تاريخ الاستلام: 2022/12/07 تاريخ القبول: 2023/03/01

الحماية القانونية للعمليات المصرفية الالكترونية في التشريع الجزائري

Legal protection for electronic banking Operations in Algerian Law .

ط د: بومنايل عبد المالك د. سنيسنة فضيلة

كلية الحقوق والعلوم السياسية ، مخبر الدراسات القانونية ومسؤولية المهنيين ،

جامعة طاهري محمد ، بشار ، (الجزائر)

malikrachida1993@gmail.com

ملخص

يهدف هذا المقال إلى دراسة مدى إمكانية تطبيق وإعمال النصوص القانونية العامة والخاصة لحماية العمليات المصرفية الالكترونية و معرفة مدى كفاية القوانين و التشريعات الوطنية الحالية في تامين العمليات المصرفية الالكترونية في مواجهة الإجرام التقني الماس بسلامتها وأمنها.

وقد تبين من خلال هذا البحث صعوبة تطبيق القوانين العامة والخاصة و إعمالها لحماية العمليات المصرفية الإلكترونية نظرا لخصوصية هذه العمليات كون القوانين الحالية تقليدية لم تنظم هذا النوع من الإجرام التقني الماس بالعمليات و الخدمات المصرفية الالكترونية الحديثة ، ما يستوجب على المشرع تعديل القوانين الحالية لتتماشى و الطبيعة الخاصة لهذا النوع المستجد و المستحدث من الإجرام أو إصدار قوانين جديدة تنظم هذه العمليات وتجرم أشكال المساس بها من اجل تامين العمل المصرفي الإلكتروني .

كلمات مفتاحية: العمليات المصرفية الالكترونية _ الحماية القانونية _ الإجرام الالكتروني _ التشريع الجزائري _ القوانين العامة والخاصة.

Abstract:

This article aims to study the extent to which public and private legal texts Can be applied to protect electronic banking operations from electronic crimes.

through the research the difficulty of applying public and private laws to protect electronic banking operations in view of the privance of this type of banking services ،which requiers the algerian legislator to amend traditional laws to suit the specificity of this new type of crimes to issue new laws to provide adequate protection operations and ensure their safety and SecurityKeywords: Electronic banking operations _ – legal protection _ – cyber crime_ algerian legislation _ public and privâtes laws.

*المؤلف المرسل.

. مقدمة:

تعد العمليات المصرفية الرقمية والتي تستخدم فيها الوسائل الالكترونية ووسائل الاتصال والتكنولوجيا الحديثة حاضر ومستقبل العمل المصرفي الحديث، تجاوبا مع عصر السرعة وظهور التجارة الالكترونية وكذا لتسهيل العمليات المصرفية وتوفير المال والجهد ،حيث تأثرت البنوك والمصارف بهذا التطور وتأقلمت معه بسرعة ولحقها في ذلك المجرم الذي استفاد بدوره من التكنولوجيا في أعماله الإجرامية وأصبح يهدد امن وسلامة العمليات المصرفية الرقمية وبيانات الزبائن وأموالهم ، كل هذا في ظل تأخر المشرع في إصدار قوانين تواكب التطور التكنولوجي و الإجرام الرقمي وظهور هذا النوع من الجرائم المستحدثة التي أصبحت تهدد هذه العمليات . وفي ظل الفراغ القانوني و صعوبة تطبيق القوانين والنصوص القانونية العامة خاصة في قانون العقوبات وفشلها في توفير حماية كافية ، لجا المشرع إلى إصدار قوانين خاصة لحماية تكنولوجيا الاتصال وتنظيم الاتصالات الالكترونية يمكن إعمال نصوصها لحماية العمليات المصرفية الرقمية ، وتبرز أهمية الموضوع من خلال تزايد الجرائم الماسة بالخدمات المصرفية الرقمية مايعرض المنظومة الاقتصادية بصفة عامة ونجاح العمل المصرفي الرقمي للخطر، وضرورة إيجاد حلول قانونية وتوفير الحماية القانونية لهذه العمليات ، ومعرفة مدى إمكانية تطبيق القوانين العامة لحماية العمليات المصرفية الرقمية ؟ بالإضافة إلى معرفة مدى توفيق المشرع من خلال القوانين الخاصة في توفير حماية حقيقية وفعالة لهذه العمليات؟ من خلال تحليل مختلف النصوص القانونية العامة والخاصة ووصف مختلف الجرائم الماسة بالخدمات المصرفية الرقمية ، بإتباع المنهج التحليلي و الوصفي وتقسيم البحث إلى مبحث أول بعنوان الحماية القانونية للعمليات المصرفية الرقمية في القوانين العامة ،أما الثاني فيتمحور حول الحماية القانونية للعمليات المصرفية الرقمية في القوانين الخاصة.

المبحث الأول: الحماية القانونية للعمليات المصرفية الالكترونية في القوانين العامة.

في ظل عدم مواكبة المشرع الجزائري للتطور الحاصل في المجال الالكتروني وما نجم عنه من تطور للفكر الإجرامي وظهور أشكال جديدة للإجرام المبني على استخدام الوسائل الالكترونية و المعلوماتية كأجهزة الحاسب والهواتف الذكية، والاستفادة من طرق الاتصالات الحديثة كالانترنت وغيره في الجرائم المستحدثة وانتشارها الكبير، حيث تتسم هذه الجرائم بسهولة ارتكابها وصعوبة الكشف عنها وإثباتها، كما تختلف فيها صفة المجرم عن صفة المجرم في الجرائم التقليدية كون المجرم الالكتروني أكثر ذكاءا واقل عنفا ولا تظهر عليه ملامح الإجرام ، وفي ظل احترام مبدأ الشرعية حيث انه "لا جريمة و لا عقوبة أو تدابير امن بغير قانون " (ج.ر، 1966.) وفي ظل غياب قانون خاص ينظم مسالة الجرائم المعلوماتية يثار التساؤل حول إمكانية تطبيق النصوص القانونية العامة الموجودة في قانون العقوبات لحماية هذه العمليات (المطلب الأول) في ظل وجود قاعدة عدم جواز القياس في القانون الجزائي و المحافظة على مبدأ المشروعية (kahloula, 2011) .

وتعتبر العمليات المصرفية الرقمية ميدانا خصبا للإجرام الناعم والثراء السهل عبر سرقة الأموال الالكترونية سواءا من البنوك أو الزبائن عبر عدة طرق ووسائل كالاحتيال والنصب وغيره كما تشكل جرائم القرصنة والتعدي على المنظومة المصرفية الرقمية تهديدا بالغا لأمن وسلامة هذه العمليات ما اوجب على المشرع توفير الحماية القانونية لأنظمة المعالجة الآلية للمعطيات (المطلب الثاني) من خلال تعديل قانون العقوبات لتجريم جميع أشكال المساس و التعدي على هذه المنظومات الآلية .

المطلب الأول: إعمال نصوص قانون العقوبات لحماية العمليات المصرفية الالكترونية .

تتعدد أشكال المساس بالعمليات المصرفية الالكترونية سواءا من خلال التعدي على الأجهزة الالكترونية أو أجهزة ووسائل الاتصال وكذا أنظمة المعالجة الآلية لهذه العمليات والقصد الجنائي الأهم للمجرم يتمثل في سرقة المال الرقمي الذي يعتبر أساس ومحور العمليات المصرفية الرقمية ،حيث يقوم المجرم بسرقة بطاقات الائتمان أو سرقة بيانات الزبائن لسرقة أموالهم(الفرع الأول) عبر عدة وسائل وطرق كالاحتيال

والنصب (الفرع الثاني) الذي تتعدد صوره في جرائم المساس بالعمليات المصرفية الالكترونية ، من خلال إرسال رسائل غير صحيحة ومن مصادر غير حقيقة و إيهام الضحية من اجل الحصول على بياناته وأرقامه السرية أو القيام بعمليات نقل أو تحويل للأموال .

الفرع الأول: جريمة السرقة في العمليات المصرفية الالكترونية .

من أهم أسباب الإجرام تحقيق الثراء وتعتبر السرقة قديمة قدم الإنسان وتطورت بتطوره فكلما حدث تطور إلا واستغل في السرقة ، ولجريمة السرقة الالكترونية في المجال المصرفي الالكتروني عدة صور وطرق يستخدمها المجرمون ومهما تعددت هذه الصور إلا أن الغاية واحدة وهي الوصول إلى الأموال ،حيث سنتطرق إلى بعض هذه الصور ونحاول إسقاط نصوص السرقة عليها لمعرفة مدى إمكانية تطبيقها ونجاعتها في التصدي للسرقة الالكترونية .

تتم العمليات المصرفية الالكترونية باستخدام وسائل معلوماتية وتكنولوجية كالحواسيب و الهواتف بواسطة تكنولوجيا الاتصال كالانترنت ،حيث تربط هذه الوسائل بين البنك والعميل باستخدام بيانات وكلمات مرور سرية بواسطة الايميل أو بواسطة البطاقات المصرفية ما قد يعرض هذه البيانات للسرقة أو حتى سرقة الأجهزة ووسائل العمليات الرقمية كالبطاقة المصرفية المغنطة ، حيث سنتطرق إلى هذين الشكلين من أشكال السرقة ومدى نجاعة نصوص السرقة التقليدية في التصدي لهما والمشاكل التي تثار بشان ذلك.

أولا – سرقة بطاقات الائتمان.

تعتبر البطاقة المغنطة من أهم وسائل العمليات المصرفية الرقمية التي تبنتها المصارف نظرا لمزاياها وسهولة استخدامها وقد عرفها المشرع الجزائري على أنها "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال وتعتبر بطاقة سحب كل بطاقة صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب أموال " (ج.ر، _ المادة رقم 543 مكرر 23 من الأمر رقم 75/ 54 ، المؤرخ في20رمضان عام 1395الموافق ل26 سبتمبر سنة 1975، يتضمن القانون التجاري ، ج ر101 الصادرة في16 ذو الحجة عام1395 الموافق ل 19ديسمبر سنة 1975 .، 1975) ، فهي وسيلة لسحب وتحويل الأموال بطريقة رقمية حيث يمكن أن تتعرض هذه البطاقات للسرقة حيث سمح المشرع بإمكانية الاعتراض على الدفع في حالة ضياع أو سرقة البطاقة (سابق).

كما عرف المشرع في قانون العقوبات السرقة على أنها " كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة إلى خمس سنوات وغرامة من 100 ألف دج إلى 500 ألف دج " (ج.ر، ،المتضمن قانون العقوبات ، مرجع سابق . 165/ 66 من الأمر رقم 350_ المادة رقم) ، ولا شك أن بطاقة الائتمان شيء مادي يمكن أن يتعرض للسرقة وتدخل في نطاق الجرائم التي تقع على المنقولات وتطبق على اختلاسها المواد المتعلقة بالسرقة في قانون العقوبات (بوسقيعة، 2008)، مع تحقق أركان جريمة السرقة المتمثلة في الركن المادي وهو فعل الاختلاس أو الأخذ بدون رضا وعلم المجني عليه والاستيلاء على حيازة الشيء أي البطاقة حيازة كاملة وإنهاء سلطة المجني عليه (زيدات، 2019) كونها تعتبر من قبيل الأشياء المادية ، وهنا يجب التفرقة بين تطبيق نصوص السرقة على سرقة البطاقة المصرفية كشيء مادي دون استعمالها وبين استعمال البطاقة المسروقة ففي هذه الحالة تصبح البطاقة وسيلة وتصبح سرقتها من ضمن الأعمال التحضيرية لارتكاب (زيدات، ، مدى استيعاب النصوص التقليدية للسرقة الالكترونية دراسة مقارنة ، مرجع سابق ،) جريمة سرقة أموال رقمية بطريقة الكترونية إلا أن سرقة البطاقة بحد ذاته يعتبر جريمة لا تثير إشكالا في إمكانية تطبيق نصوص السرقة التقليدية عليها.

ثانيا : سرقة معلومات وبيانات الزبائن والبنوك

إن العمليات المصرفية الالكترونية تعتمد أساسا على الوسائل الالكترونية تقوم بهذه العمليات ويتم الربط بينها عبر الانترنت، حيث يتم نقل وتبادل الأوامر والقيام بهذه العمليات عبر إرسال واستقبال معلومات وبيانات خاصة يمكن من خلالها التعرف على الزبائن وتلبية

طلباتهم ، حيث قد تتعرض هذه البيانات للسرقة وقد تكون هذه البيانات عبارة عن أسماء الزبائن أو بريدهم الالكتروني أو معلومات خاصة بذممهم المالية أو عبارة عن كلمات المرور سرية وغيره، وهنا يثار الإشكال حول إمكانية تطبيق نصوص السرقة التقليدية على البيانات والمعطيات فمن خلال تعريف المشرع للسرقة استعمل المشرع عبارة "شيئا غير مملوك له " ولم يحدد ما إذا كان الشيء ماديا أو معنويا وإطلاق اللفظ على العموم يفهم منه عدم الاقتصار على الأشياء المادية بل يتعدى إلى الأشياء المعنوية وأما كون البيانات و المعلومات أشياء معنوية قابلة للسرقة ولها قيمة مادية يتجلى في إمكانية بيعها أو استعمالها لسرقة الأموال الرقمية وتحويلها إلى أموال ملموسة كأوراق مالية ، فالقيمة الاقتصادية لهذه البيانات و المعلومات قد تفوق قيمة الأموال العادية لذلك تم اللجوء إلى المعيار الاقتصادي للشيء إذ يعتبر مالا ليس بالنظر إلى كيانه الملموس المادي وإنما لقيمته الاقتصادية (العتيق، 2006) ، كما يمكن ابتزاز أصحابها لغرض الحصول على منافع منهم سواءا كانت مادية أو وظيفية أو غيرها من المنافع وكما سبق الإشارة في الجزء الأول من هذا الفرع كون استخدام هذه البيانات لأجل القيام بجريمة أخرى كالابتزاز مثلا أو السرقة أو غيره يعتبر من قبيل الأعمال التحضيرية ويعاقب عليه من خلال العقاب عل الجريمة المتحققة بواسطة هذه المعلومات أو البيانات وليس كون سرقة البيانات و المعلومات جريمة منفردة.

كما أن سرقة المعلومات والبيانات تتوفر على أركان جريمة السرقة حيث يتحقق الركن المادي باختلاس أي اخذ المعلومات والبيانات دون علم ورضا المجني عليه مع وجود فرق جوهري كون اختلاس المعلومات والبيانات قد لايتم خلاله نقل حيازتها إلى الجاني نقلا تاما أي احتكار أو حيازة المعلومات حيازة منفردة وحرمان المجني عليه منها عكس السرقة التقليدية حيث يتم نزع الشيء من المجني عليه ، بحيث لا تصبح له سلطة عليه عكس المعلومات التي يمكن تقاسم حيازتها وهنا نتحدث عن سرقة البيانات دون استعمال وسيلة الكترونية أي عبر مشاهدة كلمة مرور لشخص ما مثلا وحفظها أو عبر الاطلاع على وثائق للمجني عليه تتضمن معلوماته وبياناته الشخصية التي ينعدم حق الغير في الاطلاع عليها مراعاة لخصوصيتها إلا بإذن صاحبها أو السلطة المختصة (الرومي، 2004) ، أما الحصول عليها بواسطة استخدام وسائل تكنولوجية سنتطرق إليه لاحقا، أما الركن المعنوي فيتمثل في علم الجاني أن المعلومات والبيانات سرية وملك للغير وانه يعتدي عليها وإرادته إلى إتيان هذا الفعل و حيازة هذه المعلومات ويتحقق الركن المعنوي من خلال سوء نية الجاني في حفظ تلك المعلومات وإلا فما الفائدة والغاية من تسجيل تلك المعلومات الشخصية ، أما الركن الشرعي فيتمثل في المادة 350 من قانون العقوبات الجزائري المتعلقة بالسرقة و بالرغم من أن البيانات و المعلومات ليست من قبيل الأشياء المادية و السرقة تقع على الشيء المادي فهي اعتداء على حق الملكية أي ضرورة أن يكون الشيء الذي ينصب عليه السلوك الإجرامي محلا لحق الملكية (زيدات، مدى استيعاب النصوص التقليدية للسرقة الالكترونية ، مرجع سابق) ،أي أن تتم الجريمة بمجرد اختلاس الشيء وان لا يكون اختلاس الشيء من قبيل الأعمال التحضيرية لجريمة أخرى مثل سرقة المال تعتبر جريمة بمجرد اختلاس المال ،مع توفر شروط الركن المادي و المعنوي لفعل الاختلاس أما سرقة المعلومات وبيانات الزبائن والبنوك وكلمات مرور بطاقات المصرفية فهو عبارة عن عمل تحضيري لجريمة أخرى كالسرقة أو الابتزاز وغيره وهنا يكمن القصور الموجود في قانون العقوبات في جريمة السرقة كونها نصوص تقليدية يجب تعديلها لتتماشى مع الطرق المستحدثة للسرقة أو السرقة الالكترونية ،ووجوب تجريم سرقة المعلومات والبيانات بنص واضح لا يترك مجالا للتأويل أو الشك أو الدفع بعدم التجريم خاصة وان النصوص القانونية تفسر تفسيرا ضيقا وغالبا لمصلحة المتهم.

الفرع الثاني : تطبيق نصوص النصب والانتحال في جرائم المال الرقمي .

تتم العمليات المصرفية الرقمية عبر تبادل البيانات السرية التي تعرف البنك بالزبون والتي تسمح للزبون بالقيام بمختف العمليات المصرفية ، حيث تقدم هذه البيانات والتي تقتضي الخصوصية عدم كشفها للغير و الامتناع عن الاعتداء عليها أو استعمالها (الزغبي، 2006) ، تعريفا كاملا للزبون من اسمه و رصيده ورقم حسابه وغيره وبمجرد إدخال هذه البيانات يتعرف البنك على الزبون ويقوم بانجاز طلباته وإتمام عملياته فتكون هذه البيانات الباعث على انجاز هذه العمليات ،حيث قد تتم سرقتها واستخدامها فيقوم الجاني بانتحال اسم

الشخص وصفته كزبون للبنك عبر استخدام هذه البيانات حيث تعتبر انتحال الشخصية من أسهل الطرق المتداولة للدخول إلى الحسابات و المواقع المصرفية (خليفة، 2007) خاصة وان اغلب العمليات المصرفية الرقمية لا يتم فيها التأكد من هوية الزبون مثلا عبر كاميرا الحاسوب أو البصمة أو عبر كاميرا الصراف الآلي .

وفي هذه الصورة يقوم الجاني بانتحال صفة واسم الزبون وينجز بذلك مختلف العمليات (سعد، 2007)

أو قد ينتحل اسم أو صفة البنك عبر تصميم تطبيق مماثل لتطبيق البنك مثلا أو عبر إرسال رسائل موهما الزبون انه البنك وإعطاء أوامر للزبون أو طلب تغيير بياناته ، وهنا نتساءل عن إمكانية تطبيق النصوص المتعلقة بانتحال الأسماء والصفات على هذا الفعل فمن خلال استقراء نصوص قانون العقوبات من المادة 242 إلى المادة 253 مكرر (ج.ر، ، المتضمن قانون العقوبات ، المعدل 66/156مكرر من الأمر رقم 253إلى المادة 242_ المواد من المادة) ، يظهر جليا قصور هذه النصوص في احتواء هذا الشكل من الانتحال والإجرام كون هذه النصوص وعلى عكس نصوص السرقة التي جاءت عامة وفضفاضة فان نصوص المتعلقة بانتحال الوظائف والألقاب و الأسماء أو إساءة استعمالها يصعب إعمالها حماية للعمليات المصرفية من جرائم الانتحال لأسماء وصفات الزبائن أو البنك، كون المشرع ربط هذه الجرائم بالوظائف أو ببعض الوثائق بحيث ضيق من إمكانية تطبيق هذه النصوص ولذلك وجب على المشرع تدارك هذا الفراغ القانوني عبر تعديل هذه النصوص لتشمل جريمة انتحال الأسماء والصفات في الجرائم المصرفية الالكترونية .

أما المادة 372 من قانون العقوبات المتعلقة بجريمة النصب فمن خلال استقراء هذه المادة ومحاولة معرفة مدى إمكانية تطبيقها في مجال الخدمات المصرفية الرقمية حيث أن المشرع الجزائري عرف جريمة النصب على أنها "كل من توصل إلى استلام وتلقي أموالا أو أوراق مالية " والمال الرقمي مال أي ذو قيمة مادية بالرغم من طبيعته الخاصة اللامادية إلا انه يمكن تحويله إلى مال ملموس أو مادي حيث ينطبق عليه وصف المال ، وأضاف المشرع "أو شرع في ذلك وكان ذلك بالاحتيال " أي باستعمال أساليب وطرق لاتدع مجالا للشك في نفس المجني عليه سواءا كان الزبون أو البنك بأنه يتعامل مع الجهة الصحيحة ، حيث يستعمل الجاني أساليب وأفعال كاستخدام اسم البنك في الايميلات أو الرسائل النصية أو تقليد تطبيقات البنك أو موقعه الالكتروني أو يقوم بأفعال و ممارسات كي يظهر للبنك بمظهر الزبون أو صفته وتكون هذه الأفعال الباعث على تلقي الأموال أو إرسالها أو في إجراء عمليات مصرفية الكترونية ، وأضاف المشرع باستعمال "أسماء وصفات كاذبة "وهو الجرم المنتشر بكثرة في العالم الافتراضي لسهولة انتحال الأسماء و الصفات وتقليدها أو سرقة حسابات الأشخاص واستعمالها للنصب ، وفي ظل توفر أركان الجريمة من ركن مادي المتمثل في القيام بأفعال و أعمال بطرق احتيالية من اجل تلقي أموال من المصرف أو الزبون وتوافر القصد الجنائي المتمثل في علم وإرادة الفاعل إلى ارتكاب جريمة من خلال تلقي أموال باستعمال صفات وأسماء الغير ، بالإضافة إلى وجود الركن الشرعي المتمثل في المادة 372من قانون العقوبات بحيث يمكن تطبيق العقوبات المتعلقة بجريمة النصب التقليدية على جرائم النصب الالكتروني للعمليات المصرفية الرقمية حيث عاقب المشرع على ذلك بالحبس من سنة إلى خمس سنوات وغرامة من 50ألف إلى 100 ألف دينار جزائري بالإضافة إلى العقوبات التكميلية .

المطلب الثاني: حماية نظم المعالجة الآلية للمعطيات في قانون العقوبات .

تعتمد العمليات المصرفية الرقمية اعتمادا كليا على الوسائل التكنولوجية ووسائل الاتصال الحديثة في تبادل المعطيات و الأوامر وتنفيذها ، ويتم من خلالها القيام بمختلف العمليات المصرفية عبر منظومات آلية لمعالجة المعطيات و المعلومات وتحليلها حيث أن المشرع لم يعرف المنظومة الآلية لمعالجة المعطيات في قانون العقوبات ولكن بالرجوع إلى القانون رقم09 / 04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها ، نجد أن المشرع عرف المنظومة الآلية لمعالجة المعطيات بذكر وظيفتها و الغاية منها المتمثلة في المعالجة الآلية للمعطيات تنفيذا لبرنامج معين (رقم، 2009) ، ولذلك سنحاول التطرق إلى مكونات وأبعاد المنظومة

الآلية وطريقة عملها في معالجة المعطيات المتعلقة بالعمليات المصرفية الرقمية والحماية القانونية للنظام المصرفي الآلي من خلال نصوص قانون العقوبات (الفرع الأول) ، من ثم التطرق إلى أشكال المساس بالمعطيات المعالجة أليا في البنوك (الفرع الثاني) .

الفرع الأول : الحماية القانونية للنظام المصرفي الآلي من خلال نصوص قانون العقوبات .

يرتبط البنك بالزبون عبر تبادل وإرسال واستقبال البيانات والمعلومات عبر منظومة آلية لمعالجة المعطيات الكترونيا تتصل عبر النت أو وسائل اتصال أخرى ،وتتكون المنظومة المصرفية الآلية من أجهزة آلية كالحواسيب أو الصراف الآلي وترتبط بالزبون بواسطة الانترنت إما باستعمال الكمبيوتر أو البطاقات المصرفية والصراف الآلي وغيره والتي تسمح بتبادل البيانات عن طريق الاتصال بالتطبيقات أو مواقع البنوك الالكترونية ، وتتم انجاز مختلف العمليات بصفة آلية كجمع المعلومات وتحليل البيانات وتسجيلها وتعديلها وتوفيرها وغيره من عمليات المعالجة (سابق، المادة رقم.04 / 09من القانون رقم 02_)، ويتم الاعتداء أو المساس بهذه المنظومة جراء الاعتداء على مكوناتها أو طريقة عملها أو طرق الاتصال بها.

أولا : تجريم الدخول أو البقاء في منظومة معالجة آلية للمعطيات.

لقد عاقب المشرع الجزائري بالحبس كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك (ج.ر، المادة رقم 394 ، المتضمن قانون العقوبات . من الأمر رقم 66/156_ مكرر،مرجع سابق).

ا _ تجريم الدخول إلى المنظومة الآلية لمعالجة المعطيات.

لابد من التفرقة بين المنظومة التي يسمح بالدخول إليها من خلال تطبيقات أو المواقع الالكترونية التي تستخدمها البنوك والمصارف في عملياتها الرقمية والتي تسمح للزبون من الدخول إلى نظام المعالجة الآلية من اجل إجراء العمليات المصرفية ، وبين الدخول إلى أنظمة غير مسموح بالولوج إليها واستعمل المشرع عبارة " عن طريق الغش " للإشارة إلى القصد الجنائي والركن المعنوي للجريمة فمجرد الدخول يعتبر فعلا مجرما يعاقب عليه حتى وان لم يعقبه مساس بالنظام وبطريقة عمله أو بمعطياته ، وكذلك بالنسبة إلى الدخول إلى الجزء الغير مسموح الدخول إليه بالنسبة للأنظمة المفتوحة للجمهور أو الزبائن أو حتى دخول الموظف في البنك إلى جزء من المنظومة متعديا بذلك الحدود المسموح له بها يعتبر دخولا مجرما يعاقب عليه القانون.

ب _ تجريم البقاء في منظومة آلية لمعالجة المعطيات.

جرم المشرع الدخول إلى منظومات المعالجة الآلية للمعطيات وتثير عبارة "عن طريق الغش " التساؤل إذا ما تم الدخول دون قصد هل يعتبر فعلا مجرما ؟ في ظل عدم وجود القصد الجنائي حيث أشار المشرع لهذه الحالة باستعمال عبارة "أو يبقى " أي البقاء في منظومة آلية عن قصد وبطريقة الغش وان كان الدخول غير مقصود ،حيث يثير البقاء إشكالا كونه لا يمكن معرفة متى علم الفاعل بدخوله الغير مشروع وإرادته البقاء داخل المنظومة حيث يرى جانب من الفقه انه بمجرد تصفح النظام والتجول فيه يقوم الركن المادي للجريمة ، أما الركن المعنوي لجريمة البقاء يقترن بالغش يظهر في سلوك الفاعل كحفظ البيانات أو الدخول مرة أخرى لنفس المنظومة وتنتشر هذه الفعال بكثرة في مواقع البنوك الالكترونية وتطبيقاتها ، كما ضاعف المشرع العقوبة في حالة ترتب على الدخول أو البقاء حذف أو تغيير في معطيات المنظومة (ج.ر، ، المتضمن قانون العقوبات، مرجع سابق.66/156 من الأمر رقم 394_ الفقرة الثانية، من المادة رقم) ، أما إذا تم تخريب المنظومة فالعقوبة تكون الحبس من ستة أشهر إلى سنتين وغرامة من 50 ألف إلى 150 ألف دينار جزائري.

ج _ تجريم إدخال أو إزالة معطيات في نظام المعالجة الآلية أو تعديلها.

عاقب المشرع الجزائري بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500 ألف إلى 2 مليون دينار جزائري كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها (ج.ر، المادة رقم 394_ مكرر1، من الأمر66/156 مرجع سابق .) ، وفي العمليات المصرفية الرقمية قد تتم هذه العمليات أو الأفعال المجرمة الثلاثة إما من الموظف في

المصرف الذي بحكم وظيفته واطلاعه وإمكانية وصوله السهلة إلى نظام المعالجة يقوم بإدخال معطيات مثلا كإضافة أموال إلى رصيد شخص ما أو إزالة أو تعديل رصيد الزبائن وغيره من الأفعال كون هذه الأموال عبارة عن معطيات متمثلة في أرقام يسهل تعديلها ، وقد يتم من الزبون أو الغير الذي يقوم بالدخول إلى النظام وإزالة أو تعديل المعطيات أو تحويل الأموال إضرارا بالغير أو المصرف أو لفائدته أو لمصلحة شخص أخر .

الفرع الثاني : أشكال المساس بالمعطيات المعالجة آليا .

تتعدد أشكال المساس بالمعطيات المعالجة أو المخزنة أو المرسلة عن طريق منظومة آلية حيث عاقب المشرع على هذه الأفعال المتمثلة في تصميم أو البحث أو تجميع أو توفير ونشر أو الاتجار في هذه المعطيات بالحبس من شهرين إلى ثلاث سنوات وغرامة من مليون إلى خمسة ملايين دينار جزائري عن طريق الغش بتوفر القصد الجنائي (ج.ر، المادة رقم 2 394 _ مكرر 2 .من الأمر 66/156 مرجع سابق) .

أولا : تصميم المعطيات.

التصميم هو كل رسم أو تخطيط والمقصود به في نصوص المعالجة الآلية للمعطيات هو كل إنشاء للمعطيات والمعلومات والبيانات التي تسمح بالدخول إلى منظومة آلية مثل تصميم تطبيق للبنك وهو عبارة عن مجموعة من المعلومات والبيانات تظهر في شكل معين والذي يتم من خلاله الدخول إلى المنظومة والقيام بمختلف العمليات المصرفية الرقمية ، فقد يقوم المجرم بتقليد هذا التطبيق ووضع تصميم مشابه له ليظهر بنفس مظهره عن طريق تصميم نفس المعطيات الموجودة في التطبيق الأصلي أو عبر تصميم تطبيقات أو فيروسات تسمح بالدخول إلى منظومة المعالجة الآلية للمعطيات للمصرف.

ثانيا : البحث في المعطيات المخزنة.

تتمثل في محاولة إيجاد معلومات وبيانات التي يتم من خلالها ارتكاب إحدى الجرائم المنصوص عليها كالبحث عن المعطيات الخاصة بكيفية الدخول إلى الحسابات البنكية للزبائن ، أو الطريقة التقنية للتعرف على الزبائن وكيفية عمل تطبيقات البنك وأنظمته للمعالجة الآلية للمعطيات وغيره من العمليات التي قد تمس بسلامة وامن العمليات المصرفية الرقمية.

ثالثا : تجميع المعطيات والمعلومات.

أي القيام بتخزين المعطيات و البيانات المتعلقة بالمنظومات الآلية سواءا التي تحتويها هذه المنظومة المتعلقة بكيفية عمل المنظومة كتجميع أسماء الزبائن وأرقام حساباتهم وأرقام بطاقاتهم الائتمانية وحتى أرقام مرورهم ، أو تجميع معطيات وبيانات حول المواقع الالكترونية للبنوك أو حول تطبيقاتهم حيث قد تستخدم هذه البيانات في الجرائم المنصوص عليها في هذا الباب السالفة الذكر.

رابعا : توفير المعطيات والبيانات.

بعد جمع المعطيات والبيانات تصبح متوفرة وموجودة وجاهزة للاستخدام للأغراض الإجرامية حيث يتم تخزينها وجمعها وتثبيتها على مختلف الدعامات.

خامسا : نشر المعطيات والمعلومات.

وهي عملية عرضها للجمهور ما يمكنهم من الاطلاع على محتواها ومعرفتها و إمكانية استخدامها لأي غرض مجرم.

سادسا : الاتجار في المعطيات والبيانات.

أي الحصول على مقابل مادي وربح مقابل تقديم المعطيات وبيعها للراغبين في الحصول عليها ، ويلاحظ تسلسل هذه الأفعال من تصميم معطيات إلى البحث عنها مايؤدي إلى تجميع اكبر قدر منها فتصبح متوفرة وخزنة يمكن نشرها بسهولة مجانا أو المتاجرة فيها وبيعها.

سابعا : تجريم التعامل في المعطيات عائدات الإجرام.

حيث جرم المشرع جميع أشكال المساس بالمعطيات بالإضافة إلى ذلك جرم كذلك أشكال التعامل في المعطيات المتمثلة في الآتي :

ا _ حيازة المعطيات المتحصل عليها من الجرائم الواقعة على النظم الآلية.

يقصد بالحيازة وضع اليد على هذه المعطيات ذات الأصل الإجرامي عبر جمعها وتخزينها على أي دعامة ولأي سبب من الأسباب ، ويتمثل الركن المادي لهذه الجريمة في تخزين وجمع هذه المعطيات مع وجوب العلم بكون هذه المعطيات لايجوز حيازتها وأنها محصلة من أفعال مجرمة وإرادة الفاعل إلى القيام بالركن المادي لها وإتيان هذا الفعل.

ب _ إفشاء المعطيات المتحصل عليها من الجرائم الواقعة على النظم الآلية.

أي اطلاع الغير على معطيات لا يسمح له بالاطلاع عليها ويكون الإفشاء من شخص ائتمن على هذه المعطيات ، كإفشاء ضابط في الشرطة القضائية معطيات متحصل عليها من إحدى هذه الجرائم كانت بحوزته بسبب تحقيق في جريمة.

ج _ نشر المعطيات المتحصل عليها من الجرائم الواقعة على النظم الآلية.

إظهارها وتقديمها للجمهور في صورة تمكنهم من الاطلاع عليها حتى وان لم يتم استخدامها في أعمال إجرامية ، مع علم الفاعل بسرية المعطيات وانه لا يجوز نشرها و إرادته إلى القيام بالجريمة عن قصد.

د _ استخدام المعطيات المتحصل عليها من الجرائم الواقعة على النظم الآلية.

كل استعمال واستفادة من هذه المعطيات لأي غرض مع وجود قصد الجنائي وتوافر أركان الجريمة.

كما يلاحظ أن المشرع الجزائري عاقب على الاشتراك في الاتفاق للإعداد لهذه الجرائم بشرط وجود أفعال مادية تحضيرية بالعقوبات المقررة للجريمة ذاتها وكذا بالنسبة للشروع . (ج.ر، المادة رقم 394_ مكرر5 من الأمر رقم 66/156، المتضمن قانون العقوبات ، مرجع سابق .)

المبحث الثاني :الحماية القانونية للعمليات المصرفية الرقمية في القوانين الخاصة .

إلى جانب القوانين العامة كرس المشرع الجزائري الحماية القانونية في القوانين الخاصة في نصوص متفرقة منها ، خاصة في ظل الفراغ و النقص الكبير الموجود في القوانين العامة وعلى رأسها قانون العقوبات الذي لم يعدل ليواكب هذا النوع من الإجرام ، حيث تبرز مجموعة من القوانين التي يمكن إعمال نصوصها حماية للعمليات المصرفية الرقمية حيث تم إصدار مجموعة من القوانين من اجل حماية تكنولوجيا الإعلام والاتصال ومكافحة الجرائم الماسة بها (المطلب الأول) ، وكذا قانون لتنظيم الاتصالات الالكترونية (المطلب الثاني) من اجل توفير اكبر قد ممكن من الحماية للاتصالات الالكترونية التي تعد عصب العمل المصرفي الرقمي المبني أساسا عليها ، خاصة في ظل غياب قانون متخصص أو حتى تعديل لقانون العقوبات يضمن ويكفل حماية العمليات المصرفية الرقمية من الإجرام الرقمي الماس بها .

المطلب الأول : حماية تكنولوجيا الاتصال في مجال العمليات المصرفية الالكترونية .

يعد التطور التكنولوجي الكبير في وسائل الاتصال الحديثة وبداية عصر السرعة و التكنولوجيا أهم دوافع التحول الكبير في العمل المصرفي من الخدمات التقليدية التي تعتمد على الأوراق وحضور الأطراف وتسليم وتسلم الأوراق و الأموال إلى استخدام التكنولوجيا والعمل

المصرفي الالكتروني الحديث ، إلا أن تطور المصارف وعملها تبعه تطور الإجرام الذي استفاد بدوره من التكنولوجيا وظهور الإجرام الرقمي فتطور فكر وعمل المصارف تزامن مع تطور طرق و أشكال المساس بهذا النوع من تقديم الخدمات المصرفية باستعمال وسائل الاتصال الحديثة ، حيث تدارك المشرع أهمية حماية تكنولوجيا الاتصال ما ينجم عنه حماية العمليات المصرفية من الجرائم الماسة بتكنولوجيا الاتصال (الفرع الأول)كون تكنولوجيا الاتصال أهم عامل في إتمام العمل المصرفي الرقمي ،كما قام المشرع بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته (الفرع الثاني) .

الفرع الأول : حماية العمليات المصرفية الرقمية من الجرائم الماسة بتكنولوجيا الاتصال .

لا يمكن تصور إجراء أو القيام بالعمليات المصرفية الحديثة المعتمدة على الأجهزة الالكترونية بدون وجود وسيلة للاتصال واستعمال لتكنولوجيا الاتصال الحديثة ، حيث عرف المشرع الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات ترتكب عن طريق منظومة معلوماتية أو نظام اتصال الكتروني " (ج.ر، المادة 02 من القانون رقم،09/04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا_ الاتصال والاعلام مرجع سابق) ، ومعروف أن العمليات المصرفية الرقمية تتم بواسطة منظومة آلية لمعالجة بيانات وحسابات الزبائن والمنظومة هي عبارة عن " نظام منفصل أو متصل أو مجموعة من الأنظمة المتصلة أو المرتبطة تقوم بمعالجة الآلية للمعطيات تنفيذا لبرنامج معين " (ج.ر، الفقرة الثانية من المادة رقم 02_ ، من القانون رقم 09/04 مرجع سابق .) ، حيث تعتمد المصارف على مجموعة من الأجهزة التي تقوم بمعالجة الآلية المعطيات الرقمية والمتمثلة في " عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بواسطة برامج تجعل المنظومة تؤدي عملها (ج.ر، الفقرة جيم من المادة رقم 02_ من القانون رقم 04/ 09 مرجع سابق .)" ،وتعالج حسابات الزبائن والعمليات المصرفية ومختلف الأوامر عبر تطبيقات ومواقع الكترونية تتيح الولوج لنظام البنك وتعد بمثابة بوابة لها عن طريق الاتصال الالكتروني المتمثل "في أي إرسال أو تراسل أو استقبال علامات أو معلومات بواسطة وسيلة الكترونية " (ج.ر، الفقرة واو من المادة رقم 02_ ،من القانون رقم.09/04 مرجع سابق) ، قد تكون جهاز كمبيوتر أو الهاتف أو الصراف الآلي وغيره وللحفاظ على سرية هذه البيانات والمعلومات.

وإبرازا لمدى خطورة المساس بها قيد المشرع من إمكانية مراقبة هذه الاتصالات حتى في حالات التحقيق في الجرائم فضلا عن قيام أشخاص غير مخول لهم قانونا بالمساس بسرية الاتصالات ، حيث لم يجز ذلك إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة بحيث أجاز القيام بعمليات المراقبة في حالات من بينها المساس بالاقتصاد الوطني (ج.ر، _الفقرة باء من المادة رقم 04، من القانون رقم 09/04 مرجع سابق.) ، ولا شك أن المساس بالعمليات المصرفية الرقمية فيه مساس بالاقتصاد إما بتحجيم دور البنوك وتقليص حركة الأموال بين الزبائن و البنوك وبث الخوف في التعامل مع البنوك خاصة باستعمال الوسائل الحديثة وهو مستقبل العمليات المصرفية بل حاضره فاغلب العمليات المصرفية رقمية ما يضر بالاقتصاد الوطني ، حيث يمكن مراقبة الاتصالات الالكترونية والمعطيات التي تسمح بالتعرف على مستعملي الخدمة اللذين يقومون بتهديد امن وسلامة هذه العمليات من اجل إثبات جرائمهم وجمع الأدلة التي تدينهم ، حيث نظم المشرع وضبط القواعد الإجرائية لتفتيش المنظومات المعلوماتية و حجز المعطيات التي تكون مفيدة في كشف الجرائم ومرتكبيها كما فرض على مقدمي الخدمات تقديم المساعدة للسلطات في هذا الشأن ، لتوفير حماية حقيقية لحق الإنسان في احترام حياته الخاصة وحرمة اتصالاته والمراسلات الخاصة به . (احمد)

الفرع الثاني : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحته.

نصت المادة 13 من قانون رقم 09 / 04 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكافحته توكل لها مجموعة من المهام لتنشيط وتنسيق عمليات الرقابة على الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، ومساعدة الشرطة القضائية و السلطات القضائية في التحريات في هذه الجرائم وتبادل وجمع المعلومات في هذا الصدد (ج.ر، المادة رقم 14_ من القانون

رقم 09/04 ، مرجع سابق .) ، وفي سنة 2015 تم إصدار المرسوم الرئاسي رقم 261 يحدد تشكيل وسير وتنظيم هذه الهيئة (ج.ر، المرسوم الرئاسي رقم 15/261_الموافق ل08 أكتوبر سنة 2015يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام .2015أكتوبر سنة 08الموافق ل 1436ذو الحجة عام 24 ،الصادرة في 53ومكافحتها ، ج ر ، 2015) ، وهي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع لدى الوزير المكلف بالعدل تكلف باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و القيام بالمراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم والأعمال التحضيرية ، وتسجيل و حفظ المعطيات الرقمية وتحديد مسارها و مصدرها من اجل استعمالها في الإجراءات القضائية ، كما عرفت الاتصالات الالكترونية على أنها " كل تراسل و إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة الكترونية (ج.ر، المادة رقم 05_ من المرسوم رقم،.15/261 مرجع سابق) ، وأضاف المشرع الهاتف النقال أو الثابت وأدرجهما ضمن الوسائل التكنولوجية متمما بذلك التعريف الذي جاء في المادة الثانية من القانون رقم 09 / 04 الذي لم يتطرق للهاتف ، خاصة و أن اغلب العمليات المصرفية حاليا تتم بواسطة الهاتف عبر النت أو بواسطة الرسائل وغيره من الطرق ،حيث تطرق الفصل الثاني من هذا المرسوم إلى تشكيل الهيئة وتنظيمها حيث تظم الهيئة اللجنة المديرية و تتشكل من مجموعة من الأعضاء (ج.ر، _المادة رقم 07 ، من المرسوم رقم 15/261 مرجع سابق .) ، تكلف اللجنة بتقييم حالة الخطر واقتراح كل نشاط يتعلق بالبحث وتقيم الأعمال المباشرة في مجال الوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال (ج.ر، المادة رقم ، 08 من المرسوم رقم_15/261 مرجع سابق .) ،بالإضافة إلى مديرية المراقبة الوقاية واليقظة الالكترونية من اجل تنفيذ العمليات المراقبة الوقائية للاتصالات للكشف عن الجرائم بعد الحصول على إذن من السلطة القضائية وتحت مراقبتها ، وإرسال المعلومات المتحصل عليها إلى مصالح الشرطة القضائية و تقوم بتنفيذ طلبات المساعدة القضائية الأجنبية وتحديد مكان مرتكبي الجرائم المعلوماتية و التي تنشا عن كل استخدام غير مشروع للتقنية المعلوماتية ووسائل التكنولوجيا الحديثة أضرارا بالمصالح العامة أو الخاصة (كامل، 2003)وتقوم بتوعية مستعملي تكنولوجيا الإعلام والاتصال حول المخاطر المتصلة بها (ج.ر، المادة رقم 11_،من المرسوم رقم 15/261مرجع سابق .) ، كما تقوم بتسجيل الاتصالات الالكترونية التي تكون موضوع مراقبة وتحرر وفق الشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية، وتقدم التسجيلات والمحررات إلى مصالح الشرطة القضائية و السلطات القضائية كما سمح المشرع للقضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارسة مهامهم بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية في حالة معالجة أفعال يمكن وصفها جزائيا بعد إخطار النائب العام المختص إقليميا . (ج.ر، المادة رقم 30 _ من المرسوم رقم15/261 ، مرجع سابق .)

المطلب الثاني : الحماية القانونية للاتصالات الالكتروني و الأنظمة المعلوماتية .

تعتبر حماية الاتصالات الالكترونية و الأنظمة المعلوماتية أساس حماية العمليات المصرفية الرقمية كونها اتصالات الكترونية تتم بواسطة منظومات معلوماتية ، وكون أي تهديد للاتصالات الالكترونية ووسائلها وكذا الأنظمة الآلية و الرقمية والمساس بها يؤدي حتما إلى المساس بأمن وسلامة هذه العمليات أو يسهل ذلك ،حيث اصدر المشرع قانون خاص يحدد القواعد العامة للبريد والاتصالات الالكترونية (الفرع الأول) وتم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية (الفرع الثاني) .

الفرع الأول : تنظيم وحماية الاتصالات الالكترونية .

تتم العمليات المصرفية الرقمية عبر تبادل البيانات و المعطيات باستعمال أجهزة الكترونية تتصل فيما بينها عبر الانترنت حيث نظم القانون الاتصالات الالكترونية وحدد القواعد العامة المتعلقة بها و التي من شانها توفير وتقديم خدمات الاتصالات الالكترونية في ظروف موضوعية وشفافة وترقية استعمال هذه الاتصالات (ج.ر، المادة رقم 03 _ من القانون رقم 18/04 المؤرخ في 24 ، ،

مايو2018الموافق ل 10 شعبان1439 عام، 2018) ، واخضع نشاطات الاتصالات الالكترونية إلى رقابة الدولة ، كما تسهر الدولة على امن وسلامة شبكات الاتصالات الالكترونية ، وتجريم ومحاربة جميع أشكال المساس بها حيث جاء القسم الثاني من هذا القانون المعنون بالاتصالات الالكترونية بتعريف لها فهي "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية" ، حيث تتم العمليات المصرفية الرقمية بواسطة تراسل البيانات بين الزبائن والمصرف عبر وسائل الاتصال الالكترونية عن طريق التطبيقات أو المواقع الموجودة على الانترنت وعرف هذا القانون الإنترنت على أنها " شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة موصولة فيما بينها عن طريق بروتوكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها " ، حيث قد تتعرض هذه الشبكة للاعتداء أو القرصنة مايحتم توفير الأمن السيبراني وهو " يتمثل في مجموعة من الأدوات والبيانات والمفاهيم و الآليات الأمنية و المبادئ التوجيهية و طرق تسير المخاطر والأعمال و التكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد أي حدث من شانه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة " ، والعمليات المصرفية الرقمية عرضة لعديد من أشكال المساس بها وبأمن بياناتها وسريتها فقد يتم حجب مواقع البنوك على النت ومنع الوصول إلى خدمات المصرف عبر قطع الاتصال بين المصرف والعميل ،أو تهكير و قرصنة المعلومات الظاهرة المتنامية الانتشار كظاهرة من بين عدة ظواهر تمس بأمن النظام المعلوماتي للأشخاص والدول وسائل الاتصال أو سرقة و تهكير IP وبذلك انتهاك سرية المراسلات والبيانات بين المصرف والعميل أو الحصول على بيانات ومعلومات وسرقتها ، بل أكثر من ذلك التحكم في العمليات المصرفية وإدارتها ، ولحماية للاتصالات الالكترونية تم إنشاء سلطة ضبط مستقلة للبريد والاتصالات الالكترونية تتمتع بالشخصية المعنوية و الاستقلال المالي تدعى "سلطة الضبط " ، مقرها الجزائر العاصمة تتولى مجموعة من المهام المذكورة في المادة 13 من هذا القانون تتم استشارتها من طرف الوزير المكلف بالبريد و الاتصالات الالكترونية بخصوص تحضير و اعتماد نصوص تنظيمية في هذا الشأن ، حيث تطرق الباب الثالث من هذا القانون إلى النظام القانوني للاتصالات الالكترونية واخضع إنشاء و استغلال شبكات الاتصالات الالكترونية المفتوحة للجمهور وتقديم هذه الخدمات إلى احترام شروط خصوصية البيانات والمعلومات التي يتم إيصالها بواسطة شبكات الاتصال الالكترونية ،وكذا شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي ، وحفاظا على سرية البيانات والمعاملات ألزم متعاملي الاتصالات الالكترونية باتخاذ التدابير التي من شانها أن تضمن سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم وعدم السماح باعتراض الاتصالات ومراقبتها إلا بعد إذن مسبق من السلطة القضائية ، كما عاقب على مجموعة من الأفعال المخالف للقواعد المنصوص عليها في هذا القانون في الباب الرابع المعنون بالأحكام الجزائية حيث عاقب بالحبس من سنة إلى خمس سنوات وغرامة من 500 ألف إلى مليون دينار جزائري كل شخص ينتهك سرية المراسلات عن طريق الاتصالات الالكترونية أو يفشي مضمونها أو ينشرها أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها ، ومن سنة إلى ثلاث سنوات وغرامة من 500 ألف إلى مليون دينار جزائري كل متعامل للاتصالات الالكترونية يحول المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الالكترونية ، و من خلال استقراء نصوص هذا القانون يظهر لنا محاولة المشرع الجزائري حماية الاتصالات الالكترونية إيمانا منه بضرورة محاربة جميع أشكال المساس بها عبر إصدار مجموعة من القوانين وإيجاد آليات قانونية و تقنية لحمايتها .

الفرع الثاني : المنظومة الوطنية لأمن الأنظمة المعلوماتية .

يسعى المشرع من خلال إصدار المرسوم رقم 20 /05 إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية ، حيث تشكل هذه المنظومة أداة للدولة في مجال امن الأنظمة المعلوماتية وتشكل الإطار التنظيمي لإعداد إستراتيجية وطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها ، موضوعة لدى وزارة الدفاع تظم مجلس وطني لأمن الأنظمة المعلوماتية مكلف بإعداد إستراتيجية وطنية لأمن المنظومات المعلوماتية،

ووكالة تقوم بتنسيق تنفيذ هذه الإستراتيجية ،يرأس المجلس الوطني وزير الدفاع أو ممثله ويظم عدة وزراء من عدة مجالات أما الوكالة فلها عدة مهام من أهمها إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السبيرانية التي تستهدف المؤسسات الوطنية ، وتعمل على جمع وتحليل المعطيات المتصلة بمجال امن المنظومات المعلوماتية لاستخلاص المعلومات التي تسمح بتامين منشات المؤسسات الوطنية ، كما تقوم بمساعدة الإدارات والمؤسسات الوطنية العامة والخاصة من اجل تامين أنظمتها المعلوماتية من الهجمات الالكترونية ومعالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية و القيام بنشاطات التكوين ،حيث سبق التطرق إلى كيفية عمل المصارف الالكترونية التي تقوم بتقديم خدمات عبر أنظمة معلوماتية لتبادل البيانات و المعلومات وتنفيذ أوامر الزبائن وتستعمل في ذلك وسائل الاتصال الحديثة ما يجعلها عرضة للجرائم الماسة بأمن أنظمتها المعلوماتية ، حيث يمكن أن تستفيد هذه البنوك من تجربة الوكالة في محاربة الجرائم الالكترونية و التعاون معها من اجل محاربة هذا الإجرام وإيجاد حلول لتقوية دفاعاتها الالكترونية من هذه الهجمات .

خاتمة:

يحاول المشرع الجزائري مجارات التطور الإجرامي في المجال الرقمي قدر الإمكان عبر منظومة قانونية وهيئات وسلطات تناط بها مهام توفير الحماية للعمليات الالكترونية بصفة عامة بما فيها العمليات المصرفية الرقمية، إلا أن طبيعة هذه الجرائم التقنية والمتطورة بشكل سريع وكون القانون يعالج ظواهر اجتماعية موجودة أو يمكن توقعها إلا أن هذا النوع من الإجرام الغير المتوقع فهو يتطور بتطور التكنولوجيا و بالرغم من محاولة المشرع جعل القوانين مرنة وعامة قدر الإمكان في هذا المجال من اجل إمكانية تطبيقها لأطول مدة ممكنة و إسقاطها واحتوائها لأكبر عدد من الجرائم الالكترونية وعلى رأسها تلك الماسة بالخدمات الالكترونية الرقمية ، إلا انه يلاحظ قصور هذه القوانين في توفير الحماية القانونية الفعالة والحقيقية لهذه العمليات لعدة أسباب وعوامل سواءا من خلال التجريم فاغلب هذه الأفعال غير مجرمة أو من خلال البحث والتحري في ظل نقص الخبرات و الوسائل التكنولوجية المتاحة والمتوفرة ، وكذا صعوبة إيجاد وضبط أدلة الإجرام الالكتروني وسهولة محوها وكون هذه الجرائم جرائم عبر وطنية تثير الكثير من الإشكالات و الصعوبات لمكافحتها و التغلب عليها حيث نقترح مجموعة من الاقتراحات كمحاولة لحل هذه الإشكالات وتتمثل الاقتراحات في الأتي:

_التكوين الجيد لضباط الشرطة القضائية في المجال التقني و القانوني في الجرائم المعلوماتية.

_تكوين قضاة متخصصين في الجرائم المعلوماتية بصفة عامة بما فيها جرائم المساس بالخدمات المصرفية الالكترونية.

_التعاون الدولي في مجال مكافحة الإجرام المتعلق بالعمليات المصرفية الرقمية.

_مراقبة مدى امن وسلامة أجهزة البنوك وبيانات الزبائن.

_إخضاع أنظمة المعالجة الآلية للبنوك لمجموعة من الاختبارات لمعرفة مدى سلامتها والحماية التقنية التي تتوفر عليها قبل منها الاعتماد.

_محاول جرد الأفعال والممارسات التي تهدد العمليات المصرفية الرقمية وتجريمها.

_تشديد العقوبة في هذا النوع من الجرائم.

_الاستفادة من الخبرات الأجنبية في هذا المجال لتكوين الإطارات الوطنية سواءا في المجال القانوني و التشريعي أو المجال التقني.

_ إبرام اكبر عدد من الاتفاقيات والمعاهدات في هذا المجال خاصة في ظل انتشار التجارة الالكترونية الدولية وتبادل المعلومات والبيانات في هذا المجال .

. قائمة المصادر و المراجع :

1المادة الأولى، من الأمر رقم 66/ 156 ، المؤرخ في 18صفر عام 1386الموافق ل 08يونيو سنة 1966، يتضمن قانون العقوبات ، ج ر49 الصادرة في 21صفر عام 1386الموافق ل 11يونيو سنة 1966.

_ Mohamed kahloula ,« les délit d accès ou de maintien frauduleuse dans un système de traitement automatise de donnes « , REVUES DES sciences juridiques , Administratives et politiques ,université de Tlemcen , no , 12, 2011, p101 .

_ المادة رقم 543 مكرر 23 من الأمر رقم 75/ 54 ، المؤرخ في20رمضان عام 1395الموافق ل26 سبتمبر سنة 1975، يتضمن القانون التجاري ، ج ر101 الصادرة في16 ذو الحجة عام1395 الموافق ل 19ديسمبر سنة 1975.

،المتضمن القانون التجاري ، مرجع سابق .75/54 من الأمر رقم 24مكرر 543_المادة رقم

،المتضمن قانون العقوبات ، مرجع سابق . 165/ 66 من الأمر رقم 350_ المادة رقم

- أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول ، دار هومة ، الجزائر ، ط 9 ، سنة 2008 ص 268.

_حابس يوسف زيدات ، مدى استيعاب النصوص التقليدية للسرقة الالكترونية دراسة مقارنة ،

مجلة مركز حكم القانون ومكافحة الفساد ، دار جامعة حمد بن خليفة للنشر ، الدوحة ،

04. ، ص09، المقال رقم 2019 العدد الثاني ، سنة

- حابس يوسف زيدات ، مدى استيعاب النصوص التقليدية للسرقة الالكترونية دراسة مقارنة ، مرجع سابق ، ص 05 .
- السيد العتيق ، جرائم الانترنت ، دار النهضة العربية ، القاهرة ، 2006 ، ص 91.
- محمد أمين الرومي ، جرائم الكمبيوتر و الانترنت ، دار المطبوعات الجامعية ، الإسكندرية 2004، ص 43.

_ حابس يوسف زيدات ، مدى استيعاب النصوص التقليدية للسرقة الالكترونية ، مرجع سابق .

- علي احمد عبد الله الزغبي ، حق الخصوصية في القانون الجزائي دراسة مقارنة ، الطبعة الأولى ، المؤسسة الحديثة للكتاب ، طرابلس ، سنة 2006 ، ص 125.
- محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة للنشر ، الإسكندرية 2007 ، ص 46.
- عبد العزيز سعد ، جرائم الاعتداء على الأموال العامة و الخاصة ، الطبعة الرابعة ، دار هومة للطباعة والنشر و التوزيع ، الجزائر ، 2007، ص 99.

، المتضمن قانون العقوبات ، المعدل 66/156مكرر من الأمر رقم 253إلى المادة 242_ المواد من المادة

،53، ج ر 1975يونيو سنة 01الموافق ل 1395جمادى الثانية عام 07المؤرخ في 75/47بالأمر رقم

، والمعدل والمتمم بالقانون 1975يونيو سنة 04 الموافق ل 1395 جمادى الثانية عام 24الصادرة في

، الصادرة في 84، ج ر 2006ديسمبر 20الموافق ل 1427 ذو القعدة عام 29المؤرخ في 06/23رقم

2006 . ديسمبر سنة 24الموافق ل 1427ذو الحجة عام 04

، يتضمن 2009غشت سنة 05الموافق ل 1430شعبان عام 14 ، المؤرخ في 09/04_ القانون رقم

،47القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها ، ج ر

2009 . غشت لسنة 16الموافق ل 1430شعبان عام 25الصادرة في

، مرجع سابق.04 / 09من القانون رقم 02_ المادة رقم

، المتضمن قانون العقوبات ، مرجع سابق .66/156 مكررمن الأمر رقم 394_ المادة رقم

، المتضمن قانون العقوبات، مرجع سابق.66/156 من الأمر رقم 394_ الفقرة الثانية، من المادة رقم

، ، مرجع سابق . 66/156من الأمر رقم 1مكرر 394_ المادة رقم

، مرجع سابق . 66/156من الأمر رقم 2مكرر 394 _المادة رقم

، المتضمن قانون العقوبات ، مرجع سابق . 66/156من الأمر رقم 5مكرر 394_ المادة رقم

، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا09/04 من القانون رقم 02_ المادة

الإعلام والاتصال ومكافحتها ، مرجع سابق.

، مرجع سابق .09/04من القانون رقم 02_ الفقرة الثانية من المادة رقم

، مرجع سابق . 04/ 09 من القانون رقم 02_ الفقرة جيم من المادة رقم

، مرجع سابق .09/04 من القانون رقم 02_ الفقرة واو من المادة رقم

، مرجع سابق.09/04من القانون رقم 04_الفقرة باء من المادة رقم

- طارق عفيف صادق احمد ، الجرائم الالكترونية جرائم الهاتف المحمول ، الطبعة الأولى ، المركز القومي للإصدارات القانونية ، القاهرة 2015 ، ص 149.

، مرجع سابق .09/04 من القانون رقم 14_ المادة رقم

،2015أكتوبر سنة 08الموافق ل 1436ذو الحجة عام 24المؤرخ في 15/261_ المرسوم الرئاسي رقم

يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام .2015أكتوبر سنة 08الموافق ل 1436ذو الحجة عام 24 ،الصادرة في 53ومكافحتها ، ج ر

، مرجع سابق .15/261 من المرسوم رقم 05_المادة رقم

، مرجع سابق .15/261 من المرسوم رقم 05_المادة رقم

، مرجع سابق .15/261 من المرسوم رقم 07_المادة رقم

، مرجع سابق .15/261 من المرسوم رقم 08_المادة رقم

- فتوح الشاذلي ، عفيفي كامل ، جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي ، الطبعة الأولى ، دار الفكر الجامعي ، منشورات الحلبي الحقوقية ، بيروت ، لبنان 2003 ، ص 32.

، مرجع سابق .15/261 من المرسوم رقم 11_المادة رقم

، مرجع سابق . 15/261 من المرسوم رقم 30 _المادة رقم

، 2018مايو 10الموافق ل 1439شعبان عام 24 ، المؤرخ في 18/04من القانون رقم 03 _ المادة رقم

شعبان عام27، الصادرة في 27يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية ، ج ر

2018 . مايو سنة 13الموافق ل 1439

، مرجع سابق .18/04 من القانون رقم 03_المادة رقم

، مرجع سابق . 18/04من القانون رقم 04_ المادة رقم

، مرجع سابق . 18/04من القانون رقم 11_ المادة رقم

، مرجع سابق .18/04_المادة الأولى من القانون رقم

، مرجع سابق .18/04_ المادة الأولى من القانون رقم

- LAURE zicry , enjeux et maitrise des cyber – risques, l'argus , édition ،2014، France ،p 23

.

، مرجع سابق .18/04من القانون رقم 11_ المادة رقم

، مرجع سابق .18/04من القانون رقم 14_المادة رقم

، مرجع سابق . 18/04من القانون رقم 97_ المادة رقم

، مرجع سابق . 18/04من القانون رقم 119_ المادة رقم

، مرجع سابق .18/04من القانون رقم 165_ المادة رقم

، مرجع سابق. 18/04من القانون رقم 177_ المادة رقم

الموافق ل1441جمادى الأولى عام 24 ، المؤرخ في 05/ 20الرئاسي _ المادة الثانية من المرسوم

الصادرة04 وطنية لأمن الأنظمة المعلوماتية ، ج ر ، يتعلق بوضع منظومة 2020 جانفي سنة 20

2020. جانفي سنة 26،الموافق ل 1441في أول جمادى الثانية عام

، مرجع سابق.20/05من المرسوم رقم 03_ المادة رقم

، مرجع سابق .20/05من المرسوم الرئاسي رقم 18_ المادة رقم