

الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة
بتكنولوجيا الاعلام والاتصال

*The Criminality of information under the Penal Code and the law on the
prevention of offenses related to information and communication technologies*

مراد مشوش

مخبر البحث في السياحة، الإقليم و المؤسسات

كلية الحقوق والعلوم السياسية، جامعة غرداية - الجزائر-

البريد الالكتروني: maachouchmourad@yahoo.fr

تاريخ النشر: 2020/06/01

تاريخ القبول: 2020/05/28

تاريخ الاستلام: 2020/05/01

ملخص:

عمد المشرع الجزائري على تطبيق نصوص قانونية خاصة على السلوكيات المنحرفة في مجال المعلوماتية بإفراده نصوصا تجريبية وذلك عندما تطرق إلى تجريم المساس بأنظمة الحاسب الآلي، مما دفعه إلى تعديل قانون العقوبات بالإضافة إلى تقنينه لقانون متخصص يتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية. كلمات مفتاحية: المعلوماتية؛ الجريمة الالكترونية؛ الأنظمة المعالجة الآلية للمعطيات؛ تكنولوجيا الاعلام والاتصال؛ منظومة معلوماتية

Abstract:

The Algerian legislator has applied special legal provisions on deviant behavior in the field of computer science, in addition to abstract texts, when he mentioned the criminalization of computer systems violated, which led him to amend the Penal Code , in addition to codifying a special law containing rules for the prevention of information and communication technology offenses, what complementary procedural rules complement the Code of Criminal procedure and rules of prevention

Keywords: *Infotmatics; Electronic Crime; Automated Processing Systems; Information and Communication Technologies; Information system;*

المؤلف المرسل: مراد مشوش، الإيميل: maachouchmourad@yahoo.fr

مقدمة:

لقد شهد العالم في السنوات الأخيرة تطورا غير مسبوق في مجالات الإعلام والاتصال نظرا إلى توغل وانتشار وسائل التكنولوجيا والابتكارات المستحدثة في الأنشطة المعلوماتية، حيث أصبح العالم قرية صغيرة وهو ما قد يترتب عليه الخطر الكبير على البنيات المختلفة جراء الاستخدام غير المشروع لهذه التقنيات والمساس بالحياة الخاصة للأفراد، والخطر الأكبر هو أن الجرائم المعلوماتية قد تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية وأمنية، ليس هذا فحسب بل حتى الإضرار بالاقتصاد كونه أصبح يعتمد بصورة متزايدة على تقنية معلومات الاقتصاد الرقمي مما قد يؤثر هذا الإجرام التقني تأثيرا كبيرا على الاقتصاد الدولي والمحلي، الأمر الذي أدى إلى الإسراع من أجل محاولة التصدي لهذه الظاهرة الإجرامية المستحدثة، فتضافرت الجهود من أجل إيجاد سبل مكافحتها بفعالية ونجاعة أكبر.

كما أن القوانين التقليدية المطبقة لم تعد مجدية نظرا للاختلاف الكبير بين الجرائم التقليدية والجرائم المعلوماتية التي يعود الأساس إلى الطبيعة اللامادية لها والتي هي من أهم الصعوبات التي تعترى سبل مكافحتها وبفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات ولضمان عدم افلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن احتواء على هذه الجرائم المستحدثة، وصونا لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة بغير نص قانوني.

فالجزائر لم تتضمن في تشريعاتها قبل سنة 2004 بشكل خاص على نظام المعلوماتية أو على تكنولوجيا الإعلام والاتصال ما عدا شبكة الاتصال السلكية واللاسلكية ووسائل الاعلام السمعية والبصرية، قانون 03-2000 المؤرخ في 5 أوت 2000 والمتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية¹ وكذا الامر رقم 03-05 المؤرخ في 19 يوليو سنة 2003

¹ قانون 03-2000 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية عدد 48، المعدل والمتمم بالقانون 04-18 المؤرخ في 10 مايو 2018، الجريدة الرسمية عدد 27، الصادرة في 13 مايو 2018.

والمتعلق بحقوق المؤلف والحقوق المجاورة¹.

أما الهدف الرئيسي من هذا البحث هو إبرازه لمسيرة التطور التكنولوجي وكيف للمشرع الجزائري أن يجد الإطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الإجرامية المستحدثة، لذا تفرض علينا طبيعة هذه الدراسة استخدام كل من المنهج الوصفي والتحليلي عندما نتطرق للسوكات غير المشروعة الماسة بالنظم المعلوماتية، وعليه نطرح الاشكال التالي:

فيما تتمثل الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال؟

ومما سبق نجيب على الاشكال المطروح من خلال مبحثين، أما الاول الذي سنخصصه لدراسة الافعال المجرمة التي استحدثها المشرع الجزائري ضمن قانون العقوبات من خلال تعديلاته المتلاحقة، أما المبحث الثاني نخصصه لما أفردته المشرع بقانون مستقل جاء لتكريس إطار قانوني أكثر ملائمة وانسجام مع خصوصية وخطورة هذه الجريمة.

المبحث الأول

الجريمة المعلوماتية في ظل قانون العقوبات

تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا² بتجريم أفعال المساس بأنظمة الحاسب الآلي³ وذلك نتيجة تأثيره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهد لها البشرية من قبل، مما دفع بالمشرع⁴ إلى تعديل قانون العقوبات بموجب

¹ الأمر 05-03 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، الجريدة الرسمية عدد 44، الصادرة في 23 يوليو 2003.

² في سنة 2000 تم تعديل قانون العقوبات الفرنسي حيث تم إضافة فصلا ثالثا للباب الثاني تحت اسم "الاعتداءات على نظم المعالجة الآلية للمعطيات" Des atteintes aux systèmes de traitement automatisé de données" و جاء من Clément ENDRELIN, Les moyens juridiques de lutte contre la cybercriminalité, Diplôme universitaire sécurité intérieur/extérieur dans l'Union européenne, Institut d'études politiques de Strasbourg, France, 2011, p76

³ Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1^{er} janvier 2002.

⁴ جاء في عرض أسباب هذا التعديل: " وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني في

القانون رقم 15-04 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات¹، والذي أفرد القسم "السابع مكرر" منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات، Des atteintes aux systèmes de traitement automatisé de données" من المادة 394 مكرر إلى 394 مكرر⁷، ونص على عدة جرائم هي²، أما في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات³ بموجب قانون رقم 06-23 حيث مس ذلك التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريبية الواردة في هذا القسم من قانون 15-04، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه، كما أدخل المشرع الجزائري بالقانون رقم 16-02 المعدل والمتمم لقانون العقوبات مادتين وهما 87 مكرر 11، و394 مكرر 8 فاستعمل في الأولى عبارة (تكنولوجيات الإعلام والاتصال)، وفي الثانية عبارة (مقدم خدمات الانترنت)⁴.

المطلب الأول: صور الاعتداءات

تأخذ صور الاعتداء على النظام المعلوماتي في ق.ع.ج صورتين أساسيتين هما⁵، الدخول

بعض المجالات، وسوف يمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد، عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، مصر، 2010، ص 27.

¹ قانون 15-04 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج.ر العدد 71، الصادر 10 نوفمبر 2004، المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية عدد 84 الصادرة في 24 ديسمبر 2006.

² نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات، الجزائر، 2009، ص 128

³ قانون 06-23 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج.ر العدد 84، الصادر 24 ديسمبر 2006، المعدل والمتمم بالقانون رقم 09-01 المؤرخ في 25 فبراير 2009، الجريدة الرسمية عدد 15 الصادرة في 29 فبراير 2009.

⁴ قانون رقم 16-02 مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو سنة 2016، يتم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج.ر عدد 37، الصادرة 22 يونيو 2016.

⁵ حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير في العلوم القانونية تخصص: علم الإجرام

والبقاء في منظومة معلوماتية، أما الصورة الثانية هي المساس بمنظومة معلوماتية، كما تضمن قانون العقوبات صور أخرى للغش في حين أبقى خارج دائرة التجريم بعض الأفعال منها: المساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات حول شخص وتحويل المعلومات الاسمية عن مقصدها¹.

الفرع الأول: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج"، إذن فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

أولاً: فعل الدخول L'accès

يقصد بالدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات²، ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر³.

ثانياً: فعل البقاء Le maintien

يقصد بفعل البقاء التواجد داخل النظام ضد إرادة من له الحق في السيطرة على هذا

وعلم العقاب، كلية حقوق و العلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص 182

² أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، ج1، الطبعة العاشرة، دارهومة، الجزائر، 2009، ص 445

² عائشة بن قارة مصطفى، مرجع سابق، ص42

³ علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، 1999، ص 121

النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلاً عن الدخول على النظام، وقد يجتمعان، ويكون البقاء معاقبا عليه حين يكون الدخول إلى النظام مشروعاً، ومن أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فوراً، ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحاً له فيه الرؤية والاطلاع فقط ويتحقق ذلك أيضاً بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معاً وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلاً ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، إذا كانت تلك الجريمة على هذه الصورة تهدف أساساً إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضاً وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها¹.

أما عن الصورة المشددة لهذه الجريمة، نصت المادة 394 مكرر 3/2: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج"، لذا فإنها تشتمل على طرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الطرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون

¹ عائشة بن قارة مصطفى، مرجع سابق، ص 42

غير معقول، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة، كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير العمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

تجدر الإشارة إلى أن الولوج والتجول والبقاء داخل نظام المعالجة الآلية للمعطيات لا يجزمان إلا تما عمداً كما أن الركن المعنوي لهذه الجريمة تأخذ صورة القصد الجنائي بعنصريه العلم والإرادة، حيث يلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول¹.

الفرع الثاني: المساس بمنظومة معلوماتية

يأخذ السلوك الإجرامي لهذه الجريمة إما الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات أو الاعتداء العمدي على المعطيات²، حيث لم يورد المشرع نصاً خاصاً بالاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام وقد وضع الفقه معياراً للترقية بين الاعتداء على المعطيات والاعتداء على النظام، فإذا كان مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما

¹ علي عبد القادر قهوجي، مرجع سابق، ص 136

² هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص 47

إذا كان الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات¹، يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي والمنتظر منه القيام به، وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية للجهاز أو المعنوية مثل البرامج والمعطيات² وتتمثل النشاطات غير المشروعة لهذه الجريمة في:

أولاً: التعطيل (العرقلة)

تفترض وجود عمل إيجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة سواء مادية أو معنوية وسواء اقترنت بالعنف أم لا، فأما عن الوسيلة المادية فمثلها كسر الأجهزة المادية للنظام، أما عن الوسيلة المعنوية فهي التي تقع على الكيانات المنطقية للنظام كالبرامج والمعطيات، وذلك بإتباع إحدى التقنيات المخصصة لذلك كالفيروسات وغيرها.

ثانياً: الإفساد

هو كل فعل وإن كان لا يؤدي إلى التعطيل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بأن يعطي نتائج غير تلك المرجوة، والافساد يقترب من التعيب الذي يعتبر ظرفاً مشدداً لجريمة الدخول والبقاء غير المشروع، والفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمدياً بينما يتطلب هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات، ومن بين صور الإفساد أو التعيب نجد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال كاستخدام البرنامج المسمى بـ "حصان الطروادة" والذي يقوم بتغيير غير محسوس في البرامج أو المعطيات³، أما الاعتداءات العمدية

¹ هيام حاجب، مرجع سابق، ص 48

² عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية،

أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص 13

³ علي عبد القادر قهوجي، مرجع سابق، ص 143

على المعطيات فلقد نص المشرع الجزائري عليها في المادة 394 مكرر² في قانون العقوبات حيث تأخذ الاعتداءات العمدية على المعطيات الموجودة داخل النظام في إحدى الصور الثلاث التالية¹: الإدخال، المحو، التعديل.

المطلب الثاني: الجزاءات المقررة

أحدث المشرع الجزائري في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الاموال قسم تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات القانون رقم 04-15 السالف الذكر، الذي تضمنت مجموعة من العقوبات تتمثل في:

الفرع الأول: العقوبات المطبقة على الشخص الطبيعي

أولاً: العقوبات الأصلية

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي، يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، إذ نجد سلم الخطورة يتضمن ثلاث درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى، الدرجة الثانية هي جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فهي الجريمة الخاصة بالمساس العمدي بالمعطيات.

أ- الدخول و البقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 3 أشهر إلى سنة حبس و50000 دج إلى 100000 دج غرامة (المادة 394 مكرر).

ب- الدخول و البقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من 6 أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03).

ج- الاعتداء العمدي على المعطيات: طبقاً لنص المادة 394 مكرر² فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من 6 أشهر إلى 3 سنوات وغرامة من

¹ هيام حاجب، مرجع سابق، ص 49

500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى 3 سنوات وغرامة من 1000000 دج إلى 5000000 دج، بالإضافة إلى تشديد العقوبة في الحالات التالية:

- نصت المادة 394 مكرر/2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام الاشتغال.

- نصت المادة 394 مكرر3 على أن تضاعف العقوبات للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام.

د- استعمال تكنولوجيا الاعلام لارتكاب أفعال ارهابية: نصت المادة 87 مكرر 11 استعمال تكنولوجيا الاعلام والاتصال بغرض ارتكاب أفعال إرهابية أو تديرها أو الاعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي التدريب عليها، حيث اعتبرها جنائية يعاقب عليها بالسجن من 05 إلى 10 سنوات وبغرامة من 100.000 إلى 500.000 د.ج.¹

هـ- عدم الامتثال مقدمو الخدمات لإعذارات الموجهة لهم: حيث تضمنت هذه المادة 394 مكرر 8 صور الأفعال التي يعاقب عليها القانون مقدم خدمات الانترنت² عند رفضه لإعذارات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو صدور اوامر وأحكام قضائية، مما يترتب معاقبتهم بالحبس من سنة إلى 3 سنوات وبغرامة 2.000.000 إلى 10.000.000 د.ج أو بإحدى هاتين العقوبتين عندما لا يقوم بـ:

¹ المادة 87 مكرر 11 من القانون 02-16 المتضمن تعديل قانون العقوبات

² جاء تحت مصطلح مقدمو الخدمات ضمن المادة 02 من قانون 04-09 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها:

- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها.

- التدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.
- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة 1 من هذه المادة أو لجعل الدخول إليها غير ممكن.

ثانيا: العقوبة التكميلية

نصت المادة 394 مكرر 3 ق.ع.ج على العقوبات التكميلية والمتمثلة في:

- أ- المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.
- ب- إغلاق المواقع: والأمر يتعلق بالمواقع (Les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- ج- إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكيها مثل إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكيها.

الفرع الثاني: العقوبات المطبقة على الشخص المعنوي

إن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفهم فاعلين أو شركاء أو متدخلين في نفس الجريمة، كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 04/15 الذي ينص على أن: "العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجناح" هي:

أولا: العقوبة الاصلية

الغرامة التي تساوي من 1 إلى 5 مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة (394 مكرر 4).

ثانيا: العقوبة التكميلية

واحدة أو أكثر من العقوبات الآتية:

حل الشخص المعنوي أو غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات،

الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات، المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات، مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها أو نشر أو تعليق حكم الإدانة، الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبةه¹.

نشير بالذكر أن المشرع الجزائري لم يغفل عن معاقبة الاشتراك² حيث تنص المادة 394 مكرر 5 من قانون العقوبات: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية، يعاقب بالعقوبات المقررة بالجريمة ذاتها"، أما عقوبة الشروع في الجريمة نصت عليه المادة 11 من اتفاقية بودابست وتبناه المشرع الجزائري³ في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، كما نصت المادة 394 مكرر 7 ق.ع "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي⁴.

¹ المادة 18 مكرر من قانون 04-15 المتضمن قانون العقوبات المعدل و المتمم.

² هيام حاجب، مرجع سابق، ص 51

³ تبنى المشرع الجزائري بعض الأفكار التي طرحها الاتفاقية، رغم أن الجزائر لم توقع عليها وليست طرفا في هذه الاتفاقية الدولية، انظر، الجريدة الرسمية لمناقشات المجلس الشعبي الوطني، السنة الثالثة، رقم 122، الجزائر، 06 يوليو 2009، ص 21

⁴ عطاء الله فشار، مرجع سابق، ص 35

المبحث الثاني

الجريمة المعلوماتية في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام

والاتصال ومكافحتها

دفع القصور الذي عرفه قانون 15-04 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، مما أدى بالمشروع الجزائري إلى سد الفراغ التشريعي الذي يعرفه هذا المجال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، وذلك بوضع قانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، من أجل تعزيز القواعد السابقة، كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها، كما أخذ المشروع في عين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك تم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حتى يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا.

المطلب الأول: القواعد الإجرائية

لم يشذ المشروع الجزائري عن القواعد العامة المنصوص عليها في قانون الاجراءات الجزائية لكنه أرسى قواعد اجرائية جديدة ذات طبيعة خاصة تكمن هذه القواعد في بعض الاجراءات التي أوردها المشروع الجزائري في قانون 04/09 المشار له سابقا ولعل أهمها يتمثل في:

الفرع الأول: التفتيش

أجاز هذا القانون للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، مع إمكانية اللجوء لمساعدة السلطات الأجنبية

¹ القانون 04-09 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، كما يسمح هذا القانون في المادتين 5 و6 للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها¹، وحجزها.

أولاً: خصائص التفتيش

يمكن استخلاص أهم خصائص التفتيش نظم الحاسوب والانترنت وهي:

أ- إجراء من اجراءات التحقيق: إذ أنه واستنادا لهذا القانون وتحديدًا بموجب نص المادة 5؛ والتي احدثنا على المادة 4 نجد أنه في الفقرة ج "ولمقتضيات التحريات والتحقيقات القضائية" يجوز للسلطات القضائية المختصة وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد"، حيث يوكل التفتيش إلى جهات مختصة قانونًا ويضم خبراء وفنيين في مجالي الحاسوب والإنترنت ويملك هؤلاء المحققون الاستعانة بدورهم بخبراء متخصصين أكثر دراية في هذا المجال.

ب- يهدف إلى البحث على أدلة مادية أو معنوية للجريمة وضبطها: فالتفتيش هو إجراء عملي وليس فني كإجراء مضاهاة البصمات²، وهو يرمي إلى اكتشاف الجريمة والتأكد من وقوعها تم كشف ملامساتها وإقامة الدليل عليها، حيث يركز على نقاط أساسية تسبق عملية التفتيش مثل: مراعاة مدى أهمية الأجهزة والشبكات المتضررة من الجريمة لعمل الجهة المعتدي عليها، مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها، مستوى الاختراق الأمني الذي تسبب فيه لجاني، بعد مراعاة كل ذلك تأتي عملية التفتيش التي تحدد للمحققين نوعية الأدلة الواجب البحث عنها.

ثانياً: محل التفتيش في البيئة الرقمية

يرد التفتيش في نظم المعالجة الآلية للمعلومات على المكونات المادية (HARD WARE)

¹ عطاء الله فشار، مرجع سابق، ص36

² عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب العلمية الالكترونية، دبي،

الإمارات العربية المتحدة، 2003، ص612

والمكونات المنطقية (SOFTWARE) على شبكات الاتصالات البعيدة¹.

أ- تفتيش المكونات المادية لحاسوب: لا تثار أي مشكلة في تفتيش المكونات المادية للحاسوب، كونها ترد على أشياء مادية، وهو ما أكدته المادة 64 من قانون الاجراءات الجزائية سواء كان الحاسوب وملحقاته المادية موجود في أماكن خاصة أو عامة، المنزل أو محمول باليد أو مقهى الانترنت، إلا أن المشرع استثنى في تعديل قانون رقم 22/06 في المواد 3/45 و 2/47 و 3/64 من قانون الإجراءات الجزائية تطبيق هذه الضمانات فيما يخص الجرائم للمعلوماتية؛ أي أن هذه الضمانات لا تراعى في جرائم المعلوماتية، ويرجع السبب في ذلك إلى سهولة التلاعب بالأدلة في الجرائم لمعلوماتية، وسهولة التخلص من الأدلة وإتلافها ومحوها بسرعة كبيرة².

ب- تفتيش المكونات المعنوية للحاسوب: فقد أجاز المشرع الجزائري صراحة تفتيش النظم المعلوماتية بموجب نص المادة 05 من نفس القانون، "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول، بغرض التفتيش، ولو عن بعدة إلى منظومة معلوماتية أو جزء منها وكذا المعطيات لمعلوماتية المخزنة فيها.

ج- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب: نجد أن المشرع الجزائري أجاز صراحة تفتيش نظم المعلومات المتصلة بالحاسوب محل التفتيش، وتسجيل كل البيانات، اللازمة كأدلة إثبات ضد المتهم وفقا المادة 05 من قانون 09-04.

الفرع الثاني: حجز المعطيات

ما من شك أن الهدف الرئيسي لعملية التفتيش هو وضع اليد على الأدلة المادية. وعليه فإن المشرع الجزائري وطبقا لأحكام المادة 6 من القانون 04/09 السالف الذكر، عندما يتوصل المحققون أثناء التفتيش في منظومة معلوماتية إلى وجود معطيات أو بيانات ما من شأنها الافادة في التحقيق وضبط الادلة للكشف عن الجريمة المعلوماتية، يمكن لهم حجز المنظومة برمتها

¹ ابراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، 2009، ص 371

² نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية، مذكرة ماجستير في العلوم القانونية تخصص:

العلوم الجنائية، كلية حقوق و العلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص 145

إذا كان ضرورياً لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق¹.

أولاً: تدابير الحجز

أضفى المشرع الجزائري حماية قانونية لقواعد البيانات بموجب نص المادة 5 الفقرة 2 من الأمر رقم 03-05 المؤرخ في 2005/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، واعتبرها من المصنفات المحمية سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، وطبقاً لنص المادة 6 الفقرة 1 من القانون 04-09 التي تنص: "... يتم نسخ كل المعطيات اللازمة على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقاً للقواعد المقررة في قانون الإجراءات الجزائية"، حيث استعمل المشرع مصطلح دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز مثل: القرص المرن والقرص الصلب والقرص المضغوط والذاكرة الوميضية والأشرطة المغناطيسية... إلخ، كما ترك المجال مفتوحاً أمام ظهور تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها².

ثانياً: الحجز عن طريق منع الوصول إلى المعطيات و حدود استعمالها

يخلق تتبع المجرم المعلوماتي صعوبات تقنية بالغة تحول في كثير من الأحيان دون الكشف عنه و بالتالي إفلاته من العقاب، لذلك نص المشرع في المادة 7 من نفس القانون "إذا استحال إجراء الحجز وفقاً لما هو منصوص عليه في المادة 6 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعية تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة"، والملاحظ، هو عدم تحديد المشرع للأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة بسبب نظام حماية يصعب اختراقه، أو ما تعلق بعملية

¹ عطاء الله فشار، مرجع سابق، ص 36

² أمير فرج يوسف المحامي، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الاسكندرية، مصر، 2012، ص 237.

نسخ المعطيات، إضافة إلى ضمان تكوين دوري بقصد اكتساب أعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم المعلوماتية المهارات المطلوبة لمكافحتها¹. ويبقى الهدف عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية لاستعمالها أو نسخها أو الاطلاع عليها، لأنها تشكل محل الجريمة إذ تحتوي على أدلة قد يتمكن المجرم من تهريبها أو تدميرها أو تعديلها. كما نص المشرع تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة إلا فيما تتطلبه التحريات والتحقيقات القضائية وهذا بموجب نص المادة 09 من القانون 09-04 السالف الذكر.

المطلب الثاني: القواعد الوقائية

تستدعي الجريمة المعلوماتية امكانات و خبرات تقنية لا يمكن مواكبتها إلا عن طريق إنشاء هيئة متخصصة بالإضافة إلى بعض الاجراءات الوقائية سواء من ناحية توعية مستعملي تكنولوجيايات الاعلام والاتصال بخطورة الاستعمال غير الشرعي وكذا محاولة استباق الأفعال الاجرامية من خلال ترصد مكالماتهم وتعقبها.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال

أنشئت بموجب المادة 13 من القانون رقم 04-09، حيث تعتبر الهيئة حسب المرسوم الرئاسي 19-172 الذي يحدد تشكيلتها، مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية، تحت سلطة وزارة الدفاع الوطني كما حدد مقرها بمدينة الجزائر مع امكانية نقله الى مكان اخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني².

أولاً: مهام الهيئة

تمارس الهيئة العديد من المهام في ظل احترام الأحكام التشريعية تتمثل أساساً في:

أ- الوقاية من الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال: وتكون بتوعية مستعملي تكنولوجيايات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون

¹ المرجع نفسه، ص 238

² مرسوم رئاسي 19-172 مؤرخ في 3 شوال 1440 الموافق ل 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيايات الاعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، ج.ر ع 37، الصادرة 9 يونيو 2019

أويستعملون هذه التكنولوجيات ومن أهم هذه الجرائم التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحساب العملاء، أو بطاقات إئتمانهم.... إلخ

ب- مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب المادة 14 من قانون 04-09 نوعان من المكافحة التي تقوم بها هذه الهيئة: مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجرئها بشأن الجرائم المتصلة بهذه التكنولوجيات بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية (المادة 14/ب)، - تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعلومات والمعطيات المفيدة في التعرف على مرتكبي الجريمة وتحديد مكان تواجدهم.

ثانيا: تشكيلة الهيئة وتنظيمها

يتضمن المرسوم 19-172 السالف الذكر تعديلات¹ في الهيكل التنظيمي للهيئة حيث باتت تنظم في مجلس توجيه ومديرية عامة، بعدما كانت تسيرها سلطة إدارية لدى وزير العدل.

أولاً: مجلس التوجيه

أ- تشكيلة المجلس: حدد المادة 05 من نفس المرسوم أعضاء المجلس الذي يرأسه وزير الدفاع أو ممثله، الذي يضم ممثلي وزارات الدفاع، الداخلية، العدل والمواصلات السلوكية واللاسلكية، حيث تتولى المديرية العامة أمانة المجلس، ويجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

ب- مهام المجلس: يكلف المجلس بحسب المادة 6 م نفس المرسوم على الخصوص بالتداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، القيام دورياً بتقييم حالة التهديد في مجال الجرائم

¹ ألغت المادة 24 من المرسوم الرئاسي 19-172 المذكور أعلاه، المرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 53، الصادرة في 8 أكتوبر 2015

للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام والأهداف المنشودة بدقة¹.

ثانيا: المديرية العامة

تتولى المديرية السهر على حسن سير الهيئة من حيث اعداد مشروع ميزانيتها، اعداد وتنفيذ برنامج عملها كما تعمل على تبادل المعلومات مع مثيلاتها الاجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والتعرف عليهم، كما حدد نفس المرسوم كيفية تعيين المدير العام (المادة 19)، الامر بصرف ميزانية الهيئة وكذا مستخدموها طبقا للتنظيم المعمول به في وزارة الدفاع الوطني كما يعاد ادماج القضاة والمستخدمين التابعين للدوائر الوزارية الاخرى العاملين بالهيئة في هياكلهم الاصلية (المادة 20)، كما تضم المديرية العامة مديرية تقنية ومديرية للإدارة والوسائل.

أ- المديرية التقنية: تضم المديرية العامة مديرية تقنية تتكفل على وجه الخصوص بمهمة المراقبة الوقائية للاتصالات الالكترونية في اطار الوقاية من الجرائم الموصوفة بالأفعال الارهابية والتخريبية والاعتداء على أمن الدولة اضافة الى مساعدة السلطات القضائية ومصالح الشرطة بما في ذلك في مجال الخبرات القضائية في اطار مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتلك التي تتطلب اللجوء الى أساليب التحري للهيئة².

ب- مديرية الادارة والوسائل: والى جانب المديرية التقنية تضم المديرية العامة مديرية للإدارة والوسائل توكل لها مهمة تسيير الموارد البشرية والوسائل المالية الخاصة بالهيئة، الاسناد التموييني والتقني، صيانة العتاد والوسائل والمنشآت القاعدية وكذا اعداد احتياجات الهيئة في اطار تحضير تقديرات الميزانية³

الفرع الثاني: مراقبة الاتصالات الالكترونية

نصت المادة 4 من قانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات

¹ للتفصيل أنظر المادة 06 من المرسوم الرئاسي 172-19 السالف الذكر

² جاء ذكر المديرية التقنية ضمن الفرع الأول من القسم الثاني من المرسوم الرئاسي 172-19 في المواد 11، 12، 13 و14.

³ كما جاء ذكر مديرية الادارة والوسائل ضمن الفرع الثاني من القسم الثاني من نفس 172 في المادة 15.

الاعلام والاتصال ومكافحتها الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية¹:

- للوقاية من السلوكيات الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة، بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.

- في حالة توافر معلومات على احتمال القيام بالاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية كما في مجال تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

أولاً: أسباب إباحة مراقبة الاتصالات

لقد قام المشرع الجزائري باستحداث نصوص قانونية تتضمن مصطلحات تحمل مفاهيم تقنية تتناسب مع ضبط الرسائل الإلكترونية، في حالة التلبس، أو التحقيق الابتدائي بصدد عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وتتميز عن النصوص التقليدية في كوها تضمنت جوانب تقنية تسمح بمقتضاها لقاضي التحقيق، أو ضابط الشرطة القضائية المناب أو المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، حيث نصت المادة 65 مكررة على أنه: " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال والإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، حيث يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلوكية أو اللاسلوكية، وتنفذ العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق، كما نصت المادة (3) من نفس القانون على أنه "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات

¹ يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون تخصص: القانون الدولي للأعمال، كلية

الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2013، ص 113

القضائية الجارية، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية¹.

ثانيا: الضمانات المقررة لتنفيذ المراقبة

أ- سرية الإجراءات: تتم العملية بسرية تامة سواء في مواجهة الأشخاص، حيث تتم بدون علمهم، ودون رضاهم كما أنها تتم بسرية في مواجهة الكافة، احتراماً لمبدأ السريته المقر في المادة 45 فقرة 4 من في إ.ج.ج

ب- التسخير: حيث أنه يجوز لوكيل الجمهورية، أو لقاضي التحقيق، أو لضابط الشرطة القضائية أن يسخرعون مؤهل لدى هيئة المكلفة بالاتصالات سواء كانت عامة، أو خاصة للقيام بهذا الإجراء، كما يمكنه طلب المساعدة من قبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، لأن من ضمن مهام هذه الهيئة قانونا هي مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تحبها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال.

ج- المحاضر: يحضر الشخص المكلف بالعملية محضرا يحوي، العناصر الأساسية للعملية، التاريخ، الساعة لبداية ونهاية الإجراء، نسخ المراسلات أو الصور، تحميل البيانات المفيدة للتحقيق... الخ"، ويودع المحضر لدى الجهة القضائية المكلفة، بمعنى أمام وكيل الجمهورية، أو قاضي التحقيق في حالة فتح تحقيق.

د- حماية المعطيات المتحصل عليها: حيث أنه جاء في المادة التاسعة (09) من القانون 04-09 أنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، في حالة استعمال هذه المعطيات خارج هذه الحدود أي التحريات، أو التحقيقات القضائية.

¹ تم المشرع الجزائري الباب الثاني من الكتاب الأول بالقانون رقم 02-06 المؤرخ في 20 ديسمبر 2006 بفصل رابع بعنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" ويشمل المواد 65 مكرر إلى 5 مكرر 10

هـ- الإذن: أشار المشرع الجزائري في نص المادة 04 من القانون 04-09 أنه في حالة ما إذا تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته إذن لمدة ستة (6) أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة، والأغراض الموجهة لها.

أما في غير هذه الجرائم الثلاث فيلجأ إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، وهي تقدم الإذن من قبل قاضي التحقيق، أو وكيل الجمهورية كل حسب اختصاصه، بهدف اعتراض المراسلات مع تحديد العناصر المهمة في الإذن، ويسلم مكتوبا لمدة أربع (4) أشهر قابلة للتجديد عند الضرورة¹.

خاتمة:

حاولت هذه الدراسة إبراز ما قام به المشرع الجزائري من خلال إدراجه لنصوص تجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات ضمن تعديله لقانون العقوبات سنة 2004 ثم 2016، كما استحدث المشرع نصا خاصا في هذا السياق هو قانون الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال، الذي جمعت نصوصه بين قواعد اجرائية خاصة التي تكمل نصوص القواعد العامة المدرجة ضمن ق.إ.ج، وبين الإجراءات الوقائية التي من أهمها استحداثه لسلطة ادارية مستقلة وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمسماة في نفس القانون "بالهيئة"، والتي تعنى ببعض المهام التي تهدف أساسا إلى الوقاية والمكافحة لنوع معين من الجرائم ترتكب بواسطة تكنولوجيات الاعلام والاتصال.

مع هذا ينبغي الاعتراف بحقيقة وهي انه رغم الجهود الجبارة التي يبذلها المشرع الجزائري في

¹ فطيمة جبار، مراقبة الاتصالات الالكترونية بين الحظر والاباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، جامعة مولود معمري تيزي وزو العدد الثالث، الجزائر، ديسمبر 2016، ص 18

سبيل التصدي لهذه لظاهرة الاجرامية، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه نظرا للتطورات السريعة والمستمرة التي تعرفها هذه الظاهرة من جهة، نظرا للطابع العالمي والعابر للحدود الذي تتميز بها هذه الظاهر من جهة أخرى، لذلك لا بد من التفكير في التوجه إلى التعاون التشريعي والقضائي والأمني مع الدول العربية ولما لا مع الدول الغربية والرائدة في هذا المجال والاستفادة من خبراتها في مجال مكافحة هذا النوع المستحدث من الجرائم.

قائمة المصادرالمراجع:

أولاً: باللغة العربية

1. المراجع العامة

- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009.

- ابراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، 2009.

- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، الاسكندرية، مصر، 2010

2. المراجع المتخصصة

- أمير فرج يوسف المحامي، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية الاسكندرية، 2012.

- نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات، الجزائر، 2009

- علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999.

3. النصوص القانونية

- قانون 03-2000 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلوكية و اللاسلوكية، الجريدة الرسمية عدد48، الصادرة في 06 أوت 2000

- القانون 04-15 مؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004.

- القانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 55-165 المؤرخ في 08 يونيو 1965 المتضمن قانون الإجراءات الجزائية، ج.ر.ع 84، الجزائر، 24 ديسمبر 2006.

- القانون 04-09 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .
- قانون رقم 16-02 مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو سنة 2016، يتم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية عدد 37، الصادرة 22 يونيو 2016.

4. الأوامر

- الأمر 05-03 المؤرخ في 19 يوليو 2003 المتعلق ب بحقوق المؤلف و الحقوق المجاورة، الجريدة الرسمية عدد 44، الصادرة في 23 يوليو 2003، ص.3.

5. المراسيم:

- مرسوم رئاسي 19-172 مؤرخ في 3 شوال 1440 الموافق ل 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر ع 37، الصادرة 9 يونيو 2019

6. الرسائل الجامعية

أ- الماجستير

- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير في العلوم القانونية تخصص: علم الإجرام وعلم العقاب، كلية حقوق و العلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012.

- نعيم سعيداني، آليات البحث و التحري عن الجريمة المعلوماتية، مذكرة ماجستير في العلوم القانونية تخصص: العلوم الجنائية، كلية حقوق و العلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012.

- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون تخصص: القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.

ب- المذكرات

هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لإجازة مدرسة القضاء، المدرسة العليا للقضاء، الجزائر، 2008

7. التظاهرات العلمية

- أحمد عمراني، نظام المعلومات في القانون الجزائري، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض، 2010
- عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.
- عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب العلمية الالكترونية، دبي، الامارات العربية المتحدة، 2003.

8. المقالات

- فطيمة جبار، مراقبة الاتصالات الالكترونية بين الحظر والاباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة، جامعة مولود معمري تيزي وزو، العدد الثالث، ديسمبر 2016.
- ثانيا: الفرنسية .

- Clément ENDRELIN, Les moyens juridiques de lutte contre la cybercriminalité, Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen, Institut d'études politiques de Strasbourg, France, 2011.
- Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002.