المجلة الدولية للإتصال الإجتماعي
ISSN: 2437 – 1181

جامعة عبد الحميد بن باديس-مستغانم . الجزائر
المجلد: 5 العدد: 4 (2018) ص: 07 - 31

واقع الجريمة الالكترونية في مواقع التواصل الاجتماعي الحماية النظامية في دول مجلس التعاون الخليجي

The reality of cybercrime in social networking sites

د. فيصل كامل نجم الدين – باحث اكاديمي

faisalkamil79@gmail.com

تاريخ الإرسال: 14-10-2018 **تاريخ المراجعة: 11-11-2018** **تاريخ القبول: 04-12-2018**

ملخص البحث

تعتبر مواقع التواصل الاجتماعي ميدان خصب للجريمة المعلوماتية لانها تمثل قلب الثورة المعلوماتية ، وتأثيره على جمهور عريض من مستخدمي شبكة الانترنت ، ممثلاً في جرائم الإنترنت وشبكات التواصل الاجتماعي في العالم العربي، والتي منها جرائم المعلوماتية والإنترنت، وقد انتشرت جرائم المعلوماتية والإنترنت بشكل نسبي ، وترتَّب على هذا المخالف أضرار بالغة في حق الأفراد والمؤسسات، بل والدول ذاتها، فمنظومة الأمن القومي لأى من الدول قد يخترقها أي من المجرِمين الإلكترونيين (مخرب او مجرم معلوماتي) مثلاً، فالأمر لا يحتاج أكثر من شخص اعتاد المخالفات الإلكترونية، لكى يقوم باختراق مواقع الجهات المالية، والاطلاع على أسرارها وخصوصياتها، فضلاً عن ذلك، فالجرائم الإلكترونية تأتي على أشكال وتصنيفات متنوعة، كما أن المجرم الإلكتروني له صفات خاصة تختلف عن تلك التي يتصف بها المجرم العادي.

وقد سلكت دول الخليج مسلك أغلب دول العالم في حماية المعلومات، عن طريق قوانين حقوق الملكية الفكرية، بحيث تمتد حماية هذه القوانين، لتشمل برامج الحاسب الآلي وتطبيقاته، قبل أن إضافة إلى ذلك، أصدرت دولة الإمارات العربية المتحدة عام 2002م، في إطار حرصها على تغطية الفجوة التشريعية في مجال الاتصالات – وهو الأمر الذي تفتقده معظم الدول العربية – قانون التوقيع الإلكتروني والتجارة، وقد قضى هذا القانون بمنع مزودة خدمات الإنترنت من كشف أية معلومات يحصلون عليها في أثناء تزويد الخدمة .

مصطلحات البحث :

جريمة الكترونية : أعني بها في هذا البحث هي السلوكيات الخارجة عن القانون بأستخدام الحاسبات الالكترونية في مواقع التواصل الاجتماعي من (سب – القذف – روح الكراهية – الخ) بقصد إذاء الاخرين .

مواقع التواصل الاجتماعي : اعني بها في هذا البحث مجموعة التطبيقات المتاحة على الشبكة العنكبوتية والتي يستعملها الناس من أجل التواصل والتفاعل مع الآخرين .

الحماية النظامية : اعني بها منع الأشخاص من الاعتداء على حقوق بعضهم البعض بموجب أحكام قواعد قانونية معينة ومحددة . فالحماية بهذا المعنى تختلف من نوع لآخر تبعاً لاختلاف الحقوق المحمية، فقد تكون الحماية متعلقة بالحقوق المدنية أو الجنائية أو النشر أو غيرها .

Abstract

Social networking sites are considered fertile ground for cybercrime because they represent the heart of the information revolution and its impact on a wide audience of Internet users, represented by the crimes of the Internet and social networks in the Arab world, including cybercrime and the Internet. This violates the right of individuals and institutions, and even the States themselves, the national security system of any country may be penetrated by any of the cyber criminals (a terrorist or a criminal information) For example, it does not need more than a person accustomed to violations of the electronic Intention, in order to penetrate the financial party sites, and access to its secrets and privacy, in addition, electronic forms come Crimes and ratings varied, and the electronic offender has special qualities different from those that characterize the ordinary criminal.

The Gulf countries have followed the path of most countries in the world in the protection of information, through the laws of intellectual property rights, extending the protection of these laws, to include computer programs and applications, before

In addition, in 2002, the United Arab Emirates (UAE), in the framework of its keenness to cover the legislative gap in the field of telecommunications - which most Arab countries lack - the Electronic Signature and Trade Law. This law has prevented Internet service providers from disclosing any information they receive While providing service

Search terms:

Cyber crime: I mean in this research are the behaviors outside the law by the use of computers in the social networking sites of (insult – libel – the spirit of hatred – etc.) for the purpose of others.

Social media: I mean in this research the set of applications available on the web that people use to communicate and interact with others.

Systematic protection: I mean preventing people from attacking one another's rights under specific and specific legal rules. Protection in this sense varies from one type to another depending on the difference of protected rights. Protection may be related to civil, criminal, publishing or other rights.

مقدمة

عندما نتحدث عن الخلافات داخل شبكات التواصل الاجتماعي فتكون الجريمة الإلكترونية cyber crimes هي اساس هذا الخلاف ، وتتكون الجريمة الالكترونية 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 معنوي للضحية مباشر او غير مباشر باستخدام شبكات التواصل الاجتماعي ، والموبايل . 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 .

ما هي الجريمة المعلوماتية :

عقد في فينا عام 2000 م مؤتمر الامم المتحدة لمنع الجريمة الالكترونية ومعاقبة المجرمين ، فالجريمة المعلوماتية هي جريمة الحاسب الالي ويقصد بها : اي جريمة يمكن ارتكابها بواسطة الحاسوب او شبكة حاسوبية ، وهذه الجريمة من ناحية مبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية .

ايضا هناك تعريف الخبير الامريكي باركر الذي حدد مفهوم اوسع للجريمة المعلوماتية ، فهي من وجهه نطره : كل فعل اجرامي متعمد له صلة بالبيئة الالكترونية ينشأ عنة خسارة تلحق بالمجني عليه ، او كسباً يحققه الفاعل .

كثرت تعريفات جرائم المعلوماتية بتعدد النظم والقوانين وايضاً تعريف منظمة التعاون الاقتصادي والتنمية يعتبر من التعاريف المهمة ، والتي عرفتها : بانها كل فعل من شأنه الاعتداء على الاموال المادية والمعنوية ، ويكون ناتجاً بطريقة مباشرة او غير مباشرة من تدخل التقنية المعلوماتية .
[1]

ماهي دوافع الجريمة الالكترونية هل هي سرقة ام للتسلية او هي انتصار للذات ، ويمكن تصنيف المهاجمين الالكترونيين كما يلي :-

1/ الباحثون عن التسلية Vandals :

وتعتبر هذه الفئة من الفئات الرئيسية لجرائم المعلوماتية اذ تظهر بمظهر برئ هدفها اللهو والتسلية دون قصد الي الحاق الضرر والاذى لضحاياهم ومع استمرارهم في هذه التسلية شياً فشياً حتى تتحول الى قرصنة ومن امثلتهم من يقوم بحجوزات وهمية لدى شركات الطيران والفنادق والبواخر السياحية وغيرها ، وهؤلاء الاشخاص حين يخرجون الى الفضاء الانترنت فأن ذلك يكون من باب الفضول وليس بهدف الحاق الضرر ، او يتسببون بالضرر دون قصد ومن هؤلاء من تجذبهم المواقع المشهورة من وكالة ناسا الامريكية لابحاث الفضاء او وكالة CNN للانباء او موقع البيت الابيض الامريكي وغيرها من المواقع الهامة. [2]

2/ اثبات الذات : وغالباً يكون دوافع هذه الفئة هو الرغبة في اثبات الذات وتحيقق انتصار على تقنية نظم المعلومات ومن دون ان تكون لديهم نوايا سيئة ، ومنهم من يرغبون الي تحقيق ارقام قياسية او لديهم الشعور بالتحدي في اقتحام اشياء صعبة ويعتبر اصحاب هذه النوايا لديهم ميول للشهرة ، لان المعلومات التي يتحصلون عليها هي معلومات قيمة من الناحية المادية او المعنوية

، وغالباً هذه الفئة ليست مؤهلة علميا او فنياً حيث يستخدمون برامج ويتبعون تعليمات التي سبق استخدامها ، ونتيجة لكثرة عددهم يتسببون عند انتشال المعلومات عن الموقع الذي ينجحون في اقتحامه في انتشار المعلومات . [3]

3/ المخربون (الهاكرز) : وتعتبر هذه الفئة مهمتهم الاساسية التجوال في فضاء الانترنت وهم يفعلون ذلك من باب التخريب لان لهم مصلحة مادية او معنوية في هذا التخريب ، وغالباً يكون التخريب مباشر وقصير الاجل مثل قيامهم بمسح بعض البيانات من جهاز حاسوب او شبة معلوماتية او تخريب تطبيقات على احدى المواقع او تحريف بيانات او تزوير بعض المعاملات او غير ها من التصرفات التي تنقلهم الي مرتبة مجرمي الانترنت .

4/ التهديد والانتقام : يمكن ان يكون دافع الجريمة المعلوماتية بغرض تهديد الشخص والضغط عليهم من الاخرين في مجال الاعمال التجارية او سعي بعض الموظفي الي الانتقام من بعض المنشآت ، وقد يكون الهدف تهديد الاشخاص وابتزازهم لحملهم على فعل شئ معين مثل الامتناع عن مشروع معين او التخلي عن بعض المستندات والوثائق الهمة .

5/ الدوافع السياسية : وتعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق مواقع تخص دول منافسة افتصادياً او سياسياً او استراتيجياً وذلك بغرض الضغط على الدول للتخلي عن مواقفهم ، وايضا اصبح الانترنت مجالاً خصباً لنشر الافكار الايدلوجية من افراد وجماعات ووسيلة للترويج لاخبار وامور عديدة تحمل في ثناياها تهديداً لامن الدول او قدحا لشخصيات بارزة ذات ثقل سياسي او اقتصادي ، ومنهم من يتعمد سرقة اسرار اقتصادية او يتحصلون على معلومات سرعان ما تتحول الى اموال بعد بيعها او استخدامها خاصة اذا كانت المعلومات المسروقة تخص رقم بطاقة ائتمان او ارقام استخدام احدى شبكات العالمية .[4]

6 / الدوافع الارهابية : امتدت الجريمة الالكترونية لتشمل الجريمة المنظمة حيث ظهر الارهاب الالكتروني على شبكة الانترنت واخذت الجماعات الارهابية الي نشر افكار تهدد السلام الاجتماعي وتمارس اعمالاً كالتحريض على القتل بالاضافة الى تعليم صنع الاسلحة ، وبعض هذه الجماعات تقوم بهجوم الكتروني من خلال التلاعب ببعض البيانات او تسريب ما من شأنه ان يصنع تشويه او تضليل بالراي العام .

الحماية النظامية والقانونية للمعلومات في دول مجلس التعاون:

تبدأ الحماية النظامية والقانونية غالبًا من نصوص الدساتير وخاصة حماية وسائل الاتصال، التي تعد من العوامل المهمة لعمل وسائل التقنية الحديثة، وعلى وجه الخصوص الشبكة العالمية (الإنترنت)

وقد سلكت دول الخليج مسلك أغلب دول العالم في حماية المعلومات، عن طريق قوانين حقوق الملكية الفكرية، بحيث تمتد حماية هذه القوانين، لتشمل برامج الحاسب الآلي وتطبيقاته، قبل أن تتوجه بعض دول الخليج إلى إصدار نظم وقوانين خاصة بالجرائم المعلوماتية.

فمثلاً في دولة الإمارات العربية المتحدة، صدر القانون الاتحادي رقم (40) لسنة 1992م في شأن المصنفات الفكرية وحقوق المؤلف، وقد شمل هذا القانون برامج الحاسب الآلي بالحماية، علاوة على أن المشرع الإماراتي في هذا القانون قد اعتبر مخالفة نصوص الحماية الفكرية لبرامج الحاسب الآلي جرائم يعاقب عليها القانون بعقوبة جنائية، على عكس النظام السعودي الذي عدَّ هذه العقوبات لقاء مخالفة أحكام النظام، ولم يذكر مسمى جريمة.

إضافة إلى ذلك، أصدرت دولة الإمارات العربية المتحدة عام 2002م، في إطار حرصها على تغطية الفجوة التشريعية في مجال الاتصالات – وهو الأمر الذي تفتقده معظم الدول العربية – قانون التوقيع الإلكتروني والتجارة، وقد قضى هذا القانون بمنع مزودة خدمات الإنترنت من كشف أية معلومات يحصلون عليها في أثناء تزويد الخدمة.

أما في البحرين :فقد صدر المرسوم بقانون لحقوق المؤلف برقم (10) لسنة 1993م، وقد ورد ضمن هذا القانون نص خاص حماية برامج الحاسب الآلي (م 2).

وفي قطر: نص الدستور القطري لعام 2003م على حرمة خصوصية الإنسان من خلال المادة (37)، إضافة إلى صدور القانون رقم (25) لسنة 1995م بشأن حماية المصنفات الفكرية وحقوق المؤلف، والذي تضمن نصًا لحماية برامج الحاسب الآلي بوصفها من المصنفات (م 2) .

أما عن الكويت،فقد صدر القانون بالمرسوم رقم (5) لسنة 1999م، متضمنًا حماية المصنفات والحاسب الآلي من البرامج وقواعد البيانات (م1)، وفي عمان، صدر القانون رقم 37/ 2000 بشأن الحماية القانونية لحقوق المؤلف والحقوق المجاورة، مع نص النظام الأساسي للسلطنة الصادر في عام 1996م (م 30) على حماية الحريات الشخصية وحرمتها.

2 –الحماية الجنائية للمعلومات في دول مجلس التعاون:

مما تقدم يتضح أن دول مجلس التعاون الخليجي سعت إلى حماية المعلوماتية، من خلال حماية نظم الاتصال وحرمتها، وأهمية المحافظة على سريتها، وعدم اطلاع الآخرين عليها، حتى لو كانت السلطات الرسمية، ما عدا الأحوال التي حددتها القوانين والنظم، وبضوابط خاصة.

وقد بدأت الحماية من خلال الدساتير التي تعد القوانين العليا في التدرج التشريعي، وتركت التفاصيل لنظم أخرى .[5]

ومن المعروف أن الدساتير نصوص لا يمكن تطبيقها مباشرة، ونظرًا للزيادة المضطردة في استخدام وسائل التقنية الحديثة، والاعتماد عليها في منطقة الخليج، وبروز ظاهرة التعدي على البرامج والبيانات والكيان المنطقي للحاسب الآلي بأفعال تعد من قبيل الجرائم، ولا يمكن تطبيق نصوص التجريم التقليدية عليها، فقد ظهرت الحاجة إلى قوانين ونظم أخرى يتم على أساسها تكييف الجرائم المعلوماتية تشريعيًا.

كما لجأت دول مجلس التعاون إلى نظم حماية الملكية الفكرية وحقوق المؤلف وقوانينها، لحماية البرامج والبيانات بوصفها من المصنفات

الفكرية لمواجهة الفراغ التشريعي الذي لم يتم التغلب عليه من خلال النظم السابقة.

ونظرًا لإحساس دول مجلس التعاون بخطورة الجرائم المعلوماتية وتزايدها، فقد أوصت بإصدار نظم وقوانين لمواجهتها، وصدرت تلك القوانين بالفعل.. ونستعرض بعضها فيما يلي:

في عُمان، صدر أول قانون عربي لمواجهة الجرائم المعلوماتية من خلال التعديل الذي أُدخل على قانون الجزاء العماني رقم (7) الصادر عام 1974م، بموجب المرسوم السلطاني رقم 72/ 2001م، ويُعد هذا القانون باكورة القوانين العربية في مجال مواجهة الجرائم المعلوماتية من خلال تعديل قانون العقوبات.

أما الإمارات :فهي أول دولة عربية تصدر قانونًا خاصًا بمكافحة جرائم المعلومات، حيث أصدر صاحب السموالشيخ خليفة بن زايد آل نهيان – رئيس الدولة – القانون الاتحادي رقم 2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات.

وقد حدد المشرع الإماراتي الأفعال التي يُعد ارتكابها جريمة من جرائم المعلومات، كما حدد العقوبات الملائمة لها تبعًا لخطورتها وضررها المتوقع، وقد شمل القانون أغلب الجرائم المعلوماتية، ومنها: التوصل بغير وجه حق إلى موقع أو نظام معلوماتي بدخول الموقع أو النظام، أو يتجاوز مدخل مصرح

به، والتعدي على البيانات الشخصية، وإلغاء بيانات أو معلومات، أو حذفها، أو تدميرها، أو إفشاؤها، أو إتلافها، أو تغييرها، أو إعادة نشرها... وغير ذلك .[6]

وتعد المملكة العربية السعودية الدولة العربية الثالثة التي أصدرت نظامًا لمكافحة الجرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428هـ، وهو لا يختلف كثيرًا عن القانون الإماراتي من حيث التجريم ونوعية الجرائم، إلا أن المشرع السعودي حدد العقوبة لكل فعل من خلال بداية كل مادة بعقوبة معينة، ثم إدراج عدد من الجرائم تحت كل مادة.

وقد حدد النظام السعودي أغلب الجرائم المعلوماتية، التي تشمل الأفعال التي تشكل خطرًا على المعلومات، إضافة إلى الأحكام الخاصة بالإسهام الجنائي، وتشديد العقوبة، والشروع فيها، والإعفاء من العقاب، والعقوبة التكميلية.

من السمات العامة للنظام السعودي والإماراتي ما يأتي:

وضوح الألفاظ والمعاني عن طريق إفراد مادة، تعني بالمصطلحات الواردة في النظام أو القانون، وإيضاح معانيها؛ حتى لا تثير بعض الإشكالات عند التطبيق، وتطبيق مبدأ الشرعية الجنائية من خلال الدقة والوضوح في نصوص التجريم، والتدرج في العقوبة تبعًا لجسامة الجريمة ووضوح أركانها، وتحديد صور الاشتراك في الجريمة، وتحديد حالات الإعفاء من العقاب في النظام السعودي.

ويُعد صدور النظام السعودي والقانون الإماراتي من الأمور المهمة التي ستغطي الفراغ التشريعي الذي يعانيه أغلب دول العالم، وخاصة بتزايد الاعتماد على وسائل التقنية الحديثة على المستويين: الرسمي والشخصي في دول مجلس التعاون لدول الخليج العربية.

ومهما كان في النظام السعودي والقانون الإماراتي من قصور، فإن المعالجة النظامية والقانونية كفيلة بالتعديل، وخاصة بعد التجربة والتطبيق، وظهور أوجه القوة .

وعلى الرغم من أن دول مجلس التعاون الخليجي من أوائل الدول التي واجهت الجرائم المعلوماتية، فإن الواقع يدل على أن هناك نوعًا من عدم الاتفاق على مفهوم موحد للجرائم المعلوماتية، واختلافًا في تقسيمات الجرائم المعلوماتية تبعًا للنظرة القانونية إليها، وكذلك على تحديد الطبيعة القانونية للمعلومة، مع اختلاف سمات الجرائم المعلوماتية عن الجرائم التقليدية، وعدم كفاية النصوص القانونية المعنية بالجرائم التقليدية لمواجهة الجرائم المعلوماتية.

ومن هنا؛ فإن الحاجة ماسة لزيادة التعاون الخليجي لمواجهة الجرائم المعلوماتية، مع التعاون الخليجي – الدولي في ذلك المجال عن طريق الاتفاقيات والمعاهدات الدولية، وضرورة عقد المؤتمرات والندوات الدولية للوصول إلى تحديد مفهوم عام للجرائم المعلوماتية، وزيادة مستوى التعاون العربي – الخليجي لمواجهة هذه الجرائم .[7]

المجرم المعلوماتي.

إن الشخص الذي يرتكب الفعل الإجرامي المعلوماتي، ليس كالمجرم العادي الذي يرتكب جريمة القتل أو السرقة العادية، فهو مختلف تمام إذ يتميز بصفات خاصة أولا، وأسباب مختلفة تدفعه إلى ارتكاب هذا النوع من الجرائم ثانيا.

أولا: صفات المجرم المعلوماتي.

إذا كان المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الحاسوب، فلابد وأن يكون إنسانا اجتماعياً ويقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية، وأيضا لابد أن يكون الشخص الذي ترتكب جريمته المعلوماتية إنسانا محترفا يتمتع بقدر كبير من الذكاء.

أ . المجرم المعلوماتي :

يختلف الإجرام المعلوماتي عن الإجرام العادي الذي يميل عادة إلى العنف مع ذلك إذا كانت الجرائم المقصور وقوعها في بيئة النظام المعلوماتي تتفق أحيانا مع الإجرام التقليدي من حيث تتطلب العنف في سبيل ارتكابها، إلا أن الإجرام المعلوماتي ينشأ من تقنيات التدبير الناعمة، وبمعنى آخر يكفي أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسوب لكي يمحو هذه البيانات أن يعطل استخدام البرامج، وليس عليه سوى أن يلجأ إلى زرع الفيروسات في هذه البرامج أو باستخدام القنابل الزمنية أو برامج الدودة لكي يشل حركة النظام المعلوماتي، ويجعله غير قادر على القيام بوظائفه الطبيعية. قد يصل الأمر إلى حد احتراف الإجرام مما يشكل خطرا كبيرا على المجتمع سواء كان فردا أو جماعة منظمة أو غير ذلك.[8]

ب . الشباب الحديثي العهد بالتكنولوجيا المعلوماتية.

وهم الشباب الذين انبهروا بالثروة المعلوماتية وانتشار الحواسيب، ولذلك كان أولئك الشباب يرتكبون الجرائم المعلوماتية عن طريق استخدام الحواسب الخاصة بهم . وهذه الطبقة من الشباب لديها قدر لا بأس بها من الخبرة المعلوماتية، ومن ثمة فهم يمارسون مواهبهم في استخدام الحاسوب بغرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية سواء الخاصة بالوزارات الخاصة أو الشركات العملاقة أو الشركات التجارية أو المؤسسات المصرفية والبرامج العسكرية.... وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب خاصة إذا كان بينهم من لديه علم ومعرفة بعملية البرمجة.

ومع ذلك فهؤلاء الشباب تكون غايتها مجرد التسلية والملاحظة وليس لديهم النية في ارتكاب أفعال الجريمة المعلوماتية، ومع ذلك خطر انزلاق هذه الفئة إلى احتراف الأفعال الغير مشروعة وارتكاب الجرائم المعلوماتية هو احتمال كبير و قائم، وعندئذ يتحول من مجرد هاوي إلى محترف.[9]

ج . الأشخاص المحترفون ارتكاب الجريمة المعلوماتية.

هؤلاء الأشخاص الذين يحترفون ارتكاب الجريمة المعلوماتية تتراوح أعمارهم ما بين 25 إلى 45 سنة. ومرحلة السنة الأولى تمثل الشباب الحديثي العهد بالمعلوماتية والحسابات أو الحواسيب الآلية، ولم يكن لديهم ميل لارتكاب الأفعال الغير المشروعة أي أنه مجرد هاوي، أما المرحلة الثانية فهي تمثل نضوج هؤلاء الشباب ويتزامن هذا النضوج مع تزايد انتشار الوسائل المعلوماتية، وتكون ثورة قد وصلت مرحلة لا بأس بها من التقدم التكنولوجي. من ثم يتحول من مجرد هاوي إلى مجرم محترف في استخدام المعلوميات واحتراف ارتكاب الأفعال غير المشروعة.

وغالبا ما يتم ارتكاب الجرائم المعلوماتية في هذه المرحلة من هؤلاء الأشخاص وهم يعملون في نوادي ما أو في منشأة أو في إطار نظم معلوماتية أي أنهم مسؤولون عن الأنظمة المعلوماتية، إذ يعرفون التقنيات اللازمة للتلاعب بالحواسب، ومن تم يقومون بتنفيذ أفعالهم غير المشروعة.

ثانيا: أسباب انتشار الإجرام المعلوماتي.

إن أهم ما يتميز به الإجرام الملعوماتي عن الإجرام التقليدي هو وجود تقنية المعلوماتية وثورة المعلومات التي تلقي بظلالها على نموذج الجريمة المعلوماتية حتى أن أسباب انتشار الإجرام المعلوماتي يتأثر بلاشك بهذه الثورة، وإذا كانت الأنماط المختلفة للمجرم المعلوماتي تكشف عن انتشار هؤلاء المجرمين عند ارتكابهم الجريمة المعلوماتية في غرض واحد هو مجرد الهواية واللهو نتيجة انبهارهم بثورة المعلوميات، ثم من ناحية أخرى قد يكون الهدف هو تحقيق الثراء السريع أو إحدى الأسباب الشخصية.

أ: الانبهار بالتقنية المعلوماتية.

مع ظهور التقنية المعلوماتية وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو الحواسب، فإن الأمر في النهاية يؤدي إلى انبهار المجرمين بهذه التقنية الحديثة، لذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة، ونعطي مثلا على ذلك ما نشر في مجلة Expresse الفرنسية في شتنبر 1983 قصة بعنوان "ميلاد نزعة".[10]

وتدور أحداث هذه القصة في أن عامل طلاء مباني قد توجه إلى أحد البنوك لإيداع شيك خاص به وتزامن ذلك لحظة مشاهدته مشكله في الماكينة الآلية للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية، وهو يقوم باستخراج النقود من الآلة، عند الطلب عن طريق استخدام بطاقة خاصة، وقد أحدث هذا الإبتكار للآلة تصدعا في الحياة العادية لعامل الطلاء وقد حرص هذا الأخير على التدريب على تقنية الحاسوب لمدة عامين، ثم قام بالسطو على صانع الماكينات الآلية للنقود ، وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب وألقي القبض عليه قبل أن يستفيد من نزعته المستحدثة.[11]

ب . الرغبة في تحقيق الثراء السريع.

قد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الإطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود، ولذلك فإن هذا السبب يعد من أكثر الأسباب التي تدفع إلى انتشار الإجرام المعلوماتي، تبرز الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات...) مثالاً ذلك استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على اثنين وعشرين شريطا تحتوي على معلومات بخصوص عملاء إنتاج الشركة، وقد هدد السارق ببيعها للشركة المنافسة ما لم تدفع له فدية بمقدار 200000 دولار، وقامت الشركة بتحليل الموقف ففضلت الأداء مقابل استرداد الشرائط الممغنطة حيث أن قيمتها تفوق المبلغ المطلوب.[12]

ج . الأسباب الشخصية.

يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توفر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى ارتكابه للجريمة المعلوماتية، هذا وتتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الحقد أو الإنتقام ، او الرغبة في التطور السريع .

ومع انتشار المعلوماتية، ووسائلها المختلفة، تبدأ الرغبة لدى الشباب نحو العبث بالأنظمة المعلوماتية من أجل ممارسة هواية اللعب او تحدي لأثبات الذات ، أو تعود إلى وجود ميل زائد لدى البعض بأن الإعتقاد بأن كل شيء يرجع إليهم وتأترهم بمقوله ان المستقبل للشباب وهم الذين يبنون المستقبل ، إذن تلك تمثل آفة نفسية تصيبهم ويتفاخرون بما قاموا به من جرائم، ليظهروا تفوقهم على الأنظمة المعلوماتية، وقد يكون الدافع نحو ارتكاب الجريمة المعلوماتية هو عامل الإنتقام أو اثبات الذات ، وذلك عندما يتم فصل العامل من عمله فإن ذلك من شأنه أن يهيء له المناخ لجريمته، كأن يدمر البرامج المعلوماتية بالفيروسات عن طريق زرعها أو القنابل المنطقية التي تنشأ عنها أضرارا.

ضحايا الإجرام المعلوماتي.

يمكن القول أن ذيوع المعارف التكنولوجية نتيجة لثورة المعلوميات ترتب عنه انتشار كبير للوسائل المعلوماتية في جميع الأنشطة سواء منها الإقتصادية، الاجتماعية، العسكرية أو المؤسسات المالية والتجارية في الدولة.

ولما كانت الجرائم المعلوماتية تنصب أساسا على المعلومات سواء عن طريق بيعها أو مقايضتها أو إتلافها، وتتمثل المعلومات العسكرية محل الإعتداء على أسرار الدولة والمشروعات العامة، وكل ما يمس الأمن القومي لهذه الدول، وتتمثل المعلومات المالية فيما يتعلق بالمراكز الإدارية والمالية والإستثمارات في المنشآت العامة، ويتبين رد فعل ضحايا الإجرام المعلوماتي ما بين السكوت وعدم الكشف على أنهم وقعوا ضحية للأفعال غير المشروعة وذلك حفاظا على سمعتهم.

فالجرائم المعلوماتية لا عنف فيها، ولا آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، بمعنى آخر فإن جرائم المعلوماتية هي جرائم فنية تتطلب من المجرم مهارات لا تتوفر في الشخص العادي تتطلب تقنية معينة في مجال الحاسوب، إذن هي جريمة هادئة لا تتطلب العنف، ورغم ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف، مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة نظرا للتماثل دوافع المعتدين على نظم الحاسوب مع مرتكبي العنف. [13]

فإذا تم اكتشاف الجريمة المعلوماتية، فغالبا لا يكون إلا بمحض الصدفة نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات حيث يتم بالنبضات الإلكترونية نقل المعلومات، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها عبر مختلف الدول والقارات وذلك باستخدام شبكات الإتصال ودون تحمل عناء الإنتقال وإلى جانب ذلك الرغبة في استقرار حركة المعاملات ومحاولة أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين.

فكل –هذه الأسباب– تدفع المجني عليه في الجرائم المعلوماتية إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها.

وحتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين، حيث يكون المجني عليه عادة بنكا أو مؤسسة مالية أو مشروع صناعي ضخم يهمه المحافظة على ثقة عملائه وعدم اهتزاز سمعته أكثر من اهتمامه بالكشف عن الجريمة ومرتكبها، ولذلك يفضل المجني عليه تقديم ترضية سريعة لعمليه وينهي الأمر داخليا حتى لا يفقده.

وايضا هناك جرائم معلوماتية لا تقل خطرا من الاعتداء على مواقع البنوك او المؤسسات الحساسة او المنشآت الصناعية الكبرى وهي جرائم المعلوماتية التي تقع في مواقع التواصل الاجتماعي، خاصة تلك الجرائم التي تمس السلام الاجتماعي او النسيج الاجتماعي ، حيث تتميز برامج التواصل الاجتماعي بالسرعه في الانتشار ، وايضا التفاعل الكبير بين مستخدمي هذه البرامج ليس على مستوى دولة معينة فحسب بل على مستوى العالم حيث تتخطى الحواجز الجغرافية، والتعقيدات الالكترونية التي تصاحب الحواسيب حيث من الممكن ان تقع الجريمة المعلوماتية من خلال الهاتف المحمول من خلال تحميل صور خاصة او انتشار اخبار كاذبة (الاشاعه) ، او التعدي على خصوصية الاخرين او انتحال شخصيات لها دورها في المجتمع، او التحريض او التشجيع على الكراهية والتمييز . [14]

مخالفات مواقع التواصل الاجتماعي :

ايضا مواقع التواصل الاجتماعي تعتبر ميدان خصب للجريمة المعلوماتية لانها تمثل قلب الثورة المعلوماتية والهياج الالكتروني ، وتأثيره على جمهور عريض من مستخدمي شبكة الانترنت ، ممثلاً في جرائم الإنترنت وشبكات التواصل الاجتماعي في العالم العربي، والتي منها جرائم المعلوماتية والإنترنت، وقد انتشرت جرائم المعلوماتية والإنترنت بشكل نسبي ، وترتَّب على هذا المخالفة أضرار بالغة في حق الأفراد والمؤسسات، بل والدول ذاتها، فمنظومة الأمن القومي لأى من الدول قد يخترقها أي من المجرِمين الإلكترونيين كالهاكرز(مخرب او مجرم معلوماتي) مثلاً، فالأمر لا يحتاج أكثر من شخص اعتاد المخالفات الإلكترونية، لكى يقوم باختراق مواقع الجهات المالية، والاطلاع على أسرارها وخصوصياتها، فضلاً عن ذلك، فالجرائم الإلكترونية تأتي على أشكال وتصنيفات متنوعة،وممكن ان تكون الجريمة المعلوماتية اجتماعية فمثلاً قد تكون رسائل نصية تحمل قدراً كبيرا من السخرية والتهكم على فئة من المجتمع او كثرة النكات عليها ومع مرور الزمن يحدث الشرخ الاجتماعي والتمييز ، كما أن المجرم الإلكتروني له صفات خاصة تختلف عن تلك التي يتصف بها المجرم العادي.

و جدير بالذكر أن المخالفات او الجريمة الإلكترونية، هي ظاهرة إجرامية جديدة ومستجدَّة تقرعُ في جنباتِها أجراس الخطر؛ لتنبِّه مجتمعات العصر الراهن لحجم المخاطر، وهول الخسائر الناجمة عن جريمة الحاسب الآلي او عن طريق الهاتف المحمول، التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فجريمة الحاسب الآلي جريمة تقنية، تنشأ في الخفاء، يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءآتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وتمس الحياة الخاصة للأفراد، وتهدِّد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية، وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية الجرائم الإلكترونية مَنُوط بتحليل وجهة نظر الدارسين لتعريفها، والاصطلاحات الدالة عليها، واختيار أكثرها اتفاقًا مع الطبيعة الموضوعية لهذه الجرائم، واظهار موضوعها وخصائصها ومخاطرها، وحجم الخسائر الناجمة عنها، وسمات مرتكبيها ودوافعه .

إن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال؛ حيث إن هذه الوسائل تعرضت لسوء الاستغلال من قبل الكثيرين، ومن الثابت أيضًا أن المجرمين وظَّفوا الاتصال تاريخيًّا لخدمة النشاطات الإجرامية التي يقومون بها ، حيث القصص الاجرامية المنتشرة في فضاءآت الشبكة العنكبوتية ساهمت في تطور الجريمة الالكترونية ، لان المجرم سيستفيد من تجارب المجرمين السابقين ويقوم بتطوير الطريقة التي سينفذ بها جريمته .

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تُسلَب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون

دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب.

وغني عن البيان أن الدول العربية ليست ببعيدة عن مرمى الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلدًا من بلاد العالم إلا واخترقتها، ونالت من أهداف محددة فيها، فالسعودية، والإمارات، وسلطنة عمان، والكويت، فلسطين، وغيرهم من الدول العربية بادروا إلى وضع تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

ونظرًا لسهولة حركة المعلومات في مجال أنظمة تقنية المعلومات؛ حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة، بينما يتحقق نتيجة هذا الفعل الإجرامي في دولة أخرى، وهو الأمر الذى استلزم ضرورة وجود تعاون دولي محكم في مجال مكافحة هذا النوع من الجرائم، ولأجل توفير حماية حقيقية لأنظمة الاتصالات.

شبكات التواصل الاجتماعي

التعريف :

تقوم شبكات التواصل الاجتماععلى بناء وتفعيل المجتمعات الافتراضية على الانترنت وهي عبارة عن محاكاه للمجتمعات على ارض الواقع ، حيث يتشارك الناس اهتماماتهم وأنشطتهم من خلال برمجيات تحقق صفة الاجتماعية، وهى تحقق اتصالات تفاعلية باتجاهين.

الشبكات الاجتماعية هي مصطلح يطلق على مجموعة من المواقع على شبكة الإنترنت، تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد، جامعة، مدرسة، شركة... إلخ)، كل هذا يتم عن طريق خدمات التواصل المباشر؛ مثل: إرسال الرسائل، أو الاطلاع على الملفات الشخصية للآخرين، ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض. [15]

وتعرف مواقع التواصل الاجتماعي بأنها عبارة عن تطبيقات تكنولوجية مستندة إلى الويب تتيح التفاعل بين الناس، وتسمح بنقل البيانات الإلكترونية وتبادلها بسهولة، وتوفر للمستخدمين إمكانية العثور على آخرين يشتركون فى نفس المصالح، وبناء عليه ينتج عن ذلك ما يسمى بالمجتمعات الافتراضية Virtual Communities ؛ حيث يستطيع المستخدمون التجمع فى كيانات اجتماعية تشبه الكيانات الواقعية.

ومواقع التواصل الاجتماعى هى مصطلح يطلق على مجموعة من المواقع على شبكة الإنترنت، وقد ظهرت هذه المواقع مع الجيل الثانى للويب؛ لتساعد الأفراد على التواصل والتفاعل فى بيئة مجتمع افتراضى يجمعهم حسب مجموعات اهتمام أو انتماء أو مشاركة فى قضية بعينها .

والشبكات الاجتماعية هى مواقع التي تعطي المستخدمين مجموعة من الخدمات على أساس تكنولوجيات الويب التي تسمح للأفراد ببناء محتوى خاص بصفحة شخصية، ونظام من العلاقات الاجتماعية المتعددة ومشاركة الآخرين والتواصل معهم من بعد دون قيود، عرض وبناء وتشكيل المحتوى فى إطار من التعاون والتفاعل من خلال مجموعة من الروابط والاهتمامات المشتركة .

ونستنتج من التعريفات السابقة أن مضمونها يتبنى فكرة تدور حول مفهوم مواقع التواصل الاجتماعى بأنه: "عبارة عن تطبيقات تكنولوجية الكترونية قائمة على نظم الجيل الثانى للويب لتحقيق التواصل والتفاعل بين مختلف الأفراد المنتشرين حول العالم بالمراسلات المكتوبة والمسموعة والمرئية مع تحقيق الاتصال الفورى والمرجأ بما يحقق أكبر فائدة لتجميع الشعوب فى موقع للتواصل من بعد ."

والتعبير عن التواصل الاجتماعى Social networking على شبكة الانترنت استخدام له العديد من المصطلحات منها: (المواقع التفاعلية – وشبكات التواصل الاجتماعى – والشبكات الاجتماعية – ومواقع التواصل الاجتماعى)، وجميع هذه المصطلحات تعبر عن التواصل والتفاعل بين مجموعة من الأفراد من خلال شبكة اجتماعية على الويب .[16]

مميزات شبكات التواصل الاجتماعي:

وبالرغم من ذلك فإن الشبكات الاجتماعية تتميز عن غيرها من المواقع في الشبكة العنكبوتية بعدة ميزات، من أبرزها:

- إن هدف المواقع الاجتماعية خلق جو من التواصل في مجتمع افتراضي تقني يجمع مجموعة من الأشخاص من مناطق ودول مختلفة على موقع واحدة، تختلف وجهاتهم ومستوياتهم وألوانه، وتتفق لغتهم التقنية.
- إن الاجتماع يكون على وحدة الهدف سواء التعارف أو التعاون أو التشاور أو لمجرد الترفيه فقط وتكوين علاقات جديدة، أو حب للاستطلاع والاكتشاف.
- إن الشخص في هذا المجتمع عضو فاعل، أي أنه يرسل ويستقبل ويقرأ ويكتب ويشارك، ويسمع ويتحدث، فدوره هنا تجاوز الدور السلبي من الاستماع والاطلاع فقط، ودور صاحب الموقع في هذه الشبكات دور الرقيب فقط، أي الاطلاع ومحاولة توجيه الموقع للتواصل الإيجابي.
- ان المواقع التفاعلية تصنف اعضائها حسب المهنة او الجامعه او الموقع الجغرافي او اهتمامات افراد المجموعه مثالاً لذلك موقع لينكد إن او منتديات كورة عالمية او تويتر .

كما تتميز الشبكات الاجتماعية عن غيرها بعدة ميزات:

1 – العالمية: حيث تلغى الحواجز الجغرافية والمكانية، وتتحطم فيها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب، في بساطة وسهولة.

2 – التفاعلية: فالفرد فيها كما أنه مستقبل وقارئ، فهو مرسل وكاتب ومشارك، فهي تلغي السلبية المقيتة في الإعلام القديم – التلفاز والصحف الورقية وتعطي حيزًا للمشاركة الفاعلة من المشاهد والقارئ.

3 – التنوع وتعدد الاستعمالات، فيستخدمها الطالب للتعلم، والعالم لبث علمه وتعليم الناس، والكاتب للتواصل مع القراء... وهكذا.

4 – سهولة الاستخدام: فالشبكات الاجتماعية تستخدم بالإضافة للحروف وبساطة اللغة، تستخدم الرموز والصور التي تسهل للمستخدم التفاعل.

5 – التوفير والاقتصادية: اقتصادية في الجهد والوقت والمال، في ظل مجانية الاشتراك والتسجيل، فالفرد البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي، وليست ذلك حكرًا على أصحاب الأموال، أو حكرًا على جماعة دون أخرى. [17]

إيجابيات وسلبيات شبكات التواصل الاجتماعي:

وبما أن لكل شيء إيجابيات وسلبيات فإن شبكات التواصل الاجتماعي كذلك لها إيجابياتها وسلبياتها، حيث تضاربت الآراء مع قبول ورفض لانتشار المواقع الاجتماعية على الشبكة العالمية العنكبوتية (الانترنت) ، معتمدًا ذلك على دراسات وبحوث أقامها العديد من الباحثين الاجتماعيين والأطباء في مجال علم النفس والطب أيضا، حيث استنتجوا من خلالها أن هناك العديد من التأثيرات السلبية التي تنتج من الإدمان عليها لاسيما تلك العوارض النفسية وهي الانعزال في غرفة واحدة أمام شاشة، وان كانت صغيرة ولكنها تضع العالم بأكمله بين يدي المستخدمين وبسهولة كبيرة يصل الى حيث يشاء، فإنها وبحسب آراء بعض الأطباء النفسيين هي حالةالسكون والخمول لأن الشخص عندما يقوم بذلك فهو سيفقد متعة الحياة من مغامرة وتشويق وتعارف مباشر واطلاع اقرب وتجارب أكبر. [18]

امثله لبعض جرائم التواصل الاجتماعي :

ينص القانون الاتحادي رقم 5 لعام 2012 لمكافحة الجرائم الإلكترونية في دولة الامارات على العديد من الانتهاكات التي يعاقب عليها بالسجن أو الغرامة أو. وفيما يلي قائمة بأكثر هذه الانتهاكات شيوعاً بحسب :

1- السب أو الإهانة أو اتهام شخص آخر بما يعرضه للازدراء من قبل الآخرين.

العقوبة: السجن وغرامة لا تقل عن 250 ألف درهم ولا تتجاوز 500 ألف درهم. أو إحدى هاتين العقوبتين.

2- انتهاك خصوصية أي شخص عن طريق التنصت أو التسجيل أو نقل أو الكشف عن المحادثات بالصوت والصورة.

العقوبة: السجن لمدة لا تقل عن 6 أشهر وغرامة مالية لا تقل عن 150 ألف درهم ولا تتجاوز 500 ألف درهم. أو إحدى هاتين العقوبتين.

3- تصوير شخص أو التقاط أو نقل أو حفظ الصور على الأجهزة الإلكترونية دون إذن صاحبها.

العقوبة: السجن لمدة لا تقل عن ستة أشهر وغرامة لا تقل عن 150 ألف درهم ولا تزيد عن 500 ألف درهم. أو إحدى هاتين العقوبتين.[19]

4- نشر الأخبار والصور الإلكترونية والمشاهد والتعليقات بصورة غير مشروعة حتى لو كانت حقيقية وصحيحة.

العقوبة: السجن لمدة لا تقل عن ستة أشهر وغرامة لا تقل عن 150 ألف درهم ولا تزيد عن 500 ألف درهم. أو إحدى هاتين العقوبتين.

5- الحصول على البيانات التي تتعلق بالفحوص الطبية والتشخيص والعلاج والرعاية والسجلات الطبية أو حيازتها أو التعديل عليها أو تدميرها دون إذن.

العقوبة: السجن المؤقت.

6- ابتزاز أو تهديد شخص لإجباره على ارتكاب جناية أو التورط في المسائل المخلة بالشرف أو الآداب العامة.

العقوبة: السجن لمدة تصل إلى 10 سنوات.

7- إنشاء و إدارة وتشغيل مواقع على شبكة الإنترنت أو نقل إو إعادة نشر المواد الإباحية أو النشاطات المتعلقة بالقمار.

العقوبة: السجن وغرامة لا تقل عن 250 ألف درهم ولا تتعدى 500 ألف درهم أو إحدى هاتين العقوبتين.

8- الإغراء أو المساعدة أو تحريض شخص آخر على ممارسة البغاء أو الفجور.

العقوبة: السجن وغرامة لا تقل عن 250 ألف درهم ولا تتعدى مليون درهم أو بإحدى هاتين العقوبتين.

9- الإفصاح دون إذن عن معلومات سرية تم الحصول عليها أثناء أو بسبب العمل.

العقوبة: السجن لمدة لا تقل عن 6 أشهر وغرامة مالية لا تقل عن 500 ألف درهم ولا تزيد عن مليون درهم أو بإحدى هاتين العقوبتين.

10 – إنشاء و إدارة أو تشغيل موقع على شبكة الإنترنت أو نشر معلومات لصالح مجموعة أو جمعية أو منظمة أو هيئة غير مصرح بها بقصد تسهيل التواصل مع قادتها وأفرادها أو جذب أعضاء جدد أو تعزيز وامتداح أفكارها وتمويل أنشطتها أو توفير المساعدة الفعلية لتصنيع الأجهزة الحارقة أو أي مواد و أجهزة أخرى تستخدم في الأعمال الممنوعة .

العقوبة: السجن لمدة لا تقل عن 5 سنوات وغرامة مالية لا تقل عن مليون درهم ولا تزيد عن 2 مليون درهم.ش

وتنص المادة 42 من القانون أيضاً على أنه يجوز للمحكمة أن تقرر ترحيل الوافدين بموجب الأحكام المختلفة إذا اقتضى الأمر.[20]

مكافحة جرائم المعلوماتية :

إن مكافحة الجرائم المرتبطة بتكنولوجيا المعلوميات التي باتت في مظهرها وتجلياتها الحديثة لن تكون مجدية إلا إذا كان هناك تعاون وتآزر دوليين على أكبر قدر من التنسيق، ومن هنا بدأت بعض الأصوات ترتفع للمطالبة بضرورة سن قوانين لحماية المعلومات على الشبكات، بالإضافة إلى إدراك الدول والحكومات حجم المخاطر التي تزداد معها جرائم الأنترنيت، فأنشئت جهات رسمية لمكافحة هذه الجرائم وسنت قوانين لحماية شبكة المعلومات، من بين هذه الدول المغرب.

بالإضافة إلى أن وعي هذه الدول بمدى خطورة هذه الجرائم العابرة للحدود كان نتيجة لإبرام عدة اتفاقيات ومعاهدات دولية، في مجال مكافحة هذه الجرائم التي باتت تهددها خاصة مع ازدياد استعمال التكنولوجيا الحديثة يوما بعد يوم.

المعاهدات الدولية في مكافحة الجريمة المعلوماتية :

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ومن تلك المعاهدات معاهدة بودابيست والمعاهدة الأوروبية، معاهدة برن، معاهدة تريبس .[21]

معاهدة بودابيست لمكافحة جرائم لإنترنيت:

شهدت العاصمة المجرية بودابيست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنيت وتبلور التعاون والتضامن الدولي في محاربتها، ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات.

وبعد التوقيع على تلك المعاهدة الدولية، التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنيت والتي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم من الحالات ودون أي غرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص، وتتمثل في الاحتيال والإختلاس وجرائم تهديد الحياة، وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الإنترنيت للخطر، – هو الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت واستخدامها الإستخدام الأسوأ ويعد التوقيع على تلك الإتفاقية – من المسؤولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب افريقيا، هو نتاج مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقية حتى يتم التوقيع عليها من جميع الأطراف دون أن تجد أي اعتراض من أي منهم بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائرة الدول التي توافق على الانضمام إلى تلك الإتفاقية ويتم توسيع الإتحاد الدولي والتضامن الدولي في مجال مكافحة جرائم الإنترنيت.[22]

وعليه، فالتعاون الدولي أمر هام جدا في مجال مكافحة جرائم الإنترنيت وبدون هذا التعاون الدولي لن يكون هناك أي أثر لأي مجهود تقوم به أي من الدول بمفردها نظرا لأنه سيكون عديم الفائدة وبلا أثر تقريبا، ولن يؤدي إلى الحد من ارتكاب تلك الجرائم التي تكون في الاغلب الأعم من الحالات جرائم عابرة للحدود .

هذا من جهة، ومن جهة أخرى، فحتى الجرائم التقليدية التي تتم عبر الأنترنيت مثل النصب والإحتيال والإختلاس وانتهاك حقوق الملكية الفكرية، فهي أيضا من الجرائم التي يمكن مواجهتها بصفة فردية كل دولة على حدة، بل أن تلك الجرائم أيضا تحتاج إلى التعاون الدولي ليكون في الإمكان مكافحتها، والعقاب على ما اقترفت أيديهم من ارتكابها وملاحقة مرتكبيها وضبطهم لينالوا العقاب على ما اقترفت أيديهم، فوضع قوانين تحمي الملكية الفكرية في كل دولة على حدة لا يكفي بأي حال من الأحوال للمحافظة على تلك الحقوق وإنما التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليتم احترام مثل تلك الحقوق التي تجد دائما من ينتهكها أو على الأقل من يحاول انتهاكها.

وقد كان الخلاف الوحيد فيما بين الدول الموقعة على الإتفاقية هو مجال محاربة العنصرية، فالدول الأوروبية تعتبر أن التحريض على الكراهية العنصرية هي جريمة، ومن المعروف أن هذه الجريمة يعاقب عليها القانون الدولي.

المعاهدة الأوروبية لمكافحة جرائم الأنترنيت.

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الإنترنيت وسط انتقادات من دعاة حماية الحرية الشخصية، وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الإتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الإحتيال والتزوير التي لها صلة بالكومبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

وتتضمن بنود المعاهدة التي تم تعديل مسودتها 27 مرة قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها البعض في جمع الأدلة وفرض القانون .[23]

معاهدة بيرن لحماية المصنفات الادبية والفنية :

تعتبر معاهدة برن التي تم التوقيع عليها في عام 1971 في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الإتفاقية 120 دوله وتعد المادة التاسعة من تلك الإتفاقية هي أساس في تلك الإتفاقية لأنها تنص على منح أصحاب حقوق المؤلف حق في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان.

وفضلا عن ذلك، تمنح اتفاقية برن صاحب الحق المؤلف الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذا تلزم الإتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه مواطنا أم أجنبيا.

ويرجع الاهتمام بحق المؤلف إلى أنه الوسيلة القانونية الرئيسية لحماية حقوق المؤلفين، فحق المؤلف من أهم الحقوق التي تكفلها النظم القانونية على اختلافها للمبدعين والمؤلفين حماية لإبداعاتهم الفكرية، إن لم يكن أهمها على الإطلاق، ويوفر هذا الحق –بشروط معينة– لمؤلفي مصنفات معينة في الآداب والفنون والعلوم، أيا كان نوع هذه المصنفات، أو أهميتها، أو طريقة التعبير عنها، أو الغرض من تصنيفها، حماية قانونية لا بأس بها، لمدة زمنية معينة، وتنظيم هذه الحقوق في كافة الدول العربية بمقتضى تشريعات تكاد تتشابه أحكامها تقريبا، كما تستند في مجملها إلى اتفاقية برن لحماية المصنفات الأدبية والفنية التي أبرمت في 9 سبتمبر 1886 وهي أول اتفاقية دولية لحماية حق المؤلف، المعدلة في باريس عام 1971.

ومن أهم الإتفاقيات الثمانية والعشرين التي وقعت عليها الدول الموقعة على اتفاقية الجات، الإتفاقية المعروفة باسم اتفاقية المجالات المتعلقة بالتجارة في حقوق الملكية الفكرية، وأهم ما تضمنته في نظرنا أنها أعطت لموضوع الملكية الفكرية بشكل عام بعدا عالميا مهما، وربطت موضوعات الملكية الفكرية بآليات دولية محددة قد لا تستطيع دول كثيرة الفكاك منها، ولا أن يكون لهذه الإتفاقية تأثيرات مهمة سواء على اقتصاديات كثير من الدول ومنها الدول العربية أو على تشريعاتها الوطنية، ومن الموضوعات التي تناولتها هذه الإتفاقية تناولا صريحا موضوع الحماية القانونية لبرامج الكومبيوتر.[24]

التدابير القانونية المتخذة لمكافحة الجرائم المعلوماتية :

عرفت دولة الإمارات بأنها دولة قوانين وتشريعات وأن المؤسسات في الدولة تعمل وفقاً لأنظمة وقوانين واضحة ومحددة ، و من حرص الدولة على حماية حقوق وحريات الأفراد قامت الدولة بإصدار وتعديل العديد من القوانين حيث قامت بإصدار العديد من التشريعات المكملة للقوانين وذلك لجعل التشريعات الوطنية مواكبة للواقع وهذا ما تمليه الاتفاقيات والمعاهدات الدولية ، وفي مجال تقنية المعلومات حسناً فعل المشرع الإماراتي حيث كان له السبق في إصدار القانون رقم 2 لسنة 2006 والمتعلق بجرائم تقنية المعلومات وذلك لحماية الحقوق والحريات .

ونظراً لسرعة التطور في مجال تقنية المعلومات قام المشرع الإماراتي بإصدار المرسوم بقانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات ، والذي يعد من أحدث التشريعات في هذا المجال ، ولو نظرنا إلى مدى الحماية التي وفرها القانون لمستخدمي الشبكة الإلكترونية لعرفنا مدى حرص المشرع الإماراتي على حماية حقوق وحريات الأفراد ، حيث أن القانون رقم 5 لسنة 2012 وفر الحماية القانونية اللازمة لأصحاب المواقع الإلكترونية من علميات القرصنة والاختراق سواء أكانت تلك القرصنة للمواقع الإلكترونية بقصد سرقة بعض البيانات أو المستندات الإلكترونية أو تدميرها أو تعديلها والتزوير فيها و غيرها من وسائل الاعتداء على حقوق الأفراد كسرقة بيانات بطاقتهم الائتمانية وما يتصل بذلك من أمور ، وكذلك الحال بالنسبة للحرية الشخصية حيث وفر القانون الحق لأفراد كما أنه وفر الحماية الاجتماعية والاخلاقية للمجتمع .

مرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات:

1. الجريمة الإلكترونية هي كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الشبكة المعلوماتية أو تقنية معلومات .
2. يهدف المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات إلى توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية .

3. يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل إلى موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو تجاوز حدود التصريح ، أو بالبقاء فيه بصورة غير مشروعة .
4. إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر البيانات أو المعلومات على الموقع الالكتروني أو وسيلة تقنية المعلومات يعتبر جريمة يعاقب عليها القانون .
5. يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائة وخمسون ألف درهم ولا تتجاوز سبعمائة وخمسون ألف درهم كل من زور مستندا الكترونيا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية أو غيرها من الجهات أو استعمال المستند المزور .
6. يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات.
7. يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلا للعقاب أو الازدراء من قبل الآخرين وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.
8. يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق إلى عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية أو أي وسيلة من وسائل الدفع الالكتروني . ويكون ظرفا مشددا إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير.
9. كل من حرض ذكر أو أنثى أو إغوائه لارتكاب الدعارة أو الفجور عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
10. يعاقب بالحبس أو الغرامة التي لا تقل عن مائة ألف درهم ولا تتجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع الكتروني أو نظام معلومات الكتروني
11. التحايل على العنوان البروتوكولي للانترنت باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها يعتبر جريمة يعاقب عليها القانون .
12. يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من انتفع أو سهل للغير بغير وجه حق الانتفاع بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية المعلومات .

13. الاعتداء على خصوصية الأشخاص في غير الأحوال المصرح بها قانوناً باستراق السمع أو تسجيل أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية ، أو التقاط صور للغير، أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها يعتبر جريمة معاقب عليها قانوناً.[25]

الوقاية من الجرائم الالكترونية :

- تجنب فتح أي رسالة بريد إلكتروني قبل التأكد من مصدرها وخاصة عند طلب أية بيانات شخصية أو مصرفية
- يجب التأكد من مصداقية الإعلانات التي ترسل على البريد الالكتروني أو الهاتف المتحرك وتجنب الانجراف وراء الإعلانات المضللة على المواقع الالكترونية .
- الحذر من رسائل الاصطياد التي ترد عبر الهاتف المتحرك أو البريد الالكتروني لتجنب الوقوع ضحية للاحتيال الإلكتروني .
- يجب على الآباء والأمهات مراقبة أبنائهم عند استخدامهم الانترنت أو الهواتف الذكية .
- تجنب نشر أو تداول الشائعات عبر مواقع التواصل الاجتماعي لما لها من أثر سلبي على الأفراد والمجتمع .

إن سوء استخدام الشبكة المعلوماتية أو وسيلة تقنية المعلومات يعرض مستخدمها للمسائلة القانونية .

المراجع :

1. د. ناصر البقمي . مكافحة جرائم المعلوماتية وتطبيقاتها . مركز الامارات للبحوث . ط1. 2008. ص6 .
2. د. عبدالفتاح بيوسي حجازي .جرائم الكمبيوتر والانترنت في النشر العربي .دار النهضة . 2009 القاهرة . ط1. ص111.
3. د. ناصر البقمي . مرجع سابق . ص 15 .
4. د. ناصر البقمي . مرجع سابق.ص11 .
5. د. صالح عمير . الحماية النظامية في دول مجلس التعاون الخليجي . ط1 2010 . ص46
6. د. صالح عمير . المرجع السابق . ص57.
7. د. عبد الفتاح بيوسي . مرجع سابق . ص73.
8. محمد أحمد أمين الشوابكة: "الجريمة المعلوماتية". دار الثقافة، عمان. طبعة2004 . ص76.
9. محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004ص: 64.
10. محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية.ط 2. القاهرة 2007.ص. 48.
11. محمد سامي الشوا: المرجع السابق. ص: 48.
12. محمد علي العريان. مرجع سابق، ص: 66.
13. Computer Hackers : Tomorrows Tarrarts Dynamics, News for and about members of the American society for in dustrialseturdy jam varylfebrauary. 1990. p: 7.
14. جميل عبد الباقي الصغير."القانون الجنائي والتكنولوجيا". الكتاب الأول . الجرائم الناشئة عن استخدام الحاسب الآلي. دار النهضة العربية سنة 2011. ص: 1 وما بعدها.
15. حمزة اسماعيل ابو شنب . تقنيات التواصل الاجتماعي الاستخدامات والمميزات . شبكة الالوكة للثقافه والمعرفة . اغسطس 2013.
16. محمد جابر خلف الله. مفهوم مواقع التفاعل الاجتماعي . الموقع الرسمي للباحث محمد جابر خلف الله . مارس 2013 .
17. حمزة اسماعيل ابو شنب . مرجع سابق ص 78
18. يحي اليحياوي . التكنولوجيا والإعلام والديمقراطية . دار الطليعة بيروت ط 2004 . ص123 .
19. منير محمد الجنبيهي، ممدوح محمد الجنبيهي: "جرائم الأنترنيت والحاسب الآلي ووسائل مكافحتها". مرجع سابق ص 97 .
20. مجله الحياه . http://www.hayatfm.ae/gallery/10-4
21. جميل عبد الباقي صغير . مرجع سابق .ص 23
22. منير محمد الجنبيهي، ممدوح محمد الجنبيهي . مرجع سابق ص 97 .

23. منير محمد الجنبيهي .مرجع سابق . ص: 102

24. فاروق علي الحفناوي:"قانون البرمجيات". دراسة معمقة في الأحكام. الكتاب الأول، القانونية لبرمجيات الكومبيوتر. دار الكتاب الحديث. سنة 2000. ص: 112-113.

25. http://www.adjd.gov.ae/portal/site/adjd/.