مجلة العلوم القانونية و الاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

التنظيم القانوني للجريمة المعلوماتية في الجزائر

Legal Regulation of Cyber-Crime in Algeria

بدر الدين خلاف*

جامعة عباس لغرور خنشلة، (**الجزائر**)، badro.khellaf@gmail.com

تاريخ ارسال المقال: 2021/04/30	تاريخ القبول: 2021/05/17	تاريخ النشر: 2021/06/01

***المؤلف المرسل**

الملخص:

وإن تأخر المشرع الجزائري مقارنة مع بقية التشريعات الوطنية الأخرى في معالجة الجريمة الإلكترونية والتصدي لها إلا أن تطور وسائل الاتصال وتشعبها والاعتماد عليها في المعاملات والعلاقات الاجتماعية بشكل كلي سواء تلك المتعلقة بمواقع التواصل الاجتماعي أو الوسائل المعلوماتية وفي ضل تزايد خطورة هذه الجرائم على الدولة والمجتمع واستجابة لتوقيع الجزائر، على المعاهدات الدولية و الإقليمية التي تكافح هذه الظاهرة بادر المشرع الجزائري إلى سن مجموعة من القوانين من أجل مكافحة الجرائم المتعلقة بالحاسب الآلي، بما يساعد على مكافحة هذه الجريمة وتعاقب مرتكبيها وطنيا ودوليا.

الكلمات المفتاحية: الجريمة الالكترونية; وسائل الاتصال ; الحاسب الالي; مواقع التواصل الاجتماعي; الاتفاقيات الدولية

Abstract :

The Algerian legislator was late compared to other national legislations in dealing with and addressing cybercrime. However the development of the means of communication, its bifurcation and the complete reliance on it in transactions and social relations, whether those related to social media or information means, and in the light of the increasing seriousness of these crimes on the state and society and in response to the signature of Algeria on the regional international front that combats this phenomenon, the Algerian legislator has initiated a set of laws in order to combat computer-related crimes, in a way that will help combat this crime and punish its perpetrators nationally and internationally.

Keywords: cyber-crime; Means of communication; computer; Social Media; International agreements.

مقدّمة:

تعتبر الجريمة المعلوماتية من الجرائم التي ارتبطت تسميتها بتقنية التكنولوجيا المعاصرة، إذا ما وقعت على الحاسب الآلي أو داخل نظامه، فمتى ما كان محل الجريمة هو الحاسب وما يحتويه من مضامين معلوماتية ومعطيات وبيانات، أو نظامه المعلوماتي تحمل الجريمة وصف المعلوماتية، وقد اقترن هذا النوع من الجرائم بما تشهده الحياة اليومية من تطورات متسارعة في مجال تقنيات المعلومات، مما جعل هذه البيئة مجالا خصبا لارتكاب صور متعددة من الجرائم عبر وسائل الاتصال الحديثة التي تعتمد بشكل كبير على وجود الشبكة العنكبوتية، وتباينت صور هذه الجرائم بين ما يمثل اعتداء على ذات النظام الإلكتروني، ومنها ما يتعلق بالاعتداء على المعلومات، ومنها ما يتعلق

بالاحتيال والتزوير الإلكتروني[1]، وغيرها من الأشكال الأخرى التي هي في تطور مستمر من حيث الأساليب التي يتم اعتمادها في ممارسة هذا النوع من الجرائم.

ان التطور الزمني المرتبط بتكنولوجيا المعلومات والاتصالات[2] لم يمنع من وجود جملة من الآثار السلبية التي أفرزها سوء استخدام هذه التكنولوجيا أو كذلك بسبب أن كل تطور في مجال يكون دائما سلاح ذا حدين، وهو ما ينطبق على استخدام شبكة الأنترنت التي لها انعكاسات سلبية كبيرة على الأفراد والمجتمعات في حال سوء استخدام الأنظمة المعلوماتية التي تحتويها، مما ساهم في انتشار نوع جديد من الجرائم التي لا تختلف عن الجرائم التقليدية إلا من حيث الوسيلة التي أصبحت متطورة.

وادراكا من الدول لخطورة هذه الجريمة، كان من الضروري تعديل النصوص القانونية بما يوفر الحماية الكافية من أجل التصدي لها، كما هو الحال بالنسبة للمشرع الجزائري الذي عمد الى تعديل بعض القوانين واستحداث قوانين جديدة من أجل التصدي للجريمة المعلوماتية.

وعليه يمكننا صياغة الإشكالية التالية: الي أي مدي تمكن المشرع الجزائري من إيجاد منظومة قانونية فعالة لمكافحة الجريمة المعلوماتية؟

وقد اعتمدنا على النهج الوصفي التحليلي للإجابة على هذه الاشكالية وذلك بالتعرف علي النصوص القانونية لردع الجريمة المعلوماتية وتحليلها للوقوف علي مدي فاعليتها في التصدي لها

اما تقسيم الدراسة فكان وفقا للمحاور التالية:

المبحث الاول–مفهوم الجريمة المعلوماتية.

المبحث الثاني–أركان الجريمة المعلوماتية.

المبحث الثالث–مواجهة الجريمة المعلوماتية في التشريع الجزائري.

المبحث الأول: مفهوم الجريمة المعلوماتية

إن تحديد مفهوم الجريمة المعلوماتية يقتضي منا تعريفها وبيان خصوصيتها وفقا لما سنوضحه ضمن الآتي:

المطلب الأول: تعريف الجريمة المعلوماتية

تباينت تعاريف الجريمة الإلكترونية بحسب ما إذا ارتكبت في مجال معلوماتي مغلق أو مفتوح على الشبكات المعلوماتية[3]، ومن التعريفات التي أدرجت بشأن هذه الجريمة:

الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته من ناحية أخرى[4].

الجريمة المعلوماتية هي كل فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية[5]، فهي تعتمد بشكل أساسي على وجود الحاسب الآلي الذي يمثل الأداة الرئيسية لوجود جريمة معلوماتية.

اتجه جانب كبير من الفقه الى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية للجريمة المعلوماتية، بأنها" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو

نقلها"، هذا التعريف يشتمل على كل من وصف السلوك الإجرامي واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها[6].

الجريمة المعلوماتية هي الجريمة التي ترتكب بهدف تحقيق عوائد مالية ضخمة جراء أعمال غير شرعية في الاقتصاد الدولي عبر شبكة الانترنت، وقد تكون هادفة الى التخريب والاضرار بالغير ، أو سلوك مناف للأخلاق وغير مشروع يرتبط بالمعالجة الآلية للبيانات أو نقلها، ويمكن حصر مجالها في نوعين النوع الأول يقع على جهاز الكمبيوتر والوسائل الالكترونية نفسها وما يشملها من أنظمة وبرامج والنوع الثاني يتعلق بالجرائم التي تتخذ الوسائط الالكترونية وسيلة لتحقيق مآربها الجرمية[7].

ومن الاتفاقيات الدولية المهمة التي تم إبرامها لمكافحة الجريمة المعلوماتية، الاتفاقية الخاصة بالإجرام المعلوماتي بودابست في 23-11-2001 التي نصت في المادة (11)، " تقوم كل دولة طرف بالاتفاقية بإقرار هذه الاجراءات التشريعية وغيرها من الاجراءات الأخرى، كلما كان ذلك ضروريا، لإصدار نص تشريعي أو قانوني بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكاب عن قصد، من حيث المساعدة، أو التحريض على ارتكاب أية جريمة من الجرائم النصوص عليها وفقا للمواد من 2-10 الخاصة بالاتفاقية بقصد ارتكاب مثل هذه الجريمة"، فقد جرمت كل فعل اتفاق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات في عبارة من حيث المساعدة، واعتبرت ذلك من قبيل الجريمة المعلوماتية.

أما المشرع الجزائري فقد اعتمد في تعريفه للجريمة المعلوماتية على اصطلاح المساس بأنظمة المعالجة المعلوماتية الآلية للمعطيات للدلالة على هذه الجريمة، وينصرف هذا المصطلح الى المعلومات والنظام الذي يحتوي عليها، من خلال المادة (02) من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، اذ نصت على أنه يقصد في مفهوم هذا القانون ما يأتي:

– الجرائم المتصلة بتكنولوجيات الاعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات في المواد من 394 مكرر الى 394 مكرر7، وأي جريمة أخرى يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية.

– منظومة معلوماتية وهي أي نظام منفصل أو مجموعة من الانظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

– معطيات معلوماتية وهي كل عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها مقدمو الخدمات سواء كان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، وأي آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعمليه[8].

ومن خلال ذلك فإن نظام المعالجة الآلية يعتبر شرط أساسي يلزم وجوده حتى نكون أمام جريمة إلكترونية، حيث ان هذا النظام يمثل كل متكامل من آلية منظمة لجمع وتخزين وتوفير معلومات ومعطيات وبيانات

على الحاسب الآلي سواء كانت منقولة عليه أو مخزنة في إحدى آليات التخزين الإلكترونية كالبريد الإلكتروني أو الأقراص أو الأجهزة البرمجية للحاسوب، والتي يسهل الاطلاع عليها واسترجاعها بفضل في أي وقت ممكن وبكل سهوله عند الحاجة إليها.

والجريمة المعلوماتية وفقا لذلك هي كل تصرف يترتب عليه القيام بفعل أو سلوك من شأنه الاعتداء على خصوصية الأفراد ساء كانوا أشخاص عاديين أو موظفين في إطار عملهم، باستخدام تقنية الأنترنت التي تعد الشرط الأساسي لتوافر هذه الجريمة بعد وجود الحاسب الآلي الذي يمثل مخزن نظام المعالجة الآلية للمعطيات.

كما أن المشرع لم يتقيد بتعريف محدد لنظام المعالجة الآلية للمعطيات، وإنما جعل ذلك مرتبطا بالتطورات الواسعة والمستمرة التي تعرفها البيئة الافتراضية، التي قد تقتضي وجود وسائل تقنية جديدة تترتب عنها وجود أشكال أخرى من الجرائم الإلكترونية، واكتفى بإعطاء الإطار العام الذي تدخل تحت نطاقه مختلف الجرائم المعلوماتية الموجودة والتي تستجد مع كل تطور، إذ تتمثل الجريمة المعلوماتية في الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء، كما تشمل الأفعال التي يعتمد في ارتكابها على المنظومة المعلوماتية، فهي تشمل كل أنواع الجرائم التي يتم ارتكابها في البيئة الإلكترونية.

المطلب الثاني: خصوصية الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بخصائص معينة، تعطيها الطابع الخاص لهذا النوع من الجرائم الذي يميزها عن غيرها من الجرائم التقليدية، كما أنها تحدد آثارها التي تنسحب على التحقيق فيها وعلى أطرافها وهي[9]:

أولا– الجريمة المعلوماتية متعدية أو عابرة للحدود الجغرافية:

تقوم هذه الخاصية على وجود بيئة افتراضية تقع في وسط معلوماتي مفتوح، مما يجعل عدم وجود حدود مرئية او ملموسة تقف امام نقل المعلومات عبر الدول والحدود الجغرافية لأي منطقة، كما أن السرعة التي يتم من خلالها تنفيذ الجريمة وحجم المعلومات والمسافة التي تفصل الجاني عن هذه المعلومات، ميزت الجريمة المعلوماتية عن التقليدية بصورة كبيرة، ما يجعل ملاحقة الجناة وكشف جرائمهم عبر الحدود تقتضي من الناحية العلمية أن يتم ذلك في نطاق دولة أخرى[10]، فأهم الخصائص التي تميز هذه الجريمة هي تخطيها الحدود الجغرافية واكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية، لأن أماكم متعددة في مختلف الدول قد تتأثر بجريمة تكنولوجيا المعلومات الواحدة في آن واحد، بالنظر الى سهولة حركة المعلومات عبر تقنية الأنترنت[11].

ثانيا– الجريمة المعلوماتية سهلة الارتكاب:

تقوم خصوصية الجريمة المعلوماتية على سهولة ارتكابها بصورة فردية، إذ لا تحتاج احيانا الاستعانة بأشخاص آخرين لارتكابها، بعكس الجريمة التقليدية، فالمجرم المعلوماتي قادر على تنفيذ مخططه الإجرامي لوحده وهو جالس أمام الكمبيوتر في منزله أو مكتبه أو مقهى للأنترنت ضد ضحية موجودة في دولة أخر تبعد عنه آلاف الأميال، دون الحاجة الى بذل جهود عضلية لممارسة جريمته، كما هو الشأن في الجريمة التقليدية التي تحتاج الى التخطيط والاستعانة بمعدات لتنفيذ الفعل، فقط كل ما يحتاج اليه المجرم المعلوماتي قدر كافي من الخبرة والمعرفة الواسعة بتقنية المعلومات وشبكة الأنترنت والإحاطة ببعض البرامج التشغيلية، وهذه الخاصية بدورها تقلل من

إمكانية تخلف آثار مادية عن الجريمة الواقعة، وهو ما يصعب بدوره من مهمة اكتشاف هذه الجرائم والتحقيق فيها[12]، لكونها تفتقر الى الدليل المادي الملموس وإمكانية تدمير المعلومات التي تستخدم كدليل في الإثبات في مدة تقل عن الثانية الواحدة[13].

ثالثا– الجريمة المعلوماتية تقع في بيئة إلكترونية:

يرتبط وجود الجريمة المعلوماتية بوقوعها في بيئة الكترونية يستلزم التعامل معها استعانة الجاني بوسائل أجهزة تقنية تتمثل في الغالب بوجود الكمبيوتر وملحقاته الأساسية من أجهزة الطبع والمسح الضوئي وأجهزة الربط بالشبكات وغيرها، وحتى أجهزة الهواتف الذكية تعتبر من الوسائل التي تمارس بها هذه الجريمة، وهذه الخاصية هي الأخرى تصعب بدورها من مهمة اكتشاف هذه الجريمة والتحقيق فيها[14].

وعليه فإن الجريمة المعلوماتية يرتبط وجودها بجهاز الحاسوب وشبكة الأنترنت وهو ما يضفي عليها الطابع الخاص الذي يميزها عن غيرها من الجرائم التقليدية، الى جانب الخصوصية التي يتمتع بها المجرم المعلوماتي، بحكم الدراية الكافية والقدرة على استعمال جهاز الحاسب الآلي وسهولة التعامل مع شبكة المعلوماتية للدخول والاعتداء بالفعل أو الامتناع على المعلومات والبيانات التي تخص الغير أيا كانت صفاتهم، كما أن قدرة شبكة المعلومات على نقل وتبادل المعلومات ذات الطابع الشخصي وسعي الأشخاص لربط حواسيبهم بالشبكة للحصول على الخدمات التي يحتاجونها بشكل أسهل وأسرع وبتكلفة أقل، سهل كثيرا من انتشار الجريمة المعلوماتية وتوسعها.

المطلب الثاني: أركان الجريمة المعلوماتية

تقوم الجريمة الإلكترونية على أركان ثلاث، وهي لا تختلف عن الجرائم التقليدية إلا من حيث محلها الذي يكون إما معلومات أو بيانات إلكترونية تتعلق بالمال أو الحياة الخاصة أو مصالح عامة، وتتمثل هذه الأركان في:

المطلب الاول: الركن المادي

ينصب الركن المادي في هذه الجريمة على النظام الإلكتروني الذي يتم الإساءة اليه باستعماله أو لاقتحامه على نحو غير مشروع، بما يكون لذلك الاستعمال من أثر مادي ملموس يأخذ صورة تدمير للمعلومات أو إتلاف عمدي للمعلومات المخزنة على الحاسب الآلي، إذ يكون من الصعب رؤية السلوك الإجرامي في هذه الجريمة على عكس الجريمة التقليدية، لأن هذه الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي بصورة لا يمكن الإمساك بها ماديا، تماما كما هو الحال بالنسبة للتيار الكهربائي الذي يسري في توصيله دون رؤيته[15].

ويمثل الفعل المادي هنا في الدخول والبقاء غير المشروع في نظام المعالجة الآلية ولذي يترتب عليه عرقلة وتعطيل النظام، إضافة الى الاعتداء العمدي على هذا النظام من خلال إدخال ومحو وتعديل للبيانات والمعطيات والمعلومات المحفوظة في النظام.

معنى ذلك أن الركن المادي في الجريمة المعلوماتية يتمثل في الوسط الذي تتم فيه الجريمة ما نعني به الجانب التقني الذي يعتمد على استخدام أجهزة الحاسب الآلي وشبكة الأنترنت، مما يتطلب ضرورة معرفة الوقت الذي

يتم فيه بداية النشاط التقني أو الشروع فيه، حيث يصعب الفصل في هذا المجال بين العمل التحضيري ومرحلة البداية للنشاط الإجرامي، لأن تلك التصرفات لا يمكننا تحديدها بدقة في ظل البيئة الافتراضية التي ترتكب فيها الجريمة المعلوماتية.

المطلب الثاني: الركن المعنوي

يرتبط الركن المعنوي في إطاره العام للجريمة المعلوماتية بالحالة النفسية التي يكون عليها الجاني وبكل شكل من أشكالها، من توافر للقصد الجنائي الذي يكون فيه الجاني محيطا علما بكافة عناصر الجريمة التي يرتكبها، وله علم بأن الفعل الذي يقوم به بنصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج، باعتبارها محل حق يحميه المشرع[16]، فهو يمثل العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، والتي تكون محل جرم يستدعي العقاب ومن ثم يوجه لها لوم القانون وعقابه، ويتوفر القصد الجنائي للجاني في الجريمة المعلوماتية في حالات أساسية[17]:

- إذا كان الجاني يتوقع ويريد أن يترتب على فعله او امتناعه حدوث الضرر أو وقوع الخطر الذي حدث، الذي يعلق عليه القانون حدوث الجريمة المعلوماتية.

-إذا نجم عن الفعل أو الامتناع ضرر او خطر أكثر جسامة مما يقصده الفاعل، وهي حالة جواز القصد التي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف.

- الحالات التي يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضا نتيجة لفعله او امتناعه.

فالجاني في الجريمة المعلوماتية يجب ان يعلم بان نشاطه الجرمي يؤدي إلى تعطيل أو إفساد نظام المعالجة الآلية للمعطيات، وذلك من دون رضاء صاحب الحق مما يجعل هذه الجريمة عمدية وتقوم على تجاهل حقوق الغير من خلال أساليب الدخول والبقاء غير المرخص أو الغش.

المطلب الثالث: الركن الشرعي

يقوم الركن الشرعي في الجرمية المعلوماتية على وجود الصفة غير المشروعة للأفعال المادية الصادرة عن الأفراد، وتتمثل قاعدة التجريم والعقاب في الجرائم الإلكترونية فيما ورد النص عليه من نصوص عقابية خاصة بالأفعال التي تشكل جريمة معلوماتية، إذ يقوم الركن الشرعي على مبدأ الشرعية الجنائية الذي يمنع المساءلة الجنائية ما لم يتوافر النص القانوني لذلك، ومتى انتفى النص على تجريم هذه الأفعال التي لا تطالها النصوص القانونية القائمة، امتنعت المسؤولية.

غير أن تطبيق هذا المبدأ على بعض الجرائم التي ترتكب عبر الأنترنت يعتبر أمرا صعبا، لعدم وجود نصوص كفيلة بمعالجة هذه المشكلات المرتبطة بالاستخدام غير المشروع لشبكة الأنترنت، فهناك أفعال جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص القائمة لمكافحتها، كالاعتداء على حرمة الحياة الخاصة التي لا يعاقب عليها قانون العقوبات الا إذا كان مرتبطا بمكان خاص، أما تجميع المعلومات عن الأفراد وتسجيلها في الكمبيوتر فإنه لا يخضع للتجريم وفقا للقواعد العامة، الى جانب التداخل في نظام الحاسب الآلي وتغيير البيانات،

تعد صور جديدة لا يعرفها قانون العقوبات، مما يؤمد قصور القواعد التقليدية في مكافحة هذا النوع من الجرائم[18].

المبحث الثالث: مواجهة الجريمة المعلوماتية في التشريع الجزائري

من أجل مواجهة الجريمة المعلوماتية، عمد المشرع الجزائري الى إعادة النظر في العديد من التشريعات الوطنية الموجودة، كما استحدث قوانين خاصة من أجل ضمان الحماية الجنائية للمعاملات الإلكترونية، نوضحه كما يلي[19]:

المطلب الاول: مواجهة الجريمة المعلوماتية في إطار القوانين العامة

ركز المشرع في التصدي لظاهرة الجريمة المعلوماتية على تعديل أحكام قانون العقوبات بموجب القانون رقم 04-15، الذي استحدث فيه مجموعة من النصوص جرم خلالها كل الأفعال والسلوكيات المرتبطة بالمعالجة الآلية وحدد لكل فعل الجزاء المقرر له، وتأخذ هذه الأفعال إما وصف الاعتداء على نظام المعالجة الآلية أو وصف الاعتداء على معطيات نظام المعالجة الآلية، كما تأخذ وصف الاعتداء على سير نظام المعالجة الآلية:

أولا: الاعتداء البسيط على نظام المعالجة الآلية للمعطيات:

تعني المعالجة الآلية للمعطيات وفقا للتعريف الذي وضعه مجلس الأمة الفرنسي على أنه" كل مجموعة منسجمة تتكون من وحدة أو عدة وحدات معالجة، ذاكر، برامج، معطيات، وحدات إدخال أو اخرج، واتصال بين هذه المكونات التي تؤدي الى إعطاء نتيجة محددة تكون محمية تقنيا بموجب أي وسيلة أو ميكانزيم ائتمان[20].

وبالرجوع الى تعريف المشرع الجزائري وفقا للمادة (02) من القانون رقم 09-04، نجدها تنصت في الفقرة أن المنظومة المعلوماتية أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وتتمثل صور هذه الجريمة في:

1- الدخول غير المرخص: يمثل فعل الدخول غير المرخص الركن المادي لجريمة الاعتداء على نظام معالجة المعطيات، باستعمال الوسائل الفنية و التقنية الى النظام المعلوماتي ويتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص، ويحدد له المشرع عقوبة الحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج، كما توضحه المادة (394) مكرر من قانون العقوبات، والمشرع بذلك لا يعاقب على الفعل الكامل أي على الجريمة التامة، وإنما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، فلا يكون الدخول صدفة أو خطأ.

2- البقاء غير المرخص: يقصد بالبقاء غير المرخص هو كل تواجد غير كاتصال بواسطة الشبكة المعلوماتية، بالنظام المعلوماتي أي الدخول او النظر في المعطيات التي يتضمنها وغيرها من التصرفات الغير مسموح

بها والتي تشكل بقاء غير مشروع[21]، ويمثل البقاء في رأي نظر المشرع الجزائري ركن مادي للجريمة مثله مثل الدخول، وهو يحمل صورتين مختلفتين[22]:

3- تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعا، حتى وإن كان خطأ أو صدفة، غير انه وبتفطن الفاعل للوضع وبدلا من الانسحاب أو مغادرة النظام فورا، يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.

تحقق فعل البقاء غير المرخص به متصلا ومجتمعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشآن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله.

وفي شأن التداخل المادي بين جريمتي الدخول والبقاء في نظام المعالجة الآلية للمعطيات، من حيث الحد الفاصل بينهما والنطاق الزماني الذي تنتهي فيه كل جريمة، يمكن القول أن بداية سران جريمة البقاء داخل النظام تتحقق بمجرد امتداد الجاني الى التجول والتنقل والاطلاع على ما يحتويه النظام من معلومات وبيانات، دون النظر الى الفترة التي يأخذها في ذلك لأنه هو من يتحكم في هذه المدة، وبرأينا فإن مجرد الدخول لا يعتبر جريمة كاملة فقد يكون ذلك غير مقصود أو بالصدفة بالنسبة للتقنيين والباحثين في مجال التكنولوجيا الذين يرغبون في الاكتشاف المستمر لجديد هذه التكنولوجيا، لكن مجرد اكتشاف الجاني لخصوصيات ومعلومات وفضوله في الاطلاع عليها يعتبر جريمة دخول واعتداء على نظام معلوماتي، وفعل البقاء بذلك يعتبر ركن مادي تتحقق معه نتيجة الاعتداء ووقوع الجريمة.

ثانيا- الاعتداء المشدد على نظلم المعالجة الآلية للمعطيات:

شدد الشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية . بموجب الفقرة الثانية من المادة 394 مكرر من قانون العقوبات على أنه" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج الى 150.000 دج"، ويتمثل ظرفي التشديد في:

- الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام.
- الدخول أو البقاء وتخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته.

وما يلاحظ من ذلك أن المشرع يشترط البحث في النتيجة الإجرامية التي تترتب على الدخول والبقاء، لأن الفعل تجاوز مجرد الدخول أو البقاء الى تغيير في نظام المعالجة الآلية سواء كان ذلك بالمحو أو التبديل للمعطيات أو تعطيل النظام، مما يترتب عليه وجود نتيجة إجرامية تستوجب العقوبة، وبالتالي فإن المشرع أصاب في التشديد هنا، والهدف من ذلك هو الحد من تفاقم الإجرام المعلوماتي وما يرتبه من أضرار بالغة ووخيمة على المجتمع والفرد والدولة ككل[23]، فنكون بذلك أمام إفساد لسير النظام المعلوماتي وتغيير السير العادي له من خلال التأثير السلبي على البرامج والمعطيات الموجودة بداخله[24].

ثالثا- العقوبات المقررة للاعتداء على معطيات نظام المعالجة الآلية:

اقر المشرع عقوبات تختلف بحسب ما إذا كان فعل الاعتداء يخص المعطيات الداخلية للنظام المعلوماتي أو المعطيات الخارجية

1- الاعتداء على المعطيات الداخلية: أقر المشرع لفعل الاعتداء على المعطيات الداخلية عقوبة " الحبس من أشهر إلى 3 سنوات وبالغرامة من 500.000 دج وإلى 2000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنه"، حسب المادة (394) مكرر1 من قانون العقوبات.

2- الاعتداء على المعطيات الخارجية للنظام: أقر المشرع لفعل الاعتداء على المعطيات الخارجية عقوبة" الحبس من شهرين الى 3 سنوات، وغرامة مالية من 1.000.000 الى 5000.000 دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

3- الاعتداء على سير نظام المعالجة الآلية: يقصد بذلك الاعتداء على النظام بتخريبه كما نصت عليه المادة 393 مكرر من قانون العقوبات، والذي من شانه أن يعيب عملية سير النظام والاعتداء على المعطيات الداخلية له واستعمال برامج الفيروسات وبرامج القنابل المعلوماتية من شأنه التأثير في سير أو حسن سير النظام المعلوماتي[25]، وتتخذ الأفعال الماسة بسير النظام عدة صور نذكر منها:

- التعطيل: يصيب التعطيل الأجهزة المادية للنظام مثل تحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي الى عرقلة سير النظام.

- الإفساد: يقصد منه جعل النظام غير صالح للاستعمال بإحداث خلل في نظام سيره وفقدان توازن في أداء وظائفه، كأن يعطي نتائج غير التي كان من الواجب الحصول عليها، ومثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فإنه يحول دون تحقيقه لوظائفه بشكل صحيح.

ما يلاحظ على هذا النوع من الاعتداء أنه لم يخصص له نص خاص بتجريمه، وهو ما يعتبر من النقاط الهامة التي أغفل المشرع عنها، وبالرغم من ذلك حاول المشرع في إطار قانون العقوبات تجريم الجريمة التامة وحتى مجرد الشروع فيها ، كما جرم أفعال وسلوكيات الفاعل والشريك على حد السواء وهو يعد أمر إيجابي للحد من الإجرام المعلوماتي قدر المستطاع، كما حدد مجموعة من العقوبات المقررة لمواجهة الوجه الجديد من الإجرام المعلوماتي وهي[26]، عقوبات أصلية وتتمثل في الحبس والغرامات المالية الى جانب عقوبات تكميلية تكمن في مصادرة الأجهزة والوسائل المستعملة المستخدمة والبرامج.

كما أقرّ بمسؤولية الشخص المعنوي المرتكب لإحدى الجرائم الإلكترونية، ورفع من الحد الأقصى للعقاب إلى 5 مرات عن ذلك القدر المحدد للغرامة المطبقة على الشخص الطبيعي، وتم الإقرار في المادة 394 مكرر 04 من قانون العقوبات بمسؤولية الأشخاص الطبيعيين، حسب المادة (394) مكرر 6، إلا أن المشرع لم يضع عقوبات خاصة للأشخاص المعنوية في حالة ارتكاب إحدى الجرائم التي تتعلق بنظام المعالجة الآلية للمعطيات، والتي حددتها المادة(18) مكرر من قانون العقوبات باستثناء وجود عقوبة الغرامة المقررة للشخص الطبيعي والتي يعاقب بها المجرم المعلوماتي، ونظرا لخصوصية هذه الجرائم فإنّ مشرعنا خصص لها مجموعة من الإجراءات ذات طبيعة مميزة، تنفرد بها هذه الجرائم مقارنة بتلك الجرائم التقليدية، وهي التي جاءت مفصلة في تعديل قانون الإجراءات الجزائية سنة 2006 بموجب القانون رقم 06، تتعلق ب:

4- تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية طبقا للمادة 37 من قانون الإجراءات الجزائية.

- خصوصية التفتيش المنصب على المنظومة المعلوماتية عن ذلك التفتيش المتعارف عليه.
- تمديد آجال التوقيف للنظر لمقترف هذه الجرائم طبقا للمادة 51 فقرة 06 من القانون نفسه.
- نص على إجراءات خاصة للتحري والتحقيق ولاسيما استحداث أسلوب "اعتراض المراسلات والتقاط الصور وتسجيل الأصوات"، طبقا للمواد من 65 مكرر 05 إلى 65 مكرر 10 من القانون رقم 06 -22 سالف الذكر.
- أضاف أسلوب "التسرب" في المواد من 65 مكرر 11 إلى 65 مكرر 18 من القانون، كإحدى الأساليب التي يمارسها ضباط الشرطة القضائية وأعوانهم عند ضرورة التحري أو التحقيق في مجموعة من الجرائم، وفيما يتعلق بشأن إجراءات المحاكمة والمتابعة فهي نفس الإجراءات المطبقة على الجرائم المألوفة والعادية.

المطلب الثاني: مواجهة الجريمة المعلوماتية في إطار القوانين الخاصة

سعيا منه لمواجهة الجريمة المعلوماتية والإحاطة بها بشكل يحد منها فعليا، عمد المشرع الجزائري الى نصوص خاصة تساهم في تفادي وقوع الجريمة المعلوماتية والكشف عنها من خلال:

اولا-القانون رقم 09-04:

وضع المشرع بموجب هذا القانون ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، سعيا منه للحفاظ على النظام العام ومستلزمات التحريات والتحقيقات القضائية[27]:

1- مراقبة الاتصالات الإلكترونية: حددت المادة (04) من القانون رقم 09-04 الحالات التي يسمح فيها بالمراقبة الإلكترونية، سعيا من المشرع لمكافحة الجريمة المعلوماتية وحصرها في:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب او التخريب او الجرائم الماسة بأمن الدولة.
- توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني.

– مقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية.

– تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، استنادا الى اذن مكتوب من السلطة القضائية المختصة.

ومن أجل السير الحسن لآلية مراقبة الاتصالات، وضمان تحقيق الاغراض التي اوجدتها عد المشرع إلى وضع عدة ضمانات، تحقق الممارسة الفعلية لهذه الرقابة منها[28]:

–وضع آلية اقرار المراقبة الالكترونية تحت سلطة القضاء إذ لا يجوز اجراء عمليات المراقبة، الا بإذن مكتوب من السلطات القضائية المختصة، وعندما يتعلق الامر بجرائم الاهاب او التخريب او الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية اذنا لمدة 6 أشهر قابلة للتجديد على اساس تقرير يبين الترتيبات التقنية المستعملة والاغراض الموجهة له.

–تحديد تقنيات الرقابة الالكترونية وحدود استعمال المعطيات المتحصل عليها والتي ترتبط بتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر السابقة، والتقنيات التكنولوجية التي يمكن استعمالها في إطار المراقبة الالكترونية تتمثل في اعتراض المراسلات الالكترونية، تسجيل الاصوات، التقاط الصور، تفتيش المنظومات المعلوماتية وحجزها.

– سن عقوبات لإفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الالكترونية، خاصة وان الموظفين بإمكانهم الاطلاع على عمليات المراقبة الالكترونية والمعلومات ذات الطابع الجرمي أو ذات الطابع الشخصي، فانهم ملزمون باحترام السر المهني وفي حال استغلال عمليات المراقبة لأغراض شخصية او كل تجاوز لحدود المراقبة الالكترونية، نحو انتهاك الحرمة الخاصة للأفراد او افشاء مستندات ناتجة عن التفتيش واطلاع الغير عليها بصفة غير قانونية.

ومن أجل ضمان الحماية الجنائية الفعالة للمعاملات الإلكترونية، تم انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلال المرسوم الرئاسي رقم 15-261 المؤرخ في اكتوبر 2015، الذي يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، تتولى ممارسة اختصاصاتها الحصرية في مجال مراقبة الاتصالات تحت رقابة قاض مختص[29].

2- تفتيش المنظومة المعلوماتية: الى جانب التدابير الوقائية التي أقرها المشرع في القانون رقم 09-04، المتعلقة بمراقبة الاتصالات الإلكترونية، أضاف تدابير إجرائية جديدة نص عليها في قانون الإجراءات الجزائية، منح من خلالها جواز الدخول للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، بغرض تفتيش المنظومة المعلوماتية ولو عند بعد:

– فيما يتعلق منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إن تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى وان هذه المعطيات يمكن الدخول اليها، يجوز تمديد المنظومة او جزء منها بعد اعلام السلطة القضائية المختصة مسبقا.

– منظومة تخزين معلوماتية، فإن ان كانت المعطيات المبحوث عنا مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، يختلف الأمر على الحالة الأولى، لأن الحصول عليها يكون مرتبط بطلب المساعدة من السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، وهذا ما يثير اشكالية القانون الواجب التطبيق، طالما ان ذلك يتعدى حدود اقليم الدولة.

كما أشارت المادة(05) في الفقرة الأخيرة الى اجراء آخر يتمثل في اللجوء الى الاشخاص المؤهلين كالخبراء والتقنيين في الاعلام الآلي وفن الحاسوب لإجراء عمليات التفتيش على المنظومة المعلوماتية وتزويد السلطات المكلفة بالمعطيات التي تحتاجها لعملية التفتيش، ومن اجل تسهيل اجراءات المراقبة.

3– حجز المعطيات المعلوماتية: يتم اللجوء الى هذا الإجراء عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية، واذا استحال اجراء الحجز وفقا لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المعلوماتية والى نسخها، والتي تكون موضوعة تحت تصرف الاشخاص المرخص لهم باستعمال هذه المنظومة، وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، الا في الحدود الضرورية للتحريات والتحقيقات القضائية[30].

ثانيا– القانون رقم 03–05:

أكد المشرع الجزائري في القانون رقم 03–05 المتعلق بحقوق المؤلف والحقوق المجاورة، علىّ ان المصنف الفكري يعتبر من معطيات الحاسب الآلي التي تحتاج الى حماية وعقوبة على من يتعدى على الحق المالي أو الأدبي لمؤلف البرنامج والبيانات، ويُشكل فعل من أفعال التقليد المنصوص عليها في المادة 151 من الأمر رقم 03 – 05 السابق، التي تقرر العقوبات الجزائية المكرسة في المواد 153 – 156 – 157 – 158 من الأمر نفسه[31]، وتحدد المادة (151) فقرة 1 من الأمر رقم 03–05 الجنح المرتبطة بالحق المعنوي للمؤلف، وهي تتمثل في الكشف غير المشروع على المصنف الأدبي والفني، كأن يتم الكشف عن برنامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة، والمساس بسلامة المصنف الأدبي أو الفني، كأن يقوم شخص بتعديل أو تغيير أو حذف أو إضافة أو تحويل على البرنامج أو بيانات الحاسب دون إذن من المؤلف.

أما الجنح المرتبطة بالحق الأدبي للمؤلف، فتتمثل في الاستنساخ غير الشرعي للمصنف يعتمد على قيام الشخص باستنساخ برنامج أو بيانات الحاسب بأي أسلوب كان وجعله في شكل نسخ مقلدة دون إذن المؤلف، كذلك الإبلاغ غير الشرعي للمصنف كأن يقوم شخص بإبلاغ وإعلام عموم الجمهور بمصنف برنامج وبيانات الحاسب دون علم وترخيص من المؤلف سواء كان الإبلاغ مباشر أو غير مباشر، اما الجنح المرتبطة بالمصنف المقلد

فهي تتعلق بالتصرفات والتعاملات التي ترد على المصنف المقلد الذي يمكن ان يكون برنامج أو بيانات الحاسب الآلي.

وفيما يتعلق بالعقوبات المقررة لهذه الجنح، حددت المادة (153) من الأمر رقم 03-05 عقوبات أصلية تتمثل في عقوبة الحبس من 6- أشهر إلى 03 سنوات على كل من ارتكب جنحة تقليد مصنف بما فيها المصنفات المعلوماتية، وبغرامة مالية تتراوح بين500.000 دج و1000.000 دج إضافة الى عقوبات تكميلية تتمثل في:

-مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف.

-مصادرة وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة.

-الأمر بطلب من المتضرر بتعليق ونشر أحكام الإدانة على نفقة المحكوم عليه.

ثالثا- المرسوم الرئاسي رقم 261-15:

يتضمن هذا المرسوم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[32]، تكلف هذه الهيئة الوطنية بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية،

تعمل الهيئة وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائرية وفي هذا المرسوم ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات بحسب مقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، ومن مهامها في مجال مكافحة الجريمة المعلوماتية:

-تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف على الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على رخصة من السلطة القضائية.

-جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المعلوماتية ومكافحتها.

- تزويد السلطات القضائية ومصالح الشرطة بكل ما تحتاج اليه بناء على طلبها او تلقائيا على المعلومات والمعطيات التي تحتاجها في مواجهة الجريمة الإلكترونية والتصدي لها[33].

فالمشرع الجزائري كغيره من الدول قام بسن قوانين من أجل سد الفراغ في مجال الأعمال الإلكترونية وإضافة الى قانون العقوبات الذي تناول فيه بالتجريم مختلف الاعتداءات التي تطرأ على نظم المعالجة الآلية، دعمه بالقانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الى جانب بعض القوانين الخاصة التي أشار فيها الى الحالات التي تعد من قبيل الجريمة المعلوماتية، وقرر لها عقوبات تتناسب والفعل المرتكب.

خاتمة:

إن الجريمة المعلوماتية جريمة مستحدثة ذات طبيعة خاصة لكونها ترتبط بوجود العالم الافتراضي الذي نعيشه والتي يصعب إثباتها لصعوبة الحصول على الدليل المادي الذي يثبتها، بسبب سهولة ارتكابها وعدم التمكن من كشفها في حينها لأنها تقع ضمن بيئة إلكترونية واسعة الفضاء ويصعب التحكم فيها، فهي جريمة تقع

نظام معلوماتي يشمل بيانات أو برامج او صور او معطيات أو رموز مخزنة أو هي في طور النقل والتبادل ضمن وسائل الاتصال المدمجة في الحاسب الآلي.

ولكون الجريمة وإن كانت ترتكب بطريقة إلكترونية تعتمد على تقنية الحاسب الآلي وشبكة الأنترنت، فإنها في كل الأحوال تمثل اعتداء على خصوصية وحقوق الغير، مما يجعلها كغيرها من الجرائم التقليدية تستوجب العقاب على الأفعال التي تؤدي إليها، من حيث البدء في الفعل والأشخاص المشاركين فيه.

وهو ما دفع بالمشرع الى التدخل بإصدار قواعد قانونية تحظر مثل هذه الأفعال، والتي تترتب عليها آثارا خطيرة تمس بخصوصية الفرد والمجتمع، مما يتطلب وجود نصوص تجرمها وتعاقب مرتكبيها تتنوع بين العقوبة البسيطة في حالات لا يكون منها القصد الدخول والاعتداء على معطيات ما والتشديد في الحالات التي يعمد فيها المجرم المعلوماتي للدخول أو الاعتداء على خصوصيات الغير أيا كانت صفتهم، وتكون العقوبة بقدر جسامة الفعل وبقدر ما يخلفه من آثار سلبية تعود على صاحب النظام.

الهوامش:

[1]- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص، 11.

[2]- ملياني عبد الوهاب، جرائم المعلومات في بيئة العمال الإلكترونية، أطروحة دكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر قايد، تلمسان، 2017، ص، 18.

[3]- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير في القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013، ص، 8.

[4]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة1 ، بيروت، 2005، ص 28.

[5]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي الاسكندرية، 2006، ص، 2.

[6]- سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، عدد 7، جامعة محمد خيضر، بسكرة، 2010، ص، 278.

[7]- سمير دنون، العقود الالكترونية في إطار تنظيم التجارة الالكترونية، المؤسسة الحديثة، طبعة 1، لبنان، 2012 ص، 90.

[8]- القانون رقم 09-04 المؤرخ في 5 اوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد 47، بتاريخ 16 اوت 2009.

[9]- ملياني عبد الوهاب، مرجع سابق، ص، 56، 59.

[10]- رابحي لخضر، بن بعلاش خليدة، معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية، الملتقى الدولي حول الجريمة المعلوماتية بين الوقاية والمكافحة، مرجع سابق، ص، 3.

[11]- ملياني عبد الوهاب، مرجع سابق، ص، 57.

[12]-ملياني عبد الوهاب، مرجع سابق، ص، 60.

[13]- رابحي لخضر، مرجع سابق، ص، 4.

[14]- ملياني عبد الوهاب، مرجع سابق، ص، 62.

[15]- عبد الله دغش العجمي، مرجع سابق، ص، 27.

[16]- نائلة عادل محمد فريد قورة، مرجع سابق، ص، 366.

[17]– عبد الله دغش العجمي، مرجع سابق، ص، 30.

[18]– عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015، ص، 17

[19]– ناجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، المجلد 09، عدد 02، كلية الحقوق والعلوم السياسية، جامعة حمة لخضر، الوادي،2018، ص، 688.

[20]– دردور نسيم، مرجع سابق، ص، 20.

[21]– دردور نسيم، مرجع سابق، ص، 34.

[22]– ناجية شيخ، مرجع سابق، ص، 691.

[23]– المرجع نفسه، ص، 692.

[24]– دردور نسيم، مرجع سابق، ص، 38.

[25]– براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، 2016، ص، 137.

[26]– ناجية شيخ، مرجع سابق، ص، 694.

[27]– المادة 03 من القانون رقم 09-04، مرجع سابق.

[28]– امحمدي بوزينة امنة، اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لاحكام قانون الاجراءات الجزائية وقانون الوقاية من جرائم الاعلام، الملتقى الوطني، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص، ص، 73، 74.

[29]– المادة 41 مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة 1436 الموافق 8 اكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية، عدد 53، بتاريخ 8 اكتوبر 2015.

[30]– امحمدي بوزينة أمنة، مرجع سابق، ص، 77.

[31]– ناجية شيخ، مرجع سابق، ص، ص، 265، 266.

[32]– المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر بتاريخ 08 اكتوبر 2015، جريدة الرسمية عدد 16 الصادرة بتاريخ 08 اكتوبر 4051

[33]– المادة 11 من المرسوم الرئاسي رقم 15-261.