ردمد ورقي: 2571-9971 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2020 المجلد: الرابع العدد: الاول

واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر

The reality of combating information crime and its legislative trends in Algeria

أ/ حنان مسكين

جامعة الدكتور مولاي الطاهر سعيدة

تاريخ إرسال المقال: 06 /01/ 2020 **تاريخ قبول المقال:** 11 /03/ 2020

الملخص:

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت كان سلاح ذو حدين لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجرائم الالكترونية بشتى أنواعها، والتي تعتبر من أخطر الجرائم وأعقدها والتي فرضت على العالم ضرورة تكييف قوانينها مع هذا النوع من الإجرام الذي بات يهدد أمن المجتمعات ونتيجة ذلك فقد تبنى المشرع الجزائري سياسة جنائية مغايرة ، وذلك وفق المعطيات التي برزت في الواقع منها تجريم السلوكيات الإجرامية التي يتم استعمال فيها التكنولوجيا بما يؤدي إلى مواكبة التطورات و الحفاظ على النظام العام.

الكلمات المفتاحية: تكنولوجيا المعلومات والاتصال، الانترنت، جرائم الانترنت، الحماية القانونية .

Abstract :

The development in information and communication technology and the emergence of the Internet was a double-edged sword because، to the extent that it had positive effects and changed the lifestyle of societies and contributed to development and advancement in all fields، especially electronic transactions، as much as it had a negative impact on the lives of people and the interests of countries، all this It was manifested in the adaptation of the internet and electronic means to be a world of crime، and thus cybercrime of all kinds emerged into existence، which are among the most serious and complex crimes that imposed on the world the necessity of adapting their laws to this type of crime that has threatened the security of societies and as a result D The Algerian legislator adopted a different criminal policy، according to the data that emerged in fact، including criminalizing criminal behaviors in which technology is used in a manner that leads to keeping pace with developments and maintaining public order.

Key words: information and communication technology، internet، cyber crime، legal protection.

المقدمة:

تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، باعتبارها المحرك الأساسي في التطورات الحادثة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات حيث أن التطور الكبير في تكنولوجيا الحاسبات قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات. وقد كان من نتاج التطور في الجانبين ظهور أدوات واختراعات وخدمات جديدة في مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.كما أن انتقال الأفراد من العالم الواقعي إلى العالم الافتراضي و اعتمادهم على وسائل تكنولوجيا الحديثة أسفر عنه ظهور نوع مستحدث من الجرائم ألا وهي الجرائم المعلوماتية ، فالاهتمام بدراسة جرائم التطور التكنولوجي يعكس جانبا من الوعي والإدراك بخطورة هذا النمط المستحدث من السلوك الإجرامي الذي انتشر في العالم منذ بداية السبعينيات من القرن الماضي وبدأ يظهر منذ بداية التسعينيات في المجتمعات وخاصة فيما يتعلق بالجرائم الإلكترونية، فجرائم التطور التكنولوجي ظاهرة عالمية تكاد تعانى منها كافة دول العالم.

ورغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني و ما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، و محاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام و الاتصال، و قام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية، و مع هذا فيبقى السؤال **مطروح إلى أي مدى ساهمت التطورات و تكنولوجيات الحديثة في ظهور الجرائم المعلوماتية و ما مدى نجاعة و فعالية هذه القوانين في مواجهة هذه الجرائم المستحدثة ؟** للإجابة عن هذا التساؤل سيتم تقسيم موضوع هذه الورقة البحثية إلى مبحثين أساسيين.

المبحث الأول: الإطار لمفاهيمي للجرائم المعلوماتية

لقد أفرزت ثورة الاتصالات و المعلومات وسائل جديدة للبشرية لتجعل الحياة أفضل من ذي قبل غير أنه فتحت الباب على مصراعيه لظهور صور من السلوك الاجتماعي التي لم تكن من الممكن وقوعها، فقد أتاحت نظم الكمبيوتر (حاسوب) ظهور صور جديدة من الجرائم لم تكن موجودة من قبل مثل سرقة المعلومات

والأسرار المودعة في قواعد المعلومات و غيرها، لا تختلف الجرائم المعلوماتية في طبيعتها عن الجرائم التقليدية إلا أنها تعتمد على تقنيات الحديثة في استعمالها.[1]

ومن خلال هذا المبحث سيتم معالجة مفهوم الجريمة المعلوماتية و خصائصها، وأهم أنواعها.

المطلب الأول: مفهوم الجريمة المعلوماتية

ما يلاحظ في مجال الجريمة المعلوماتية أنه لا يوجد مصطلح موحد للدلالة على هذه الظاهرة فهناك من يطلق ظاهرة الغش المعلوماتي أو الاختلاس لمعلوماتي أو الجريمة الالكترونية، جرائم الفضاء الافتراضي جرائم كمبيوتر الانترنت، جرائم مجتمع ما بعد المعلومات و غيرها من المسميات وعلة هذا الاختلاف هو خشية حصر هذه الجريمة في نطاق ضيق ، فتعددت تعريف بشأنها و سنورد أهمها:[2]

1)- التعريف اللغوي: إن الجريمة عموما هي سلوك إنساني غير سوي يستوجب العقاب أما مصطلح المعلوماتية يقصد بها المعالجة الآلية وتعني تكنولوجيا تجميع، informatique للمعلومات، وهي ترجمة للمصطلح الفرنسيTraitematique ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، وقد استعمل مصطلح أيtélématique ويعني المعالجة الآلية للبيانات ومصطلحautomatise des domnes في اللغة الإنجليزية وإن كان ليس لها أصل في tlematic اتصالات، وهي تعادل مصطلح القاموس الإنجليزي مستمدة من اللغة الفرنسية.

2)- التعريف الاصطلاحي للجريمة المعلوماتية: يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فلهذا نجد بعض الفقهاء وضعوا تعريف الجريمة المعلوماتية في مجالين :مجال واسع ومجال ضيق.

أ- تعريف الضيق للجريمة المعلوماتية: ذهب الفقيه merwe إلى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية. فيما عرفه الفقيه rosblat بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والى تحويل طريقته. وعرفها كلاوس تايدومان بأنها: كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي .

ويرى البعض أن تعريف كلا من marwe و rosblat جاء مقصورين على الإحاطة بأوجه الظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه إن بالغ في العمومية و الاتساع ، لأنه يدخل فيه كل

1- عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، ط1 ، المركز القومي للإصدارات القانونية ، القاهرة ، 2012، ص39.

2 - طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2015، ص 15.

سلوك غير مشروع أو ضار بالمجتمع . ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها: الجرائم التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا.[3]

ب- التعريفات الموسعة لمفهوم الجريمة المعلوماتية : هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالأتي : كَل فعل أو امتناع عمدي ، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية الخبير الأمريكي parker عرف الجريمة المعلوماتية أنها : "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل" .

يعرف الأستاذ hestanc و vivant الجريمة المعلوماتية : مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمك أن تكون جديرة بالعقاب.[4] وعليه جرائم الكمبيوتر فهو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء أداة الجريمة أو كان هدف الجريمة ويدخل من ضمنها جرائم معلوماتية وجرائم الإنترنت ، كما يدخل من ضمنها الاعتداء على الشبكات المحلية خاصة بالهيئات والمنشات الخاصة والعامة.

3)- التعريف القانوني للجريمة المعلوماتية : تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث.[5]

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم09 -04 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه": المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة ، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين"[6]

3 - عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص 40-41 .
4- نهلا عبد القادر المنمي ، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، ط1، دار الثقافة للنشر والتوزيع ، 2008 ص 49 .
5 - القانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ولاتصال و مكافحتها ، جريدة رسمية ، عدد 47 ، صادرة بتاريخ 16 أوت 2009 .
6 - نشناش منية ، الركن المفترض في الجريمة المعلوماتية ، مداخلة مقدمة بمناسبة الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة ، جامعة بسكرة، المنظم يومي 16-17 نوفمبر 2015 ، ص 04 .

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتي من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان :المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر07 . وقد وفق المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينه ، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات .

المطلب الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة لارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد كان لظهور شبكة الإنترنت في إضفاء شكل جديد للجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

أولا: خصائص تشترك فيها مع بعض الجرائم.

أ –**خطورة الجرائم المعلوماتية** : وذلك لمساسها بالإنسان في فكره وحياته، وتمس المؤسسات في اقتصادها والبلاد في أمنها القومي والسياسي والاقتصادي، ومن شأن ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الإضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات.

ب –**الطبيعة المتعدية الحدود.** : من أهم خصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن اكتسابها طبيعة متعددة الحدود ، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات عبر الدول المختلفة فالقدرة التي تتمتع المعلومات بين أنظمة يفصل بينها ألاف الأميال، قد أدت إلى نتيجة مؤداها إن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال.

1. **ثانيا: خصائص تنفرد بها الجريمة المعلوماتية عن الجرائم الأخرى.** : تختلف الجريمة المعلوماتية عن باقي أنواع الجرائم في:

أ –**تتطلب لارتكابها وجود كمبيوتر ومعرفة تقنية باستخدامها.** : حيث يعتبر الاستعانة بجهاز الكمبيوتر أساسا لارتكاب الجريمة المعلوماتية وليس سرقة الجهاز أو إتلافه لأنه يدخل في نطاق الاعتداء أو سرقة الأموال المادية المنقولة، وترتكب الجريمة بتدمير برامج الكمبيوتر أو سرقتها أو العبث بالبيانات

أو المعلومات المخزنة ويصعب على المحقق التقليدي التعامل .كما تعتمد هذه الجرائم على قمة الذكاء في ارتكابها مع هذه الجرائم، إذ يصعب عليه متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها، فهي بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، جرائم تتسم بالغموض وإثبات ،كما انه كلما تقدمت المعرفة التقنية كلما زادت احتمالية توظيف هذه المعارف بشكل غير مشروع وزيادة خطورة الجرائم المعلوماتية.[7]

ب –صعوبة اكتشافها وإثباتها : تتسم الجريمة المعلوماتية بأنها لا تترك أثرا بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني أبآثارها إن وجدت، فليس هناك أموال مادية منقولة تم اختلاسها وإنما هي أرقام تتغير السجلات، كما أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد مرور وقت طويل إضافة انه لا يتم في الغالب الإبلاغ عن الجرائم المعلوماتية أما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به لذلك ما يرتكب فعلا من جرائم معلوماتية اكبر بكثير ما يصرح به.

يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي بعدة خصائص تتمثل أ ساسا في:

1. المجرم المعلوماتي مجرم متخصص و محترف في تنفيذ جريمته الالكترونية ، حيث أن ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر.
2. خلافا على المجرم العادي المجرم المعلوماتي لا يلجا إلى العنف في تنفيذ جرائمه فهو مجرم دكي يتمتع بالمهارة و المعرفة و بدرجة عالية من الثقافة و الذكاء.[8]

ويوجد عدة أنواع من المجرمين المعلوماتيين فهناك:

أ –**المازحون Prankesters**: الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم و يندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية.

ب –قراصنة الانترنت Hackers : فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحسابات الآلية غير المصرح لهم وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة أو بدافع الفضول أو بمجرد إثبات القدرة على اختراق هذه الأنظمة.

7 - مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر واليات مكافحتها ، المجلة الجزائرية للاقتصاد و المالية، جامعة المدية، المجلد 1 العدد 01 ، أفريل2014، ص 96-97 .

8 - نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة ، مداخلة بمناسبة الملتقى الدولي الرابع عشر الجرائم الالكترونية بطرابلس، المنظم يومي 24-25 مارس 2017 ،ص 101.

ت –القراصنة المجرمون: Malicious hackers هدفهم إلحاق خسائر بالمجني عليهم أن يكون الحصول على مكتسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرة من مخترقي فيروسات الحاسبات الآلية وموزعيها.

ث –المنتقمون: Personnel Problem solvers فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

ج –ممتهنوا الإجرام Career criminals : وهم مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة بحيث ينطبق على أفعالهم الجريمة المنظمة،ا وعلى الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ،ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

ح –المتطرفون Extreme advocates: فتدخل في عداداها الجماعات الإرهابية أو المتطرفة، والتي تكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي،ويركز نشاكهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من اجل لفت الأنظار إلى ما يدعون إليه، وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحسابات الآلية في انجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في اغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات.

خ –الإهمال The criminality negligent و التي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحسابات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي اغلب الأحيان نتائج خطيرة قد تصل إلى حد القتل.[9]

المطلب الثالث: أنواع الجرائم المعلوماتية

تصنف الجريمة المعلوماتية(الالكتروني)إلى عدة أصناف فهناك من يصنفها تبعا لمرتكبها، وهناك الجرائم المعلوماتية التي صنفت تبعا لطريقة تنفيذها، وأخرى تبعا لغرض أو هدف الاعتداء وتم تصنيفها وفق أسس متعددة بغرض تسهيل التعامل معها، ويمكن الإشارة إلى تصنفين رئيسيين:[10]

أولا: التصنيف الشكلي : ويتضح من خلاله الشكل العام للجريمة والتغير الذي طرأ عليها بفعل التقنية المعلوماتية وينقسم إلى نوعين وهما :

9- مزيود سليم، المرجع السابق ، ص 99.
10- منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، مداخلة ملقاة بمناسبة مؤتمر الجرائم المعلوماتية لرياض أكاديمية نايف العربية للعلوم الأمنية، المنظم يومي 12-13 أكتوبر 2009 ، ص06.

1)- الجرائم الالكترونية التقليدية :وهي الجرائم المعروفة من السابق كالسرقة مثلا، ولكنها أصبحت ترتكب بتسخير قدرات التقنيات المعلوماتية كوسيلة لتنفيذها مما أعطاها مسميات أخرى كالسرقة الالكترونية تتفق وطبيعتها الجديدة.

2)- الجرائم الالكترونية الجديدة :وهي عبارة عن أشكال إجرامية مستحدثة لم تكن معروفة من السابق وتعتمد بشكل رئيسي في تنفيذها على التقنيات المعلوماتية أو الالكترونية كونها لم تعرف إلا بعد ظهور التقنيات الرقمية، كنشر الفيروسات الرقمية أو عمليات الاختراق لقواعد البيانات مثلا.

ثانيا: تصنيف العملي :ويعتمد على الدور الذي تلعبه تقنية المعلومات في الجريمة المنفذة ويندرج تحته ثلاثة أنواع وهي:

1)- الجرائم التي تستهدف النظام المعلوماتي :وهي الجرائم الالكترونية التي تستهدف احد مكونات النظام المعلوماتي أو الالكتروني كجرائم الاختراق وجرائم إتلاف المعلومات.[11]

2)- الجرائم المنفذة باستخدام النظام المعلوماتي :وهي الجرائم التي يتم ارتكابها بواسطة التقنيات الرقمية كجرائم التعدي على البيانات وانتهاك الخصوصية.

3)- الجرائم المنفذة في بيئة النظام المعلوماتي :وتتمثل في الجرائم التي تتم في البيئة الالكترونية دون الإضرار بالبيئة ذاتها، بل يكون الضرر على الأطراف المستخدمة أو المستفيدة من تلك البيئة كجرائم التشهير والجرائم الإباحية والأخلاقية

المبحث الثاني: جهود المشرع الجزائري في تجريم الأفعال المتصلة بتكنولوجيا الحديثة

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية، وذكر بعض الخبراء أن الأرباح الضخمة التي تحققها الجرائم الإلكترونية تجاوزت أرباح تجارة المخدرات. والجزائر كغيرها من الدول لم تسلم هي الأخرى من ما يسمى الجريمة الالكترونية، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات، من عملية السطو على الصور والبيانات الشخصية واستعمالها كوسيلة للابتزاز والمساومة و التشهير، ناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة إلى الاعتداء على أنظمة المعلومات مما جعل المشرع الجزائري يتدخل بوضع ترسانة قانونية لمكافحة هده الجرائم .[12]

11- أسامة بن غانم العبيدي، جريمة إتلاف المعلومات ، مجلة دراسات المعلومات، العدد 04 ، يناير 2009، ص 93-123.
12- حفوظة الأمير عبد القادر، غرادين حسام، الجريمة الالكترونية واليات التصدي لها، مداخلة بمناسبة الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة، المنظم يوم 29 مارس 2017 ، ص 97-98 .

المطلب الأول: واقع الجريمة المعلوماتية في الجزائر و مكافحتها

تعد جرائم الانترنت احد مساوئ تطبيق تكنولوجيا المعلومات والاتصال، وان الحديث عن موقع الجزائر من التطورات التشريعية لمواجهة الإجرام المعلوماتي يقودنا إلى ذكر أولى بدايات استعمال الانترنت في الجزائر التي تعود لسنة 1993عن طريق مركز الأبحاث CERIST ، وبعد إن تم تحرير القطاع سنة 1998 ازداد عدد مقدمي خدمة الانترنت و مستعمليها ليشهد تزايد غير مسبوق في الوقت الحالي .

وتجدر الإشارة إلى انه رغم تأخر الجزائر في استخدام تكنولوجيا المعلومات والانترنت لم يقف حائلا دون أن تصدر تشريعات تكفل الحماية الجنائية للأنظمة المعلوماتية ، وتحفظ حقوق الإفراد من مخاطر الاستخدام السيئ لتكنولوجيا المعلومات ، وضرورة عدم الاكتفاء بالنصوص التقليدية ، بالا صافة إلى ذلك فقد ضمن المشرع الجزائري الحماية الجزائية لنظم المعلوماتية من خلال القانون رقم 04- 15 المؤرخ في 10نوفمبر2004 المعدل والمتمم للأمر 66-156 المتضمن الجرائم المساس بأنظمة المعالجة الآلية للمعطيات[13] والذي تم تعزيزه بالقانون رقم09—04 المؤرخ في 05اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها . وعليه فان ظاهرة الجريمة المعلوماتية بدأت تظهر في الجزائر إلى سنة 2005 أين سجلت ظاهرة واحدة فقط ومع تزايد انتشار الانترنت في الجزائر حيث وصل عدد المشتركين فيها إلى واتجاه إلى استعمال تكنولوجيا الاتصال بدأت ترتفع حجم الظاهرة حيث سجلت سنة 2009 حوالي 88 حالة شخص متهما تتعلق بالجريمة المعلوماتية وتؤكد معطيات أمام ملتقى دولي حول الجريمة المعلوماتية أن هذا النوع من الجرائم لم ينتشر على نطاق واسع في الجزائر غير انه اخذ في التقدم وان المخالفات المسجلة تتعلق بالاطلاع غير الشرعي على البيانات قصد إتلافها والقرصنة ضد المواقع الرسمية والخاصة والدعاية المغرضة والإرهاب وسرقة المعلومات والتعدي على الحياة الشخصية وتستهدف الجريمة المعلوماتية % 60 منها تستهدف الإدارات العامة والمؤسسات الصناعية ونسبة % 20 الشركات الخاصة و% 11 الشركات الأجنبية و6% الأشخاص.[14]

المطلب الثاني: موقف المشرع الجزائري من الجرائم المعلوماتية

إن معظم التشريعات جرمت الأعمال الإلكترونية ولكنها تباينت واختلفت اختلافا كبيرا وذلك راجع أساسا ألي اختلاف المستوى الرقمي أو التكنولوجي للدول المتقدمة.

13 - القانون رقم 04 -15 المؤرخ في 10 نوفمبر2004 المعدل و المتمم للأمر 66-156 مؤرخ في 08-06-1966 المتضمن قانون العقوبات جريدة رسمية، عدد 71 لسنة 2004 المعدل و المتمم.
14 - مزيود سليم، المرجع السابق ، ص 103.

أولا: تجريم الأعمال الالكترونية في قانون العقوبات الجزائري : لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى394 مكرر.[15]

في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات[16] بموجب قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون04 -15 ، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الانترنت كوسيلة لنقل المعلومات وتزايد سريع لمستخدمي الانترنت.

ثانيا: تجريم الأعمال الالكترونية في قانون الإجراءات الجزائية الجزائري :تناول موضوع الجرائم الافتراضية من خلال:[17]

1- إحداث المحاكم الجزائية ذات اختصاص الموسع التي أجاز لها تمديد اختصاصاتها 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 (المادة 16)

3- التنصيص على قواعد استثنائية في التفتيش المواد 45- 47 و نص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة6.

4- إمكانية استعمال أساليب خاصة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية ' التقاط و التثبيت و بث و تسجيل

15- لمزيد من المعلومات راجع المواد 394مكرر 1- 2- 3- 4- 6- 7 من قانون العقوبات السالف الذكر.
مع العلم أن تعديل الجديد لقانون العقوبات رقم 16- 02 مؤرخ في 19 يونيو 2016 المتضمن قانون العقوبات أضاف المادة 294مكرر 8 الجريدة الرسمية، العدد37، الصادرة في 22 يونيو 2016.
16- القانون رقم 06-23 المؤرخ في 20ديسمبر 2006 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 48، الصادرة في 24 ديسمبر 2006 المعدل و المتمم.
17- القانون رقم 04-14 مؤرخ في 10 نوفمبر 2004 يعدل و يتمم الأمر رقم 66-156 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية العدد 71 ، الصادرة في 10 نوفمبر سنة2004 المعدل و المتمم.

الكلام و صور الأشخاص في الأماكن الخاصة و التسرب (المواد 65مكرر5 إلى 65 مكرر10. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية .[18]

ثالثا: تجريم الإعمال الالكترونية في القوانين الخاصة: وهذه القوانين شملت الحماية في قانون التأمينات الاجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية وأيضا الحماية في نصوص التوقيع الالكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلكية واللاسلكية.

1. **الحماية في قانون التأمينات الاجتماعية:** بمقتضى إحكام قانون التأمينات الاجتماعية رقم 08-01 المؤرخ في 23- 01 -2008 الذي حدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا ، وعاقب المشرع الجزائري كل من يسلك أو يستسلم بهدف الاستعمال غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا المفتاح الالكتروني لهيكل العلاج أو المفتاح لمهني الصحة طبقا للمادة 93مكرر2 من نفس القانون [19] كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية أو نسخ البرمجيات المتعلقة باستعمال البطاقة الالكترونية أو محاولة على ارتكاب الفعل طبقا للمادة 93 مكرر3 منه ، كما اقر المشرع أيضا عقوبة الشخص المعنوي ليشمل الغرامة ضعف المقررة لشخص الطبيعي طبقا لنص المادة 93 مكرر 5 من ذات القانون ، ومصادرة الأجهزة المستعملة وكذا غلق المحلات و أساس الاستغلال التي محل الجنح.

2. **الحماية من خلال قانون الملكية الأدبية و الفنية:** حاول المشرع الجزائري مواجهة الجريمة الالكترونية من خلال قانون الملكية الأدبية و الفنية المتعلق بحق المؤلف و الحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 23-07-2003 المتعلق بحقوق المؤلف و الحقوق المجاورة[20] حيث وسع قائمة المؤلفات المحمية ، وذلك باندماج برامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات برامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.[21]

3. **الحماية في نصوص التوقيع الالكتروني** :اصدر المشرع الجزائري قانون رقم 15-03 المتعلق بعصرنة العدالة حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل و الإشهاد على صحة

18- قصعة خديجة ، جمال بن زردق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الالكترونية في العالم و الجزائر ، مجلة تاريخ العلوم ،الجلفة ، المجلد 03، العدد 06 ، 2017، ص 252 .

19 - القانون رقم 08- 01 المؤرخ في 23- 01- 2008 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية ، عدد 04 الصادرة في 27جانفي 2008 .

20- الأمر رقم 03- 05 المؤرخ في 19- 07- 2003 المتعلق بحقوق مؤلف و الحقوق المجاورة، الجريدة الرسمية، عدد44، صادرة بتاريخ 13 جويلية 2003.

21- تجدر الإشارة إلى أن القانون الدستوري الجديد رقم 16-01 أكد هو الأخر في مادته 44 على حماية حقوق المؤلف وعدم جواز حجز على أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي.

الوثائق الالكترونية وضمان حمايتها ، أما الفصل الثالث تعرض إلى إرسال الوثائق و الجزاءات القضائية بالطريق الالكتروني ، والفصل الخامس تعرض إلى الأحكام الجزائية لحماية التوقيع و التصديق الالكترونيين طبقا لنص المادتين و 17 و 18 منه. [22]

4. **الحماية المتعلقة بالموصلات السلكية واللاسلكية :** تضمن الفصل الثاني من الباب الرابع من القانون رقم 2000-03 المتعلق بالبريد والمواصلات السلكية و اللاسلكية[23] الأحكام الجزئية المترتبة على مخالفة النظام القانوني ، فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية و اللاسلكية و العمال متعامل الشبكات العمومية الذين ينتهكون المراسلات السلكية و اللاسلكية أو المساعدة على دلك يعاقبون طبقا لنص المادة 137 من قانون العقوبات أم غيرهم يمكن يرتكب هده الأفعال فيعاقب بالحبس و الغرامة.

5. **الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها**[24]

يتميز هذا القانون بأنه الإطار القانوني الأكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام و الاتصال لا سيما الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت. باستقراء فحوى هذا القانون يتبين لنا بأن المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للتصدي لجرائم المعلوماتية تتمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و رصد مرتكبيها، و تدابير أخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات جزائية .

أولا: التدابير الوقائية المستحدثة: لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و عن مرتكبيها في وقت مبكر و هي كالتالي: [25]

1)- مراقبة الاتصالات الالكترونية :لقد نصت المادة 04 من القانون09 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بم ا رقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية.[26]

22- القانون رقم 15- 03 المؤرخ في 01- فيفري 2015 المتعلق بعصرنة العدالة، الجريدة الرسمية ، عدد 02 ، صادرة في 10فيفري 2015 .

23 - القانون رقم 2000- 03 المؤرخ في 05-أوت 2000 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية و اللاسلكية، الجريدة الرسمية عدد48 ، المؤرخ في 06أوت 2000.

24- قانون رقم 09-04 مؤرخ في 05-أوت 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا ت الإعلام و الاتصال و مكافحتها ، جريدة رسمية ، عدد 47 ، صادرة بتاريخ 16 أوت 2009 .

25- تجدر الإشارة إلى أن هذه التدابير هي نفسها المنصوص عليها في المادة 20فقرة (ب) و المادة 21 من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية لعام 2001.

26- المادة 04 من القانون رقم 09-04 السالف الذكر .

2)- إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية[27]

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 11 و 12 من نفس القانون

ثانيا : التدابير الإجرائية : إضافة إلى التدابير الوقائية السالفة الذكر تبنى المشرع في القانون رقم 09-04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام و الاتصال تتلخص فيما يلي:

1. السماح للجهات القضائية المختصة و ضباط الشرطة بالدخول لغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و المعطيات المعلوماتية المخزنة فيها و استنساخها، مع أمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.
2. إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، و ذلك طبقا للاتفاقيات الدولية و مبدأ المعاملة بالمثل .
3. توسيع دائرة اختصاص الهيئات القضائية الجزائية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام و الاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية و الدفاع الوطني و المصالح الإستراتجية للدولة الجزائرية مستهدفة.
4. السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق و جمع ألأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام و الاتصال عبر الوطنية و مرتكبيها، و ذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل .

يستنتج في الأخير أن أحكام القانون رقم 09-04 جاءت عامة و مطلقة في مكافحة الجرائم المتصلة بتكنولوجية الإعلام و الاتصال، بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال، و يطبق على كافة التكنولوجيات القديمة و الجديدة، بما فيها شبكة الانترنيت و على أي تقنية يمكن

أن تظهر مستقبلا .وهو الأمر الذي يجعله قانونا فعالا و يساير التطور التكنولوجي السريع .[28]

27- عرفت المادة 2 فقرة (د) من القانون 09-04 مزودي الخدمات بأنه:" أي كيان عام أو خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها. "

28 - برا هيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، المجلد02، العدد 02، 2016، ص 153-154.

المطلب الثالث: أفاق المستقبلية لمكافحة الجريمة الالكترونية في الجزائر

أكد فاروق قسنطيني رئيس اللجنة الوطنية لترقية وحماية حقوق الإنسان، صعوبة تطبيق القوانين المعاقبة على الجريمة الإلكترونية في الجزائر، لقلة خبرتها في هذا الشق، وغياب المختصين والخبراء القادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها، وقال قسنطيني في تصريح ل"السلام" :"إن استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدة أضرارها قبل إصدار العقوبة، هذا فضلا عن غياب التوصل الدائم بين القضاء والمختصين في الاتصالات، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم."

وفي السياق ذاته أوضح أن القانون الجزائري، يعاقب في الغالب مرتكبي هذه الجرائم بالسجن القصير المدى أو بالغرامة المالية،" بحكم أن جل الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنف قانونيا كسرقة"، مبرزا أن المعدل العام لهذه الجرائم في الجزائر متوسط مقارنة بباقي دول العالم، محذرا من تنامي هذه الجرائم في السنوات الأخيرة على المستوى الوطني، مع بداية مرحلة إدمان الجزائري على الإنترنت، وما يصاحبها من خدمات إلكترونية، ودعا الحكومة إلى ضرورة استحداث إستراتيجيات عقابية وتقنية حماية ضحايا هذه الجرائم، خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها وكانت الجزائر ضمن مجموعة الدول المدرجة في مشروع إعداد بحث لتحديد آلية تطور الهجمات الإلكترونية خلال السنوات الثمانية المقبلة من طرف منظمة" **التحالف الدولي لحماية أمن الانترنت**"، والذي يتضمن تقديم إرشادات لحكومات الدول والسلطات المحلية حول أفضل السبل المتاحة لمواجه هذه الهجمات.[29]

الخاتمة

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجرائم الالكترونية بشتى أنواعها وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد أو المؤسسات أو حتى الحكومات، وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدة هذا النوع من الجرائم مما جعل المشرع الجزائري يتدخل بوضع ترسانة قانونية لمواجهة هذا النوع من الجرائم المستحدثة.

29 - ياسمينة بونعارة ، المرجع السابق، ص 29.

ومن خلال دراستنا خلصنا إلى عدة نتائج أهمها أن المشرع الجزائري قد تبنى سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتية، بحيث اهتدى من جهة إلى تعديل الجوانب الموضوعية والإجرائية للتشريعات العقابية العامة (قانون العقوبات و قانون الإجراءات الجزائية) وجعلها تواكب التحديات الجديدة الناتجة عن التطور الهائل للتكنولوجيات الحديثة.

ومن جهة أخرى قام باستحداث قوانين أخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم الالكترونية. وهذا التنوع التشريعي من شانه أن يساهم بشكل فعال على الأقل في الوقت الراهن في الحد من تفاقم ظاهرة الإجرام الالكتروني في الدولة الجزائرية .مع هذا ينبغي الاعتراف بحقيقة و هي انه رغم الجهود الجبارة التي يبذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه، نظرا للتطورات السريعة و المستمرة التي تعرفها ظاهرة الإجرام الالكتروني من جهة، و نظرا للطالع العالمي والعابر للحدود الذي تتميز بها هذه الظاهر من جهة أخرى لذلك لابد من التفكير في التوجه إلى التعاون التشريعي و القضائي و الأمني مع الدول العربية و لما لا مع الدول الغربية الأكثر دراية بالجرائم الالكترونية والاستفادة من خبراتها في مجال مكافحة هذه الجرائم.

وفي الختام الدراسة نخلص إلى جملة من التوصيات والتي يمكن إجمالها على النحو التالي:

أولاً : – التوصيات المتعلقة بآليات التدخل على مستوى التشريعات والسياسات؛

1- ضرورة الالتزام بأحكام الدستور بشأن حماية سرية المراسلات والخصوصية والحرية الشخصية والطمأنينة ونشر المعرفة بها.

2- ضرورة مشاركة المجتمع المدني في مناقشة مشاريع القوانين المتعلقة بالجرائم الإلكترونية وأمن المعلومات الشخصية وضمانات الحق في الخصوصية دون مساس بحرية الرأي والتعبير ودون تضيق على المساحة التي يتيحها الإنترنت للحصول على المعرفة والمعلومات ولتسهيل التواصل الاجتماعي.

3- أهمية التأكد من مراعاة السرية وحماية الخصوصية ومراعاة النوع الاجتماعي في النصوص التشريعية وفي التطبيقات والإجراءات والممارسات ذات الصلة ، مع ضرورة توقي عقوبات رادعة ومؤثرة في مواجهة الجرائم الإلكترونية من خلال إساءة استخدام وسائل التواصل الاجتماعي وتكنولوجيا المعلومات كجرائم التنصت وسرقة البيانات والابتزاز والتحرش والإيذاء والملاحقة وغيرها من الجرائم وخاصة جرائم العنف ضد النساء والأطفال.

4- أهمية الحد من ضرر الجرائم الإلكترونية من خلال عقوبات متناسبة ورادعة وتعويضات تسهم في جبر الضرر، وإعادة النظر في قيمة الغرامات المقررة باتجاه رفعها لتحقق النتائج المرجوة وتنويع الجزاءات.

5- تشديد العقوبة وزيادة مدة الحبس إذا كان المعتدى عليه / عليها شخص قاصر بسبب الإعاقة أو بسبب صغر السن لعدم إتمام الثامنة عشر من العمر. و النص على إجراءات قانونية تضمن الإسراع في البت بقضايا الجرائم الإلكترونية.

6- النص على إلزام شركات الاتصالات بإلغاء المحتوى الإلكتروني المنطوي على ضرر وإساءة بأمر مستعجل من الجهة القضائية المختصة بناء على طلب المتضرر/ ة.

7- النص على عدم جواز إفشاء أو تقديم بيانات تتجاوز حدود البيانات اللازمة في قضية ما والنص على وجوب تحديد طلبات الجهات الرسمية الإدارية والقضائية بصورة شديدة التحديد والوضوح وخاصة لجهة تحديد أطراف القضية لمنع سوء الاستخدام واقتصار الطلب على هذه البيانات دون تعميم.

ثانياً :آليات التدخل على مستوى رفع الوعي وبناء المهارات والقدرات- البرامج والخدمات والتوعية:

1- ضرورة تكثيف الجهود الوطنية لنشر المعرفة وزيادة الوعي بالجرائم الإلكترونية ومدى خطورتها ووسائل الوقاية منها وسبل مواجهتها.

2- نشر المعرفة والمعلومات حول جهات الإرشاد والمساعدة القانونية والفنية للمتضررات والمتضررين والجهات الرسمية التي تستقبل الشكاوى المتعلقة بالجرائم الإلكترونية.

3- أهمية نشر الوعي لتعزيز الثقة بسرية ونجاعة الإجراءات المتاحة قانونياً لملاحقة الجرائم الإلكترونية والتحقيق فيها ومحاكمة مرتكبيها.

4- ضرورة تضمين المناهج الدراسية المعارف والمعلومات والقيم السلوكية المتعلقة باستخدام تكنولوجيا المعلومات والاتصال الحديثة ومتطلبات صيانة الخصوصية والأمن الشخصي وسبل مواجهة مخاطرها.

5- إعداد ونشر مواد توعية وتثقيف وتوزيعها على نطاق واسع وإتاحتها إلكترونياً لنشر الوعي بالاستخدام الآمن لتكنولوجيا المعلومات والاتصال ومسألة الخصوصية ووسائل الوقاية من الجرائم الإلكترونية.

6- نشر الإحصائيات والأرقام المتعلقة بالجرائم الإلكترونية والأحكام القضائية الصادرة بها لتحقيق المزيد من الردع وللتوعية وتحفيز المزيد من الحذر من الاستخدام الخاطئ لوسائل التواصل الاجتماعي والإنترنت

7- التوعية بأساليب التحايل والجوانب السلبية لعدم الاستخدام الآمن لوسائل التواصل الاجتماعي والإنترنت بشكل عام.

8- تكثيف برامج بناء القدرات والتدريب الموجهة للوالدين و المرشدات والمرشدين التربويين والقائمين على إنفاذ القانون بشأن الجرائم الإلكترونية وسبل الوقاية منها والتعامل معها وحماية الأطفال بشكل خاص منها

9- إنشاء وإتاحة برامج وخدمات متخصصة موجهة للفئات الأكثر عرضة لمثل هذه الجرائم.

10- تعزيز منهج الحذر والتعامل الواعي مع البرامج والخدمات الإلكترونية وتحفيز الاستعانة بالمختصين لضمان الحماية والأمان.

ثالثاً : – آليات التدخل على مستوى الرصد والإعلام؛

1- تكثيف الحملات الإعلامية الخاصة بموضوع الجرائم الإلكترونية، وإعداد وبث برامج إعلامية توعية مرئية ومسموعة توعية موجهة للأسرة وخاصة للنساء والأطفال.

2- تعزيز التعاون مع وسائل الإعلام بما فيه الإعلام الإلكترونية لمتابعة ورصد وتطوير مواثيق وأخلاقيات ومدونات سلوك وآليات محاسبة ذاتية بشأن استخدام وسائل المعلومات والاتصال الإلكتروني ومواجهة الجرائم الإلكترونية.

3- تعزيز التعاون والتنسيق مع الهيئات والجهات الممثلة للإعلاميين كنقابة الصحفيين ومنظمات المجتمع المدني المعنية بالحريات الصحفية في هذا المجال.

قائمة المراجع:

1- أسامة بن غانم العبيدي، جريمة إتلاف المعلومات ، مجلة دراسات المعلومات، العدد 04 ، يناير 2009.

2- برا هيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، المجلد02، العدد 02 2016.

3- حفوظة الأمير عبد القادر، غرادين حسام، الجريمة الالكترونية واليات التصدي لها، مداخلة بمناسبة الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، الجزائر العاصمة، المنظم يوم 29 مارس 2017.

4- طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية 2015.

5- عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، ط1 المركز القومي للإصدارات القانونية ، القاهرة ، 2012.

6- قصعة خديجة ، جمال بن زردق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الالكترونية في العالم و الجزائر ، مجلة تاريخ العلوم ،الجلفة ، المجلد 03، العدد 06 ، 2017.

7- مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر واليات مكافحتها ، المجلة الجزائرية للاقتصاد و المالية جامعة المدية، المجلد 1 العدد 01 ، أفريل2014.

8- منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، مداخلة ملقاة بمناسبة مؤتمر الجرائم المعلوماتية لرياض أكاديمية نايف العربية للعلوم الأمنية، المنظم يومي 12-13 أكتوبر 2009.

9- نشناش منية ، الركن المفترض في الجريمة المعلوماتية ، مداخلة مقدمة بمناسبة الملتقى الوطني للجريمة المعلوماتية بين الوقاية و المكافحة ، جامعة بسكرة، المنظم يومي 16-17 نوفمبر 2015.

10- نمديلي رحيمة ، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة ، مداخلة بمناسبة الملتقى الدولي الرابع عشر الجرائم الالكترونية بطرابلس، المنظم يومي 24-25 مارس 2017.

11- نهلا عبد القادر الممني ، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، ط1، دار الثقافة للنشر والتوزيع، 2008.