المعالجة التشريعية للجريمة الرقمية في القانون الجزائري.

تاريخ استلام المقال: 2017/01/12 تاريخ قبول المقال للنشر 2018/03/08

د.مـــزاولي محمد

أستاذ محاضر بكلية الحقوق والعلوم السياسية – جامعة أحمد دراية – أدرار.

البريد الالكتروني:mezaouli@hotmail.com

الملخص:

من منطلق أن تكنولوجيا المعلومات والاتصالات (TIC) تتطور بوتيرة متسارعة وبمعدل أسرع من وتيرة الإصلاحات القانونية، مما يطرح وفي الكثير من الأحيان مسألة الفراغ القانوني، بين ما هو مكرس بموجب نصوص قانونية محددة، وبين التطور الآني الذي تشهده البيئة الرقمية. ذلك أن الإطار القانوني الحالي – في الجزائر على وجه الخصوص – أصبح لا يتماشى والرهانات التكنولوجية الحالية. مما قد يؤدي إلى حالة من التناقضات الناجمة عن تقاطعات يفرضها التطور المذهل لتكنولوجيا المعلومات والاتصالات، والتي غالبا ما لا تحددها الدولة في حد ذاتها، وإنما يفرضها الفاعلين سواء كانوا منتمين للدولة ذاتها، أو أجانب يسيطرون على هذا المجال، بالإضافة إلى مجرمي البيئة الافتراضية.

الكلمات المفتاحية: بيئة إجرامية – أمن– شخص اعتباري –مسؤولية – مؤسسة – قانون – منظومة معلوماتية.

Résumé

Etant donné que la technologie de l'information et de la communication (TIC) évoluent à un rythme plus rapide que les réformes juridique, ce qui engendre le problème du vide juridique. Cela conduira à l'état de contradictions résultant des intersections entre les deux domaines, qui sont déterminées par l'état lui-même, mais plutôt imposées par les acteurs nationaux et étrangers, ainsi que les criminels de l'environnement virtuel. Par conséquent, la première question qui se pose, est de savoir si cette environnement grandissent et se développent en dehors du cadre juridique, au détriment de la sécurité et les intérêts nationaux du point de vue des

institutions juridique et législatives qui sont encore confrontés à des retards dans l'environnement numérique juridique…
Mots Clés: Environnent criminelle– sécurité juridique– société –personne morale –system informatique.

مقدمة:

يعتبر القانون رقم 15-03، المتعلق بعصرنة العدالة،[1] نقطة تحول هامة في منظومة القضاء الجزائري، حيث غير النمط التسييري الكلاسيكي المعتمد بشكل اساسي عن الوثائق المادية، إلى أساليب حديثة تتماشى والتطور العالمي في مجال المعاملات الرسمية، من خلال الولوج الى بيئة الرقمية، تعتمد على منظومة مركزية للمعلوماتية، تؤطر كافة التعاملات القضائية من خلال التصديق الالكتروني وإرسال الوثائق إلكترونيا، إلى جانب استعمال المحادثة عن بعد أثناء الإجراءات والجلسات القضائية.

ولم يكتف التشريع الجزائري عند هذا الحد، بل وسع مجال التعامل في البيئة الرقمية، ليشمل المجالات خارج القطاع القضائي، من خلال القانون رقم 15-04، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين،[2] أين عالج آليات التوقيع الالكتروني، وكذا السلطات التي تشرف عليه، إلى جانب النظام القانوني لتأدية خدمات التصديق الالكتروني.

أهمية الموضوع:

من خلال ما سبق، نلاحظ مدى الأهمية التي اولاها التشريع الجزائري للمعاملات لا سيما المالية منها، والتي تتم وفق نظام شبكات الكترونية، مما

[1] - القانون رقم 15-03 مؤرخ في 11 ربيع الثاني عام 1436، الموافق اول فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية رقم 06، الصفحة 04.

[2] - القانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436، الموافق اول فبراير سنة 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية رقم 06، الصفحة 06.

استوجب ضرورة الوقوف على الأبعاد التي يمكن ان تتخذها المسؤولية الجزائية في هذه البيئة.

فبعد المعالجة التقنية لجريمة المساس بأنظمة المعالجة الآلية للمعطيات[1]، وإمكانية اسناد المسؤولية الجزائية للشخص الاعتباري[2]، والتي اقتصرت بشكل خاص على النصوص الواردة في قانون العقوبات[3]، وقانون الاجراءات الجزائية[4]، سنحاول في هذه الدراسة توسيع مجال البحث لتشمل النصوص القانونية الواردة خارج قانون العقوبات والتي حاولت أن تحدد مجال تطبيق النص الجزائي في البيئة الرقمية بشكل عام، مع التركيز دائما على حدود المسؤولية الجزائية في هذا النوع من الجرائم.

وعلى هذا الأساس يسأل الشخص الإعتباري، عن جرائم تابعيه التي تقترف باسمه ولمصلحته، عن الخطأ في حسن اختيارهم، وعدم بسط الرقابة اللازمة على تصرفاتهم التي أفضت إلى الفعل المجرّم.

ولعل هذا ما قصده الإتجاه التشريعي الجزائري عندما أقرّ مسؤولية الاشخاص الاعتبارية عن الجرائم المتعلقة بالمساس بأنظمة المعالجة الالية للمعطيات، في المواد من 364 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري، ثم رسم محدداته وأبعاده بموجب القانون رقم 09-04 بتاريخ 05

---

[1] - مزاولي محمد، المسؤولية الجزائية للأشخاص الاعتبارية في مجال المعالجة الآلية للمعطيات، بحث منشور في المجلة الالكترونية الشهرية، القانون والفقه، المملكة المغربية، رقم 23، 2014، ص 39-46.

[2] - مزاولي محمد، المسؤولية الجزائية للأشخاص الاعتبارية الخاصة – دراسة مقارنة، رسالة دكتوراه، جامعة تلمسان، 2014، ص 115 ومايليها.

[3]- بموجب القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج/ر رقم 71 لسنة 2004.

[4] - بموجب القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-157 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج/ر رقم 71 لسنة 2004.

أوت 2009، المتعلق بالوقاية ومكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات[1].

إشكالية البحث ومنهج دراسته:

من هذا المنطلق ونظرا لحداثة مبدأ مسؤولية الشخص الاعتباري في القانون الجزائري، سنحاول الوقوف على موقف المشرع الجزائري، إعتمادا على المنهج المقارن، من خلال طرح الاشكالية التالية، إلى أي مدى يمكن مسائلة الاشخاص الاعتبارية عن الجرائم المرتكبة في البيئة الرقمية، وكيف عالج المشرع الجزائري ذلك ؟، وللإجابة على ذلك ،سنحاول دراسة الموضوع اعتماد خطة ثنائية، نعالج فيها المدى الذي يمكن أن يصل إليه إقرار هذه المسؤولية من خلال الوقوف على تجريم الشخص الإعتباري عن هذا النوع من الجرائم (مبحث أول)، ثم نقف على سبل مكافحة هذه الجريمة وفق القانون الجزائري (مبحث ثاني).

المبحث الأول: نطاق التجريم في إطار البيئة الرقمية.

مع ازدياد الاعتماد على نظم الكمبيوتر والشبكات في الأعمال أثيرت مشكلة أمن المعلومات، وحماية محتواها من أنشطة الاعتداء عليها، سواء من داخل المؤسسة أو من خارجها، وأنماط الاعتداء عديدة تبدأ من الدخول غير المصرح به لملفات البيانات إلى إحداث تغيير فيها وتحوير بمحتواها أو صناعة بيانات وملفات وهمية، أو اعتراضها أثناء نقلها، أو تعطيل عمل النظام، أو الاستيلاء على البيانات لأغراض مختلفة أو إحداث تدمير أو احتيال للحصول على منافع ومكاسب مادية أو لمجرد الإضرار بالآخرين وأحيانا مجرد أنشطة تستهدف المزاح الذي سرعان ما يكون عملا مؤذيا يتجاوز المزاح.

[1] – قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، ج/ر رقم 47، لسنة السادسة والأربعون، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صفحة 5.

المطلب: تعريف نظام المعالجة الآلية للمعطيات.

حسب الامم المتحدة تعتبر جريمة إلكترونية، كل جريمة ترتكب عن طريق نظام أو شبكة معلوماتية، أو ضد نظام أو شبكة معلوماتية، وتستغرق كافة السلوكيات غير المشروعة داخل البيئة الالكترونية[1].

وتنقسم الجرائم المعلوماتية الى قسمين؛ جرائم تكون المعلوماتية موضوعا للجريمة، كالمساس بأمن الشبكة الإلكترونية بشكل يؤدي إلى المساس بالسرية وبخصوصية النظام المعلوماتي[2].

وجرائم يكون فيها النظام المعلوماتي وسيلة ارتكاب الجريمة، مثل إنشاء شبكة للمتاجرة بالبشر أو المخدرات أو الاسلحة، أو اختراق الانظمة بشكل يمس بخصوصيات افارد والمؤسسات، كحالات الاعتداء على الملكية الصناعية أو الفكرية أو جرائم التمييز العنصري أو التحريض على الارهاب ...الخ[3].

فبالنظر إلى ما يفرزه التطور التقني في الكيانات الذكية، لا تقع بالتالي الجريمة المنصوص عليها إذا وقع الاعتداء على عنصر بمفرده لا يشكل جزءا في هذا النظام، كما إذا وقع الاعتداء على برامج معروضة للبيع، أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن أو على قطع الغيار، أو على الأجهزة التي مازالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما وكذلك تلك التي في سبيلها إلى الكسر، ولكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات

[1] - حامد قشقوش هدى: الحماية الجناية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000، ص 49.

[2] - نفس المرجع السابق، ص 49 وما يليها,

[3] - فتوح الشاذلي وعفيفي كامل عفيفي: جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) منشورات الحلبي الحقوقية، بيروت – لبنان، 2003، ص 232.

تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، وكان يمكن إصلاحه.

وتقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال ووقع اعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة المرتبطة، فان الجريمة تقع في هذه الحالة[1].

وإذا كان الدخول إلى هذا الجهاز مشروع، فان البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع والاعتداء المفروض على الأنظمة ككل، ومدى حسن أو سوء نية المتدخل، كما تقع الجريمة إذا وقع الاعتداء على شبكة الاتصال.[2]

ونظرا للطابع التقني للجريمة المعلوماتية، غالبا ما يطرح مشكل المصطلح لابتعادها عن حقل البحث القانوني مثلEnregistrement ، Informatique، Captation... . الخ.

فالتشريعات الأنجلوساكسونية، غالبا ما تعتمد طريقة إعطاء تعريفات في صلب القانون، أما الطريقة الفرنسية فهي تعتمد على إسناد مهمة تحديد معاني المصطلحات التقنية للقضاء وهي الطريقة الأفضل نظرا لسرعة تطور تقنيات الإعلام الآلي وعدم إمكانية مواكبة القانون الجزائي لهذا التطور. ويلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك

[1] - قارة أمال: الجريمة المعلوماتية، مذكرة ماجستير، 2001– 2002، بن عكنون، الجزائر، ص 34.

[2] - نفس المرجع والصفحة.

من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي أو الجريمة المعلوماتية،[1] ومن هذه التعريفات:

أنها تشمل أي جريمة ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية، وهناك جانب من الفقه الفرنسي حاول وضع تعريف لها في الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح.[2]

المطلب الثاني: الطبيعة القانونية لجريمة المعالجة الآلية للمعطيات.

للتأكد من وجود اعتداء على قواعد بيانات معالجة آليا، لابد ان يكون هناك قاعدة معالجة آلية للبيانات او المعلومات، وقد اقترح مجلس الشيوخ الفرنسي تعريفا لذا النظام على انه كل مركب يتكون من وحدة او مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات أو أجهزة الإدخال او الإخراج واجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات، على ان يكون هذا المركب خاضع لنظام المعالجة الفنية، ولذلك ونظرا لقيمة المعلومات المذكورة، وجب ضرورة تجريمها، سواء كان ذلك التعدي في صورة تدمير لها او تعيين لهذه النظم او إعاقة عملها.[3]

[1] - بن سعدون رضا: المسؤولية الجنائية للأشخاص المعنوية على ضوء تعديل قانوني العقوبات والإجراءات الجزائية، مذكرة تخرج المدرسة العليا للقضاء، المدرسة العليا للقضاء، دفعة 2006، ص 32.

[2] - العريان محمد علي: الجرائم المعلوماتية، دار الجامعة الجديدة، للنشر طبعة 2005، ص43-44.

[3] – عرفت الاتفاقية الدولية للإجرام المعلوماتي النظام المعلوماتي في المادة الثامنة منها على انه:

« Système informatique désigne tout dispositif isole ou ensemble de dispositifs interconnectes ou apparentés ; qui assure ou dont un ou plusieurs éléments assurent ; en exécution d'un programme un traitement automatisé de donnée ».

والحقيقة ان تدمير نظم البيانات والمعلومات، يفوق في الضرر المترتب عليه، ذلك الضرر الناجم عن إتلاف المعدات المادية الخاصة بنظم المعلومات، أصبحت له قيمة مالية واقتصادية كبيرة.[1]

أما التشريعالجزائري فلم يحدد تعريفا لهذه الجريمة واكتفى بتجريمها، تحت اسم المعالجة الآلية للمعطيات في المواد من **394 مكرر** إلى **394 مكرر7**من الفصل الثالث القسم السابع مكرر وأفرد نص المادة**394 مكرر4** كأساس لمساءلة الأشخاص الإعتبارية عن هذه الجريمة**(يعاقب الشخص الإعتباري الذي يرتكب إحدى الجرائم المنصوص عليه في هذا القسم...)**

وأمام هذا الاختلاف في وضع تعريف موحد كيف يمكن متابعة الشخص الإعتباري ومساءلته عن هذه الجريمة ؟ وللجواب نتطرق إلى أركان الجريمة المجسدة في صورتين أساسيتين، الدخول والبقاء في منظومة معلوماتية، وكذا المساس بمنظومة معلوماتية:[2]

الفرع الأول: الدخول والبقاء في منظومة معلوماتية:

قبل معالجة المقصود بعملية الدخول والبقاء في منظومة معلوماتية، لابد من تحديد أولا الجوهر الذي تدور في فلكه قيمة المنظومة المعلوماتية، ألا وهي البيانات الالكترونية وبخصوص تحديد البيانات ويقابلها باللغة الانجليزية DATA، فهي جمع لكلمة بيان، وفي الاصطلاح هي تعبير يستخدم لوصف البيانات الممثلة رمزيا على وسائط آلية او للإشارة اليه، والتي تمثل أطراف الأوامر والعمليات والعناصر التي تحتوي على ارقام وحروف او علامات

[1]- حجازي عبد الفتاح بيومي: التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الكتب القانونية، 2008، ص 21.

[2] – بوسقيعة أحسن : الوجيز في القانون الجزائي العام، الطبعة الثانية، منقحة ومتممة، سنة2004،.ص 434 وما بعدها.

خاصة للتعبير عن الأسماء او الأفعال او القيم الرقمية، وهي العناصر التي تخضع للمعالجة بواسطة البرنامج باستخدام إمكانات المجموعة الآلية للنظام.[1]

وعلى أساس ذلك فان البيانات DATUM تمثل مجموعة حقائق وأفكار ومشاهدات أو ملاحظات، تكون على صورة أعداد او كلمات او رموز مكونة من ارقام وحروف ابجدية او رمزية خاصة، وتعرف البيانات الخاضعة للمعالجة، اي التي لم تعالج ، والتي عولجت ولم تتم تصفيفها بشكل نهائي بالمدخلات INPUT DATA، اما نتائج المعالجة فيطلق عليها المخرجات OUTPUT DATA.

البند الأول: الدخول في منظومة معلوماتية

لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات . ولم يحدد التشريعوسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.[2]

وتتسع هذه العبارة على إطلاقها لتشمل كل فنيات الدخول الاحتيالي، والبقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أداء إتاوة من طرف احد ممثلي الشخص الإعتباري ولحسابه.[3]

---

[1] - الهيتي محمد حماد: البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الاسمية) المخزنة في الحاسب الآلي، مجلة الشريعة والقانون – العدد السابع والعشرون – جمادى الثانية، 1427 هجرية – يوليو 2006، ص 383.

[2] - سلامة محمد عبد الله ابو بكر: جرائم الكومبيوتر والانترنت (موسوعة جرائم المعلوماتية)، دار المعارف، بالإسكندرية، 2006، ص 7.

[3]- بن سعدون رضا، المرجع السابق، ص 32.

ويرتكب الجريمة من يعمل على الحاسب ولكن بنظام معين، فيدخل في نظام آخر.كما تقع الجريمة سواء تم الدخول إلى النظام كله أم إلى جزء منه فقط، أي يكفي لتوافر الجريمة أن يتم الدخول على بعض عناصر النظام، أو على عنصر واحد منه ،أو منطقة ضيقة منه، كان هذا بشرط أن يكون العنصر الذي تم الدخول إليه فقط يدخل في برنامج متكامل قابل للتشغيل .وفي النهاية فان الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو بعضها أو استعمال تلك المعلومات، بل إن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام[1].

ولعل هذا ما ذهب اليه التشريع القانوني الجزائري بموجب نص المادة 17 من القانون رقم 15-03 المتعلق بعصرنة العدالة، من سنة الى خمس سنوات وبغرامة تتراوح بين 100,000 دج إلى 500,000 دج كل شخص يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر.

ونتساءل هنا لماذا لم يسند التشريعالجزائري المسؤولية الجزائية للشخص الاعتباري هن هذا النوع من الجرائم رغم إمكانية ارتكابه لها. وندعوه بدورنا إلى ضرورة إعادة النظر في صياغة هذا القانون بشكل تتسع فيه مجال المسؤولية لتطال هذه الكيانات، أو أن يحذف مبدأ التخصيص من صلب نص المادة 51 مكرر، وبذلك تستقيم كافة النصوص التشريعية التي يمكن على أساسها إسناد المسؤولية لهذا الكيان الاعتباري.

[1]-SEUVIC Jean-François : Commerce électronique. Communication en ligne. Cryptologie. Cybercriminalité. « Télécommunications ». Analyse de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique Revue de science criminelle 2004 p. 925

و يختلف الأمر بالنسبة للقانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكتروني، حيث نص التشريعالجزائري صراحة على إمكانية إسناد المسؤولية للشخص الاعتباري، بموجب نص المادة 75 منه، حيث نص على أن يعاقب الخص المعنوي (الاعتباري)، الذي ارتكب إحدى الجرائم المنصوص غليها في هذا الفصل بغرامة تعادل خمس مرات الحد الاقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

البند الثاني: البقاء في منظومة معلوماتية

قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام، وقد يجتمعان . ويكون البقاء معاقبا عليها استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي[1].

و تبدأ جريمة البقاء داخل النظام منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام، أو يستمر في التجول بداخله بعد انتهاء الوقت المحدد، لأن الفرض يتعلق بدخول غير مشروع، أي مع علم الجاني أن ليس له الحق في الدخول، وتتحقق جريمة البقاء داخل النظام كله أوفي جزء منه ويكفي

[1]- SEUVIC Jean-François : Commerce électronique,,,

البقاء داخل النظام لتوافر الركن المادي لتلك الجريمة، فلا يشترط أن يضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر[1].

البند الثالث: التصريح عمدا بمعطيات خاطئة

نعتقد أن من أهم الجرائم التي يمكن أن تسأل عنها شركات تزويد خدمات الانترنت باعتبارها أشخص إعتبارية، التصريح عمدا بمعطيات خاطئة لمزود خدمات التصديق الإليكتروني أو الأطراف العملية التجارية ذاتها، ويستوي في المعطيات الخاطئة، ان تكون يدوية او معالجة، بمعنى ان تكون معلومات لم تدخل بعد ضمن نظام معلوماتي او معطيات ضمن نظام معلوماتي له علاقة بالتعاقد في نطاق التجارة الالكترونية، كما يستوي ان يتم الإدلاء بهذه البيانات الى مزود خدمة التصديق شخص طبيعي او اعتباري، حصل على الترخيص بممارسة هذه المهنة من جهة مختصة.

كما يستوي أيضاً ان يتم الإدلاء بهذه المعطيات غير الصحيحة الى أطراف التعاقد وهما البائع والمشتري او المستهلك والمنتج، وهذه البيانات غير الصحيحة قد توقع احدهما في غلط او تعد تدليسا يدفعه الى التعاقد، ومن ثم يصيبه ذلك بضرر جسيم نظرا لأثر هذا الكذب الذي دفعه الى التعاقد.[2]

و يندرج في هذا الاطار ما ذهب إليه التشريع الجزائري، عندما نص في المادة 18 من القانون رقم 15-03 المتعلق بعصرنة العدالة، على أن يعاقب بالحبس من سنة إلى خمس سنوات، وبغرامة من 100,000 دج إلى 500,000 دج كل شخص حائز لشهادة إلكترونية يواصل استعمالها رغم علمه

[1] - Roman (M) Faux Juris class,1996 art 441/1 à 441/12 n°19 P456

[2] – حجازي عبد الفتاح بيومي: التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الاولى، ص 68،- 2006 .

بانتهاء مدة صلاحيتها أو إلغاءها. ونفس الملاحظة التي لاحظناه على المادة 17 أعلاه، نسجلها كذلك على المادة 18 من قانون عصرنة العدالة.

الفرع الثاني: المساس بمنظومة معلوماتية:

حسب بيان المديرية العامة للأمن الوطني الجزائري[1]، هناك 221 قضية إجرام تتعلق بالمساس بالمنظومة المعلوماتية، تم تسجيلها ومعالجتها من طرف سرية مكافحة الجريمة المعلوماتية التابعة لمدرية الامن الوطني لسنة 2015 حسب تقرير صادر عن الوكالة الجزائرية للأنباء.

205 شخص من بينهم 28 امرأة متورطون في هذه القضايا المرتبطة بأنظمة المعالجة الالية للمعطيات (75) حالة تتعلق بالمساس بالحياة الخاصة (59) حالة تتعلق بالتهديد (28) حالة تتعلق بانتحال الهوية (26) حالة. وحسب بيان المديرية العامة للأمن الطن دائما، تم التصريح بقضايا تتعلق بنشر صور مخلة بالآداب العامة (09) حالة، النصب عن طريق الانترنت (03) حالات، الاهانة والاحتقار (06) حالة الاستعمال غير المشروع للبطاقات الممغنطة (02 حالة)[2].

في هذا الصدد نصت المادة 394 مكرر 1 عن كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

وعلى ذلك يأخذ الفعل صورتين:

أولا: إدخال معطيات في نظام المعالجة الآلية غريبة عنه بهدف تحقيق أرباح طائلة من وراء ذلك، سواء تم ذلك في مؤسسة مالية أو بنك أو شركة، كأن يقوم الشخص الإعتباري بواسطة أحد أجهزته أو ممثليه باسمه ولحسابه

[1] - Abdelkader DERDOURI, Journal le soir d'Algérie du Mardi 28 Avril 2015, page 6 et 7.

[2] - أنظر الرابط: http://www.huffpostmaghreb.com/2015/01/16/cybercriminalite-221-affa_n_6485396.html، أطلع عليه في 2016/03/22.

خاصة في الشركات الكبرى حيث يكثر عدد الموظفين وبطبيعة الحال فيهم من يترك الوظيفة لأسباب متعددة حينها يتمكن مسئول إدارة بالإبقاء عليهم مع الاحتفاظ بالمعلومات الخاصة بهم ومن ثم يقوم بتحصيل دخلهم بعد استلام الشيكات النقدية الخاصة بهم.

ثانيا: تخريب المعطيات التي يتضمنها نظام المعالجة الآلية، إذ من بين تقنيات التدمير الناجمة والتي تصيب النظام المعلوماتي بأضرار جسيمة يصعب تفاديها، تبرز فيروسات الحاسب الآلي وهي تمثل المركز الأول في هذه التقنيات تصيب البيانات والبرامج بالشكل التام.

ومن التطبيقات القضائية في فرنسا قضى بأنه يقع تحت طائلة المادة 3/329 ق ع المقابلة للمادة 394/ مكرر 1 تعمد إدخال فيروس معلوماتي في برنامج logiciel الغير والامتناع عن إخباره بذلك، كذلك بالنسبة لشركات صانعي البرامج عندما يكونوا مسؤولين عن الصيانة طبقا للعقد المبرم بينهم وبين المستخدم، إذ يقوموا بزراعة فيروس معين يعطل البرنامج وفي نفس الوقت يعطي انطباعا يفيد أن سبب العطل هو سوء استعمال المستخدم وخطاه، ومن ثم يهرع لطلب الصيانة وتكون هذه الوسيلة لابتزاز المستخدم والإثراء على حسابه ،كما جرمت المادة 394 مكرر2:

1 – كل 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 إحدى هذه الجرائم سالفة الذكر.

2 – إضافة إلى حيازة أو إنشاء واستعمال لأي غرض كان المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي.

في حين أبقى قانون العقوبات الشخص الإعتباري خارج دائرة التجريم في بعض الأفعال كتلك المتعلقة بالمساس بحقوق الأشخاص عن طريق المعلوماتية

ومنها: جمع المعلومات حول الأشخاص والمعالجة المعلوماتية للمعلومات التي تم جمعها وتحويل المعلومات الاسمية عن مقصدها.

4 – تزوير الوثائق المعالجة إعلاميا كبطاقات القرض التي لا تشملها جريمة التزوير كما هي معرفة في قانون العقوبات لاسيما المادة 222 وما يليها.[1]

أمام هذه المعطيات نتساءل عن كيفية إثبات أركان هذه الجريمة وربطها مع شروط المادة 51 مكرر قانون عقوبات في مواجهة الشخص الإعتباري؟ خاصة مع تزايد الاعتماد على وسائل تقنية المعلومات في إدارة الأعمال المختلفة، والتوجه نحو عالم البيانات والملفات المخزنة في أنظمة المعلومات كبديل للبيانات المحررة على الورق وحوافظ الملفات التقليدية، يزداد الاهتمام بمدى حجية وقوة وسائل التخزين التقني للمعلومات في الإثبات ومدى حجية مستخرجات الحاسوب ومدى إمكان النظام القانوني للإثبات استيعاب هذه الأنماط المستجدة من وسائل إثبات التصرفات التعاقدية .

ولا يقف التساؤل عند حد التصرفات القانونية المدنية والتجارية والمصرفية، بل يتعداه الى التساؤل حول قوة وحجية الدليل ذي الطبيعة الالكترونية في المواد الجزائية، نقف على مسائل وتحديات الإثبات الإلكتروني في المواد الجزائية وما يتصل بها من مسائل إجرائية تتعلق بأمن المعلومات.

المبحث الثاني: مكافحة جريمة المساس بأنظمة المعالجة الالية للمعطيات في القانون الجزائري

لقد أظهرت الدراسات والتجارب الدولية، أن مثل هذا القانون من شأنه أن يساعد على تنظيم قطاع تكنولوجيا المعلومات والاتصالات، وتقوية دور السلطة

[1] - بوسقيعة أحسن: المرجع السابق ص435.

العمومية في ردع المجرمين وتسمح أيضا بحماية أفضل للبنية التحتية الحيوية، مثل قطاعات الطاقة والمياه والنقل والمالية وتكنولوجيا المعلومات والاتصالات وغيرها، كونها المجالات الأساسية لنشاط الدولة، والمستهدفة بانتظام من طرف مجرمي البيئة الالكترونية.

المطلب الاول : مراقبة الاتصالات الالكترونية

حسب المادة 4، من قانون 09-04، يمكن القيام بعمليات المراقبة في الحالات التالية:

ا- للوقاية من الأفعال الموصوفة بجرائم الإرهاب او التخريب او الجرائم الماسة بأمن الدولة،

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الإقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الالكترونية

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

في هذا الصدد لا يجوز اجراء عمليات المراقبة، الا بإذن مكتوب من السلطة القضائية المختصة عندما يتعلق الامر بالحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص غليها في الفقرة (أ) موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفرع الأول: التزامات مقدمي الخدمات في إطار مساعدة السلطات العمومية

لعل ما يميز الجرائم المرتكبة في الفضاء الافتراضي ويجعلها مغايرة للطرح التقليدي للجريمة، هو ميزة الاستتار والاختفاء، كون الضحية ولو وقعت أثناء وجوده على الشبكة، فلا يشعر بأثرها الا بعد وقت من وقوعها، كحالات إرسال الفيروسات، أو تحويل الاموال والبيانات الخاصة او اتلافها، أو دس بعض البرامج وتغذيتها ببعض البيانات التي تؤدي الى عدم شعور المجني عليه بوقوعها[1].

[1] - ولعل أحسن مثال على ذلك القضية الشهيرة في القضاء الامريكي المعروفة بحادثة المواقع الاستراتيجية –: وفي 19 تشرين الثاني 1999 تم ادانة المدعو إريك بورن Eric burns من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهرا والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد ان اقر بمسؤوليته بأنه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضررا بالغا في كل من ولايات فيرجينيا واشنطن واضافة الى لندن في بريطانيا، وقد تضمن هجومه الاعتداء على مواقع لحلف الاطلسي اضافة الى الاعتداء على موقع نائب رئيس الولايات المتحدة كما اعترف بانه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الابيض، وقد قام Eric بتصميم برنامج اطلق عليه web bandit ليقوم بعملية تحديد الكمبيوترات المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها، وباستخدام هذا البرنامج اكتشف ان الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق، فقام في الفترة ما بين آب 1998 وحتى كانون الثاني 1999 باختراق هذا النظام 4 مرات، واثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIA للمعلومات، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى الى اغلاق هذا الموقع لثمانية ايام، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة LASER.NET في منطقة فيرجينيا والعديد من مؤسسات الاعمال في واشنطن اضافة الى جامعة واشنطن والمجلس الاعلى للتعليم في فيرجينيا رتشموند ومزود خدمات إنترنت في لندن، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسمZYKLON او باسم صديقته باسم . CRYSTAL

كما أن هذا النوع من الجرائم لا تتطلب عنفا أو مجهود كبير لتنفيذها، لاعتمادها على الخبرة في المجال المعلوماتي بشكل اساسي، بالإضافة إلى صعوبة إثبات الدليل، من منطلق ان المعلومات والبيانات في البيئة الافتراضية غالبا ما تكون في شكل مصفوفات ورموز مخزنة على وسائط تخزين ممغنطة ولا تقرأ الا بواسطة الحاسب الالي، وهو ما يجعل الدليل الكتابي او المقروء، أمر يصعب بقاءه او اثباته، بالإضافة إلى سهولة محو الدليل من شاشة الكمبيوتر في زمن قياسى باستعمال البرامج المخصصة لذلك، مما يتطلب وجود مختصين للبحث وتفحص موقع الجريمة وهو ما يتعارض مع قلة الخبرة لدى اجهزتنا الامنية والقضائية، رغم الجهود المبذولة من طرف الدولة في هذا المجال[1].

هذا الامر يستوجب ضرورة مشاركة مقدمي الخدمات في المجال الإفتراضي مع السلطات العمومية للتصدي لهذه الجرائم، تحت طائلة العقوبات الجزائية والمنصوص عليها بمقتضى الفصل الثاني المتعلق بالأحكام الجزائية، من القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين.[2]

ففي إطار تطبيق أحكام القانون المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما عالجت المادة 10، الالتزامات التي تقع على عاتق مقدمي الخدمات في إطار مساعدة السلطات العمومية المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها.

[1] - Roman (M) Faux Juris class,1996 art 441/1 à 441/12 n°19 P456

[2] - إرجع إلى القانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، المواد من 66 إلى 75 منه.

حيث يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، وتتسع هذه الالتزامات لتشمل الالتزامات الخاصة بمقدمي خدمات الانترنت كذلك.

الفرع الثاني: الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

وهنا كذلك ووفقا للمادّة 12 من القانون المشار إليه أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة مخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول الى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

ففي بداية عام 2015، تم التصريح عن عدة هجمات سيبرانية ضد الجزائر والجزائريين، من طرف "مجموعة معادلة" باستخدام أحد أخطر فيروس التجسس السيبراني، والذي اكتشف حديثا، رغم أن عمليات التجسس قد بدأت منذ سنوات، وهو فيروس تجسس يختار ضحاياه من فئات الحكومة والدفاع والطاقة والمالية.

كما يمارس كذلك "مجموعة صقور الصحراء" عمليات التجسس والتي تستهدف المؤسسات الاقتصادية والسياسيين والمسؤولين في مجال مكافحة غسل الأموال، وكذا الاشخاص والمؤسسات التي تحوز معلومات استراتيجية أو

جيوسياسية حساسة، وقد ثبت تواجد هذا الفيروس في عدة مناطق في الاقليم الجزائري [1].

بالإضافة إلى سلسلة من البرامج الضارة، كبرنامج بابار، الأرنب، كاسبر، دينو، آن بوت، وتافاكالو، والتي تعود ملكيتها إلى أجهزة إستخباراتية، والتي ساهم في صناعتها ما لا يقل عن ثلاثة شركات أمن تكنولوجيا المعلومات الكبرى في الولايات المتحدة وأوروبا، وذلك للاطلاع على بيانات المنظمات الحكومية والشركات في العديد من البلدان والتي من بينها الجزائر[2].

ويعتبر هذا المجال الامثل لظهور شركات تمارس أعمال غير مشروعة لمتعلقة بالبيئة لرقمية، فالقانون الجزائري، قد حصر الجرائم التي يمكن أن يسأل عنها الشخص الإعتباري، ويترتب على اشتراط أن تكون الجريمة، مرتكبة ممن يملك زمام أمور الشخص الإعتباري، ألا يسال الشخص الإعتباري عما يرتكبه ممن ليست له هذه الصفة، حتي ولو ارتكب جريمة من الجرائم المشار إليها.[3]

ويستخلص من ذلك، أنه لا يشترط أن يكون ممثل الشخص الإعتباري، فاعلا أصليا للجريمة، بل يمكن أن يكون شريكا فيها، بشرط أن ترتكب الجريمة لحساب الشخص الإعتباري[4].

ويعتقد بعض المتخصصين في تقنية الانظمة المعلوماتية، أن العاملين في شركة ما يتمتعون بحكم مراكزهم ومهاراتهم الفنية استخدام الانظمة المعلوماتية وبرامجها لأغراض شخصية، ومن شأن ذلك أن يؤدي الى تمادي بعضهم إلى

[1]- Abdelkader DERDOURI, Journal le soir d'Algérie du Mardi 28 Avril 2015, page 6 et 7.
[2]- Ibid, page 6 et 7.
[3]- SAINT-PAU Jean-Christophe : La présomption d'imputation d'une infraction aux organes ou représentants d'une personne morale, Recueil Dalloz 2007 p. 617
[4] -ألعوجي مصطفى: المسؤولية الجنائية في المؤسسة الاقتصادية، مؤسسة نوفل بيروت، الطبعة الأولى 982.

استخدام الانظمة بصفة غير مشروعة تصل الى ارتكاب جرائم خطيرة قد يسئل عنها الشخص الاعتباري[1].

ومن أمثلة ذلك قيام مستشار أحد البنوك يسمى ستانلي ريفكان STANLEY Rifkin، تحويل مبلغ 10 مليون دولار إلى حساب بنكي مفتوح بإسمه في سويسرا كونه كان متمتعا بثقة البنك ولأن اختصاصاته سمحت له بالولوج إلى مفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك لآخر، وقد تمكن بفضل معالجته الالية للمعلومات وخبرته التقنية الى الوصول الى المفتاح الثالث.[2]

الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

تضمن هذه الهيئة وظيفة السلطة الوطنية لأمن المعلومات، إذ تتولى تحديد التدابير التقنية والتشريعية للدفاع والحماية، ومسؤولة أيضا عن الضوابط والتفتيش على نظم المعلومات المتعلقة بالبنية التحتية الحيوية.

ولعل إنشاء هذه الهيئة في الجزائر، لم يأتي من العدم، وإنما جاء متماشيا والاتجاه الدولي في هذا الصدد، فقد أنشئت المملكة المتحدة "مركز حماية البنية التحتية الوطنية (CPNI)،" سلطة حكومية التي تقدم المشورة الأمنية للشركات والمؤسسات. أما في الولايات المتحدة، فوضعت قانون الأمن الإلكتروني الذي يوجب على الحكومة وضع معايير موحدة في مجال الأمن التكنولوجي من قبل NIST (المعهد الوطني للمعايير والتكنولوجيا)، لتحليل الهجمات السيبرانية وتطبيق النتائج. بحيث يقوم هذا المعهد بتحديد معايير

[1] - Roman (M) Faux Juris class,1996 art 441/1 à 441/12 n°19 P456

[2] - مذكور في سوير سفيان : جرائم المعلوماتية، رسالة ماجستير، جامعة أبو بكر بالقايد – تلمسان، 2010– 2011، رسالة غير منشورة، ص 29.

الأمن القابلة للقياس والمراجعة بشأن أمن البرمجيات وتطوير عملية لفحص المطابقة مع القواعد القانونية والتقنية .

بالرجوع الى القانون الجزائري، نصت المادّة 13، على أن تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تتولى المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ب – مساعدة السلطات القضائية ومصالح الشرطة في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

المطلب الثاني : القواعد الاجرائية المتعلقة بتفتيش المنظومات المعلوماتية

بالرجوع الى نص المادة 5 من قانون09-04، المذكور أعلاه، نلاحظ أنها نصت على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، الدخول بغرض التفتيش ولو عن بعد، الى :

أ– منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب– منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة أ من هذه المادة، اذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبعوث عنها مخزنة في منظومة معلوماتية اخرى وأن هذه المعطيات يمكن الدخول اليها انطلاقا من المنظومة او جزء منها بعد أعلام السلطة القضائية المختصة مسبقا بذلك.

و إذا تبين مسبقا بان المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الاولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا الاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية الضرورية لإنجاز مهمتها.

الفرع الأول: حجز المعطيات المعلوماتية

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 وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، ويجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز والسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يودي ذلك إلى المساس بمحتوى المعطيات[1].

الفرع الثاني: الحجز عن طريق منع الوصول إلى المعطيات

إذا استحال إجراء الحجز وفقا الأشكال القانونية المشار إليها آنفا حسب المادة 6 لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

أولا: المعطيات المحجوزة ذات المحتوى المُجرّم

يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

ولقد تضاربت الآراء حول تحديد المعطيات ذات المحتوى المجرم، فهناك من عددها بحسب موضوع الجريمة، وآخرون اعتمدوا في تحديدها بالنظر إلى طريقة ارتكابها، وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية، فاعتبر ان الصنف الأول يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة[2].

[1] - أسامة أحمد المناعسة، جلال محمد الزعبين صايل فاضل الهواوشة – جرائم الحاسب الآلي والانترنت– دار وائل للنشر، الأردن، 2004 ص159.

[2] - Abdelkader DERDOURI, Journal le soir d'Algérie du Mardi 28 Avril 2015, page 6 et 7.

والصنف الثاني تضمن دعم الأنشطة الإجرامية، ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال، المخدرات، الاتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات، بينما يتعلق الصنف الثالث بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب، بينما الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الانترنت، وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها باي صورة طبقا لقانون حماية الملكية الفكرية[1].

بينما يذهب الاتجاه العالمي الجديد خاصة ما ورد بالاتفاقية الأوربية لعام2001 لجرائم الكمبيوتر والانترنت فقد قسمت هذه الجرائم إلى، أولا الجرائم التي تستهدف عناصر المعطيات والنظم، ثانيا الجرائم المرتبطة بالمحتوى بالكمبيوتر "التزوير والاحتيال"، وثالثا " الجرائم المرتبطة بالمحتوى " الافعال الإباحية والأخلاقية"، ورابعا الجرائم المرتبطة بحقوق المؤلف والحقوق المجـــاورة[2].

بينما لم يحدد القانون الجزائري المقصود بالمعطيات ذات المحتوى المجرم، مما يفهم منه الاخذ بما استقر عليه الفقه والاجتهاد الدولي في هذا المجال.

[1] - Ibid, page 6 et 7.

[2] - أسامة أحمد المناعسة، المرجع السابق، ص159.

ثانيا: حدود استعمال المعطيات المتحصل عليها

يعد مبدأ المشروعية، القيد الذي يرسم النطاق الذي لا يجوز لأي كان الخروج عنه، فمشروعية الأدلة هي أحد صور المشروعية بوجه عام، وحلقة من حلقات المشروعية الجنائية بوجه خاص، فهي تشكل القيد الذي يجب أن يتقيد به التشريع الجزائي لكفالة احترام الحرية الشخصية في مواجهة السلطة.

فلا جريمة ولا عقوبة إلا بنص، مع وجوب احترام مشروعية الإجراءات الجزائية التي تضمن احترام الحرية الشخصية، فحين تُمس حرية الإنسان عن طريق الإجراءات التي تباشر ضده يبرز مبدأ المشروعية ليحدد النطاق المسموح به[1].

هذا ما يستوجب ضرورة التساؤل حول نطاق استعمال التقنيات في مجال التحقيق الجزائي؟ تعتبر القواعد العامة أن عملية المراقبة الفعلية دون قيد أو شرط هي عمل إجرامي لمساسها بالحق في حرمة الحياة الخاصة، هذا الحق الذي كفله الدستور والمعاهدات الدولية، إلا أن هذه القاعدة ليست بمطلقة، وإنما تحمل معها استثناء تقتضيه المصلحة العامة لأجل الموازنة بين حماية المصالح الحيوية العليا للدولة وبين حق الأفراد في التمتع بسرية الحياة الخاصة وعدم انتهاكها.

تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

[1]- مقابلة حسن يوسف مصطفى: الشرعية في الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2003، ص 120.

ثالثا: حفظ المعطيات المتعلقة بحركة السير

مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د – المعطيات المتعلقة بالخدمات التكميلية المستعملة أو المطلوبة أو مقدميها.

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها، بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ " وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، ويتم تحديد مدة حفظ هذه المعطيات بسنة واحدة ابتداء من تاريخ التسجيل.

في ذات السياق ودون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام هذه الالتزامات، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والاعتباريين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج. كما يعاقب الشخص الإعتباري بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

المطلب الثالث: التعاون القضائية الدولي

يمثل التعاون القانوني والقضائي بين الدول، ضرورة لازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة، على نحو يتكامل مع دور القوانين الوطنية في

التعاون بين سيادات دول مختلفة ترمي جمعيها إلى مكافحة الجريمة وتفعيلها بوجه عام.[1]

وينطبق المفهوم المتقدم للتعاون الدولي، على مسؤولية الشخص الإعتباري الخاص، التي اكتسبت خلال القرن العشرين قدرا من الأهمية، أثر اقترانها بظاهرتين معاصرتين، أولهما ظاهرة "التقدم التقني" وما أحدثته من ثورة واسعة النطاق، في مجالات الانتقال والاتصال ونظم المعلومات، وثانيهما عولمة النظم المصرفية والخدمات المالية، وما أفرزته من إمكانات وتسهيلات غير مسبوقة في هذين المجالين على وجه التحديد[2].

ويعد التعاون الدولي القائم في المجال القضائي وقواعده الاجرائية كالمساعدة القضائية والقانونية وتجميد الارصدة والمصادرة، ومحاربة الرشوة، والعمل على توحيد الرؤية حول تجريم الاشخاص الاعتبارية الخاضعة للقانون الخاص[3]، من أهم الخطوات في مواجهة هذه ظاهرة الإجرام العابر للحدود، رغم العراقيل التقليدية التي تبقى عائقا أمام فعالية هذا العمل.

ضف إلى ذلك ما تشكله اليوم المراكز المالية المتجاوزة للإقليم Les centre financiers extraterritoriaux، أو المناطق المعروفة بـ (Les zones offshores)، مرتعا للمال غير المشروع بما تقدمه من تسهيلات

---

[1] – بوزير محمد عبد الرحمن: بحث في المسؤولية الجنائية للأشخاص الاعتباريين عن جرائم غسل الأموال، دراسة تأصيلية مقارنة للقانون رقم 35 لسنة 2002، بشأن مكافحة عمليات غسل الأموال، موقع الدليل الالكتروني للقانون العربي، www.arablawinfo.com أطلع عليه بتاريخ: 2008/05/23.

[2] – ماهر مصطفى: المواجهة التشريعية لظاهرة غسل الأموال المحصلة من جرائم المخدرات، القاهرة 2002، ص447.

[3]- Voir en ce sens : la convention pénale sur la corruption-Strasbourg 27.01.1999, du conseil de l'Europe ; La convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, O.C.D.E, du 17.12.1997.

وامتيازات مالية، وتمثل تهديدا للاستقرار المالي العالمي في وجه التعاون القضائي الدولي[1].

بالرجوع الى التوصية رقم 12 (R81)، للمجلس الأوروبي حول موضوع الإجرام في مجال الأعمال، وكذلك اتفاقية المجلس الأوروبي، والتي تسمى كذلك باتفاقية ستراسبورغ في 1999/1/27، التي حددت لنا المجالات الكبرى للإجرام في مجال قانون الأعمال[2]، بشكل يستغرق الجرائم المتعلقة بأمن المعلومات.

الفرع الأول: الاختصاص القضائي

يقصد بالاختصاص القضائي، ولاية أو سلطة الحكم بمقتضى القانون في خصومة معينة معروضة على المحاكم، بحيث يؤدي فقدان هذه السلطة إلى عدم الاختصاص[3].

وإذا كان الاختصاص النوعي بالنسبة للقضايا المعروضة على القضاء حسب نوعها لا يطرح إشكالا بالنسبة للأشخاص الإعتبارية، فإن الأمر يختلف

---

[1] - CARTIER BRESSON. Jean, **et al** : Les délinquances économiques et financières transnationales et Globalisation, I.H.E.S.I, France, Juillet 2001, p22.

[2] – تتمثل هذه المجالات أساسا في:

- تشكيل التكتلات والكارتل Formation des cartels.
- الممارسات السلبية وإساءة الاستغلال الاقتصادي من قبل الشركات المتعددة الجنسيات.
- تحويل الاموال أو الحصوص بواسطة الغش على الاموال الممنوحة من طرف الدولة أو المنظمات الدولية، وإنشاء الشركات الوهمية.
- تزوير حسابات الشركات ومحاسباتها.
- المخالفات في ميدان الاعلام الالي كسرقة البرامج وانتهاك الاسرار واستغلال المعطيات المعلوماتية.
- الغش في المجال التجاري ورأسمال الشركات.
- المخالفات ضد المستهلكين، والمخالفات الجبائية.
- مخالفات الصرف والعملية، مخالفات البورصة، المخالفات الجمركية.
- الرشوة بجميع صورها واستغلال النفوذ.
- المسؤولية الجزائية للأشخاص الاعتبارية.

[3] – الغوثي بن ملحة، القانون القضائي الجزائري، ديوان المطبوعات الجامعية، الطبعة الثانية سنة 1989، صفحة 63.

بالنسبة للاختصاص المحلي، على اعتباره قاعدة تنظيم وتوزيع الاختصاص بين المحاكم على أساس إقليمي سواء على مستوى دولي أو داخلي، في هذه المرحلة تُطرح العديد من الأسئلة تتمحور بشكل كبير حول موضوعين أساسيين، الموضوع الأول، يتعلق بالقواعد المحددة للجهات القضائية المختصة، ويتعلق الموضوع الثاني بالمرحلة التحضيرية

زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة، الدفاع الوطني أو المجالات الاستراتيجية للاقتصاد الوطني.

وفي إطار المساعدة القضائية الدولية المتبادلة، تتم التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

كما يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

الفرع الثاني: تبادل المعلومات واتخاذ الإجراءات التحفظية.

يكون تبادل المعلومات عندما ترغب دولة، في البحث عن عناصر جريمة معينة، أو عن شبكة إجرامية أو مجرم معين يحمل جنسيتها، بحيث يتم جمع

المعلومات، وترسل بمعرفة مصالح شرطة الدولة المطلوب منها، إلى شرطة الدولة مصدرة الطلب[1].

مثال ذلك شركة متعددة الجنسيات مقرها الرئيسي في فرنسا، إرتكبت أعمال رشوة بالخارج، تتولى الشرطة الفرنسية إرسال المعلومات حول الشخص والجريمة، إلى جهاز الشرطة التي ارتكبت على إقليمها الجريمة[2]، ويدخل في هذا الإطار نشاطات الشرطة الدولية Interpol، والشرطة لاقليمية Europol ...الخ.

ولا يتم البحث عن وسائل الإثبات بالخارج، إلا وفق نظام اتفاقيات بين الدول، بحيث ينتقل أعوان الشرطة للبحث عن أثار الجريمة، بالتعاون مع عناصر الشرطة المضيفة، للقيام بتحريات[3]، وتقييم وسائل الإثبات.

غير أنه وحسب القانون الفرنسي، وحتى في حالة غياب اتفاقيات دولية، يمكن لأي جهاز شرطة بعد الحصول على إذن مسبق من وزارة العدل، بموجب طلب تعاون قضائي، القيام بتحريات على الإقليم الفرنسي، والقيام كذلك بتسربات طبقا لمواد من 706-81 إلى 706-87 من قانون الإجراءات الجزائية الفرنسية، بخصوص الجريمة المنظمة.

وهذا ما نص عليه القانون الجزائري كذلك بموجب نص المادة 65 مكرر11، من قانون الإجراءات الجزائية، والتي تحيلنا إلى نص المادة 65

---

[1]- HUET. A. et KOERING-JOULIN. R : Droit pénal international, 3ème éd., PUF, 2005, p.332.

[2] – هناك العديد من الاتفاقيات الثنائية، التي تفرض فيها فرنسا مسألة تبادل المعلومات بخصوص الجرائم، من بينها، الجزائر(الأمر رقم 65-194، مؤرخ في 30 ربيع الاول، عام 1385، الموافق 29 يوليو سنة 1965)، جنوب افريقيا (الجريدة الرسمية الفرنسية الصادرة بتاريخ 17 جانفي 1999)، المجر(الجريدة الرسمية الفرنسية الصادرة بتاريخ 27 جانفي 2000)، هولاندا(الجريدة الرسمية الفرنسية الصادرة بتاريخ 06 ماي 1999)، جمهورية سلوفاكيا(الجريدة الرسمية الفرنسية الصادرة بتاريخ 09 أفريل 2005)، جمهورية التشيك(الجريدة الرسمية الفرنسية الصادرة بتاريخ 06 نوفمبر 1997)، أوكرانيا(الجريدة الرسمية الفرنسية الصادرة بتاريخ 02 سبتمبر 2004).

[3] - HUET. A. et KOERING-JOULIN. R., op. cit., p.335.

مكرر05، بخصوص الجريمة المنظمة العابرة للحدود، والتي يمكن أن يسأل عنها شخص إعتباري[1].

وتتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل، كما يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

ويمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

الخـــاتمـة:

من خلال استقرائنا لمختلف النصوص القانونية المؤطرة للبيئة الرقمية في القانون الجزائري، وفي عالم يعلي قيم المعلوماتية ويسعى للاستفادة منها، يتعين التيقظ لما يتعين علينا التعامل معه، مما يستوجب التعامل مع النماذج التشريعية القائمة، ولقد بدأت الجزائر بداية موفقة في حصر الواقع التشريعي المتصل بالتجارة الالكترونية والبنوك الالكترونية، فان الخطوة التالية إنتاج تشريعات توافق احتياجاتنا تعكس تعاملا موضوعيا ومعمقا مع إفرازات عصر التقنية.

على الرغم من الاستثمار المالي المستمر والمتزايد في أمن تكنولوجيا المعلومات (13 مليار التي تنفقها الشركات في السنة في أنظمة جدار الحماية ومنع الاقتحام)، فمن الواضح أن الحرب ضد البرامج الخبيثة الأكثر تطورا لم

[1]- SAINT-PAU Jean-Claude : L'entraide judiciaire internationale et européenne, D.P., juillet-août 2004, p.6.

تنته بعد. فالقوانين في مجال الأمن التكنولوجي وسيلة لتخفيف ومواجهة التهديد غير المتناظر الماس بالبنية التحتية الحيوية.

وما يمكن قوله عن التجريم في مجال البيئة الرقمية لا يزال دون تطلعات المجتمع الجزائري، ذلك أن التشريعالجزائري ورغم الجهد المبذول في مجال الجرائم المتعلقة بأمن المعلومات، وأنظمة المعالجة الآلية للمعطيات، إلا أننا نعتقد بأن ذلك غير كاف، لا سيما في مجال إسناد المسؤولية للكيانات الإعتبارية، بل لابد من اعتماد دراسة شاملة تأخذ بعين الاعتبار الخصوصية الفنية لمثل هذه الجرائم، ذلك أن الاكتفاء بالقواعد العامة يفلت مجالات عديدة من المسؤولية الجزائية للأشخاص الإعتبارية، الأمر الذي يصعب الوضع على القاضي المقيد بمبدأ الشرعية فيكون ملزما بإيجاد حلول وتكييفات متقاربة للنزاعات التي تعرض عليه، كما قد يجد نفسه أمام ضرورة عدم إقرار هذه المسؤولية أصلا في غياب النص المجرّم، مثل ما لاحظنا في القانون المتعلق بعصرنة العدالة.

لقد أدخلت عدة آليات تتعلق بجمع المعلومات وحمايتها ونشرها وذلك في إطار مكافحة الإرهاب في الجزائر. ونعتقد أنه يمكن الاستفادة من هذه الآليات بتكييفها بما يتماشى وهذه المرحلة، ووفقا للتقرير السنوي للشركة ديل، تضاعف عدد الهجمات البيئة الرقمية ضد نظام المراقبة وجمع البيانات (سكادا) الخاصة بالبنية التحتية الحيوية في عام 2014، ولم يتم الإبلاغ عن معظم هذه الحوادث رغم أن معظم الهجمات كانت من نوع APT (التهديد المستمر المتقدم) ذات الاهداف السياسية.

وعليه فإننا نعتقد بأن المبادرة بالإبلاغ عن الهجمات في مصلحة الجميع، بحيث يتم تبادل المعلومات المتعلقة بتهديد الأمن الالكتروني، وكذا مواطن الضعف في النظم، وتحديد نقاط الضعف في الشبكات وتبادل المعلومات.

نعتقد بأنه ليست هناك إلى حد الساعة معايير دقيقة وواضحة لتحديد ما إذا كان الهجوم عبر الانترنت هو عمل إجرامي، أو عمل إختراق مبرمج (hacktivisme) أو عمل إرهابي، أو مجرد استعراض تحكم دولة ما في مجال التعاملات الالكترونية، وعليه فإلى أي مدى سيكون تأثير القانون في هذه البيئة المتسمة بالتغير المستمر تتقاطع فيها مصالح الجهات الحكومية وغير الحكومية ؟

إن وضع قانون لحماية المعاملات في البيئة الإلكترونية، لا يجب أن ينظر إليه كغاية في حد ذاتها، ولكنه يندرج ضمن متطلبات تدابير الحماية والوقاية التي أقرتها نصوص قانونية سابقة. فهو سيمسح كأداة فعالة في مكافحة على سبيل المثال، إدانة الأسلحة البيئة الرقمية أو ما يسمى cyberarmes مثل (Botnet, DDoS، .....الخ) والتي لم تم تعريفها في أي نص من نصوص القانون الجزائري ويتم تسويقها الآن بحرية في سوق الانترنت المظلم Darknet، وهي مسألة تستوجب مجرد ترخيص للحصول على الآليات الدفاعية ضدها.

ونوصي بدورنا في الاخير، بضرورة تطوير الجهود الدولية لمكافحة جرائم الانترنت من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية وثنائية، مع الدعوة إلى تكريس التوصيات التي نادت بها اتفاقية بودابست ودليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسب ومكافحتها.

ضرورة تنمية وعي الثقافة القانونية المعلوماتية بالنسبة للعاملين في هذا المجال، مع وضع إطار قانوني ينظم تعاملات مقدمي الخدمة لتسجيل بيانات مستخدمي الشبكة الانترنت، والاحتفاظ بالبيانات الاساسية والحقيقية لمستخدمى مواقعهم على الشبكة.

المراجع والمصادر باللغة العربية

I - النصوص القانونية:

1- القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج/ر رقم 71 لسنة 2004.

2- القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق ل 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-157 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج/ر رقم 71 لسنة 2004.

3- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، ج/ر رقم 47، لسنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صفحة 5.

4- القانون رقم 15-03 مؤرخ في 11 ربيع الثاني عام 1436، الموافق اول فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية رقم 06، صفحة 04.

5- القانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436، الموافق اول فبراير سنة 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية رقم 06، صفحة 06.

II- المؤلفات

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الثانية، منقحة ومتممة، سنة2004.

2. ألعوجي مصطفى: المسؤولية الجنائية في المؤسسة الاقتصادية، مؤسسة نوفل بيروت، الطبعة الأولى.

3. جمال محمود الحموي واحمد عبد الرحيم عودة، المسؤولية الجزائية للشركات التجارية، دراسة تحليليا مقارنة، دار وائل للنشر، الطبعة الاولى، 2004.

4. حسن يوسف مصطفى مقابلة، الشرعية في الإجراءات الجزائية، دار الثقافة للنشر والتوزيع، عمان، 2003.

5. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، دار

6. الفكر الجامعي، الطبعة الاولى، 2006 .

7. عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الكتب القانونية، 2008.

8. عقيدة محمد أبو العلا: الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، دار الفكر العربي، 1998.

9. الغوثي بن ملحة، القانون القضائي الجزائري، ديوان المطبوعات الجامعية، الطبعة الثانية سنة 1989.

10.فتوح الشاذلي وعفيفي كامل عفيفي: جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت – لبنان، 2003.

11.محمد عبد الله ابو بكر سلامة، جرائم الكومبيوتر والانترنت (موسوعة جرائم المعلوماتية)، دار المعارف، بالاسكندرية، 2006.

12.محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، للنشر طبعة 2005.

13.مصطفى ماهر، المواجهة التشريعية لظاهرة غسل الأموال المحصلة من جرائم المخدرات، القاهرة 2002.

14.هدى حامد قشقوش: الحماية الجناية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000.

III- المقالات والبحوث

1. بوزبر محمد عبد الرحمن: بحث في المسؤولية الجنائية للأشخاص الاعتباريين عن جرائم غسل الأموال، دراسة تأصيلية مقارنة للقانون رقم 35 لسنة 2002، بشأن مكافحة عمليات غسل الأموال، موقع الدليل الالكتروني للقانون العربي،www.arablawinfo.com أطلع عليه بتاريخ: 2008/05/23.

2. محمد حماد الهيتي: البحث عن حماية جنائية للبيانات والمعلومات الشخصية (الاسمية) المخزنة في الحاسب الآلي، مجلة الشريعة والقانون – العدد السابع والعشرون – جمادى الثانية، 1427 هجرية – يوليو 2006.

3. مزاولي محمد: المسؤولية الجزائية للأشخاص الاعتبارية في مجال المعالجة الالية للمعطيات، بحث منشور في المجلة الالكترونية الشهرية، القانون والفقه، المملكة المغربية، رقم 23، 2014.

IIII- الرسائل الجامعية

1. بن سعدون رضا: المسؤولية الجنائية للأشخاص المعنوية على ضوء تعديل قانوني العقوبات والإجراءات الجزائية، مذكرة تخرج، المدرسة العليا للقضاء، الجزائر، دفعة 2006.

2. سوير سفيان: جرائم المعلوماتية، رسالة ماجستير، جامعة أبو بكر بالقايد – تلمسان، 2011.

3. قارة أمال: الجريمة المعلوماتية، مذكرة ماجستير، بن عكنون، جامعة الجزائر2002.

4. مزاولي محمد: المسؤولية الجزائية للأشخاص الاعتبارية الخاصة – دراسة مقارنة، رسالة دكتوراه، جامعة تلمسان، 2014.

ثانيا المراجع والمصادر باللغة الاجنبية.

I.OUVRAGES :

1. ANTONA Jean-Paul, **et al** : La Responsabilité Pénale des cadres et des dirigeants dans le Monde des Affaires, édition Dalloz, 1996.

2. CARTIER BRESSON. J., **et al** : Les délinquances économiques et financières transnationales et Globalisation, I.H.E.S.I, France, Juillet 2001.

3. DELMAS-MARTY Mireille et GUIDICELLI-DELAGE Geneviève : Droit pénal des affaires, 4ème édition refondue, Thémis, Puf, 2000.

4. GUYON Yves : Droit des affaires, Tom 1,9ème édition, Economica, 1996.

5. HUET. A . et KOERING-JOULIN. R : Droit pénal international, 3ème éd., PUF, 2005.

6. Jean- Claude Soyer, Droit pénal et procédure pénale, 12ème édition, DELTA, L.G.D.J, 1995.

7. LEROY. J : Droit pénal général, manuel, 2ème éd., L.G.D.J., 2007.

II. ARTICLES ET JURISPRUDENCES :

8. BELGHOUL Fréderic : « L'extension de la responsabilité pénale des personnes morales », mémoire de DEA de droit économique et des affaires d'Orléans, 2004, p. 37, paru sur site village-justice.com, vu le 21/02/2005.

9. BOULOUC Bernard : « Le domaine de la responsabilité pénale des personnes morales », Dalloz, Colloque sur la responsabilité pénale des personnes morales, université de Paris 1 le 7 avril 1993.

10. BOULOUC. B : Responsabilité pénale des personnes morales. Faute commise par un représentant. Portée, Revue de science criminelle 2002, p. 99

11. Cass. Crim. Inédit titré pourvoi n°01-82521.

12. La convention pénale sur la corruption-Strasbourg 27.01.1999, du conseil de l'Europe.

13. La convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, O.C.D.E, du 17.12.1997.

14. MBONGO. P : De l'inflation législative comme discours doctrinal. D., 2005, N°20, point de vue, p.130.

15. PLANQUE. J.C : Plaidoyer pour une suppression réfléchie de la spécialité de la responsabilité pénale des personnes morales, P.A., N°5, 7 janvier 2004., p.3.

16. SAINT-PAU Jean-Christophe : La présomption d'imputation d'une infraction aux organes ou représentants d'une personne morale, Recueil Dalloz 2007.

17. SAINT-PAU. J.C : L'entraide judiciaire internationale et européenne, D.P., juillet-août 2004, p.6.

18. SAUTEL. O : La mise en œuvre de la responsabilité des personnes morales ; Entre litanie et liturgie, D., 2002,, p.1148.

19. SERVERIN.E : L'application des sanctions pénales en droit social : un traitement juridictionnel marginal, D.S., N° spécial juillet août 1994, p.654.

20. SEUVIC Jean-François : Commerce électronique. Communication en ligne. Cryptologie. Cybercriminalité. « Télécommunications ». Analyse de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique Revue de science criminelle 2004 p. 925.

21. Abdelkader DERDOURI, Journal le soir d'Algérie du Mardi 28 Avril 2015, page 6 et 7.