معالم الجريمة المعلوماتية في القانون الجزائري

الدكتورة/ حوالف حليمة – جامعة أبوبكر بلقايد –تلمسان–
Email :halima1178@hotmail.fr

ط–د/ مهاجي فاطمة الزهراء – طالبة السنة الثانية دكتوراه – جامعة تلمسان–

تاريخ الإرسال:25–11–2021----تاريخ القبول/12–02–2021

ملخص

الجرائم المعلوماتية هي واحدة من أعظم ويلات هذا القرن إذا أصبحت واقعا مفزعا للدول والأفراد ويعود ذلك أساسا إلى الإمكانيات المتاحة للمجرم الإلكتروني ذلك بتقدم وسائل الاتصال والمعلومات وذيوع استعمال الحاسوب وسهولة استخدام الأنترنت فبالتخفي خلف شاشتهم يستطيعصناعة ونشر الفيروسات، الاختراقات، تعطيل الأجهزة...إلخ.

ومن جهة أخرى فإن مكافحة الجريمة المعلوماتية تواجهها عدة عقبات بالنظر إلى طبيعتها الافتراضية لهذا أفرزت تحديات واضحة للقوانين التي وضعت لمكافحتها فقد تغيرت الجريمة من صورتها المادية التقليدية إلى أخرى معنوية ونتج عن ذلك مشكلة في تفسير النصوص ومبدأ الشرعية الجنائية.

ومن هنا كان لابد للتشريع الجزائري أن يواكب هذا التطور الملحوظ في الجرائم المعلوماتية فالمواجهة التشريعية ضرورية للتعامل مع الجوانب التقنية للجريمة الرقمية وذلك بقواعد قانونية غير تقليدية.

ولبلوغ الهدف المرجو من الدراسة نثير الإشكالية التالية: ما مدى كفاية النصوص العقابية الحالية لمنع الجرائم المرتكبة في نطاق المعاملات الإلكترونية؟ وهل المواجهة الجنائية هي الحل الأمثل؟

الكلمات المفتاحية: الجرائم المعلوماتية، المعالجة الآلية للمعلومات، الأمن المعلوماتي.

مقدمة

تعد الجريمة المعلوماتية من الجرائم المستحدثة فقد تزامن ظهورها مع ظهور أعظم اختراع في العالم الحديث الحاسب الآلي والأنترنت، وهي إفراز لما نعيشه من ثورة معلوماتية، فرغم حداثتها إلا أنها تشكل تهديدا حقيقا لاقتصاديات الدول وخصوصيات الأفراد.

إن هذه الجرائم تتميز بطبيعة خاصة تختلف عن الجرائم العادية فهي لا تترك آثار مادية يمكن من خلالها التوصل إلى الجاني كما في الجرائم العادية، كما أنه يمكن إتلاف أو تغيير الأدلة في هذه الجرائم خلال لحظات دون أن يترك هذا التغيير آثار مادي.

ومن ناحية أخرى فإن الصعوبة في مواجهة الجريمة المعلوماتية تبدأ من الطبيعة الافتراضية التقنية التي ترتكب فيها،فمن السهل ارتكاب جريمة ما حيث أن نقرة بسيطة من الكمبيوتر كافية للتصرف أو الوصول على الضحية المحتمل رغم أن التقنيات المستحدثة في كثير من الأحيان تكون دقيقة جدا، كما أنها تتم في الخفاء فكثيرا ما يعمد المجرم المعلوماتي إلى إخفاء نشاطه عن طريق تلاعبه بالبيانات فضلا عن سهولة تدمير الدليل.

وعلى ضوء ذلك فإن الظاهرة الإجرامية المعلوماتية باتت تشكل بعض التحديات القانونية والعملية التي وضعت لمكافحتها ونتج عن ذلك مشكلة في تفسير النصوص القانونية وحظر القياس في المواد الجنائية وهذه العوامل تؤدي إلى إفلات الكثير من مجرمي المعلوماتية من العقوبات.

والجزائر كغيرها من الدول ليست في منأى عن هذه الأشكال من الجرائم كونها خطت خطوات لا بأس بها في مجال المعلوماتية وطبيعي أن المشرع لم يبقى مكتوف الأيدي إزاء هذه الوضعية فتم إدراج أحكام تتعلق بالجرائم المعلوماتية في قانون العقوبات

وبناءا على ما سبق يمكن طرح الإشكالية التالية:ما مدى كفاية النصوص العقابية الحالية لمنع الجرائم المرتكبة في نطاق المعاملات الإلكترونية؟ وهل المواجهة الجنائية هي الحل الأمثل؟

المبحث الأول:مفهوم الجريمة المعلوماتية و خصائصها

المطلب الأول: مفهوم الجريمة المعلوماتية

وصفت الجريمة المعلوماتية بأنها جريمة تقاوم التعريف، نتيجة اختلاف التعريفات وتفاوتها حيث تعددت الآراء والأفكار بشأن المفهوم، فهناك من اعتمد في تعريفه على الجانب الفني وهناك من اعتمد على الجانب القانوني وهناك من اعتمد على معايير أخرى مختلفة ومن بين هذه المحاولات التعريف الصادر عن منظمة التعاون الاقتصادي للتنمية (OCDE)حيث عرفت الجريمة المعلوماتية "بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1]

ومن جهة أخرى قد عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا 2000الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو

[1]أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، مصر ،2005، ص96.

شبكة حاسوبية أو داخل نظام حاسوب والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي ارتكابها في بيئة إلكترونية"[1]

قد عرفت كذلك بكونها "كل فعل غير مشروع اقترن بالتواصل مع منظومات معلوماتية وشبكات الاتصال الخاصة به، والتي يحميها قانون العقوبات ويفرض عقابا لها "[2]

وصفوة القول فإن مفهوم الجريمة المعلوماتية يكتنفه العديد من الصعوبات كونه يستخدم لوصف طائفة واسعة من الأفعال الإجرامية.

المطلب الثاني:خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بخصائص تميزها عن الجرائم التقليدية وتمنحها طابعا خاصا، ولعل أبرز هذه الخصائص فيما يأتي:

1-الطبيعة العالمية والافتراضية للجريمة المعلوماتية

فهي جريمة عالمية بطبيعتها، إن شبكة الأنترنت تتيح ممارسة أي نشاط غير مشروع على الصعيد الدولي ولذلك من الضروري ان تغير جميع الدول قدارتها المحلية في المكافحة حتى لا تظل الجريمة المرتكبة في الفضاء الإلكتروني بعيدة المنال، ويستخدم المجرمون عباءة الأنترنت ليتصفحوا في فضاء لا يعرف له حدود فهو عالم افتراضي يتمتع دوما بمكان للاختباء[3]فقد ترتكب الجريمة عن طريق حاسوب في دولة ما فحين يتحقق الفعل

[1] خالد عباد الحلبي، إجراءات التحدي والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 29.

[2] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، مصر،2009، ص158.

[3] Titoutche Radia,Territorialité du droit pénal et cybercriminalité,revueCahiers de Politique et de Droit, n°1, Janvier2019, p30.

الإجرامي في دولة أخرى فتثير الطبيعة القانونية لهذه الجرائم عدة مشاكل كمشكلة السيادة والاختصاص القضائي منها مبدأ إقليمية النص الجزائي الذي يفيد قواعد القانون الجنائي لا تطبق إلا في حدودالإقليم الخاضع للدولة وتكمن الصعوبة في أن القوانين الجزائية تخلف من بلد لآخر وقبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى لذلك وجب التعاون الثابت بين الدول الذي بدونه ستدمر كل الجهود.

2-الجريمة المعلوماتية فادحة الأضرار

تتميز الجريمة المعلوماتية بكلفتها الباهضة فقد أشارت دراسة جديدة أصدرها مركز الدراسات الاستراتيجية والدولية CSIS إلى أن الجرائم الإلكترونية تكلف الاقتصاد العالمي نحو 445 مليار دولار سنوياً، وأن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة الملكية الفكرية تتسبب بخسارة للأفراد بحوالي 160 مليار دولار.وذكرت الدراسة أن الجريمة الإلكترونية تعتبر صناعة نامية تضر بالتجارة والقدرة التنافسية والابتكار .وتشير التقديرات الخاصة بالدراسة التي ترعاها شركة البرمجيات الأمنية "مكافي" إلى أن الخسائر وصلت إلى 375 مليار دولار، في حين أن الحد الأقصى لتقديرات الخسائر قد يبلغ 575 مليار دولار. ومن جهته قال جيم لويس، أحد المحللين في مركزCSIS ، إن الجريمة الإلكترونية هي عبء ثقيل على الابتكار، كما أنها تبطئ وتيرة الابتكار العالمي من خلال تقليل معدل العائد للمبدعين والمستثمرين.[1]

3-صعوبة اكتشاف وإثبات جرائم المعطيات

[1] الجرائم الإلكترونية تكبد الاقتصاد العلمي خسائر باهضة، مقال منشور في الموقع الإلكتروني https://www.mcit.gov.sa/ar/media-center/news/94698 اضطلع عليه يوم 2020/03/19.

صاحب ظهور الحاسوب وشبكة الأنترنت تحديات جديدة للقانون الجنائي بشقيه الموضوعي والإجرائي، بما يفقد قانون الإجراءات الجزائية أهميته وفعاليته. ومما يزيد الأمر صعوبة جمع الجريمة المعلوماتية بين سرعة الانتشار وصعوبة الإثبات فإذا كانت سرعة الانتشار تعود الي الطبيعة العالمية لهذه الجريمة فإن صعوبة إثباتها راجع إلى طبيعتها اللامادية التي تجعل من محو الأدلة أمرا سهلا إذا يمكن للمجرم الإلكتروني محو مئات الآلاف من البيانات في ضغطة زر.[1]

4- عدم قدرة نصوص التجريم التقليدية على مسايرة الجريمة الإلكترونية

يعد التطور السريع في الميدان المعلوماتي من أهم العوائق التي تحول دون مكافحة الجريمة المعلوماتية بطريقة ناجعة .ففي كل يوم تظهر تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مجاراته من طرف السلطة التشريعية، بحيث أصبحنا نعيش فيما يمكن أن نسميه الطوفان الرقمي، فإن أكثر دول العالم تعتمد في مواجهة جرائم المعلوماتية التي وجدت لمواجهة الجرائم التقليدية المتعارف عليها .وفي المقابل تعجز السلطات القضائية أحيانا، عند تعهدها بعض القضايا المتعلقة بالجريمة المعلوماتية ،على ردع المتهمين احتراما لمبدأ الشرعية [2]

[1] محمد فتحي، تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة، المركز القومي للإصدارات القانونية، مصر،2012، ص504.

[2] Titouche Radia, Territorialité du droit pénal et cybercriminalité, *Op cit*, p32.

المبحث الثاني:الجرائم الواقعة على أنظمة المعالجة الأليات للمعطيات في القانون الجزائري

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه للتدارك الفراغ التشريعي عمد منذ الألفيةالثانية الى تعديلالعديد من القوانين الوطنية، بما فيها التشريعاتالعقابيةوعلى رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال.

المطلب الأول:الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات

لقد استحدث المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون 15/04 المؤرخ في 10 نوفمبر 2004 [1] بإدراج القسم السابع مكرر وخصصه للاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات حيث جرم بعض الأفعال وحدد لها عقوبات

- جريمة الدخول والبقاء الغير المشروع إلى نظام المعالجة الآلية

لقد نص المشرع على فعل الدخول L'accès في المادة 394مكرر[2]"يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة مالية من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

---

[1] قانون رقم 04-15 مؤرخ في10نوفمبر2004يعدل ويتمم الأمر 66-156المؤرخ في 08جوان 1966المتضمن قانون العقوبات ج رعدد 71.

[2] المادة 394مكرر منالقانون رقم 06-23 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر 66-156المتضمن قانون العقوبات ج رالعدد84.

ويقصد بالدخول هو ذلك النشاط المتمثل في الاتصال بنظام الكمبيوتر، يهدف الفاعل من خلاله إلى الاطلاع على المعلومات التي يحتويها النظام وحسب نص المادة المذكورة أعلاه لكي يكون الدخول مجرما لا يشترط أن يقع على كامل النظام، بل يكفي أن يقع الدخول على جزء منه واشترط كذلك أن يكون الدخول عن الغش غير أنه لم يحدد وسائل وطرق الغش.

فضلا عن الدخول في النظام فإن المشرع أضاف ما يعرف بالبقاءle maintien في نظام المعالجة الآلية للمعطيات ويتمثل هذا النشاط في مكوث الفاعل واستمراره داخل نظام الكمبيوتر بعد دخوله ولو عرضا أو يجاوز الوقت المسموح به للبقاء [1]

وقد نصت في الفقرة الثانية من المادة 394 مكرر على "تضاعف العقوبة إذا ترتب على ذلك حذف أو حذف لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتعال المنظومة تكون العقوبة من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى300.000 دج."[2]

- جريمة التلاعب بأنظمة المعالجة الآلية للمعطيات

نص عليها المشرع الجزائري في المادة 394 مكرر1 على أنه "يعاقب بالحبس من ستة أشهر (6) أشهر إلى ثلاث (3) سنوات وبغرامة مالية من 500.000 دج إلى 400.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."[3] فقد تختلف أسباب الاختراق باختلاف

[1] شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة للنشر، مصر ،2007، ص99.

[2] المادة 394 مكرر/2 من القانون06-23المعدل والمتمم، المرجع السابق.

[3] المادة 394 مكرر1 من القانون 06-23 المعدل والمتمم، المرجع نفسه.

أهداف المخترق فمنهم من يخترق لمجرد الفضول والبعض الذي يخترق لسرقة المعلومات من حواسب الغير قد يكونوا عرضوها مقابل بدل مالي للاطلاع عليها. أما سبب الاختراق الذي أشار إليه المشرع فيكمن في نية المخترق في تبديل أو تحريف أو إزالة المعلومات في أجهزة الغير وهذا أخطر أنواع الاختراق.

- جريمة الاستعمال الغير المشروع لأنظمة المعالجة الآلية للمعطيات

نصت المادة 394 مكرر2[1] من قانون العقوبات "يعاقب من بالحبس من شهرين (2) إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 10.000.000دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل من إحدى الجرائم المنصوص عليها في هذا القسم"

وعليه يعد مرتكبا لهذه الجريمة كل من يستخدم البرامج المخزنة آليا بقصد الحصول على منفعة غير مشروعة، بمعنى الاستخدام الغير مصرح به لإمكانيات نظام المعالجة الآلية للمعطيات من أجل تحقيق منفعة شخصية.

- التشديد في حالة المساس بالمصالح العليا للوطن

[1] المادة 394 مكرر2من القانون 06-23المعدل والمتمم، المرجع السابق.

نص المشرع الجزائري في المادة 394مكرر3 [1]"تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد"

المطلب الثاني:الجرائم المعلوماتية الماسة بالأشخاص

لقد أتاحت الثورة الرقمية للمجرم المعلوماتي تسخير الحاسوب لتحقيق أغلب صور الاعتداء على الأشخاص وذلك بأبسط الأساليب من خلال التلاعب بأنظمة المعالجة الآلية للمعطيات

- جرائم السب والقذف في صورتها المعلوماتية

تعد جرائم السب والقذف من أكثر الجرائم انتشار، وهي جرائم للمساس بشرف الغير وسمعتهم ويكون عن طريق القذف والسب كتابيا، أوعن طريق المطبوعات أور رسوم، عبر البريد الإلكتروني، صفحات الويب بعبارات تمس الشرف[2]ولقد اعتبر المشرع الجزائري صراحة أن من بين مكونات الركن المادي لارتكاب هذه الجريمة أن تكون موجة لشخص الرئيس لاعتبار هذا الأخير من رموز السادة الوطنية وهذا ما نصت عليه المادة 144 مكرر[3]"يعاقب بغرامة من 100.000دج إلى 500.000دج،كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو

[1]المادة 394 مكرر3 من القانون 06-23المعدل والمتمم، المرجع نفسه.

[2]خالد حسن أحمد لطفي، جرائم الأنترنت "بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني"، دار الفكر الجامعي، مصر، الطبعة الأولى، 2018، ص31.

[3]المادة 144من القانون 11-14 المؤرخ في 2 غشت 2011يعدل ويتمم الأمر 66-156المتضمن قانون العقوبات ج رالعدد44.

التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية "

- جرائم الاعتداء على حرمة الحياة الخاصة

تعتبر جرائم الاعتداء على حرمة الحياة الخاصة من الجرائم القديمة التي عرفتها المجتمعات الإنسانية القديمة ولكنها سرعان ما تطورت نظرا للتقدم التكنولوجي الذي لعب دور في سرعة وسهولة انتشار الأخبار والصور الذي من شأنه أن يمثل تهديدا لخصوصية الأشخاص وسهولة الاعتداء على حرمة حياتهم الخاصة ومن هنا كانت الحاجة إلى وجود حماية قانونية صارمة تساهم في الحد من هذه الجرائم [1] وهذا نصت عليها المادة 303 مكرر[2]" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث سنوات وبغرامة من 50.000دج إلى 300.000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1-بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2-بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه."

المطلب الثالث:مكافحة الجريمة المعلوماتية بموجب هياكل خاصة

[1] جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص، مقال منشور على الموقع الإلكتروني https://scholarworks.uaeu.ac.ae/cgi/viewcontent اضطلع عليه يوم 03/21 /2020.

[2] المادة 303 مكرر من القانون 06-23المعدل والمتمم لقانون العقوبات.

تدخل المشرع الجزائري لمكافحة هذه الظاهرة الإجرامية الحديثة بوضع هيئات قانونية لمكافحة هذا النوع من الجرائم

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته

نصت على إنشاء هذه الهيئة المادة 13 [1]من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وحسب نص المادة من الثانية من مرسوم الرئاسي 19-127[2]تعتبر " الهيئة مؤسسة عمومية ذات الطابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع "

أما فيما يخص مهامها فنصت عليها المادة 14 من القانون 09/04[3]"تتولى الهيئة الذكورة في المادة 13 أعلاه، خصوصا المهام الآتية:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

-مساعدة السلطات القضائية ومصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

_تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد تواجدهم."

---

[1] المادة 13 من القانون 04/09 المؤرخ في 5غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ج ر العدد 47.

[2] المادة 02 من مرسوم 19-127 المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما وتنظيميها وكيفيات سيرها ج ر العدد 37.

[3] المادة 14 من القانون 04/09، المرجع نفسه.

أما فيما يخص تشكيلها قد نص عليه المادةالثالثة من مرسوم 19-127[1] " تنظم الهيئة من مجلس توجيه ومديرية عامة " حيث يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثله ويتشكل من ممثلي الوزارات الآتية:وزارة الدفاع الوطني، وزارة المكلفة بالداخلية وزارةالعدل الوزارة المكلفة بالمواصلات السلكية واللاسلكية وتتولى المديرية العامة أمانة المجلسفحين تضم المديرية العامة: مديرية ومديرية للإدارة والوسائل ومصالح[2].

بعدما كانت تضمهذه الهيئة حسب المادة 06 مرسوم 15 – 261 [3]الذي يحدد تشكيلة وتنظم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لجنة مديرة ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية التنسيق الإلكتروني ومركز للعمليات التقنية وملحقات جهوية حيث يترأس اللجنة المديرة الوزير المكلف بالعدل

فنستشف من المرسومين السالف ذكرهما أنه تغيرت الوصاية على الهيئة من وزارة العدل إلى وزارة الدفاع الوطني فحين لدى هذه الهيئة مديرية تقنية مسؤولة على مساعدة السلطات القضائية في مكافحة جرائم تكنولوجيا المعلومات والاتصالات ويبقى السؤال المطروح فإذا كان هذا الجهاز في خدمة العدالة فلماذا لا يبقى تحت سلطته؟

الخاتمة

أصبحت المعلوماتية سمة العصر وبات استخدام الأنظمة المعلوماتية من قبل الأفراد والمؤسسات المقياس الذي يحدد مدى تطور الشعوب وتقدمها، فتكنولوجيا المعلومات

[1] المادة 03 من المرسوم 19-127، المرجع السابق.

[2] المادة05 و10 من المرسوم 19-127، المرجع نفسه.

[3] المادة 06 من المرسوم 15-261 المؤرخ في 8 أكتوبر 2015،الذي يحدد تشكيلة وتنظم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر53.

تساهم في تسريع إنجاز الأعمال، الأمر الذي يعني تنفيذ الأهداف والخطط التي ترسمها الدول وذلك في وقت قياسي.

فمن البديهي ان تكون نتيجة هذا التطور السريع والمتواصل في مجال المعلوماتية وتكنولوجيا الإعلام والاتصال ظهور أنماط جديدة من الجرائم لم تكن معهودة في السابق، إذا ان المجرم والجريمة في تطور مستمر حيث أضحى النظام المعلوماتي ذاته محلا للاعتداء.

ولقد ألقى هذا التطور المعلوماتي مسؤولية كبيرة على عاتق المشرع الجزائري مما أدى إلى تعديل قانون العقوبات وظهور قوانين خاصة لمكافحة جريمة المعلوماتية وكان يهدف من خلاله لخلق قاعدة قانونية موضوعية تحدد بالتفصيل كل الجرائم المتعلقة بتقنية المعلوماتية ووضع إطار لها حتى يتسنى للقضاء متابعتها وفقا لإجراءات خاصة.

وفيما يلي بعض الاقتراحات التي ارتأينا أن تكون ناجعة لتعزيز لمكافحة جريمة المعلوماتية

–التوقيع على اتفاقيات الدولية بشأن التعاون القضائي مع أكبر عدد ممكن البلدان.

– ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.

– الاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن صورة.

– تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية والحد من أوثارها.

قائمة المراجع

أولا مراجع باللغة العربية

- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، مصر ،2005.
- خالد عباد الحلبي، إجراءات التحدي والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، مصر،2009.
- محمد فتحي، تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة، المركز القومي للإصدارات القانونية، مصر،2012.
- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة للنشر، مصر ،2007.
- خالد حسن أحمد لطفي، جرائم الأنترنت "بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني"، دار الفكر الجامعي، مصر، الطبعة الأولى، ،2018.
- القانون 11-14 المؤرخ في 2 غشت 2011يعدل ويتمم الأمر 66-156المتضمن قانون العقوبات.
- القانون 04/09 المؤرخ في 5غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- مرسوم 19-127 المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما وتنظيميها وكيفيات سيرها.

- القانون رقم 06-23 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر 66-156المتضمن قانون العقوبات.

ثانيا: المراجع الأجنبية

- Titoutche Radia,Territorialité du droit pénal et cybercriminalité,revueCahiers de Politique et de Droit, n°1, Janvier2019.

ثالثا: مواقع الأنترنت

https://scholarworks.uaeu.ac.ae/cgi/viewcontent

https://www.mcit.gov.sa/ar/media-center/news/94698