تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الالكترونية في العالم والجزائر

أ. قصعة خديجة جامعة قسنطينة 03
د. جمال بن زروق جامعة سكيكدة

الملخص:

تهدف هذه الدراسة إلى التعريف بالجريمة الإلكترونية، وتوصيفها ،و تمييزها و تبيان خصوصيتها مقارنة بالجريمة التقليدية في الفضاء الحقيقي أو مسرح الجريمة ، و كيف أن خصوصيتها تتطلب جهدا ماديا وتقنيا و بشريا و قانونيا مضاعفا لا بل حتى تظافرا للجهود الدولية و الإقليمية فهي من الجرائم العابرة الحدود،ثم إن مرتكبيها ليسووا مجرمين عاديين و إنما لديهم خصوصيات نفسية و معرفية لا سيما في مجال التكنولوجيات و الشبكات أو ما يتعلق بأنظمة معالجة المعلومات فمكان حدوثها الذي يرتبط بالأنظمة المعلوماتية والحاسبات أو الأنظمة في حد ذاتها كمسرح للجريمة والفضاء الافتراضي بحدوده غير المعرفة و المتشابكة يصعب من متابعتها و تقفي أثر مرتكبيها و جمع الأدلة الجنائية و من تكييف العقوبات مع طبيعة الجرم المرتكب.و لهذا سنت الدول ومن بينها الجزائر مجموعة من القوانين و التشريعات التي تسهم في المواجهة و التصدي لهذا النوع من الجرائم ومحاولة ردع مرتكبيها من خلال عقوبات تتراوح بين غرامات مالية و السجن.

الكلمات المفتاحية :الجريمة ،الجريمة الالكترونية ،الحماية القانونية .

Summary

This study aims to identify and characterize the electronic crime. It distinguishes and show its specificity as well in comparison to conventional crime in the real space or the scene of the crime and double financial, technical, human and legal efforts it's specificity requires ,not only that but also the collaboration of regional and international efforts because the electronic crime is a cross-border crime. The perpetrators of this crime are not common criminals but rather ,they have cognitive and psychological specifications especially in the field of technologies and networks or what is related to the processing system of information .its place occurrence that is linked to the computing informatics systems themselves as a crime scene .the virtual space with its unidentified dimensions makes it difficult to follow up it and track down its perpetrators and collection of criminal evidence and the conditioning of penalties with the nature of the offence this led countries including Algeria to edict a set of regulations and legislations that contribute to the confrontation to this type of crimes and an attempt to deter the perpetrators through penalties ranging from fines and imprisonment.

مقدمة:

شهدت البشرية خلال قرون مضت العديد من التطورات والتغيرات والثورات فلم تكتف بالثورة الزراعية بل أردفتها بالثورة الصناعية، وصولا إلى ثورة تكنولوجيا المعلومات والاتصالات ثم إلى ثورة المعرفة واقتصاد المعلومة التي أصبحت مصدر سلطة ورأس مال لا ينضب أسال لعاب الطامعين من صائدي الفرص والكنوز، فمنذ ولادة تكنولوجيا المعلومات ترافقت مع صور إجرامية جديدة ارتبطت بالاعتداء على المعلومات ، وأنظمتها وبيئتها عن طريق الحاسوب الآلي والانترنت فكانت الجرائم الإلكترونية والمعلوماتية التي تمثل فعلا غير مشروع بالتعدي على المعلومات و أنظمتها في بيئتها عن قصد أو عن غير قصد بالنسخ أو التعديل أو الولوج غير المشروع وغيرها من الأفعال التي تستهدف المساس بالمعلومات و أنظمتها أو الأمن على الشبكة أو تطال الأفراد والمؤسسات ، ومعها مجرم جديد ذكي رقمي إلكتروني قادر على الولوج إلى مواقع أضخم المؤسسات الحكومية والبنوك والمصارف ذكي بإمكانه اختراقها وحجبها وتخريبها ليس بحاجة لرخصة لنسخ وتقليد ما شاء من برمجيات ومعلومات، إنه قرصان إلكتروني لا يحتاج سفينة أو سلاح.

هذا النوع من الجرائم يشكل تهديدا للأفراد و المؤسسات والحكومات فهو يتعلق أيضا بأمنها القومي و هذا ما يجعل من مسألة التأمين لمعلوماتها و حمايتها مطلبا حتميا ما يستدعي تطوير الأنظمة المعلوماتية في مجال أمن المعلومات،كما أن هذا

النوع من جرائم المعلوماتية له سمات خاصة و كذا مرتكبيه فإنه أيضا يستوجب المعاملة بقوانين وتشريعات خاصة وملاحقته في بيئته، و تظافر الجهود الدولية في مواجهته .

من خلال ما تم عرضه يمكن طرح التساؤل الرئيسي الآتي :ما دور تفعيل آليات الحماية القانونية في الحد من الجريمة الالكترونية في العالم و في الجزائر ؟

ويقودنا هذا التساؤل إلى مجموعة من الأسئلة الفرعية هي:

- ✓ ما هي الجريمة الالكترونية و ما أنواعها ؟
- ✓ ماهي أهم التجارب الدولية في مجال الحماية القانونية في العالم ؟
- ✓ ما هي القوانين الجزائرية في مجال الحماية القانونية لمواجهة الجريمة الالكترونية ؟

يتسم هذا الموضوع بأهمية بالغة لارتباطه بمجال حساس وهو المعلومة وتأمينها من الأخطار لا سيما كونها عصب الحياة في عصرنا الحالي ،و الاهتمام بها في مختلف المستويات الفردية أو الحكومية أو من قبل المنظمات الإقليمية والدولية و في شتى المجالات الاقتصادية و السياسية و الإدارية و غيرها من المجالات و القطاعات ، ففي ظل تنامي معدلات الجريمة الالكترونية و انتشارها إما بالتعدي على المعلومات بالحذف أو التعديل أو الدخول غير المشروع أو الاختراق أو الحجب و التعطيل ...الخ .كما أن خصائص الإبحار على الشبكة العالمية و إتاحتها بمجرد أن تكون موصولا بالانترنت ساهمت في الانتشار الواسع ضف إلى الخصائص الأخرى التي تجعل من الصعوبة متابعة هذه الجرائم و تقفي أثر مرتكبيها مما يستدعي تكاثف الجهود لمواجهة هذه الجرائم العابرة للحدود و تفعيل آليات الحماية القانونية من أجل ردع مرتكبيها و الحد منها .

ويهدف هذا الموضوع إلى توضيح أهمية آليات الحماية القانونية و التشريعات في الحد من الجرائم الالكترونية التي تشهد تناميا ملحوظا مست آثاره الحياة الخاصة للأفراد و المؤسسات الاقتصادية وأسرار المؤسسات الحكومية مما شكل تهديدا قوميا لأمن الدول في مرات عدة وهذا من أجل تحقيق مطلب الأمن المعلوماتي .

منهج البحث: سنعتمد في هذا الموضوع على المنهج الوصفي التحليلي للوصول إلى الهدف من الدراسة ،و يعتبر هذا المنهج الأنسب لدراستنا من أجل توصيف الظاهرة الجريمة الالكترونية و الكشف عن الأسباب المتعلقة بها كمشكلة و ظاهرة إنسانية وهذا باعتمادنا على مجموعة من الكتب و الدراسات و كذا إحصائيات،ومنه الوصول إلى استنتاجات تساهم في معالجة الموضوع .

1-الجريمة الإلكترونية، الماهية والأنواع:

1- الجريمة ألإلكترونية إن الجريمة عموما هي سلوك إنساني غير سوي[1] يستوجب العقاب أمَّا الجريمة الإلكترونية فلها مسميات كثيرة فهي الجريمة المعلوماتية ،جرائم الفضاء الافتراضي، جرائم الكمبيوتر والانترنت، جرائم مجتمع المعلومات و جرائم مجتمع المعرفة، جرائم مجتمع ما بعد المعلومات،وعلى اختلاف التسميات وبتعدد مداخل الدراسات وزاياها الفقهية والتقنية والمعلوماتية والقانونية تعددت التعاريف وسنورد منها ما يأتي:

أ- التعريف الفقهي: يميل أصحاب هذا الموقف إلى القول بأن الجريمة المعلوماتية هي: نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[2]،وهذا التعريف يجعل من الجريمة الالكترونية كل فعل غير مشروع يرتبط بالحاسب الآلي كأداة أساسية في الجريمة أو كمعتدى عليه .

ب- أمَّا في الفقه الجنائي: فجرائم الحاسب الآلي هي جرائم الاستخدام غير المشروع للحاسبات[3]وهذا التعريف بقدر ما هو مقتضب إلا أنه شامل فتعدد استخدامات الكمبيوتر يعني تعدد أنواع الجرائم المقترفة ومجالاتها.

ت- التعريف التقني: قدمت مكتب تقييم التقنية في الو.م.أ تعريفا للجريمة المعلوماتية من خلال تعريف جريمة الحاسب الآلي بأنها: الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا [4].

هذه التعاريف كلها تتفق على عنصر وحيد رئيسي لمفهوم الجريمة الإلكترونية وهو الحاسب الآلي كأداة لكنه أيضا قد يكون معتدى عليه أو بيئة الجريمة.وعليه سنقدم تعريفات أكثر دقة وشمولا منها:

- يعتبرها كل من Jack Bologna Robert و J Lindquist جريمة يستخدم الحاسوب كوسيلة Mens أو أداة instrument لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها[5]

- يعرفها أمير يوسف فرج "مستشار قانوني": الجريمة المعلوماتية هي كل استخدام في صورة فعل أو امتناع غير مشروع لتقنية المعلوماتية ويهدف الاعتداء على أي مصلحة مشروعة سواء كانت مادية أو معنوية [6]

2-أنواع الجريمة الإلكترونية والمعلوماتية: على اعتبار أن ثورة المعلومات وتكنولوجياتها، قد مست كل المجالات وكل القطاعات الاقتصادية والإنتاجية وخدمات فإن الجريمة أيضا تعددت وتنوعت وتلونت بلون مجالاها فاستهدفت الأشخاص والمؤسسات والحكومات لا بل حتى الحياة الخاصة وأسرارها، وعليه سنقدم التصنيفات التالية:

1-تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة: هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات وهو التصنيف الذي يعكس أيضا التطور التاريخي لظاهرة جرائم الكمبيوتر والانترنت ونجد حسب هذا المعيار الأنواع التالية:

أ- الجرائم الماسة بقيمة معطيات الحواسب: وهي أولا الجرائم الواقعة على ذات المعطيات كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة التقنية الفيروسات وثانيا الجرائم الواقعة على ما تمثله المعطيات آليا، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات وجرائم التحرير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة، آليا واستخدامها).

ب-الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة [7]

ت-الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه: جرائم قرصنة البرمجيات، التي تشمل نسخ وتقليد ما يتوفر على الشبكة من إنتاج فكري وأدبي دون ترخيص والاعتداء على العلامات التجارية وبراءة الاختراع.

وقد ترتب على نشاط الجاني خسائر مادية غير محددة تتجاوز الضرر المترتب على ارتكاب جريمة من الجرائم التقليدية [8]

2- تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة : الاتجاه العالمي الجديد يقسمها إلى جرائم هدف ووسيلة ومحتوى وأفضل ما يعكس هذا الاتجاه أي التقسيم، الاتفاقية الأوربية لجرائم الكمبيوتر والانترنت لعام 2001، حيث أن العمل منذ 2000 يتجه إلى وضع إطار عام لتضيق جرائم الكمبيوتر والانترنت وعلى الأقل وضع قائمة الحد الأدنى في محل التعاون الدولي، وعليه أوجدت هذه الاتفاقية أربع طوائف جديدة :

أ- الجرائم التي تستهدف عناصر السرية والسلامة والموفورية ، المعطيات والنظم وتضم:

- الدخول غير قانوني(غير مصرح به) – الاعتراض غير القانوني تدمير المعطيات، اعتراض النظم، إساءة استخدام الأجهزة.

ب- الجرائم المرتبطة بالمحتوى : وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

ج- الجرائم المرتبطة بالكمبيوتر .

د- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة قرصنة البرمجيات.[9]

3- صفات القائم بالجريمة الإلكترونية : تختلف الجريمة الإلكترونية عن الجريمة التقليدية في أساليبها وبيئتها، وكذا مرتكبها فلم يعد ذلك الجاني أو المجرم أو اللص أو السارق الذي يعتدي ويحمل أسلحة مادية. هذه المرة إنه لص ذكي سارق إلكتروني قرصان لا يحمل سيفا، لكنه يملك برمجيات وقادر على تفخيخ وتحطيم واختراق وحجب أي موقع، انه يصنع فيروسات شبيهة بفيروس فقدان المناعة لكنها معلوماتية إن صح القول والتشبيه.

إن التسلل HACKING إلى داخل أجهزة الحاسب الالكتروني بنية الإزعاج أو سرقة البيانات أو تشويه المعلومات الموجودة عليه أمر مرعب للشركات والأفراد أما القائمين بهذه الجرائم فيمكن تصنيفهم كالآتي: المتطفلون ومحبو المال والمحترفون.

1- المتطفلون: مجموعة من الناس الذين يحاولون التسلل إلى الحاسبات الإلكترونية أو الانترنت لغرض إثبات مقدرتهم أو تحديهم أو لمجرد المزاج وليس لغرض الكسب المادي كهدف أساسي.

2- محبو المال: وهم مجموعة من الناس من داخل المؤسسات أو الشركات الذين يحاولون التسلل إلى الحاسبة الإلكترونية لغرض سرقة المال واغلبهم من المبرمجين الموهوبين والأذكياء الذين يعرفون كيف يكتبون البرامج بذكاء لمساعدتهم على سرقة المال أو الاحتيال بمساعدة الحاسبة لسرقة الأموال من المصارف ومؤسسات الأعمال.

3- المحترفون: وهم مجموعة من الناس الذي يحاولون التسلل إلى الحاسبة الإلكترونية لغرض سرقة معلومات قيمة جدا وحساسة وسرية والدوائر الحكومية والعسكرية هي إحدى الجهات الرئيسية التي تحتفظ بملفات سرية ومهمة ومن الصعوبة في هذا النوع من الجرائم حماية المعلومات[10] كما يتصف هؤلاء بسمات معينة :

أ- أعمارهم ما بين 18- 46 سنة عادة والمتوسط العمري لهم 25 عاما.

ب-المعرفة والقدرة الفنية الهائلة.

ت-الحرص الشديد وخشية الضبط وافتضاح الأمر.

ث-ارتفاع مستوى الذكاء ومحاولة التخفي.

4.أشكال العلاقات و القواعد للتشريعات القانونية المتأثرة بتقنية المعلومات:

1-أثر تقنية المعلومات: القانون المدني والإثبات التجاري،التعاقد الالكتروني والإثبات الالكتروني، التجارة الالكترونية ونقل التكنولوجيا المنظم ضمن القانون التجاري.

_ الملكية الفكرية = حماية المصنفات الرقمية بأنواعها ومسائل نقل التكنولوجيا والأسرار التجارية.

_ تشريعات البنوك= البطاقات الالكترونية والدفع الالكتروني والبنوك.

_ القانون الجنائي والموضوعي والإجرائي= جرائم الكمبيوتر والانترنت والقواعد الجنائية الإجرائية.

_ حقوق الإنسان= حماية الخصوصية والحق في الوصول إلى المعلومة.

_ الاستثمار والتجارة الدولية= الأسواق المالية الالكترونية وتحرير الخدمات وتشجيع الاستثمار.

_ التعليم والتأهيل= التعليم الالكتروني والتعليم عن بعد.

_ الخدمات والمصالح الحكومية= الحكومة الالكترونية.

ـ التنظيم القطاعي وحماية المستهلك= المعايير والمواصفات والتشفير وتنظيم قطاعات الاتصالات وتقنية المعلومات وحماية المستهلك ووسائل المنافسة ومنع الاحتكار.

ـ الإعلام والإعلان= النشر الالكتروني والإعلان الالكتروني.

ـ الأتمتة القانونية= أتمتة النظام القضائي وإدارة خدمات المحاماة والتسويات الالكترونية.[11]

2- الجريمة الإلكترونية لمحة عن تجارب بعض الدول في مواجهة الجريمة الإلكترونية والمعلوماتية في مجال التشريعات والحماية القانونية:

سنقوم باستعراض الأنظمة والتشريعات الخاصة بالجريمة الإلكترونية في مجموعة من الدول يذكر (الشوابكة 2004) أن المشرع الفرنسي أصدر القانونين الخاصة بحماية المعلومات على الشبكة العالمية للمعلومات والتي تكون محلا للاعتداء ويضيف أن المشرع الأمريكي أصدر القوانين الخاصة في التصدي للجرائم باستخدام تلك التقنية ويوقع العقوبة على جرائم القذف والسب وانتهاك الآداب العامة.ويذكر Lessiy أن تقنية المعلومات والاتصال لها دور فعال في خلق فرع آخر من القانون وأهمية بالغة في وقتنا الحاضر لحماية المعلومات والبيانات المتدفقة عبر الشبكة العالمية للمعلومات.

1- في و.م.أ: النظام الأمريكي يسمح للأشخاص أو المؤسسات التي تم الاعتداء على حواسبهم بتفويض السلطات لمراقبة تحرك المعتدين وبالتالي تتولى السلطة متابعة اتصالات المعتدي التي بثها إلى تلك الأجهزة المحمية Protected Computer وعند طلب التفتيش بواسطة المعتدي عليه لابد من توافر: يجب أن يحول المعتدي عليه لمراقبة المعتدي ومن الأفضل الحصول على موافقة كتابية أو من وكيله.

- يجب أن يكون المراقب لتلك الاتصالات عضوا في لجنة التحقيقات .

- يجب أن تتوافر لدى مراقب الاتصالات المعرفة حتى يتمكن من أن الاتصالات التي تحدث لها علاقة في الجريمة.

- يجب أن تكون المراقبة خاصة بالاتصالات من و إلى منتهك الحاسوب[12] وإذا لم يكن تفادي الاتصالات الأخرى فيجوز مراقبة جميع الاتصالات.

- عندما يتم الحصول على الدليل الإلكتروني في خارج حدود الو.م.أ تخزن في أي جهاز حاسوبي أو بواسطة الخدمة ، فال،م،أ، تسعى للحصول على الدليل بواسطة رجال الضبط القضائي وهذا على النحو التالي:

1- موافقة الدول الأجنبية على التحقق مع متردد الخدمة أو صاحب ذلك الجهاز.

2- موافقة Office,Ofinternational Affair : مكتب الشؤون الدولية مع وزارة العدل الأمريكية.

وحسب المشرع الأمريكي فالجرائم الإلكترونية محددة على النحو التالي:

1- من يتجاوز الصلاحيات المخولة له بالدخول إلى الحاسب الآلي والدخول العمد غير مصرح به، وحصل بناء عليه على معلومات تسيء إلى الو.م.أ أو تم نقلها عمدا لدول أجنبية بغرض إلحاق الضرر بالو،م،أ، أو تسليمها لأشخاص آخرين أو الاحتفاظ بها أو عدم تسليمها إلى الأشخاص المخولين باستلامها.

2- الوصول إلى الحاسبات المحمية بمعرفة وبقصد الغش بدون إذن شرعي .

3- ككل من يلجأ إلى حاسب آلي محمي وبدون إذن شرعي ويكون من نتائجه الإضرار بالمنشأة.

4- التهديدات الخاصة بالحسابات المحمية والذي له دور في التأثير على نقل أي اتصالات خاصة بالتجارة بين الدول أو التجارة الخارجية الأمريكية وتتراوح العقوبات لمرتكبي الجرائم ما بين غرامة مالية أو الحبس الذي يصل 10 سنوات أولهما معا[13]

2- فرنسا:إن الموجات التشريعية بدأت في حقل ما يعرف بتنظيم الأمن المعلوماتي والمعايير التقنية وتحديدا ما يتصل بتشفير البيانات التي انطلقت من فرنسا في عام 1990[14] وقد سبقه قبل ذلك الإثارة صراحة إلى البرمجيات ضمن المصنفات المشمولة بالحماية في القانون رقم (85- 660) المؤرخ في 03 يوليو 1985 [15]، وينص التشريع الوارد في الجزء 3 الخاص في الاعتداء على أنظمة المعلومات :

1- أي نشاط من شأنه التحايل على النظام الآلي والدخول إلى جميع أجزاء النظام أو جزء منه يتعقب بالسجن لمدة تصل إلى سنة وغرامة 100000 فرنك فرنسي.

2- أي نشاط يعيق أو يعطل أو يدمر وظائف النظام الآلي تنص المادة بالسجن 3 سنوات وعقوبة تصل إلى 300000 فرنك فرنسي.

3- أي نشاط إلى تقديم بيانات إلى النظام معالجة البيانات أو التحاليل لطمسها أو تعديلات فالعقوبة تصل للسجن لمدة 3 سنوات وغرامة مالية تصل 200 ألف فرني فرنسي .

4- أي مشاركة جماعية أو اتفاق للتعامل أو التعاون فكريا بواسطة أنشطة مادية يتم تطبيق ما ورد في المواد 3،2،1.

4- الإمارات العربية المتحدة (إمارة دبي):أصدرت إمارة دبي قوانين خاصة في مجال الجريمة الإلكترونية بتاريخ 30 ذي العقدة 1422م و تنص على:

1- يعاقب كل من أفشى متعمدا المعلومات أو المستندات أو المراسلات الإلكترونية المؤتمن عليه بحكم السلطات الممنوحة بالحبس وبغرامة لا تتجاوز 100 ألف درهم أو إحداهما وعند ما يتم إفشاء هذه المعلومات بسبب الإهمال يعاقب بغرامة لا تتجاوز 100 ألف درهم.

2- عندما يتم استخدام وسيلة الكترونية لتنفيذ جريمة فان العقوبة تنص على الحبس لا تتجاوز 6 أشهر وبغرامة مالية لا تتجاوز 100 ألف درهم وعندما يكون هناك عقوبة اشد في أي قانون آخر يتم الأخذ بالعقوبة الأشد.

كما أصدرت الإمارات العربية المتحدة تشريعات خاصة أخرى، ويعتبر القانون الاتحادي لعام 2006م أحدها على ما يلي:

- عقوبة بالسجن لمدة سنة وغرامة مالية لا تقل عن 50 ألف درهم لأي شخص اعتدى على القيم والمبادئ الإسلامية أو من اعتدى على الحياة الخاصة أو العائلية بنشر الصور أو اعتدى على حرمتها.
- كل من استخدام الوسائل التقنية للاستيلاء على الأموال مثل سرقة بطاقة الفيزا يعاقب بالسجن لمدة سنة وغرامة مالية.
- في حالة اختراق المواقع تكون العقوبة على النحو التالي:
- يعاقب بالسجن مدة ستة أشهر وغرامة مالية لمن تلف بيانات الموقع.
- يعاقب بالسجن مدة لا تقل عن سنة وغرامة عشرة آلاف درهم.
- يعاقب بالسجن والغرامة لكل من بزور المعلومات بالمتدفقة في نظم المعلومات .
- يعاقب بالغرامة مدة لا تزيد عن 10 سنوات والغرامة لكل مستخدم شبكة المعلومات أو وسائل تقنية لابتزاز أي شخص.
- يعاقب بالسجن لمدة سنة وغرامة لا تتجاوز 30 ألف درهم لم يتجسس على الوسائل الالكترونية[16].
- كما تم إعداد اتفاقية المجلس الأوربي لمكافحة الجريمة الافتراضية التي انضمت إليها كل من الو.م.أ(تصديق) وكندا واليابان وجنوب إفريقيا (توقيع دون تصديق)، وهي حاليا الاتفاقية الدولية المرجعية، وقد تمت تكملة الاتفاقية ببرتوكول

إضافي يتعلق بتجريم الأفعال ذات الطابع المعادي للأجانب والطابع العنصري، المرتكبة عن طريق الأنظمة المعلوماتية(28-09-2003م بستراسبورغ)، كما تم أيضا إعداد مشروع بروتوكول يتعلق بتجريم الرسائل الإرهابية وفك ترميزها.

3- الجريمة الإلكترونية في الجزائر وإطارها التشريعي: تعتبر الاتفاقيات الدولية المشار إليها سابقا، مرجعية للقانون الجزائري ومن أهم مصادره، خاصة فيما يتعلق بتعريف وتحديث المصطلحات التقنية وحسب القانونيين والمختصين فالتشريع الجزائري من أحدث التشريعات وأكثرها انسجاما مع المعايير الدولية.

1- الفضاء القانوني للجريمة الإلكترونية والمعلوماتية في الجزائر:

يشمل الإطار القانوني المتعلق بجرائم المعلوماتية نصوص قانونية مختلفة:

أولا:قانون العقوبات: المعدل بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2010 .

تم بموجب هذا القانون إحداث قسم جديد في قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وأحتوى أهم الجرائم التي تستهدف أهم الأنظمة المعلوماتية وهي:

الجرائم المنصوص عليها في المادة 394 مكرر:الدخول خلسة للأنظمة المعلوماتية،البقاء غير المشروع في الأنظمة المعلوماتية، تعديل أو حذف معطيات المنظومة نتيجة الدخول غير المشروع، الإضرار بنظام تشغيل المنظومة على اثر الدخول أو البقاء غير المشروع.

2- الجرائم المنصوص عليها في المادة 394 مكرر 1: إدخال المعطيات في منظومة معلوماتية خلسة، إزالة أو تعطيل معطيات في منظومة معلوماتية خلسة.

3- الجرائم المنصوص عليها في المادة 394 مكرر 2 : القيام عمدا وخلسة بتصميم أو بحث أو تجميع أو توفير أو نشر معطيات تمكن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

4- الجريمة المنصوص عليها في المادة 394 مكرر 3: ارتكاب الجرائم سالفة الذكر إضرار بالدفاع الوطني أو الهيئات أو المؤسسات الخادعة للقانون العام.

ثانيا: قانون الإجراءات الجزائية:المعدل بموجب القانون 04-14 المؤرخ في 10-2004 تناول موضوع الجرائم الافتراضية من خلال:

1- إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجازا لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات(المواد 37 ،40، 329) .

2- تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني (المادة16).

3- التنصيص على قواعد استثنائية في التفتيش:(جواز التفتيش في المحلات السكنية وغير السكنية بناءا على إذن مسبق من وكيل الجمهورية المختص المادة 47) والتفتيش داخل المساكن دون حضور المشتبه فيه ودون شهود (المادة 45 الفقرة الأخيرة) هذه القواعد الاستثنائية لا تعفي من اتخاذ التدابير اللازمة لاحترام السر المهني عند التفتيش.

4- إمكانية استعمال أساليب خاصة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات (اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، التقاط وتثبيت وبث وتسجيل الكلام وصور الأشخاص في الأماكن الخاصة)، والتسرب.

5- التنصيص على إمكانية تمديد فترة التوقيف للنظر المحددة ب 48 ساعة مرة واحدة.

ثالثا:القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:(القانون09-04 المؤرخ في 05 أوت2009): جاء هذا القانون بقواعد للوقاية ودعم وسائل مكافحة الجرائم الافتراضية من خلال رصدها المبكر وجمع الأدلة عنها ويتلخص أهم ما ورد فيه فيما يلي:

1- تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: المادة 02 جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة بقانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

– وضع تعريفات تقنية للمنظومة المعلوماتية والمعطيات المعلوماتية ، ومقدمي الخدمات والمعطيات المتعلقة بحركة السير والاتصالات الإلكترونية.- وضع قواعد خاصة تجيز مراقبة الاتصالات الإلكترونية(المادتان 03و 04) في الحالات التالية: الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. في إطار تنفيذ طلبات التعاون القضائي الدولي.- قواعد خاصة بتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية (المواد من 5 إلى 9) .- التزام مقدمي الخدمات بالمساعدة(المادة10).- إنشاء هيئة وطنية لتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الإلكترونية ومدها بالمساعدة والاستشارة اللازمة (المادة14) كما جاءت المواد (11-15-16-17) في نفس هذا السياق اما المادة (18) فأشارت إلى إخضاع التعاون الدولي لقيود عدم المساس بالسيادة الوطنية والنظام العام مع جواز التعاون بشرط المحافظة على سرية المعلومات المبلغة.

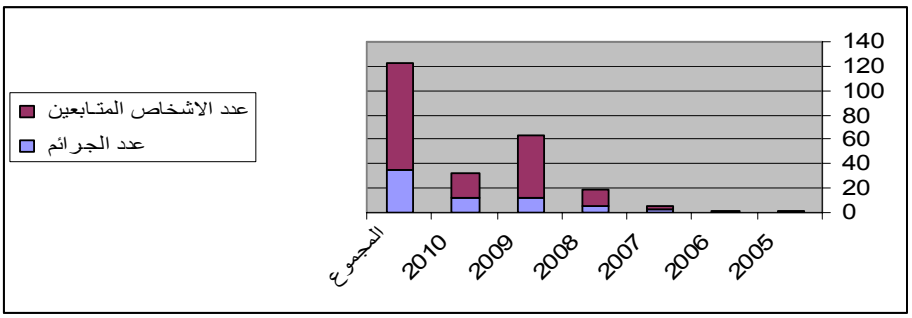
رابعا:القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة:صدر في 19 يوليو 2003 نص على تجريم انتهاك حقوق المؤلف والحقوق المجاورة عن طريق التقليد بأي وسيلة كانت ، بما فيما منظومة معالجة معلوماتية (المادة 152).

خامسا:القانون 2000- 03 المؤرخ في 05 اوث 2000:وضع هذا القانون القواعد التي تنظم مختلف شبكات المواصلات السلكية واللاسلكية مهما كانت الوسيلة المستعملة.(المادة 08-21).

سادسا: المرسوم التنفيذي رقم 98-256:المرسوم التنفيذي رقم (98-256 المؤرخ في 25 أوت 1998المعدل والمتمم للجزء التنظيمي من الأمر 75- 89 المؤرخ في 30 -12-1975: وتضمن تعريف خدمات الانترنت، شروط ممارسة مقدمي الخدمة ومستضيفي المواقع لنشاطهم، واجباتهم اتجاه السلطات العمومية، مسؤوليتهم عن محتوى الصفحات التي يطوروها أو يستضيفوها ، واجباتهم تجاه زبائنهم.

1- قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم وعدد الأشخاص المتابعين (إلى غاية 30 أفريل 2010)

السنة	2005	2006	2007	2008	2009	2010	المجموع
عدد الجرائم	01	01	03	06	12	12	35
عدد الأشخاص المتابعين	00	01	03	13	51	20	88



المصدر:الأخضري مختار، الإطار القانوني لمواجهة جرائم المعلوماتية والفضاء الافتراضي، الملتقي الدولي حول محاربة الجريمة المعلوماتية، الجزائر، ماي 2010م،ص3_9.

2- قضايا المساس بأنظمة المعالجة الآلية للمعطيات مفصلة حسب نوعها (2005-أفريل 2010)

نوع الجريمة	العدد	النسبة المئوية
الدخول غير المشروع مع إتلاف المعطيات أو تعديلها	13	%34
الدخول غير المشروع	11	%29
حيازة معطيات متحصل عليها من دخول غير مشروع	03	%08
إدخال معطيات خلسة	08	%21
المتاجرة في معطيات المتحصل من دخول غير مشروع ويمكن أن ترتكب بها جرائم معلوماتية	02	%05
نشر صور للاستغلال الجنسي للأطفال	01	%03
المجـــــــــــــــموع	38	%100

المصدر: الأخضري مختار، المرجع نفسه، الصفحة نفسها.

3-معلومات عن مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات

السن: ما بين 25و 30 سنة، له معرفة بالمعلوماتية تقني أو طالب 99%، له علاقة بالضحية غالبا مهنية 84% ، الدوافع : مادية 65%، انتقامية 15%، الفضول 15%، التحدي 05%.

المصدر:الأخضري مختار،المرجع نفسه.

4-معلومات عن ضحايا جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

الضحية	العدد	النسبة المئوية
إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري	21	%60
شركات خاصة	07	%20
شركة خاصة أجنبية	04	%11
أشخاص طبيعيين	02	%06
هيئة عمومية أجنبية	01	%03
المجموع	35	%100

المصدر: الأخضري مختار، المرجع نفسه، الصفحة نفسها.

خاتمة:

بعد دراستنا لهذا الموضوع و الجوانب المتعلقة به توصلنا إلى :

- فرضت تكنولوجيا المعلومات مجموعة من التحديات و الرهانات على مختلف الأصعدة، نظرا لاختراقها كافة أنشطة المؤسسات والأفراد، وتضمنت هذه الدراسة أنظمة المعلومات وتقنياتها وما أفرزته في عالم الجريمة.

– الجانب القانوني، الذي لم يعد قانونا للعالم المادي و الجريمة التقليدية أو المجرم التقليدي، وإنما لنوع قانوني جديد،قانون جرائم المعلوماتية في البيئة الافتراضية، لجرائم إلكترونية أدواتها الكمبيوتر والبرمجيات، ومقترفها مجرم ذكي رقمي، جريمة عابرة للحدود لا تحمل جواز سفر لكن مخاطرها تدق في كل مكان.

– التصدي للجريمة الالكترونية بأنظمة أمن معلوماتي وأمن إعلامي، وتفعيل القوانين و التشريعات الدولية و العالمية، فالوضع يتطلب تكاثف الجهود الدولية والإقليمية وعمل المنظمات من أجل أمن الجميع.

– على الجزائر أن تكون أحد الأطراف الفاعلة إذا ما أرادت الاستقرار سياسيا واقتصاديا وأمنيا وإعلاميا، وهذا بتطويع القوانين وتطويرها،و تفعيل دورها في الحد من الجرائم الالكترونية وكذا تطوير أنظمة الأمن المعلوماتي على مستوى المؤسسات الحكومية والخاصة، وحماية المعلومات وأنظمتها وتطويرها بشكل مستمر.

الهوامش:

1. أبو جلال إسماعيل، سلمان، الإذاعة ودورها في الوعي الأمني، ط1، دار أسامة للنشر والتوزيع، الأردن،2011م، ص 154.
2. حجازي بيومي، عبد الفتاح، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2007م، ص20.
3. المرجع نفسه، ص20.
4. المرجع نفسه، ص24.
5. المصري يوسف، الجرائم المعلوماتية والرقمية للحاسوب والانترنت، ط1، دار العدالة، مصر، 2011م، ص7.
6. فرج يوسف،أمير، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ط1، مكتبة الوفاء القانونية، مصر، 2011م، ص154.
7. فرج يوسف، أمير، مرجع سابق، ص95.
8. دروش فهيم، محمد، الجريمة وعصر العولمة: ملف لأشهر المحاكمات في مصر، السر الذهبي للطباعة، مصر، 2000م، ص221.
9. فرج يوسف، أمير، مرجع سابق، ص98،99.
10. صادق دلال، القتال ناصر، حميد، أمن المعلومات، هيئة التعليم التقني، دار اليازوردي العلمية للنشر والتوزيع، الأردن، 2008م، ص143.
11. يونس عرب، قانون تقنية المعلومات والتجارة الالكترونية: برنامج تدريب المحامين الأردنيين، الأردن، 2003م_2004م، ص7،8.
12. بن أحمد الشهري، حسن أحمد، صالح محمد، العطيوي، الوضع الحالي لتدريس وتطبيق أنظمة وتشريعات قوانين الجريمة الالكترونية في المملكة السعودية، دس، ص10.
13. المرجع نفسه، ص11،ص13.
14. فرج يوسف، أمير، مرجع سابق، ص377.
15. بن زيطة، عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الأمر رقم (03-05)، ط1، دار الخلدونية، الجزائر، 2007م، ص50.
16. بن أحمد الشهري، حسن أحمد، صالح محمد، العطيوي، مرجع سابق، ص21.
17. الأخضري مختار، الإطار القانوني لمواجهة جرائم المعلوماتية والفضاء الافتراضي، الملتقى الدولي حول محاربة الجريمة المعلوماتية، الجزائر، ماي 2010م،ص3_9.