وزارة التعليم العالي والبحث العلمي

الجامعة الإفريقية العقيد أحمد دراية- أدرار-

كلية العلوم الاجتماعية والإنسانية والإسلامية

قسم : العلوم الإنسانية تخصص: اتصال (صحافة مطبوعة وإلكترونية)

مذكرة لنيل شهادة ماستر في العلوم الانسانية

تحت عنوان:

آليات مكافحة الجريمة الالكترونية في القانون الجزائري

من إعداد الطالبتين

- **بن جدو فاطمة الزهراء**
- **كوكي حياة**

تحت إشراف:

_ أ/د كوار فوزية

لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
كوار فوزية	أستاذ محاضر	مشرفا ومقررا
كعواش عبد الحميد	أستاذ محاضر	رئيسيا
بايشي عبد الحميد	أستاذ محاضر	مناقشا

الموسم الجامعي2022/2021

الجمهورية الجزائرية الديمقراطية الشعبية
People'sDemocraticRepublic of Algeria

وزارة التعليم العالي و البحث العلمي
جامعة احمد دراية- ادرار
المكتبة المركزية
مصلحة البحث الببليوغرافي

Ministry of Higher Education and Scientific Research
University Ahmed Draia of Adrar
The central library

شهادة الترخيص بالإيداع

انا الأستاذ(ة): بن دية يمينة

المشرف على مذكرة الماستر الموسومة بـــ : أثر الديون المتعثرة على المقدرة التمويلية للبنوك الجزائرية دراسة تحليلية للفترة 2006-2018

من إنجاز :

الطالب(ة) صنقلي بسمة
الطالب(ة) مبروكي صالحة

كلية :العلوم الاقتصادية والتجارية وعلوم التسيير

القسم : العلوم الاقتصادية

التخصص: اقتصاد نقدي وبنكي

تاريخ تقييم / مناقشة: 2022/06/20

أشهد ان الطلبة قد قاموا بالتعديلات والتصحيحات المطلوبة من طرف لجنة التقييم / المناقشة، وان المطابقة بين النسخة الورقية والإلكترونية استوفت جميع شروطها. وبإمكانهم إيداع النسخ الورقية (02) والاليكترونية (PDF).

امضاء المشرف:

ادرار في :.....

مساعد رئيس القسم:

ملاحظة :لاتقبل أي شهادة بدون التوقيع والمصادقة.

وزارة التعليم العالي والبحث العلمي

الجامعة الإفريقية العقيد أحمد دراية– أدرار–

كلية العلوم الاجتماعية والإنسانية والإسلامية

قسم : العلوم الإنسانية تخصص: اتصال (صحافة مطبوعة وإلكترونية)

مذكرة لنيل شهادة ماستر في علوم الاعلام والاتصال

تحت عنوان:

آليات مكافحة الجريمة الالكترونية في القانون الجزائري

من إعداد الطالبتين: تحت إشراف:

- بن جدو فاطمة الزهراء _ أ/د كوار فوزية
- كوكي حياة

لجنة المناقشة:

كعواش عبد الحميد	أستاذ محاضر	رئيسا
أ.د كوار فوزية	أستاذ محاضر	مشرفا ومقررا
أبا لحبيب عبد القادر	أستاذ محاضر	مناقشا

الموسم الجامعي:2022/2021

إهداء

نهدي ثمرة هذا العمل المتواضع إلي :

إلى والدي رحمه الله والى والدتي أطال الله في عمرها

والى أخواتي بالإضافة إلى كل من ساهم وساعد في بناء هذه المذكرة من قريب أو من بعيد

فاطمة الزهراء

إلى شرايين القلب النابض الذي احتضنني بشوق واحتراق إلى التي لا أجد لذة العيش إلا بجانبها ولا أجد السعادة إلا في فجر ابتسامتها أمي الغالية .

إلي الذي تكبد مشقة الحياة لإسعادنا إليك أيها الجبل الشامخ والرجل النموذج الذي احمل اسمه بكل افتخار أبي الغالي .

إلي النجوم التي تتلألأ في سماء منزلنا إخوتي الأعزاء.

حياة

شكر و عرفان

الحمد لله الذي بنعمته تتم الصالحات

أولا نحمد الله ونشكره على توفيقنا في انجازنا لهذا العمل

بعد شكر الرحمان نتقدم بجزيل الشكر والعرفان وكثير الثناء والامتنان

إلي الأستاذ المشرف *كوار فوزية*شاكرين أياها على كل ما قدمته لنا حتى زالت العقبات والصعاب ، جزاكي الله عنا كل خير و زادكي في الإحسان كما لا يفوتنا أن نشكر كل من مد لنا يد العون من أساتذة وإداريين والي اللجنة العلمية فائق التقدير والعرفان.

إلي اللواتي دخلنا قلبي بلا استئذان وملكنا الفؤاد و الوجدان إلي رفيقات دربي ومزيلات الكرب و الأحزان .. زهور ،إكرام ، فاطمة الزهرة ، سعاد .

إلي كل من لم يدخر جهدا في مساعدتنا،

إلي كل من ساهم في تلقيني و لو بحرف في حياتنا الدراسية .

حيلة ، فاطمة الزهراء

بسم الله الرحمن الرحيم

فهرس المحتويات

الإهداء .....

شكر وعرفان .....

فهرس المحتويات.....

فهرس الجداول .....

مقدمة .....أ-ب

مدخل الى الإشكالية.....**13**

الفصل الأول: الطبيعة الخاصة للجريمة الالكترونية واليات مكافحتها **21**

- الطبيعة الخاصة للجريمة الالكترونية.....21

1.تعريف الجريمة الالكترونية.....21

2.التطور التاريخي للجريمة الالكترونية.....24

3.خصائص الجريمة الالكترونية 26

4.أسباب الجريمة الالكترونية 29

5.أنواع الجرائم الالكترونية في القانون الجزائري.....30

6.أصناف الجريمة الالكترونية 36

7.دوافع الجريمة الالكترونية.....38

- اليات مكافحة الجرائم الالكترونية في القانون الجزائري.....42

8.تعريف القانون بصفة عامة.....42

9.إجراءات جمع الأدلة والبحث في الجريمة الالكترونية.....43

10.الصعوبات التي تواجه عناصر التحقيق عند البحث وجمع الأدلة.....48

11.المواجهة الموضوعية في إطار قانون العقوبات.....50

12.التصدي للجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....52

13.مكافحة الجريمة الالكترونية بموجب قانون الإجراءات الجزائية.....56

14.كيفية التصدي للجرائم الالكترونية من خلال القانون المدني.....57

الفصل الثاني: نماذج وإحصائيات عن بعض الجرائم ونتائج تحليل الاستبيان.....60

1.جريمة الاحتيال.....60

2.جريمة التجسس 60

3.جريمة التهديد والمضايقة 60

4.الجرائم الجنسية الواقعة عبر الانترنيت 61

5.جريمة انتهاك الآداب العامة الواقعة عبر الانترنيت 61

6.جريمة المطاردة 62

7.جريمة الاعتداء على الحياة الخاصة عبر الانترنيت 62

8.جريمة القذف والسب والتشهير عبر الانترنيت 63

9.جريمة السرقة الالكترونية 63

10. جريمة غسيل الأموال عبر المواقع الالكترونية 63

11.نماذج عن بعض الجرائم في أمريكا.....64

12.بعض الجرائم الواقعة في الجزائر 65

13.إحصائيات عن بعض الجرائم في الجزائر.....67

14.تحليل الاستبيان ونتائجه.....67

خاتمة 76

قائمة المصادر والمراجع 80

الملاحق .....

فهرس الجداول

الرقم	عنوان الجدول	الصفحة
01	يوضح عينة الدراسة حسب متغير السن	
02	يوضح عينة الدراسة حسب متغير المستوى التعليمي	
03	يوضح نسبة الجهود المبذولة للحكومة والسلطة لمنع الجرائم الالكترونية .	**68**
04	يوضح نسبة خطورة الجريمة الالكترونية .	**68**
05	يوضح الأسباب الرئيسية التي تجعل الشباب يرتكبون مثل هذه الجرائم .	**69**
06	يوضح مدى نسبة تلقي التهديد الالكتروني للعينة.	
07	يوضح عدد الأفراد الذين لديهم فكرة عن الجرائم الالكترونية .	**70**
08	يوضح نسبة معرفة الأفراد للرقم الخاص بالابتزاز الالكتروني .	**70**
09	يوضح مدى تعدي الجريمة الالكترونية النطاقات الواسعة وتأثيرها على البنوك والمؤسسات .	
10	يوضح نسبة انتشار السرقات العلمية والتي تعتبر خطورة من مخاطر الجريمة الالكترونية .	**71**
11	يوضح نسبة إقبال الفرد على أن الحماية في المواقع كافية لاختراق وسرقة البيانات	**71**
12	يوضح نسبة مدى علم الأفراد بوجود إجراءات وقائية تمنع الوقوع ضحية لهذه الجرائم .	**72**
13	يوضح نسبة إجابات الأفراد عن السؤال أن الشباب مسئولون عن الاضطرابات والجرائم التي تحدث في المجتمع.	**72**
14	يوضح مدى إقبال الأفراد على أن عقوبة السجن تكفي للحد من الجرائم الالكترونية .	**73**
15	يوضح دور الفرد في مكافحة الجريمة الالكترونية .	**74**

16	يوضح مدى نسبة تمتع المجتمع الجزائري بالثقافة القانونية اتجاه الجريمة الالكترونية .	**74**

مقدمة

مقدمــة

تطور العالم بفضل التكنولوجيا الحديثة حيث عزت الإنترنت العالم وانتشرت بشكل واسع وسريع في العصر الحالي فقد باتت هذه الأخيرة المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات تعتمد عليها في أداء عملها بشكل أساسي وعلى استخدام أنظمة المعلومات لما تتميز بهما من عنصرين السرعة والدقة في تقديم المعلومات ونقلها وتبادلها، وهذا ما جعلها أيضا ضرورة من الضروريات لكل مواطن في الحياة اليومية على المستوى المعيشي لتسيير شؤون الحياة كالتواصل وتبادل المعارف فلا يقف أمامها أي عائق مادي أو جغرافي ولكن على الرغم من المزايا الهائلة التي تحقق بفضل هذه التقنية على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة إلا أن هذه الثورة التكنولوجيا المتنامية صاحبتها في المقابل مجموعة من الانعكاسات السلبية التي تسيء وتلحق الضرر بالفرد والجماعة والتي كان سببها فئة تستغل وسائل الإعلام والمواقع الالكترونية ومواقع التواصل الاجتماعي وتنشط فيه للأركاب جرائمها وهذه الفئة تسمى بـ "المجرم ألمعلوماتي" فيقوم هذا الأخير بالاعتداء على الأشخاص عن طريق الوسائل الإلكترونية بهدف الابتزاز و تشويه سمعة الضحية من اجل تحقيق مكاسب مختلفة فمن هنا ظهرت الجرائم المعلوماتية أو الجرائم الإلكترونية كما يطلق عليها البعض والمقصود بها الجرائم التي ترتكب ضد الفرد أو الجماعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية أو التسبب بالأذى الجسديّ أو النفسي لصاحبه بشكل مباشر أو غير مباشر باستخدام شبكة الاتصال الحديثة (غرف الدردشة، البريد الإلكتروني..).

ومن أجل الحد من خطورة الجرائم الإلكترونية اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بـ "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب

المادة 02 من القانون 09 /04 المؤرخ في 05 غشت 2009 على أنها جرائم المساس بأنظمة المعالجة الآلية المحددة في قانون العقوبات، وقد قام القانون الجزائري بوضع تشريعات عقابية تتجاوب مع التطورات الإجرامية على أمل الحد من هذه الجرائم.

للبحث في هذه الدراسة اخترنا خطة اعتمدت فيها على تقسيم موضوع البحث إلى فصلين:

جانب نظري: شمل الفصل الأول عنصريين أساسيين كل عنصر احتوى عدة عناصر بالنسبة للعنصر الأساسي الأول احتوى التعريف بالجريمة الالكترونية، أنواعها وخصائصها والدوافع، اما العنصر الأساسي الثاني احتوى على الآليات التي تتم بها مكافحة الجرائم الالكترونية في القانون الجزائري.

جانب تطبيقي: شمل الفصل الثاني على التعريف ببعض الجرائم وبعض النماذج عنها وإحصائيات للجريمة الالكترونية في الجزائر إضافة إلى الاستبيان والنتائج المتحصل عليها .

مدخل إلى الإشكالية

المدخل

ظهور شبكة الانترنيت والتطور الحاصل في وسائل الإعلام والاتصال بكل ما تحمله من تطور وتقدم، وبقدر ما أحدثته من أثار إيجابية ،بقدر ما كان لها آثر سلبي على حياة الناس ومصالح الدول وكل هذا كان نتيجة إدخال وحشر الانترنيت والوسائل الإلكترونية في شؤوننا الحياتية و اليومية والذي أسفر عن ذلك وجود الجرائم الإلكترونية بشتى أنواعها فتطلب هذا تدخل القانون ووضع تشريعات عقابية للحد من هذه الجرائم، ومن هذا الصدد نطرح الإشكالية التالية:

ماهي التدابير والوسائل التي تبناها المشرع الجزائري لمعالجة هذه المشكلة؟ أو بصيغة أخرى ماهي الآليات الكفيلة التي اتخذها القانون الجزائري لمكافحة الجرائم الإلكترونية؟

ومن هذه الإشكالية تتفرع عدة تساؤلات منها:

- ما المقصود بالجريمة الإلكترونية؟ وما هو المجرم ألمعلوماتي؟
- ماهي الصعوبات التي تقع عائق في سير البحث في هذه الجرائم؟
- ما هو الإجراء الذي يقوم المحقق به للبحث أو التحري عن الجريمة الإلكترونية؟
- ماهي الحلول الوقائية الفاعلة التي يجب على المشرع الجزائري أن يقوم بها لمكافحة أو الحد من هذه الآفة الاجتماعية المستحدثة؟

الفرضيات:

- الجريمة الإلكترونية تتمثل في اعتداء معلوماتي يقوم فيه الجاني باستخدام وسائل اتصال حديثة بهدف ابتزاز الضحية وتشويه سمعتها وما إلى ذألك سواء بغرض تحقيق مكاسب مادية أو سياسة.

- صعوبة الكشف عن الجريمة و الوصول الى الجناة، بالإضافة إلى عدم القدرة على إثبات هذه الجريمة إلا بعد مدة من التحقيق لعلاقتها بالعالم الافتراضي، أيضا إمكانية المجرم أن يمحو أو يغير البيانات أو المعلومات.
- توجد العديد من البرمجيات التي تساعد المحققين في جمع الأدلة بشكل أسرع من أهمها الوسائل المادية (العناوين، البريد الإلكتروني..) نظام الكشف عن الاختراق..
- إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، رفع مستوى الوعي العام اتجاه مخاطر الانترنت ونتائجها.
- سن نصوص تتماشى مع تطورات هذه الأخيرة وتتأقلم مع تغيراتها .

أسباب اختيار الموضوع:

- **الأسباب الذاتية:** أن الجريمة الإلكترونية موضوع مستجد يمس الواقع الاجتماعي، بالإضافة إلى فضولي في معرفة هذه الجرائم كونها متعلقة بالعالم الافتراضيّ، وأيضا التعرف على هذه الجرائم والحلول المقترحة من طرف المشرع الجزائري لمواجهتها.
- **الأسباب الموضوعية:** تبحث هذه الدراسة في مفهوم الجريمة الإلكترونية والمشكلات الموضوعية والإجرائية المتعلقة بها وكذألك الحلول التشريعية والعملية لمواجهة هذه الآفة الاجتماعية المستحدثة لأنها مست الواقع المعاش.

أهمية الموضوع: التعريف بظاهرة جديدة هي الجرائم الإلكترونية التي باشرت بالانتشار والتوسع دون سابق إنذار، مما أسفر عن ضرورة تتبعها والتعامل معها سواء من الناحية

التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات، أو سواء من الناحية القانونية وهي مهمة المشتغلين بالقانون، مما استدعى دراسة هذه الظاهرة باعتبارها غير معروفة في القانون وبعض المجتمعات ومساسها بمصالح الدولة.

الدراسات السابقة: استعنت في بحثي هذا ببعض الدراسات التي لامست بشكل كبير موضوعي، نذكر منها على وجه الخصوص:

الدراسة الأولى:"الجريمة الالكترونية في التشريع الجزائري" أثبتت أنعدم إجماع الفقهاء على تعريف موحد للجريمة الإلكترونية يعود أساسا إلى الاختلاف حول تحديد نطاق هذه الجريمة، خصوصا أن البعض وسع كثيرا من نطاقها واعتبر أن كل فعل غير مشروع يكون للحاسب الآلي دورا فيه جريمة إلكترونية، وقد تبنى هذا الاتجاه المشرع الجزائري حيث نص على ذلك في القانون رقم09-04، وحدد نطاق الجريمة الإلكترونية الجريمة التي تمس بالنظام المعلوماتي، أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات، وهو توسيع لا يتفق وماهية الجريمة الإلكترونية، باعتبارها تستهدف بالدرجة الأولى الجانب البرمجي للنظم المعلوماتية.

-إن هذه الجريمة مع تعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه، فإن لها جوانب سلبية خطيرة تهدد امن وسلامة الفرد والمجتمع تتسم بالغموض، حيث يصعب إثباتها والتحقيق فيها، مما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء.

-قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم 04- 15و المساس بمنظومة معلوماتية وبعض الأفعال الأخرى أفعال إجرامية وسطر لها عقوبات ، حيث اعتبر الدخول غير المشروع للنظام المعلوماتي

والبقاء فيه،/ واستدرك النقص المحال الإجرائي، بإصدار قانون رقم09-04 إذ تضمن قواعد إجرائية وأخرى وقائية وهذه خطوة إيجابية إلا أنها غير كافية لمواجهة خطر الجريمة الإلكترونية.

-إن المشرع الجزائري تطرق للجريمة الواقعة على النظام المعلوماتي، وأغفل الجرائم الماسة

بمنتوجات الحاسب الآلي، حيث لم ينص على جريمة التزوير المعلوماتي، وإنما أخضعها للنصوص التقليدية الخاصة بتزوير المحرر، ولم يوسع من مفهوم المحرر ليشمل المستند المعلوماتي.

- المشرع الجزائري لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي، وترك واسع ليدخل في نطاقها كلما تفرزه التقنية الجديدة وتطوراتها.

الدراسة الثانية: "مكافحة الجريمة المعلوماتية" توصلت هذه الدراسة إلى أنه لا يوجد لحد الآن مفهوم موحد بين الفقهاء حول الجريمة المعلوماتية، لذلك يجب دائما أن يرتكز مفهومها على فكرة عالمية المعلومات والاتصالات، حتى يكون هذا المفهوم واضحا على مستوى العالم، كما يجب أن يكون مواكبا دائما للتطور التكنولوجي المتلاحق والمؤثر في مفهوم هذه الجريمة، مع وجوب الأخذ بعين الاعتبار الخصوصيات التي تتميز بها الجريمة المعلوماتية، في تحديد مفهومها خاصة خاصية كونها جريمة متعدية الحدود وكون المجرم فيها ليس مجرما عاديا أو كالمجرم التقليدي، فهو غالبا ما يكون إنسانا متكيفا اجتماعيا وعلى مستوى معين من الثقافة العلمية.

إن تحديد أنواع الجرائم المعلوماتية يمكن استخلاصه من الأفعال التي تجرمها الدول أو الاتفاقيات الدولية باعتبارها جرائم معلوماتية أملا؟ فلحد الآن هناك جرائم معلوماتية مباحة

في بلدان ومجرمة في بلدان أخرى، لذلك تظهر صعوبة تحديد أنواع هذه الجريمة وأقسامها، غير أن النتيجة المتفق عليها بين غالبية الدول والمنظمات العالمية والاتفاقيات هي أنه توجد تقسيمات متفق

عليها وهي تلك الجرائم المعلوماتية التي يكون الحاسب الآلي محلا لها، كجرائم الدخول والبقاء والاستعمال غير المصرح به للحاسب الآلي وجرائم الاعتداءات الواقعة على المعلومات كجرائم النسخ غير المشروع والقرصنة و للإتلاف المعلوماتي والغش والتزوير المعلوماتي وجرائم يكون الحاسب الآلي وسيلة أو أداة لارتكابها.

إن للجريمة المعلوماتية خصائص منفردة ومميزة عن غيرها من الجرائم التقليدية، لذلك وجدت معظم الدول نفسها مضطرة لإيجاد حلول لمواجهتها، وهذه الحلول كانت بتعديل النصوص التقليدية وتطويرها وتشريع نصوص جديدة حتى لا تترك سلوكيات مستهجنة ومجرمة دون عقاب، وفي نفس الوقت حتى لا تخرج عن مبدأ الشرعية الذي هو مبدأ مكرس عالميا وفي كل التشريعات العقابية.

إن الجريمة المعلوماتية جريمة خطيرة أو هي وباء القرن (21) الواحد والعشرين لآثارها الوخيمة ليس فقط على القطاعات المالية والتجارية والاقتصادية.

فما كان على هذه الدول إلا التشريع للتصدي لهذه الجرائم ومكافحتها ليس فقط الجرائم التي تمس الأموال بل حتى الجرائم التي تمس الحياة الخاصة للأشخاص.

إن المشرع الجزائر يرغم مواكبته للدول السباقة في مكافحة الجريمة المعلوماتية من الناحية الموضوعية والإجرائية إلا أنه لم يتناول الجرائم المعلوماتية بشكل واسع حيث نجده قد أغفل النص على تجريم بعض الجرائم المعلوماتية الحساسة والتي انتشرت بشكل

خطير في كل المجتمعات وحتى في المجتمع الجزائري وهي جرائم الاستغلال الجنسي للأطفال وتحريضهم على الدعارة والمخدرات عن طريق الشبكات المعلوماتية.

المنهج المتبع: طبيعة هذا الموضوع تتطلب المنهج الوصفي التحليلي وذألك لدراسة الطرق التي يتم بها مكافحة الجرائم الإلكترونية وكيفية التصدي لها في ظل القانون الجزائري فالمنهج الوصفي يتلاءم مع الموضوع لوصف المصطلحات والمفاهيم التي يتضمنها الجانب النظري، أما التحليلي استخدم للدراسة الميدانية لتفسير وتحليل الفرضيات وكذا استخلاص نتائج الاستبيان.

أداة جمع البيانات:

الاستبيان: والذي هو أداة بحث تتكون من مجموعة من الأسئلة تهدف إلى جمع المعلومات من المستجيب للحصول على نتائج .كما قمنا بتوزيع مجموعة من الاسئلة على 20 شخص وزعت بين 17 و18 /2020/05 بجامعة احمد دراية وثانوية احمد ديدي وان هذا الاستبيان يهدف الي معرفة مدى تأثير الجريمة الالكترونية على المجتمع المعلوماتي ومعرفة الاسباب الناجمة عن ارتكاب الجريمة الالكترونية فعلى الرغم من هذا الا اننا لا يمكننا ان نفهم مختلف جوانب بحثنا هذا دون التطرق الي نماذج تطبيقية واقعية وهي طرح مجموعة من الاسئلة على الاشخاص وتكون على اساس ان المعالجة النظرية تبقى شاملة وعامة حتي يتم التطبيق عليها ، لتأكيد من صحة الجوانب النظرية .

الكلمات المفتاحية:

الجريمة / الجريمة الالكترونية /المجرم المعلوماتي / مكافحة/ التشريع / الآليات

الجريمة: هي الإتيان بفعل منتقض مع المعايير الجمعية والقانونية والدستور أيضا .والتي يتم العقاب عليها عند فعله.

الجريمة الالكترونية: تم ارتكابها بطريقة مباشرة وغير مباشرة واستغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة ومصلحة الفرد الخاصة.

المجرم ألمعلومـاتي : هو الذي يقوم بالتطفل على الحياة الخاصة للغير مستخدما في ذلك برنامج فيروسي أو وسيلة أخرى للوصول إلى معلومات عن الغير لاستخدامها ضده بغية تحقيق مصالح معينة.

مكافحـة: محاربة الشيء ومقاومته ردعه أو القضاء عليه.

التشريــع : هو مجموعة من القواعد القانونية المكتوبة العامة الملزمة المجردة التي تصدرها السلطة العامة المختصة في الدولة بهدف تنظيم العلاقات وسلوك الأفراد في المجتمع

الآليـــات أو الطرق: هي الأساليب التي اتخذت للحد من الجريمة وذلك باستخدام عقوبات جنائية كوسيلة لردع الناس من ارتكاب الجرائم.

الجانب النظري

الفصل الأول: الطبيعة الخاصة للجريمة الإلكترونية و آليات مكافحتها في القانون الجزائري

- **الطبيعة الخاصة للجريمة الالكترونية**

تعتبر شبكة الإنترنت أضخم شبكة كمبيوتر على مستوى العالم، تندمج فيها كل من تكنولوجيـــــا الحاسب الآلي مع تكنولوجيـــــا الاتصالات، الأمر الذي جعلها مهمة بحيث لا يمكن الاستغناء عنها في كثير من المجالات سواء كانت تجارية أو علمية بحثية أو خدمية أو مصرفيـــــة.

ولكن هذا التطور التكنولوجي الهائل لا يمكن أن ننظر إليه من جانب إيجابي فقط حيث أن ازدياد العمل به أدى إلى إفراز جانب سلبي لا يمكن إغفاله أو غض النظر عنه، وهذا الجانب هو الجرائم الإلكترونية.

العنصر الأول: تعريف الجريمة الالكترونية:

لم يتفق الفقه الجنائي على إيراد تسمية موحدة لجريمة الالكترونية فهناك عدة تسميات لها منها الجريمة المعلوماتية ،جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ، جرائم الكمبيوتر والانترنت ،الجرائم المستحدثة ،الجريمة الناعمة ،إجرام ذوي الياقات البيضاء وقد انقسم الفقهاء إلى اتجاهين ، منهم من ينظر إلى تعريف الجريمة الالكترونية بمفهوم ضيق ،ومنهم من ينظر إليها بمفهوم واسع وسأحاول التعرض لهذه التعارف من خلال الاتجاهين المواليين[1]:

[1] عادل يوسف عبد النبي الشكري ، بحث بعنوان : الجريمة المعلوماتية وازمة الشرعية الجزائية ، جامعة الكوفة 2008، ص 112.

أولا: الاتجاه المضيق من تعريف الجريمة الالكترونية :

يعرف أنصار هذا الاتجاه الجريمة الالكترونية بأنها ،كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الإلية بقدر كبير لازم لارتكابه من ناحية ،لملاحقته وتحقيقه من ناحية أخرى . حسب هذا التعريف يجب أن تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة ،بل كذلك لملاحقتها ،والتحقيق فيها .وهذا التعريف يضيق بدرجة كبيرة من الجريمة الالكترونية بمعنى يجب أن يتوفر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة ،والمتخصصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها الفعل غير المشروع الذي يتورط فيه ارتكاب الحاسوب ،أوهي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية. حسب هذا التعريف فان الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم . ويرى الأستاذ بار كار أن الجريمة الالكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشا عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل.

.ثانيا: الاتجاه الموسع من تعريف الجريمة الالكترونية:

على عكس الاتجاه السابق ، يرى فريق أخر من الفقهاء ضرورة التوسع من مفهوم هذه الجريمة وبالتالي هي جريمة تتم بوسيلة الكترونية كالحاسوب مثلا ، وذلك باستخدام شبكات الانترنت من خلال غرف الدردشة ، واختراق البريد الالكتروني ومختلف وسائل التواصل الاجتماعية ،بهدف إلحاق الصرر لفرد ومجموعة من الأفراد ، وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي ، أو الاقتصادي ، أو الإصرار بسمعها آو العكس ويبقى الهدف واحد ، وهو الكشف عن قضايا متستر عليها ، أو نشر معلومات لفائدة طرف او إطراف أخرى من باب التسريب . ودائما حسب أنصار هذا الاتجاه يرى البعض أن الجريمة الالكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن

لديه معرفة بتقنية الحاسوب نظاما حاسوبيا أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها أو تجريبها، وجعلها غير صالحة، أو حيازتها أو توزيعها بصورة غير مشروعة[1].

ومن خلال هذه التعريف يتضح لنا صعوبة قبول هذا التوجه، لان جهاز الحاسوب الآلي قد لا يغدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، ومن ثم لا يمكن إعطاء وصف للجريمة الالكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة الالكترونية، كما انه قد ترتكب الجريمة ويستعمل الحاسب الآلي ولا نكون أمام جريمة الكترونية، كما يقوم الاتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك.

أما بالنسبة لتعريف القانوني للجريمة الالكترونية. فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 2من القانون 4 و9 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكررالى394 و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية.[2]

وحسب المشرع الجزائري: فانه قد تتحقق الجريمة الالكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الالكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الالكترونية يندرج ضمن مصطلح المنظومة المعلوماتية. ومن

[1] محمد امين احمد الشوابكة ، جرائم الحاسوب والانترنت ، مكتبة دار ثقافة لنشر والتوزيع ، عمان الاردن ، 2004، ص8-9.

[2] القانون رقم 09-04 ، الصادر في 05 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، ج ر العدد 47.

أمثلة الجريمة الالكترونية المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي القي عليه القبض من طرف الشرطة الفيدرالية الأمريكية.[1]

العنصر الثاني :التطور التاريخي للجريمة الالكترونية

يتجلى صراع الإنسان من اجل حاضره ومستقبله في حاجته الدائمة الي اتخاذ القرارات السلمية، وتتوقف صحة القرارات علي مدى توفر المعلومات المتصلة بالمشكلة المطروحة، ومن هنا يكمن الدافع الأساسي وراء حرص الإنسان علي تجميع المعلومات المرتبطة بالإنجازات السابقة وأهمية تنظيمها[2] ومفهوم جريمة الكومبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ويمكن تقسيمها الي ثلاثة مراحل:

المرحلة الأولي: من شيوع استخدام الكومبيوتر في الستينات ومن ثم السبعينات:

بظهور استخدام الكومبيوتر وربطه بالشبكة في الستينات الي السبعينيات ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكومبيوتر والتجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة وظاهرة إجرامية مستجدة؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسيع الدراسات تدريجيا وخلال السبعينات بدا الحديث عنها كظاهرة إجرامية جديدة.

[1] سوير سفيان ، جرائم المعلوماتية مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، جامعة ابو بكر بلقايد ، تلمسان ، 2010-2011 ، ص16/14.

[2] حسن مكاوي : تكنولوجيا الاتصال الحديثة في عصر المعلومات ، الدار المصرية اللبنانية ، القاهرة ، ط4 ، 2005، ص 28.

المرحلة الثانية: في الثمانينات:

وفي الثمانينات ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكومبيوتر، الذي سبب تدمير الملفات والبرامج أين شاع اصطلاح "الهاكرز"، المعبر عن مقتحمي النظم وبقي دائما الحديث عن دوافع هذه الجرائم محصور في اختراق امن المعلومات وإظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذه المجال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم خاصة بعد تحول الجريمة من مجرد مغامرة وإبداء التفوق آلي أفعال تستهدف التجسس والاستيلاء على البيانات الاقتصادية والاجتماعية والسياسية والعسكرية.

المرحلة الثالثة: في التسعينات

التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أنماط جديدة كأنشطة إنكار الخدمة، التي تقوم علي فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد شهدت مواقع الانترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر مواقع الانترنت لما تسهله من انتقادها آلي الملايين المستخدمين[1] في ذات الوقت ،وظهرت أنشطة الرسائل والمواد الكتابية المنشور علي الانترنت أو المرسلة عبر البريد الالكتروني، المنطوية علي إثارة الأحقاد أو المساس

[1] يونس عرب جرائم الكمبيوتر والانترنت –ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحظة والاثبات، ابوظبي 2002/12/12، ص08.

بكرامة واعتبار الأشخاص أو المستهدفة الترويج لمواد غير قانونية وغير مشروعة (جرائم المحتوي الضار).

العنصر الثالث : خصائص الجريمة الالكترونية .

تعد جرائم المعلوماتية إفرازا ونتاجا لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما اكسبها لونا وطابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من السمات، قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فان اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية.

أن متابعة جرائم الحاسب الآلي والانترنت والكشف عنها من الصعوبة بمكان حيث أن هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها، وتعود أسباب صعوبة إثبات جرائم الحاسب الآلي الي خمسة أمور هي:

أولا: أنها كجريمة لا تترك أثرا لها بعد ارتكابها[1].

ثانيا: صعوبة الاحتفاظ الفني بآثارها أن وجدت.

ثالثا: أنها تحتاج آلي خبرة فنية ويصعب علي المحقق التقليدي التعامل معها.

رابعا: أنها تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها.

خامسا: أنها تعتمد على قمة الذكاء في ارتكابها.

[1] محمد عبد الله منشاوي ، جرائم الانترنت من منظور شرعي وقانوني ، ص11، الجمعية الدولية للمترجمين تاريخ 2020/8/22.

كما أن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت، أضفى عليها مجموعة من الخصائص والسمات التي ميزتها عن الجرائم التقليدية ولعل من أهمها ما يلي:

1 –الجرائم المعلوماتية جرائم ترتكب عبر شبكة الانترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم.

2–الجريمة المعلوماتية جريمة عابرة للحدود فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهو ما يعني أن مساحة مسرح الجريمة المعلوماتية لم تعد محلية، بل أصبحت عالمية، الأمر الذي خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة الي إشكاليات تتعلق بالإجراءات الملاحقة القضائية، وغير ذألك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[1].

3–صعوبة إثبات الجريمة الالكترونية نظرا لارتكابها في الخفاء، وعدم وجود أي اثر ايجابي لما يجرى خلال تنفيذها من أفعال إجرامية، حيث يتم نقل المعلومات الكترونيا، أضف الي ذلك أحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجني عليها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.[2]

[1] رصاع فتيحة : الحماية الجنائية المعلومات ، مذكرة ماجستير منشورة ، تخصص القانون العام ، جامعة ابو بكر تلمسان ،2011-2012 ص43.

[2] محمد علي العريان : الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، 2004، ص 53.

4- ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية، فقد أكدت "انتل سيكيوريتي" الشركة العالمية المتخصصة في تقنيات حماية وامن المعلومات، أن قطاعات الأعمال العالمية تتكبد خسائر سنوية تصل الي400 مليار دولار أمريكي، وأوضحت الشركة أن الهجمات الالكترونية أصبحت اقتصادا متناميا قائما بذاته تبلغ قيمته ما بين 2الي3 ترليون دولار سنويا، أو ما يشك15الي20 من القيمة الاقتصادية الناتجة عبر الانترنت ، وقد تكبدت شركة بريطانية خسائر بلغت 1,3 مليار دولار بسب هجوم الكتروني واحد، وخسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة، وأعلنت الهند عن تعرض 308371 موقعا الكترونيا للاختراق بين العامين 2011و2013.

5- الصورة التقليدية للمجرم تكاد في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي آلي مستوى اجتماعي مرتفع عن غيره من المجرمين، ونادرا ما يكون محترفا للإجرام أو عائدا، كما انه لا ينظر إليه كمجرم بالمعنى المتعارف لهذه الكلمة وذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية[1].

6- قلة الإبلاغ عن وقوع الجريمة المعلوماتية وذلك راجع لسببين، أولهما: هو الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، أو بعد فترة طويلة من ارتكابها، والسبب الثاني: هو عدم اكتشاف الضحية للجريمة ، مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها.[2]

[1] سوير سفيان : جرائم المعلوماتية ، تخصص العلوم الجنائية والاجرام ،جامعة ابو بكر بلقايد ،تلمسان 2011-2012، ص19-18 .

[2] خالد ممدوح : امن الجريمة الالكترونية ، الدار الجامعية 2008، ص 51.

إذا فالجريمة الالكترونية من احدث أنواع الجرائم، مسرحها العالم الافتراضي غير الملموس، بعيدة عن أي مظهر من مظاهر الجريمة التقليدية، هي جريمة معلومة عابرة للحدود، ينفذها مجرمون من الطراز العالي، أذكياء ومتميزون تقنيا، مما يؤدي الي تشتيت الجهود الدولية في محاولة تعقبها أو التحري عنها، أو الوصول آلي مرتكبيها.

العنصر الرابع: أسباب الجريمة الالكترونية:

هناك عدة أسباب أدت الي ظهور وانتشار الجريمة الالكترونية نذكر منها ما يلي:

ب1:الانبهار بالتقنية المعلوماتية .

مع ظهور التقنية المعلوماتية وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو الحواسب فان الأمر في النهاية يؤدي آلي انهيار المجرمين بهذه التقنية الحديثة. لذلك فان هؤلاء ليسوا علي جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة.

ب2: الرغبة في تحقيق الثراء السريع .

قد تدفع الحاجة البعض الي تحقيق الثراء السريع عن طريق إتاحة الاطلاع علي معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب الأزمة للوصول الي هذا الهدف المنشود، ولذلك فان هذا السبب يعد من أكثر الأسباب التي تدفع الي انتشار الإجرام الالكتروني، بحيث تظهر الحاجة الي تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات).

ب3: الأسباب الشخصية .

يتأثر الإنسان في بعض الأحيان ببعض مؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توفر هذه المؤتمرات، فان الأمر يؤول في النهاية الي ارتكابهم للجريمة المعلوماتية، هذا وتتعدد المؤثرات التي تدفع الإنسان الي اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الحقد أو الانتقام.

تبدأ الرغبة لدى الشباب نحو العبث بالأنظمة المعلوماتية من اجل ممارسة هواية اللعب، أو تعود الي وجود ميل زائد لدى البعض بان الاعتقاد بان كل شيء يرجع إليهم، إذن تلك تمثل آفة نفسية تصيبهم ويفتخرون بما قاموا به من جرائم، ليظهر وتفوقهم علي الأنظمة المعلوماتية، وقد يكون الدافع نحو ارتكاب الجريمة المعلوماتية هو عامل الانتقام، وذلك عندما يتم فصل العامل من عمله فان ذلك من شانه أن يهيئ له مناخ لجريمته، كان يدمر البرامج المعلوماتية بالفيروسات عن طريق زراعتها.[1]

العنصر الخامس: أنواع الجرائم الالكترونية في القانون الجزائري .

عرفت الجريمة الالكترونية اختلاف حول تقسيمها، وذلك بسب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة ،والبعض الأخر يستند إلى دوافع ارتكابها وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه. إما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الثاني

[1] مصطفى سمارة ، الجريمة الالكترونية –مجلة المعلوماتية ، العدد 29 شهر 2008.

من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات، وهذا ما سيتم ذكره في العناصر التالية[1]:

أولا : الجريمة الالكترونية المرتكبة باستخدام النظام المعلوماتي .

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار.

الجريمة الالكترونية الواقعة على الأشخاص الطبيعية . تنقسم هذه الجرائم بدورها الي جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.[2]

1- الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية . يكون النظام المعلوماتي وسيلة الاعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتحزين واستخدام هذه المعلومات دون إذن صاحبها، لان استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق المعني، إضافة إلى كونه اعتداء على قيمتها المالية كون أن المعلومة قيمة أدبية بجانب قيمتها المادية ،ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، اذ تمثل فكرة للمخترع تحتوي على حق معنوي وأخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الآمر رقم03- 05 الصادر في 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03- 07 الصادر في 2003 المتعلق ببراءات الاختراع[3].

[1] احسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الديوان الوطني للأشغال التربوية ، 2002، ص24.
[2] رصاع فتيحة ، رسالة الماجستير السابقة الذكر ، ص 69.
[3] سوير سفيان ، رسالة الماجستير السابقة الذكر ، ص33.

02- الجريمة الالكترونية الواقعة على حرمة الحياة الخاصة . لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين اكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بأعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعنى ولكن يقوم المكلف يحفظها باطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص أخر[1].

03-الجريمة الالكترونية الواقعة على النظم المعلوماتية الأخرى . تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز لمعالجة المعلوماتية، أو استخدام أداة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدم البطاقة الائتمانية . بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الاستيلاء علي المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة، واستخدام شاشة النظام. والاطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، إما الحالة الثانية تكون في حالة إساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية شروط العقد المبرم بينه

[1] سوير سفيان ، رسالة الماجستير السابقة الذكر ، ص34-35.

وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة صلاحيتها أو تم إلغاؤها، إما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات[1].

04- الجريمة الواقعة الالكترونية الواقعة على الأسرار. تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة وأسرار خاصة تتعلق بالجرائم الواقعة على أسرار الدولة، حيث أتاح الانترنت للكثير من الدول ممارسة التجسس على دول أخرى وذلك بالإطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي تكون فيها نزاعات، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر ويستخدمها للضغط على أصحابها من اجل القيام بعمل والامتناع عن القيام بعمل. وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح صد الشيء العمومي . من المادة 61الى 96مكررمن قانون العقوبات .

05-الجريمة الالكترونية الواقعة على النظام المعلوماتي: من اجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04- 15الصادر في نوفمبر 2004، المتضمن قانون العقوبات بتحريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر إلى 07، وتأخذ صور الاعتداء صورتين وهما: الدخول

[1]. سوير سفيان ، رسالة الماجستير السابقة الذكر ، ص 35-36-37

والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تصمن صور أخرى للغش[1].

06-جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية:

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل وجزء من منظومة للمعالجة الآلية للمعطيات ويحاول ذلك، أو نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فان العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[2] .

01- فعل الدخول غير المشروع :لا نعني هنا الدخول بالمعنى المادي، أي الدخول آلي مكان معين وغيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول آلي فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي تقوم بها نظام المعالجة الآلية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سوء كان شخص يعمل في المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أو لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول الي النظام أو من الذين ليس لهم الحق في الدخول بطريقة التي دخلوا بها، كما تقع الجريمة سوء تم الدخول الي النظام كله أو إلى جزء منه فقط، أيأن الجريمة تقوم بفعل الدخول إلى النظام مجرد عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط وحصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوفر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل فنيات

[1].سوير سفيان ، رسالة الماجستير السابقة الذكر ، ص38.
[2]الامر رقم 04-15 ، القانون السابق الذكر.

الدخول الاحتيالي في منظومة محمية كانت وغير محمية، كما تشمل استعمال من لاحق له في ذلك المفتاح للدخول إلى المنظومة.

02- فعل البقاء غير المشروع : يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات صد إرادة من له الحق في السيطرة على هدا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقبلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تتحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فانه يعاقب على جريمة البقاء غير المشروع ، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له في الاطلاع فقط ،ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، التي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية[1].

- **جريمة المساس بمنظومة معلوماتية :**نص قانون العقوبات من معاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية وهذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال والمحو والتعديل كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوفر الركن المادي وأفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآنية للمعطيات، سوء

[1] حمزة بن عقون ، رسالة الماجستير السابقة الذكر ، ص182-183 .

بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من اجل إتلافها[1].

العنصر السادس: أصناف الجريمة الالكترونية:

لم يستقر الفقهاء علي معيار واحد لتصنيف الجرائم الالكترونية وذلك راجع آلي تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع الي وسيلة ارتكاب الجريمة، أو دافع، أو على أساس محل الجريمة، وعلى هذا يمكن تقسيمها الى[2]:

الجرائم الواقعة علي الأموال: في ظل التحول من المعاملات التجارية التقليدية آلي المعاملات التجارية الالكترونية، وما انجر عنه من تطور في وسائل الدفع والوفاء، وفي خصم التداول المالي عبر الإنترنت لشتى أنواع الجرائم ومنها:

السطو على أرقام بطاقات الائتمان والتحويل الالكتروني الغير مشروع .

القمار وغسيل الأموال عبر الانترنت .

جريمة السرقة والسطو علي أموال البنوك .

تجارة المخدرات عبر الانترنت .

[1] حمزة بن عقون ، نفس الرسالة ، 184.

[2] صغير يوسف ،الجريمة المرتكبة عبر الانترنت ، رسالة الماجستير في القانون ،جامعة مولود معمري تيزي وزو 2013،ص80,43.

الجرائم الواقعة علي الأشخاص :

مع تطور شبكة الانترنيت أصبحت المعلومات المتعلقة بلا فراد متداولة بكثرة عبرها، مما جعلها عرضة لانتهاك والاستعمال منصرف هؤلاء المجرمين وجعلت سمعة وشرف الأفراد مستباحة، ومن أهم هذه الجرائم ما يلي:

جريمة التهديد والمضايقة والملاحقة.

انتحال الشخصية والتغرير والاستدراج.

صناعة ونشر الإباحة.

جرائم القذف والسب وتشويه السمعة.

الجرائم الواقعة على امن الدولة: من أهم الجرائم الالكترونية التي تهدد امن الدول ومجتمعاتها ما يلي :

ا/ الجماعات الإرهابية: استغلت الكثير من الجماعات المتطرفة الطبيعية الاتصالية للإنترنيت من اجل بث معتقداتها وأفكارها، بل تعداه الأمر الي ممارسات تهدد امن الدولة المعتدى عليها.

ب /الجريمة المنظمة: استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والانترنيت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.[1]

[1] سامي علي حامد عياد، الجريمة المعلوماتية واجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية 2008، ص38.

ج /الجرائم الماسة بالأمن الفكري: يبقى الأمن الفكري من بين اخطر الجرائم المرتكبة عبر الانترنيت، حيث تعطى الانترنيت فرصا لتأثير علي معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

د/ جريمة التجسس الالكتروني: سهلت شبكة الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي[1].

العنصر السابع: دوافع ارتكاب الجريمة الالكترونية:

من خلال ما سبق يتضح لنا، أن الجريمة التقليدية والمجرم التقليدي يختلفان تماما عن الجريمة الالكترونية والمجرم الالكتروني، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع أي الباعث، الغرض أو الغاية مفاهيم لكل م0نها دلالته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة الالكترونية، وهي مسالة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الإجرامي، وأن الباعث لا اثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فأنها من حيث الدلالة تتمايز، فالدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام ،وهو إذن قوة نفسية تدفع الإرادة الي ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى. إما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي اصرف إليها القصد الجنائي أو الاعتداء على الحق الذي

[1] علي عدنان الفيل ، الاجرام الالكتروني ، منشورات زين الحقوقية ، 2011 ص،98,96.

يحميه قانون العقوبات. وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام، أو سلب مال المجني عليه في جريمة القتل.[1] وبالنسبة للجريمة الالكترونية فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم، واهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين:

.1/**الدوافع الشخصية لارتكاب الجريمة الالكترونية.** تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية ، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الالكترونية ، تأثير العنصر الذهني المعنوي على المجرم الالكتروني ودفعه لارتكاب جريمته .

الدوافع المادية . يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الالكترونية ، وذلك لان الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الالكتروني آلي تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الاختراق حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك اثر ورائه ، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية أن كان احد موظفيها، واختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحساب شركائه، أو لحساب من يعمل لحسابهم أن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب وفي حقيقة الأمر أن في حال نجاح المجرم الالكتروني في ارتكاب جريمته فان ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع

[1] حمزة بن عقون ، رسالة الماجستير السابقة الذكر ، 46-47.

من الجرائم من خلال احدث خلاصة لأحدى الدراسات الواردة بالتقرير السادس لمعهد امن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية ، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الالكترونية حيث تبين ان85 من المشاركين في الدراسة تعرض ولاختراقات بالنسبة للأنظمة المعلوماتية ، وان 64 لحقت بهم خسائر مادية جراء هذه الاعتداءات.[1]

2/الدوافع الذهنية لارتكاب الجريمة الالكترونية . تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي واثبات الذات .وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في التحدي وقهر النظام والتفوق على تعقيد وسائل التقنية ، فاختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه ، وعلى الصعيد أخر قد يكون إقدام المجرم الالكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الالكترونية والتغلب عليها، اذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي واثبات المقدرة.

الدوافع الموضوعية لارتكاب الجريمة الالكترونية.

قد يتأثر المجرم الالكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام الالكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، و يمكن إبراز أهم الدوافع من خلال الفرعيين المواليين:

[1]سعيداني نعيم ، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة نيل شهادة الماجستير في العلوم القانونية ' جامعة الحاج الاخضر ' باتنة 2012-2013، ص60-61 .

1/ دوافع الانتقام وإلحاق الضرر برب العمل.

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية ،فهذه الأمور تجعله يقدم على ارتكاب جريمته، كما يعتبر هذا الدافع من اخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك انه غالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الالكتروني الرغبة في الانتقام من رب العمل، ومثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه[1].

- **دافع التعاون والتواطؤ.** هذا النوع يتكرر كثيرا في الجرائم الالكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وأخر من المحيط وخارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكـــاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبـــــادل المعلومـــات بصفة منتظمة حول أنشطتهم.[2] وإذا كانت هذه ابرز الدوافع لارتكاب الجريمة الالكترونية ، مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لان السلوك الإجرامي والدوافع لارتكاب الجريمة الالكترونية قد تتغير وتتحول بسرعة من حالة العبث ومحاولة تحدى والتغلب على الأنظمة إلى تدميرها وعلى الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فان هذه الدوافع قد لا تتوقف عند هذا الحد، اذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الوحدة لها

[1] سعيداني نعيم ، رسالة الماجستير السابقة الذكر ص 61-62.
[2] صغير يوسف ، رسالة الماجستير السابقة الذكر ، ص 42.

دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة ..

- **آليات مكافحة الجرائم الالكترونية في القانون الجزائري**

تسعى كل دولة لمحاربة جرائم الإنترنت بتدخل المشرع لحمايتها من أي مساس بها سواءً عن طريق القول أو الكتابة، وقد اختلفت الأساليب التي لجأت إليها التشريعات في مختلف الدول في صياغة النصوص القانونية الخاصة بالجرائم المعلوماتية.

عملية المكافحة للجريمة المعلوماتية ضرورة حتمية يجب التصدي لها لمكافحة هذه الظاهرة واحتواء هذا النوع الجديد والخطير من الإجرام، ففي الجزائر قام القانون الجزائري بتعديل قوانين وإصدار قوانين عقابية جديدة أخرى تتصدى لمختلف أنواع الإجرام المعلوماتي الجديد.

العنصر الأول: تعريف القانون بصفة عامة

يرجع أصل كلمة معربة أخذت من الكلمة اليونانية *kanun* أو من الكلمة اللاتينية*kanun* ومعناها العصا المستقيمة أو النظام أو المبدأ أو الاستقامة في القواعد القانونية واستعملت كلمات أخرى تدل على نفس المعنى فاستعملت اللغة الانجليزية *Law* والفرنسية *Droit* ويتضح ممن ما سبق أن كلمة قانون تحمل معنى الاستقامة وتستخدم في المجال القانوني كمعيار لقياس مدى احترام الفرد لما تأمره به القاعدة القانونية أو تنهان عليه أو انحرافه عن ذلك فإذا هو سار وفقا لمقتضاه كان سلوكه مستقيما وان هو تمرد عنها كان سلوكه غير مستقيم[1].

[1] محمد سعيد جعفور، مدخل الى العلوم القانونية الوجيز في نظرية القانون الجزائر، دار هومة،2004،ص14.

فيعرف القانون على انه مجموعة من القواعد القانونية التي تنظم حياة المجتمع وسلوك الأشخاص فيه، أيا كان مصدر هذه القواعد أو الموضوع الذي تنظمه، فقد يكون مصدر القواعد القانونية التشريع أو سواه من المصادر الأخرى، وقد تنم هذه القواعد أمورا مدنية أو تجارية أو جزائية أو غيرها، ومع ذلك فإنها جميعها بصرف النظر عن مصادرها أو موضوعها هي التي يتكون منها القانون بمعناه العام الذي بيناه.[1]

العنصر الثاني: إجراءات جمع الأدلة والبحث في الجرائم الالكترونية

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسية في المعاينة والتفتيش والخبرة.

المعاينـــة:

وهي تتطلب أن ينتقل مأمور الضبط القضائي إلى مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء". هي إجراء جائز في كافة الجرائم إلا أن غالبية التشريعات "كالتشريع الجزائري في المادة 42 من ق إ ج ج و المادة 91 من ق إ ج المصري"، تقصرها على الجنايات والجنح الهامة بحيث تعد إجراء وجوبيا في الجنايات وجوازي في الجنح، وهي قد تتم في مكان عام أو مكان خاص.

والهدف من إجراء المعاينة هو ضبط ما استعمل في ارتكاب الجريمة أو ما نتج عنها ووضع الأختام في الأماكن التي أجريت فيها المعاينة، إذا وجدت آثار أو أشياء تفيد في

[1] هشام القاسم، المدخل الى علم القانون، الطبعة الخامسة، سوريا، منشورات جامعة دمشق،2003،ص،07-،06.

الكشف عن الجريمة كما يجوز لمأمور الضبط القضائي أن يعين حراسا على هذه الأماكن مع ضرورة إخطار النيابة العامة بهذه الإجراءات[1].

ونظرا لطبيعة هذه الجرائم وكيان بيئتها غير المحسوس تظهر صعوبة دور الشرطة في الكشف عنها ومتابعة مرتكبيها الأمر الذي أدى بالدول السباقة في مكافحة الإجرام ألمعلوماتي إلى إيجاد وحدات من الشرطة متخصصة بالعمل في هذا المجال، تكون مزودة بالخبراء المدربين وتنظيم دورات لهم للتخصص في مجال مكافحة الجريمة المعلوماتية، وذلك بتلقينهم المعلومات الخاصة بتقنية الحاسبات والجوانب الفنية، لها حتى تسهل عليهم عملية الكشف عن الجرائم ومنع وقوعها بإحكام الرقابة على المحلات العامة كنوادي الانترنت ...الخ، والتي تعد المجال الخصب لاقتراف جرائم المعلوماتية[2].

ولنجاح المعاينة يجب ما يلي:

- ✓ القيام بتصوير الحاسب وما قد يتصل به من أجهزة طرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة، وتصوير أجزائها لخلفية وملحقاته، مع مراعاة تسجيل زمان وتاريخ ومكان الذي التقطت فيه كل صورة.
- ✓ يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات(الخيوط الكهربائية للحاسب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليلها عند عرض الموضوع على المحكمة، عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة.

[1] طرشي نورة، مكافحة الجريمة المعلوماتية ،مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي ،الجزائر، كلية الحقوق ، جامعة الجزائر ،2012,2011،ص111

[2] نفس المرجع ،ص112.

- ✓ الاحتفاظ بما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.
- ✓ القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.
- ✓ يجب أن تقتصر عملية المعاينة على مأموري الضبط سواء كانوا من الباحثين أو المحققين ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[1].

-التفتيـش:

وردت من الناحية التشريعية تعاريف متعددة للتفتيش منها أنه "إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها فيمحل يتمتع بحرمة المسكن أو الشخص وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة[2] "كما عرف التفتيش أيضا على أنه "البحث في مستودع سر المتهم عن أشياء تفيد فيكشف الحقيقة ونسبتها إليه أو الاطلاع على محل منحه القانون

[1] د /هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية / دراسة مقارنة،–الطبعة الرابعة، أسيوط، مكتبة الآلات الحديثة،1994،ص114.

[2] هلالي عبد الله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، الطبعة الرابعة ، القاهرة ،دار النهضة العربية ، ،سنة 1994،ص 47

حماية خاصة باعتباره مستودع سر صاحبه ويستوي في ذلك أن يكون المحل مسكنا أو ما في حكمه أو أن يكون شخصا[1]".

محل التفتيش في جريمة الانترنيت هو مكونات جهاز الكومبيوتر سواء كانت مادية ومعنوية ، أو شبكات الاتصال الخاصة به .فيشترط ان تكون هناك جريمة وقعت على البيانات والمعلومات المخزنة بالكومبيوتر او بإساءة استخدام الكومبيوتر كأداة في ارتكاب جرائم عبر الانترنيت وشبكات المعلومات، كذا يخضع التفتيش للخصائص العامة التي تخضع لها كافة الإجراءات التحقيق الابتدائي، وهي وجوب التدوين بمعرفة الكاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم كلما أمكن ذلك[2].

الشهـــادة:

في الجريمة الالكترونية الشاهد هو الفني صاحب الخبرة والتخصص في التقنية وعلوم الحاسب الآلي ،لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات ،إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ، ويطلق عليه اسم الشاهد الالكتروني ،تمييزا له عن الشاهد التقليدي [3]، نتيجة لقصور إحكام الشهادة في الحصول على الدليل الالكتروني ، يرى بعض الفقهاء ضرورة البحث عن وسيلة قانونية جديدة ، ما لم تستطيع فكرة الالتزام بالشهادة أن تؤديه وهذه الوسيلة هي الالتزام بالإعلام في الجريمة الالكترونية ، وذلك بضرورة وجود نص صريح في القانون بفرض تقديم معلومات

[1] احمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجزائية ،رسالة دكتوراه، سنة 1959، جامعة القاهرة ،ص 140.

[2] أسامة احمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنيت\دراسة تحليلية مقارنة ،عمان،، دار وائل للنشر والطبع ، ،سنة 2001، ص 278.

[3] نايري عائشة ،الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الاداري ،سنة 2016 2017،كلية الحقوق والعلوم السياسية، جامعة احمد دراية ،أدرار، ص 51.

ضرورية من اجل إعانة سلطات التحقيق والاستدلال في الحصول على الدليل، وفرض هذا الالتزام قد يلعب دور وقائي في حفظ النظام المعلوماتي[1].

الخـــبرة :

ويطلق لفظ الخبير على كل شخص توافرت لديه معرفة عملية وفنية لتخصصه في مادة معينة وتستعين به السلطة القضائية وجهات التحقيق في تقدير المسائل الفنية استكمالا لنقص معلومات القاضي في هذه النواحي ومساعدة له في اكتشاف الحقيقة لهذا الغرض يجب أن يتوفر لديه القدرة على تطبيق تلك القواعد النظرية على الحالات الواقعية ولا يتحقق ذلك إلا بالممارسة العملية.

فالخبرة هي احد أهم وسائل جمع الأدلة، يلجا إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات[2].

إذا كان للخبرة أهمية في الجرائم التقليدية، فإن أهميتها ازدادت وأصبحت حتمية في إثبات الجرائم المرتكبة عبر الإنترنت، فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية وهي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات.

تستعين الشرطة وسلطات التحقيق أو المحاكمة منذ ظهور الجرائم المرتكبة من خلال شبكة الإنترنت بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض

[1] المرجع نفسه، ص 52.
[2] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية|دراسة مقارنة، شهادة ماجستير في القانون العام،2014، كلية الحقوق والعلوم السياسية، جامعة الشرق الأوسط ،ص78.

كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، ويلاحظ أن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون بكفاءة وتخصص هؤلاء الخبراء[1].

إضافة إلى ذلك فقد شرعت بعض الدول في إعداد أجهزة متخصصة في الخبرة في الإجرام غبر الانترنيت .وعلى رأس تلك الدول الولايات المتحدة التي قامت بإنشاء وحدة تابعة للمباحث الأمريكية الفدرالية *FBI*أطلق عليها المعمل الإقليمي الشرعي للحاسوب، ومقره سان ديجو*San Diego*والذي تم افتتاحه في نوفمبر 2000 كمركز خبرة عام متعدد النواحي القضائية غرضه مكافحة الجرائم الالكترونية عبر الانترنيت، حيث يتم إعداد محللين للحاسب الآلي والذين يعملون بدورهم على تكثيف مواجهة الجريمة عبر الانترنيت[2].

العنصر الثالث: الصعوبات التي تواجه عناصر التحقيق عند البحث وجمع الأدلة

تتميز الجريمة الالكترونية بصعوبة اكتشافها، وحتى في حالة اكتشاف وقوعها والإبلاغ عنها فان إثباتها أمر صعب، فهي تتم في بيئة غير تقليدية حيث تقع خارج إطار مادي غير ملموس لتقوم أركانها في بيئة الحاسوب والانترنيت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، فتقد الآثار التقليدية للجريمة نظرا لان ارتكابها يتم عادة عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون،2013،كلية الحقوق والعلوم السياسية، جامعة مولود معمري ،تيزي وزو، ص 89.
[2] نادر عبد الكريم العزوالي ،الحماية الجنائية من جرائم الانترنيت (دراسة مقارنة)، د ط، د س، القاهرة ص128

تنساب عبر أجزاء الحاسب الآلي، وشبكة الاتصالات العالمية (الإنترنت) بصورة آلية، كما تنساب الكهرباء عبر الأسلاك[1].

فهذه الجرائم ترتكب على العمليات الالكترونية والتي تعتمد في موضوعها على الشفرة والرموز السرية...الخ فيصعب هنا ان تخلف وراءها اثأر مرئية قد تكشف عنها أو يستدل من خلالها على مرتكبيها والقبض عليهم ،فالجهة المكلفة بالتحريات لا تستطيع تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية[2].

يعمد المجرمون عبر الإنترنت عادة إلى إخفاء جرائمهم، وإزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر والبرامج، ودون ترك اثر، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة عبر الإنترنت وثباتها فلا مرية أن المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب[3]، فيصعب التوصل إلى الجاني، لأنه كثيرا ما يقوم بالدخول لشبكة الانترنيت باستخدام اسم مستعار، وغالبا ما يقوم بالدخول إلى الانترنيت عن طريق مقاهي الانترنيت ويصعب معرفة الجاني وتحديد موقع اتصاله[4].

وقد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم بالإضافة إلى ذلك يقوم المجرمون

[1] محمد حماد مرهج الهيتي ،جرائم الحاسوب ، ماهيتها ،موضوعها، أهم صورها، والصعوبات التي تواجهها \دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع ، عمان،2006،ص214.

[2] بو خبزة عائشة ،الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي 2013,2012، كلية الحقوق ،جامعة وهران، وهران، ص34

[3] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون،2013،كلية الحقوق والعلوم السياسية،، جامعة مولود معمري ،تيزي وزو،ص118

[4] جعفر حسن حاسم الطائي، جرائم تكنولوجيا المعلومات، ، عمان ،دار البلدية الأردن،2007، ،ص 22

عبر الإنترنت بإخفاء هويتهم أو انتحال شخصية أخرى حتى لا يمكن التعرف عليهم في حالة اكتشاف الجريمة، وهنا يصعب على التحريين اكتشافهم وان دل هذا فإنما يدل على انخفاض مستوى مهارة وخبرة الجهات القائمة على التحقيق[1].

إضافة إلى عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على شبكة المعلومات والسيرة عليها[2].

العنصر الربع :المواجهة الموضوعية في إطار قانون العقوبات

إن القانون الجنائي التقليدي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا الجديدة لاسيما أن نصوصه وضعت في عصر لم تكن فيه الانترنيت ولم تظهر المشاكل القانونية الناتجة عن استخدامه[3]،لكن تدارك المشرع الجزائري خلال السنوات الأخيرة لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم15_04 المؤرخ في10نوفمبر 2004المتمم لأمر رقم15_ 22المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، فقد قام المشرع الجزائري بموجب القانون رقم15_04 باستحداث جملة من النصوص والتي جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات[4]، فاتجه اتجاها ايجابيا لحماية الحياة الخاصة التي أصبحت عرضة للانتهاكات عن طريق

[1] م م صفاء حسين نصيف ،التحديات الإجرائية المتصلة بالجرائم المعلوماتية ، مجلة العلوم القانونية والسياسية ، جامعة ديالى، المجلد الخامس، العدد الثاني،2016،ص 260

[2] بو خبزة عائشة ،الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي 2013,2012، كلية الحقوق ،جامعة وهران، وهران،2013،ص 253

[3] نايري عائشة ،الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري ،سنة 2016 2017،كلية الحقوق والعلوم السياسية، جامعة احمد دراية ،أدرار، سنة 2016 2017،ص 56

[4] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،جامعة محمد بوضياف ،المسيلة ،العدد الحادي عشر، سنة 2018،ص363

الحاسبات الآلية بأفعال مستهجنة عواقبها جد خطيرة[1]، وحدد لكل فعل منها ما تقابله من الجزاء، إذ قام المشرع الجزائري بسن « جملة من القواعد القانونية الموضوعة والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة، وإلى جانب ذلك فقد قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22.

إذ نصت المادة394 مكرر منها على ما يلي: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من50000 إلى 100000دج إلى كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، ونصت المادة 394 مكرر من قانون العقوبات الجزائري على انه: يعاقب... كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكبها الجرائم المنصوص عليها فيهذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها فيهذا القسم[2].

و تضيف المادة 394 مكرر 09 أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية: "يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محل الجريمة من

[1] طرشي نورة، مكافحة الجريمة المعلوماتية ،مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي ، الجزائر، كلية الحقوق ، جامعة الجزائر ،2012,2011، ص52

[2] نفس المرجع ،ص 58

الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو المكان إذا كانت الجريمة قد ارتكبت بعلم مالكها"[1].

وفي سنة 2006 قام المشرع بإدخال تعديلات جديدة، حيث تم تشديد العقوبة على كل الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها، ويعود ذلك بالتأكيد إلى إقرار المشرع بان الظاهرة جديدة ومستحدثة متميزة عن الجرائم التقليدية من محلها وأشخاص مرتكبيها، وسعيا منه في ضمان المكافحة لم يميز بين نوعية المعلومات التي تطالها الحماية سواء كانت مادية أو اقتصادية أو مسائل أمنية غرضه في ذلك هو حتما تحقيق الردع العام على اثر التزايد الخطير لنسب الجرائم المرتكبة وتنوعها وخطورتها على الأفراد من جهة وعلى الاقتصاد الوطني من جهة أخرى[2].

العنصر الخامس: التصدي للجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

لقد جاء في القانون 09_ 04 مجموعة من التدابير الوقائية التي يتم اتخذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و عن مرتكبيها في وقت مبكر . وهي كالتالي:

[1] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،جامعة محمد بوضياف ،المسيلة ،سنة 2018،ص363

[2] سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، العدد الأول، جامعة الإخوة منتوري قسنطينة،الجزائر،2019ص49

1 – التدابير الوقائية

أ – مراقبة الاتصالات الإلكترونية:

لقد نصت المادة 04 على من القانون 09_ 04 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي [1]:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2].

ب –الاستعانة بمزودي الخدمات للوقاية من الجرائم المعلوماتية :

ويتم ذلك من خلال تقديم المساعدة للسلطات المكلفة بالتحريات القضائية بجمع وتسجيل المعطيات ووضعها تحت تصرف السلطات وتتمثل في :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

[1] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،جامعة محمد بوضياف ،المسيلة ،سنة 2018،ص366

[2] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار النشر دار الهدى، مكان النشر عين مليلة – الجزائر سنة2011 ص 127 128

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات التي تسمح بالتعرف إلى المرسل إليه أو المرسل إليهم ، الاتصال وكذا عناوين الموقع المطلع عليه... الخ

زيادة على ذلك افرد المشرع الجزائري مجموعة من الالتزامات خاصة بمقدمي خدمات الانترنيت (المادة 12 من القانون 04 -09 ص 08) تشمل :

التدخل الفوري لسحب المحتويات المخالفة للقوانين وتخزينها أو حضر الدخول إليها .

الالتزام بموضع ترتيبات تقنية تحضر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام أو الآداب العامة[1].

2 – التدابير الإجرائية

أ–التفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

وذلك وفقا للمعايير العالمية والمعمول في هذا الشأن ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة، وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى منظومة المعلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء المساعدة الأجنبية المختصة من اجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم او مرتكبيها[2].

[1] مهدي رضا، الجرائم السيبيرانية والليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات،ص118

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون، تيزي وزو ،2013،ص 114

ب-إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

من بين الآليات التي أوجدها المشرع الجزائري في مجال الوقاية والمكافحة من الجريمة المعلوماتية إنشاء هيئة وطنية للوقاية والمكافحة من جرائم الإعلام والاتصال ومكافحتها ويكمن دورها الأساسي في تنسيق وتنشيط عمل السلطات المكلفة بمكافحة الجريمة الافتراضية ومدها بالمساعدة والاستشارة اللازمة.

وقد تم استحداثها بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص مادته 15 منه التي تنص على ما يلي:

"تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته" ليترك تحديد تشكيلة هذه الهيئة وتنظيمها وكيفية سيرها على طريق التنظيم ،وقد أنيطت بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته بجملة من المهام أوردتها بالذكر المادة 14من القانون 09-04 السابق ذكره والتي تنـــص على مـا يلي:

تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام التالية:

- ❖ تنسيق وتنشيط عمليات الوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحته.
- ❖ مساهمة السلطات القضائية ومصالح الشرطة القضائية بالتحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم[1].

العنصر السادس: مكافحة الجريمة الالكترونية بموجب قانون الإجراءات الجزائية:

لقد أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شانها تفادي وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدركه المشرع بتضمين القانون 06-22 المعدل لقانون الإجراءات الجزائية بتدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية[2].

فيا يتعلق بمتابعة الجريمة الالكترونية فهي تتم بنفس الإجراءات التي تتم بها التقليدية كالتفتيش والمعاينة والضبط ...الخ، غير أن هذه الإجراءات لا تعطي النتائج المرجوة فقام المشرع الجزائري بموجب قانون الإجراءات الجزائية باستحداث مجموعة من الإجراءات الخاصة تتماشى مع العالم الافتراضي وتتمثل في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات وإجراء التسرب ،حيث سمح المشرع الجزائري باللجوء إلى اعتراض المراسلات بالتقاط الصور وتسجيل الأصوات لمقتضيات التحري والتحقيق في جرائم محددة حصرا ومن بينها الجرائم الماسة بأنظمة المعالجة الإلية للمعطيات ، ولابد أن

[1] بو خبزة عائشة ،الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي 2013,2012، كلية الحقوق ،جامعة وهران، وهران، ص 254 ،255.

[2] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،جامعة محمد بوضياف ،المسيلة ،سنة 2018،ص 364

تراعي في ذلك شروط محددة قانونا، والمتمثلة في الإذن، طبيعة الجريمة، وكتمان السر المهني، وتحرير محضر من طرف ضابط الشرطة القضائية المأذون له بالعملية[1].

و مع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق و الحريات العامة والحياة الخاصة للأفراد[2].

العنصر السابع: كيفية التصدي للجرائم الالكترونية من خلال القانون المدني:

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر وذلك في المادة 124 من التقنين المدني الجزائري "كل عمل أي كان يرتكبه المرء يسبب ضرر للغير يلزم من كان سببا في حدوثه بالتعويض" وقد جاء هذا النص شاملا وعاما لأي اعتداء يقع على أي حق من الحقوق الملازمة الشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهما وهو حق من وقع عليه اعتداء على حياته في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في التعويض "فالفعل الضار هو أساس المسؤولية" وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الالكترونية التي تمس بالحياة الخاصة على شبكة الانترنيت ، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على مواقع الالكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدى، وفي هذه المسالة المشرع الجزائري

[1] مهدي رضا، الجرائم السيبيرانية واليات مكافحتها في التشريع الجزائري، مجلة اليزا للبحوث والدراسات، جامعة محمد بوضياف المسيلة الجزائر، المجلد السادس، العدد الثاني،2021 ،ص 117

[2] براهيمي جمال، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة مولود معمري ، تيزي وزو، العدد الثاني،2016،ص 125,124

حذا حذو المشرع الفرنسي الذي أقام المسؤولية على الفعل الالكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس الحياة الخاصة بل يجب أن يكون ذلك الفعل الالكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وان وقع على الشبكة[1].

[1] بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ،جامعة محمد بوضياف ،المسيلة ،سنة 2018،ص361.

الجانب التطبيقي

الفصل الثاني: التعريف ببعض الجرائم ونماذج عنها ونتائج تحليل الاستبيان

1. **تعريف جريمة الاحتيال:** يتم ذلك بطرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه(125)، وقد يتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الإلكتروني للأموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في إيهام الحاسب والاحتيال عليه فيسلمه النظام المال.[1]

2. **تعريف جريمة التجسس:** ينتج عن الاستخدام المتزايد للحاسبات الآلية في العديد من المجلات، تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريتها.

يقصد بالتجسس في هذا الموضع هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر، وليس مسموحا لغير المخولين بالاطلاع عليها.[2]

3. **جريمة التهديد والمضايقة والملاحقة:** تتم في هذا النطاق جرائم الملاحقة عبر شبكة الإنترنت باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة، وتشمل الملاحقة رسائل تخويف ومضايقة، وتتفق مع مثيلاتها خارج

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون،2013،كلية الحقوق والعلوم السياسية، جامعة مولود معمري ،تيزي وزو،ص45.
[2] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون،2013،كلية الحقوق والعلوم السياسية، جامعة مولود معمري ،تيزي وزو،ص57.

الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة.[1]

4. **تعريف الجرائم الجنسية الواقعة عبر الانترنت:** لقد تحولت شبكة الانترنت إلى أرشيف ضخم تجمع فيه الصور الماجنة والمقالات الفاضحة والأفلام الخليعة والتي تبث عبر مواقع مخصصة لذلك، غايتها تحقيق الربح المادي تسمى بالمواقع الجنسية الإباحيةunihibitedlocatins وعن طريق الدردشة الإباحية والقوائم البريدية الجنسية، التي أصبحت تجتاح عالمنا وتقتحم منازل ومكاتب الجميع. فهي لا تفرق بين صغير وكبير ولا بين أنثى وذكر، أي أنها لا تستثني أحد.

و عليه يمكن تعريف الجرائم الجنسية عبر الانترنت بأنها: "بث الصور الماجنة والمقالات الفاضحة والأفلام الخليعة عبر الانترنت و على مواقع مخصصة لذلك، غايتها تحقيق الربح المادي تسمى بالمواقع الجنسية الإباحية unihibitedlocatins أو عن طريق الدردشة الإباحية والقوائم البريدية الجنسية".[2]

5. **تعريف جريمة انتهاك الآداب العامة الواقعة عبر الإنترنيت** يمكن تعريف هذه الجريمة التقليدية التي تقع عن طريق الانترنت بأنها: "هي كل فعل يتضمن مخالفة القواعد الأخلاقية الأساسية التي يبنى عليها المجتمع و كذا تعاليم كافة الأديان السماوية باستخدام الانترنت كنشر و بث الصفحات الخادشة والمخلة

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون،2013،كلية الحقوق والعلوم السياسية، جامعة مولود معمري ،تيزي وزو، ص 50

[2] هروال هبة نبيلة، جرائم الانترنيت دراسة مقارنة، اطروحة دكتوراه، جامعة ابي بكر بلقايد، كلية الحقوق والعلوم السياسية،تلمسان،2013,2014 ص 155.

بالحياء عبر مواقعه أو إنتاج أو إعداد أو تهيئة ذلك أو إرسال أو تخزين أو ترويج أي محتوى يخل بالحياء أو النظام العام والآداب عن طريق شبكة المعلومات"[1].

6. **تعريف جريمة المطاردة عبر الإنترنت.** يقصد بالمطاردة عبر الإنترنت": كل سلوك يتسم بالتطفل والخبث على شبكة الإنترنت وتستخدم فيه هذه الشبكة لارتكاب نوعين من هذا السلوك:

1 – جمع معلومات خاصة عن المجني عليه ليقرر ويدعم المطاردة.

2 – أو الاتصال بالضحية مع تهديدها الضمني أو العلني لتعزيز الخوف".

ويعرفها أخرون بأنها: "مجموعة من السلوكيات التي تقع على الشخص أو عدة أشخاص أو منظمات باستخدام الإنترنت وتكنولوجيا الاتصالات لإحداث إزعاج أو ضرر، ومثل هذا السلوك قد يشمل الأفعال المجرمة الآتية: نقل التهديدات، الاتهامات الزائفة، سرقة الهوية، سرقة بيانات، تدمير البيانات والأجهزة بإغراء المستخدمين القصر وتحريضهم على ارتكاب أفعال جنسية.[2]

7.**تعرف جريمة الاعتداء على الحياة الخاصة عبر الانترنت:** بأنها كل اعتداء على البيانات الاسمية عبر الانترنت، و ذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت و العمل على تسجيل البيانات المتبادلة فيما بين الأنظمة المعلوماتية، أي عن طريق استغلالهم النقاط الضعيفة في منظومة الأمن باستخدامهم لمبرمجات الحواسيب، والتي هي عبارة عن جسيمات تنصت على الويب تمثل بنقاط على الشاشة تعمل كأجهزة

[1] هروال هبة نبيلة، جرائم الانترنيت دراسة مقارنة، اطروحة دكتوراه، جامعة ابي بكر بلقايد، كلية الحقوق والعلوم السياسية،تلمسان،2013,2014ص 144,145

[2] عمر محمد ابو بكر بن يونس، الجرائم التنشئة عن استخدام الانترنيت، دار النهضة العربية ، القاهرة 2004 ص475

إرسال متناهية صغيرة، وبالتالي يسهل انتهاكهم وإطلاهم على البيانات الموجودة على شبكة ومن دون أن تصدهم أية صعوبات أو إعاقات.[1]

8. **تعريف جريمة القذف و السب و التشهير عبر الانترنت.:** و يعرف القذف الالكتروني بأنه:" هو إسناد واقعة محددة تستوجب عقاب من تنسب إليه، و قد يكون بالقول أو الإشارة أو الكتابة. كما يمكن أن يكون في مواجهة المقذوف في مجلس أو مكان عام، أو في غيابه أمام الناس أو عبر وسائل الإعلام المقروءة أو المسموعة أو المرئية، كما يمكن أن يكون عبر المواقع الالكترونية كالمنتديات و شبكات التواصل الاجتماعي و الصحف الالكترونية و البريد الالكتروني، كما أنه يمكن أن يحدث عبر أجهزة الاتصالات كالجوال و الرسائل النصية و رسائل الوسائط المتعددة.[2]

9.**تعريف جريمة السرقة المعلوماتية:** هي كل سلوك غير قانوني يتم باستخدام الأجهزة الالكترونية ينتج عنها حصول الجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من اجل سرقة أو إتلاف المعلومات.[3]

10.**تعريف جريمة غسيل الأموال: غسل الأموال:** يتمثل إما في تحويل الأموال أو نقلها مع العلم أنها من نتاج جرائم مخدرات، أو في إخفاء أو تمويه حقيقة الأموال أو مصدرها أو تمويه حقيقة الأموال أو مصدرها أو في اكتساب أو حيازة أو استخدام الأموال، وجريمة

[1] وليد الزيدي، القرصنة على الانترنيت والحاسوب، التشريعات القانونية، دار اسامة للنشر والتوزيع، الاردن،2003 ص56.

[2] هروال هبة نبيلة، جرائم الانترنيت دراسة مقارنة، اطروحة دكتوراه، جامعة ابي بكر بلقايد، كلية الحقوق والعلوم السياسية،تلمسان،2013,2014 ص82

[3] عبر موقع الكتروني، 11:10،/2022/05/25/wiki<https||ar.m.wkipedia.org

غسل الأموال من الجرائم ذات الإبعاد المتعددة وتكمن صعوبة البحث فيها لأنها تعد من اخطر الجرائم المنظمة دوليا.[1]

- **بعض النماذج عن الجرائم الالكترونية .**

أصبحت الجريمة الالكترونية موجودة بشكل يومي فمع تزايد عدد مستخدمي شبكة العنكبوتية زادت نسبة ارتكاب الجرائم الالكترونية وزادت خطورتها على المجتمعات والأفراد.

7. نماذج عن بعض الجرائم في أمريكا :

وقعة 1:

جريمة حدثت بتاريخ 1998/02/17 حيث اعتقل الرئيس السابق السيد ثيموتي الين لويد بعد إن تم فصله من الشركة لمدة عشرين يوم والسبب في ذلك هو إطلاقه لقنبلة الكترونية استطاعت إلغاء كافة التصميمات وبرامج الإنتاج في كبرى مصانع التقنية في نيو جيرسي والتي ترتبط مع نظام التحكم في وكالة وناسا الأمريكية مما سبب بخسائر ضخمة جدا تقدر بعشرة ملايين دولار وهي من اكبر الجرائم الإلكترونية في تلك الفترة.

واقعة 2:

حدث في عام 1999على يد ايرك بيرنز الذي قام باختراق أجهزة حواسب آلية محمية وتسبب في ضرر كبير لها في واشنطن بأمريكا فقام بالاعتداء على المواقع الالكتروني الخاص بالحلف الأطلسي ومواقع نائب الرئيس الأمريكي آنذاك، واعترف بأنه قام بتعليم برنامج الاختراق الآخرين بأساليب بسيطة وسهلة يمكنهم من خلالها اختراق أجهزة

[1] موقع الكتروني ،8:00،2022/05/26/ http:\\www.maher.sandroses .com

الحواسب المتصلة بشبكة الانترنت التي لديها نقاط ضعف يمكن اختراقه ى، ولذلك قامت محكمة فيرجينيا بالحكم عليه لمدة خمسة عشر عام والخضوع لرقابة لمدة ثلاث سنوات بعد اعترافه بذنبه .[1]

11.بعض نماذج عن الجرائم الالكترونية في الجزائر

شهدت الجزائر في سنوات الماضية تصاعد مخيف للجريمة الالكترونية التي باتت تخلف مصائب مجتمعية فنذكر بعض الجرائم التي وقعت على بعض الأشخاص.

وقعة 3:

تذكر المحامية ب سماح 26 سنة أو رسالة وردتها من هكر قرصان الكتروني بالفايسبوك تتعلق بصورة عن زواجها الذي لم يمضي على تاريخه سوى شهرين حيث هددها بنشر صورة لها في حين لم ترسل له مبلغ مالي على الحساب البريدي قال انه سيحدده لاحقا ، تتنهد سماح وتواصل حديثها الخاص ل dw تسترت عن ذلك في البداية إلا أني وبعد ذلك أخبرت زوجي الذي لم يبالي واعتبر ذلك لعب صبيان ، إلا أن الهاكر أرسل رسالة أخرى يطلب المال دون تحديد المبلغ .

بعد أن استنفذت المحامية زوجها كل الوسائل قررا اللجوء للشرطة "نجحت الشرطة في تحديد هوية الجناة وهما شابان أخدهما مراهق والأخر بالغ ، حيث اعترفا بجرمهما واني لست المرأة الوحيدة ، بل الضحايا بالعشرات " .

كان الجانيان يطلبان من الضحايا تعبئة بطاقة رصيد هاتفهم " ما يعرف بالفليكسي " وانتهت المصيبة التي كادت أن تهدم عش زوجية المحامية بان تم إيداع الجاني البالغ

[1] موقع الكتروني10:06. 26\05\2022،https://cyberone.co..

ستة شهور في الحبس والقاصر وضع تحت الرقابة القضائية حسب ما أخبرت به ب سماح dw عربية .

واقعة 2:

عاشت ليلى بلقاسم ، أستاذة لتاريخ بالمركز الجامعي لمحافظة غليزان في غربي الجزائر ، حياتها بلا من ضغطات تقريبا إلى أن تسلل شخص لا تربطه صلة بي أي صلة حياتي إلي جحيم وتتابع السيدة الجزائرية : بادر باتهامي بعدة أشياء من بينها ، الانتماء إلي نادي الروتاري والي الماسونية .

وتنكر ليلى بلقاسم معرفتها بذلك الشخص لا في العالم الحقيقي ولا الافتراضي وتواصل الأستاذة بلقاسم وبمرارة ، رواية فصول مأساتها في حديث خاص ب dw عربية راحت المناشير اليومية تتهمني حتى في شرفي وأخلاقي وإنني "سحاقية "وعلى علاقة بفلان واتهامات أخرى كان هدفها الابتزاز وضرب سمعتي بما فيها نشاطاتي الفكرية التي باشرتها منذ 2015 ، فما كان علي إلا التوجه نحو العدالة .

أما عن أثار هذه المناشير الاستفزازية ، فتؤكد الأستاذة الجامعية أنها حاولت حياتها إلي جحيم لا يطاق خاصة وان شائعات وصلت إلي الطلبة : "سرت حديث الجميع في المجالين العام والخاص فتعرقلت حياتي الأسرية والعائلية والمهنية وعلاقاتي مع طلبتي وزملائي "وتتابع ليلى " أعاني من أثار ذلك حني اليوم ، الجاني ما يزال حر طليق ويواصل تلفيق والكذب عبر صفحاته حتى الساعة"[1].

[1]موقع الكتروني 10:04، 2022/05/25 <http://www.dw.com..

8. إحصائيات عن بعض الجرائم الالكترونية في الجزائر.

سجلت مصالح الدرك الوطني والشرطة حسب الأرقام التي تحوزها "الشروق "، قرابة ثمانية الآف جريمة الكترونية خلال سنة 2020 ، حيث سجلت المديرية العامة لأمن الوطني ارتفاعا قياسيا أي من 500 جريمة سنة 2015 ، الى 5200 قضية .خاصة بالجرائم الالكترونية سنة 2020 ، في حين سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020 وبينت عملية تحليل المعطيات للجرائم المسجلة إن القذف والسب عبر الفضاء الافتراضي احتل الصدارة بنسبة تفوق 55 بالمئة ، تليها الجرائم ضد الأمن العمومي ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار وأخيرا الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة وقضايا مشابهة .

وأكدا المختصون في مكافحة الجريمة السيبرانية انه وفقا لأخر تقرير للموقع الالكتروني datariporta داتاريبورتال المختص في الإحصائيات المتعلقة بأنترنيت الهاتف الثابت والنقال في العالم فان عدد مستخدمي الانترنيت ارتفع ب 3.6 مليون في ظرف سنة متنقلا بذلك إلى26.35 مليون مستخدم ومعلومات تخص وضع الرقمنة في العالم .[1]

[1] موقع الكتروني2022/05/28 12:30 <.http://.www.echoroukonline.com..

14. تحليل استبيان مع تقديم نتائج الدراسة .

لقد قمنا باختيار مجموعة من الأسئلة توجيهية وإرشادية أي أن كل محور ينطوي تحته موضوع فلمحور الأول موضوعه الجريمة الالكترونية أما المحور الثاني تحدثنا فيه عن آليات التصدي للجريمة الالكترونية وقدرت نسبة العينة المدروسة ب 20 % شخص وزعت في فترة لا تتجاوز 15 يوما.

يهدف هدا الاستبيان إلى :

1/ معرفة مدى تأثير الجريمة الالكترونية علي المجتمع المعلوماتي .

2/ معرفة الأسباب الناجمة عن ارتكاب الجريمة الالكترونية .

والأداة التي اعتمدناها في دراستنا هي التحليل للإحصاء النتائج .

1/المحور الأول خاص بالجريمة الالكترونية :

1. هل الحكومة أو السلطة القضائية والمحلية تبذل ما يكفي لمنع الجرائم الالكترونية ؟

نعم	النسبة	لا	النسبة
11	**55=20/100*11**	**05**	**20/100*5 25=**

من خلال الجدول نلاحظ أن الإجابة معظمها كانت بنعم وقدرة 55% أي أن السلطة القضائية والمحلية تبدل ما يكفى لمنع الجرائم الالكترونية وهذا راجع لوعي القانون الجزائري أما البقية من الأشخاص استدلوا ب لا بنسبة 25 % وهذا راجع لجهلهم بالقوانين وقلة وعيهم له .

2/ هل الجريمة الالكترونية خطيرة ؟

نعم	النسبة	لا	النسبة
16	100*16 /20= 80	3	3*100/ 15=20

اتضح لنا من خلال الجدول أن نسبة 80 %أقرت على أن الجرائم الالكترونية خطيرة وهذا راجع لحرص القضاء الجزائري على السهر وحماية الأفراد في حين أن 15 %اقروا عكس ذلك وهدا راجع لجهلهم للقوانين مع غياب الوعي .

3/ في رأيك ماهي الأسباب الرئيسية التي تجعل الشباب يرتكبون مثل هذه الجرائم؟

1/ الحصول على الأموال.

2/ الفراغ .

3/ البطالة .

4/ سوء الأخلاق.

5/ ضعف الإيمان.

4/ هل سبق لك أن تلقيت تهديد الكتروني ؟

نعم	النسبة	لا	النسبة
1	1*100/20=5	19	19*100/20= 95

نستكشف من خلال معطيات الجدول آن نسبة 95% من الإجابات دلت على عدم تعرض الأفراد أو تلقيهم أي تهديد الكتروني في حين إن البعض الأخر قال عكس ذلك .

5/ هل لديك فكرة عن الجرائم الالكترونية ؟

اعلم	النسبة	لا اعلم	النسبة
19	**95=20/100*19**	**1**	**5=20/100*1**

نلاحظ من خلال معطيات الجدول بان جل الإجابات كانت بأعلم وهذا راجع لتطور وسائل الإعلام والوعي الفكري لدى الكثير منهم في حين إن أدنى نسبة قالت عكس ذلك.

6/ هل تعلم بان هناك رقم خاص بمكافحة الابتزاز الالكتروني ؟

نعم	النسبة	لا	النسبة
9	**45=20/100*9**	**11**	**55=20/100*11**

اتضح لنا من خلال معطيات الجدول أن نسبة 55 % لهم علم بوجود رقم خاص بمكافحة الابتزاز الالكتروني في حين أن 45 %منهم لا يعلمون بوجوده وهذا راجع الي عدم بحثهم في موضوع مع جهلهم للقوانين.

7/ هل تتعدى الجرائم الالكترونية أثار نطاقات الواسعة أم تؤثر على الجماعات والبنوك فقط ؟

1/ توثر على حياة الفرد سلبا

2/ كما أنها تشمل مستعملي مواقع التواصل الاجتماعي وغيرها

المحور الثاني آليات التصدي للجريمة الالكترونية .

1/ هل انتشار السرقات العلمية يعتبر خطورة من مخاطر الجريمة الالكترونية ؟

6)نعم	السنة	لا	النسبة
12	**60=20/100*12**	**8**	**40=20/100*8**

نلاحظ من خلال معطيات الجدول بان جل الإجابة كانت بنعم بنسبة 60 % لان السرقات العلمية تؤثر على كتابات ومؤلفات الفرد ولأن السرقة هي من تساهم في خلق مثل هذه الجرائم كما أن القانون يعاقب كل مواطن آو فرد يقوم بسرقة معلومات ليست له ونسبيها له .

في حين أن الإجابة بلا كانت نسبتها 40 % ونرجح ذلك لعدم إدراك مدى خطورة السرقات العلمية وتأثيراها.

2/ هل الحماية التي في المواقع كافية لمنع اخترقك وسرقتك ؟

7)نعم	النسبة	لا	النسبة
8	**40=20/100*8**	**11**	**55=20/100*11**

من خلال معطيات الجدول لاحظنا أن الإجابة جلها كانت بنعم التي قدرت نسبتها ب 55 % وهدا راجع لاقتناع الأشخاص بان الحماية المواقع كافية لمنع اختراقهم وسرقتهم . في حين أن الإجابات بلا قدرت نسبتها ب 40 % حيث اقروا بان الحماية في مواقع غير كافية لأنه لو كانت كافية لما تعرض الأشخاص يوميا لاختراق والابتزاز الالكتروني.

3/ هل تعلم بوجود إجراءات وقائية تمنع من وقوعك ضحية لهذه الجرائم ؟

نعم		لا	النسبة
14	**70=20/100*14**	**6**	**30=20/100*6**

نلاحظ من خلال معطيات الجدول أن نسبة 70 % من الإجابات أقرت إن لديها علم بوجود إجراءات وقائية تمنع من وقوع الأشخاص كضحية لهذه الجرائم الالكترونية أما بنسبة ل 30 %من الأشخاص استدلوا بان ليس لديهم علم بوجود إجراءات تحميهم وتمنعهم من الوقوع ضحية لهذه الجرائم وذلك راجع إلي عدم الاطلاع علي المنظومة القانونية التي تستدل بذلك .

4/ هل توافق أن الشباب مسئولون عن الاضطرابات والجرائم التي ارتكبت في مجتمعك؟

لا أوفق بشدة	النسبة	أعارض	النسبة	محايد	النسبة	موافق بشدة	النسبة
3	**15=20/100*3**	**1**	**5=20/100*1**	**4**	**20=20/100*4**	**12**	**60=20/100*12**

من خلال ملاحظتنا للمعطيات في الجدول نلاحظ أن نسبة 60 %من الإجابات تدل على الموافقة بشدة على أن الشباب هم المسئولون عن الاضطرابات والجرائم التي ارتكبت في المجتمع وذلك نتيجة للجرائم التي تحدث في المجتمع إما نسبة 20 % من الإجابات كانت محايدة في رأيها .

وان نسبة 5 كانت معارضة حيث رشحت بان الشباب هم غير مسئولون عن كل هذه الجرائم التي في المجتمع .

وان نسبة 15 % أقرت إجاباتهم بان الشباب غير مسئولين عن الجرائم ولاضطرابات .

5/ هل عقوبة السجن تكفى للحد من الجرائم الالكترونية وذا كانت عقوبات أخرى اذكرها؟

نعم	النسبة	لا	النسبة
5	**25=20/100*5**	**15**	**75=20/100*15**

نلاحظ من حلال معطيات الجدول إن نسبة 75 % أقرت بان عقوبة السجن لا تكفى للحد من هذه الجرائم لان العقوبات التي تفرضها الحكومة على مستعملي الجرائم الالكترونية عادية بالنسبة له ومن بعض الأمثلة للعقوبات التي أدلوا بها هي عقوبة منع استخدام الشبكة العنكبوتية ،إضافة إلي القصاص وغرامات مالية وكذا تشديد العقوبات القاسية لمرتكبي هذه الجرائم .

أما بنسبة 25 % من الأشخاص اقروا بان عقوبة السجن كافية للحد من هذه الجرائم الالكترونية لان السجن هو العقاب الأنسب للمجرم الالكتروني في نظرهم .

6/ ما هو دورك كفرد في مكافحة الجريمة الالكترونية ؟

1/ التوعية والإرشاد.

2/ التصدي لها عن طريق نصح الشباب .

3/ التبليغ عن أي جرائم مشبوهة .

4/ الإبلاغ عن مرتكبي هذه الجرائم .

5/ منع هذه الظاهرة من خلال إعلام ناس بخطورتها.

7/ هل لدى المجتمع الجزائري ثقافة قانونية اتجاه الجرائم الالكترونية ؟

نعم	النسبة	لا	النسبة
8	**40=20/100*8**	**12**	**60=20/100*12**

نستكشف من خلال معطيات الجدول بان نسبة 40 % من الإجابات ساندت بأن المجتمع الجزائري لديه ثقافة قانونية اتجاه هذه الجرائم وذلك راجع إلى توجهه الكبير لدى المجتمع بضرورة التعامل معها والتصدي لها .

في حين أن نسبة 20 % أقرت بان المجتمع الجزائري ليست لديه ثقافة قانونية اتجاه الجرائم لأنها وكانت لديه ثقافة قانونية بالمعايير الكافية لاما وقع في أخطائها يوميا .

خاتمة

خـــاتمة

من خلال التطرق لآليات مكافحة الجرائم الالكترونية في التشريع الجزائري نستخلص انه لابد من الوقاية من هذا النوع من الجرائم قبل انتشارها ،واللجوء إلى مكافحتها وذلك بتربية النشا على الوازع الديني والأخلاق الفاضلة، اللذان هما بمثابة واقي للفرد يحول دون ارتكاب أي نوع من الجرائم .

بعد دراستنا لهذه القضية توصلنا إلى مجموعة من النتائج والتي من أهمها :

- يوجد للجريمة الالكترونية أكثر من تعريف اذ لم يتفق الفقهاء على تعريف شامل لما تعنيه هذه الأخيرة.
- إن الجريمة الالكترونية عابرة للحدود ومعنى ذلك أن المجتمع المعلوماتي منفتح عبر شبكات تخترق الزمان والمكان وهي لم تعد محلية بل أصبحت عالمية ،تكتسي أهمية بالغة وهي المساهمة في التعرف على ظاهرة إجرامية جديدة.
- جرائم الانترنيت صعبة الإثبات، حيث أن الجاني لا يترك أثر حتى وإن وجد ما يدل على ارتكابه لتلك الجريمة فيسهل عليه تدميرها.
- عدم قدرة القوانين التقليدية على مجابهة هذه الجرائم المستحدثة لأنها تحتاج قوانين أكثر نجاعة تتلاءم معها.
- يعاقب القانون الجنائي الجزائري على الجريمة الالكترونية كونها خطيرة تمس المجتمع وامن الدولة، وذلك من خلال القوانين التالية:

- قانون العقوبات(المعدل بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004).

- القانون رقم 09-04المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال(الصادر في 5 غشت 2009).إضافة إلى القانون المدني وقانون الإجراءات الجزائية...الخ

- رغم جهود المشرع الجزائري للحد من هذه الجرائم إلا انه لم يتمكن من تخصيص قانون قائم بذاته للتحكم فيها بصرامة.

من خلال هذه النتائج ننوه إلى عدة توصيات والتي ارتأينا أنها ذات أهمية وهي كالتالي:

- نشر الوعي لدى المواطنين وتنبيههم من الجرائم الالكترونية وللعقوبات المترتبة عليها.
- ضرورة توفير حماية الجنائية لحياة الأفراد وخاصة الأطفال عبر هذه التقنية في القوانين الجزائرية
- ضرورة مراجعة بعض التشريعات الجزائرية وتعديل النصوص والقوانين الإجرائية الخاصة بالجرائم الالكترونية وجعلها تتناسب وطبيعتها
- تدريس مناهج خاصة بالحاسوب والمعلوماتية من قبل متخصصين للقائمين بالتحقيق في هذه الجريمة وجعلهم قادرين على تشخيص الجريمة مع توفير كل الوسائل اللازمة لأداء العمل على أكمل وجه.
- ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الالكترونية وذلك من خلال الدخول في اتفاقيات ومعاهدات من اجل تبادل الخبرات والمعلومات للحماية والوقاية من المسائل المتعلقة بها.

- إنشاء مراكز خاصة و مرصد مراقبة في الجزائر لأمان الحاسبات والمعلومات وشبكة الانترنيت كلها.

في أخر المطاف لاحظنا أن جرائم الانترنيت أصبحت واقعا معاشا، لا يمكن تجاوزها ولا تناسيها، لهذا يجب التعامل معها بجدية تقنية وعلمية، من حيث سد كل الثغرات التقنية ، واستيعاب الخبراء في مجال الكومبيوتر، حتى نستطيع التعامل مع العالم التقني الافتراضي ،علما أن الإعلام الجديد أصبح بيت كل الجرائم التي ستفكك الإنسان ومجتمعه، وسيظل هنالك صراع دائم بين طرفي المعادلة الاجتماعية للمحافظة على الإنسان من تغول التقنية على قيمه وعاداته وتقاليده وعقيدته.

قائمة المصادر والمراجع

1 .احمد فتحي لمسرور، نظرية البطلان في قانون الإجراءات الجزائية ، رسالة دكتورة سنة 1959، جامعة القاهرة.

2 . القانون رقم 4,9 ، الصادر في 05 أوت 2009 يتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .

3 .أسامة احمد المناعسة ، جلال محمد الزغبي ، فاضل الهواوشة ، جرائم الحاسب الأولي والانترنت، دراسة تحليلية مقارنة الطبعة الأولى، عمان، دار وائل لنشر ، سنة 2001.

4 .براهيمي جمال، مكافحة الجريمة الالكترونية و التشريع الجزائري ، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولودي معمري، تيزي وزو ، العدد الثاني ، 2016 .

5 .بوضياف اسمهان ، الجريمة الالكترونية والإجراءات التشريعية لواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف ، المسيلة ، سنة 2018 .

6.بوخبزة عائشة ، الحماية الجزائية من الجريمة الالكترونية في التشريع الجزائري ، مذكرة لنيل شهادة الماجستير في القانون الجنائي 2012,2013 ، كلية الحقوق ، جامعة وهران

7. حسين مكاوي : تكنولوجيا الاتصال الحديثة في عصر المعلومات ، الدار المصرية اللبنانية ، القاهرة ، ط 4 ،2005.

8. حمزة بن عفون ، السلوك الاجرامي للمجرم المعلوماتي ، بخث مكمل لنيل شهادة الماجستير في العلوم القانونية ، تحصص علم الاجرام ، جامعة باتنة ، 2012، .2013

9. خالد ممدوح : امن الجريمة الالكترونية ، الدار الجامعية ، .2008

10. رصاع فتيحة : الجرائم المعلوماتية مذكرة ماجستير منشورة ، تخصص القانون العام، جامعة أبو بكر تلمسان 2011، .2012

11. طرشي نورة ، مكافحة الجريمة المعلوماتية ، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي ، كلية الحقوق ، جامعة الجزائر 2011,2012 .

12. محمد امين احمد الشوابكة ، جرائم الحاسوب والانترنت ، مكتبة دار الثقافة ، عمان الأردن ، 2004، ط 1 .

13. محمد عبد الله منشاوي ، جرائم الانترنت من منظور شرعي وقانوني .

14 محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة لنشر ، 2004، ص 53.

15. محمد حماد مرهج ، الهيتي ، جرائم الحاسوب ، ماهيتها ، موضوعها ، اهم صورها ، والصعوبات التي توجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لهالا الحاسوب ، الطبعة الأولى ، دار المناهج للنشر والتوزيع ، عمان 2006، 214.

16. مصطفى سمارة ، الجريمة الالكترونية ، مجلة معلوماتية ، العدد 29 شهر ، 2008.

17. ممهدي رضا ، الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري ، مجلة اليزا للبحوث والدراسات ، جامعة محمد بوضياف المسيلة الجزائر ، المجلد السادس ، العدد الثاني ، .2021

18. نايري عائشة . الجريمة الالكترونية في التشريع الجزائري ، مذكرة لنيل شهادة الماجستير في القانون الإداري ، سنة 2016، 2017، كلية الحقوق والعلوم السياسية ، جامعة احمد دراية ادرار ، 2016، 2017.

19. نادر عبد الكريم العزاوي ، الحماية الجنائية من جرائم الانترنت دراسة مقارنة ، د، ص ، ر ، س ، القاهرة.

20. صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة الماجستير في القانون ، جامعة مولودي تيزي وزو ، 2013.

21. صفاء حسين نصيف ، التحديات الإجرائية المتصلة بالجرائم المعلوماتية ، مجلة العلوم القانونية والسياسية ، جامعة ديالي ، المجلد الخامس ، العدد الثاني ، .20160

22. عبد الله دغش العجمي ، المشكلات العلمية والقانونية للجرائم الالكترونية ، دارسة مقارنة ، شهادة ماجستير في القانون العام ، 2014، كلية الحقوق والعلوم السياسية ، جامعة الشرق الأوسط .

23.عادل يوسف عبد النبي الشكري ، بحث بعنوان : الجريمة الالكترونية وأزمة الشرعية الجزائية ، جامعة الكوفة ، 2008.

24. عمر محمد ابو بكر بن يونس، الجرائم التنشئة عن استخدام الانترنيت، دار النهضة العربية ، القاهرة 2004

25.سامي علي حامد صياد ، للجريمة الالكترونية وإجرام الانترنت ، دار الفكر الجامعي الإسكندرية ، 2008، .

26. سوير سفيان جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، جامعة أبو بكر بلقايد ، تلمسان ، 2010، ، .2011

27. سعيدني نعيم ، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة لنيل شهادة الماجستير في العلوم القانونية ، جامعة الحاج الأخضر باتنة ، 2012.

28. هشام محمد غريد ، الحواسب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، الطبعة الرابعة ، مكتبة الآلات الحديثة ، .1994

29. هلالي عبد الله اخمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، الطبعة الرابعة ، القاهرة ، دار النهضة العربية ، سنة 1994،.

30. هشام القاسم ، المدخل آلي علم القانون ، الطبعة الخامسة ، سوريا ، منشورات جامعة دمشق2006.

31. يونس عرب ، جرائم الكمبيوتر ، ايجار المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحظة ، والاليات ، أبو ظبي ، 2002./12/12

32. هروال هبة نبيلة، جرائم الانترنيت دراسة مقارنة، اطروحة دكتوراه، جامعة ابي بكر بلقايد، كلية الحقوق والعلوم السياسية،تلمسان،.2013

33.وليد الزيدي، القرصنة على الانترنيت والحاسوب، التشريعات القانونية، دار اسامة للنشر والتوزيع، الاردن،2003 ص56

المواقع الالكترونية:

1. موقع الكتروني ،8:00،2022/05/26/ http:www.maher.sandroses .com

2. موقع الكتروني 10:04، 2022/05/25 www.dw.com <http:// ..

3. موقع الكتروني12:30 2022/05/28 .www.echoroukonline.com ..<.http://

4. عبر موقع الكتروني،

wiki<https||ar.m.wkipedia.org2022/05/25/،11:10

5. موقع الكتروني10:06. 2022\05\26،.https://cyberone.co..

الملاحق

الجمهورية الجزائرية الدمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة احمد دراية ادرار

كلية :العلوم الانسانية والاجتماعية تخصص: الصحافة مطبوعة الكترونية

ارشادات:

يتضمن هذا الاستبيان مجموعة من العبارات بعضها يتطلب وضع علامةx اما م الاجابة التي تختارها وبعضها يتطلب ابداء الراي في المكان المخصص .

كما يهدف هذا الاستبيان الي التعرف على وجهة نظر المجتمع المعلوماتي ومدى تأثير الجرائم الالكترونية عليه .

الجريمة الالكترونية :هي مخالفة التي ترتكب ضد الافراد والجماعات بدافع جرمي ونية الاساءة لسمعة الضحية او لجسدها او عقليتها ، سواء كان ذلك بطريقة مباشرة وغير مباشرة، وان يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الانترنت، البريد الالكتروني.

البيانات الشخصية :

1/ الجنس : ذكر : ☐ **انثى :** ☐

2/ السن : .....

3/المستوى التعليمي : ☐ **ثانوي :** **جامعي:** ☐

4/ الحالة العائلية : أعزب : ☐ **متزوج :** ☐ **مطلق :** ☐

ارمل : ☐

المحور الاول : الجريمة الالكترونية .

1/ هل تعتقد ان الحكومة او السلطة القضائية والمحلية تبذل ما يكفى لمنع الجرائم الالكترونية؟

نعم : ☐ لا : ☐

2/هل الجرائم الالكترونية خطيرة؟ نعم : ☐ لا : ☐

3/ في رايك ماهي الاسباب الرئيسية التي تجعل الشباب يرتكبون مثل هذه الجرائم الالكترونية؟

.....

.....

4/هل سبق لك ان تلقيت تهديد الكتروني؟ نعم: ☐ لا : ☐

..اذا كانت الاجابة بنعم كيف ذلك

.....

.....

.....

.....

5/هل لديك فكرة عن الجرائم الالكترونية؟

اعلم: ☐ لا اعلم : ☐

6/هل تعلم بان هناك رقم خاص بمكافحة الابتزاز الالكتروني؟

نعم :☐ لا : ☐

7/ هل تتعدى الجرائم الالكترونية اثار النطاقات الواسعة ام تؤثر على الجماعات والبنوك العالمية فقط؟

التعليل.....

.....

.....

.....

المحور الثاني : اليات التصدي للحريمة الالكترونية

1/ هل انتشار السرقات العلمية يعتبر خطورة من مخاطر الجرائم الالكترونية؟

نعم : ☐ لا : ☐

اذا كانت الاجابة بنعم كيف ذلك

.....

.....

.....

.....

2/ هل الحماية التي في المواقع كافية لمنع اخترقك وسرقتك؟

.....

.....

3/هل لديك علم بوجود إجراءات وقائية تمنع من وقوعك ضحية لهذه الجرائم؟

نعم : ☐ لا : ☐

4/ هل توافق ان الشباب مسؤولون عن الاضطرابات والجرائم التي ارتكبت في مجتمعك ؟

لا اوفق بشدة : ☐ اعارض : ☐ محايد : ☐

موافق بشدة : ☐

5/ هل عقوبة السجن تكفي للحد من الجرائم الالكترونية اذا كانت هناك عقوبات اخرى اذكرها في التعليل؟

نعم : ☐ لا : ☐

التعليل :

.....

.....

.....

6/ ما هو دورك كفرد في مكافحة الجرائم الالكترونية؟

.....

.....

7/ هل لدى المجتمع الجزائري ثقافة قانونية اتجاه الجرائم الالكترونية؟

نعم : ☐ لا : ☐

التعليل :

.....

.....

الملخص

ان هذا النمو والتطور المستمر لثورة المعلوماتية الالكترونية الذي نعيشه حاليا ويشهده حاضرنا فأصبحنا نواجه العديد من الاخطار التي تنشا بشكل تلقائي . فدخول الانترنت الي عالمنا وتمكن الصغير والكبير والجاهل والمتعلم من استخدامه دون اي رقابة ادي الي زيادة هذه الاخطار وتفشي النهب والسرقات الالكترونية بشكل ملحوظ ان الجرائم الالكترونية تعد من الجرائم التي تحتاج الي تظافر الجهود من اجل مكافحتها وضبط تمددها.

فلهذا تناولنا في دراستنا هذه اليات مكافحة الجرائم الالكترونية في القانون الجزائري فقد قسمنا بحثنا هذا الي جانبين جانب نظري واخر تطبيقي فقد تحدثنا في جانب النظري على طبيعة الجرائم الالكترونية واليات مكافحتها في القانون الجزائري اما في الجانب التطبيقي تحدثنا عن نماذج واحصائيات عن بعض الجرائم ونتائج تحليل الاستبيان .

الكلمات المفتاحية:

الجريمة / الجريمة الالكترونية /المجرم المعلوماتي / مكافحة/ التشريع / الآليات

Summary

This growth and continuous development of the electronic information revolution that we are currently living and witnessed by our present, we are facing many dangers that arise automatically. The entry of the Internet into our world and the ability of the young, the old, the ignorant and the educated to use it without any control led to an increase in these dangers and the spread of looting and electronic theft significantly.

That is why we dealt in our study with these mechanisms of combating cybercrime in Algerian law. We divided this research into two sides, a theoretical side and an applied one. On the theoretical side, we talked about the nature of cybercrime and the mechanisms for combating it in Algerian law. On the practical side, we talked about models and statistics on some crimes and the results of the questionnaire analysis .

key words:

Crime / Cybercrime / Cybercrime / Combating / Legislation / Mechanisms