلى فهم جريمة القرصنة الإلكترونية , التي تعد من أخطر جرائم المعلوماتية ,و السبل التي لجأ المشرع الجزائري إليها لمكافحتها نظرا لخطورتها و تأثيراتها السلبية على الأنظمة المعلوماتية , بالتأثير غير المرغوب فيه على البيانات من إتلاف , حذف أو تغيير . حيث تطرقت في هذا البحث إلى مفهوم جريمة القرصنة الإلكترونية بشكل عام بالإضافة إلى المكافحة الموضوعية و الإجرائية التي اعتمدها المشرع الجزائري لردعها.

الكلمات المفتاحية:

1/القرصنةالإلكترونية 2/الجريمة المعلوماتية 3/الأمن السيبراني 5/مكافحة الجرائم السيبرانية 6/النظام المعلوماتي

Abstract of Master's Thesis

This research aims to understand the crime of electronic piracy, which is considered one of the most serious information crimes, and the methods that the Algerian legislator has resorted to to combat it due to its seriousness and negative effects on information systems, through its undesirable impact on data, such as destruction, deletion or change. In this research, I touched on the concept of the crime of electronic piracy in general, in addition to the objective and procedural control adopted by the Algerian legislator to deter it.

Keywords:

1/electronic piracy 2/cybercrime 3/cybersecurity 4/combating cyber crimes 5/ information system