عن خصوصية الجريمة المعلوماتية

بن عميروش ريمة
جامعة محمد الصديق بن يحي -جيجل -
Benamirouche.ry@gmail.com

تاريخ الإرسال: 2020/12/12 تاريخ القبول: 2020/04/21 تاريخ النشر:2020/10/23

الملخص:

إن الجريمة المعلوماتية من الجرائم المستحدثة؛ وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات وهي من الجرائم ذات الطبيعة الخاصة، إذ تتسم بخصائص منفردة لا تتوفر في الجرائم التقليدية الأخرى، لأنها تتخطى الحدود الجغرافية لاتصالها بعالم الانترنيت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، بسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها، و بالتالي صعوبة اكتشافها أو تحديد مصدرها ونسبتها لمرتكبها، ومن هنا يثور الإشكال حول إمكانية تطبيق إجراءات لضبط واثبات جريمة ارتكبت في عالم رقمي.

الكلمات المفتاحية : انترنت ، نظام معلوماتي ، خصائص ، مجرم معلوماتي.

Abstract:

Cybercrime is an emerging crime because it is linked to the advanced technology which is Information Technology, and it is one or crimes of a special nature because it has individual characteristics that are not available in other conventional crimes, because it transcends the geographical boundaries of its connection to the world of the Internet and information technology, where many countries may be affected by this crime at the same time, and Because of the great speed with which they are executed, the amount of funds and the persons targeted through them, and thus the difficulty of detecting or determining their origin and proportion to the perpetrator, Hence, problems arise about the possibility of applying procedures to arrest and prove a crime committed in a digital word

Key words : Internet, information system, characteristics, cybercriminal.

مقدمة :

عصر الانترنت أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية؛ كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت، ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة باعتبارها من مستحدثات العصر الراهن، والتي انعكست على كافة نواحي الحياة وأصبح هذا العصر عصر المعلومات بامتياز، حيث أصبحت مصدر قوة اقتصادية وسياسية وفكرية تسعى البلدان لامتلائها، وأضحى الوعي بأهميتها وقيمتها مظهرا من مظاهر رقي الشعوب والأمم وتحضرها، فهناك شواهد كثيرة على ايجابيات التسهيلات التي أتاحها التقدم العلمي والتكنولوجي، والتي فتحت أفاقا جديدة وفرصا متزايدة لتحسين أحوال معيشية الشعوب والأفراد، وتيسير حياتهم وممارساتهم لمهام الحياة المختلفة، و توفير الجهد و الوقت.

غير أن انحراف هذه الوسائل والصناعات التكنولوجية الحديثة عن مسارها، يجعل الإنسان يدفع ضريبتها، فلم يكن أحد من مخترعي الانترنت يعلم انه في يوم من الأيام سوف تشغل هذه الوسيلة الاتصالية في الإجرام، فالشبكة بوصفها نتاج المعلوماتية وأداة ربط واتصال بين مختلف شعوب العالم شكلت أداة لارتكاب الجريمة أو محلا لها وذلك بإساءة استخدامها واستغلالها على نحو غير مشروع أدى إلى ظهور طائفة جديدة من جرائم الانترنت عرفت بالجريمة المعلوماتية .

شهدت هذه المرحلة تناميا هائلا في حقل الجرائم الالكترونية وتغييرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات وظهرت أيضا أنماط تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بالعملية المعتادة.

وأكثر ما مورس ضد مواقع الانترنت الهامة التي يتسبب انقطاعها عن الخدمة ساعات في خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج، فشاع استعمال مصطلح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني ولكن هؤلاء المغامرون أصبحوا أداة إجرامية، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة للقدرة على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية والاجتماعية والسياسية والفكرية.

لقد أثارت هذه الظاهرة الإجرامية المستخدمة عدة مشاكل منها مسالة تكييف الاعتداء، ما إذا كان يشكل جريمة أم لا، بالإضافة إلى ما تثيره من مشكلة تحديد الاختصاص القضائي والقانون الواجب التطبيق على الجرائم المرتكبة عبرها بداية فيما يتعلق بالقانون الجنائي الموضوعي، بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم، واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجنائية.

و من هنا يمكن طرح الإشكالية التالية :

ما مدى خصوصية الجريمة المعلوماتية و تميزها عن الجرائم التقليدية ؟

للإجابة عن هذه الإشكالية تمّ تقسيم الموضوع إلى ثلاث محاور ، بالحديث في الأول عن عدم وجود مفهوم مشترك و موحد للجريمة المعلوماتية (**المبحث الأول**) ثم نعرج إلى خصائص الجريمة المعلوماتية (**المبحث الثاني**) و أخيرا نتطرق الطابع الخصوصي لمرتكب الجريمة المعلوماتية (**المبحث الثالث**).

المبحث الأول : عدم وجود مفهوم مشترك و موحد للجريمة المعلوماتية:

شكلت الجريمة المعلوماتية ظاهرة إجرامية وأخذت حيزا كبيرا من الدراسات من أجل تحديد مفهومها مما انجر عنه وضع عدة مصطلحات للدلالة عليها، من بينها جرائم الحاسب، جرائم التقنية العالية، جرائم المعلوماتية، جرائم الغش المعلوماتي، وصولا إلى جرائم الإنترنت ، ويعتبر عدم الاستقرار على مصطلح واحد للدلالة على الجريمة المرتكبة عبر الإنترنت، من الصعوبات الواردة عليها، والتي كانت هناك اتجاهات فقهية مختلفة في تعريفها إذ لم يتم التوصل إلى توحيد أو الإجماع على مفهوم موحد للجريمة المعلوماتية .

قبل التطرق إلى التعاريف المقدمة للجريمة الالكترونية، لابد أن نقر بعدم وجود مفهوم مشترك لها بين مختلف دول العالم، ويعود السبب في ذلك إلى اختلاف الأنظمة المعلوماتية المتبعة في جميع أنحاء العالم.

الفرع الأول : تباين التعاريف الفقهية للجريمة المعلوماتية

عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيرا احترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، وعلى المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم [1].

أدى اختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على وضع تعريف موحد لهذه الظاهرة الإجرامية، و تباين التعاريف المقدمة سواء من الفقه الذي انقسم إلى أربعة اتجاهات تقوم على أسس مختلفة في تعريف الجريمة المرتكبة عبر الإنترنت وهي:

أولاً: على أساس وسيلة ارتكابها

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما أن وسيلة ارتكاب الجريمة هو الحاسوب أو إحدى وسائل التقنية الحديثة المرتبطة به فتعتبر من جرائم الإنترنت، ومن ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا .[2]

عرف بعض الفقه الجريمة المرتكبة عبر الإنترنت بأنها :

" هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي وشبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف" .[3]

بصياغة أخرى عرفها البعض الآخر بأنها :

" بأنها الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه"[4].

تعتبر الجريمة المعلوماتية من هذا المنطلق، أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو بمعنى آخر هي كل فعل غير مشروع يكون علم تكنولوجيا الحاسبات الآلية بقدر كبير

لازماً لارتكابه[5] ، ويعتبر هذا التعريف بالغ العمومية والاتساع، لأنه يدخل فيه كل سلوك ضار بالمجتمع يستخدم فيه الحاسب الآلي .[6]

لقي تعريف الجريمة المرتكبة عبر الإنترنت المعتمد على الوسيلة المستخدمة في ارتكابها عدة انتقادات مفادها أن تعريف الجريمة يستوجب الرجوع إلى الفعل والأساس المكون لها [7] وليس إلى الوسائل المستخدمة لتحقيقها فحسب،أو لمجرد أن الحاسب استخدم في جريمة يتعين أن نعتبرها من جرائم الإنترنت[8].

والحجة التي اعتمد عليها منتقدي هذا التعريف مفادها، أنه لا يمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العمل الأساسي المكون لها، أي بمعنى آخر لكي تعرف الجريمة لا يجب الرجوع فقط إلى الوسائل المستخدمة لتحقيقها، ويترتب على ذلك أنه لا يكفي أن نعتبر مجرد استخدام الحاسب الآلي في الجريمة أنها من جرائم الانترنت .

ثانياً : على أساس توافر المعرفة التقنية

يستند أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية إلى معيار شخصي، والذي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات[9]، ومن بين هذه التعريفات نجد تعريف الأستاذ Thomson David" بأنها :

" كل جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب ".[10]

عرفها كذلك بعض من الفقه على أنها : " ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها ".

فمن منظور أصحاب هذه الاتجاه، يستلزم لتعريف الجريمة المرتكبة عبر الإنترنت توافر سمات شخصية لدى مرتكبها، ولقد حصروا هذه السمات أساسا في الدراية والمعرفة التقنية.[11]

إن اقتصار تعريف الجريمة المرتكبة عبر الإنترنت على شخصية الفاعل الذي لابد أن يكون لديه إلمام بالتعامل مع تقنية أجهزة الحاسب لآلي يعتبر قاصرا، إذ لابد الأخذ بالاعتبارات أخرى والمتعلقة بموضوع الجريمة[12] ، حيث أنه من غير المقبول و لا المعقول أن مجرد توافر المعرفة التقنية بعلم الحاسب و تقنياته لا يكفي في ظل عدم توافر العناصر الأخرى لتصنيف الجريمة ضمن الجرائم المتعلقة بذلك العلم .

ثالثا : على أساس موضوعها

يرى أصحاب هذا التعريف أن الجريمة المرتكبة عبر الإنترنت ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه [13]، ومن أشهر فقهاء هذا الاتجاه الفقيه rosenblatt" الذي عرف جريمة الإنترنت بأنها :

" نشاط غير مشروع موجه لنسخ، أو تغيير أو حذف، أو للوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تحول عن طريقه ".[14]

كما عرفت الجريمة المرتكبة عبر الإنترنت كذلك على النحو التالي :

" الجريمة المرتكبة عبر الإنترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة، وإساءة استخدام المخرجات، إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الكمبيوتر" .[15]

سايرت منظمة الأمم المتحدة هذا الاتجاه، حيث وصفت الجريمة المرتكبة عبر الإنترنت بأنها: " كل تصرف غير مشروع من أجل القيام بعمليات إلكترونية تمس بأمن الأنظمة المعلوماتية والمواضيع التي تعالجها".

تعرضت كل التعاريف السابقة لعدة انتقادات بسبب عدم دقتها في تحديد تعريف الجريمة المرتكبة عبر الإنترنت، إذ يكفي وفقا لهذه التعاريف أن يكون السلوك غير اجتماعي أو غير أخلاقي أو ضد المجتمع حتى يمكن اعتباره من قبيل جرائم الإنترنت، كما أن هذه التعاريف تعتمد على وصف الجريمة، و ليس على تحديد ماهيتها، ولا تتسع للعديد من الصور الإجرامية الممكن اقترافها.

نظرا للانتقادات الموجهة لهذا التعاريف السابقة ذهب بعض الفقه إلى الاعتماد على دمج كل هذه المعايير، مما يعطيه صفة الكمال ولو نسبيا، في انتظار أن يأتي الفقه بتعريف أكثر شمولاً .

المطلب الثاني: التعريف القانوني

تجنب أغلب المشرعين في الأنظمة المقارنة وضع تعريف تشريعي للجريمة المعلوماتية، وتركوا مهمة ذلك للفقه والقضاء، غير أن بعضهم قاموا بوضع عدة تعاريف لنظام المعلومات، لذا سنتطرق إلى تعريف القانون الجزائري، بالإضافة إلى بعض تعريفات الدول الأخرى .

الفرع الأول : تعريف الجريمة المعلوماتية في التشريع الجزائري

طبقا لقانون العقوبات الجزائري المعدل والمتمم الذي لم يعرف الجرائم المعلوماتية، واكتفى بالعقاب على بعض الأفعال تحت عنوان "الجرائم الماسة بالنظام المعالجة الآلية للمعطيات"[16].

و لكن في نص المادة 02 من قانون 04/09[17] عرفها، ولكن تبنى للدلالة على الجريمة مصطلح " المساس بأنظمة المعالجة الآلية للمعطيات"على أنها:

"جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات، أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ويلاحظ على هذا التعريف ما يلي:

- أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة، وهو نظام الاتصالات الإلكتروني، وثانيها معيار موضوع الجريمة المتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

- كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية، كونه أقر أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها فيه، وهذا ما يوسع نطاق مجال الجرائم الإلكترونية في القانون الجزائري.

الفرع الثاني : تعريف الجريمة المعلوماتية وفقا للتشريعات المقارنة :

من بين التشريعات التي عرفت النظام المعلوماتي، والذي يعد مكونا أساسيا لصور الجرائم الإلكترونية نذكر:

1.قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001:

حيث عرف هذا القانون بدوره من خلال نص المادة 02 فقرة 10 نظام المعلومات (المعالجة المعلوماتية) على أنه:

" النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو تخزينها أو تجهيزها على أية وجه آخر"[18].

2. قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية رقم 02 لسنة 2002:

وقد عرفها هذا القانون من خلال نص المادة 02 فقرة 06 على أنه:

" نظام إلكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا"[19].

3.أما المشرع السعودي فقد عرف نظام المعلومات من خلال نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، بموجب نص المادة 01 النظام المعلوماتي بأنه "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية".

المبحث الثاني: خصائص الجريمة الالكترونية:

نظرا لارتباط الجريمة الالكترونية بجهاز الحاسوب، وشبكة الانترنت بصفة عامة، ووسائل الاتصال الاجتماعي بصفة خاصة، فان ذلك قد ميزها بمجموعة من الخصائص عن الجريمة التقليدية وأهم هذه الخصائص ما يلي:

الفرع الأول: جريمة عابرة للحدود.

إن انتشار شبكة الانترنت أعطى إمكانية واسعة لربط عدد كبير من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية، دون أن تخضع لحدود الزمان والمكان، لذلك فمن السهولة أن يكون المجرم في بلد والمجني عليه مقيما في بلد أخر، وهنا تظهر الحاجة لوجود تنظيم دولي وداخلي متلائم معه لمكافحة هذا النوع من الجرائم وضبط فاعليتها.[20]

هذه الطبيعة التي تميزت بها الجريمة المعلوماتية كونها عابرة للحدود خلفت عدة مشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق بالإضافة إلى إشكالية تتعلق بإجراءات الملاحقة القضائية.

ومن القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية،، تلك القضية المعروفة باسم مرض نقص المناعة المكتسبة (الايدز) وتتلخص وقائعها في قيام أحد الأشخاص بتوزيع بعض النسخ التي كانت هدفها

في الظاهر إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أنها في الحقيقة كانت تحتوي على فيروس (حصان طروادة).

تدخل الجرائم المرتكبة عبر الانترنت في نطاق القانون الجنائي الداخلي، وحيث أنها جرائم تتخطى حدود الدولة الواحدة فهي تدخل في نطاق دراسات القانون الجنائي الدولي، ونظرا لنمو تزايد التجارة الالكترونية من خلال المبادلات والمراسلات، فأصبحت لصيقة بالقانون التجاري، وكذلك أدى ظهور الإنسان المعلوماتي وتكون المجتمع الالكتروني إلى تزايد استهلاك الحقوق والحريات الفردية التي تقلها القوانين الدستورية أي ارتباطها أيضا بالقانون الإداري والدستوري.

بصفة عامة إن إساءة استخدام شبكة الانترنت تتداخل مع جميع فروع القانون الداخلي والخارجي.

الفرع الثاني: صعوبة اكتشافها وإثباتها.

تتميز الجرائم الالكترونية بصعوبة اكتشافها وإثباتها، ويعود السبب في ذلك لعدم ترك الجاني آثارا تدل على إجرامه، فالجرائم تتم بواسطة رموز وأرقام، وهذه الأخيرة تكون دقيقة جدا يصعب اكتشافها وغالبا ما يتم اكتشافها عن طريق الصدفة.

إن الجرائم الالكترونية لا تترك أثرا ملموسا، وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم، ومن الصعب العثور على دليل مادي في الجرائم الالكترونية، ويعود السبب في ذلك، إلى استخدام الجاني وسائل فنية وتقنية معقدة في اغلب الأحيان، وهذا السلوك المادي في ارتباطها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به.

الفرع الثالث: وقوعها في بيئة المعالجة الآلية للمعطيات.

من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا الشرط الأساس الذي يجب أن يتوفر حتى يمكننا القول في قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام المعالجة للبيانات، وإذا تخلف هذا الشرط تنتفي الجريمة المعلوماتية.[21]

الفرع الرابع: قلة الإبلاغ عن وقوع الجريمة المعلوماتية.

إن الإبلاغ عن الجريمة التي تحدث في مجال الانترنت يكون نادرا وذلك لعدم الاكتشاف من قبل الضحايا لها، أو خشية من التشهير، لذلك فان اكتشافها في الغالب يكون صدفة، أو بعد مرور وقت طويل من ارتكابها.

فالأضرار الناتجة عن الجرائم المعلوماتية والتي تعتبر جريمة مستحدثة في تزايد مستمر وذلك نتيجة الغش والاختلاس الذي ينتج عن اختراق المواقع الكبرى للشركات والبنوك العالمية.[22]

الفرع الخامس : سرعة محو الدليل وتوفروسائل تقنية تعرقل الوصول إليه

يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب، على اعتبار أن الجريمة تتم في صورة

أوامر تصدر إلى الجهاز، وما إن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، و هو الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها،أمرا في غاية الصعوبة،[23] وهذه الخاصية ساهمت في الانتشار الواسع لهاته الجريمة بالرغم من حداثتها، وفي وقت قصير جدا تمكنت من غزو العالم بأسره وتهديد مصالح الأفراد والدول في جميع مجالات الحياة، وهذا ما أثبتته عديد الدراسات والإحصائيات التي أجريت في عديد الدول سواء المتقدمة منها أو النامية.

وأظهرت دراسة لموقع "أرقام ديجتال" أن عدد ضحايا الهجمات والجرائم الالكترونية، يبلغ555 مليون مستخدم سنويا، وأكثر من 1.5 مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات وأكثر أنواع الجرائم سرقة هويات، وعددها 224 مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ بينت أن أكثر من 600 ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100 مليار دولار، بعدما كانت في حدود 63,1 مليار دولار سنة 2011، ومن المتوقع هذا المبلغ في السنوات القادمة [24].

و بحسب تقرير نشرته شركة مشاريع الأمن السيبراني (CYBERSECURITY VENTURES) بعنوان Cyber Security Economy predictions 2017-2021 ، فإن العالم سينفق ما قيمته 1 تريليون دولار خلال الفترة التي تمتد من 2017 الى غاية 2021 على منتجات وخدمات الأمن السيبراني لمكافحة الجريمة الالكترونية، و في هذا الإطار فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن السيبراني خلال سنة 2016، ومن المتوقع أن يكون هناك عجز بحوالي 1,5 مليون وظيفة خلال عام 2021 .[25]

المبحث الثالث :الطابع الخصوصي لمرتكب الجريمة المعلوماتية.

شاع استعمال مصطلح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني ولكن هؤلاء المغامرون أصبحوا أداة إجرامية، وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة للقدرة على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية والاجتماعية والسياسية والفكرية.

لذا كان لابد من البحث عن أسباب ارتكاب الجريمة المعلوماتية و التي غالبا ما تكون دوافع شخصية لمرتكب الجرائم المعلوماتية يمكن ردّها إلى دوافع مالية لتحقيق الكسب السريع و السهل و قد يكون الدافع هو المتعة والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات، فاختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية لتغطية أوقات فراغه.

لذا سنتطرق في الاول في الصفات الخاصة في المجرم المعلوماتي (مطلب أول) ثم نبحث عن دوافع ارتكابه لهذا النوع من الجرائم (مطلب ثان).

المطلب الاول : المجرم المعلوماتي ذو صفات خاصة :

يطلق على الشخص الذي يرتكب الجريمة المعلوماتية اسم المجرم المعلوماتي، ويتسم هذا الأخير بمجموعة من الخصائص تميزه بصفة خاصة عن غيره من المجرمين الذي يرتكبون الجرائم التقليدية، فهو شخص يتمتع بصفات خاصة، كالمهارة والمعرفة والذكاء، وعند ارتكابه للجريمة يبررها بمبررات مختلفة لأنه يخاف من كشف جريمته نفصل هذه الصفات فيما يلي:

الفرع الاول :المهارة:

تعتبر المهارة من أهم خصائص المجرم المعلوماتي، وهي ضرورية لتنفيذ النشاط الإجرامي ويكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال المعلومات، إلا أن هذا لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج.

الفرع الثاني :السلطة

تتم ارتكاب الجرائم المعلوماتية عادة بتعاون أكثر من شخص على ارتكابها، بقصد الأضرار بالمجني عليه، وغالبا ما يساهم في إخراج ذلك إلى الحيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بتنفيذ الجانب الفني من المشروع الإجرامي، كما يقوم شخص آخر بتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج هذه الجريمة إلى حيز الوجود قد يكون سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة محاولة منه تسهيل إتمامها، كما قد يكون ايجابيا وهو غالبا ما يتمثل في مساعدة فنية ومادية.[26]

الفرع الثالث :الميل إلى ارتكاب الجرائم

يتميز مرتكبو الجرائم الإلكترونية بوجود النزعة الإجرامية والميل إلى ارتكاب الجرائم لديهم، هذا على الرغم مما يكتسبونه من مهارات في مجال في مجال التقدم التكنولوجي، فمرتكب الجريمة الإلكترونية يتعلم ويتقن المهارات التكنولوجية لكي تساعده على ارتكاب الجرائم، وتكون تلك النزعة الإجرامية لدى الشخص نتيجة لتأثره بعوامل عضوية وعوامل نفسية صاحبت نشأة الشخصن ومع اقتران تلك العوامل بعنصر آخر جديد يساعده على استثارة الحالة الإجرامية[27] ، كما يمكن أن نطلق عيهم بالأشخاص المهووسين من حيث مهاراتهم التقنية و استغلالها الشنيع و المضر .

الفرع الرابع :التطور السريع في السلوك الإجرامي للمجرمين

يؤدي وجود الفرد في جماعة إجرامية مهما بلغت قدرتها العلمية أو المهارية إلى التأثير في قدرته العقلية، وسرعة اكتشاف المهارات التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى محاولة الوصول إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة[28].

المطلب الثاني: دوافع مرتكب الجريمة الالكترونية.

عادة ما تسبق الحاجة الدوافع، فالحاجة تنشأ من الشعور بالنقص أو الحرمان من شيء ما لدى الفرد، بغرض إشباع هذه الحاجات التي يحقق تواجدها حالة من الرضا النفسي، وتتنوع دوافع الأقدام على الجريمة المعلوماتية باختلاف مرتكبيها، ويمكن تصنيف هذه الدوافع إلى صنفين: دوافع شخصية ودوافع خارجية.

الفرع الأول: الدوافع الشخصية.

إن الدوافع الشخصية لمرتكب الجرائم المعلوماتية يمكن ردّها إلى دوافع مالية ودوافع ذهنية أو نمطية.

أولا: الدوافع المادية لتحقيق الكسب السريع و السهل للمال.

يعتبر الدافع المادي من أهم الدوافع على ارتكاب الجرائم المعلوماتية، والذي يهدف إلى تحقيق الكسب المالي والذي هو في الغالب غاية الفاعل، ومن مميزات هذه الجرائم، أن حجم الربح الكبير الممكن تحقيقه من بعض الجرائم خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب الذي يعزز هذا الدافع بما تحققه من ثراء فاحش، ودليل ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000 فرنك فرنسي، أما جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي ما يعادل أكثر من 38 مرة.

ولقد أثبتت الدراسات وأشارت إلى أن الدافع الرئيسي لأنشطة احتيال الكمبيوتر هو تحقيق الكسب المالي.

ثانيا: الدوافع المعنوية

قراصنة الكومبيوتر يكرس كل جهده في تعلم كيفية اختراق المواقع الممنوعة للحصول على المعلومات ويكون القراصنة مجهولون وذلك من اجل الاستمرار لأطول فترة ممكنة، كما يشكلون مجموعة يكون الهدف منها هو التعاون وتبادل المعلومات وتقاسم البرامج والأخبار.[29]

غالبا ما يكون الدافع لارتكاب هذه الجرائم هو المتعة والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات، فان اختراق الأنظمة الاليكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية لتغطية أوقات فراغه.

الفرع الثاني: الدوافع الخارجية.

إن الإنسان يتأثر في بعض المواقف ويستسلم للمؤثرات والدوافع الخارجي بارتكابه بعض الجرائم وتتمثل هذه الدوافع في ما يلي:

أولا: دافع الانتقام وإلحاق الضرر .

إن الدوافع لارتكاب الجريمة المعلوماتية قد يكون بهدف الانتقام من شخص معين أو مؤسسة ما أو من بعض الأنشطة السياسية في بعض الدول أو من رب العمل.[30]

إن الانتقام موجود في النفس البشرية، فنجد أن الكثير من الأشخاص يتم فصلهم من الشركات أو المؤسسات التي يعملون فيها، بحيث يكون هؤلاء الأشخاص يملكون معلومات، ومعرفة كافية بخفايا هذه المؤسسات، فيقوم الجاني بارتكاب هذه الجريمة رغبة منه في الانتقام ليجعل هذه الجريمة رغبة منه في الانتقام

ليجعل هذه الشركة أو المؤسسة تصاب بخسائر مالية كبيرة من جراء ما يسببه لها من أضرار بحيث يحتاج لإصلاحه وقت لا بأس به. [31]

ثانيا: دوافع التعاون والتواطؤ على الأضرار.

إن هذا النوع غالبا ما يحدث من متخصص في الأنظمة المعلوماتية، بحيث يقوم بالجانب الفني من المشروع وأخر من المحيط أو خارج المؤسسة المجني عليه لتغطية عملية التلاعب وتمويل المكاسب وعادة ما يمارسون التنصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم. [32]

ثالثا: الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية.

إن الهدف من هذا الدافع هو إظهار مرتكب الجريمة تفوقه ومستوى ارتقاء براعته إزاء ظهور أي تقنية مستحدثة، لذا فان مرتكب الجريمة لديه شغف في محاولة استكشافها و التغلب عليها مهما بلغت درجة تعقيدها، وينتشر هذا الدافع لدى فئة صغار السن، الذين يمضون وقتا طويلا أمام حواسبهم الشخصية، محاولة منهم كسر حواجز الأمن لأنظمة الحواسيب، و شبكات المعلومات بإظهار تفوقهم على الوسائل التقنية.

خاتمة

تكمن الطبيعة الخاصة للجريمة المعلوماتية في خصائصها المتميزة، والمتمثلة في أنها جريمة عابرة للحدود باعتبارها ترتكب عن طريق الانترنت، كما تتميز بسرعة تنفيذها والتطور المتسارع في ارتكابها، وقد أثارت عدة تساؤلات كثيرة باعتبارها ظاهرة جديدة نظرا لجسامة أخطارها، وفداحة خسائرها وسرعة انتشارها، فأصبحت موضع اهتمام بالغ من المختصين والمهتمين بالأمن المعلوماتي لتحديد مفهومها وخصائصها، كما أن هذه الجريمة الإلكترونية أخرجت طائفة جديدة من المجرمين يتسمون بصفات خاصة لدرجة انه يصعب حتى تقويم سلوكهم أو محاولة إيقافهم .

لذلك نقدم بعض الحلول و المقترحات سعيا لمواجهه الجريمة المعلوماتية والحد من انتشارها من خلال ما يلي:

- ✓ باعتبار أن الأسرة هي أساس المجتمع يجب أن يتم توعية الأولياء، و توفير الوسائل التي من شأنها أن تساعدهم للقيام بدورهم كاملا كمراقب أولي.
- ✓ إدراج مواد أساسية، أو على الأقل دروس توعية على مستوى جميع الأطوار التعليمية، تركز فيها على مخاطر الاستغلال السيئ للانترنت.
- ✓ وضع تعريف يتلاءم مع جرائم المعلوماتية وطبيعتها وخصائصها محاولا فيها توحيد مختلف التعريفات المتعلقة، بها دون إهمال فكرة العالمية ، بحيث يكون متفقا عليه على المستوى العالمي وان يكون مرنا بحيث يمكن له مسايره التطور التكنولوجي المتسارع.

✓ ضرورة استحداث نصوص قانونية جديدة خاصة في قانون الإجراءات الجزائية، حتى تتلاءم في مجال الضبط والتحقيق لعدم ملائمة الإجراءات التقليدية في مواجهة هذه الجرائم إضافة إلى تحديث الأساليب الإجرائية المتبعة في الجرائم المعلوماتية، دون أن تتعرض حقوق الأفراد وحرياتهم للخطر عند الإثبات في مجالها.

✓ ضرورة عقد ملتقيات والتعاون المكثف بين التقنيين والخبراء في الحقول الالكترونية مع ضباط الشرطة القضائية والقضاة بشكل دوري ودائم، للاستفادة من خبراتهم وإرشاداتهم ابتداء من مرحلة التحري والاستدلال وجمع الأدلة وانتهاء بأحكام المحاكم، خاصة فيما يتعلق بالخبرة والشهادة في المجال المعلوماتي، وتفعيل الدور الوقائي للقضاء المستعجل في مجال الجرائم المتعلقة بالإنترنت.

قائمة المراجع :

اولا :الكتب :

1. احمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006.
2. خالد ممدوح ابراهيم، الجرائم المعلوماتية، طبعة الأولى، دار الفكر الجامعي، مصر ،2009.
3. محمد امين الرومي، جرائم الكومبيوتر الانترنت، دار المطبوعات الجامعية، الجزائر، 2003.
4. محمد حماد مرهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الأولى، دار المناهج للنشر والتوزيع، الأردن، 2006 .
5. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية القاهرة،2009.
6. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005 .
7. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها، مكافحتها)، دار الكتب القانونية، مصر 2005 .
8. نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الاردن، 2008.
9. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، الجزائر،2009.

ثانيا: الرسائل و المذكرات الجامعية :

أ/ رسائل الدكتوراه :

1. عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية جامعة نايف العربية للعلوم الأمنية كلية الدراسات العليا، قسم العلوم الإدارية، الرياض 2010.

2. غازي عبد الرحمن هيان الرشيد، ، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت) أطروحة لنيل شهادة الدكتوراه في القانون الجامعة الإسلامية كلية الحقوق ، لبنان ،2004.

ب/ مذكرات الماجستير:

1. قارة امال، ، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الجنائي و العلوم الجنائية ، كلية الحقوق جامعة الجزائر ،2002.

2. عبد الله دعش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، مذكرة لنيل شهادة الماجستير، قانون عام، جامعة الشرق الأوسط، 2014.

3. منصور بن صالح السلمي ، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية الرياض، 2010.

ثالثا : المقالات

1. عارف خليل أبو عيد , "جرائم الإنترنت (دراسة مقارنة)" ، مجلة الشارقة للعلوم الشرعية والقانونية المجلد 5، العدد 3، أكتوبر 2008.

2. كحلوش علي، « جرائم الحاسوب وأساليب مواجهتها »، مجلة الشرطة، تصدر عن المديرية العامة للأمن 14 الوطني، العدد 84 ،جويلية 2007.

رابعا: المداخلات :

1. رحمة نمديلي، خصوصية الجرائم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الجرائم الإلكترونية، يومي 24، 25 مارس 2017، طرابلس.

2. موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، 2009، أكاديمية الدراسات العليا، طرابلس.

3. هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي ، بحوث مؤتمر القانون والكمبيوتر والإنترنت، من 1-3 ماي 2000،جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، الامارات العربية المتحدة .

4. يونس عرب، جرائم الكمبيوتر والانترنت (إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات) ، مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، يومي 10 -12 فيفري 2002، أبو ظبي.

خامسا: النصوص القانونية

أ/ القوانين الجزائرية :

1. قانون رقم 04-15 المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156، يتضمن قانون العقوبات الجريدة الرسمية عدد 71، مؤرخ بتاريخ 2004/11/10، المعدل والمتمم.
2. قانون رقم 09-04 المؤرخ في 5 /08/ 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، مؤرخ في 06 اوث 2009.

ب/ القوانين الأجنبية :

1. قانون رقم 85 سنة2001، المتضمن المعاملات الإلكترونية للمملكة الهاشمية، الجريدة الرسمية رقم 4524 الصادر بتاريخ 2001/12/31 .
2. قانون إمارة دبي رقم 02 لسنة 2002، متعلق بالمعاملات والتجارة الإلكترونية، الصادر بتاريخ 12 فبراير 2002.

سادسا : المحاضرات

بورزام أحمد، وكيل الجمهورية لدى محكمة باتنة، محاضرة تحت عنوان (جرائم المعلوماتية)، المجلس القضائي بباتنة، 20 جوان 2006.

سابعا : مواقع الانترنت

احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 2015/10/25 متوفرة على موقع http://digital.argaam.com :

– cyber security economy predictions 2017-2021,cybersecurity ventures https://cybersecurityventures.com/2019/05/ 14 .

.

الهوامش:

[1] - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية القاهرة،2009، ص32.

[2] - محمد عبيد الكعبي، مرجع سابق ، ص33.

[3] - مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية(ماهيتها، مكافحتها)، دار الكتب القانونية، مصر، 2005 ص56 .

انظر كذلك : كحلوش علي، « جرائم الحاسوب وأساليب مواجهتها »، مجلة الشرطة، تصدر عن المديرية العامة للأمن 14 الوطني، العدد 84 ،جويلية 2007 ،ص51 .

[4]- رحمة نمديلي، خصوصية الجرائم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الجرائم الإلكترونية، المنعقد يومي 24، 25 مارس 2017،طرابلس ، ص 98.

[5]- عارف خليل أبو عيد , جرائم الإنترنت (دراسة مقارنة) ، مجلة الشارقة للعلوم الشرعية والقانونية، المجلد 5 العدد 3، أكتوبر 2008 ، ص82.

[6]-عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، أطروحة مقدمة استكمالاً لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية كلية الدراسات العليا، قسم العلوم الإدارية، الرياض 2010 ،ص21.

[7]- قارة امال، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون ، تخصص القانون الجنائي و العلوم الجنائية ، كلية الحقوق جامعة الجزائر ،2002، ص19.

[8]- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية كلية الحقوق ، لبنان ،2004، ص107.

[9]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005 ،ص 16 .

[10]- هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي ، بحوث مؤتمر القانون والكمبيوتر والإنترنت، من 1-3 ماي 2000، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، ص407 .

[11]- بورزام أحمد، وكيل الجمهورية لدى محكمة باتنة، محاضرة تحت عنوان (جرائم المعلوماتية)، المجلس القضائي بباتنة، 20 جوان 2006، ص 7 .

[12]- منصور بن صالح السلمي ، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية كلية الدراسات العليا، قسم العدالة الجنائية الرياض، 2010 ، ص63 .

[13]- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2006 ،ص ص85-86 ،

أنظر كذلك: محمد حماد مرهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الأولى، دار المناهج للنشر والتوزيع، الأردن، 2006 ،ص78.

[14] - غازي عبد الرحمن هيان الرشيد، مرجع سابق، ص106 .

[15] - يونس عرب، جرائم الكمبيوتر والانترنت (إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات) ، مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، 10 -12 فيفري 2002، أبو ظبي ،ص8 .

[16]- قانون رقم 04-15 المؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156، يتضمن قانون العقوبات، الجريدة الرسمية عدد 71، مؤرخ بتاريخ 2004/11/10، المعدل والمتمم.

[17]- قانون رقم 09-04 المؤرخ في 5 /08/ 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، مؤرخ في 06 اوث 2009.

[18] - قانون رقم 85 سنة2001، المتضمن المعاملات الإلكترونية للمملكة الهاشمية، الجريدة الرسمية رقم 4524 الصادر بتاريخ 2001/12/31 ص 6010.

[19]- قانون إمارة دبي رقم 02 لسنة 2002، متعلق بالمعاملات والتجارة الإلكترونية، الصادر بتاريخ 12 فبراير 2002.

[20]- عبد الله دعش العجمي، المشكلات العلمية والقانونية للجرائم الالكترونية دراسة مقارنة، مذكرة لنيل شهادة الماجستير، قانون عام، جامعة الشرق الأوسط، 2014، ص20.

[21]- خالد ممدوح ابراهيم، الجرائم المعلوماتية، طبعة الأولى، دار الفكر الجامعي، مصر ،2009، ص83.

[22]- خالد ممدوح ابراهيم، مرجع سابق، ص86.

[23] - موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون أكاديمية الدراسات العليا، 2009، طرابلس، ص3.

[24] - احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 2015/10/25 متوفرة على موقع http://digital.argaam.com :

[25] – cyber security economy predictions 2017-2021,cybersecurity ventures 2016

https://cybersecurityventures.com/ 2019/05/ 14 .

[26]- نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، الجزائر،2009، ص58.

[27]- خالد ممدوح إبراهيم، مرجع سابق، ص 135.

[28]- مرجع نفسه، ص 137.

[29]- محمد امين الرومي، جرائم الكومبيوتر الانترنت، دار المطبوعات الجامعية، الجزائر، 2003، ص24.

[30]- نهلا عبد القادر المؤمني ، مرجع سابق، ص94.

[31]- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الاردن، 2008، ص25.

[32]- احمد خليفة الملط، الجرائم المعلوماتي، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006، ص90.