وزارة التعليم العالي والبحث العلمي
جـــامعة عمار ثليجي بالأغواط

كـــلية العلوم الاجتماعية
قسم علم الاجتماع و الديمغرافيا

الشعبة : العلوم الاجتماعية

الموضوع:

الجريمة الإلكترونية في الجزائر

"دراسة وصفية من خلال محاضر الشرطة"

مذكرة مكملة لنيل شهادة الماستر الأكاديمي في علم الإجتماع

تخصص: علم اجتماع الاتصال

إعداد :
- أسامة بن شاعة
- جمال بوحنية

اشراف الأستاذة الدكتورة:
- أ.د حفصة جرادي

السنة الجامعية : 2021/2020

بسم الله الرحمن الرحيم

الشكر والتقدير

نتقدم بجزيل الشكر الى استاذتنا المشرفة الأستاذة الدكتورة

المحترمة **حفصة جرادي** مرافقتنا وسندنا خلال مسارنا الجامعي

والثناء لكل الاساتذة الذين درسونا وكان لنا الحظ في

توجيهاتهم ونصائحهم وكل الاساتذة في كلية العلوم

الإجتماعية لجامعة عمار ثليجي بالأغواط.

أسامة بن شاعة

جمال بوحنية

الاهداء

اهدي هذا العمل المتواضع الى والدي رحمه الله برحمته الواسعة واسكنه الفردوس الأعلى من الجنة ووالدتي التي لطالما كانت المؤثر الاول لنجاحي ولقراراتي والثقة التي منحتني اياها خلال كل مراحل تعليمي حفظها الله والى من آمنة بي وبقدراتي.

الى كل شخص محب للعلم للمثابرة يسعى لمستقبل جميل .

ولكل من ساندنا من قريب وبعيد نقول له شكرا.

وفقني الله واياكم .

أسامة بن شاعة

الاهداء

الفضل والمنة لله وحده وليس للعبد الضعيف أن هدانا الى طريق النجاح وجعلنا نعيش في هذا العصر بثقة بالله عزوجل.

بعملي المتواضع هذا اسأل الله عزوجل الحفظ والستر لكل من احبه.

إلى من استقي منهم نور الحياة وبهجتها ، إلى عيناي أمي نور قلبي وأبي سند ظهري حفظهما الله لي واطال في عمرهما.

ولكل من ساندنا من قريب وبعيد نقول له شكرا.

جمال بوحنية

فهرس المحتويات

فهرس	
شكر و عرفان	
اهداء	
ملخص	
مقدمة	أ-ج
الفصل الأول : الجانب المنهجي للدراسة	
1. مشكلة الدراسة	3
2. الإشكالية	3
3. اهداف الدراسة	3
4. أهمية الدراسة	4
5. تحديد المفاهيم	5
6. الدراسات السابقة	6
7. الإطار النظري للدراسة	7
8. المنهج المستخدم	7
الفصل الثاني : الجريمة الإلكترونية	
المبحث الأول: الإطار المفاهمي للجريمة الإلكترونية.	**9**
المطلب الأول: مفهوم الجريمة الإلكترونية	9
الفرع الأول : تعريـــــف الجريمة الإلكترونية	9
الفرع الثاني:أركان الجريمة الإلكترونية.	13
الفرع الثالث: الطبيعة القانونية للجريمة الإلكترونية و خصائصها	16
المبحث الثاني: مراحل تطور الجرائم الإلكترونية أنواعها و مشكلة إثباتها	**18**
المطلب الأول :مراحل تطور الجريمة الإلكترونية	18
الفرع الاول: أنواع الجرائم الإلكترونية	20
الفرع الثاني: مشكلة إثبات الجريمة الإلكترونية.	22
الفصل الثالث:الجريمة الإلكترونية من الجانب القانوني	
المبحث الأول: موقف المشرع الجزائري من الجريمة الإلكترونية.	**26**

فهرس المحتويات

المطلب الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية:	27
الفرع الأول: الدستور الجزائري	27
الفرع الثاني: قانون العقوبات	28
المبحث الثاني: قانون الإجراءات الجزائية الجزائري.	**32**
المطلب الأول: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:	34
الفرع الأول: القوانين الخاصة للتصدي للجرائم الإلكترونية	34
الفرع الثاني: الهياكل الخاصة للتصدي للجرائم الإلكترونية	36
الفصل الرابع: الجانب الميداني للدراسة	
1) إحصائيات القضايا المعالجة على المستوى الوطني	39
2) إحصائيات عدد الأشخاص المتورطين في القضايا المعالجة على المستوى	41
3) ضحايا القضايا المسجلة في سنة 2017 معزات للجنس	43
4) المتورطين في القضايا المسجلة في سنة 2017 معزات للجنس	44
5) عدد القضايات المسجلة في ولاية الأغواط معزات للأشهر (جانفي , فيفري , مارس) و سنوات (2017, 2018, 2019)	45
الخاتمة	48
قائمة المصادر و المراجع	51
الملاحق	

قائمة الجداول

رقم الجدول	العنوان	الصفحة
01	*إحصائيات القضايا المعالجة على المستوى الوطني*	39
02	إحصائيات عدد الأشخاص المتورطين في القضايا المعالجة على المستوى	41
03	ضحايا القضايا المسجلة في سنة 2017 معزات للجنس	43
04	المتورطين في القضايا المسجلة في سنة 2017 معزات للجنس	44
05	عدد القضايات المسجلة في ولاية الأغواط معزات للأشهر (جانفي , فيفري , مارس) و سنوات (2017, 2018, 2019)	45

الملخص:

تتكون الجريمة الإلكترونية أو الافتراضية(crimes cyber) من مقطعين هما الجريمة (crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والموبايل) ((2011). Taishankar & Halder) ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". (2013 , UNODC .)

كما تتناول أسباب الجريمة الإلكترونية، حيث تم تصنيف هذه الأسباب على ثلاثة مستويات من النظم هي :النظام الشخصي، والنظام الوسيط والنظام الكلي. فقد انطلقت من أن الجرائم الإلكترونية هي الأفعال الإجرامية التي ترتكب بواسطة الحاسب أو النطاق التقني مثل الإنترنت والشبكات، أو التي يكون فيها الحاسب والحيز التقني مستهدف للجريمة الإلكترونية. وتشمل الجرائم الإلكترونية ضمن هذا التحديد وليس حصرا على (الإرهاب الإلكتروني، والاحتيال وسرقة الهوية، والملاحقة والتحرش، وبريد النفايات، والفيروسات، وشم كلمات السر، والقنابل الذكية.

وتتلخص أسباب الجرائم الإلكترونية بانها ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي، حيث انتقل نشاط الناس من الواقع الفعلي (المادي) إلى الواقع الافتراضي، وهي جريمة عابرة للحدود الوطنية .وقد سهل انتشار الجرائم الإلكترونية سهولة الوصول للمستهدفين وانخفاض الكلفة، والغفلة في تنفيذها وضعف الرقابة والسرعة في تنفيذها وتوظيف الاتصالات والتفاعلات في ارتكابها، وقلة الخطورة على الجناة، وسرعة الكسب غير المشروع، والفرص المتاحة لارتكابها، والضغوط الشخصية والعامة على الجناة، وضعف الرقابة ت عامة. كما ساهمت عوامل التحضر السريع، والبطالة والرغبة بسرعة الثراء، وضعف التشريعات وضعف أدوات الحماية، وتوافر الفرصة لارتكابها وغياب الحراسة التقنية في انتشارها. وينفذها شباب يسعون للشهرة أو مجرمون محترفون يسعون للكسب والثراء، أو إرهابيون.

Abstract :

Electronic or virtual crime (crimes cyber) consists of two parts, crime (crime) and (cyber). The term electronic is used to describe the idea of a part of the computer or the information age. The crime is the behavior and actions outside the law. Electronic crimes are "violations committed against individuals or groups of individuals motivated by the crime and with the intent to harm the victim's reputation or physical or mental harm to the victim, directly or indirectly, using communication networks such as the Internet (such as chat rooms, e-mail, and mobile phones)" (Taishankar, 2011). & Halder.) and represents the core of cybercrime. Beyond this description, however, computer-related acts for personal purposes, financial gain or harm, including forms of identity-related crime, and acts related to computer contents all fall within the broader meaning of the term "crime." electronic." (2013, UNODC.)

It also addresses the causes of cybercrime, as these reasons are classified into three levels of systems: the personal system, the intermediary system and the total system. It proceeded from the fact that electronic crimes are criminal acts committed by means of a computer or technical domain such as the Internet and networks, or in which the computer and the technical space are targeted for cybercrime. Electronic crimes within this definition include, but are not limited to (electronic terrorism, fraud and identity theft, stalking and harassment, waste mail, viruses, password sniffing, and smart bombs.

The causes of cybercrime can be summed up as a social phenomenon compatible with the transition of societies to a digital society, where people's activity has moved from actual (physical) reality to virtual reality, which is a transnational crime. The spread of cybercrime has facilitated easy access to the targets, low cost, negligence in its implementation, weak oversight and speed in its implementation, use of communications and interactions in its commission, low risk for perpetrators, speed of illicit gain, opportunities to commit it, personal and public pressures on perpetrators, and weak oversight in general. The factors of rapid urbanization, unemployment, the desire to get rich quickly, weak legislation and weak protection tools, the opportunity to commit it, and the absence of technical guards also contributed to its spread. It is carried out by young people seeking fame, professional criminals seeking to gain and riches, or terrorists.

مقدمة

مقدمة:

في عام 2011،كان هناك مليار شخص على الأقل كان لهم وصول إلى شبكة الإنترنت ، أي ما يعادل أكثر من ثلث إجمالي سكان العالم. وأن أكثر من 60 في المائة من جميع مستخدمي الإنترنت هم من البلدان النامية ، وهناك 45 % من جميع مستخدمي الإنترنت دون سن 20عاما. كما تشير التقديرات أنه قبل عام 2017، فأن اشتراكات (broadband) المتنقل سوف تقترب من 70% من إجمالي عدد سكان العالم. وبحلول العام 2020، فأن عدد أجهزة الشبكة ("إنترنت الأشياء") سيفوق عدد الناس بمعدل (106) ستة إلى واحد، محولين المفاهيم الحالية للإنترنت. في عالم الغد عالم الشبك فائق السرعة ، سيصبح من الصعب أن نتخيل الجريمة الإلكترونية "، وربما أي جريمة، لا تنطوي على أدلة الإلكترونية مرتبطة مع بروتوكول الإنترنت الاتصال**IP**) **(UNODC, 2013)**

تميز القرن 21باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسعت الإنترنت أضعافا مضاعفة. حاليا ، حوالي هناك 820مليون شخص يستخدمون الإنترنت ، بزيادة قدرها 126 في المئة من 2000–2005InternetWorldStats.com,لقد وفرت السهولة النسبية لاستخدام الإنترنت، والحصول على الإنترنت على نحو متزايد أكثر للأنترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة، كل ذلك مكن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة ، والترفيه ، والتعلم، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت. وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني ، والذي يعرف بأنه "مكان لأجل غير مسمى حيث يتفاعل الأفراد والتجمعات . **(Britz, 2004, P2**) ويتصف الفضاء الإلكتروني بأنه مكان بلا حدود مادية أو اجتماعية تحرم الأفراد من العيش فيه.

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة. ولنا إن نتصور حجم التفاعلات التي تتم في الواقع الافتراضي سواء كانت شخصية أو مؤسسية أو في مجال الأعمال أو الخدمات أو الثقافة... فعلى سبيل المثال على الفيس بوك (Facebook) أعجب بصورة أوباما وهو يحتضن زوجة فيما سمي لحظة الفوز 4 مليون شخص، ومتوسط عدد الأصدقاء على حساب الفيس بوك 130 صديق وعدد المشتركين 850 مليون منهم 21% في أسيا، و 488 مليون يستخدمون الفيس بوك الجوال، و 23% من المشتركين يتفقدون حسابهم 5 مرات في اليوم. وهناك أكثر ن مليون موقع متصل مع الفيس بوك وتوضع 250 مليون صورة يومية، وفي عام 2012تم تشغيل 210000 سنة من الموسيقى. من المشتركين 43% ذكور و 57% إناث (**Vitality , 2012**)

وللأسف، فان الفضاء الإلكتروني ينتج أنواع جديدة من الجريمة تسمى الجريمة الإلكترونية cyber crimesمن خلال خلق فرص جديدة للمجرمين) **Wall 2005,**) قد مكنت مجرمي الفضاء الإلكتروني من تصفح الأنترنت وارتكاب جرائم مثل القرصنة، والاحتيال، والتخريب للكمبيوتر ، والإتجار بالمخدرات ، والتعامل في معلومات العدالة، والمواد الإباحية، والملاحقة **United**) **Nations Crime and Justice 1999 ,information UNCJIN**) دون القبض عليهم أو الكشف عن الجرائم. لقد تكونت أنماط جديدة من الجرائم من منها: لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم التي تخترق الحماية الأمنية في النظم القانونية ويتم تجنب العقاب فيها (**البداينة،1999**)

ووفقا لمكتب إحصاءات العدل فأن (BJS) انخفض معدل جرائم العنف في البلاد 10 في المئة في عام 2001 واستمر في الانخفاض منذ عام 1994. كما سجلت جرائم الإيذاء العنيف والممتلكات أدنى مستوى لها معدلات الجريمة منذ استخدام المسح الوطني لضحايا الجريمة (cvs) في العام 1973 من

ناحية أخرى، فإن عدد ضحايا الجريمة الإلكترونية على ارتفاع، نظرا لزيادة في عدد مستخدمي الإنترنت. لقد تزايد عدد ضحايا الجرائم الإلكترونية وخاصة الذين يعانون من خسارة مالية، أو المهددين أو المطاردين، فهي مشكلة تستحق الدراسة. ويمكن دراسة الجريمة الإلكترونية يمكن من خلال وجهات نظر مختلفة، بما في ذلك نظر المجرم أو وجهة نظر الضحية. وتمثل الجريمة الإلكترونية المجال الجديد من الأبحاث في مجال علم الجريمة**2003 .(Torosyan,)**

إن المعلومات والبيانات مثلها مثل أية سلعة ذات قيمة مادية عالية عرضة للجريمة بما في ذلك الاحتيال والسرقة والتعدي والتخريب..ألخ. وتزداد جرائم المعلومات يومية، وأصبحت محط حديث وسائل الإعلام والباحثين والعلماء. عندما سئل ويلي سوتن (Sutton) لماذا سطى على البنك أجاب "لأن المال موجود هناك"، والمال اليوم هو المعلومات، ولقد تعلم المجرمون اليوم مكان وجود المال ويمكنهم سرقة كميات بمخاطرة أقل. ولقد تأزمت العلاقات بين الدول بسبب سرقة المعلومات (أسرار عسكرية تتعلق بتقنيات متقدمة) (والأمثلة على ذلك بين الولايات المتحدة والصين، وكندا، والصين).

لقد أصبحت الجريمة الإلكترونية وجرائم الحاسوب ونظمها، بلا حدود، وهي عالمية، التحقيق فيها والحكم عليها عملية معقدة. وترتكب هذه الجرائم من قبل الأفراد أكثر مما ترتكب من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب وشبكات المعلومات. كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة (**البداينة، 1998**).

الفصل الأول:

الجانب المنهجي للدراسة

1.مشكلة الدراسة

إن التطور التقني أساليب إرتكاب الجرائم وخصوصا تلك التي تتم عبر الإنترنت والحاسوب ووسائل التواصل الاجتماعي، تتطلب من سلطات إنفاذ القانون أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي، لذلك تكمن مشكلة الدراسة في كيفية تقديم دليل رقمي إلكتروني مقبول وذي حجية أمام القاضي الجزائي.

كما تثور إشكالية أخرى تتعلق بمدى كفاية القواعد التقليدية في التشريع الجزائي الجزائري لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في ظل الفراغ التشريعي بخصوص التنظيم القانوني لهذا النوع من الجرائم في التشريع الجزائري.

2.الإشكالية :

- ما هو مفهوم الجريمة الالكترونية ؟
- ما هي طبيعة المشكلات الموضوعية والإجرائية التي يثيرها هذا النوع من الجرائم ؟
- ما مدى كفاءة معالجة المشرع الجزائري لمواجهة مثل هذه المشكلات ؟

3. أهداف الدراسة

تهدف هذه الدراسة إلى التعريف بماهية الجريمة الإلكترونية، و المشكلات الموضوعية والإجرائية التي تثيرها، كذلك تهدف إلى المساهمة في إيجاد الحلول للمشكلات العملية والقانونية في الجرائم الإلكترونية، ومحاولة التعمق في كيفية مجابهتها من خلال التشريعات .

وأيضا تهدف إلى وضع ما توصلت إليه من نتائج وتوصيات بين يدي المشرع الجزائري على أمل أن نجد أذنا صاغية من المشرع الجزائري في ضرورة التدخل، ووضع تشريع خاص متكامل يهدف إلى مجابهة الجرائم الإلكترونية، والحد منها، للحفاظ على حقوق الأشخاص في المجتمع الدولي والداخلي على السواء لسد الثغرات في وجه التطور السريع للجرائم الإلكترونية.

4.أهمية الدراسة

يكتسب موضوع هذه الدراسة أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثة من قبل مرتكبي الجرائم لتسهيل ارتكابهم لجرائمهم.

إن موضوع هذه الدراسة أهمية نظرية وعملية لكونه يمس كثيرا من مصالح انباء المجتمع، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام الإلكتروني ونظم الشبكات، وتحديد صور الاعتداء على المعلومات، والأنماط المستجدة للجرائم الإلكترونية، كما تظهر أهمية الموضوع من خلال التعرف على الاتجاهات التشريعية الدولية والإقليمية لحماية المعلومات ونظمها الإلكترونية.

كما تكمن أهمية هذه الدراسة في محاولة إيجاد الحلول للمشكلات التي تثيرها الجرائم الإلكترونية في التشريع الجزائري فالمشرع الجزائري قد يستفيد من هذه الدراسة المتواضعة، من خلال التعرف على أكثر المشكلات العملية والقانونية بشقيها الموضوعي والإجرائي التي تثيرها هذه الجرائم المتجددة بشكل مستمر.

كما أن هذه الدراسة تظهر أهميتها من خلال استفادة الباحثين والقضاة من نتائجها وتوصياتها والبناء عليها وتطويرها لإجراء دراسات معمقة في مجال تقنية المعلومات وقانون الكمبيوتر.

5.تحديد المفاهيم

المصطلحات الإجرائية:

من المصطلحات ذات العلاقة، هي:

-**نظام المعلومات:** مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونية، أو إرسالها، أو تسلمها، أو معالجتها، أو تخزينها، أو إدارتها.

- **البيانات:** الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها.

-**المعلومات:** البيانات التي تمت معالجتها وأصبح لها دلالة.

-**الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها.

-**الموقع الإلكتروني:** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان.

-**التصريح:** الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع إلكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول اليها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته.

- **البرامج:** مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات.

- **الفيروسات:** هي برامج يتم إنتاجها خصيصا لكي تلحق نفسها ببعض البرامج المشهورة وذلك عن طريق تزييف أو تعديل بسيط للتوقيع الخاص بالبرنامج الأصلي (مجموعة الأرقام الثنائية)، وتتمكن هذه البرامج من تدمير البرامج والمعلومات أو إصابة الأجهزة بالخلل بعدة طرق، فمنها ما يبدأ بالعمل

مباشرة عند الإصابة، وبعضها عند تنفيذ بعض الأوامر، وتتميز هذه الفيروسات بقدرتها على التكاثر والانتقال من جهاز إلى أخر عن طريق الملفات المتبادلة بين المستخدمين .[1]

– **المستند الإلكتروني:** هو عبارة عن سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر ويكون قابل للاسترجاع بشكل يمكن فهمه).

– **الجريمة الإلكترونية:** هي فعل غير مشروع ناتج عن إرادة آثمة يقرر لها القانون عقوبة وهي أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.[2]

6.الدراسات السابقة:

من الدراسات ذات الصلة بموضوع هذا البحث:

–دراسة العنزي، سليمان بن مهجع (2003) دراسة بعنوان: "وسائل التحقيق في جرائم نظم المعلومات"، أكاديمية نايف العربية للعلوم الأهلية، رسالة ماجستير.

هدفت هذه الدراسة إلى تحديد وسائل التحقيق في الجرائم المعلوماتية وذلك بالكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتجديد أنماطها ودوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل مجرمين نظم المعلومات، وبذلك تختلف عن دراستي كون الدراسة الحالية تبحث في التعريف و المشكلات الناجمة عن الجرائم الإلكترونية دون البحث في وسائل التحقيق فيها.

– الدسوقي، محمد (2003) دراسة بعنوان: "الحماية الجنائية لسرية المعلومات"، دار الكتب القانونية، مصر.

تناولت هذه الدراسة مسألة ضخامة التدفق والمخزون المعلوماتي الإلكتروني وتنوعه وانطوائه على أسرار البشر وخصوصياتهم مشيرة إلى أن هذا المخزون بات ميدانا خصبا للمتطفلين والمجرمين.

[1].المومني، نهلا عبد القادر (2012). الجرائم المعلوماتية، دار الثقافة، عمان، طا، الإصدار السادس،ص 50
[2].المومني، نهلا عبد القادر ،المرجع السابق ص 51

7.الإطار النظري للدراسة

قمت بتقسيم هذه الدراسة إلى اربعة فصول تناولت في الفصل الأول الجانب المنهجي للدراسة، وفي الفصل الثاني مفهوم الجريمة الإلكترونية من خلال التعريف بها .

وفي الفصل الثالث سنتكلم عن إطارها القانوني ، وفي الفصل الرابع سوف نقوم بتسليط الضوء على الحلول التشريعية والعملية من أجل مكافحة تحديات ومشكلات الجرائم الإلكترونية، وفي الخاتمة سوف نتعرض للنتائج والتوصيات التي خلصت إليها الدراسة.

8.المنهج المستخدم

سأتبع المنهج التحليلي الوصفي من خلال محاضر الشرطة في الجزائر ، للوصول إلى نتائج وتوصيات تجيب على أوجه النقص التشريعي لدى المشرع الجزائري بخصوص مواجهة تحديات ومشكلات الجرائم الإلكترونية.

الفصل الثاني:

الجريمة الإلكترونية

المبحث الأول: الإطار المفاهمي للجريمة الإلكترونية.

سوف نتعرض في هذا المبحث إلى مفهوم الجرائم الالكترونية المتصلة بشبكة الانترنت،من حيث تعريفها،أركانها وتحديد طبيعتها القانونية وخصائصها(المطلب الأول) مراحل تطور الجريمة الإلكترونية أنواعها ومشكلة إثباتها (المطلب الثاني)

المطلب الأول: مفهوم الجريمة الإلكترونية:

أصبحت الجريمة الإلكترونية موضوعا واسعا ،ورغم صعوبة إيجاد تعريفا جامعا مانعا لها إلا أن اجتهاد كل من الفقهاء و الباحثين أدى إلى عدة تعريفات لها وإن كانت قد تباينت تبعا لمحل اهتمام كل فئة، فمنهم من عرفها من الجانب التقني الفني والبعض الآخر من الجانب القانوني،و من أجل مفهوم شامل للجريمة لا بد من تعريفها من كل هذه الجوانب (الفرع الأول)،و بيان أركانها (الفرع الثاني) الطبيعة القانونية للجريمة الإلكترونية وخصائصها(الفرع الثالث)

الفرع الأول : تعريـــــف الجريمة الإلكترونية:

1- من الجانب التقني الفنـــــــــــــي.

الجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي.كما يعرفها البعض الآخر: بأنها تصرف غير مشروع يؤثر في الاجهزة و المعلومات الموجودة عليها.[1]

[1].عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2006 ، ص، 01 و02 .

كما يعرفها البعض الآخر: بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها.[1]

فقد أنقسم أنصار تعريف الجريمة من الجانب التقني والفني فالبعض استند إلى موضوع الجريمة والبعض الآخر إلى وسيلة الجريمة

ا- أهم التعريفات التي أستندت على موضوع الجريمة:

انها " نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه "[2]وتعريفها بانها " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات "[3] او هي " أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " [4]او هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "[5]

[1].عبد الفتاح بيومي حجازي ،نفسه ص 01-02

[2]. هشام محمد رستم : الجوانب الاجرائية للجرائم المعلوماتية ــ مكتبة الالات الحديثةــ اسيوط 1994، ص 31

[3].هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992 ، ص 20 .

[4]. د/هشام محمد رستم ، المرجع نفسه ، ص 31

[5].www.goa.gov – :- انظر GOA مكتب المحاسبة العامة للولايات المتحدة الامريكية.

ب- أهم التعريفات التي أستندت على وسيلة الجريمة:

فان أنصار هذا الاتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة ، وبالتالي تعرف[1] على أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" كما تعرف بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك تعرف بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا" [2]،وانها " كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية "[3] يعتبر هذا التعريف الأخير الرأي الراجح لتبنيه من قبل العديد من الباحثين والدارسين [4] نظرا لشمولته بحيث يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

2- من الجانب القانوني

تعرف بأنها: " مجموعة الأفعال و الأنشطة المعاقب عليها قانونا و التي تربط بين الفعل الإجرامي و الثورة التكنولوجية ." و تعرف كذلك على أنها :" نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي" [5]كما أن هناك من عرفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني "[6]وبأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة

---

[1] . Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts 1989, P. 104

[2]. هشام محمد رستم ، المرجع نفسه ، ص 29 و 30

[3].هدى قشقوش،المرجع السابق،ص22

[4]. هشام محمد رستم ، المرجع السابق ، ص 35

[5]. عبد الفتاح بيومي حجازي، المرجع نفسه، ص 06

[6].محمد عادل ريان ، جرائم الحاسب الالي و أمن البيانات،بيروت،2002،ص 03

المعلوماتية بغرض تحقيق الربح" [1]وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال .كما عرفت بأنها : "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب."

أما بالنسبة لبعض الفقه المصري ، فهي تنشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية وهناك فريق أخر يرى أن الجريمة المعلوماتية هي " عمل أو إمتناع يأتيه إضرارا بمكونات الحاسب ،وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا ". كما عرفها آخرون بأنها " كل فعل إيجابي أو سلبي عمدي يهدف إلى الإعتداء على تقنية المعلوماتية أية كان غرض الجاني".[2]

أما المشرع الجزائري لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة[3] إستنادا إلى قانون العقوبات الجزائري المعدل والمتمم لم يعرف جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال ، تحت عنوان " الجرائـــــم الماسة بنظـــــام المعالجـــــة الآلية للمعطيات"[4]

---

[1]. محمد عادل ريان،المرجع نفسه،ص 18

[2]/أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية ، الأسكندرية ، 2009 ، ص 106

[3]المقدم عز الدين عز الدين ، ملتقى حول الجرائم المعلوماتية ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ،بسكرة في:2015/11/16 .

[4].القانون رقم 15/04 المؤرخ في 2004/11/10

الفرع الثاني:أركان الجريمة الإلكترونية.

تتمثل أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن الشرعي و المادي والمعنوي:

1- الركن الشرعي:

معناه إعتراف المشرع والنص على تجريم الفعل المرتكب،"لاجريمة ولا عقوبة إلا بنص..." بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات.[1]

2-الركن المادي:

يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية ،علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقيق نتيجتها ، (مثلا: انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الا أنه لا مناص من معاقبة الفاعل.(

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب،(مثلا: جريمة الغش المعلوماتي : الركن المادي فيها هو تغيير الحقيقة في التسجيلات الكترونية أو المحررات الإلكترونية.[2]

3- الركن المعنوي: يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها أي العلم و ارادة.

[1]. القانون رقم04-15 المؤرخ في10 نوفمبر2004، المادة394 مكرر.

[2].محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992. ص 4 .

– العلم :هو إدراك الفاعل للأمور . – أما الإرادة : فهي اتجاه السلوك الإجرامي لتحقيق النتيجة. طبقا للمبادئ العامة المعروفة في قانون العقوبات ،قد يكون القصد الجنائي عاما و خاصا ،القصد الجنائي العام : هو الهدف المباشر للسلوك الإجرامي و ينحصر في حدود إرنكاب الفعل.

أما القصد الجنائي الخاص : هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة (مثلا: في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه).وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الالكترونية ؟

الأصل إن الفاعل في الجريمة الالكترونية يوجه سلوكه ألإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هــذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الانترنيت ، و جرائم نشر الفيروسات عبر الشبكة) .وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي[1]

4-مرتكبو الجريمة الإلكترونية:

أنواع الجناة في جرائم الانترنت كما يُطلق عليهم إسم القراصنة،و يمكن حصر هؤلاء في ثلاثة فئات :

[1].محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، المرجع نفسه. ص 13

أ- الهاكرز: ويُطلق هذا الاسم على القراصنة الذين يتّخذون من الجرائم الإلكترونية، والقرصنة هواية أو فضولي ليس أكثر ويكون غرضها تخريبيّاً ليس هادفاً لغايات ، وتكون غالباً من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الإلكترونية والحاسوب.

ب- الكراكرز: وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.

ت- الطائفة الحاقدة: تستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية،وقد يكون(تطرف أو جاسوس أو مخترق الأنظمة)[1]

ويمكن رد دوافع إرتكاب الجريمة الإلكترونية إلى دوافع مادية، سعياً لإشباع الرغبة بتحقيق الثراء أو دوافع شخصية، التعلّم، التعلّم، الانتقام ،التسلية سياسية.

حتى يتمكن القراصنة من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات عدة وأبرزها:

الاتصال بشبكة الإنترنت، توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب،وسائل التجسس، ومنها ربط الكاميرات بخطوط الاتصال الهاتفي،البار كود، وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز،طابعات ،هواتف رقمية ونقالة [2]

[1].عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005 ،65

[2].عبد الفتاح مراد ,المرجع نفسه،ص،68

الفرع الثالث: الطبيعة القانونية للجريمة الإلكترونية و خصائصها:

تعتبر الجرائم التي ترتكب من خلال شبكة الانترنت ، جرائم ذات طبيعة خاصة وخصائص منفردة ، لا تتوافر في الجرائـــــــــــــــــــــــم التقلـــيدية، سواء من حيــث أسلوب وطـــــرق ارتكابها،او شخـــــص مرتكبيها.

أولا:الطبيعة القانونية الجريمة الإلكترونية:

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى إرتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة . على أساس أن هذه الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال أو معالجة النصوص . و صعوبة التكييف القانوني للهذه الجرائم تكمن في طبيعتها الخاصة.

بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة ، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات ،و متابعة مرتكبيها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[1]

[1].محمد زكي أبو عامر وعلي عبد القادر القهوجي ، قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة1993 ، ص9 .

ثانيا:خصائص الجريمة الإلكترونية

- 1جريمة عالمية:

بمعنى انها تتعدى الحدود الجغرافية للدول،إنها جرائم عابرة للقارات ، لأنه مع إنتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن ان يكون الجاني في بلد و المجني عليه في بلد آخر.[1]

-2جرائم صعبة الإثبات:

صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم إكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أتها تفتقر إلى الدليل المادي التقليدي كالبصمات. كما يصعب الاحتفاظ الفني بآثارها أن وجدت، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها،لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع و التضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول الى الدليل وقد يلجا مرتكبيها لتشفير التعليمات لمنع إيجاد أي دليل يدنيه.[2]

-3جرائم ناعمة: إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة ،وغيرها ، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن ، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم

[1].عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، المرجع السابق، ص 42

[2].هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999 ، ص،24 .

بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.[1]

4-عدم التبليغ : عند وقوع الجريمة بواسطة الانترنت نجد ان بعض المجني عليهم يمتنعون عن ابلاغ السلطات المختصة خشية على السمعة و المكانه ،و عدم اهتزاز الثقة في كفاءته خاصة اذا كان كيان او هيئة معينة وقد اقترح في و م أ بان تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها، بالإبلاغ عما يقع عليها من جرائم متى وصل الى علمهم ذلك مع تقرير جزاء في حالة إخلالهم بهذا الالتزام.

المبحث الثاني: مراحل تطور الجرائم الإلكترونية أنواعها و مشكلة إثباتها:

عرفت الجرائم الالكترونية تطورا لا يستهان به، وهي كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها مما أدى إلى صعوبة إثباتها،و هذا راجع إلى التطور المستمر للشبكة و الخدمات التي تقدمها ،وعليه خصصنا هذا المطلب لمراحل تطور الجرائم الإلكترونية (الفرع الول) أنواع الجرائم الإلكترونية(الفرع الثاني) مشكلة إثبات الجريمة الإلكترونية(الفرع الثالث)

المطلب الأول :مراحل تطور الجريمة الإلكترونية:

مر تطور الجرائم الإلكترونية بثلاثة مراحل تبعا لتطور التقنية واستخدامات الحاسوب.

1-المرحلة الأولى: بظهور استخدام الكمبيوتر و ربطه بالشبكة في الستينات إلى السبعينيات ،ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة و تدمير

[1].عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي ، دار الكتب والوثائق المصرية،2006 ص 46

أنظمة الكمبيوتر و التجسس ألمعلوماتي ،و شكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة جرمية مستجدة ؟و هل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟ ، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني و مع توسع

الدراسات تدريجيا و خلال السبعينات بدا الحديث عنها كظاهرة إجرامية جديدة.

– 2المرحلة الثانية: في بداية الثمانينات، تأكد مفهوم جديد لجرائم الكمبيوتر والانترنت حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر و زرع الفيروسات الالكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج،و شاع إصطلاح "الهاكرز " المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي المتفوق.

–3المرحلة الثالثة: حيث شهدت فترة التسعينات تناميا هائلا في حقل الجرائم الالكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيلات لعمليات دخول الأنظمة واقتحام

شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت[1].

بحيث نمت الإنترنت بشكل مذهل خلال هذه الفترة ، بعد ما كانت مجرد شبكة أكاديمية صغيرة وتحولت الى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات ، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها ، دون مراعاة تحديات أمن المعلومات ، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة .وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية و تسببت في

[1]. عبد الفتاح مراد، المرجع السابق ص 47.

أضرار بالغة ، وهو ما أدى الى لفت النظر الى حاجة شبكة الإنترنت الى توفير معايير من الأمن ، وبدأ التفكير مليا في الثغرات ونقاط الضعف.

.وعليه قد يكون الكمبيوتر هدفا للجريمة، وغايته المعلومات المخزنة و السيطرة على النظام دون التصريح و السرقة و الاعتداء على الملكية الفكرية لخ....

كما قد يكون الكمبيوتر محل للجريمة ، كحالة استغلال الكمبيوتر للإستلاء على أموال الغير بإجراء تحويلات غير شرعية .كما أن الكمبيوتر قد يعد أداة للجريمة،كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد غير قانونية[1]

الفرع الاول: أنواع الجرائم الإلكترونية:

إن الجرائم الالكترونية جرائم متعددة ومتنوعة، ويستعصي حصرها بسهولة ،بحيث توجد عدة تصنيفات لجرائم الحاسب الآلي والانترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي ، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكابها ،غير أننا يمكن أن نجمل الجرائم التي وردت في أغلب التشريعات على النحو الآتي:

_ 1جريمة الدخول غير المشروع : معناه دخول الشخص إلى شبكة الانترنت بدون ترخيصا من الجهة المخولة منح هذه الصلاحية ،هذا الفعل يؤكد إرتكاب الجريمة عمدا عن طريق خرق التدابير الأمنية بقصد الحصول على بيانات الكمبيوتر.

_ 2تخريب أو إتلاف أجهزة المعلومات أو احدي مكوناتها: إن حماية شبكة المعلوماتية يستلزم التدخل لتجريم الأفعال التي تهدف إلي تخريب أو تعطيل أو إتلاف الأجهزة المادية و المتمثلة في

[1].مني الاشقر ، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، الناشر ش م م 2008 ص 70 وما يليها.

الحاسوب أو البيانات و المعلومات الموجودة بداخله لأن علة التجريم هي حماية المعلومات والأجهزة المادية من أفعال التخريب.

_ 3صناعة الفيروسات أو نشرها: هي وسيلة تستخدم لتدمير المعلومات و البيانات و البرامج و تعطيل شبكة المعلومات.[1]

-4الغش أو التغيير في مواصفات و خصائص تقنية المعلومات:

تتحقق الجريمة بتغير الخصائص أو المواصفات بسلوك إيجابي يأتيه الفاعل بطرق تدليسية إحتيالية بحيث تعرض تقنية المعلومات أو مكوناتها وما في حكمها إلى الغش الذي يعد انتهاكا لحقوق الملكية الفكرية.

– 5سرقة الأجهزة أو المكونات أو المعلومات و ما في حكمها:

تعتبر جريمة سرقة وإخلال بحقوق الملكية الفكرية أو براءة الاختراع أو العلامات المسجلة على أساس أن محل السرقة الحاسوب ككيان مادي.

-6جرائم النظام العام والآداب العامة الاتجار في الجنس البشري: الإخلال بالنظام العام والآداب، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام الآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة،والدعارة والمخدرات وغسيل الأموال.

-7 الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية.

[1].محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان بعنوان الاعلام والقانون الذي عقد فى الفترة من 14-15/ مارس 1999م ص 3 وما يليها .

إن التمعن في قراءة النصوص المنظمة لجرائم الانترنت في التشريعات العربية تكشف عن حقيقة متواترة في جل هذه التشريعات، ألا وهي اهتمامها الكبير عند تنظيم الانترنت وضبطه، بجعل حماية الدولة وأمنها كهدف أسمى من طرف المشرع قبل حماية أمن المواطن، وهذه مسألة واضحة على مستوى النصوص.

-8جرائم الإرهاب الاعتداء على الملكية الفكرية : إن المتضرر الأول من إساءة إستخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة والمتعلقة بالبرامج والإصدارات الخاصة بنظم المعلومات أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية ويتم نسخها و تداولها دون أن تنسب إلي صاحبها الأصلي وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية.[1]

مما لا شك فيه إننا بأمس الحاجة إلي التشدد في مواجهة منتهكي حقوق الملكية الفكرية خاصة وأ ن القوانين ذات العلاقة لم تجرم الأفعال التي تتم بإساءة استخدام تقنية المعلوماتية هذا من ناحية و من ناحية أخري أن قانون حماية المؤلف والحقوق المجاورة الوطني لا زال قاصرا في مواجهة هذه الانتهاكات.

الفرع الثاني: مشكلة إثبات الجريمة الإلكترونية.

الجريمة الإلكترونية ظاهرة اجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الاجرامي المجسدة للركن المادي لكل جريمة على حدى ، مع تطور أنماطها يوما بعد يوم وما أتاحته الشبكة من فرص جديدة لارتكابها،مما جعل إثباتها من العقبات التي

[1].عمر الفاروق ، المشكلات الهامة فى الجرائم المتصلة بالحاسوب الالي وأبعادها الدولية ، دراسة مقارنة ، ،مصر، ط 2 ،1995 ص 15 .

يعمل الخبراء على كسرها من أجل إيجاد وسائل إثبات ناجعة على أساس أنها تتطلب خبرة فنية عالية واعتماد أسلوب واضح في التحقيق.

-1أسباب صعوبة اكتشاف وإثبات الجرائم الإلكترونية.

أ- تمتاز الجرائم المعلوماتية بصعوبة الإكتشاف وإثباتها وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه ، فالجرائم التي تتم بواسطة إدخال الرموز و الأرقام ، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة.

ب- فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية،يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.

ت-كذلك وسيلة التنفيذ فيها تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها ، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات

ث- يصعب العثور على دليل مادي للجريمة وذلك راجع إلى إستخدام الجاني وسائل فنية وتقنية معقدة لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به

ج – تتطلب خبـــرة وتحكمـــا فـــي التكنـــولـــوجيـــا المعلـــوماتية عنـــد متـــابعتهـــا ، ولذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري ، لابد أن يكون المحقق متخصص حتى لا يتسبب في إتلاف الدليل الالكتروني[1].

ح– عدم وجود تعاون دولي، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين و لكن النتيجة تحدث في بلد أخر ليس بالضرورة أن ينتج هذا السلوك أثاره في بلد المجرمين .

خ– إختلاف النظم القانونية، و بالتالي عدم الإتفاق على الفعل المجرم ، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في غيرها من الدول .

د– التطور السريع للجريمة و المعالجة البطيئة لقضايا ،أستفادة المجرم من هذه العقبات للعبث والتخريب و الإستمرار في الجريمة.

ولهذه الأسباب وكذا الطبيعة الخاصة التي تتسم بها الجريمة أدى ببعض التشريعات الى تبنى الخبرة و المعاينة كأسلوبين للإثبات و التحقيق وكشف الجريمة.

2-الخبـــــــــرة والمعاينة:

أ–الخبرة: يجب أن تكون الخبرة في هذا المجال من نوع خاص يتماشى و خصوصية الجريمة الإلكترونية ،و قد تعمل بعض الدول على إعادة تأهيل بعض القراصنة من أجل الإستفادة من خبراتهم في الاختراق.وفي هذا الصدد يجب أن يتحلى الخبير بمؤهلات و مقدرة فنية عالية ،معرف تركيب الكمبيوتر،معرفة شاملة لشبكة الأنترنت، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.[2]

[1]. عمر الفاروق ، المرجع السابق ، ص16

[2].أسامة أبو الحجاج ،دليلك الشخصي الى الأنترنت ،دار النهضة المصرية،القاهرة ،1998 ،ص20

ب- المعاينـــــــــــة :قد تكون المعاينة حلا كإجراء لكشف بعض الجرائم الإلكترونية ، و لتكون المعاينة لا بد من وجود مسرحا للجريمة ، و هذا ما يصعب تحديده و بالتالي صعوبة الحفاظ عل الآثار المادية إن وجدت ،و كما قد يحدث أن الفارق الزمني بين حدوث الجريمة و إكتشافها واسعا مما يؤثر سلبا في اكتشاف الدليل المادي و لإجراء المعاينة لا بد من تبليغ الجهة المؤهلة عالميا بتقنية خاصة من أجل التحفظ على الأدلة الموجودة وحتى أن تكون معاينة محكمة يجب توافر عدة تدابير منها، ضمان عدم إنقطاع التيار الكهربائي، العمل ضمن فريق.

و خلاصة القول فإن تأهيل الضبطية القضائية و إعادة النظر في التشريع الذي يحكمها أضحى ضرورة لا بد منها من أجل فتح المجال للعمل الاستدلالي.

الفصل الثالث:

الجريمة الإلكترونية من الجانب القانوني

المبحث الأول: موقف المشرع الجزائري من الجريمة الإلكترونية.

رغم صعوبة ضبط و مكافحة جرائم الانترنت على الصعيد الوطني إلا أن هناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة جريمة الانترنت، فعلى امتداد الوطن العربي من المحيط إلى الخليج، نجد ترسنة قانونية تنظم جرائم الانترنت، وبدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام. كما أنه ركز كل اهتماماته على حماية الدولة، وجعلها من أسمى أهدافه.

حاول المشرع الجزائري ، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام أدى إلى اتساع نطاق الجريمة الإلكترونية فهي أصبحت لا تقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر ،ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي ومن جهة أخرى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة ضيف إلى ذلك المحافظة على مبدأ الشرعية الجنائية ، متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها.،وعليه خصصنا هذا المبحث إلى ،القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية(المطلب الأول)،القانون الإجراءات الجزائية(المطلب الثاني)،والقوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية(المطلب الثالث)

المطلب الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية:

قد أخص المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة، وعليه قسمنا المطلب الأول، الدستور(الفرع الأول)، القانون العقوبات(الفرع الثاني)،قانون الإجراءات الجزائية(الفرع الثالث)

الفرع الأول: الدستور الجزائري:

كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016[1]حماية الحقوق الأساسية و الحريات الفردية، و على أن تضمن الدولة عدم إنتهاك حرمة الإنسان. و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و الإجراءات الجنائية وقوانين خاصة أخرى و التي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة:

المادة 38 : الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة

لمادة 44: حرّيّة الابتكار الفكريّ والفنّي والعلمي مضمونة للمواطن. حقوق المؤلّف يحميها القانون. لا يجوز حجز أيّ مطبوع أو تسجيل أو أيّة وسيلة أخرى من وسائل التّبليغ والإعلام إلاّ بمقتضى أمر قضائيّ.الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون. تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

[1].القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14

لا يجوز انتهاك حرمة حياة المواطن الخاصة ، وحرمة شرفه ،ويحميها القانون ، سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة". أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي.

الفرع الثاني: قانون العقوبات:

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 بموجب القانون العقوبات رقم 04-15 المؤرخ – في 10 نوفمبر 2004 المتمم لأمر رقم- 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394المادة مكرر7.

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص ، الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات.

أولا- أنواع الجرائم الإلكترونية في قانون العقوبات الجزائري والعقوبات المقرر لها:

طبقا لقانون العقوبات الجزائري المعدل والمتمم والذي أستحدث فيه المشرع الجزائري قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات[1]،وعلى هذا الأساس يمكن تصنيفها إلى مايلي:

-1الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات

-2حذف أو تغيير لمعطيات المنظمة.[2]

-3ادخال او تعديل في نظام المعطيات.

- 4تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار

-5حيازة أو إفشاء أو نشر أو استعمال المعطيات.[3]

-6تكوين جمعية أشرار.[1]

---

[1]القانون رقم04-15 المؤرخ في10 نوفمبر2004 ،المعدل والمتمم

[2]أنظر: المادة394 مكرر " يعاقب بالحبس من ثلاثة اشهر الى سنة و بغرامة من خمسين ألف الى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات أو يحاول ذلك . تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة . و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من06 اشهر الى سنتين و غرامة من خمسين ألف الى مائة و خمسون ألف دينار "

[3]أنظر: المادة394 مكرر2 " يعاقب بالحبس من شهرين الى03 سنوات و بغرامة من1000.000 دج الى5000.000 دج كل من يقوم عمدا و عن طريق الغش بما يلي:

-1 تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-2 حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم

من خلال المواد القانونية السابقة والتي تمثل الركن الشرعي للجريمة الإلكترونية في التشريع الجزائري يمكن تكييف هذه الأفعال المجرمة بأنها جرائم ضد أموال الغير والمضرة بالمجتمع وهي تعتبر من ضمن جرائم الاختلاس و خيانة الأمانة و النصب غير السرقة لاعتبار أن السرقة فعل الاستيلاء على مال الغير ماديا.

ثانيا:العقوبات المقررة لهذه الجرائم:

طبقا لقانون العقوبات وبناءا على للمواد 11،12و13 من الاتفاقية الدولية للإجرام ألمعلوماتي فإن العقوبات المقررة للإجرام ألمعلوماتي يجب أن تكون رادعة وتتضمن عقوبات سالبة للحرية والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، و الشخص المعنوي.

-1العقوبات المطبقة على الشخص الطبيعي:

أ- العقوبات الأصلية : - عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات، حسب الفعل المرتكب و الغرامة تتراوح قيمتها من خمسين ألف دج إلي خمسة مائة ألف دج،حسب الفعل المرتكب :الدخول والبقاء بالغش (الجريمة البسيطة)،الدخول والبقاء بالغش (الجريمة المشددة)و تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،الاعتداء ألعمدي على المعطيات.[2]

[1]أنظر: المادة394 مكرر5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها ."

[2].أنظر: المواد القانونية السابقة،394مكرر،394مكرر1، 394مكرر2

ب-العقوبات التكميلية:

– المصادرة تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية. و إغلاق المواقع والأمر يتعلق بالمواقع (les sitesالتي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها .[1]

ت- عقوبة الشروع في الجريمة : جاءت به المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي واعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية ،بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ أصبح الشروع معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها .[2]

ث –الظروف المشددة: نص القانون على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، تضاعف العقوبة اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات العامة .[3]

---

[1]"أنظر: المادة394 مكرر6 " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

[2].أنظر:المادة394 مكرر7 " يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها"

[3]أنظر: المادة394 مكرر3 " تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات اشد".

2- العقوبات المطبقة على الشخص المعنوي:

يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي [1] . علما أن نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات امقررة.

3-عقوبة الاتفاق الجنائي: تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 [2]، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ،وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد.

المبحث الثاني: قانون الإجراءات الجزائية الجزائري.

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية،كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة . غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية.[3]

---

[1] أنظر: المادة394 مكرر4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي "

[2] .أنظر المادة: 394مكرر5،السابق ذكرها

[3] أنظر:المادة 37 من قانون الإجراءات الجنائية المعدل والمتمم بأمر رقم 15-02 مؤرخ في 23 يوليو سنة 2015 ،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8

كما نص على التفتيش في المادة 45 الفقرة 7من نفس القانون[1] المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه ، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطته المشرع بقواعد صارمة،وبالتالي لا تطبق الأحكام الواردة في المادة 44 من فانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم ٱلكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة6 [2]وكذا على "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10[3]. كما أن قانون الإجراءات الجنائية نص على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل و المتمم في الفصل الرابع تحت عنوان "في إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور". نصت المادة (65 مكرر5/3)على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالإعتراض و وضع ترتيبات تقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام

يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،الجريدة الرسمية عدد 40 .

[1]أنظر:المادة 45 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص 6.

[2].أنظر:المادة 51 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84،ص7

[3]أنظر:تمم الباب الثاني من الكتاب الأول بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص8 ،بفصل رابع

بعنوان "في اعتراض المراسلات و تسجيل الأصوات والتقاط الصور"ويشمل المواد من 65 مكرر5حتى 65مكرر10.

المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة[1]. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

المطلب الاول: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:

تناولنا في هذا المطلب،القوانين الخاصة للتصدي للجرائم الإلكترونية (الفرع الأول)، والهياكل الخاصة للتصدي للجرائم الإلكترونية(الفرع الثاني) كما يلي:

الفرع الأول: القوانين الخاصة للتصدي للجرائم الإلكترونية

أولا:قانون البريد والاتصالات السلكية واللاسلكية:

باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 منه[2]) ، كما نصت المادة2/ 84 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية"[3] .،كما نص في

---

[1]انظر: القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل و يتمم الأمر رقم 66–155المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. و المتضمن قانون الإجراءات الجنائية الجزائري. المادة 65 مكرر 3/5 "إذا أقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخذرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أوالإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم الفساد، يجوز لوكيل الجمهورية المختص بأن يأذن بما يأتي : – وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية .".. .

[2]المادة87 من قانون البريد والإتصالات السلكية واللاسلكية رقم 03– 2000 المؤرخ في2000/08/05. على أنه " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني "

أنظر: المادة 2/84 من نفس القانون،" تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية"[3]

المادة 105منه على إحترام المراسلات.[1] بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.[2]

ثانيا:قانون التأمينات:

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي[3]،في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني،وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع او من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93مكرر2.[4]

ثالثا:القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها:

---

[1]"أنظر:المادة 105من نفس القانون"لايمكن في أي حال من الأحوال ابتهاك حرمة المراسلات

[2]" أنظر :المادة127 من نفس القانون،" كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000 دج إلى 500.000 دج ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها .ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات

أنظر المادة 6 مكرر1،والمادة 65مكرر1 من القانون رقم 08/01 المؤرخ في 2008/01/23والمعدل والمتمم لقانون 83/01[3] المتعلق بالتامينات

[4]أنظر المادة 93 مكرر2و3 من نفس القانون، "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة "

جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والإتصال وكل ما يتعلق بالمنظومة

المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية.[1]من مراقبة و تفتيش المنظومات المعلوماتية عند الضرورة،و حجز المعطيات المعلوماتية،و حفظ المعطيات المتعلقة بحركة السير.على الإلتزامات الخاصة بمقدمي خدمة الإنترنت ،وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: الهياكل الخاصة للتصدي للجرائم الإلكترونية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال : وأنشئت بموجب القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية أللاقتصاد الوطني.[2]

ثانيا:الهيئات القضائية الجزائية المتخصصة : أنشئت بموجب القانون 14/04المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.تتمتع اختصاص إقليمي موسع طبقا للمرسوم

[1]أنظر:المواد من المادة الثانية حتى 14من قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا ّالإعلام والإتصال ومكافحتها.

[2]أنظر:القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكره.

التنفيدي رقم 348/06 المؤرخ في 2006/01/05.بحيث تنظر فيالقضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.[1]

ثالث:المعهد الوطني للأدلة الجنائية وعلم الجرائم .يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة ، جميعها تضمن إنجاز الخبرة ، التكوين والتعليم و تقديم المساعدات التقنية ،و دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.[2]

رابعا:المديرية العامة للأمن الوطني: تتصدى هده المديرية للجريمة الإلكترونية من عدة جوانب وأ منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم ،فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائيةINTERPOL هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين ، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.[3]

---

[1]أنظر: هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق،2016،ص3 .

[2]أنظر:د/ حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، جامعة بسكرة كلية الحقوق ، 2016 ، ص 40

[3]أنظر:د/علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الالي ، دار الجامعية للطباعة والنشر ، بيروت ، د ط، ، ص120 .1999

الفصل الرابع

الجانب الميداني

دراسة حالة من خلال "محاضر الشرطة"

إحصائيات القضايا المعالجة على المستوى الوطني

السنة	عدد القضايا المعالجة	النسبة%
2012	47	1.10
2013	108	2.59
2014	246	5.78
2015	567	13.33
2016	1055	24.80
2017	**2230**	**52.43**
مجموع	**4253**	**100**

من خلال الجدول الموضح نجد أن أكثر القضايا المعالجة كانت سنة 2017م بنسبة 52.43% و بعدها القضايا المعالجة في 2016م بنسبة 24.80% و تليها قضايا معالجة في 2015م بنسبة 13.33 % وكماتمثل نسبة 5.78% القضايا المعالجة في سنة 2014م و أما نسبة 2.59% فتمثل القضايا المعالجة في سنة 2013م لتكون في الأخير القضايا التي تم معالجتها في سنة 2012م نسبة 1.10% .

من خلال الإحصائيات السابقة نلاحظ أن معالجة القضايا الخاصة بالجريمة الإلكترونية سواء عبر مواقع التواصل الاجتماعي أو الإنترنت بصفة عامة هي في تزايد من سنة 2012م الى غاية 2017م و قد

يرجع هذا التحسن في معالجة مثل هذه القضايا لتطور تقنيات المراقبة و الحراسة لهذه الجرائم و الاهتمام الجاد و الضروري الذي فرضته قرع أجراس الخطر في مجتمعنا الجزائري منبها عن حجم الخسائر التي يمكن أن تنجم عن الجريمة الإكترونية و التي هي في تزايد مستمر و هو الأمر الذي جعل مصالح الدرك الوطني تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة إستعمال هذه التكنولوجيا . إضافة الى أن المواطن الجزائري كسر حاجز الخوف و أصبح أكثر وعي في الإبلاغ الجرائم الإكترونية و بما أن الفيسبوك و غيره من مواقع تواصل الاجتماعي و الإنترنت بصفة عامة بقوم على الصورة والكتابة و الفيديوهات فهو يساعد بسهولة في محاربة مثل هذه الجرائم و إذا أرجعنا هذه النتيجة الى مقاربة نظرية نجد أنها تتوافق مع مقاربة التفاعلية الرمزية التي تقول بأن" المعاني تتعدل وتتشكل من خلال عملية التأويل عبر الرموز " حيث أن الإنترنت ككل عبارة عن رموز و إشارات تستعمل في محاربة هذه القضايا حيث تسهل نشر الوعي و طرق التي يتبعها الفرد للتبليغ عن مثل هذه القضايا.

إحصائيات عدد الأشخاص المتورطين في القضايا المعالجة على المستوى

السنة	عدد الأشخاص المتورطين	النسبة%
2012	48	1.37
2013	91	2.60
2014	296	8.47
2015	543	15.54
2016	946	27.08
2017	1570	44.94
مجموع	3494	100

من خلال الجدول الموضح نجد أن أكثر الأشخاص المتورطين في القضايا المعالجة كانت سنة 2017م بنسبة 44.94% و بعدها الأشخاص المتورطين في القضايا المعالجة في 2016م بنسبة 27.08% و تليها الأشخاص المتورطين في القضايا المعالجة في 2015م بنسبة 15.54 % وكماتمثل نسبة 8.47% الأشخاص المتورطين في القضايا المعالجة في سنة 2014م و أما نسبة 2.60% فتمثل الأشخاص المتورطين في القضايا المعالجة في سنة 2013م لتكون في الأخير الأشخاص المتورطين في القضايا التي تم معالجتها في سنة 2012م نسبة 1.37% .

من خلال الإحصائيات السابقة نلاحظ أن عدد الأشخاص المتورطين في القضايا التي تم معالجتها في هذه سنوات هم في تزايد من سنة 2012م الى2017م و يمكن إرجاع هذا إلى التطور التكنولوجي الهائل في التقنية و الإنتشار الواسع الذي لاقته شبكة الإنترنت ساهم في عملية الإنجاز الرقمي و تسهيل الإنخراط في الشبكة حيث يقضي العديد من الشباب أوقاتهم أمام شاشات الحاسوب و في كثير من الأحيان تتحوال إلى إدمان لما لها من تأثير على نفسية الأشخاص المستخدمين و من بين هذه التأثيرات جرهم إلى الجريمة الإلكترونية و التي شاعت يكثرة في المجتمع الجزائري , حيث أن هذه الجريمة نتيجة إستغلال الأفراد تفتية المعلوماتية في غير الغرض الذي أنشئت من أجله سواء يقصد أو بغير قصد حيث أصبحت مواقع التواصل الاجتماعي أصبحت لترويج والتسخيرو الإبتزاز و التحايل مثلا , الفيسبوك فضاء واسع و إفتراضي بحيث لا تدري إذا كانت الشخصية التي تتواصل معها حقيقية أو مزورة, بإضافة إلى مشاركة في مجموعات على أساس أنها ثقافية أو تجارية وفي الحقيقة قد تكون مجموعة غير أخلاقية أو إجرامية فتتوراط معها , كما أن هناك مواقع تقترح في الفايسبوك وتكون بداية لصتياد الضحايا و ابتزازها .و إذا أردنا إستخدام مفاهيم الإتجاه التفاعلي الرمزي الذي يقول " أن النموذج الإنساني التفاعلي الرمزي إنما يعتمد على السلوك الذي يتحلى به و العلاقة التفاعلية التي تنشأ بينه و بينهم هذه العلاقة يتمخض عنها ظهور رموز لها أهميتها في تقويم الإفراد , و هي تحدد استمرار العلاقة أو انقطاعها " بإسقاط هده المقولة على موضوعنا يظهر لنا إمكانية تعرض الفرد لأحد الجرائم المذكورة سابقا في الفيسبوك أو غيره من مواقع التواصل من طرف مجموعة أو صفحة أو شخصية مزيفة جعلته يكون رموز تنعكس سلبا على حياته ا الأمر الذي يمكن أن يجعله يتوارط أكثر فأكثر في الجريمة.

ضحايا القضايا المسجلة في سنة 2017 معزات للجنس

الجنس / ضحيا القضايا المسجلة في 2017	ذكر		أنثى		مجموع	
	ت	%	ت	%	ت	%
الضحايا البالغين	94	74.01	33	25.98	127	92.02
الضحايا القصر	4	36.36	7	63.63	11	7.98
مجموع	98		40		138	100

يوضح الجدول التالي ضحايا القضايا المسجلة في سنة 2017 حيث نجد أن الضحايا البالغين يمثلون نسبة 92.02% مدعمة بنسبة 74.01% ذكور تقابلها نسبة 25.98 % إناث , و من جهة خرى بلغة نسبة الضحايا القصر 7.98% مدعمة بنسبة 63.63% إناث تقابلها نسبة 36.36% ذكور.

من خلال الإحصائيات نلاحظ أن أغلب ضحايا القضايا المسجلة في سنة 2017م هم أشخاص بالغين من جنس ذكور قد يرجع هذا الذكر في المجتمع العربي عامةو الجزائر خاصة له مساحة واسعة من الحرية سواء في العالم الواقعي أو حتى الإفتراضي حيث أن الذكر في مواقع تواصل الاجتماعي يستقبل كل ما يدخل لديه من طلبات صداقة و مجموعات وصفحات ممايزيد خطر وقوعه كضحية , إضافة الى ميل الذكور الى الألعاب الإلكترونية , كما يرجح أن الذكور يستخدامون الإنترنت أكثر من الإناث للبحث عن المعلومات و مع توفر الكثير من المعلومات على شبكة الإنترنت قد يقع المستخدم في محتوى غير صحيح وغير لائق مع غياب الخبرة قد يقعون في شباك المواقع الإلكترونية الإجرامية , وما يجعل هذه النسبة مرتفعة برغم من أن الضحايا بالغين وليسو بقصر هو خصائص الجريمة الإلكترونية والتي هي من أكثر أخطار الإنترنت تهديدا للمجتمعات هو خصائصها التي تتمثل في أنها تتسم بسهولة الوقوع في فخها و صعوبة الكشف عن مرتكب

الجريمة إلا بأساليب أمنية و تقنية عالية و سهولة إخفاء أثار الجريمة و الأدلة التي تدل على الجاني وهذا ما يجعل ضحاياها في تزايد , مثلا الفيسبوك فضاء واسع و متشعبة حيث أنه عالم افتراضي يحوي على مختلف الأجناس المختلفة في هويتها و انتمائها ودينها وشخصياتها لهذا لا يخلو هذا العالم الأزرق من مثل هذه الأخطار

المتورطين في القضايا المسجلة في سنة 2017 معزات للجنس

الجنس / متورطين في القضايا المسجلة في 2017	ذكر		أنثى		مجموع	
	ت	%	ت	%	ت	%
المتورطين البالغين	81	86.17	13	13.82	94	94.95
المتورطين القصر	4	80	1	20	5	5.05
مجموع	85		14		99	100

يوضح الجدول التالي المتورطين في القضايا المسجلة في سنة 2017 حيث نجد أن المتورطين البالغين يمثلون نسبة 94.95% مدعمة بنسبة 86.17% ذكور تقابلها نسبة 13.82 % إناث , و من جهة خرى بلغة نسبة المتورطين القصر 5.05% مدعمة بنسبة 80% إناث تقابلها نسبة 20% ذكور

نلاحظ من الإحصائيات أن أغلب المتورطين هم بالغين و من جنس الذكور ذلك راجع الى أن الذكور يتمتعون بمهارات تقنية عالية و دراية بالأسلوب المستخدم في مجال أنظمة الحاسب و كيفية تشغيله و كيفية تخزين المعلوماتي و الحصول عليها , كما أن الذكر دائما عنده فضول و الرغبة في قهر النظام و هذه الرغبة قد تزيد عنده الى أن يتورط في قضايا إجرامية إلكترونية , مثل رغبته في الحصول على المال أو التجسس من باب الفضول و سرقة حسابات الأفراد من باب المتعة حتى تصبح هذه الأساليب عادة وإدمان و طريقه لتورط في دوامة الإجرام الإلكترونية ,وما يدعم هذا غياب الرقابة و التوعية و الجهل بمخاطر و يسلبيات الإنترنت , فالفرد الجزائري يستهلك كل ما هو جديد بدون أن يكون له رصيد معريفي حول الشئ الذي يستهلكه , وهو الأمر الذي جعل سلبيات و أخطار الإنترنت على مجتمع الجرائري أكثر من إجابياتها ومنافعها

عدد القضايات المسجلة في ولاية الأغواط معزات للأشهر (جانفي , فيفري , مارس) و سنوات (2017, 2018, 2019)

	2017		2018		2019	
	ت	%	ت	%	ت	%
جانفي	05	35.71	14	28	22	31.42
فيفري	05	35.71	28	56	28	40
مارس	04	28.58	08	16	20	28.58
المجموع	14	100	50	100	70	100

يوضح الجدول عدد القضايا المسجلة في ولاية الأغواط حيث كانت نسب القضايا المسجلة في سنة 2017م على التوالي شهر جانفي و فيفري بنسبتين متساويتين تمثلت في 35.71% أما مارس فمثلت نسبة القضايا المسجلة فيه 28.58% , و من جهة أخر تشكلت نسب القضايا المسجلة في سنة 2018م على النحو التالي فيفري 56% جانفي 28% شهر مارس 16 % , أما فيما يخص سنة 2019م كانت القضايا المسجلة في كل من شهر فيفري بنسبة 40% و جانفي 31.42% و مارس 28.58% .

من خلال الإحصائيات حول القضايا المسجلة في ايطار الجريمة الإلكترونية بولاية الأغواط خلال ثلاث سنوات 2017-2018-2019م نلاحظ أن النسب المسجلة مهددة مما يعني تفشي و إستفحال هذه الظاهرة في هذا المجتمع الأغواطي المحافظ و هذا قد يعود إلى الهجرة من الريف الى المدينةهذه الظاهرة التي شهدتها ولاية الأغواط بشكل ملحوظ و ما يحمله أفراد الأرياف من رصيد معرفي ضئل جدا و تقليدهم لأفراد المدينة على جهل هو من أكبر مسببات الوقوع في الجريمة الإلكترونية , و ممكن أن نضيف سبب أخر وهو جد

مهم ومتفشي في ولاية الأغواط ألا وهو الطلاق الذي تحل فيه الولاية المراتب الأولى و التي تؤثر على الشاب أو المراهق الذي يكون قابل لتأثر و تعرض لأي معطى قد يعطى له بكونه ينتقل بيولوجيا ونفسيا من مرحلة الى مرحلة , إضافة الى الفراغ الذي يعاني منه الفرد الأغواطي و الجزائري عامة والذي يخلق لديه الفضول في الغوص في فضاء الإنترنت الى أن يقع في شباك أخطارها , كما لا ننسا غياب الضبط الغير الرسمي يدء من الأسرة الى مؤسسات المجتمع وهو الأمر الذي يعطل و لا يساعد الضيط الرسمي في الحد أو تقليل على الأقل من هذه الظاهرة المستفحلة في المجتمع الأغواطي خاصة و الجزائري عامة .

خاتمة

الخاتمة:

في خاتمة هذا العمل المتواضع، والذي لا أعتبره بحثا معمقا ،وإنما محاولة للإلمام بالموضوع وما يطرحه من إشكالات عديدة و مبادئ جديدة ،لقد توصلنا إلى نتائج جد هامة كما قدمنا بعض الاقتراحات التي رأيناها مفيدة لموضوع الدراسة.

أ- النتائج:

أهم النتائج التي توصلت لها الدراسة:

- ❖ لم يتفق على تعريف جامعا مانعا للجريمة الإلكترونية.
- ❖ تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.
- ❖ قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.
- ❖ رغم إجتهاد المشرع الجزائري للتصدي لهذه الجريمة،إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.
- ❖ إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية ، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في بيئة الرقمية.
- ❖ أن النصوص الوضعية لحماية حقوق المؤلف والحقوق المجاورة تعتبر غير كافية لمواجهة الاعتداءات الواقعة عليها عبر الانترنت.

ب- الاقتراحات:

- من واجب المشرع أن يوضع نصوصا قانونية واضحة وخالية من الغموض، بحيث أنها ستؤطر ظواهر اجتماعية جديدة مستقبلا.
- عند وضع النصوص يجب أن يدقق في حماية المواطن، على أساس أن حماية الأمن الرقمي يمكن أن تحيل على مفاهيم متعددة تتراوح مابين حماية الأشخاص، وحماية المجموعات وغيرها.
- ضرورة التعاون الدولي لمكافحة هذه جرائم من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية.
- عقد الدورات التدريبية التي تعتني بمكافحة الجرائم الإلكترونية.
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وبالتعاون مع التقنيين من أصحاب الخبرة.
- احتراما لحقوق الإنسان عامة ولحقوق المواطن خاصة وحتى تتكامل يجب أن يكفلها المشرع الجنائي بحماية القانونية الرادعة، وهذا بالتصدي لمواقع ووسائل اختراق المواقع بمختلف صورها.

قائمة المصادر و المراجع

قائمة المصادر و المراجع:

أولا: المصادر باللغة العربية:

1. أسامة أبو الحجاج ،دليلك الشخصي الى الأنترنت ،دار النهضة المصرية،القاهرة، 1998.
2. أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية الأسكندرية ، 2009.
3. عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2006.
4. عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005 .
5. عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي ، دار الكتب والوثائق المصرية،2006.
6. عر الفاروق ، المشكلات الهامة فى الجرائم المتصلة بالحاسوب الالي وابعادها الدولية ، دراسة مقارنة ، مصر ، ط 2، 1995.
7. محمد زكي أبو عامر وعلي عبد القادر القهوجي ، قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة1993.
8. محمد عادل ريان ، جرائم الحاسب الالي و أمن البيانات،بيروت،2002.
9. محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992.
10. مني الاشقر ، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، .2008.

11. هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992.

12. هشام محمد رستم ، الجوانب الاجرائية للجرائم المعلوماتية ــ مكتبة الالات الحديثة، اسيوط ، 1994.

13. هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999.

ثانيا: المؤتمرات وندوات علمية:

1) حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، جامعة بسكرة كلية الحقوق ، 2016.

2) محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق، جامعة حلوان بعنوان الاعلام والقانون الذي عقد فى الفترة من 14-15/ مارس 1999.

3) المقدم عز الدين عز الدين ، ملتقى حول الجرائم المعلوماتية ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، بسكرة في:2015/11/16.

ثالثا:القوانين والأتفاقيات:

1. القانون رقم04-15 المؤرخ في10 نوفمبر2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمي عدد71.
2. قانون الإجراءات الجنائية المعدل والمتمم بأمـــــــر رقـــــم 15-02 مـــؤرخ في 23 يـــولـــيـــو ســـنـــة 2015 ،يـــعـــدل ويـــتـــمـــم الأمـــر رقـــم 66-155 المـــؤرخ في 8 يـــونـــيـــو ســـنـــة 1966 والمـــتـــضـــمن قـــانـــون الإجـــراءات الجزائية،الجريدة الرسمية عدد 40.
3. قانون الإجراءات الجنائية المعدل والمتمم بقانون رقـــــم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص6 و7و8.
4. قانون البريد والإتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ 2000/08/05،الجرية الرسمية عدد48.
5. القانون رقم 08/01 المؤرخ في 2008/01/23والمعدل والمتمم لقانون 83/01 المتعلق بالتامينات ،الجريدة لرسمية عدد29
6. قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا ّالإعلام والإتصال ومكافحتها. الجريدة الرسمية، عدد 47.
7. اتفاقية بودابست للاتحاد الاوروبي 2001 المادة الاولى بالخصوص التي حددت مفاهيم المصطلحات

رابعا:المصادر باللغة الفرنسية والانجليزية:

1- Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989,

2- P . Catala , Les transformations de droit par l’ informatique , émergence du droit l’ informatique , ed des Parques 1983 .

3- Merle et Vitu , droit penal special . Paris 1976 no 2213 .Crim 29 Avril 1986 J .C.P 1987 – 11-20