الجمهورية الجزائرية الديمقراطية الشعبية

جامعة ابن خلدون –تيارت

كلية الحقوق والعلوم السياسية

قسم: الحقوق

أوجه الحماية الجنائية لمستخدمي الانترنت

مذكرة لنيل شهادة ماستر في شعبة الحقوق

تخصص : قانون جنائي

اعداد الطالب:

زغبة عبد القادر

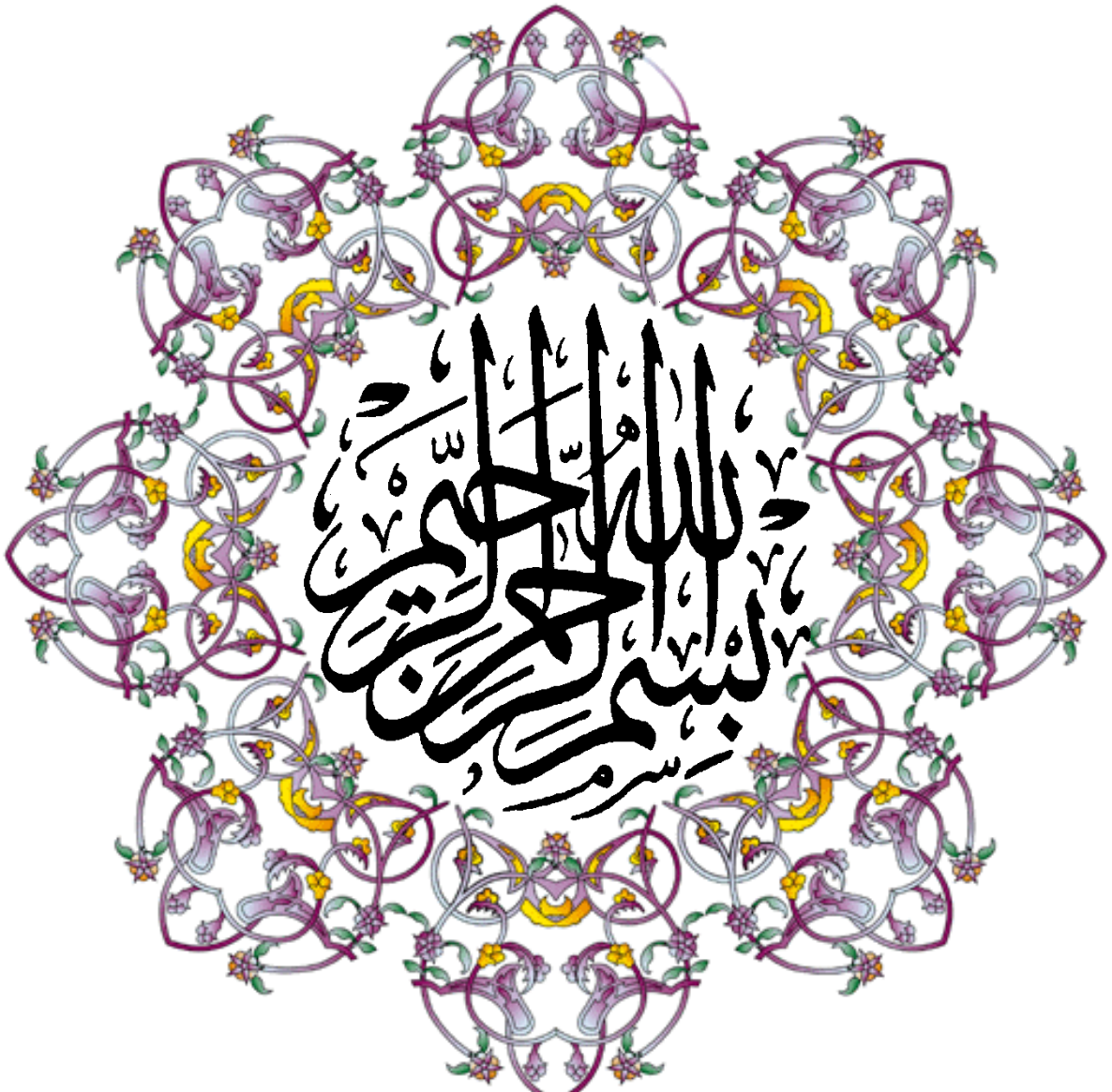
تحت إشراف :

أ.د- قايد ليلى

اعضاء اللجنة المناقشة

أ.د- حاج شعيب فاطيمة	استاذ محاضر "ب"	رئيسا
أ.د- قايد ليلى	استاذ التعليم العالي	مشرفا ومقررا
د. عبيدفتيحة	استاذ محاضر "أ"	مناقشا

السنة الجامعية : 2022-2023



﴿وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ ۚ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ﴾

سورة هود 88

-اولا وجوب شكر وحمد المولى عز وجل على توفيقه وتيسره الامور حتى اتمكن من انجاز هده المذكرة في احسن الظروف فالحمد لله على نعمه بالشكر تدوم النعم وصلى الله على مُحَمَّد واله وصحبه ومن تبعه بإحسان الى يوم الدين

-كما لا يفوتني ان اشكر الاستاذة المشرفة موضوع المذكرة الاستاذة قايد ليلى على توجيهاتها ونصاحها اثناء القيام بإنجاز هذه المذكرة وجميع الاساتذة الذين قدموا لي المساعدة في القيام بهذا الموضوع

الى زملائي الذين قاموا بمساعدتي في القيام بهذه المذكرة اقدم لهم كل الشكر ووفقهم الله في امورهم

– الى من قالى تعالى فيهم ﴿ وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُلْ رَبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا﴾.

– الى الوالدين الكريمين الغالين حفضهما الله اغلى من في الوجود الذان ربياني وقدما لي كل شيئ حتى اتوفق في حياتي ودراستي فبفضلهما ما وصلت اليه اهدي اليهم ثمرة جهدي هذا

– الى اخوتي واخواتي على دعمهم وتشجيعهم دائما وفي القيام بهذه المذكرة

– الى زملائي في الدراسة الجامعية بمناسبة التخرج وختام الدراسة الجامعية اتمنى لهم التوفيق في حياتهم .

مقدمة

مقدمة :

يعيش العالم في عصر رقمي يتسم بتطور مذهل في تكنولوجيا المعلومات والاتصالات. تعد شبكة الإنترنت من أبرز الابتكارات التي غيرت العالم بشكل جذري، إذ أصبحت واحدة من أهم وسائل الاتصال والمعلومات في حياة الملايين حول العالم. ومع زيادة استخدام الإنترنت، تزايدت أيضًا التحديات والمخاطر المرتبطة بهذه التكنولوجيا الرقمية.

من بين تلك التحديات والمخاطر التي يواجهها مستخدمو الإنترنت هي التهديدات الجنائية المتعلقة بالسلامة والأمان الشخصي. فالإنترنت أصبحت مجالًا لارتكاب الجرائم المختلفة مثل الاحتيال الإلكتروني، وسرقة الهوية، والتجسس، والتحرش الجنسي، وانتهاكات الخصوصية، والتحريض على الكراهية والعنف، والتهديدات الإلكترونية، وغيرها من الأعمال الإجرامية.

لذلك، يأتي هذا البحث لتسليط الضوء على مسألة الحماية الجنائية لمستخدمي الإنترنت ودراستها بمنهجية مذكرات التخرج. يهدف البحث إلى تحليل وتقييم التهديدات الجنائية المتعلقة بالإنترنت وتأثيرها على سلامة المستخدمين، وتقديم توصيات وحلول فعالة للحد من هذه التهديدات وتعزيز الأمان الرقمي

بفضل التقدم التكنولوجي السريع وانتشار الإنترنت، أصبحت الحماية الجنائية لمستخدمي الإنترنت أمرًا حيويًا وملحًا في عصرنا الحالي. فعلى الرغم من الفوائد الهائلة التي يوفرها الإنترنت، إلا أنه ينطوي أيضًا على تحديات أمنية جديدة وتهديدات جنائية متزايدة.

تعتبر الجرائم الإلكترونية مثل الاحتيال الإلكتروني وسرقة الهوية والتجسس والتحرش الجنسي وانتشار المحتوى الضار على الإنترنت من بين التهديدات الشائعة التي يواجهها المستخدمون. تزداد تعقيدات هذه الجرائم وتطورها باستمرار، مما يتطلب منا أن نتبنى منهجيات قوية وفعالة للحماية والمواجهة.

لذا، فإن الدراسة في مجال الحماية الجنائية لمستخدمي الإنترنت تأخذ أهمية بالغة. إنها تساهم في تحليل وفهم عميق للتهديدات الجنائية والتحديات التي تواجه المستخدمين والمجتمعات على الإنترنت. كما تعزز الوعي والتثقيف حول أفضل الممارسات والسلوكيات الآمنة وتساعد على تطوير السياسات والتشريعات اللازمة لمكافحة الجرائم الإلكترونية.

اسباب اختيار الموضوع :

تزايد التهديدات الجنائية عبر الإنترنت: مع تطور التكنولوجيا الرقمية، زادت أيضًا التهديدات الجنائية التي يواجهها مستخدموا الإنترنت. من المهم فهم هذه التهديدات ودراستها بشكل مفصل لتحسين الأمان الرقمي وحماية المستخدمين.

حماية حقوق المستخدمين: يتمتع المستخدمون بحقوق مشروعة للحماية من الجرائم الإلكترونية والانتهاكات الرقمية. يهدف هذا البحث إلى توضيح هذه الحقوق ودراسة السبل الممكنة لحمايتها بشكل فعال.

الأثر الاجتماعي والاقتصادي: تعد الجرائم الإلكترونية والانتهاكات الرقمية من أبرز التحديات التي تؤثر على المجتمع والاقتصاد. يعمل هذا البحث على فهم الأثر الاجتماعي والاقتصادي لتلك الجرائم وتوفير حلول للتصدي لها.

الحاجة للتوعية والتدريب: يعد التوعية والتدريب الفعال للمستخدمين أمرًا ضروريًا للحماية الجنائية على الإنترنت. يهدف هذا البحث إلى تقديم توصيات فيما يتعلق ببرامج التوعية والتدريب لتمكين المستخدمين من حماية أنفسهم.

التطورات التكنولوجية: يتسارع التطور التكنولوجي وتتطور أساليب الهجمات الإلكترونية والاحتيال الإلكتروني. يجب مواكبة هذه التطورات وتطوير إستراتيجيات حماية جديدة للحد من التهديدات

أهداف الدراسة :

تحليل التهديدات الجنائية: تهدف الدراسة إلى تحليل وتصنيف التهديدات الجنائية المرتبطة بمستخدمي الإنترنت، مثل الاحتيال الإلكتروني وسرقة الهوية والتجسس والتحرش الجنسي والتهديدات الإلكترونية الأخرى. ستتم دراسة أنماط الجرائم الإلكترونية وتحليل طرق تنفيذها والتحولات الجديدة في هذا المجال.

تقييم تأثير التهديدات الجنائية: يهدف البحث إلى تقييم التأثير الذي يترتب على هذه التهديدات الجنائية على المستخدمين الأفراد والمؤسسات سيتم دراسة الأضرار المحتملة التي يمكن أن تلحق بالمستخدمين من الناحية الشخصية والمهنية والمالية.

مقدمة :

أهميد الدراسة :

حماية المستخدمين: تهدف الدراسة إلى تعزيز حماية المستخدمين الأفراد والمؤسسات من التهديدات الجنائية على الإنترنت. يعتبر ضمان الأمان الرقمي للمستخدمين أمرًا حاسمًا للحفاظ على خصوصيتهم وحقوقهم الرقمية وتجنب الأضرار الجسيمة التي يمكن أن تلحق بهم.

التوعية والتثقيف: تساعد هذه الدراسة في توعية المستخدمين حول التهديدات الجنائية على الإنترنت وتعزيز مستوى وعيهم بأفضل الممارسات والسلوكيات الآمنة. يمكن أن يؤدي زيادة الوعي والتثقيف إلى تقليل فرص الوقوع في الجرائم الإلكترونية وزيادة مستوى الحماية الفردية والجماعية.

الحماية الاقتصادية: يعد الإنترنت جزءًا حيويًا من النشاط الاقتصادي في العصر الرقمي. تساهم الحماية الجنائية لمستخدمي الإنترنت في تعزيز الثقة في التجارة الإلكترونية والتعاملات المصرفية عبر الإنترنت وتشجيع الابتكار والنمو الاقتصادي.

الحماية القانونية والتشريعية: يواجه المجتمع تحديات قانونية في مجال الجرائم الإلكترونية والانتهاكات الرقمية. تساهم الدراسة في تحليل التشريعات الحالية والفجوات القانونية وتوفير توصيات لتطوير السياسات والقوانين للحماية الجنائية الأكثر فاعلية

المنهج المتبع

مراجعة الأدبيات: ستتضمن هذه الخطوة مراجعة الدراسات السابقة والأبحاث المنشورة والمصادر الأكاديمية ذات الصلة بموضوع الحماية الجنائية لمستخدمي الإنترنت. ستستخدم قواعد البيانات المتخصصة والمكتبات الأكاديمية للعثور على المصادر المناسبة واستخلاص المعلومات المهمة.

تصميم البحث: ستتم تحديد أهداف البحث وتحديد الأسئلة البحثية والفرضيات الأساسية التي ستوجه الدراسة. سيتم أيضًا تحديد المتغيرات المستقلة والمتغيرات التابعة التي ستستخدم في جمع وتحليل البيانات.

جمع البيانات: سيتم جمع البيانات من مصادر متنوعة، سواء كان ذلك عن طريق استبانة أو مقابلات شخصية أو تحليل المستندات ذات الصلة وعلى هذا الأساس تطرح الاشكالية :

"ما هي أفضل السبل والاستراتيجيات لتعزيز الحماية الجنائية لمستخدمي الإنترنت والحد من التهديدات الجنائية الرقمية التي يواجهونها ؟

و للاجابة عن هذه الاشكالية اقترحت الخطة الاتية محاولة الالمام بالموضوع من جميع جوانبه و تسليط الضوء على أهم النقاط تستدعي الدراسة فقد قمت بتقسيم هذا البحث الى فصلين تناولت في الفصل الأول المفهوم العام لجرائم الانترنيت و ذلك من خلال التعرف على ماهية جرائم الانترنيت (المبحث الأول) و الأنواع و الدوافع (المبحث الثاني) أمافي الفصل الثاني فتطرقت الى الحماية الجنائية المقررة لمستخدمي الانترنيت و تناولت الحماية الجنائية للمعلومات و أهميتها (المبحث الأول) و التدابير الوقائية لحماية المعطيات في المجال المعلوماتي.

الفصل الأول

المفهوم العام لجرائم الأنترنت

المبحث الأول: ماهية جرائم الانترنت

تعتبر الجرائم الالكترونية احدى اخطر الأوجه السلبية التي نتجت عن التقدم السريع الذي مس جميع المجالات العلمية و الحياتية في عصرنا الحالي هذه الجرائم التي عانت منها الدول المتقدمة لذلك تنوعت أساليب ارتكاب جرائم الانترنت تنوعا كبيرا و ازداد عددها و شكلها لاستغلالها التقنيات الحديثة المتواجدة في الحاسب الالي و شبكات الانترنت حيث أدى التطور الملحوظ الذي شهدته هاته الجريمة في الآونة الأخيرة الى صعوبة مواجهتها و تعقد أساليب مكافحتها و لكي نستطيع إيجاد اليات مكافحة ناجحة لا بد من التعرف جيدا على هذه الظاهرة الاجرامية لذا فانه لا بد لنا من التطرق لبعض المفاهيم والمصطلحات التي تعد معرفتها بمثابة مدخل لموضوع الدراسة ولأجل دلك تم تقسيم هذا المبحث الى مطلبين.

المطلب الأول: الايطار المفاهيمي للجرائم الانترنت

جرائم الانترنت هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الإتصال الحديثة مثل الإنترنت.

تحدث الجرائم الالكترونية بهدف سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص، تتشابه جرائم الانترنت مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة، ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة، فجرائم الانترنت يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الإتصال الحديثة والشبكات المعلوماتية[1].

الفرع الأول: تعريف جرائم الانترنت

كانت هناك العديد من التعريفات والمتنوعة المتعلقة بجرائم الانترنت كظاهرة جديدة لا تزال قيد البحث والدراسة من قبل المتخصصين القانونيين والعديد من المهنيين القانونيين ، وبالمثل لا يوجد تعريف محدد ومتفق عليه لهذا النوع الجديد من الجرائم أو جرائم المعلومات التي تنطوي على التكنولوجيا. بينما يعتقد البعض الآخر أنها إساءة استخدام لتقنيات المعلومات والاتصالات.

1- نشناش منية، الركن المفترض في الجريمة المعلوماتية، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة المنظمة من قبل قسم الحقوق والحريات في الانظمة المقارنة، بكلية الحقوق والعلوم السياسية بجامعة بسكرة، يومي 16-17 نوفمبر 2015، ص12.

جرائم الانترنت. جرائم المستحدثة واستخدم الاخرون مصطلح تكنولوجيا المعلومات والاتصال من جهة أخرى اطلق عليها بعضهم جرائم المساس بأنظمة المعالجة الالية للمعطيات و هي التسمية التي اطلق عليها المشرع الجزائري في تعديل قانون العقوبات لسنة 2004 حيث أضاف فصلا ثالثا في القسم السابع مكرر و الذي شمل المواد من 394 مكرر الى 394مكرر 7ثم في سنة 2009 سماها الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و قد عرفها وزير الداخلية الفرنسي بانها*المصطلح المستخدم لوصف جميع الجرائم الجنائية التي ترتكب عبر شبكات الكمبيوتر و لا سيما على الانترنت و في تعريف اخر لها قيل *انهاكي فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الالية بقدر كبير لازما لارتكابه من ناحية و لملاحظته و تحقيقه من ناحية أخرى اعتبر أصحاب هذا التعريف ان الفعل غير المشروع يعد جريمة الكترونية اذا توفر على قدر كبير من العلم بتكنولوجيا الحاسبات الالية حتى ارتكابها و حين التحقيق فيها من جهة و حين ملاحقة مرتكبيها من جهة أخرى و لكن يؤخذ على هذا التعريف انه ضيق مفهوم جرائم الانترنت اذ ربطها بتوفر العلم بتكنولوجيا الحاسبات الالية لدى مرتكبيها دون ان يتوفر ذلك القدر الكبير من المعرفة بتكنولوجيا الحاسبات الالية لدى مرتكبيها و كمثال بسيط على ذلك اتل فالبيانات المخزنة داخل نظام الحاسب الالي هذا الفعل الذي يعتبر احد صور الاجرام المعلوماتي.

يمكن ارتكاب الجريمة في القوانين المختلفة من قبل أي شخص لديه خبرة قليلة مع أجهزة الكمبيوتر عن طريق تنزيل البرامج التي تساعدهم مثل الفيروسات التي تفسد البيانات الموجودة على الكمبيوتر.

اولا : التعريف القانوني للجرائم الانترنت:

المشرع الجزائري كغيره من التشريعات المقارنة لم يعطي تعريفا معينا للجريمة بل لم يستعمل مصطلح جرائم الانترنت او المعلوماتية او السيبرانية في القوانين التي سنها في هذا المجال إذا كانت الجرائم الالكترونية قبل تعديل قانون العقوبات الجزائري سنة 2004تصنف ضمن جرائم النظام العام كالسرقة، خيانة الأمانة، اختلاس وغيرها من الجرائم.

فالجرائم الالكترونية رغم خصوصيتها واختلافها عن الجرائم التقليدية الا انها كانت في غياب النص تلبس ثوب العقوبات المقررة لنظيرتها التقليدية.

وهو ذات الامر الذي حدث في المملكة الغربية[1]. قبل صدور القانون رقم 03-07القاضي بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الالية للمعطيات فقبل صدور هذا القانون كان هناك تضارب قضائي على مستوى محاكم الدار البيضاء قبل توحيدها فيما يخص سرقة المعطيات المعلوماتية بين اتجاهين .

الأول: يسندها لمقتضيات الفصل 505من ق.ع.م المتعلق بالسرقة.

الثاني: يطبق عليها مقتضيات الفصل 521 من نفس القانون والمتعلق باختلاس قوى كهربائية[2] وهو ما بين الدور البارز الذي كان يلعبه القضاة في معالجة جرائم الانترنت وفي تطوير القانون بصورة عامة قبل تدخل المشرع.

وفي سنة 2004اطلق عليها المشرع الجزائري تسمية جرائم المساس بأنظمة المعالجة الالية للمعطيات وذلك بمقتضى القانون رقم 04-15المعدل و المتمم لقانون العقوبات وهي ذات التسمية كما راينا في القانون الغربي من خلال القانون 03-07 اما في سنة 2009 عاد المشرع الجزائري وسماها *الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال *بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها اذ جاء في نص المادة2 فقرة ا منه ان :الجرائم المتصلة بتكنولوجيا الاعلام والاتصال جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام الاتصالات الكترونية .

من خلال التعريف السابق يتبين ان المشرع الجزائري قد وسع من تعريف جرائم الانترنت خاصة حين اعتبر بانها جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية ونحن نرى انه قد أحسن ما فعل لكي تدخل في دائرة التجريم أنواع جديدة أخرى من الجرائم الالكترونية والتي قد تكشف مستقبلا.

1- القانون رقم03-07 القاضي بتتميم مجموعة القانون الجنائي فيما يتعلق بالجزائر المتعلقة بنظم المعالجة الالية للمعطيات الصادر بتنفيذ الظهير الشريف رقم 197-03-1 بتاريخ 16رمضان1424 الموافق ل 11نوفمبر 2003 بالج. ر العدد 5171 بتاريخ 22ديسمبر 2003 الموافق ل 27 شوال 1424، ص4284.

2-هشام ملاطي، خصوصية القواعد الاجرائية للجريمة المعلوماتية –محاولة المقاربة –مدى ملائمة القانون الوطني مع المعايير الدولية –مطبعة الامنية بالرباط 2014ص76.

اما عن التشريعات العربية الأخرى فنجد بعضها اعطى تعريفا للجرائم الانترنت كما فعل كلا المشرع الكويتي والمشرع السعودي

فالمشرع الكويتي تطرق الى تعريفها في المادة 1 من قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 كما يلي: في تطبيق احكام هذا القانون يقصد بالمصطلحات التالية المعنى الموضح قرينا لكل منها .... الجريمة المعلوماتية كل فعل يرتكب من خلال استخدام الحاسب الالي او الشبكة المعلوماتية او غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هدا القانون[1] اما نظام مكافحة الجرائم المعلوماتية السعودي[2] فقد عرفها في الفقرة 8من المادة1 بانها: أي فعل يرتكب متضمنا استخدام الحاسب الالي او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام

ويمكننا القول ان المشرعين الكويتي والسعودي تقدما على التشريعات العربية الأخرى عندما عرفا جرائم الانترنت ذلك ان تعريفها يعد نقطة ارتكاز مهمة لتشريع محل البحث لما للجرائم الانترنت من أهمية كونها من الجرائم المستحدثة في العصر الحالي والتي تتطلب بيان مفهومها وتعريفها في صلب النصوص[3].

وبناءا على ما ذكر أعلاه يتضح لنا ان جرائم الانترنت لم تحظى بتعريف شامل او متفق عليه اذ ان وضع تعريف محدد لها امر ليس باليسير لذلك ذهب بعضهم الى القول بضرورة مراعاة عدة اعتبارات مهمة عند وضع تعريف لها منها:

- ان يكون التعريف مقبولا ومفهوما على المستوى العالمي
- ان يراعي التطور السريع والمتلاحق في تكنولوجيا المعلومات
- ان يحدد ذلك التعريف الدور الذي يقوم به جهاز الحاسب في إتمام النشاط الاجرامي
- ان يفرق التعريف بين الجريمة العادية وجرائم الانترنت وذلك عن طريق إيضاح الخصائص المميزة للجرائم الانترنت

1- قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015 الصادر يوم الاحد يوليو 2015 العدد 1244.

2- اقر نظام مكافحة الجرائم المعلوماتية السعودي مجلس الوزراء في جلسة الاسبوعية يوم الاثنين 1428/03/07 هـ الموافق 2007/03/26 وصدر بموجب المرسوم الملكي رقم (م/17) بتاريخ 8-3-1428 هـ القانون موجود على الموقع الإلكتروني للجريدة الرسمية للمملكة العربية السعودية .

تم الاطلاع عليه يوم 2009/12/16 https:/www.upn.go.govsa

3- لورنس سعيد الحوامدة، الجريمة المعلوماتية اركانها والية مكافحتها دراسة تحليلية مقارنة مجلة الميزان للدراسات الاسلامية والقانونية 2007 ص، 09.

المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة المعلوماتية اولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني وثانيهما معيار موضوع الجريمة المساس بأنظمة المعالجة الالية للمعطيات وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات

كما اعتمد المشرع على معيار رابع في تحديد نطاق الجريمة المعلوماتية كونه اقر ان الجريمة المعلوماتية ترتكب في نظام معلوماتي او يسهل ارتكابها عليه وهذا ما يوسع من نطاق مجال الجرائم المعلوماتية في القانون الجزائري.

حاول المشرع الجزائري اصدار قوانين عامة و خاصة و هياكل و أجهزة للتصدي للجرائم المعلوماتية و يعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الاعلام أدى الى اتساع نطاق الجريمة المعلوماتية فهي أصبحت لا تقتصر على جريمة واحدة انما اتسعت الى عدة جرائم و من جهة أخرى كون القانون الجنائي التقليدي غير قادر على استعاب الجرائم المعلوماتية الحديثة إضافة الى ذلك المحافظة على مبدا الشرعية الجنائية متكلا على تعزيز التعاون بين الجهات القانونية و الخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها

و تجد الإشارة الى ان المشرع الجزائري لم يعرف جرائم الانترنت في القانون 04-15 المؤرخ في 10-11-2004 المعدل و المتمم لقانون العقوبات بل عدد الجرائم الماسة بأنظمة المعالجة الالية للمعطيات و التي تعتبر جزء من ظاهرة إجرامية حديثة و خطيرة تسمى الجريمة المعلوماتية و اكتفى بالعقاب عليها في الكتاب الثالث المعنون بالجنايات و الجنح و عقوباتها في الفصل الثالث المعنون بالجنايات و الجنح ضد الأموال و في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات في المواد394مكرر الى غاية المادة 394مكرر7.

ثانيا : التعريف الفقهي للجرائم الانترنت:

يمكن القول انه من الصعوبة الاتفاق على تعريف موحد جامع مانع لهذه الجريمة وذلك راجع الى التطور المتلاحق الذي تمر به وتنوع واختلاف وسائل ارتكابها وظهور اشكال جديدة مستحدثة إضافة الى اختلاف الزاوية التي ينظر من خلالها من يحاول تعريفها.

ثالثا : تعريفات ركزت حول وسيلة ارتكاب الجريمة[1]:

نجد الفقهان الالمانيين tiedeman-carle Benson عرف الجريمة المعلوماتية على انها: *كل اشكال السلوك غير المشروع-او الضار بالمجتمع الذي يرتكب باستخدام الحاسوب وانها فعل اجرامي يستخدم الحاسوب في ارتكابها كأداة رئيسة

رابعا : تعريفات ركزت حول موضوع الجريمة: [2]

أنصار هذا الاتجاه الفقيه ROSANPLATI الذي عرفها *انه نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه

-كما عرفت الدكتورة هدى قشقوش جرائم الانترنت بانها: *كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات

التعريف المسند الى وجوب المام الفاعل بتقنية المعلومات:

عرفها DAVID THOMSON بانها: *اية جريمة يكون متطلبا لاقترافها ان تتوفر لدى فاعلها معرفة تقنية الحاسب اذ يرى ان تعريف هذه الجريمة يجب ان يسند الى معيار شخصي اذ على الفاعل ان يكون ملما بتقنية المعلومات [3].

التعريف المسند الى معايير مختلفة:

لقد اختلف هذا الاتجاه في المعايير المتبناة في تعريفه للجريمة المعلوماتية بعيدا عن المعايير السابقة اذ عرفها الفقيه الفرنسي الأستاذ MASSA ان الجريمة المعلوماتية هي: *الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح

وتعريف اخر للخبير الأمريكي PARKER-D الذي قال: انها فعل اجرامي أيا كانت صلته بتقنية المعلومات فيه بتكبد المجني عليه ونتيجة له خسارة ويحقق الفاعل ربحا عمديا.

1- رضا قولي عثمان، المشكلات العلمية والقانونية للجريمة المعلوماتية في العصر الرقمي http://www.al-fadjr.com/ar/realite/3531.html 20نوفمبر 2020 الساعة 11:25 .

2-لعقال فريال الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر ، قانون جنائي ، جامعة اكلي محند اولحاج البويرة سنة 2015، ص 7.

3- معاشي سميرة مفهوم الجريمة المعلوماتية –دراسة تحليلية-جامعة مُحَّد خيضر بسكرة، مجلة المفكر العدد 17 ، 2018، ص402.

ويرى يونس عرب ان جرائم الكمبيوتر تعرف انها: *الأفعال غير المشروعة المرتبطة بنظم الحواسب وانه سلوك غير مشروع معاقب عليه قانون صادر عن إدارة جرمية محلها معطيات الكمبيوتر

اما الأستاذ عبد الفتاح بيومي الحجازي انها: *نشاط اجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة او غير مباشرة كوسيلة او كهدف لتنفيذ الفعل الاجرامي المقصود[2]

الفرع الثاني : التعريف الواسع و الضيق لجرائم الانترنت

اولا : الإتجاه الضيق للجرائم الانترنت.

يعرف أنصار هذا الإتجاه جرائم الانترنت ،"كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته و تحقيقه من ناحية أخرى."[1] حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها. وهذا التعريف يضيق بدرجة كبيرة من جرائم الانترنت، بمعنى يجب أن يتوافر قدر كبير من العلم ذه التكنولوجيا لدى الجناة ،والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أ ا "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية." كما يرى الأستاذ tredmann أن الجريمة المعلوماتيةتشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[2].

ويرى الاستاذ rosenblatt بأن جرائم الانترنت هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه"[3].

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكا ا تخرج من نطاق التجريم.ويرى الأستاذ باركار أن جرائم الانترنت هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق با ني عليه أو كسب يحققه الفاعل[4].

1حمزة بن عقون ،**السلوك الإجرامي للمجرم المعلوماتي**، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة ،2012/2011، ص 13، نقلا عن قورة نائلة، جرائم الحاسب الإقتصادية، القاهرة ،2004، ص21.

2حمزة بن عقون، الرسالة السابقة الذكر، ص14، نقلا عن أحمد هلالي عبد اللاه، ص13.

3حمزة بن عقون ،نفس الرسالة، ص14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية، ص213.

4محمد أمين أحمد الشوابكة ،**جرائم الحاسوب والأنترنت**، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن ،2004، ط 1، ص 8 – 9.

الثانيا: الإتجاه الواسع للجرائم الانترنت .

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية، دف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب[1].

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر ا لس الأوروبي بقيام المخالفة (الجريمة) في كلحالة يتم فيها تغيير معطيات، أو بيانات، أو برامج، أو محوها، أوكتابتها، أو أي تدخل آخر فيمجال إنجاز البيانات، أو معالجتها, وتبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر[2].

ودائما حسب أنصار هذا الإتجاه يرى البعض أن جرائم الانترنت هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حياز ا، أو توزيعها بصورة غير مشروعة[3]. أما البعض من الفقهاء يعرفو ا بأ ا كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي و شبكة الأنترنت) بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف[4].

1سميرة بيطام،**الجريمة الإلكترونية وتقنية الإجرام المستحدث**ص04/01 .

culture/net.alukah.www//http/br 2016/11/ 30 ، 20h30.

2مليكة عطوي، ا لة السابقة الذكر، ص 09، نقلا عن الطاهر روابنية، المسائلة، مقال، العدد 01، 1991، ص 15.

3كامل فريد السالك ،**الجريمة المعلوماتية**، ندوة التنمية ومجتمع المعلوماتية، حلب ،23/21/تشرين الأول ،2000، بدون صفحة.

4صغير يوسف ،**الجريمة المرتكبة عبر الأنترنت**، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال ،جامعة مولود معمري، تيزي وزو ،2013/03/06، ص09، نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها مجلةصادرة عن مديرية الأمن الوطني، العدد84، 2007، ص 51.

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف جرائم الانترنت على سلوك الفاعل رد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة،كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا نكون أمام جريمة إلكترونية ،كمن يقوم بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك. أما بالنسبة للتعريف القانوني للجرائم الانترنت فقد اصطلح المشرع الجزائري على تسميتهابمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب أحكام المادة 02 منالقانون رقم 09 -04 [1] على أ ا: "جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكا ا عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية."

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الألية للمعطيات،كما بينها في قانون العقوبات[2] من المادة 394 مكرر إلى 394 مكرر 07، وترك ا ال واسع لإي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق جرائم الانترنت بمجرد أن ترتكب الجريمة، أو يسهل ارتكا ا عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[3].ومن أمثلة جرائم الانترنت المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية[4].

1القانون رقم 09 -04، الصادر في 05أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر العدد 47.

2القانون رقم ،04 -15، الصادر في 10 نوفمبر2004، يعدل ويتمم الأمر رقم156/66، الصادر في 08جوان 1966، المتضمن قانون العقوبات، ج رالعدد 71.

3سوير سفيان ،**جرائم المعلوماتية**، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة ابوبكر بلقايد، تلمسان ،2010 -2011، ص من 14 إلى 16.

4جازية سليماني، موقع العربي الجديد،تاريخ الدخول2017/02/09،الساعة

20htt//www.alaraby.co.uk/media news.30h

المطلب الثاني: خصائص و اركان جرائم الانترنت

الفرع الأول: خصائص جرائم الانترنت

تتميز جرائم الانترنت بطبيعة خاصة تميزها عن الجريمة التقليدية ولذا اتصفت بعدة صفات وحقائق سواء تعلق الامر بمرتكبيها او ما يسمى بالمجرم المعلوماتي او بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي وسوف نبين هذه الخصائص التي ميزت الجريمة المرتكبة عبر الانترنت عن غيرها بداية بانها جريمة عابرة للحدود الدولية وصعبة الاكتشاف والاثبات وبانها جريمة خفية ومستمرة وخصوصية الجاني المرتكب لهذه الجريمة[1]

أولا: وجود الحاسب الالي

ان الحاسب الالي يعتبر من المتطلبات الرئيسية لارتكاب جرائم الحاسب حتى تعتبر كذلك، إضافة الى ما سبق فإن هذه الجرائم تتطلب الماما كافيا، بمهارات ومعارف فنية، كالمعرفة التقنية بالحاسب الالي وكيفية تشغيليه واستخدامه و هذا ما تؤكده الدراسات و الإحصاءات التي تناولت الموضوع ، و ذلك ان مقترفي هذه الجرائم هم من المتخصصين في معالجة المعلومات اليا.

ثانيا: الجرائم الالكترونية عابرة للحدود الدولية

تتسم جرائم الانترنت غالبا بالطابع الدولي ذلك لان الطابع العالمي لشبكة الانترنت و ما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخطONLI NE يسهل ارتكاب الجريمة من دولة الى دولة أخرى فجرائم الانترنت لا تعترف بالحدود بين الدول و القارات لذلك فهي جريمة عابرة للقارات فهي تعتبر شكلا جديدا من اشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة اذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل :جرائم التعدي على قواعد البيانات و تزوير و اتلاف المستندات الالكترونية و الاحتيال المعلوماتي و سرقة بطاقات الائتمان و القرصنة و غسيل الأموال .

وتشير خاصية عالمية الحدود للجرائم الانترنت عدة اثار قانونية أهمها القانون الواجب التطبيق عليها والقضاء المختص بيها فهل هو قانون الدولة التي وقع فيها النشاط الاجرامي ام الدولة التي يقيم فيها الجاني

1- رضا قولي عثمان، المشكلات العلمية و القانونية للجريمة المعلوماتية في العصر الرقمي http://www.al-fadjr.com/ar/realite/3531.html، 20نوفمبر 2020 الساعة 11:25.

2-نمديلي رحمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، كلية الحقوق والعلوم السياسية -جامعة محمد لمين دباغين سطيف الجزائر 2، كتاب اعمال مؤتمر الجرائم الالكترونية طرابلس لبنان يومي 24و25 مارس 2017، ص95.

او الدولة التي أضر بمصالحها هذا التلاعب لذا بات من الضروري إيجاد الوسائل المثالية لتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق ابرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة لمكافحة هذا النوع من الجرائم.

وتجدر الإشارة ان المشرع الجزائري قد خطى خطوة الى الامام في هذا المجال بصدور القانون رقم 04-15 المعدل والمتمم للأمر رقم66-156 المتضمن قانون العقوبات والذي استحدث بموجبه احكام خاصة بالجرائم الماسة بالأنظمة المعلوماتية من المادة 394مكرر الى غاية المادة394مكرر 7من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الالية للمعطيات إضافة الى القانون رقم 09-04 السابق الذكر.

المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال هذه الجرائم كما أنشئت هيئة وطنية للوقاية من الاجرام المتصل بتكنولوجيا الاعلام والاتصال ومكافحته وبين احكام خاصة بتعاون والمساعدة القضائية الدولية ولا تتطلب جرائم المعلومات عنفا لتنفيذها في تنفيذ بأقل جهد مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود الذي يكون في صورة ممارسة العنف والايذاء كما هو الحال في جريمة القتل او الاختطاف او الخلع[1].

وعلى هذا الأساس كل ما احتاج اليه هو عامل من الخبرة والذكاء والقدرة على التعامل مع جهاز الحاسوب بالمستوى التقني.

ان البيئة الافتراضية لا تعترف بالقيود ولا الحدود فالجريمة المعلوماتية جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت وتقنية المعلومات فغالبا ما يكون الجاني في بلد والمجني عليه في بلد اخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه وهي الجرائم لا يتواجد الفاعل على مسرح الجريمة بل يرتكبها عن بعد أي عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة

ويثير الطابع الدولي لهذه الجريمة عدة إشكاليات وصعوبات قانونية لاسيما مشكلة تحديد المحكمة صاحبة الاختصاص القضائي. ادلة الاثبات وقبولها امام القضاء دولة أخرى وكذا القانون الواجب التطبيق بالإضافة الى إشكاليات تتعلق بإجراءات الملاحقة القضائية لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق ابرام اتفاقيات دولية خاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

– 1-بعيش تمام شوقي، كتاب الجريمة المعلوماتية، دراسة تأصيلية مقارنة، جامعة مُحَّد خيضر، كلية الحقوق والعلوم السياسية مخبر اثر الاجتهاد القضائي على حركة التشريع سنة2019، ص 28.

ثالثا: الجرائم الالكترونية صعبة الاكتشاف والاثبات:[1]

من اهم خصائص جرائم الانترنت انها صعبة الاكتشاف والاثبات لأسباب ترجع الى الجاني او المجني عليه والى وسيلة تنفيذها حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الانترنت أضف الى ان الجاني *المجرم المعلوماتي *كما اسلفا الذكر مجرم معترف ذكي مثقفا لا يترك اثار جانبية خارجية للجريمة مما يصعب اثباتها كما ان المجني عليهم وهم غالبا مؤسسات عامة او خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة الى السمعة وهز الثقة فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية.

فاذا كانت الجريمة التقليدية تمتاز بكونها تترك خلفها اثارا خاصة مرئية كالجثث او الدماء المسفوكة فانا ذلك غير متوافر في ايطار الجريمة كونها ترتكز على تغيير او تعديل او مسح البيانات كليا او جزئيا بالدخول الى السجلات المخزنة في ذاكرة الحاسب الالي الامر الذي يجعل إمكانية اكتشافها في غاية الصعوبة وبالتالي الصعوبة في توقيع الجزاء على مرتكبيها وهذا النوع من الجرائم لا يترك اثرا خارجيا ومرئيا نتيجة ارتكابها في الخفاء.

وهي أيضا صعوبة متابعتها واكتشافها بحيث لا تترك اثرا فهي مجرد ارقام تتغير في السجلات فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها ويلاحظ ان الجرائم التي تكتشف هي أكثر بكثير من تلك التي تم اكتشافها على أساس انها تفتقر الى الدليل خاصة يتعذر على المحقق التقليدي من لها او التعامل معها لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل به من برامج او وضع كلمات سرية ورموز تعوق الوصول الى الدليل وقد يلجا مرتكبيها لتشفير التعليمات لمنع إيجاد أي دليل يدينه[2].

رابعا: خفاء الجريمة وسرعة التطور في ارتكابها:

تتسم الجرائم الناشئة عنها استخدام الانترنت بانها خفية ومستمرة في اغلبها لان الضحية لا يلاحظها رغم انها قد تقع اثناء وجوده على الشبكة لان الجاني يتمتع بقدرات فنية تمكن من جريمته بدقة مثلا ارسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة او اتلافها والتجسس وسرعة المكالمات وغيرها من الجرائم

1-سوبر سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلوم الاجرام، كلية الحقوق، جامعة ابو بكر بالقايد، تلمسان، 2010-، ص12.

2- محمد زكي ابو عامر، علي عبد القادر، قانون العقوبات ،، القسم الخاص، (د ط)، دار النهضة العربية، القاهرة، 1993، ص9.

و جرائم الانترنت في اكثر صورها خفية لا يلاحظها المجني عليه او لا يدري حتى بوقوعها و امعان الجاني في حجم السلوك المكون لها و اخفاءه بطريق التلاعب غير المرئي في النبهات او الذبذبات الالكترونية التي تسجل البيانات عن طريقها امر ليس في الكثير من الأحوال اثباته بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها يستفيد المجرمون في مختلف المواقع من الشبكة في تبادل الأفكار و الخبرات الاجرامية فيما بينهم و يظهر لنا ذلك جليا في مختلف المواقع الالكترونية و المنتديات القراصنة التي تتضمن الانتقال فيما بينهم من اجل تبادل المعارف و الخبرات في مجال القرصنة و ذلك اجل ارتكابهم لجرائمهم بعيد عن اعين الامن.

تجدر الإشارة في هذا الصدد ان الجريمة المرتكبة عبر الانترنت أسرع تطورا من التشريعات وذلك راجع الى التطور التكنولوجي الهائل والمشارع الذي تجسده شبكة الانترنت بإضافة الى مختلف المؤتمرات التي يعقدها القراصنة تسمح لهم بابتكار وسائل وطرق في غاية التعقيد لم تعرفها التشريعات من قبل وذلك من اجل ارتكابهم لجرائمهم ومعظم مرتكبي الجرائم يختفون تحت اسماء وهمية مستعارة خشية ملاحقتهم عند تسجيل بياناتهم الشخصية للحصول على بريد الكتروني او الدخول الى مواقع[1].

خامسا: جرائم ناعمة

إذا كانت الجريمة التقليدية تحتاج الى مجهود عقلي في ارتكابها كالقتل، السرقة وغيرها.... فالجرائم الالكترونية لا تتطلب أدنى مجهود عقلي ممكن بل تعتمد على المجهود الذهني المحكم والتفكير العلمي المدروس القائم على المعرفة التقنية الممتازة بالحاسب الالي والتعامل السليم بالشبكة على أساس ان الجاني في الجرائم الالكترونية هو انسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو او لمجرد اظهار تفوقه على الة الكمبيوتر او على البرامج التي يشغل بها واكيد لتحقيق مصلحة ما.

ان الطبيعة الخاصة لهذه الجريمة تبرز بصورة واضحة في أسلوب ارتكابها فالجريمة المعلوماتية جريمة هادئة تقع بمجرد الدوس على ازرار لوحة المفاتيح[2].

سادسا: عدم التبليغ

عند وقوع الجريمة بواسطة الانترنت نجد ان بعض المجني عليهم يمتنعون عن ابلاغ السلطات المختصة خشية على السمعة والمكانة وعدم اهتزاز الثقة في كفاءتهم خاصة إذا

1- وهذا ما جسده القانون رقم09-04 في الفصل السادس.

2-عبد الفتاح مراد، شرح التحقيق الفني والبحث الجنائي، (د ط) الكتب والوثائق المصرية، 2006، ص46.

كان الكيان او هيئة معينة وقد اقترح في *الولايات المتحدة الامريكية*بان تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عمة يقع عليها من جرائم متى وصل الى علمهم ذلك مع تقرير جزاء في حالة اخلالهم بهذا الالتزام.

الفرع الثاني : أركان جرائم الانترنت.

1- الركن المادي للجرائم الانترنت:

تنهض الجريمة على ركنين رئيسيين هما الركن المادي والركن المعنوي، فلا بد للجريمة المعلوماتية إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها ،ولا بد أويضا من ركن معنوي يعبر عن إرادة المجرم المعلوماتي.

- **الركن المادي:**

لابد من فعل أوو إمتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أوفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصرالجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أوو تهديد أوو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر ، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أون هناك أونواعا من السلوك يتطلب التمييز بينها وبين سابقتها ، وهذا ما يدعو للتدخل التشريعي[1].

يتكون الركن المادي للجرائم الانترنت من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أونه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها،)مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الإ أونه لا مناص من معاقبة الفاعل.(

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب)مثلا : جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أوو المحررات الإلكترونية[2].

بن غدفة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأوة على صفحات الأنترنات وطرق محاربتها ،أوعمال الملتقى الوطني، ''آليات مكافحة الجرائم الالكترونية في التشريع الجزائري''، الجزائر ،29مارس 2017، ص 48 1.

فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية »،طرابلس، بتاريخ 24-25 مارس 2017، ص 1182

- **الركن المعنوي للجرائم الانترنت:**

تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام)العلم، والإرادة(لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أون يسبقه القصد العام ،أوما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أوو إرتكاب الجريمة[1].

يتكون الركن المعنوي للجرائم الانترنت من عنصرين هما العلم والإردة.

- العلم: هو إدراك الفاعل للأمور.
- أوما الإرادة: فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا، القصد الجنائي العام: هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود إرتكاب الفعل.

أوما القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بإرتكابه 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 جرائم الانترنت؟

الأصل إن الفاعل في جرائم الانترنت يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أوو 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 الإلكترونية دون أوي استثناء ولكن هذا لا يمنع أون بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص)مثلا: جرائم تشويه السمعة عبر الأنترانت، وجرائم نشر الفيروسات عبر الشبكة(. وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاسي[2].

ويرى الباحث أون القصد العام والخاص في جرائم المعلوماتية هو أساسي لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أوو النية الخاصة للجاني والتي يمكن استشفائها من مكونات كل جريمة على حدا وبشكل مستقل، وبالتالي فإن الجرائم

1لورنس سعيد الحوامدة، ''الجرائم المعلوماتية أوركانها وآلية مكافحتها'' دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن ،2016/08/13، ص24.

2فضيلة عاقلي ، مرجع سابق، ص 120.

المعلوماتية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة ولا يتصور قيام أوي نوع من أونواع الجرائم المعلوماتية دون وجود الركن المعنوي.

أوما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا، والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات وتمحيصها بما لها من صلاحية بإعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أومامها [1].

1 لورنس سعيد الحوامدة، مرجع سابق، ص 25-26.

المبحث الثاني : أنواع و دوافع جرائم الانترنت

المطلب الاول : أنواع جرائم الانترنت:

تنقسم جرائم الانترنت الى[1]:

الفرع الاول : جريمة التخريب ونقل الأموال الالكترونية : وهي بدورها تنقسم الى:

1/**جريمة اتلاف معطيات الحاسوب او تخريبها:** والمفهوم منه هو التدمير أو التخريب الذي يحدث على البيانات والمعلومات وبرامج الحاسوب على الكيان المادي ذاته ، ولا يشكل هذا الجانب أي صعوبة في تحديد الجريمة ووسائل حمايتها ، فجدولان هما:- تم مسح المعلومات بالكامل وتدميرها إلكترونيًا- المعلومات أو البرامج الفاسدة بحيث تصبح غير قابلة للاستخدام

2/**الجرائم المصرفية:** ** تحويل الأموال * يرتكب جرائم الكمبيوتر ضررًا من قبل أفراد يتمتعون بخبرة طويلة ومعرفة في التعامل مع هذه الأجهزة المتقدمة. هذه الجريمة * الانتهاك * ترتكب في الغالب لأسباب شخصية أو سياسية أو اقتصادية ، حيث يدخل المجرمون عن علم إلى بنك ويحولون الأموال من حسابات إلى حسابات أخرى ، وهي أصعب جريمة ، وأقسى جريمة هناك ، لأنها بغض النظر عن الحدود ، المكان أو الزمان. تكمن الصعوبة الأكبر في المخاطرة بانتشار هذا النوع من الجرائم في صعوبة العثور على الجاني.في كثير من الحالات ، يكتشف الشخص الحاصل على تأشيرة دخول من دولة ما أن البطاقة تستخدم لشراء سلع في متجر في دولة أخرى ، بينما الجاني في دولة ثالثة ، وتحدث الواقعة على موقع متجر البائع. على شبكة الويب العالمية .[2]

ثانيا: جرائم الحاسوب والانترنت:

1/**جرائم التزييف والتزوير:**

يعاقب تزييف النقود والجرائم الأخرى ذات الصلة على ما يلحقه من ضرر بالمواطنين في أنشطتهم اليومية وآثاره المدمرة على الاستقرار والسلام الاقتصادي ، ويشكل اعتداءً مباشرًا على سيادة دولة وحق في الصميم. حذر المسئولين من هذه الظاهرة التي اجتاحت المجتمعات البشرية منذ أن عرف الإنسان المال كوسيط للتبادل. أصبح التقليد منتشرًا بشكل خطير في العصر الحديث ، سهولة وسرعة النقل والحدود بين الدول.

1-نزلي بشرى ، اثبات الجريمة الالكترونية ، مذكرة ماستر ، جامعة ورقلة ،كلية الحقوق و العلوم السياسية ، 2018، ص10

- نزلي بشرى ، اثبات الجريمة الالكترونية ،مرجع سابق، ص11. 2

2/النسخ غير المرخص للمصنفات الرقمية:

هناك بعض الظواهر السلبية التي ظهرت على الإنترنت مثل: ب:

أ- تسهيل الدعارة ، ونشر المواد الإباحية ، ونشر بعض القيم السلبية ، وما إلى ذلك. من خلال محاكاة الجريمة وإبرازها ، يكون الحدث المنحرف جاهزًا للرد على أي حدث خارجي. التأثير الذي يؤدي إلى الميل الداخلي والميل للانحراف ،، وبالتالي يوفر الإنترنت مادة خصبة للمواد الإباحية ، وصور الخلفية ، والمراسلات مع الأقران التي تنتهك الميول الأخلاقية ، حيث تملأ الإنترنت المساحة الواسعة بالفضائح بجميع أنواعها. أو تشويه سمعة شخص دون استشارة قانونية 16.000.000 دولار سنويا من جراء القرصنة والتداول غير المشروع لمنتجاتها

3/جرائم الكترونية أخرى:

تتعدد وتتنوع الجرائم الالكترونية مما لا يسعنا لذكرها بالتفصيل لذا سنورد بعض منها بالإيجاز:[1]

1-انشاء المواقع السياسية والدينية المعادية.

2-انشاء المواقع المعادية للأشخاص او الجهات السياسية او الفكرية

3-جرائم القرصنة

4-جرائم التجسس الالكتروني

5-الإرهاب الالكتروني: يقوم به الارهابيون بإنشاء وتصميم مواقع لهم على شبكة الانترنت لنشر أفكارهم والدعوة الى مبادئهم

6-جرائم الجنسية والممارسة الغير أخلاقية

7-الجرائم المنظمة عبر الانترنت تتمثل في تجارة المخدرات وغسيل الأموال، السطو على أموال البنوك وقيادة الجماعات عن بعد[2].

1- العربي قندوز واخؤون، جرائم الحاسوب، مذكرة مقدمة للتخرج دفعة الاثنية لمفتشي الشرطة، مدرسة الشرطة طيبي العربي، سيدي بلعباس، الجزائر، 2008، ص 25 وما بعدها.

2-عادل عية الجواد، الانترنت والاجرام، المنظم، مجلة الامن والحياة، العدد 303، 26 سبتمبر 2007ص 30-32.

الفرع الثاني : جرائم الانترنت المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص ،الجريمة الواقعة على النظم المعلوماتية الآخرى، الجريمة الواقعة على الأسرار[1]، وسأوضح كل نوع منها في البنود الآتية.

أولا: جرائم الانترنت الواقعة على الأشخاص الطبيعية.

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعةعلى حرمة الحياة الخاصة.

1 – جرائم الانترنت الواقعة على حقوق الملكية الفكرية.

يكون النظام المعلوماتي وسيلة للإعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الإختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع.وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 03 –05 الصادر في 2003، المتعلق بحقوق المؤلف والحقوق ا اورة، والأمر رقم 03– 07 الصادر في 2003 المتعلق ببراءات الإختراع.[2]

2 – جرائم الانترنت الواقعة على حرمة الحياة الخاصة.

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الإعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

1سوير سفيانن ، ص 33.

2سوير سفيانص34 – 35.

ثانيا: جرائم الانترنت الواقعة على النظم المعلوماتية الآخرى.

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الآخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية.

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الإستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة ،أو استخدام شاشة النظام، أو الإطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الإئتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الإئتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة إئتمانية إنتهت مدة صلاحيتها أو تم إلغاؤها، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة إئتمانية للحصول على السلع والخدمات.[1] البند الثالث: جرائم الانترنت الواقعة على الأسرار.

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين ،الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[2]، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والإقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات[3]، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية ،

والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أوبيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحا ا من أجل القيام بعمل أو الإمتناع عن القيام بعمل.[4]

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة61 إلى المادة 96 مكرر من قانون العقوبات ،بالإضافة إلى المادة394

1سوير سفيان، رسالة الماجستير السابقة الذكر، ص 35 – 36 –37.

2سوير سفيان، نفس الرسالة، ص 38.

3صغير يوسف ، ص 54.

4سوير سفيان، رسالة الماجستير السابقة الذكر، ص 38.

مكرر 03 التي تنص على: " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد." [1]

المطلب الثاني : دوافع ارتكاب جرائم الانترنت.

من خلال ما سبق يتضح لنا، أن الجريمة التقليدية والمجرم التقليدي يختلفان تماما عن جرائم الانترنت والمجرم الإلكتروني، لذا من الطبيعي أن نجد نفس الإختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع(الباعث)، الغرض، الغاية، مفاهيم لكل منها دلالته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الإستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإ ا من حيث الدلالة تتمايز، ف الدافع هو العامل المح رك للإرادة والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غايةمعينة، وهو يختلف من جريمة إلى أخرى. أما الغرض فهو الهدف الفوري المباشر للسلوكالإجرامي، ويتمثل بتحقيق النتيجة التي اصرف إليها القصد الجنائي أو الإعتداء على الحق الذي يحميه قانون العقوبات. وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الإنتقام، أو سلب مال المجني عليه في جريمة القتل.

وبالنسبة للجرائم الانترنت، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الإعتداء المختلفة المنطوية تحت هذا المفهوم[2]، وأهم هذه الدوافع سيتم ابيانها من خلال الفرعين الأتيين.

الفرع الأول: الدوافع الشخصية لارتكاب جرائم الانترنت.

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب جرائم الانترنت، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين.

1الأمر رقم 04 -15، القانون السابق الذكر .

2 حمزة بن عقون، 46 - 47.

الأول: الدوافع المادية.

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف جرائم الانترنت، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أواختراق نظم المعالجة الألية لها من خلال اكتشافه الفجوا الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة " securite informatique" وهي مجلة متخصصة في الأمنالمعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال ،و23% من أجل سرقة معلومات، و19% أفعال إتلاف، و15% الإستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها ا رم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشار كة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن جرائم الانترنت، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت م خسائر مادية جراء هذه الإعتداءات.[1]

ثانيا: الدوافع الذهنية لارتكاب جرائم الانترنت.

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي و إثبات الذات.

وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختر اق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة ذالأنظمة قد يشكل متعة كبيرة لمرتكبيها

1سعيداني نعيم ،**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ،2012 -2013، ص60- 61، نقلا عن لا عبدالقادر المومني، الجرائم المعلوماتية، ط02، 2010،ص 90، ونقلا عن ضاح محمود الحمود ونشأت مفضي ا الي، جرائم الأنثرنت، دارالمنار للنشر والتوزيع ،2005، ص 31.

وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها ، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي و إثبات المقدرة.[1]

الفرع الثاني: الدوافع الموضوعية لارتكاب جرائم الانترنت.

قد يتأثرالمجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال البندين المواليين.

الأولا: دافع الإنتقام وإلحاق الضرر برب العمل.

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[2]، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الإنتقام من رب العمل، ومثال ذلك أن الإنتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

ثانيا: دافع التعاون والتواطؤ.

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أي ان يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أوخارج المؤسسة الجاني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة مايمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[3].

1سعيداني نعيم ،رسالة الماجستير السابقة الذكر، ص 61 – 62.

2 صغير يوسف، 42.

3سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص62.

وإذا كانت هذه أبرز الدوافع لارتكاب جرائم الانترنت، مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب جرائم الانترنت قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازا للقيام بعملية الإبتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.[1]

1 سعيداني نعيم ،نفس الرسالة، ص 62.

الفصل الثاني:

ا

لحماية الجنائية المقررة لجرائم الانترنت

المبحث الأول: الحماية الجنائية للمعلومات وأهميتها .

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى، استوجب ذلك توفير حماية جنائية خاصة

فما المقصود بالحماية الجنائية للمعلومات؟ وفيما تكمن هذه الحماية؟ هذا ما سوف نتعرض له في هذا المبحث وذلك على النحو التالي:

- المطلب الأول: ضرورة الحماية الجنائية للمعلومات
- المطلب الثاني: الحماية الجنائية للمعلومات في النظم لمقارنة

المطلب الأول: ضرورة الحماية الجنائية للمعلومات

تجد المعلومات نفسها لها قيمة غير ملموسة واردة بداخلها، وبهذا المعنى، تنتقل المعلومات من مجرد معرفة إلى تطبيق المعرفة..

تم إنشاء المعلومات ماليًا وبالتالي تم تضمينها في أرقام رأس المال المالي. يمكن أن تكون المعلومات شخصية، كما أن إفشاءها يهدد الخصوصية بعدة طرق. بالنظر إلى التطور السريع للتكنولوجيا وتكنولوجيا المعلومات الذي تميز بظهور الإنترنت، فإن الدراسات الجنائية تطبق النصوص التقليدية على الجرائم الجديدة، مع الأخذ في الاعتبار التطور الكبير في معالجة المعلومات وأنظمة نقلها من خلال الشبكات، مما يشير إلى أن ذلك غير مناسب. وهناك حاجة لتطوير قواعد قانونية مهمة للتعامل مع هذه الجرائم. ابتكار.1

عند تحديد الحماية الجنائية للمعلومات، يجب النظر في التغييرات الجديدة التي أحدثتها ثورة المعلومات في طبيعتها، لا سيما فيما يتعلق بمسألة آثارها المتطورة. لا يمكن تحقيق ذلك بالكامل إلا عند التعامل مع المعلومات في سياق المعالجة الآلية.2

ويجب أن تستند الحماية للمعلومات على منطق التعامل التشريعي في إطار قانون المعلوماتية.

لقد سهلت تقنية الاتصالات الإلكترونية هذه تسهيل الاتصال والمعاملات بين الناس، وأتاح استخدامها تطوير مجالات مثل تقديم خدمات الرعاية الصحية والملكية الفكرية. شبكات المعلومات وأنظمة تبادل البيانات الإلكترونية هي تطبيقات لاستخدام التكنولوجيا الحديثة في مجال الاتصالات ونقل المعلومات،

1الدكتور أحمد خليفة الملط، مرجع سبق ذكره، ص.109-110.

2د .حسام الدين الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم الاقتصادية، كلية الحقوق، جامعة عين شمس ،بحث مقدم إلى مؤتمر القانون والحاسب الآلي في الكويت، نوفمبر 1989، ص.142.

وهي تختلف بشكل كبير عن وسائل الاتصال والمعلومات التقليدية الأخرى. يضع الإطار العام لهذه الاستخدامات، لكن احتمالية إساءة استخدام هذه التكنولوجيا واستخدامها يهدد السلامة العامة والمصالح الوطنية. يصبح استخدامها ممكنًا عندما تسمح وسائل الاتصال الإلكتروني الحديثة بإتمام المعاملات المالية بسرعة وبشكل موثوق، بغض النظر عن موقع التاجر. قد يسيء بعض المجرمين استخدام هذه الأدوات لارتكاب عمليات احتيال أو ارتكاب جرائم تنتهك خصوصية التجار وأسرارهم التجارية، لذا فهم لا يخلون من المخاطر. وإذا كان للتقدم التكنولوجي محاولة مكافحة الجريمة في مجال الاتصالات واللجوء إلى تشفير الجريمة بطريقة تحافظ على سريتها. ومع ذلك، أدت هذه العمليات إلى قيام الجناة بإساءة استخدام هذه العمليات لارتكاب جرائم من خلال التسلل إلى المحتوى واستخدام وسائل الاتصال التي يصعب فهم محتواها. وهذا يعني أن التقدم التكنولوجي قد زود المجرمين بوسائل قوية وفعالة للغاية لتنفيذ جرائمهم .

من ناحية أخرى، تعتبر المعلومات الإلكترونية ذات صلة بالأنظمة الإدارية والتجارية والمالية الهامة التي تغطي كل من الدول والأفراد. هذه المعلومات في مجالات مثل الخدمات المصرفية والتأمين والطبية.

حماية المعلومات الجنائية هي الوسيلة التي تحقق التجارة الدولية من خلالها أهدافها، وتكمل المعاملات، وتدخل في التدابير والاتفاقيات اللازمة لمفهوم التجارة الإلكترونية. تجعل الحماية الموثوقة للمعلومات على الإنترنت المعاملات التجارية أسهل وأسرع وأقل تكلفة.

المطلب الثاني: الحماية الجنائية للمعلومات في النظم المقارنة

لقد أثار إحصاء تقنية المعلومات تحديات كبيرة بالنسبة لقانون العقوبات في كل أنظمته القانونية، وسبب ذلك القيمة المتزايدة للمعلومات بالنسبة للاقتصاد واتمع والسياسة.

ونظرا لأن قانون العقوبات حتى فترة قريبة لم يكن يعرف إلا حماية الأشياء المادية والمرئية، إلا أنه مؤخرا وللأهمية المتزايدة للمعلومات وتقنيااا ظهرت الحماية الجنائية لها وللقيم المعنوية الأخرى.

فحدثت الموجة الأولى من التعديلات في السبعينات والثمانينات من القرن الماضي في العديد من الأنظمة القانونية الغربية. وهذه التعديلات تتعلق بالحياة الخاصة، وهذه التشريعات كانت بمثابة رد فعل إزاء التهديدات المستحدثة للحياة الخاصة.[1]

1د .رشدي مُحَمَّد علي مُحَمَّد عيد علي، مرجع سبق ذكره، ص.79.

ففي بداية الثمانينات، أصدرت العديد من الدول قوانين لمكافحة الإجرام الاقتصادي الخاصة بتقنية المعلومات والتي تشتمل على تجريم الولوج غير المسموح به إلى النظام التقني للمعلومات. وبعدها ظهرت تشريعات بغرض توفير حماية أفضل للملكية الذهنية في مجال تقنية المعلومات.

وقد استبعدت برامج تقنية المعلومات من الحماية عن طريق قانون براءات الاختراع، وصدرت قوانين أخرى لحماية البرامج.

أولا:حماية المعلومات على المستوى الدولي:

تختلف خطة التشريعات المقارنة في موضع النص على الحماية الجنائية وتتوزع إلى اتجاهاين :

الأول يرى إصدار قانون يعاقب فيه على جرائم الكمبيوتر بصورها المختلفة ، وتقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة مثلا "السجلات والتوقيع الإلكتروني" ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية.

والإتجاه الثاني من التشريعات يذهب إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى إستيعاا الصور المستحدثة من الجرائم الإلكترونية ، ثم تفرد هذه الخطة التشريعية قوانين خاصة ببعض الموضوعات مثل الإتصالات والتوقيع الإلكتروني والتي تتضمن نصوصا تتصل بتجريم الاعتداء على المستند الإلكتروني .ومن امثلة التشريعات التي تبنت هذه الخطة الأخيرة القانون الألماني والفرنسي.

ا-**القانون الفرنسي:** نص الشارع الفرنسي على تجريم الإعتداء على أنظمة معالجة البيانات ،وذلك بموجب الفصل الثالث من الباب الثاني من قانون العقوبات ومن ضمن الجرائم التي تضمنها هذا الفصل إدخال أو مسح أو تغيير معلومات بطرق الغش (المادة 323- 3)كما نص الشارع الفرنسي على تجريم عدة أفعال تقع ضد المصالح العليا للدولة وذلك إذا انصبت على المعلومات أو البيانات التي تم معالجتها إلكترونيا (المواد 411-6 إلى 411-10) وإلى جوار هذه النصوص الخاصة الواردة في قانون العقوبات فإن الشارع الفرنسي قد نص على بعض الجوانب المتصلة بالمستند الإلكتروني في قوانين متفرقة أهمها:قانون الإثبات والتوقيع الإلكتروني الصادر في 13 مارس سنة 2000/ ولائحته الصادرة في 30 مارس سنة 2001 .والذي أقر فيه الشارع الفرنسي الأخذ بالدليل الإلكتروني في الإثبات والتوقيع الإلكتروني ووضع له الضوابط التي تكفل صحته . ومن التشريعات الأخرى التي تتضمن جانبا من الحماية المقررة للمستند الإلكتروني قانون حرية الإتصالات الذي صدر في سبتمبر سنة 1986 وعدل بقانون أول أغسطس سنة 2000.

ب القانون الألماني:

تدخل الشارع الألماني بقانون 15 مايو سنة 1986 والذي عدل بمقتضاه قانون العقوبات بأن اضاف إليه المادة 202 (أ)، والتي جرما فعل التجسس على المعلومات المخزنة . وقد وردت هذه المادة في الباب الخاص بجرائم الإعتداء على الحياة الخاصة والسر اللذين جمعهما الشارع الألماني في باب واحد، وعلة ذلك الإرتباط الوثيق بين فكرة الس وبين الحياة الخاصة، وأن عناصرهما تتحددفي حماية سرية المحادثات وحماية سرية المراسلات ، وحماية الأسرار الخاصة للأفراد1.

كما أصدر المشرع الألماني قانونا للتوقيع الإلكتروني دخل حيز النفاذ في أول نوفمبر سنة 1997، وقد نص المشرع الألماني في هذا القانون على قواعد التوقيع الإلكتروني مثل تعريف الإصطلاحات الواردة في التشريع وتحديد السلطة المختصة بتطبيقه، والقواعد المتعلقة بمقدمي خدمة التوثيق والسلامة الفنية وفي الرابع نظم قواعد الإشراف وضوابطه كما نص كذلك على القواعد الخاصة بالمسؤولية والجزاءات الموقعة . وقد اصدر الشارع الالماني كذلك قانون المعلومات وخدمات الإتصالات ، والذي دخل حيز النفاذ في أول أغسطس سنة 1997.

ثانيا:حماية المعلومات على المستوى العربي او الاقليمي:

لم تكن الدول العربية غائبة عن النقاشات، التي كانت تدور داخل أروقة الأمم المتحدة حول مدى تأثير تطور التكنولوجيا الحديثة للإعلام على حقوق الإنسان وحرياته. ويعتبر انعقاد مؤتمر الأمم المتحدة الأول لحقوق الإنسان في طهران عام 1968 أكبر شاهد على ذلك. خلاله بدأت الدول العربية تعي خطورة وأهمية انتشار هذه التكنولوجيا، خاصة حينما ستنفلت من يد الدولة فتصبح متاحة للأفراد والمؤسسات يستخدموا كما شاءوا. وقد أكدت قضية "واتركيت" في الولايات المتحدة الأمريكية لدى هذه الدول خطورة استخدام الآلات الدقيقة من طرف الأفراد أو من طرف بعض المؤسسات غير الأمنية والغير عسكرية، في التلصص، والتصنت، وكشف أسرار الهيئات والمؤسسات وحتى الدول2. في السابق كانت هذه الآلات حكرا على أجهزة المخابرات، بينما اليوم يمكن الحصول عليها من طرف أي كان

1 Verboteme Schriften im internet, Juristiche Rundschau, 1997, S496. Redbruch (Gustav).

2جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجية الحديثة الكتاب الأول: الجرائم الناتجة عن استخدام الحاسب الآلي. دار النهضة العربية القاهرة 1992.

،واستخدامها لشتى الأغراض، من كشف أسرار الدولة إلى كشف أسرار الأفراد والتعدي على حيام الخصوصية في أدق تفاصيلها.

إذا كانت الدول العربية على علم ودراية بأهمية وخطورة هذه التقنيات الحديثة للاتصال الناتجة عن الثورة المعلوماتية فإنها مع ذلك تبقى كغيرها من الدول غير المنتجة لهذه التقنية، غير مبالية بانعكاساتها القانونية، تاركة في البداية أمر تدبير المشاكل الممكن أن تنتج عنها للقوانين القائمة التقليدية: مثل القانون الجنائي- وقانون الإعلام والاتصال والقانون التجاري، والقانون المدني.

فعلى المستوى الدولي شكل مؤتمر طهران 1، لحظة تحول واهتمام بالتداعيات القانونية لتطور التكنولوجيا على مجال حقوق الإنسان. فتلى ذلك إصدار الأمم المتحدة لقرارات تشدد على هذا الأمر، وبالخصوص في سنة 1973 تزامنا مع قضية "واتركيت" وأعقب ذلك انطلاق تشريعات وقوانين حماية الخصوصية وحماية البيانات الشخصية، وتجدر الإشارة هنا على الخصوص إلى التشريع السويدي لسنة 11973.

لقد كانت هذه التطورات العلمية كبداية لتأكيد الجذور الأولى للفضاء الالكتروني، والفضاء التخيلي. ولربما أن ذلك ما حدا بالكاتب "وليام جيبسون" في سنة 1984 إلى تصور ظهور عالم افتراضي، ينشأ عن ترابط الأنظمة الكمبيوترية التي تعمل ضمن الشبكة العالمية، وتتم من خلاله أنواع متعددة من المعاملات مثل: البيع، والشراء، وتجارة الأسهم.فهل في ذلك تأثير على التفكير القانوني للانترنت؟

1- البحث حول إمكانية وجود قانون خاص بالأنترنت:

يبدو أن الأمر على عكس ما يتمناه كثير من القراصنة ومستغلي الفضاء الافتراضي من أجل ارتكاب جرائم السطو والسرقات، وجرائم التشهير، والمساس بالحياة الخصوصية للأفراد، فالانترنت ليس فضاء اللاقانون، وليس فضاءا تسوده الفوضى، تحت غطاء اعتباره مجالا للحرية المطلقة الشاملة ، وليس عالما افتراضيا لا يحكمه أي ضابط، ومنفلت من أي وازع. إن هذا الأخير هو وسيلة لإرسال واستقبال المعلومات والحصول عليها من مختلف أطراف المعمور وبسرعة مذهلة. كما يمكن القيام منخلاله بمعاملات متنوعة، كالتسويق، والاتصالات، والإعلانات، وإجراء التعاقد...1، وهذا ما اصطلح عليه بالفضاء التخيلي أو الفضاء الالكتروني. هكذا إنه بفعل المهام التي يقوم ا، والخدمات التي يقدمها بسهولة ويسر، وبحكم أهمية وخطورة المعاملات التي تجرى من خلاله، صار من المفروض أن ينظم من الناحية القانونية.

1قانون حماية الكمبيوتر: بين تبادل المعلومات وحماية الابداعجريدة المساء: عدد 535 السبت/ الأحد 7/6 يونيو 2008.

وتوضع له ضوابط وقواعد تلجمه وتحكمه، ولأجل هذا الغرض ظهرت مدرسة التنظيم القانوني للانترنت التي تلح على عدم إهمال الجوانب القانونية للانترنت، خاصة في وقت صار التطور التكنولوجي يطرح إشكالات وقضايا قانونية متنوعة ومعقدة، ومن نوع خاص2. وعلى هذا فإن المبادئ القانونية التقليدية قد لا تفي بالغرض عند تطبيقها . تحت هذا الضغط فرض على الدول المتقدمة، ودول العالم الثالث وضمنها الدول العربية صياغة ووضع قوانين يتم بموجبها تنظيم الفضاء الافتراضي. فإذا كان هاجس التنظيم القانوني للانترنت قد فرض نفسه على هذه الدول، فالأمر ازداد أهمية وإلحاحية في وقت أضحى فيه العالم بفعل هذه الوسيلة التكنولوجية عبارة عن قرية الكترونية صغيرة على حد تعبير "ماكلهون"، يمكن التجول في مختلف أرجاءها شرقا وغربا، شمالا وجنوبا، بفضل الانترنت.

2- الغرض الذي أدى إلى محاولة وضع قانون (قوانين) عربية للأنترنت

كان هناك نقاش واسع حول هل من الضروري وضع آليات قانونية لتنظيم الانترنت1؟ أم أن ماهو موجود وقائم حتى الآن من قوانين كاف ليحكم ما قد ينتج عن هذه الوسيلة التكنولوجية من تصرفات وأعمال، ومخالفات. أسفر هذا النقاش على ظهور اتجاهين1.

أولهما: يرى أن الانترنت، لم ينتج بعد آثارا واضحة تقتضي التدخل المشروع لتنظيم المسائل المترتبة عنه.

الثاني: يرى أن الانترنت يسابق العصر وأن عدم الإسراع في تنظميه قاد إلى حدوث تأثيرات دون أن يكون ثمة قانون يؤتدى به في الموقف من هذه التأثيرات.

وأيا كان الأمر فإن التعامل مع الانترنت يثير التساؤلات القانونية الآتية، وهي تساؤلات غير قاصرة على تشريعات الانترنت في الأقطار العربية فقط، بل هي عامة وتتعلق بالظاهرة القانونية للأنترنت في عموميتها: وهذه التساؤلات هي[2]:

هل إبرام العقود عبر الانترنت تتوفر فيه سلامة وصحة التعبير عن الإرادة كما هو الشأن في التعاقد الكتابي أو الشفاهي في مجلس العقد؟ وهل توقيع العقود والمراسلات اليكترونيا معادل لتوقيعها ورقيا؟

1عمر مُحَمَّد بن يونس: مشكلة قواعد البيانات، موسوعة التشريعات العربية ، دار الفكر الجامعي: الاسكندرية: 2004.

2 PHILIPPE AIGRAIN : Au-delà du logiciel libre, le temps des biens communs : le monde diplomatique, Octobre 2005

- هل رسائل البريد الالكترونية ذات قيمة معادلة للمراسلات الورقية؟ [1]

- هل الاعتداء على الأشخاص وعلى الأموال في البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات نظام المعلوماتي؟

- كيف يمكن حماية الأسرار الشخصية، وبيانات الحياة الخاصة من اعتداءات المعلوماتي أو المتطفل دون تصريح أو إذن؟

- هل إغلاق المواقع أوحجبها ،مثل المواقع ذات المحتوى غير المشروع في بعض النظم والمشروع في الأخرى، يعد تجاوزا في حق ديموقراطية العالم الافتراضي.

- هل النشر الالكتروني من قبيل النشر الصحفي الذي يحكمه قانون الإعلام والاتصال.[2]

ما ذا أنجزت الدول العربية على المستوى التشريعي انطلاقا من التساؤلات المومأ إليها من قوانين فيما يخص التجارة الالكترونية وفي التوقيع الالكتروني؟

إن التساؤل عما أنجز هنا تشريعيا على المستوى العربي غير قاصر على ما أنتج بشكل فردي من قبل كل قطر على حدة، ولو أن هذا هو الأهم، ولكن كذلك ما أنتج على المستوى الجماعي ،أي في إطار النظام الإقليمي وفي ظل مؤسسة جامعة الدول العربية. لسنا في حاجة إلى التأكيد على أن الدول العربية مثلها مثل بقية الدول التي في نفس أوضاعها، تحاول جهدها ضبط ما يطرحه استخدام الانترنت، وما يطرحه الاستخدام المتوالي والسريع لتكنولوجيا الإعلام قصد تنظيمها قانونيا. وتجدر الإشارة هنا إلى الجهود التي بدلت في هذا الاتجاه من طرف بعض الدول العربية وخاصة فيما يتعلق بمجال التجارة الالكترونية، والتوقيع الالكتروني.

يمكن أن نشير على سبل المثال لا الحصر إلى جهود كل من تونس، والمغرب، والأردن ،والسعودية، والبحرين ،والإمارات العربية، ومصر ولبنان، ودبي، وسوريا والسودان...

1 لمزيد من التدقيق في هذه الأسئلة يراجع: يونس عرب: مقال في جريدة المساء: عدد: 535/ السبت الأحد 2008/8/7 تحت عنوان: قانون الكمبيوتر... بين حرية تبادل المعلومات وحماية الإبداع.

2 علي كريمي: تطور قوانين الإعلام في الدول المغاربية "ورقة مقدمة في الحلقة الدراسية المنظمة من طرف الإيسيسكو يونيو 2009 بطرابلس ليبيا"

4- التنظيم القانوني: التجارة الالكترونية، والتعاقد والتوقيع الالكتروني1

اهتمت جل الدول العربية ذا الموضوع خلال الفترة الممتدة ما بين 2000 و2009، ومن الناذر اليوم أن نجد خلو تشريع هذه الدول من قوانين تنظم التجارة الالكترونية والتوقيع الالكتروني.

ولو شئنا سوق الأمثلة لتزاحمت أمامنا النماذج بما يفيض عن غرض هذه الورقة، ولغطت هذه الأمثلة كل دول المغرب العربي، والخليج العربي، والدول الأخرى. وهكذا ففي مملكة البحرين صدر قانون التجارة الالكترونية بتاريخ:14 سبتمبر 2002، كما صدر في الأردن القانون رقم 85 لسنة 2001، قانون المعاملات الالكتروني. وفي تونس صدر القانون عدد 83 لسنة 2000 الخاص بالمبادلات الالكترونية والمؤرخ في 9 غشت 2000. ويسرى نفس الشيء على المغرب، والجزائر وتونس وليبيا ولبنان والإمارات العربية المتحدة.فإذا كان استخدام الانترنت في الأغراض التجارية بدأ في الانتشار على الصعيد العالمي منذ 1992، فصار كمروج للسلع والخدمات. وبدأ رجال الأعمال وأصحاب المؤسسات والشركات التجارية في الإقبال على المواقع الخاصة ذا الغرض، وأصبحوا يبرمون الصفقات عن طريق مراسلام عبر البريد الالكتروني، كما صاروا يعرضون منتجام وخدمام من خلال مواقعلهم على شبكة الانترنت1.

ساهمت ثورة المعلومات والاتصالات في انتشار التجارة الالكترونية، ونتج عن الصفقات التي تتم عبر الانترنت، ظهور العقود الالكترونية كوسيلة قانونية جديدة، فصارت مثار جدال قانوني خصب. فاضطرت الكثير من المنظمات الإقليمية والدولية، وكثير من مشرعي الدول إلى الإقرار ذا الواقع والاعتراف به، ومن ثمة، إجازة التعبير عن الإرادة التعاقدية عبر الوسائل الالكترونية. وهو ما يعني أن التقاء الإرادات اليكترونيا يكفي لإبرام العقد متى استوفى شروطه.

أقر القانون النموذجي للتجارة الالكترونية لسنة 1996 أن تبادل التعبير عن الإرادة من خلال تبادل البيانات الالكترونية في الأعمال التجارية حيث نصت المادة:11 منه على: "...في سياق إنشاء العقود، وما لم يتم اتفاق الطرفان على غير ذلك يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند استخدام رسالة البيانات في إنشاء العقد، لا يفقد ذلك العقد صحته أو قابليته للتنفيذ فرد استخدام رسالة بيانات لذلك الغرض".[2]

1علي كريمي: تطور قوانين الإعلام في الدول المغاربية، المرجع السابق .

2 Rachid BOUTI : les enjeux du commerce électronique pour les commerçants : cybers PME-PMI artisans on line, REMALD, sirie études, n°50, Mai-juin 2003.

كما أن قانون المعاملات الالكترونية الموحد لعام 1999 نص صراحة على أن أحكام التعاقد إلكترونيا مثل التعاقد كتابيا عندما قرر أن التسجيل الالكتروني يعادل المستند المكتوب خطيا1.

وتقر اتفاقية الأمم المتحدة بشأن عقد البيع الدولي للبضائع في مادا:10"... جواز التعاقد عن طريق وسائل الاتصال الفوري".

- لكن كيف تعاملت التشريعات العربية مع التعاقد الالكتروني؟ للجواب على هذا السؤال نستعرض بعضا من هذه التشريعات: وكمثال على ذلك: المادة:14 من قانون إمارة دبي بشأن المعاملات والتجارة الالكترونية2وتنص على "... يجوز أن يتم التعاقد بين وسائطالكترونية مؤتمة متضمنة نظامي معلوماتي أو أكثر تكون معدة، ومبرمجة مسبقا للقيام بمثل هذه المهمات، ويتم التعاقد صحيحا ونافذا ومنتجا آثره القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة".

وتأكيدا لمبدأ جواز التعاقد الالكتروني نصت المادة:7/1 من نفس القانون على:

" لاتفقد الرسالة الالكترونية آثارها القانوني أوقابليتها للتنفيذ اذا جاءت في شكل الكتروني".

- أما المشرع الأردني فإنه أكد على "أن إبرام العقود الالكترونية بواسطة الرسالة الالكترونية يعتبر صحيحا عندما قرر في المادة 13 من قانون المعاملات الالكترونية رقم 85- لسنة 3001:

"تعتبر الرسالة الالكترونية وسيلة من وسائل التعبير عن الإرادة المقبولة قانونيا لإبداء الإيجاب والقبول بقصد إنشاء التزام تعاقدي".

- وفي المغرب صدر قانون التوقيع الالكتروني بظهير رقم 1-07-129 الذي يقضي بتنفيذ القانون رقم 05- 53 المتعلق بالتبادل الالكتروني للمعطيات القانونية التي يتم تبادلها بطريقة الكترونية.2 يحدد القانون النظام المطبق على المعطيات القانونية التي يتم تبادلها بطريقة الكترونية، وعلى المعادلة بين الوثائق المحررة على الورق، وتلك المعدة على دعامة الكترونية وعلى التوقيع الالكتروني.

- ويشترط المشرع المغربي على أن تكون الوثيقة المحررة على دعامة الكترونية بنفس قوة الإثبات التي تتمتع ا الوثيقة المحررة على الورق شريطة أن يكون بالإمكان التعرف بصفة قانونية على الشخص الذي صدرت

1غزة على محمد الحسن: قانون الانترنت، شركة مطابع السودان للعملة: رقم الإبداع 404/2005

2وهو القانون رقم: 2 لسنة 2002.

3انظر الجريدة الرسمية رقم 5584 الصادرة يوم الخميس 6 دجنبر 2008.

عنه، وان تكون معدة ومحفوظة وفق شروط من شأنها أن تضمنتماميتها، إضافة إلى أنه اشتراط أن يكون التوقيع الالكتروني مؤمّنا. ويعني بذلك أن يتم إنشاؤهوفق النصوص التنظيمية والتشريعية المعمول ا في هذا (المادة 1- 497-3- 417).

- وأكدت المادة 6 من هذا القانون على أن التوقيع الالكتروني يجب أن يستوفي بعض الشروط1.

- وفي الجزائر أصبح للكتابة في الشكل الالكتروني والتوقيع الالكتروني مكانا ضمن قواعد الإثبات في القانون المدني الجزائري من خلال نصي المادتين 323 مكررا و 327 فقرة 2 من ق.م.ج .

والمقصود بالكتابة في الشكل الالكتروني حسب هذا النص.ذاك التسلسل في الحروف أو الأوصاف أو الأرقام أو أية علاقة أو رموز ذات معنى مثل المعلومات والبيانات التي تحتويها الأقراص الصلبة أو المرنة، أو تلك التي تتم كتابتها بواسطة الكمبيوتر وإرسالها أو نشرها عبر الانترنت

كما أن المشرع التونسي في القانون رقم 83-2000 الخاص بتنظيم التجارة الالكترونية والتوقيع الالكتروني أقام التكافؤ بين المحررات الالكترونية والمحررات الورقية ولكنه قيد ذلك بشروط لتفادي الاستغلال غير المشروع للتوقيع الالكتروني، وأكد على ذلك في الفصل 5 من هذا القانون ،وفي الفصل 6 منه.

عند مقارنة المشرع المغربي بالتونسي نجد أن المغربي هو الآخر يشترط أن يكون للوثيقة المحررة على دعامة الكترونية نفس القوة الاثباتية التي للوثيقة المحررة على الورق. لتأكيد ذلك أدخل تعديلات على قانون العقود والالتزامات المغربي همّ الفصول الآتية: [2-417 و 2- 417 و 3-417]، ولكنربط ذلك بشروط منها:

- أن يكون بالإمكان التعرف بصفة قانونية على الشخص الذي صدرت عنه الوثيقة المحررة بشكل الكتروني، ومحفوظة وفق شروط من ضمان تماميتها، ومدعمة للتوقيع الالكتروني.

وأقر المشرع على أن المحرر الالكتروني، يرقي إلى درجة الرسمية وذلك إذا وضع التوقيع على المحرر أمام موظف عمومي له صلاحية التوثيق.1

1تنص المادة 6 على: " يمكن لكل من يرغب في إمضاء وثيقة الكترونية إحداث إمضائه الالكتروني بواسطة منظومة موثوقا يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات".

2عمر نجوم: الحجية القانونية لوسائل الاتصال الحديثة: دراسة تحليلية في نظام الإثبات المدني. أطروحة لنيل الدكتوراه: كلية الحقوق الدار البيضاء 2003-2004 ص 137.

فإذا كانت التجارة الالكترونية والتعاقد والتوقيع الالكتروني من بين الأمور التي عمد المشرع العربي إلى الاهتمام ا بشكل معقول، فإن الجانب الأكثر أهمية الذي أولاه هذا الأخير عناية زائدة هو ما يتصل بمكافحة الجريمة الالكترونية.

5- المشرع العربي والجرائم الالكترونية

إذا كانت جرائم الانترنت جرائم متعددة ومتنوعة، ويستعصي حصرها بسهولة، فإن الأمر ذاته ينطبق على تعريفها، إلا أنه مع ذلك يمكن اعتبارها:

1-جميع الأفعال المخالفة للقانون والشريعة، والتي ترتكب بواسطة الانترنت.

2- هي الجرائم التي يتم ارتكابها، إذا قام شخص باستخدام معرفته بالانترنت بعمل غير مشروع قانونا، ومستخدما الحاسوب كموضوع للجريمة.

ورغم صعوبة ضبط وصعوبة مكافحة جرائم الانترنت على الصعيد العربي إلا أن هناك جهود جماعية وفردية في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم. ولكن أيضا هذه الجهود فيها ما هو مضاد لحرية التعبير ويمكن أن نذكر من بين الجهود الجماعية العربية، ما حصل من تعاون عربيفي هذا الصدد بمناسبة انعقاد "مؤتمر وزراء الداخلية العرب في تونس سنة 2006". عندما قدم وزير الداخلية المصري اقتراحا بتوحيد الجهود العربية للعمل على استصدار قرار من مجلس الأمن بالتزام الدول التي تتبعها المؤسسات، والشركات العالمية الكبرى، التي تباشر إدارة واستقبال شبكات المعلومات والاتصال، بإغلاق المواقع التي تبث بيانات للأفكار والأيديولوجيات المتطرفة. قد قوبل هذا المطلب بمواجهة عنيفة من قبل المنظمات الحقوقية التي اعتبرت مثل هذا الإجراء ما هو إلا تقييد لحرية الرأي والتعبير.

كما تحركت مصر والسعودية مرة أخرى في مؤتمر وزراء الإعلام العرب 2008 "بتقديم مسودة مشروع مقترح لتشكيل لجنة عليا للإعلام الالكتروني"، وهو خطوة أخرى ظاهرها مكافحة الجرائم الالكترونية وباطنها هو تقييد حرية الرأي والتعبير، مستندين على أن الإعلام الالكتروني في الدول العربية يتسم بالخطورة ولا تحكمه أية معايير أو ضوابط مهنية واضحة يمكن الالتزام.

6- نماذج من القوانين الداخلية لمكافحة جرائم الانترنت عربيا

جل الدول العربية وضعت قوانين لمكافحة جريمة الانترنت، فعلى امتداد الوطن العربي من المحيط إلى الخليج، نجد ترسنة قانونية تنظم جرائم الانترنت1.بدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، وعلى سبيل المثال ظهرت في معظم الدول العربية قوانين لمنع ومحاربة الإرهاب الذي أدخل في القوانين الجنائية، حيث تم التأكيد من خلالها على استخدام الانترنت في القضايا المتصلة بالإرهاب والتشديد عليها، والأمر هنا لا يقتصر على التشريع المغربي لسنة 2003 أو على التشريع التونسي والمصري، بل يهم جل تشريعاتدول المنطقة.

إن ما كان سائدا في الأدبيات القانونية العربية الخاصة بالانترنت هو أن هناك فراغ قانوني على الصعيد العربي يحول دون تحجيم وكبح هذا الوحش الالكتروني، لكن هذا الاعتقاد صار اليوم غير ذي جدوى. ولتأكيد ذلك بالحجة والدليل القاطع سوف نحاول إيراد بعض نماذج القوانين العربية الخاصة بمكافحة ومحاربة الجرائم المعلوماتية مثل القانون السوداني سنة 2006، وكذلك قانون الإمارات العربية المتحدة، أي القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات. وقانون المملكة العربية السعودية المتعلق: بنظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم:17 بتاريخ 1428/3/8.

إذا كان من واجب المشرع أن ينتج نصوصا قانونية تؤطر الظواهر الاجتماعية الجديدة، فإن من واجبه كذلك أن تكون القواعد التي يصوغها جد واضحة وخالية من الغموض، حتى لا تكون محل تفسير خاطئ أو مغمض من طرف السلطة التنفيذية1، ولعل المثال الذي يمكن سوقه هنا، ما يتردد في كل التشريعات العربية الخاصة بمكافحة جريمة الانترنت، بحيث لا يخلو أي قانون منها. وتتكرر فيه بنفس الغموض ،ويتعلق الأمر بالنظام العام والأمن العام والأخلاق العامة. إن هذه الألفاظ عامة وفضفاضة وتحتمل مختلف أوجه التأويل، بل إن مفهوم النظام العام قد يتسع ويضيق تبعا للظرفية السياسية التي يمر ا البلد. فمفهوم النظام العام عندما تكون الدولة في حرب، أو ا اضطرابات اجتماعية هو غير مفهوم النظام العام في حالة الاستقرار والهدوء وما نلاحظه فيما يخص التشريع العربي للانترنت هو الطابع الموحد والمشترك لنصوصه.

1الصعيد العربي هناك دول قد أصدرت قوانين لمكافحة الجريمة الالكترونية، بينما أن دول أخرى عملت على سد الفراغ التشريعي الحاصل في مجموعة القانون الجنائي فيما يتعلق بتجريم الأفعال المرتبطة بتكنولوجيا المعلومات، ووضع العقوبات الملاءمة لها.

لمزيد من التوضيح: أنظر: محمود عبده الدلالعة: الحماية القانونية لتكنولوجيا المعلومات (برامج الحاسب الآلي). مرجع سابق

إنهذه الأخيرة تكاد تكون مصاغة وبنفس الكيفية ونفس النمط، ويتضح ذلك في تشريعات الانترنيتفي جميع الدول العربية تقريبا دون أدنى تمييز بينها. ويمكن أن نجمل الجرائم التي وردت في هذه التشريعات على النحو الآتي:

جرائم نظم ووسائط شبكات المعلومات:

كدخول المواقع وأنظمة المعلومات المملوكة للغير- التصنت أو التقاط أو اعتراض الرسائل

– دخول المواقع وأنظمة المعلومات من موظف سام- جريمة دخول المواقع عمدا قصد الحصول على معلومات أوبيانات أمنية- إعاقة أو تشويش أو تعطيل الوصول للخدمة.

أ- الجرائم الواقعة على الأموال والبيانات والاتصالات بالتهديد والابتزاز:

- الاحتيال أو انتحال الشخصية أو صفة غير صحيحة- الحصول على أرقام أو بيانات بطاقات الائتمان- الانتفاع دون وجه حق بخدمة الاتصال.

ب-جرائم النظام العام والآداب العامة:

- 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.

ج- جرائم الإرهاب والملكية الفكرية:

- إنشاء أو نشر مواقع للجماعات الإرهابية- جريمة نشر المصنفات الفكرية.

هـ- جرائم الاتجار في الجنس البشري والدعارة والمخدرات وغسل الأموال- الاتجار أو الترويج للمخذرات أو المؤثرات العقلية- غسل الأموال.

و- الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية.

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. ومن أهم الأمور التي أولتها هذه التشريعات أهمية قصوى إلى جانب أمن الدولة الحفاظ على النظام العام الذي يتواتر فيها بنفس الصيغ والمعنى. ففي التشريع السعودي نجد مثلا المادة:6 المقطع "أ "منها ينص على تجريم "إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية أو الآداب العامة، أو الحياة الخاصة..."

- أما التشريع السوداني فقد خصص فصلا كاملا لجرائم النظام العام والآداب والإخلال ما.

وهو الفصل الرابع وخاصة المادة:14 منه.

- أما التشريع الإماراتي رقم 2 لسنة 2006 "في شأن مكافحة جرائم تقنية المعلومات" فنجد المادة:20 منه تنص على: "كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات".

ومن بين الأمور التي ركزت عليها التشريعات العربية المتعلقة بالجرائم الالكترونية وتتردد وباستمرار فيها مسألة حماية القيم الدينية والعائلية، ومنع البورنوغرافية. فالتشريع الإماراتي كان أكثر وضوحا فيما يخص الإساءة إلى الدين الإسلامي وإلى الديانات السماوية الأخرى، وهذا ما تؤكده المادة 15 منه- وأردف في المادة الموالية أي المادة:16 التأكيد على ما يلي:" كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر أخبارا أو وصورا تتصل بحرمة الحياة الخاصة أو العقلية للأفراد ،ولو كانت صحيحة عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات يعاقب بالحبس مدة لا تقل عن سنة، وبالغرامة التي لا تقل عن خمسين ألف درهم، أو بإحدى هاتين العقوبتين".1

- والملاحظ هنا، هو كون التشريع العربي للانترنت ركز كل اهتماماته على ما من شأنه أن يجعل حماية الدول، أسمى هدف من أهدافه، وأكبر هاجس من هواجسه وفي نفس الآن التركيز على النظام العام. بينما أن حماية المواطن لم يدقق فيها بالصورة المطلوبة والمرجوة. وهذه القاعدة تسري على جل التشريعات المنظمة لجرائم الانترنت في الدول العربية1.

ومن المعلوم أن حماية الأمن الرقمي يمكن أن يحيل على مفاهيم متعددة تتراوح مابين حماية الأشخاص، وحماية المعلومات وغيرها.

من هنا نتساءل لماذا لم تتم هذه التشريعات بحماية المعلومات الاثنية والدينية، والثقافية... لماذا لم تشدد أكثر على حقوق المرأة وعلى دعارة الأطفال وعلى الأحقاد العرقية؟ إن الأمور المشار إليها لا يمكن أن تبقى مهملة، إن لم يكن من كل قوانين الدول العربية فعلى الأقل في بعض هذه القوانين. فإذا كانت

1 Samia MIHOUB : op.cit.

الدول العربية تغالي كثيرا في مراقبة الانترنت، في نفس الآن تغيب عنها بنفس الصرامة والحدة مراقبة جرائم الدعارة و دعارة الأطفال، وجرائم العنصرية، التي تنتشر بشكل حر على فضاء الانترنت المفتوح1.

- فإذا كانت هذه الدول تلجأ باستمرار إلى محاكمة ومعاقبة مستخدمي الانترنت عندما يتعلق الأمر بارتكاب بعض الجرائم، ومن واجبها كذلك أن تبدل جهودها من أجل القيام بحملات تحسيسية للحماية من المخاطر التي يمكن أن تصادف القاصرين ومختلف مستعملي الانترنت. لقد كان من نتائج غياب التحسيس ما كشف عنه تقرير: مركز حرية الإعلام للشرق

الأوسط وشمال إفريقيا في تقريره الشهير حول "جرائم الانترنت ضد الأطفال في المغرب"2، عندماأوضح المخاطر التي تهدد الأطفال واستغلالهم على شبكة الانترنت، وذلك في غياب أية مقاربة جدية وحقيقية تتبناها هذه الدول بغية حماية الأطفال من المحتويات المشتملة على الخلاعة والدعارة المتداولة باستمرار على شبكة الانترنت.

إن الحافز المهيمن على ممارسات الدول العربية التشريعية في مجال تنظيم الانترنت محكوم بالهم السياسي وهاجس الأمن العام والنظام العام بمضمونه السياسي، ولعل ذلك ما يستشف من تقرير "برنامج الأمم المتحدة للتنمية البشرية في الوطن العربي لسنة 2004" الذي يوضح عند حديثه على قيم الحرية، والتعددية وحقوق الإنسان، كيف أن المشرع يضع نصوصا جنائية وغير جنائية، تقيد الحريات العامة، وتعتبر حرية الصحافة المكتوبة والسمعية البصرية، وممارسة حرية التعبير كنشاطات مزعجة ينبغي تحجيمها2.

وعلى العموم يمكن القول إن الدول العربية لم يعمم فيها بعد وبشكل كافي، إصدار قوانين خاصة بجرائم الانترنت، باستثناء بعض النماذج المشار إليها مثل الإمارات العربية المتحدة، وتونس ،والسودان ويبدو اليوم أن هناك لدى هذه الدول شعور عميق بتنظيم الجرائم المرتكبة عن طريق الانترنت، وهي تحضر مشاريع قوانين في هذا الاتجاه. ويعود سبب الاهتمام بتنظيم جرائم الانترنت إلى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة النشأة والتي ظهرت لأول مرة كمصطلح في استراليا عام 1988.

1مالك خدام: جرائم الحاسب والانترنت... ارتفاع معدل استغلال الأطفال جنسيا جريدة الثورة: الاثنين 2005/3/7

2مركز حرية الإعلام بالشرق الأوسط وشمال إفريقيا: القاصرون وجرائم الانترنت في المغرب سبتمبر2006. 2

Nouri LAJMI : « la liberté de l'information à l'ère du cyberespace », Revue Tunisienne de la communcation n° 37-38, Janvier/ décembre 2001

ولكي يتم التنظيم الجدي لهذه الجرائم على المستوى العربي من الضروري وضع اتفاقية إطارية جماعية تحدد جرائم الانترنت وتكون كتشريع موحد عربي لمواجهتها تدي به التشريعات القطرية ولا تخرج عن مضمونه. ولعل هذه المهمة موكولة إلى مؤسسة النظام الإقليمي العربي أي جامعة الدول العربية، على غرار ما حصل في النظام الإقليمي الأوروبي، لما وضعت الاتفاقية الأوروبية "حول جرائم الانترنت المرخص ا من قبل اللجنة الأوروبية ب "بودابيست في 13 ن وفمبر 2001، والتي يمكن اعتبارها من بين التشريعات الأكثر تطورا، حيث عرفت تسع جرائم مجتمعة في أربع فئات هي:1

- الجرائم التي تمس حرية الحاسوب وسلامته.
- سوء النية المقصود في استعمال الحاسوب (مثل جريمة التزوير أو الاحتيال المرتبطة بالحاسوب).
- الجرائم المرتبطة بمختلف قوانين النشر والترويج
- الجرائم المتعلقة بالجنس (أي الجرائم التي لها علاقة بالدعارة وبالاعتداء الجنسي على الأطفال).

ومن المعلوم أن الاتفاقية العربية لمكافحة جريمة الانترنت عند وضعها قد تتضمن ما يعبر عن الخصوصية العربية الإسلامية للمجتمعات العربية شريطة أن تكون تلك الخصوصية إضافة جديدة في مجال حقوق الإنسان، وليس نقصا لما هو متعارف عليه عالميا في هذا ا.

ولعل مؤتمر الأمم المتحدة الثاني لحقوق الإنسان في فيينا عام 1992 قد فصّل كثيرا في هذا الموضوع، موضوع الخصوصية.2

- ويدفعنا موضوع الخصوصية إلى طرح حق الخصوصية وحماية البيانات الشخصية وكيف تم التعامل معها على مستوى التشريعات العربية المنظمة للانترنت، باعتبارها حقا من حقوق الإنسان الأساسية والجوهرية.

ي_تشريعات القانون الجزائرى

صادق مجلس الأمة الجزائرى يوم الأربعاء / 8 يوليو الحالى / 2009 بالاجماع على مشروع القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

1 محمّد أحمد: حقوق الإنسان بين الخصوصية والعالمية، رسالة لنيل دبلوم الدراسات العليا المعمقة: كلية الحقوق الدار البيضاء 2003

ويتضمن القانون 19 مادة موزعة على 6 فصول و هو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء و مهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية.

كما يتضمن القانون أحكاما خاصة بالمراقبة الإلكترونية التي لايجوز إجراؤها إلا بإذن من السلطة القضائية المختصة و في حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب و الجرائم الماسة بأمن الدولة أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

وينص القانون على انشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال و مكافحته تتولى تنشيط و تنسيق عمليات الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم.

وتتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج، علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل.

قانون رقم 09-04مؤرخ في 14شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها1.

1ج.ر.ج.ج.د.ش: رقم 74.

المبحث الثاني: التدابير الوقائية لحماية المعطيات في مجال المعلوماتي

إن التدابير الوقائية لحماية المعطيات في المجال المعلوماتي تتكون من جزاءات التي قررها المشرع الجزائري لهذا النوع من الجرائم الحديثة جاءت طبقا لنص المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للجرائم المعلوماتية يجب أن تكون رادعة و تتضمن عقوبات سالبة للحرية، و المتمثلة في عقوبات تطبق على الشخص الطبيعي كما توجد عقوبات تطبق على الشخص المعنوي وكما ان المشرع الجزائري وضع اليات لحماية المعطيات في المجال المعلوماتي

المطلب الأول: الجزاءات

تناولنا في هذا المطلب العقوبات الاصلية المطبقة على مرتكبي الجرائم الماسة بأنظمة المعالجة الالية (الفرع الأول)

الفرع الاول: العقوبات الأصلية المطبقة على مرتكبي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

أقر المشرع الجزائري بموجب قانون العقوبات العقوبة الأصلية التي يمكن تسليطها على الشخص الطبيعي و المعنوي على حد سواء ما دام أنه قد تم ارتكاب أي فعل من الأفعال المجرمة الماسة بأنظمة المعالجة الآلية للمعطيات، فحصرها في عقوبة سالبة للحرية و الغرامة بالنسبة للأول، في حين أنه جعل عقوبة الثاني الغرامة التي تعادل أضعاف تلك المقررة قانونا للشخص الطبيعي، لهذا سنخصص في هذا المطلب بالدراسة و التفصيل للجزاءات المقررة قانونا لكل فعل ماس بأنظمة المعالجة الألية للمعطيات و ذلك على النحو الاتي:

اولا: العقوبات المطبقة على الشخص الطبيعي مرتكب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إن النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية تبين وجود تدرج داخل النظام العقابي، هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذ نجد سلم الخطورة يتضمن ثلاثة درجات:

تقرر الفقرة الأولى من المادة 394 مكرر من قانون العقوبات الجزائري عقوبة أصلية لجريمة الدخول أو البقاء غير المصرح بهما تتمثل في الحبس من 3 أشهر إلى سنة و غرامة خمسين ألف دينار جزائري إلى مئة ألف دينار جزائري

1-العقوبة المقررة لجريمتي الدخول أو بالبقاء بطريق الغش للأنظمة المعلوماتية:

- ظرف تشديد

تضاعف المادة 394 مكرر من قانون العقوبات الجزائري في فقرتها الثانية و الثالثة من عقوبة جريمة الدخول أو البقاء غير المصرح بهما، إذا نجم عن هذا الدخول أو البقاء إلى حذف أو تغير أو تخريب لنظام تشغيل نظام المعالجة الآلية للمعطيات. فحالتي حذف أو تغيير المعطيات ترفع العقوبة إلى ضعف تلك المقررة للجريمة في صورتها البسيطة فتصبح الحبس من ستة أشهر إلى سنتين و الغرامة من مئتي ألف إلى أربعمائة ألف دينار جزائري.[1]

2- جرائم الاعتداء العمدي على المعطيات :

إن المادة 394 مكرر 2 من قانون العقوبات تورد بالذكر العقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من شهرين إلى ثلاث سنوات و غرامة من ميلون دينار جزائري الى عشرة ملايين دينار جزائري سواء كان الاعتداء عمدي أو عن طريق الغش.1

ثانيا: العقوبة المقررة للشخص المعنوي مرتكب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي على أنه يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما يسأل عن الجريمة التامة أو الشروع فيها بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص بواسطة أحد أعضائه أو ممثليه، هذا مع الإشارة إلى أن المسؤولية الجزائية للشخص المعنوي لا يستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.2

1 قانون العقوبات الجزائري، مرجع سبق ذكره

2- عبد الله أوهايبية، مرجع سبق ذكره.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي و ذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات.1

المطلب الثاني : اجراء و آليات الوقاية من المساس بالمعطيات في مجال المعلوماتي

الفرع الأول : اجراءات الوقاية و المكافحة من جريمة المعلوماتية في ضل القانون

لقد خص المشرع الجزائري الجانب الإجرائي من أجل الوقاية و المكافحة من الجريمة المعلوماتية بالاهتمام بدليل أنه أفرد له نصوص قانونية خاصة به و الذي تبنى بموجبها صراحة إجراءات خاصة واستثنائية كالمراقبة الإلكترونية

اولا: الترتيبات التقنية لمراقبة الاتصالات الإلكترونية.

أما فقها فقد اختلفت التعريفات التي تم وضعها لتعريف المراقبة الإلكترونية فقد ذهب اتجاه للقول بأنها: " اجراء تحقيق يباشر خلسة و ينتهك سرية الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها و يتضمن من ناحية استراق السمع و من ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض2"

وهنالك من عرفها بأنها: " تعمد الإنصات و التسجيل و محلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة3"

فالاتصالات الإلكترونية التي تتم من خلال أجهزة و وسائل مختلفة يمكن ضبطها بشكل عام في ثلاثة صور:

1- التصنت
2- اجهزة التسجيل المرئية
3- المراقبة الالكترونية على شبكة الانترنت.[4]

1- القانون 09 /04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.

2- ياسر الأمير فاروق ، المرجع السابق ص 139

3- أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، الطبعة السابعة ،القاهرة ، 1993 .

4 العربي شحط عبد القادر و نبيل صقر ، الإثبات في المواد الجزائية ، دار الهدى عين مليلة الجزائر ص 51.

ثانيا: خصائص مراقبة الاتصالات الإلكترونية

من خلال التعاريف التي قيلت فإننا يمكن أن نستنبط من المراقبة الإلكترونية أربعة خصائص و التي تم الاتفاق عليها فقها و التي تميزها عن غيرها من اجراءات التحقيق و المتمثلة ف ي النقاط التالية:

1- اجراء المراقبة الاتصالات الإلكترونية بصورة سرية:

يعني أن هذا الاجراء استثنائي يباشر خلسة أي في الخفاء دون رضا أو علم صاحب الشأن و علة ذلك المحافظة على خصوصية الأحاديث و سريتها و بالتالي يمكن معه تطبيق كل الضوابط و ضمانات المراقبة و الحماية المقررة قانونا لحماية حق الفرد في سرية مراسلاته و اتصالاته.

2- مساس اجراء مراقبة الاتصالات الإلكترونية بحق الشخص في سرية مراسلاته و اتصالاته الإلكترونية:

من شأن هذه الخاصية أن تكشف عن خطورة المراقبة، فالتنصت على الأحاديث ،الخاصة للإنسان يتيح للمسترق اختراق ذاته و اقتحام عقله و التلصص بأفكاره و نواياه و الوقوف على مشاعره و أحاسيسه وعليه فلا تعد من قبيل المراقبة ضبط الرسائل و الكتابات و شهادة الشهود و الاستجواب إلى غير ذلك من الإجراءات، و المشرع الجزائري على غرار نظيره المصري و كذلك الفرنسي قرن الحق في الحياة الخاصة للفرد بالحق في سرية مراسلاته و اتصالاته الإلكترونية منها.

3-هدف المراقبة الإلكترونية الحصول على دليل غير مادي إلكتروني:

إن الغاية من اللجوء إلى مراقبة الاتصالات الإلكترونية هو الحصول على دليل من شأنه أن يساهم في كشف الحقيقة و تأكيد أدلة الاتهام لأن إسناد الجريمة لشخص معين يقتضي معه إقامة الدليل على صلته بها.

4-الاعتماد في مراقبة الاتصالات الالكترونية على الأجهزة المخصصة لذلك:

أما المشرع الجزائري و بالرجوع لنص قانون 04/09 المتعلق بالقواعد الخاصة بمكافحة جرائم الإعلام و الاتصال و الوقاية منها و باستق ارء المادة 04 المتعلقة بمراقبة الاتصالات الإلكترونية فإنه لم يشترط استخدام أي جهاز لتحقق المراقبة.[1]

1- عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون " دراسة مقارنة " ، الطبعة الثانية ص 372.

المشرع الجزائري من مسألة مشروعية إجراء مراقبة الاتصالات الإلكترونية.

1- **فيما يخص إجراءات المتابعة:** فقد تم إنشاء الأقطاب القضائية المتخصصة في هذا النوع من الجرائم بالإضافة إلى توسيع دائرة الإختصاص المحلي بالنسبة لضباط الشرطة القضائية عبر كامل التراب الوطني فيما يخص جرائم المساس بأنظمة المعالجة الآلية للمعطيات و هذا ما أوردته بالذكر المادة 16 مكرر من قانون الإجراءات الجزائية، و ذلك من أجل تسهيل عمل الضبطية القضائية في إطار البحث و التحقيق عن هذه الجرائم.

2- **فيما يخص توسيع الإختصاص المحلي لوكلاء الجمهورية و قضاة التحقيق:** إن مسألة توسيع الإختصاص المحلي لوكلاء الجمهورية و قضاة التحقيق إلى دائرة ختصاص محاكمة أخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يكون طبقا لنص المادتين 2/37 40و من قانون الإجراءات الجزائية و الذي أتبعه صدور المرسوم التنفيذي رقم06/348 المؤرخ في 05/10/2006 المتضمن تمديد الاختصاص لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق.

3- **فيما يخص إجراءات التوقيف للنظر:** فقد مدد المشرع الجزائري مدة التوقيف للنظر بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات مرة واحدة لمدة 48 ساعة بمعنى أنه يمكن توقيف الشخص المشتبه فيه لمدة 96 ساعة فقط و هذا ما تقضي به المادة 05/51 المعدلة من قانون الإجراءات الجزائية، غير أن الطبيعة المعقدة للجرائم المعلوماتية العابرة للحدود لارتباطها بالتقنية المتطورة يجعل من مهمة البحث و التحري فيها و البحث عن مرتكبيها يستوجب وقتا أكبر و بالتالي فمدة التوقيف في مثل هذا النوع من الجرائم يجب أن تكون كذلك و هو الأمر الذي ينبغي على المشرع الجزائري تداركه

4- **اللجوء إلى إجراءات التحري الخاصة** : فقد أوردها المشرع الجزائري بالذكر ضمن الفصل الربع من الباب الثاني من قانون الإجراءات الجزائية بنص المواد 65 مكرر 5 إلى 65 مكرر 18 منه و التي يمكن اللجوء إلى هذه الإجراءات فيما يتعلق بالتحري في الجريمة المتلبس بها و التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و نوردها كما يلي:

اعتراض المراسلات، التسجيل الصوتي، التقاط الصور [1]

1- بوخبزة- عائشة، الحماية الجزائية من الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق تخصص قانون جنائي، جامعة وه ارن، سنة 8103

الفرع الثاني: آليات الوقاية و المكافحة من الجرائم الماسة بالمعطيات في المجال المعلوماتي

تتشكل الاليات الوقائية والمكافحة من الجرائم الماسة بالمعطيات في المجال المعلوماتي الى الية التعاون على مستوى الضبطية القضائية المنصوص عليها في قانون الاجراءات الجزائية الجزائري

اولا:آلية التعاون الأمني في مجال الوقاية من جرائم الماسة بالمعطيات في المجال المعلوماتي:

الجزائر على غرار الكثير من الدول سعت لتفعيل الجهات الأمنية كألية فعالة يتم الاعتماد عليها من أجل الوقاية و المكافحة من الجريمة المعلوماتية، فجهاز الشرطة عموما هو المكلف بالتحري عن الجرائم و ضبطها و تلقي البلاغات و إجراء التحقيقات الأولية بشأنها و تقديمها للجهات القضائية المختصة لمباشرة الدعوى الجزائية إذا صحت هذه البلاغات أو توافرت الأدلة الكافية للسير في إجراءاتها.1

ثانيا:على مستوى جهاز الدرك الوطني الجزائري:

في سبيل سعي جهاز الدرك الوطني الجزائري للوقاية و التصدي لظاهرة الجريمة المعلوماتية عموما و ظاهرة الإرهاب على شبكة الأنترنت خصوصا وذلك بوضع إستراتجية من خلال إعادة تنظيم هياكلها و تقسيمها حسب الاختصاصات المستجدة بسبب أن الفضاء المعلوماتي أو بيئة الأنترنت باتت تشكل الملاذ الآمن للمجرمين عموما و الإرهابيين على وجه الخصوص.2

الفرع الثالث: الهيئة الوطنية للوقاية من جرائم الماسة بالمعطيات في المجال المعلوماتي

من بين الآليات التي أوجدها المشرع الجزائري في مجال الوقاية و المكافحة من الجريمة المعلوماتية إنشاء هيئة وطنية للوقاية و المكافحة من جرائم الإعلام و الاتصال و مكافحتها و يكمن دورها الأساسي في تنشيط و تنسيق عمل السلطات المكلفة بمكافحة الجريمة الافتراضية و مدها بالمساعدة و الاستشارة اللازمة.

و قد تم استحداثها بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها في نص مادته 15 منه التي تنص:

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.

1- بوخبزة عائشة، مرجع سبق ذكره .

2- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الطبعة الأولى

- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريهابشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال1

الفرع الرابع: التعاون والمساعدة القضائية الدولية المقررة للوقاية من جرائم المساس بالمعطيات في المجال المعلوماتي.

ومما لا شك فيه ان التعاون والمساعدة القضائية الدولية المقررة للوقاية من جرائم المساس بالمعطيات في المجال المعلوماتي المتضمنة العناصر التالية:

1- الإنابة القضائية الدولية.

2- نقل الإجراءات.

3- تبادل المعلومات

4- تبادل الخبرات.

5- تسليم المجرمين.2

1- **أمال قارة**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية 2007 .

2- بوخبزة عائشة، مرجع سبق ذكره

خلاصة:

نستنتج مما سبق من الجانب العملي للحماية الجنائية للمعطيات في المجال المعلوماتي ان للجريمة الماسة بالمعطيات لها اركان مثلها مثل باقي الجرائم الماسة بالحياة الخاصة بالافراد.

وحيث ان المشرع الجزائري عن طريق المعاهدات الدولية والاتفاقيات التي ابرمتها الجزائر لحماية معطيات الخاصة بالافراد في المجال المعلوماتي، وعن طريق القوانين التي نص عليها المشرع الجزائري، حيث اسفرت هاته القوانين بظهور تدابير واجراءات وقائية لحماية المعطيات في المجال المعلوماتي والمتعلقة بالحياة الفرد سواء كان شخص طبيعي او معنوي.

خاتمة

خاتمة

تتعدد أوجه الحماية الجنائية لمستخدمي الإنترنت نظرًا للتحديات الأمنية التي يواجهها المستخدمون في العالم الرقمي. في خاتمة المذكرة ، يمكن تلخيص بعض هذه الأوجه الرئيسية على النحو التالي

حماية البيانات الشخصية: يجب أن يتمتع المستخدمون بحماية قوية لبياناتهم الشخصية عبر الإنترنت. يجب تطبيق القوانين واللوائح المناسبة لحماية البيانات الشخصية ومنع استخدامها أو تسريبها دون إذن.

مكافحة الجرائم الإلكترونية: يجب تكثيف الجهود لمكافحة الجرائم الإلكترونية التي تستهدف المستخدمين على الإنترنت، مثل الاحتيال الإلكتروني والتسلل إلى الأنظمة والاعتداءات السيبرانية. يجب أن تتعاون الجهات المختلفة، بما في ذلك الحكومات والشرطة والمؤسسات الأمنية، لمكافحة هذه الجرائم وتقديم العدالة للمتضررين.

حماية الأطفال ومكافحة الاستغلال الجنسي: يجب أن تتخذ الإجراءات اللازمة لحماية الأطفال على الإنترنت والحد من الاستغلال الجنسي للأطفال والمضايقات الإلكترونية. يتعين تطوير تشريعات صارمة لمكافحة هذه الجرائم وتوفير آليات فعالة للإبلاغ ومعاقبة المرتكبين.

الحماية من التجسس والمراقبة غير القانونية: يجب حماية المستخدمين من التجسس والمراقبة غير القانونية على الإنترنت. ينبغي تنفيذ تدابير تكنولوجية وقانونية لمنع الاختراقات والاعتداءات على الخصوصية الشخصية.

تعزيز التوعية والتثقيف: يجب تعزيز التوعية بمخاطر الإنترنت وتثقيف المستخدمين بشأن الإجراءات الأمنية المهمة. يمكن تحقيق ذلك من خلال توفير مواد تثقيفية وبرامج توعية تستهدف المستخدمين من جميع الفئات العمرية.

التعاون الدولي: يجب تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وحماية مستخدمي الإنترنت. ينبغي أن تتعاون الحكومات والمؤسسات الأمنية والشركات الخاصة لتبادل المعلومات والخبرات وتطوير إطارات قانونية وتقنيات أمنية مشتركة الى جانب الأوجه المذكورة أعلاه، هناك بعض النقاط الأخرى التي يجب أيضًا النظر فيها لضمان حماية مستخدمي الإنترنت:

الحماية من الاحتيال المالي: يجب تعزيز الحماية من الاحتيال المالي عبر الإنترنت، مثل عمليات الاحتيال الائتماني والاحتيال البنكي عبر الإنترنت. يجب توفير إجراءات تحقق قوية، مثل التحقق بخطوتين والتشفير الآمن، لضمان أمان المعاملات المالية عبر الإنترنت.

حماية الملكية الفكرية وحقوق التأليف والنشر: يجب حماية المستخدمين من انتهاك حقوق الملكية الفكرية عبر الإنترنت، سواء كان ذلك في مجال البرمجيات أو المحتوى الرقمي. ينبغي تعزيز تطبيق القوانين وتوفير آليات للإبلاغ عن انتهاكات حقوق الملكية الفكرية ومعاقبة المتجاوزين.

الحماية من التحرش والتنمر عبر الإنترنت: يجب حماية المستخدمين من التحرش والتنمر عبر الإنترنت، سواء عبر وسائل التواصل الاجتماعي أو الرسائل الإلكترونية. ينبغي تشديد القوانين والتدابير لمكافحة هذه الظاهرة وتقديم الدعم النفسي والقانوني للضحايا.

النتائج

بناءً على الأوجه المذكورة لحماية مستخدمي الإنترنت في الحماية الجنائية، يمكن أن توصل دراسة إلى نتائج متنوعة ومهمة. هنا بعض النتائج المحتملة التي يمكن أن تكون جزءًا من الدراسة الخاصة بك:

زيادة الوعي والتثقيف: يمكن أن تظهر الدراسة أن التثقيف وزيادة الوعي بأمور الأمان الرقمي يلعب دورًا حاسمًا في حماية المستخدمين. قد تظهر النتائج تأثير إجراءات التثقيف، مثل حملات التوعية وورش العمل، في تعزيز ممارسات أمان الإنترنت لدى المستخدمين.

القوانين واللوائح: يمكن أن تسلط الدراسة الضوء على الأثر الإيجابي لتنفيذ وتطبيق القوانين واللوائح الخاصة بحماية المستخدمين عبر الإنترنت. قد تشير النتائج إلى فعالية الإطار التشريعي في تقليل حوادث الجرائم الإلكترونية وتحسين حماية البيانات الشخصية.

الابتكار التكنولوجي: قد تسلط الدراسة الضوء على أهمية الابتكار التكنولوجي في تعزيز الحماية الجنائية لمستخدمي الإنترنت. قد توضح النتائج تطبيقات التشفير وحماية البيانات وتقنيات الاكتشاف المتقدمة كأدوات فعالة في مواجهة التهديدات السيبرانية.

التعاون الدولي: قد تظهر الدراسة أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية. قد تبين النتائج أن التبادل الفعال للمعلومات والخبرات بين الدول يؤدي إلى تعزيز الحماية الجنائية للمستخدمين وتحقيق نتائج إيجابية في مكافحة الاعتداءات السيبرانية.

الحاجة إلى تحديثات ومزيد من الجهود: قد تشير الدراسة إلى أن التحديات الأمنية المتعلقة بالإنترنت لا تزال تتطلب تحديثات ومزيد من الجهود. قد توضح النتائج الفجوات الموجودة وتوصي باتخاذ إجراءات إضافية لتعزيز الحماية الجنائية وتطوير.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

1. أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، الطبعة السابعة ،القاهرة 1993 .

2. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية 2007 .

3. بعيش تمام شوقي، كتاب الجريمة المعلوماتية، دراسة تأصيلية مقارنة، جامعة مُحَمَّد خيضر، كلية الحقوق والعلوم السياسية مخبر اثر الاجتهاد القضائي على حركة التشريع سنة2019

4. بن غدفة شريفة و القص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنات وطرق محاربتها ،أوعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر ،29مارس 2017

5. بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق تخصص قانون جنائي، جامعة وهران، سنة 2008.

6. تجميل عبد الباقي الصغير: القانون الجنائي والتكنولوجية الحديثة الكتاب الأول: الجرائم الناتجة عن استخدام الحاسب الآلي. دار النهضة العربية القاهرة 1992.

7. حسام الدين الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم الاقتصادية، كلية الحقوق، جامعة عين شمس ،بحث مقدم إلى مؤتمر القانون والحاسب الآلي في الكويت، نوفمبر 1989

8. حمزة بن عقون ،نفس الرسالة، ص14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية،

9. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الطبعة الأولى

10. رضا قولي عثمان، المشكلات العلمية و القانونية للجريمة المعلوماتية في العصر الرقمي انظر الجريدة الرسمية رقم 5584 الصادرة يوم الخميس 6 دجنبر 2008.

11. سعيداني نعيم ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ،2012 -2013،

12. سميرة بيطام،الجريمة الإلكترونية وتقنية الإجرام المستحدث .

13. سوبر سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلوم الاجرام، كلية الحقوق، جامعة ابو بكر بالقايد، تلمسان، 2010-

14. الصعيد العربي هناك دول قد أصدرت قوانين لمكافحة الجريمة الالكترونية، بينما أن دول أخرى عملت على سد الفراغ التشريعي الحاصل في مجموعة القانون الجنائي فيما يتعلق بتجريم الأفعال المرتبطة بتكنولوجيا المعلومات، ووضع العقوبات الملاءمة لها.

15. صغير يوسف ،الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال ،جامعة مولود معمري، تيزي وزو ،2013/03/06،نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها مجلةصادرة عن مديرية الأمن الوطني، العدد84، 2007

16. عادل عية الجواد، الانترنت والاجرام، المنظم، مجلة الامن والحياة، العدد 303، 26 سبتمبر 2007

17. عبد الفتاح مراد، شرح التحقيق الفني والبحث الجنائي، (د ط) الكتب والوثائق المصرية، 2006

18. العربي شحط عبد القادر و نبيل صقر ، الإثبات في المواد الجزائية ، دار الهدى عين مليلة الجزائر

19. العربي قندوز واخؤون، جرائم الحاسوب، مذكرة مقدمة للتخرج دفعة الاثنية لمفتشي الشرطة، مدرسة الشرطة طيبي العربي، سيدي بلعباس، الجزائر، 2008

20. عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون " دراسة مقارنة " ، الطبعة الثانية

21. علي كريمي: تطور قوانين الإعلام في الدول المغاربية "ورقة مقدمة في الحلقة الدراسية المنظمة من طرف الإيسيسكو يونيو 2009 بطرابلس ليبيا"

22. عمر مُحَّد بن يونس: مشكلة قواعد البيانات، موسوعة التشريعات العربية ، دار الفكر الجامعي: الاسكندرية: 2004.

23. عمر نجوم: الحجية القانونية لوسائل الاتصال الحديثة: دراسة تحليلية في نظام الإثبات المدني. أطروحة لنيل الدكتوراه: كلية الحقوق الدارالبيضاء

24. غزة على مُحَّد الحسن: قانون الانترنت، شركة مطابع السودان للعملة: رقم الإبداع 404/2005

25. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية ،»طرابلس.

26. كامل فريد السالك ،الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب ،23/21/تشرين الأول ،2000،

27. مالك خدام: جرائم الحاسب والانترنت... ارتفاع معدل استغلال الأطفال جنسيا جريدة الثورة: الاثنين 2005/3/7

28. مُحَمَّد أمين أحمد الشوابكة ،جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن ،2004، ط 1،

29. مُحَمَّد زكي ابو عامر، علي عبد القادر، قانون العقوبات .، القسم الخاص، (د ط)، دار النهضة العربية، القاهرة، 1993

30. نمديلي رحمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، كلية الحقوق والعلوم السياسية –جامعة مُحَمَّد لمين دباغين سطيف الجزائر 2، كتاب اعمال مؤتمر الجرائم الالكترونية طرابلس لبنان يومي 24و25 مارس 2017

الاطروحات والمذكرات :

31. لعقال فريال الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر ، قانون جنائي ، جامعة اكلي محند اولحاج البويرة سنة 2015،

32.حمزة بن عقون ،السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة ،2012/2011، ص 13، نقلا عن قورة نائلة، جرائم الحاسب الإقتصادية، القاهرة ،2004.

33. مُحَمَّد أحمد: حقوق الإنسان بين الخصوصية والعالمية، رسالة لنيل دبلوم الدراسات العليا المعمقة: كلية الحقوق الدار البيضاء 2003

34. نزلي بشرى ، اثبات الجريمة الالكتنرونية ، مذكرة ماستر ، جامعة ورقلة ، كلية الحقوق و العلوم السياسية ، 2018

المجلات والجرائد

35. لورنس سعيد الحوامدة، ''الجرائم المعلوماتية أوركانها وآلية مكافحتها'' دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن ،2016/08/13،

36.لورنس سعيد الحوامدة، الجريمة المعلوماتية اركانها والية مكافحتها دراسة تحليلية مقارنة مجلة الميزان للدراسات الاسلامية والقانونية 2007

37. معاشي سميرة مفهوم الجريمة المعلوماتية –دراسة تحليلية–جامعة مُحَمَّد خيضر بسكرة، مجلة المفكر العدد 17 ، 2018

38. مليكة عطوي، ا لة السابقة الذكر، ص 09، نقلا عن الطاهر رواينية، المسائلة، مقال، العدد 01، 1991

39. نشناش منية، الركن المفترض في الجريمة المعلوماتية، ورقة بحثية قدمت في الملتقى الوطني المتعلق بالجريمة المعلوماتية بين الوقاية والمكافحة المنظمة من قبل قسم الحقوق والحريات في الانظمة المقارنة، بكلية الحقوق والعلوم السياسية بجامعة بسكرة، يومي 16-17 نوفمبر 2015.

المراجع باللغة الأجنبية

40. PHILIPPE AIGRAIN : Au-delà du logiciel libre, le temps des biens communs : le monde diplomatique, Octobre 2005

41. Rachid BOUTI : les enjeux du commerce électronique pour les commerçants : cybers PME-PMI artisans on line, REMALD, sirie études, n°50, Mai-juin 2003.

42. Nouri LAJMI : « la liberté de l'information à l'ère du cyberespace », Revue Tunisienne de la communcation n° 37-38, Janvier/ décembre 2001

المواقع الالكترونية

http://www.al-fadjr.com/ar/realite/3531.html

رضا قولي عثمان، المشكلات العلمية والقانونية للجريمة المعلوماتية في العصر الرقمي

http://www.al-fadjr.com/ar/realite/3531.html

Verboteme Schriften im internet, Juristiche Rundschau, 1997, S496. Redbruch (Gustav).

htt//www.alaraby.co.uk/media news.

culture/net.alukah.www//http/br

https:/www.upn.go.govs

43. القانون 09 /04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.
44. قانون حماية الكمبيوتر: بين تبادل المعلومات وحماية الابداعجريدة المساء: عدد 535 السبت/ الأحد 7/6 يونيو 2008.
45. القانون رقم ،04 -15، الصادر في 10 نوفمبر2004، يعدل ويتمم الأمر رقم156/66، الصادر في 08جوان 1966، المتضمن قانون العقوبات، ج رالعدد 71.
46. القانون رقم 09 -04، الصادر في 05أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر العدد 47.
47. القانون رقم03-07 القاضي بتتميم مجموعة القانون الجنائي فيما يتعلق بالجزائر المتعلقة بنظم المعالجة الالية للمعطيات الصادر بتنفيذ الظهير الشريف رقم 197-03-1 بتاريخ 16رمضان1424 الموافق ل 11نوفمبر 2003 بالج. ر العدد 5171 بتاريخ 22ديسمبر 2003 الموافق ل 27 شوال 1424،
48.قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015 الصادر يوم الاحد يوليو 2015 العدد 1244.

فهرس الموضوعات

كلمة شكر

اهداء

الفصل الأول:

الفصل الثاني

الحماية الجنائية المقررة لمستخدمي الانترنيت