

جامعة عبد الحميد بن باديس مستغانم

المرجع:

كلية الحقوق والعلوم السياسية

قسم: قانون عام

مذكرة نهاية الدراسة لنيل شهادة الماستر

جريمة المساس بالأموال الإلكترونية

ميدان الحقوق والعلوم السياسية

التخصص: القانون الجنائي والعلوم الجنائية

تحت إشراف الأستاذة:

منوس سعاد

الشعبة: الحقوق

من إعداد الطالب:

عجال بلال

أعضاء لجنة المناقشة

رئيسا

بن عوالي علي

الأستاذة:

مشرفا مقرر

منوس سعاد

الأستاذة:

مناقشا

علاق نوال

الأستاذة:

السنة الجامعية: 2024/2023

تمت المناقشة يوم: 2024/06/24

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: عجلال بلال الصفة: طالِب جامعي

الحامل لبطاقة التعريف الوطنية رقم: 495101 والصادرة بتاريخ: 18/04/2013

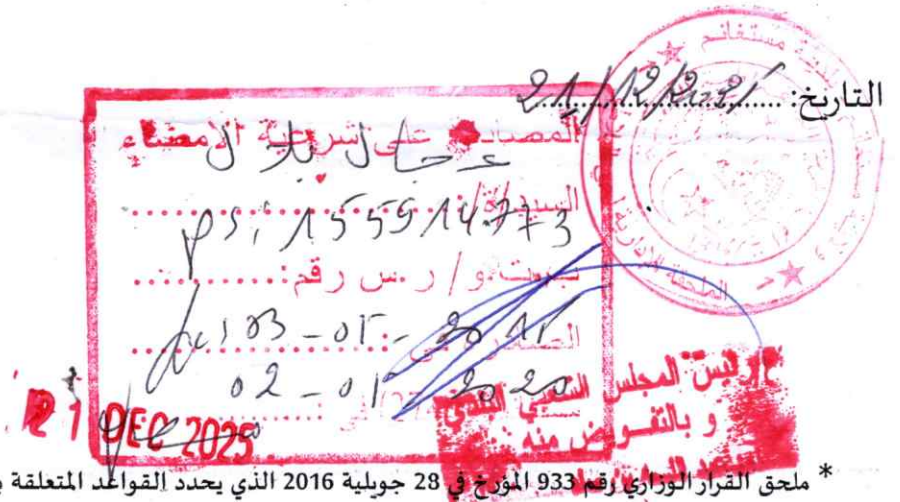
المسجل بكلية: حقوق و العلوم السياسية قسم: قانون عام

والمكلف بإنجاز مذكرة ماستر بعنوان:

جريمة الاحتيال بالائتمال الإلكتروني

أصرح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث المذكور أعلاه.

امضاء المعني



الإهداء

أهدي ثمرة جهدي وعملي المتواضع إلى أعز ما أملك، إلى من تحت قدميها الجنان،

إلى من دعواتها ترافقني الغالية "أمي"

وإلى كل عائلتي دون استثناء

وإلى من دعمني وكان لي خير السند

الشكر والعرفان

الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين، وبعد ..

فإني أشكر الله تعالى على فضله حيث أتاح لي إنجاز هذا العمل بفضله، فله الحمد أولاً وآخراً.

ثم أشكر أولئك الأخيار الذين مدوا لي يد المساعدة، خلال هذه الفترة، وفي مقدمتهم أستاذتي المشرفة على الرسالة فضيلة الأستاذة التي لم تدخر جهداً في مساعدتي، كما هي عادتھا مع كل طلبة العلم، فلها من الله الأجر ومني كل تقدير حفظه الله وتمتعه بالصحة والعافية ونفع بعلمه.

كما لا يفوتنا تقديم الشكر و الامتنان إلى كل أساتذة كلية الحقوق و العلوم السياسية لجامعة مستغانم وكل من تلقنا على أيديهم علما.

و في الأخير نتقدم بكلمة شكر و عرفان إلى من ساهم في إنجاز هذا العمل من قريب أو من بعيد ولو بكلمة تشجيعية

كما أتقدم بخالص الشكر و التقدير لأعضاء اللجنة المناقشة لتفضلهم بقبول مناقشة هذه المذكرة، وتقييمها و إبداء توجيهاتهم، رغم مشاغلهم العملية و العلمية فجزاهم الله عنا خير جزاء.

قائمة المختصرات:

ص: صفحة

ج.ر: الجريدة الرسمية

د.ط: دون طبعة

ط 1: طبعة الأولى

المقدمة

إن الثورة التكنولوجية تعد من أهم التطورات التي يعيشها العالم و بالأخص ثورة الاتصالات التي تعتبر المحرك الأساسي في التطورات الحادثة في الوقت الحالي إلا أنها ليست المحرك الوحيد فيها، حيث أن التطور الكبير في التكنولوجيا الحاسبات قد أسهم بصورة واضحة في تسارع معدلات التقدم في مجال الاتصال والمعلومات.

ومن خلال هذه الشبكة بدأ العالم بأسره يندمج مع بعضه البعض يشاهد ويتجاوز تدريجياً بدأ بتحرر من قيود المكان إلى أن أصبح العالم قرية صغيرة وهذا الفصل يرجع لشبكة الانترنت، كما نشأ مع هذا التطور العلمي للبشرية ما يسمى بالتجارة الالكترونية والتي توسع نشاطها عالمياً وزادت قيمة المبادلات النقدية الالكترونية فيها ونشأت عملة نقدية الكترونية.

وبغض النظر عن لكم الهائل من إيجابيات التطور التكنولوجي والمعلوماتي التي لا يمكن عده، إلا أنه في هذا الوسط نشأت بيئة مساعدة لتنامي الإجرام المالي، الذي أصبح يشكل خطر محقق يهدد الاقتصاد العالمي والوطني على حد سواء، كما أدى إلى تطور الجرائم المالية التقليدية التي أصبحت جرائم مالية إلكترونية لم تكن موجودة أو معروفة خاصة في المجتمع الجزائري.

فالجريمة الالكترونية من بين أخطر أنواع الإجرام الحديث في ظل الثورة التكنولوجية الرقمية الهائلة التي قزمت الألم بأسره، فهي جريمة تقنية نشأت في الخفاء وتوجه لنيل من الحق المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، وتظهر مدى خطورتها في الاعتداءات التي تمس الأموال المعلوماتية.

وتعتبر هذه الجرائم من أكثر الجرائم السيبرانية شيوعاً و تأثيراً في العصر الحديث، مما أدى لزيادة هذا النوع من الجرائم مؤخراً نظراً لسهولة ارتكابها، حيث أصبحت تغطي على معظم المعاملات التجارية سواء كانت معاملات بسيطة أو صفقات مالية كبيرة بهدف تحقيق الربح

السريع، وانتشرت بذلك مظاهر السرقة والنصب في المجال المعلوماتي وزادت المعاملات التجارية غير المشروعة التي تتم عن بعد، فهي تشير إلى أي نشاط غير قانوني يقوم بتنفيذه المجرمين بتصميم برامج خبيثة للوصول إلى بيانات المستخدمين المالية أو بجمع معلومات الدفع المالية باستخدام تقنيات الحوسبة وشبكة الانترنت.

ولهذا يعد موضوع جرائم المساس بالأموال الالكترونية من المواضيع المستحدثة والذي يرتبط وجودها بظهور التكنولوجيا المعلومات والحاسبات الآلية، ولعل أخطر المعاملات التي تمس المال الالكتروني وترتب آثار وخيمة على كل الأصعدة تتجسد في صورة تبيض الأموال باستخدام وسائط الكترونية.

والجزائر باعتبارها واحدة من الدول التي تعرضت لهذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا، فهي أيضا معينة بالتصدي لهذه الظاهرة ولهذا ألقى على عاتق المشرع الجزائري مسؤولية مواجهة هذه الجرائم في ظل قصور النصوص القانونية عن الإحاطة بها نظرا لخطورتها على الاقتصاد الوطني والدولي، وقد بات من الضروري إيجاد حلول مناسبة لسد الفراغ القانوني انطلاقا من تحديد الأحكام الموضوعية لقيام هذه الجرائم ووضع مجموعة من الإجراءات فيها ما يعتبر قاسم مشترك بين الجرائم التقليدية والجرائم المستحدثة ومنها ما يختص بالجرائم التقليدية والجرائم المستحدثة ومنها ما يختص بالجرائم المستحدثة ومنها ما يختص بالجرائم الخطيرة فقط، ومن بينها الجرائم الماسة بالأموال الالكترونية.

حيث تكمن أهمية هذه الدراسة كونه يحظى باهتمام العديد من دول العالم انطلاقا من الخطورة الإجرامية لهذه الجريمة التي أضحت تؤثر على أمن واقتصاد مختلف دول العالم، بالإضافة إلى صعوبة حصر هذا النوع من الجرائم التقليدية والتقنية الحديثة، وشخصية مرتكبيها التي تثير الفضول والانبهار ونوع العقاب المطبق على الأيادي الناعمة شديدة الذكاء والآثار الرهيبة التي تتركها، ونظرا لخطورة هذه الجرائم حاليا على أمن المجتمع والتي تنبئ بنشوب جيل على مستوى عالي من الإجرام، كان لازما على التشريعات الوطنية

تكيف نصوصها القانونية وسبل لمكافحتها وحماية الأموال الالكترونية من النصب مع ما يتماشى مع هذه الجرائم المستحدثة.

وعليه فإن موضوع بحثنا هذا "جرائم المساس بالأموال الالكترونية جدير بالدراسة والاهتمام بتفاصيله وتسليط الضوء عليه من أجل توعية الأشخاص والشركات التجارية وغيرهم سواء من الطالب الباحث أو من المشرع الجزائري، إذ أنه قد ال تنطبق النصوص القانونية التي تنظم الجرائم التقليدية على الجرائم ذات الطابع الافتراضي.

❖ وقد تجلت أسباب اختيارنا لهذا الموضوع كونه موضوع العصر فما يخص الإجراء السيبراني إلى جانب آثاره الوخيمة على المجتمع المحلي أو الدولي، فهو الكتروني خفي من مجرم خبير بالتقنية تمس المعطيات الآلية على المستوى شبكة الإنترنت، فهناك أسباب ذاتية وأخرى موضوعية، أما الأولى فتعود أساسا إلى رغبتنا الشخصية في دراسة الجرائم المعلوماتية وميولنا للبحث فيها، وأما الموضوعية فتعود إلى حيوية الموضوع وحداثه وامتداد تأثيره إلى جميع الأصعدة لارتباطه بالتطور التكنولوجي الذي أصبحنا نعتمد عليه في حياتنا اليومية بالإضافة إلى ما ينتج عليه من جرائم إلكترونية واقعة على الأموال، وتسليط الضوء على الدور الذي يلعبه المشرع الجزائري في مواجهة خطورة هذه الجريمة.

❖ تهدف دراسة هذا الموضوع في التعرف أكثر على الآليات المعتمدة لمكافحة الجريمة الماسة بالأموال الالكترونية.

❖ لقد تطرقنا إلى عدة دراسات سابقة على الجرائم الالكترونية بصفة عامة ومفصلة، دون التطرق إلى هذا النوع من الجرائم الاعتداء على الأموال الالكترونية بشكل عام، إلا أن هذا لا يمنع من الاعتماد على العديد من الدراسات التي تضمنت ثناياها عقوبات جزائية عن موضوعنا هذا ومن أهمها:

❖ أطروحة دكتوراه للطالب حنيف جمال التي جاءت بعنوان جرائم المعلوماتية الواقعة على الأموال والذي بدء دراسته بباب أول تناول فيه مدى تأثير المعلوماتية.

على المعنى والتقسيم التقليديين للأموال وحمايتها الجنائية، والملاحظ أن هذه الرسالة هي الوحيدة التي تناولت موضوع دراستنا بشكل موسع من جهة النظر الخاصة بالطالب.

❖ أما المشاكل والصعوبات التي واجهتنا في بحثنا هذا تمثلت في قلة الأبحاث حول موضوع جرائم المساس بالأموال الالكترونية كونها جريمة مستحدثة ولدراسة موضوع الجرائم الماسة بالأموال الالكترونية اعتمدنا على عدة مناهج ممثلة في:

❖ المنهج الوصفي: من خلال دراسة ووصف الجريمة الالكترونية.

❖ المنهج التحليلي: من خلال تحليل هذه الجريمة والتعرف على أنواعها وأهدافها، وذلك للوصول لمعالجة المسؤولية الجنائية عن الجريمة المعلوماتية في التشريع الجزائري.

❖ وبناءا على ما سبق نقترح الإشكالية التالية:

- ما مدى نجاعة المشرع الجزائري في التصدي لهذا النوع من الجرائم؟

❖ وعليه يمكن طرح التساؤلات التالية:

- ما المقصود بالجرائم الماسة بالأموال الالكترونية؟

- ما هي الطبيعة القانونية للجرائم الواقعة على الأموال الالكترونية؟

- فيما تتمثل الجرائم الماسة بالأموال الالكترونية؟

- ما هي أبرز الآليات التي انتهجت لمواجهة هذا النوع من الجرائم؟

وللإجابة على هذه الإشكالات تطرقنا للخطة المتمثلة في فصلين ومبحثين وفي كل مبحث مطلبين، في الفصل الأول تناولنا الإطار المفاهيمي لجريمة المساس بالأموال الالكترونية، بحيث تطرقنا في المبحث الثاني الطبيعة القانونية للجرائم الماسة بالأموال الالكترونية.

أما الفصل الثاني فخصصته للجريمة الالكترونية في التشريع الجزائري وفي المبحث الأول نظرة
المشرع الجزائري للجريمة الالكترونية، والمبحث الثاني آليات مكافحة ومعالجة جريمة المساس
بالأموال الالكترونية.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال

الالكترونية

المبحث الأول: ماهية جريمة المساس بالأموال الالكترونية

المبحث الثاني: الطبيعة القانونية للجرائم الماسة بالأموال الإلكترونية و

أنواعها

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

يشهد السنوات الأخيرة من نهاية القرن العشرين وبداية القرن الواحد و العشرين تسارع مذهل للتقدم التكنولوجي و التقني، وقد طال هذا التأثير إلى ارتقاء مستوى الجريمة من جريمة تقليدية تتم بوسائل بسيطة إلى جريمة تقنية تعتمد على وسائل حديثة ومتطورة ودقيقة، أصبحت تعرف بالجريمة الإلكترونية.

كما أن الجرائم المعلوماتية هي أعظم ويلات هذا القرن إذ أصبحت واقعا مفرعا للدول و الأفراد ويعود ذلك أساساً إلى الإمكانيات المتاحة للمجرم الإلكتروني ذلك بتقدم وسائل الاتصال و المعلومات وذيوع استعمال الحاسوب وسهولة استخدام الانترنت فبالتخفي خلف شاشاتهم يستطيع صناعة ونشر الفيروسات، الاختراق، تعطيل الأجهزة،...إلخ، وعليه قسمنا هذا الفصل إلى مبحثين و مطلبين، سندرس في المبحث الأول ماهية الجريمة الإلكترونية،

وفي المبحث الثاني الطبيعة القانونية للجرائم الواقعة على الأموال الإلكترونية و أنواعها.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

المبحث الأول: ماهية الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية ظاهرة إجرامية جديدة ومستجدة، تدق ناقوس الخطر وتنبه مجتمعات العصر الراهن بحجم المخاطر وهول الخسائر الناجمة عن الجريمة الإلكترونية بدلالاتها الواسعة، فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكيا يمتلكون أدوات المعرفة التقنية¹.

سوف نتطرق في هذا المبحث إلى مفهوم وأنواع وخصائص الجريمة الإلكترونية.

المطلب الأول: مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية جريمة مستحدثة، ويطلق عليها بالغش المعلوماتي فهي استخدام غير مشروع لتقنية معلوماتية، بهدف الاعتداء على الأموال أو الأشياء المعنوية، يستخدم فيها جهاز كمبيوتر، يظهر من جراء ذلك جرائم الإنترنت والاعتداء على الشبكات المعلوماتية للهيئات الخاصة والعامة، لذلك لا بد لنا من فهم ما هو المقصود بالجرائم الإلكترونية وما هي أنواعها وصورها ومعرفة خصائصها لكونها تختلف عن الجرائم التقليدية².

الفرع الأول: التعريف للجريمة الإلكترونية

أولاً: التعريف الضيق للجريمة الإلكترونية:

إن مسألة وضع تعريف للجريمة الإلكترونية كانت محلاً لاجتهاد الفقهاء، لذا لا يوجد تعريف متفق عليه للفقهاء القانون نتيجة اختلاف المصطلح المستخدم ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من

¹ - شفيق حسنين، الإعلام الجديدة والجرائم الإلكترونية، دار الفكر وفن للطباعة والنشر والتوزيع، (د.ط.)، (د.ب.ن)، 2015، ص10.

² - إيمان بغدادى، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، كلية الحقوق، جامعة قسنطينة، مجلة أفاق للبحوث والدراسات سداسية، العدد 04، جوان 2019، ص185.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

المعدات الرقمية، وتعرف الجرائم الإلكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال حيث هناك من يعرفها بأنها: "الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات"¹.

1) أهم التعريفات التي استندت على موضوع الجريمة:

إن الفقهاء أصحاب هذا الاتجاه الفقهي شملوا تركيزهم على الجانب الموضوعي في تعريف الجريمة الإلكترونية باعتبار أن هذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها بل تقع على الحاسب الآلي أو في داخل نظامه.

و عليه تم تعريف الجريمة الإلكترونية من قبل أنصار هذا الاتجاه بأنها "نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه" وعرفوها أيضا أنها " غش معلوماتي ينصرف إلى سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها"².

¹ - حدي نسيم، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2013/2014، ص8.

² - عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، دامعة الكوفة، كلية القانون، العدد السابع، 2008، ص 118.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

(2) التعريف الذي يستند على وسيلة ارتكاب الجريمة:

ذهب أنصار هذا الاتجاه وفقا لهذا المعيار على أساس أداة الجريمة، إذ يشترطون وجوب ارتكابها بواسطة الحاسوب، وبالتالي عرفها الفقيه توم فوريستر في مؤلفه ثورة تقنية المعلومات على أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"¹.

و عرفها الفقيه MERWE الجريمة الالكترونية بأنها: " الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه"².

ويعرفها الفقيه TIEDEMAN بأنها: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"

وكذلك تعرف بأنها: " الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسا" وأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" يعتبر هذا التعريف الأخير الرأي الراجح لتبنيه من قبل العديد من الباحثين و الدارسين نظرا لشموليته بحيث يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية³.

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: " الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا". وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي و التنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983، من أنها: " كل سلوك غير مشروع، أو غير

¹ جمال الدين بوقرة، جمال الدين عنان، (القطب الجزائري لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)، مجلة الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01 جوان 2022، ص1679.

² غنية باطلي، الجريمة الالكترونية، دار الجزائرية للنشر والتوزيع، (د.ط)، بيروت، 2015، ص5.

³ فضيلة عاقل، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الالكترونية"، طرابلس، بتاريخ 24-24 مارس 2017، ص118.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها"، وهو تعريف تبنى أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أو نقلها¹.

كما يعرفها خبراء منظمة التعاون الاقتصادي والتنمية OECD بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" ويعرفها الفقيه الفرنسي VIVANT بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب"².

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين المنعقد في فيينا سنة 2000 تعريف الجريمة الإلكترونية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الإلكترونية.

أما التعريف الدولي للجريمة الإلكترونية فهو يعتمد في الغالب على الغرض من استخدام المصطلح فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر³.

¹ - ياسمين بونعارة، الجريمة الإلكترونية، مجلة المعيار لكلية أصول الدين، جامعة الأمير عبد القادر، 2015/06/19، العدد 39، ص 4.

² - محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، الجزء الثاني، وزارة الداخلية "الأكاديمية الملكية للشرطة"، البحرين، مارس 2010، ص 02.

³ - د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018، ص 352.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

3) التعريف الذي يستند على توافر المعرفة التقنية لدى الجاني:

يستند أنصار هذا الاتجاه في تعريف الجريمة الإلكترونية إلى المعيار الشخصي، الذي يستلزم أن يكون فاعل هذه الجرائم ملماً بتقنية المعلومات.

كما عرفها الفقيه THOMSON DAVID بأنها: أي جريمة يتطلب لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسوب¹.

عرفها كذلك بعض من الفقه على أنها: " ذلك النوع من الجرائم التي تتطلب إماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"².

يستلزم حسب أنصار هذا الاتجاه، لتعريف الجريمة الإلكترونية توافر سمات شخصية لدى مرتكبيها، ولقد حصروها أساسا في الدراية والمعرفة التقنية، لكن هذا المعيار لا يستند على أساس علمي أو منطقي، إذ صحيح أن من خصائص المجرم المعلوماتي المعرفة التقنية في علم الحاسوب، إلا أنها ليست شرطا لازما أو ملازما للجريمة الإلكترونية، والكثير من الجرائم المرتبطة بالحاسوب والمعلوماتية لا تتطلب معرفة تقنية عالية لارتكابها³.

ثانيا: التعريف الموسع للجريمة الإلكترونية:

يذهب أنصار هذا الاتجاه من الفقهاء، على عكس الاتجاه الأول، من الضروري التوسع في مفهوم الجريمة الإلكترونية، ويختلف موقفهم حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها هذه الجريمة.

¹ - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار النشر والتوزيع، ط1، عمان، 2011، ص 30.

² - بن عميروش ريمة، (عن خصوصية الجريمة المعلوماتية)، مجلة الفقه القانوني والسياسي، المجلد 02، العدد 02، ديسمبر 2020، ص 76.

³ - عبد الإله النوايسه، جرائم تكنولوجيا المعلومات، دار وائل للنشر و التوزيع، ط1، الأردن، 2017، ص44.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

يرى الفقيهان CREDO , MICEL بأن الجريمة الإلكترونية تشمل استخدام الحاسب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته¹.

عرفها أيضا الخبير الأمريكي PARKER الجريمة الإلكترونية بأنها: "كل فعل إجرامي متعمد أي كان صلة بالمعلوماتية، ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"².

كذلك يعرف الأستاذ LESTANC , VIVANT الجريمة الإلكترونية بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية، التي يمكن أن تكون جديرة بالعقاب".

تناول رأي آخر من الفقه تعريف الجريمة الإلكترونية أنها: "كل سلوك سلبي أو إيجابي، يتم بموجب الاعتداء على البرامج أو المعلومات، للاستفادة منها بأية صورة كانت"³.

المنظمة الأوروبية للتعاون والتنمية الاقتصادية عرفت على أنها: "كل عمل أو امتناع بأثمه الإنسان أضرارا بمكونات الحاسب الآلي المادية و المعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها"⁴.

عمل الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"⁵.

1 - يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016-2017، ص11.

2 - محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة والتوزيع، ط1، عمان، 2009، ص08.

3 - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط2، عمان، 2010، ص49.

4 - غنية باطلي، المرجع السابق، ص19.

5 - نيا ب سليمة، بوترة بلال، الجريمة الإلكترونية الأسس والمفاهيم، مجلة تطور العلوم، المجلد 13، العدد01، الجزائر، جامعة زيان عاشور، الجلفة، 2020، ص 10.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

و أجمع الدكتور عبد الفتاح بيومي حجازي من تعريفه للجريمة الإلكترونية، "جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات".

ثالثا: التعريف القانوني للجريمة الإلكترونية

أغفل المشرع الجزائري وإلى وقت قريب تنظيم مجال الجريمة الإلكترونية قانونا، إلا أنه تدارك ذلك الفراغ من خلال سن قواعد قانونية لمواجهة هذه الجريمة¹، على خلاف المشرع الفرنسي الذي لم يعطي تعريفا للجريمة الإلكترونية فإن المشرع الجزائري استخدم للدلالة على الجريمة الإلكترونية في البداية مصطلح " جرائم المساس بأنظمة المعالجة الآلية للمعطيات" وذلك بعد استحداثها بموجب القانون 04-15 المعدل و المتمم للأمر 66-156 المتضمن قانون العقوبات، ثم بعد ذلك استعمل مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال"، وذلك بموجب قانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث عرفها في المادة 02 منه منا يلي: "الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

يلاحظ على هذا التعريف أن المشرع الجزائري قد اعتمد على جمع بين عدة معايير لتعريف الجريمة الإلكترونية، أولها معيار وسيلة الجريمة وهي منظومة المعلوماتية أو نظام للاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة وهو مساس بأنظمة المعالجة الآلية

¹ - يرمش مراد، خصوصية الجريمة الإلكترونية، أطروحة دكتوراه علوم في القانون الخاص، تخصص الملكية الفكرية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2020-2021، ص24.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

للمعطيات، فمن خلال النص القانوني المذكور نجد أن المشرع قد أحال إلى قانون العقوبات، وبالتالي كل الأفعال المجرمة في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات تشكل موضوعا للجريمة الإلكترونية، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات، كما حدد المشرع نطاق الجريمة الإلكترونية وذلك من خلال إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق الجرائم الإلكترونية في القانون الجزائري¹.

بعد تطرقنا للتعريف الفقهي و القانوني الذي طرحه المشرع الجزائري يمكن القول أن الجريمة الإلكترونية أو المعلوماتية هي سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته، يمس بالأشخاص أو الأموال أو أمن الدولة، وهو ما يبرر تجريم هذا السلوك وتقرير العقوبات المناسبة له.

الفرع الثاني: تعريف المال المعلوماتي

أولاً: تعريف المال المعلوماتي

المال المعلوماتي، هو كل ما يصلح أن يكون محلاً للحق ذو القيمة المالية، والشئ هو محل الحق وتقسم الأشياء إلى أشياء مادية وأشياء غير مادية أو معنوية، علماً بأن جرائم الأموال من وجهة النظر التقليدية لا ترد إلا على أشياء مادية، ولهذا كان تعريف المال بصدد جرائم الأموال بأنه: "كل شيء يصلح لأن يكون محلاً لحق من الحقوق المالية"².

¹ - نمذلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017، ص 100.

² - أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، حق الملكية، الجزء الثاني، دار إحياء التراث العربي، بيروت، 1952، ص 09.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

فالحاسوب بكل مكوناته هو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب، ويتكون من كيانات مادي وكيان معنوي، يضم الكيان المادي HARDWAR الأجهزة المادية المختلفة، وهي جهاز الإدخال وجهاز الإخراج ووحدات التشغيل المركزية، التي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها وجميع الأجهزة الملحقة بها، أما الكيان المعنوي SOFTWARE فيشمل البرامج المختلفة التي يتحقق من خلالها قيام الحاسب الآلي بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها¹.

كما أنه قد ازداد عدد الأشياء المعنوية مع التطور، وتفق بعضنا من حيث قيمتها على الأشياء المادية مما استدعى البحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يتمكن إسباغ صفة المال على الشيء المعنوي، ومن الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسوب الآلي، والتي تكون عادة مثبتة على دعامة أو حامل SUPPORT مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى أو أي مادة أخرى، إلا أن البرنامج مستقل عن دعامته فلا جدال في أنه شيء معنوي وبالتالي لا يصدق عليه وصف المال طبقاً للتحديد التقليدي للأموال الذي يشترط أن يكون محله شيئاً مادياً².

وعليه إذا سجل البرنامج أو نقش على دعامة فإن هذه الدعامة بما عليها من برامج تصلح لأن تكون محلاً لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرنامج تعتبر ضئيلة القيمة إذا ما قيست بقيمة البرامج، كما أن الاعتداء عليها ليس غاية في ذاته وإنما الباعث على ذلك هو البرنامج نفسه لا دعامته، ومع ذلك لا تأثير لهذه البواعث في القانون

¹ - محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، (د.ط)، القاهرة، 1994، ص217.

² - سفيان سوبر، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010/2011، ص51.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الجنائي¹، ومن ثمة إذا وقع الاعتداء على البرنامج مستقلا عن دعامته، فإن الأمر يكون قد وقع على شيء معنوي، هذا الشيء المعنوي لابد وأن تثبت له صفة المال أولا حتى يتمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه².

ثار جدال حول ما إذا كانت المعلومات صالحة لأن تكون محلا لجرائم الأموال أو لا، وانقسم الفقه في هذا الشأن اتجاهاين:

أولا: الفقه المعارض لإضفاء صفة المال على الأشياء المعلوماتية المعنوية:

رفض هذا الاتجاه إعطاء للأشياء المعلوماتية غير المادية (المعنوية) المال على أساس أن النبضات الإلكترونية والإرشادات الإلكترونية الممغنطة الني تتكون منها لا تعد من قبيل الأشياء المحسوسة، وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للكلمة ولذا لا يمكن اعتبارها من الأموال، ليس هذا فحسب بل لقد نفى هؤلاء أيضا صفة المنقول عن الأشياء المعلوماتية المعنوية، إذ طالما أنها ليست أشياء محسوسة فإنه لا يتصور قياسها أو حيازتها أو نقلها³.

وعليه ووفقا لهذا الرأي فإن المعلومات إذا لم تعالج أليا في صورة نبضات إلكترونية عن طريق الحاسب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية.

ثانيا: الفقه المؤيد لإضفاء صفة المال على الأشياء المعلوماتية المعنوية: إذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الاعتراف لها بصفة المال، فإن الفقه الحديث يرى على العكس أم المعيار في اعتبار الشيء ما ليس على أساس ماله من كيان مادي، وإنما أساس

¹ - علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، (د.ط)، بيروت، 1999، ص7.

² - سفيان سوير، المرجع السابق، ص52.

³ - جمال خفيف، جرائم المعلوماتية الواقعة على الأموال، أطروحة لنيل شهادة الدكتوراه، تخصص القانون، كلية الحقوق، جامعة الجزائر 01، 2016-2017، ص165.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

قيمتها الاقتصادية المستحدثة¹، إذ بمقدور مالك المعلومات أن يقوم بطرحها في الأسواق للتداول لبيعها أو تأجيرها أو غير ذلك من المعاملات التجارية طالما أنها ليست محظورة للتداول، كذلك بمقدوره تخزينها أو حفظها أو نقلها²، فهي صادرة عن صاحبها، أي أنها ترتبط بشخصيته وهو الذي فكر فيها، أو أنها من الحقوق اللصيقة بشخصية صاحبها.

تعد من قبيل خصائص هذه المعلومات، القابلية للانتقال، وهذا يعني أن هناك طرفا آخر، يستقبل هذه المعلومات باعتبارها نتاجا ذهنيا لمن يعطيها شكل المعلومة فهي تعد محور العلاقات مثل تلك التي تنشأ بين المالك وبين من يملك هذه المعلومات، ومن أمثلة هذه المعلومات برامج الحاسب الآلي، إذ أن هذه البرامج ترتب حقوقا لصاحبها وتخول له إبرام عقود متعلقة بها مثل الإيجار والبيع والحفظ وأي صورة أخرى من صور الاستغلال³.

في الأخير يمكننا القول، أن اعتبار المعلومات مالا قابل للتملك أو الاستغلال كما سبق توضيحه، يزيل عقبة كبيرة تسمح بإضافة هذا النوع من الأموال إلى مجموعة الأموال التي يحميها القانون الجنائي. وبالتالي، إن هذا المال يمكن أن يكون موضوع جرائم الاعتداء على الأموال، وهو ما يؤدي إلى إمكانية إسباغ حماية النصوص التقليدية عليه، كون أن هذه النصوص جاءت عامة ولم يشترط أن تقع جرائم الأموال على منقول مادي، أو يخضع للنصوص الخاصة حسب كل حالة⁴.

1 - أمال قارة، الحماية الجزائرية المعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر، (د.ط)، الجزائر، 2006، ص18.

2 - جمال خفيف، المرجع السابق، ص165.

3 - عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، 2009، ص 465-466.

4 - جفال أسماء وبوشنب ريان، الجرائم الالكترونية الواقعة على الأموال، مذكرة مقدمة لنيل شهادة الماستر علوم في القانون الخاص، تخصص قوانين أعمال، كلية الحقوق والعلوم السياسية بودواو، جامعة أمحمد بوقرة، بومرداس، 2022-2023، ص 18.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

ثانياً: صور المال الإلكتروني

للأموال الإلكترونية صور عديدة وذلك بحسب المادة محل الاختزال وبحسب آلية الدفع، فمنها بطاقات الدفع ومنها بطاقات السحب وغيرها، ولعل أهم هذه البطاقات هي:

أ- بطاقات تحمل رقمها:

وهي بطاقات مصنوعة من مادة خاصة ومزودة بشريط ممغنط يتضمن بيانات معالجة بواسطة الحاسوب تخزن عليها قيم مالية معينة بواسطة أجهزة خاصة وتحدد قيمتها بما يتم تخزينه من مقابل، وبالتالي فإن آلية شحن هذه البطاقة يتمثل بتحويل قيمة النقود المدفوعة إلى مادة مختزلة على الشريط الممغنط بصورة تحقق ذات الغاية من النقود.

ومن صور هذه البطاقات البطاقة الذكية¹ (Smart Card) ويتم التعامل بهذه البطاقة بتقديمها إلى البائع الذي يتولى تمريرها على جهاز خاص يقوم بقراءة البطاقة والتوقيع الرقمي وبمجرد قراءة الجهاز لهذه البطاقة فإنه بالإمكان الوفاء بقيمة البضاعة بخصمها مباشرة من القيمة المخزنة عليها. لذلك فلا حاجة للكشف عن مستخدم هذه البطاقة غلاف البطاقات الأخرى.

ب- بطاقات الائتمان:

هذه البطاقات تختلف عن سابقتها بأنها لا تحمل في ذاتها قيمة نقدية، وإنما تمنح حامل هذه البطاقة ائتماناً بحدود معينة، تمكن العميل التسوق حتى بحالة عدم وجود رصيد

¹ - تاريخياً: اخترعت البطاقة الذكية عام 1974 وبأ استخدامها سنة 1981 من قبل شركة فيليبس ثم أخذت في الانتشار، حيث أصبحت الذكية في بريطانيا بعد عام 1995 ممثلة لكل أنواع العملات الإنجليزية، ولمزيد من التفصيل ينظر/ علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكتروني، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان 2011، ص67.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

كاف له مقابل التزام من قبل البنك ومصدر لإستحقاق هذا المبلغ مقابل عمولة معينة وهي بعدة أنواع منها:

- **بطاقة الخصم الشهري:** أو ما يطلق عليه بطاقة الوفاء المؤجل، وهي بطاقة تمكن حاملها من استخدامها في تسوقه اليومي أو للسحب النقدي دون أن يكون لدى حاملها حساب جاري لدى مصدر البطاقة على أن يقوم مستخدمها بتسديد قيمة مشترياته خلال فترة إمهال تحت طائلة احتساب فوائد شهرية عن التأخير وبالتالي فهي أداة وفاء وائتمان معا¹.

- **بطاقة الائتمان الفرضية:** ومن خلالها لا يلتزم العميل بدفع المبلغ دفعة واحدة وإنما يتم على دفعات حسب الاتفاق، وهذا النوع من البطاقات أكثر ترتيباً للفوائد، وبالتالي لا تحتوي هذه البطاقة قيمة معينة وإنما تمكن العميل من استخدامها للشراء مع منحه مهلة لتسديد قيمة مشترياته.

- **بطاقات السحب الآلي:** هذا النوع من البطاقات يمكن العميل من الدخول إلى حسابه بواسطة أجهزة طرفية والقيام بعمليات السحب أو الإيداع من هذا الحساب.

وهذه البطاقات لا تحتوي قيمة نقدية وإنما تمكن العميل من الولوج إلى حسابه المودع لدى مصدر البطاقة والسحب منه أو الإيداع، حتى أن حاملها لا يلزمهم الذهاب إلى المصارف التي فيه حساباتهم لإجراء ذلك².

¹ - جلال محمد الزعبي وأسامة أحمد المناعة، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، 2010، ص102.

² - محمد حماد مرهج الهيبي، الحماية الجنائية لبطاقة الائتمان الممغنطة، دون طبعة، دار الكتب القانونية، 2014، ص43.

المطلب الثاني: خصائص الجريمة الإلكترونية و أركانها

المجرم الذي يرتكب الجريمة المعلوماتية يطلق عليه تسمية المجرم الإلكتروني أو المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، (المجرم التقليدي)، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب، ومن يرتكبها عادة يكون من ذو الاختصاص أو الخبرة في المجال المعلوماتي أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت¹.

مما لا شك فيه مما سبق أن الجرائم الإلكترونية تتسم بخصائص معينة عن الجرائم التقليدية، إلا أن هذا الأخير لا يعني عدم وجود تشابه بين الجرائم الإلكترونية والجرائم التقليدية، فهي تشترك بوجود الفعل غير المشروع والمجرم يقوم بهذا الفعل، من خلال هذا التشابه سوف نتطرق في مطلبنا هذا إلى خصائص الجريمة الإلكترونية في الفرع الأول، والأركان التي تقوم عليها الجريمة الإلكترونية في الفرع الثاني:

الفرع الأول: خصائص الجريمة الإلكترونية

مما لا شك فيه أن الجرائم المعلوماتية تختلف عن الجرائم التقليدية من ناحية الأفعال الإجرامية ومن تم ليس من المستغرب أن تختلف عنها في بعض الصفات التي تميزها عن غيرها من الجرائم بخلاف الصفات التي تطابق صفات الجرائم الأخرى.

¹ - نهلا عبد القادر المومن، المرجع السابق، ص 58 - 57.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

سنحاول من خلال هذا الفرع بيان خصائص الجريمة الإلكترونية، وذلك بالتطرق للسمات الخاصة بالجريمة الإلكترونية ، ثم السمات الخاصة بمرتكبيها أو ما يسمى بالمجرم المعلوماتي.

أولاً: السمات الخاصة بالجريمة الإلكترونية

تتميز الجريمة الإلكترونية بمجموعة من الخصائص تنفرد بها عن أغلب الجرائم التقليدية يمكن إجمالها فيما يلي:

1. الجريمة الإلكترونية العابرة للحدود الدولية: الجريمة الإلكترونية تتصف بالطابع دولي، أي أنها عابرة للحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، كما، ينتج عنه صعوبات سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية¹.

يدعو بعض الباحثين الجريمة الإلكترونية بأنها خمر معتق في قوارير جديدة² خاصة، حيث تقع في العالم الافتراضي انطلاقاً من حاسوب أو جهاز ذكي (هاتف محمول أو لوح الإلكتروني)، من مكان تواجد الجاني في دولة ما على محل جريمة في دولة ثانية أو دول متعددة، متجاوزاً بذلك الحدود الجغرافية التي لم يصبح لها وجود بظهور الشبكة العنكبوتية العالمية (الانترنت) التي جعلت العالم قرية صغيرة ولم تعد الحدود حاجزاً في نقل وتبادل كميات هائلة من المعلومات بين الحواسيب والأنظمة المعلوماتية المنتشرة في نقل وتبادل كميات هائلة من المعلومات بين الحواسيب والأنظمة المعلوماتية المنتشرة في مختلف أقطار العالم المتباعدة، لأنها تقع في عالم افتراضي واتصالها بعالم الانترنت و تقنية المعلومات فيسهل الاتصال بين حواسيب لا حصر لها في عدة دول. الجرائم

1 - د. بوضياف إسمهان، المرجع السابق، ص 355.

2 - عادل عزام سقف الحيط، جرائم الدم والقذح والتحجير المرتكبة عبر الوسائط الإلكترونية، شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات، دار الثقافة للنشر والتوزيع، 2019، ص 188.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الإلكترونية ترتكب عن بعد فيرتكبها شخص جالس أمام شاشة الكمبيوتر ببلد ولا يكون في مسرح الجريمة، كما قد تتضرر عدة دول وفي آن واحد بهذه الجريمة حيث يتواجد الأشخاص والأموال المستهدفة، كما قد يكون الجاني والضحية في البلد أو المجني عليه في بلد.

كما أن الجريمة الإلكترونية الواحدة قد تمس ضحايا في بلدان مختلفة في وقت واحد خاصة في ظل إزالة الحدود الاقتصادية بفضل انتشار التجارة الإلكترونية التي أزلت الحواجز الجمركية، وسمحت بسهولة انتقال ورؤوس الأموال وعالمية الجريمة الإلكترونية خلق إشكالات فيما يخص القانون الواجب التطبيق، كون التخطيط يكون في بلد والتنفيذ في بلد آخر والضحية في بلد آخر من جهة، ومن جهة أخرى مشكل¹ تسليم المجرمين المعلوماتيين هذا ما يؤدي إلى ضرورة وجود تعاون دولي في تبادل المعلومات وتسليم المجرمين عن طريق إبرام اتفاقيات وفي تسليم الأدلة والجناة وحتى التعاون في التحقيق...

إن الجريمة الإلكترونية لا تعترف بالحدود بين الدول والقارات ولذلك فهي جريمة عابرة للقارات، فهي تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل: جرائم التعدي على قواعد البيانات، تزوير و إتلاف المستندات الإلكترونية، الاحتيال المعلوماتي، سرقة بطاقات الائتمان، القرصنة، وغسيل الأموال².

2. الجريمة الإلكترونية صعبة الاكتشاف: من بين أهم خصائص الجريمة الإلكترونية أنها صعبة الاكتشاف، فهي تتم في عالم رقمي مجرد بواسطة رموز لا يترك أثرا مثل الجريمة التقليدية سواء بصمات أو أثر للحمض النووي أو غيره، مم يصعب عمل

1 - طارق عفيفي صادق أحمد، الجرائم الإلكترونية جرائم الهاتف المحمول، د ذ د ن، مصر ط1، 2015، ص35.

2 - خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، (د ط)، الاسكندرية، 2019، ص77.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الأجهزة المكلفة بمكافحتها وتتطلب إمكانيات تقنية متطورة لتتبع آثارها. لأنه لا عنف فيها ولا أثر اقتحام لسرقة مثلا، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، فهي جرائم هادئة لا تتطلب العنف، فإذا تم اكتشاف الجريمة الإلكترونية فلا يكون ذلك بمحض الصدفة، نظرا لعدم وجود أثر مادي لما يجري خلال تنفيذها من عمليات، حيث يتم نقل المعلومات بالنبضات الإلكترونية، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية¹، ما أدى إلا لضعف نسب الجرائم التي اكتشفها والإبلاغ عنها، وحتى القضايا التي طرحت على القضاء لم تكن في كثير من الأحيان أدلة كافية للإدانة فيها إلا في حدود معينة².

كما يلعب المجني عليه دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة الإلكترونية، حيث تحرص أغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة والانتهاك، على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها³.

3. الجريمة الإلكترونية صعبة الإثبات: تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، كونها تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن و أجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات

¹ - يوسف جفال، المرجع السابق، ص13.

² - بسمة خوني، جرائم الاعتداء على الأموال عبر الوسائط الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2017/2018، ص 11.

³ - نهلا عبد القادر الميموني، المرجع السابق، ص54.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

عبارة عن نبضات الالكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل كليا من قبل الفاعل أمر في غاية السهولة.

كما تجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح في غالب الأحيان في إثبات هذه الجريمة نظرا لطبيعتها الخاصة، كونها تركز على تغيير أو تعديل أو مسح البيانات كليا أو جزئيا، بالدخول إلى السجلات المخزنة في ذاكرة الحاسب الآلي، الأمر الذي يجعل إمكانية إثباتها في غاية الصعوبة، وبالتالي الصعوبة في توقيع الجزاء على مرتكبيها¹. وبالتالي يشكل نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء، عائقا أساسيا أمام إثبات الجريمة الالكترونية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحظة في بيئة الحاسوب والإنترنت، ونتيجة لنقص الخبرة وعدم إمكانية الشرطة في تقدير أهمية الجريمة الالكترونية، فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب مع هذه الأهمية، بل إن المحقق قد يدمر الدليل بمحوه محتويات الأسطوانة الصلبة عن إهمال منه أو بالتعامل بخشونة مع الأقراص المرنة².

4. أسلوب ارتكاب الجريمة الالكترونية وتعدد مرتكبيها: تبرز الجريمة الالكترونية على خلاف الجرائم التقليدية بصورة واضحة في أسلوب ارتكابها، مثلما تطرقنا في الخصائص السابقة بأنها جريمة لا تحتاج إلى جهد عضلي الذي يتخذ شكل العنف أو الإيذاء كما هو الحال في جريمة القتل مثل، فالجرائم الالكترونية هي جرائم هادئة لا تتطلب عنفا في تنفيذها أو مجهودا كبيرا، كل ما تتطلبها عدد من اللمسات الخاطفة على لوحة

¹ - شمس الدين إبراهيم أحمد، وسائل الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دار النهضة العربية، ط1، القاهرة، 2005، ص104.

² - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي و الإنترنت، بهجات للطباعة والتجليد، (د.ط)، مصر، 2009، ص28-29.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

المفاتيح حتى تؤدي إلى إسقاط الحواجز الأمنية للنظم والشبكات، حيث تحتاج إلى قدرة علمية في مجال التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية "الإنترنت"¹.

وما يميز الجريمة الإلكترونية عن باقي الجرائم بأنها تتم بتعاون أكثر من شخص على ارتكابها إضراراً بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه².

5. تتطلب وجود جهاز إلكتروني والتحكم بتقنية استخدامه:

من مميزات الجرائم الإلكترونية كذلك بأنها تعتمد في ارتكابها على جهاز إلكتروني متطور هو أداة ووسيلة الجريمة، فالجهاز الإلكتروني هو أساس الجريمة الإلكترونية و أساس تسميتها وإلا ما وجدت الجريمة الإلكترونية دون من الأساس. إضافة إلى ضرورة وجود شبكة إنترنت وتحكم الجاني في التكنولوجيا وامتلاكه دراية في مجال المعلوماتية والاتصالات، فلا نتصور ارتكاب جريمة الإلكترونية دون وجود تقنية المعلومات ولا شبكة الإنترنت، وتزيد خطورة المجرم كلما زادت قدرته على التحكم في الجوانب الثلاثة. وتتم الاعتداءات في هذه الجرائم على المعنويات (البرامج والبيانات والمعطيات) وليس على المكونات المادية فلا أثر مادي للجريمة بالكسر أو التحطيم أو السرقة. فهنا الجريمة تقليدية فالمشكل عندما يتم التعدي على المكونات المعنوية للحاسوب أي البيانات المخزنة فيه، وهنا يظهر تحكم الجاني في تشغيل الجهاز واستخدامه حتى يتمكن من الاعتداء على مكوناته

¹ - مراد يرمش، خصوصية الجريمة الإلكترونية، أطروحة الدكتوراه علوم في القانون الخاص، تخصص الملكية الفكرية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2020-2021، ص41.

² - نهلا عبد القادر المومني، المرجع السابق، ص58.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

المعنوية عند اختراق نظامه بسرقة المعلومات أو تعديلها أو مسحها أو تقليدها أو التلاعب بها وإساءة استخدامها¹.

6. **جريمة مستحدثة:** الجريمة الإلكترونية جريمة مستحدثة فهي نمط إجرامي حديث لم يكن مألوفاً من قبل، فالأساليب المستخدمة لارتكاب الجريمة أساليب حديثة، وهي وليدة التحولات التي شهدتها الحياة المعاصرة من تطور في مجال الإجرام، حيث أصبح يستعمل العلوم والتقنية كوسيلة للتنفيذ، من دول مختلفة (شبكات دولية تشارك في التخطيط والتنظيم والتنفيذ) في الخفاء بكل احترافية، كما أن الجرائم المستحدثة مازالت لم تتناول ولم تعالج بنصوص قانونية صريحة، رغم توافر كامل أركان الجريمة من (مجرم، ضحية وفعل إجرامي)، أي هناك صعوبة في التحديد الدقيق لها.

حيث أن الجريمة تسبق القانون كما يقول علماء الإجرام، وهي من أهم سلبيات ومساوئ التقدم التكنولوجي الذي ساهم في ارتكاب الجرائم واطهر جرائم جديدة، كتهبيض الأموال و التجارة بالبشر²، فشبكات الإنترنت هي حلقة الوصل بين كافة أهداف الجريمة (بنوك ومؤسسات).

7. **ارتكاب الجريمة الإلكترونية أثناء تشغيل نظام المعالجة الآلية للمعلومات:**

إن الجريمة الإلكترونية ترتكب بعد تشغيل نظام معالجة البيانات، ورغم وجود جرائم يمكن ارتكابها عند الإدخال والإخراج إلا أن مرحلة معالجة البيانات هي أخطر مرحلة وأسهلها لارتكاب هذه الجريمة، فكل جهاز في وضعية الإيقاف أو الإغلاق هو في وضع أمن سواء جهاز كمبيوتر أو جهاز إلكتروني ذكي. نستعرض المراحل التي ترتكب فيها الجريمة الإلكترونية كما يلي:

1 - خالد ممدوح، المرجع السابق، ص 86.

2 - خالد ممدوح إبراهيم، المرجع السابق، ص 86.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

- أ- **مرحلة الإدخال:** يسهل إدخال بيانات ومعلومات غير صحيحة وتكون كذلك بعدم إدخال المعلومات المطلوبة والوثائق الأساسية وهي أكثر مرحلة ترتكب فيها الجرائم المعلوماتية.
- ب- **مرحلة تشغيل نظام المعالجة الآلية للبيانات:** هنا يكون ارتكاب الجريمة الإلكترونية بإدخال تعديلات على برامج الحاسوب بالتلاعب فيقوم المجرم بإدخال معلومات غير مصرح بها، فيكون الاعتداء بتشغيل برامج جزئياً أو كلياً عمل البرامج الأصلية ويكون المجرم محترفاً ولما بالتقنية اللازمة ليحقق هدفه.
- ج- **مرحلة المعالجة الآلية للبيانات والمعطيات:** تكون هنا البيانات في حالة نشاط يجدر القول بأنها المرحلة المقصودة. حيث يكون الاعتداء على البيانات المخزنة في النظام من أجل معالجتها إلكترونياً ويمكن للمستخدم إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها أو طباعتها، وهذه العملية وثيقة الصلة بارتكاب الجرائم المعلوماتية¹.
- د- **مرحلة الإخراج:** تعتبر هذه المرحلة هي الأخيرة حيث يرتكب العمل الإجرامي على النتائج التي يخرجها لنظام المعلوماتي للحاسوب وتكون عملية إدخال البيانات صحيحة ومعالجتها صحيحة لكن التلاعب يكون في النتائج، أي أن النتائج لا تتوافق مع البيانات الموجودة في النظام.

ثانياً: السمات الخاصة بمرتكب الجريمة الإلكترونية:

يعتبر المجرم الإلكتروني شخص طبيعي لديه القدرة على تشغيل الحاسب الآلي واستخدامه، ليس المقصود بالقدرة هنا الخبرة العالية، ولكن القدرة هنا تتمثل بمعرفة طريقة ارتكاب الجريمة من خلال الحاسب الآلي، يتسم هذا المجرم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، حيث غالباً ما يكون شخصاً محترفاً يمتاز بالذكاء والدهاء ودراية

¹ - يوسف عبد النبي شكري، المعلوماتية وأزمة الشرعية، (د.ذ.د.ن)، الكوفة، (د.ذ.ط)، 2008، ص115.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

بأنظمة الحاسوب، ويكون مرتكب هذه الجرائم في أغلب الحالات متكيفا اجتماعيا، غالبا ما يكون هدفه من ارتكاب هذه الجرائم الحصول على الربح أو النفع المادي¹.

بما أن الجريمة الإلكترونية جريمة خاصة فإن المجرم الإلكتروني له صفات خاصة أيضا، حصرها الأستاذ باركر² في كلمة SKRAM وهي:

- المهارة وتعني SKITHS.
- المعرفة وتعني KNOWLEDG.
- الوسيلة وتعني RESOURS.
- السلطة وتعني AUTHORITY.
- الباعث وتعني MOTIVES.
- **المجرم المعلوماتي ذكي محترف:** حيث يمتلك مهارات تقنية تؤهله لتوظيف إمكانياته في الاختراق والاعتداء ويرتكب جريمته بمقابل مالي لصالح الغير.
- **مجرم متخصص ويعود للإجرام:** فهو مجرم له مهارة عن طريق الدراسة والتخصص، أو عن طريق الخبرة التي اكتسبها بسبب مجال عمله في مجال تكنولوجيات المعلومات فهو متخصص في التنفيذ لقدرته الفائقة ومهارته التقنية في مجال المعلوماتية، يستغلها في كسر كلمات المرور وحل الشيفرات ليقوم باختراق الشبكات والبرامج للحصول على البيانات الغالية الثمن، كما أن هذا المجرم المعلوماتي يستغل دائما قدراته في معاودة الاعتداء والاختراق على الحواسيب والمعلومات المخزنة قصد إثبات تفوقه.
- **مجرم اجتماعي وهادئ:** فلا يلجأ إلى العنف في ارتكاب جريمته معتمدا على الجهد الذهني والفكري بدل الجهد العضلي، وهو إنسان مثقف وعادي يتمتع بحقوقه السياسية

¹ - أسماء بن لعربي، خصوصية الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2021/2020، ص23.

² - خالد داودي، الجريمة المعلوماتية، دار الاصدار العلمي للنشر والتوزيع، الجزائر، ط1، 2008، ص32.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

والاجتماعية يعيش بين أفراد المجتمع ويعمل سواء في مجال المعلوماتية أو في مجال آخر، وهو اجتماعي لا تظهر عليه علامات الإجرام فهو يمارس حياته الطبيعية الهادئة ويدخل في تجمعات تظم مجرمين مثله لتبادل المعلومات والمهارات وكل ما هو جديد¹.

❖ **تصنيف المجرم المعلوماتي:** يصنف المجرم المعلوماتي إلى عدة طوائف مختلفة نرصدها فيما يلي:

(1) **القراصنة:** هم الأشخاص الذين يرتكبون الجرائم الإلكترونية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليه، ومن أمثلة هذه الطائفة صغار مجرمي المعلوماتية وينقسمون إلى نوعين وهما:

أ- **الهاكرز:** هو مصطلح أطلقه أمريكيون على المتميزين والمتمتعون بقدرة عالية من التقنية، أغلبهم صغار سن ولهم شغف بالحاسوب وهم هواة لا يبغون مالا ولا ضررا إنما إثبات قدراتهم، وهم مقتحمي النظم هواة هم شباب أو طلبة موهوبون هدفهم إثبات مهارتهم على اكتشاف أو إظهار الأنظمة المخترقة بدافع اللهو والفضول والمزاح.

ب- **الكرارز:** قراصنة محترفين هم بالغون تتجاوز أعمارهم 25 سنة فأكثر أو مهنيون ذوي اختصاص هدفهم التخريب وإلحاق الضرر بالضحية، يعيشون من عائدات جرائمهم ويعاودون فعلهم.

(2) **الحاقدون المخربون:** ليس لهم فئة عمرية محددة هدفهم ليس المكاسب ولكن الانتقام من أصحاب العمل والهيئات التي كانوا يعملون لديها، فهم موظفون سابقون تم الاستغناء عنهم، هدفهم أحداث الضرر وليس الحصول على مكاسب مالية يستغلون معرفتهم بأنظمة الحواسيب لدى هذه المؤسسات لنشر بيانات أو استعمال البيانات المخزنة في نظامها المعلوماتي أو مسحها، ويندرج عن هذه الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

¹ - غنية باظلي، المرجع السابق، ص35.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

- (3) المتجسسون: بدل الطرق التقليدية يستخدم المجرم من جهة استخباراتي ويستعمل المعلوماتية في جريمته للحصول على معلومات سرية عن دولة و إفشائها لدولة أخرى وتكون عسكرية صناعية أو اقتصادية ويكون غالبا أحد مستخدمي الجهاز المستهدف.
- (4) مخترقو الأنظمة: هم جهاز بحد ذاته يتبادلون المعلومات ويعقدون المؤتمرات لتجديد معلوماتية في جريمته للحصول على معلومات سرية عن دولة وإفشائها لدولة أخرى وتكون عسكرية صناعية أو اقتصادية ويكون غالبا أحد مستخدمي الجهاز المستهدف.
- (5) المتطرفون والإرهابيون: ينتسبون فيها إلى طائفة معينة ذات أفكار وتوجه خاص بها تستعمل الإنترنت لبث أفكارها وترويجها، والتطرق يكون دينيا أو جهويا أو عرقيا هدفه تغيير المجتمع وفقا لما يعتقد وليس لتحقيق مكاسب شخصية أو معنوية، أما الإرهابيون فعادة يرسلون رسائل تهديد ويقومون بتدمير البيانات المخزنة في الأنظمة¹ الحكومية لتسجيل وجهة نظرهم ويستعملون أساليب إقناع وتأثير أحيانا يقع ضحيتها المختصون اللذين يدرسونها لمواجهتها.
- (6) طائفة الربح المادي: هم مجرمي المعلوماتية يعملون في مجال المنظمة يهدفون من وراء نشاطهم الإجرامي تحقيق ربح مادي بطريقة غير شرعية، ويقترّب المجرم المعلوماتي من هذه الطائفة في سماته إلى المجرم التقليدي².
- (7) طائفة صغار السن: أو كما يطلق عليهم البعض صغار نوابغ المعلوماتية وفي اصطلاح القانون يطلق عليهم الأحداث³.

¹ - رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، 2018، ص108.

² - عبد العال الديبي، الجريمة المعلوماتية (تعريفها - أسبابها - خصائصها)، صادر عن المركز العربي لأبحاث القضاء الإلكتروني، 2013، http://accronline.com/article_detail.aspx?id=7509.

³ - طارق عفيفي، المرجع السابق، ص63.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الفرع الثاني: أركان الجريمة الإلكترونية

تأخذ الجريمة المرتكبة عبر الإنترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، والمجرم يقوم بهذا الفعل من خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة.

❖ الركن المادي:

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق التي يكلفها الدستور والقانون. لا بد من فعل أو إمتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة الإلكترونية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة الإلكترونية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طريق جهاز الكمبيوتر، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينهما وبين سابقتها، وهذا ما يدعو للتدخل التشريعي¹.

كما أن الدكتور رضا فرح قسم الركن المادي في حد ذاته إلى ثلاث عناصر وهما:

- السلوك الإجرامي.

- النتيجة الإجرامية.

¹ - بن غدفة شريفة والقص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الإنترنت وطرق محاربتها، أعمال الملتقى الوطني، "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017، ص48.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

- العلاقة السببية بين الفعل والنتيجة.

● **السلوك الإجرامي:** إن السلوك الإجرامي في الجريمة الإلكترونية يرتبط دائما بالمعلومات المخزنة في الحاسب الآلي، وهذا السلوك يكون بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة الإلكترونية يمكن أن نجده بنوعيه السلوك الإيجابي أو السلبي.

لا ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طوره أيضا عقلية الفاعل الذكية، والتي تمكنت أن تخرج من تقليدية السلوك الإجرامي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة¹.

● **النتيجة الإجرامية:** تعني الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى².

● **العلاقة السببية بين الفعل والنتيجة:** تكمن العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد النتيجة إلى الفعل وهو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت،

1 - أسامة أحمد المناعة، جلال محمد الزغي، ، ص51-52.

2 - بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص18.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

أما إذا كانت غير عمدية فإن نفي رابطة سببية يؤدي إلى انتفاء المسؤولية كلية عنها ذلك أنه لا شروع في الجرائم غير العمدية¹.

❖ **الركن المعنوي:** يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة².

يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور عمله بدخوله غير الشرعي³.

❖ **الركن الشرعي:** يقصد به وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبني على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينهما

1 - أسامة أحمد المناعة، جلال محمد الزغبى، المرجع السابق، ص 58-59.

2 - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص 73-74.

3 - حنان ریحان مبارك المضحاكي، الجرائم المعلوماتية الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه¹. فالقاعدة القانونية تنص على أنه (لا جريمة ولا عقوبة إلا بنص) ولقد تم التجريم في نظام مكافحة الجرائم المعلوماتية وتم وصف الجريمة وصفا دقيقا سنتعرف عليها في أنواع الجرائم المعلوماتية وفي الجزائر نص على ذلك القانون 04/09 وقانون العقوبات في المواد 394 و 394 مكرر²⁷.

المبحث الثاني: الطبيعة القانونية للجرائم الماسة بالأموال الإلكترونية و أنواعها

أدى التقدم التكنولوجي والتقني، وظهور الفضاء الإلكتروني ووسائل الاتصالات عبر الأقمار الصناعية إلى انتشار الجرائم الإلكترونية ولم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية³.

حيث أن هذا التطور الهائل قد أضفى لتقنية المعلومات واندماجها بتقنية الاتصالات فيما بعد طبيعة خاصة على جرائم كانت تقليدية قبل ظهورها، كما أن الجرائم الإلكترونية جرائم متعددة ومتنوعة، ويصعب حصرها بسهولة، فهي تشمل أي أمر غير مشروع، وعليه سنتطرق إلى الطبيعة القانونية في المطلب الأول، والأنواع الجرائم الماسة بالأموال الإلكترونية في المطلب الثاني:

1 - أسامة أحمد المناعة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان، 2014، ص45.

2 - أنظر القانون 04/09 وقانون العقوبات في المواد 394 و 394 مكرر 7.

3 - د. بخدة صفيان ود. وقاص ناصر، الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الإنترنت كنموذج، جامعة دكتور مولاي الطاهر، سعيدة، مجلة البحوث القانونية والسياسية، المجلد 03، العدد 16، 2021، ص117.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

المطلب الأول: الطبيعة القانونية للجرائم الماسة بالأموال الإلكترونية

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى ارتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال معالجة النصوص، وصعوبة التكيف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة.

بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات، ومتابعة مرتكبيها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة¹.

المطلب الثاني: أنواع الجرائم الماسة بالأموال الإلكترونية

تعددت محاولات الفقه لتحديد أنواع الجرائم الإلكترونية وذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحدثة ظهور هذه الجريمة، وكذا عدم وجود تعريف عام متفق عليه للجريمة الإلكترونية وتحديد مجالها، وكذا بالنظر للتطور التكنولوجي في كل صورة للارتباط الوثيق بينهما².

الجرائم التي تقع على الأموال هي جرائم الاعتداء على الأموال والتي تهدد ذات القيمة المالية ويدخل في نطاق هاته الحقوق حق ذو قيمة اقتصادية. كما أنه قد صاحب ظهور شبكة

1 - د. بوضياف إسمهان، المرجع السابق، ص 353.

2 - سفيان سوير، المرجع السابق، ص 32.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الإنترنت تطورات كثيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما انجر عنه تطورا وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الإنترنت انتهز بعض المجرمين الفرصة من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السطو والسرقة والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة¹.

كما أنه الأموال تختلف من مادية ومعنوية، واستقر الرأي² إلى أن المعلومات التي تعالج آليا وتأخذ حكمها البيانات المخزنة سواء في برامج الحاسوب أو في ذاكرته، تدخل ضمن الأموال وبالتالي تتمتع بالحماية الجنائية المقررة³.

و في ظل تحول الذي طرأ على المعاملات التجارية من معاملات تقليدية إلى معاملات تجارية الكترونية وما أنجز عنه من تطور وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الإنترنت، أضحت هذه المعاملات عرضة لشتى أنواع الجرائم وتنوع وسائل وأساليب ارتكابها والتي سندرسها في الفروع التالية:

الفرع الأول: كيفية ارتكاب الجريمة الإلكترونية

أولاً: وسائل ارتكاب الجرائم ماسة بالأموال الإلكترونية

1. الحاسب الآلي: يعرف الحاسب الآلي أنه عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة

¹ - صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون "تخصص القانون الدولي للأعمال"، جامعة مولود معمري، تيزي وزو - كلية الحقوق والعلوم السياسي، 2013، ص44.

² - هناك جدل فقهي حول مدى اعتبار المعلومات والبيانات كأموال يمكن تكون محلا للجريمة، وقد فضلت عدم الخوض في هذا الجدل خاصة أمام التطور التكنولوجي والذهني أين أصبحت للمنقولات المعنوية قيمة مالية كبيرة ومعياري للتطور الاقتصادي والفكري، وفي الواقع هي محل للاعتداء والاستيلاء.

³ - أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، 2007، ص20.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

ما، وذلك بتنفيذ ثلاث عمليات أساسية هي: استقبال البيانات المدخلة أي الحصول على الحقائق المجردة، ومعالجة البيانات إلى معلومات، وإظهار المعلومات المخرجة¹.

يقصد بالحاسب الآلي، الآلة الإلكترونية التي تستخدم وفق نظام معين لمعالجة وإدارة البيانات والمعلومات الرقمية المدخلة فيه وفق أوامر وتعليمات يختارها المشغل أو طالب الخدمة². لكن قد يكون الحاسب هدفا للجريمة، وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وقد يكون الحاسوب أداة لارتكاب الجرائم كما في حالة استغلال الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في للاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها والحصول على الأموال بواسطتها.

2. الهاتف الذكي: الهاتف الخليوي هو الجهاز الذي يوفر استخدامات أساسية مثل القدرة على إجراء مكالمات واستقبال وإرسال رسائل، بالإضافة إلى ذلك لديه القدرة على الاتصال بشبكة الإنترنت وتلقي وإرسال البريد الإلكتروني، والذي يسمح بإضافة تطبيقات محددة وله القدرة أيضا على الاتصال مع جهاز الحاسوب مما يتيح نقل المعلومات والوثائق المهمة وحفظها على الحاسوب والعكس³.

أما فيما يخص الجرائم التي يتم ارتكابها بواسطة الهاتف الذكي فتعرف على أنها: "كل فعل ينشأ عن استخدام غير مشروع للتقنية الاتصالية أو المعلوماتية للهاتف المحمول بهدف الاعتداء على مصلحة الغير أو تعريضها للخطر"، فبالرغم من الفوائد الجمة والعديدة التي

1 - نهلا عبد القادر المومني، المرجع السابق، ص20.

2 - بسمة خوني، المرجع السابق، ص23.

3 - بسمة خوني، المرجع نفسه، ص26.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

يقدمها هذا الجهاز إلا أن الجرائم الناتجة عن سوء استخدام هذه الوسيلة التقنية الحديثة أصبحت تتزايد مع مرور الوقت مما يجعلها مهددة لقيم المجتمع وأمن أفراد¹.

ومن أبرز هذه الجرائم نذكر جرائم الأموال التي تقع بواسطة الهاتف النقال، كما هو الحال في جرائم النصب وتبييض الأموال، أو عن طريق الاعتداء على الهاتف في حد ذاته، وهو ما يظهر في الإلتلاف مثلا والسرقة، وتأخذ جرائم الأموال المرتكبة عن طريق الهاتف الذكي عدة أبعاد خطيرة أبرزها الإضرار بالاقتصاد الوطني، والأمن المالي، خاصة إذا تعلق الأمر بالتجارة الإلكترونية أو غيرها من المعاملات التي يمكن القيام بها بواسطة الهاتف النقال².

3. شبكة الإنترنت: ويقصد بها الشبكة الدولية العملاقة التي يندرج تحت لوائها عدد لا محدود من الشبكات وأجهزة الحاسب الآلي. كما ساهم سهولة استخدام الإنترنت والخدمات المتعددة والمتنوعة التي تقدمها في جميع مجالات الحياة، ساهم بشكل فعال في زيادة أعداد المستفيدين منها، وسنقوم باستعراض أهم الخدمات الإلكترونية التي تقدمها الشبكة العالمية للمعلومات³:

أ- البريد الإلكتروني: يعد أكثر وسائل الإنترنت استخداما في العالم، وتتطلب هذه الخدمة عنوان البريدي يكون عبارة عن اسم المستخدم يتلوه علامة @ ثم اسم الموقع

¹ - أحمد حسين، حجية الأدلة المستمدة من الهواتف النقالة في الإثبات الجنائي، مجلة الفكر، د.م.ج، العدد 15، جوان 2017، ص54.

² - محمد التوجي، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2018/2019، ص25.

³ - نهلا عبد القادر المومني، المرجع السابق، ص39.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الذي يوجد فيه مقر البريد الإلكتروني وهذه الخدمة توفر إرسال واستقبال الرسائل ونقل الملفات مع أي شخص له بصورة سريعة جدا لا تتعدى دقائق¹.

ب- **محركات البحث:** هي عبارة عن برامج تساعد في الحصول على المعلومات، فكما معروف هناك كم هائل من المعلومات في شبكة الإنترنت يرغب المستخدم في معرفة المواقع التي تمكنه من الوصول مباشرة إلى مبتغاه².

ت- **المحادثات:** وهي خدمة تسمح للمستخدم بفتح خص اتصال بين حاسبه وحاسب مستخدم آخر، ومن خلال هذا الخط يستطيع كتابة رسائل له، واستقبال رسائل منه، ويمكن التواصل مباشرة كتابيا أو صوتيا أو بالصوت والصورة. أيا كانت مواقعهم، ويمكن أن تجري المحادثة بشكل جماعي يشهده جميع الموجودين وهو ما يسمى بغرفة المحادثة³ Chat Room.

ث- **التجارة الإلكترونية:** أتاحت شبكة الإنترنت لطرفي العقد التقابل وجها لوجه بالصوت والصورة والاتفاق على التفاصيل الدقيقة بعد إبداء الإيجاب ثم القبول بطريق الإنترنت، ثم إبرام العقد والتوقيع عليه الكترونيا، دون الحاجة لاجتماع المتعاقدين في مكان واحد، ويمكن للمشتري أن يسدد قيمة بضاعته عن طريق الدفع بواسطة شبكة الإنترنت، وكيفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به⁴.

1 - رضا بوغرة، شبكة الإنترنت وعلاقتها باكتساب السلوك الانحرافي لدى الشباب المراهق، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة محمد لمين دباغين، سطيف، 2017/2016، ص60.

2 - نهلا عبد القادر المومني، المرجع السابق، ص40.

3 - رضا بوغرة، المرجع السابق، ص62.

4 - نهلا عبد القادر المومني، المرجع السابق، ص41.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

الفرع الثاني: الأساليب التقنية المستخدمة في إتلاف المعلومات

أولاً/ الفيروس المعلوماتي: ويقصد به برامج مشفرة مصممة بقدرة علة التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات، والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم حيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها¹.

ثانياً/ الدودة المعلوماتية: يقوم برنامج الدودة باستغلال أية فجوة في نظم التشغيل مي ينتقل من حاسب إلى آخر أو من شبكة إلى أخرى عبر الوصلات التي تربط بينهما، وتكاثر أثناء عملية انتقالها بإنتاج نسخ منها².

ثالثاً/ القنبلة المعلوماتية: يقصد بها نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخرى، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل برامج الحاسب الآلي³.

الفرع الثالث: أنواع الجرائم الماسة بالأموال الإلكترونية

أولاً: التحويل الإلكتروني الغير المشروع

يتم ولوج مخترقي الشبكات إلى بيانات حساب الآخرين، من خلال الحصول على كلمة السر الدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسمح للجاني بالتوغل في النظام المعلوماتي عادة ما يكون هؤلاء من العاملين على إدخال البيانات في ذاكرة الجهاز أو

¹ - حمزة بن عقون ، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الاجرام وعلم العقاب، جامعة الحاج لخضر-باتنة-، كلية الحقوق والعلوم السياسية، 2012/2011، ص159.

² - نهلا عبد القادر المومني، المرجع السابق، ص131.

³ - نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الانترنت، دار نور للنشر، د.ط، الاسكندرية، 2017، ص93.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات وتتم عملية التحويل الإلكتروني للأموال بأحد الطرق المالية:

- **الاحتيال (النصب):** يتم ذلك بطرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني بطريقة معلوماتية أو من خلال تصرف الجاني في المال، وهو يعلم أن ليس له صفة التصرف فيه، وقد يتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على مال المجني عليه فيتم التحويل الإلكتروني للأموال، وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب¹.

- ومن أجل ذلك ذهب معظم التشريعات التي اعتبرت هذه الأرصدة بمثابة ديون لا يمكن أن تكون محلاً للاختلاس، رغم أن بعض الدول اعتبرت أموال وتصلح أن تكون محلاً للتحويل، خاصة أمام ما يحققه ذلك من ربح للجاني وخسارة فادحة للمجني عليه، منها الولايات المتحدة التي أصدرت عدة قوانين اعتبرت من خلالها الأموال الكتابية أو البنكية عبارة عن أموال، كذلك في الجزائر فإن المستندات والأوراق المالية تعد من الأموال².

ثانياً: الاحتيال باستخدام بطاقات الدفع الإلكتروني عبر الإنترنت

إن من أهم منتجات التجارة الإلكترونية والمصارف هي البطاقات الائتمانية وهي وسيلة إلكترونية توزعها المصارف على زبائنها بضمان رصيد بنكي حيث يستعملها لشراء سلع أو الاستفادة من خدمات.

¹ - د. بخدة صفيان - د. وقاص ناصر، الطبيعة القانونية لجرائم المستدثة ووسائل ارتكابها جريمة الإنترنت كنموذج، جامعة دكتور مولاي الطاهر سعيدة، مجلد 03، العدد 16، 18-14-2021، ص 131.

² - د. بخدة صفيان - د. وقاص ناصر، نفس المرجع، ص 132.

الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية

أصبحت البطاقة محلاً للاستهداف الإجرامي من المجرمين المعلوماتيين بسرقة البيانات الخاصة بها نماذج منها للقيام بسحب أموال أو شراء سلع بطريقة غير مشروعة من الاعتداءات التي تقع على البطاقات الائتمانية باعتبارها محل للحقوق الكلية سرقة البطاقة عن طريق حاملها بصورة مباشرة، فالسارق سواء استعمل البطاقة أو لم يستعملها، فهو يعد ارتكاب لجريمة السرقة لمجرد توافر أركان هذه الجريمة¹.

ثالثاً: جريمة القمار

ظهرت بظهور النوادي والказينوهات الافتراضية التي انتشرت عبر المواقع الإلكترونية والخاصة بألعاب القمار لكن هذه المواقع غير مسموح بها² في أغلب البلدان وغير مصرح لها بممارسة نشاطها حيث أصبحت فيما بعد مسرحاً لجريمة غسيل الأموال.

الرابعاً: جريمة غسيل الأموال

هي جريمة تقليدية تطورت عن تطور التكنولوجيا حيث يتم ارتكابها عن طريق تطهير الأموال، التي يكون مصدرها غير مشروع ويتم استثمارها بطريقة شرعية عن طريق البنوك، عن طريق نقلها بعملية اقتصادية ومالية للأموال من مصدر غير مشروع إلى دائرة الاقتصاد الشرعي، والمصدر غير الشرعي يكون مخدرات أو اختلاس، ويكمن ضرر وخطورة تبييض الأموال في أنها تدخل إلى الاقتصاد حيث أنها أموال غير مستقرة يمكن تحويلها إلى الخارج في أي وقت كما أنها جريمة مركبة حيث تغطي على الجريمة الأولى، ولها أضرار أمنية واجتماعية وقانونية وسياسية³.

¹ - عبد الكريم الردايدة، جرائم بطاقات الائتمان لدراسة تطبيقية ميدانية، الطبعة الأولى، الأردن، دار حامد، 2013، ص32.

² - عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، الأردن، ط2، 2014، ص151.

³ - مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الإرهاب الإلكتروني المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ط1، 2014، ص143.

الفصل الثاني: الجريمة الإلكترونية في التشريع الجزائري

المبحث الأول: نظرة المشرع الجزائري للجريمة الإلكترونية.

المبحث الثاني: آليات مكافحة ومعالجة جريمة المساس بالأموال الإلكترونية

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

كما هو معروف سابقاً أن الجريمة الالكترونية ما هي إلا نتاج التطور العلمي والتكنولوجي بمعنى إحدى الأعراض الجانبية للتطور المذكور، وهي كما عرفها المشرع الجزائري بموجب أحكام المادة 02 من القانون رقم 04/09 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات. وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الالكترونية"¹.

ومن خلال التعريف السابق نستنتج بأن المشرع الجزائري قد اعتمد على معيار دور النظام المعلوماتي لتحديد معالم الجريمة من أجل مكافحتها والحد والوقاية منها نظراً لأخطارها الجسمية بالعملاء وهذا ما تطرقنا له في الفصل الثاني حيث قمنا بتقسيمه إلى مبحثين رئيسيين الأول تم فيه معالجة نظرة المشرع الجزائري للجريمة الالكترونية وذلك في مطلبين، مال الأول لذكر موقف المشرع الجزائري للجريمة الالكترونية بينما المطلب الثاني فقد ذكر فيه مظاهر وتحديات الجريمة الالكترونية، أما في مظاهر وتحديات الجريمة الالكترونية. أما فيما يخص المبحث الثاني حاولنا الإلمام بآليات مكافحة ومعالجة جريمة المساس بالأموال الالكترونية حيث قسمناه هو الآخر لمطلبين الأول تمت فيه معالجة الحماية القانونية لوسائل الدفع الالكتروني، أما المطلب الثاني فيذكر الهيئات المكلفة بمواجهة المعلوماتية في الجزائر وهذا على النحو الآتي:

¹- قانون رقم 04/09 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا

الإعلام والاتصال ومكافحتها، ج.ر، العدد 74.

المبحث الأول: نظرة المشرع الجزائري للجريمة الالكترونية

نظرا لما خلفته الثورة المعلوماتية من جرائم جديدة ومتنوعة تمس بملكيات الغير فقد أقحم المشرع لإبراز موقفه واهتمامه بالموضوع نظراً لخطورته من خلال تجسيد موقفه من خلال نص من نصوص تشريعية جديدة حول الموضوع وتجديد البعض منها وهذا إن دل إنما يدل على مدى تهديدها بأمن وسلامة الملكية المالية للمواطنين والعملاء وهذا ما سندرسه في هذا المبحث من خلال تقسيمه إلى مطلبين رئيسيين يذكر في المطلب الأول موقف المشرع الجزائري للجريمة الالكترونية، أما المطلب الثاني مظاهر وتحديات الجريمة الالكترونية وهذا على النحو الآتي:

المطلب الأول: موقف المشرع الجزائري من الجريمة الالكترونية

برز موقف المشرع الجزائري للجريمة الالكترونية من خلال العديد من الطرق حيث أن المشرع الجزائري تبني مصطلح المساس بأنظمة المعالجة الآلية للمعطيات كدلالة على الجريمة الالكترونية وذلك باعتباره أن النظام المعلوماتي وما يحتويه من عناصر ومكونات غير مادية في حد ذاته محلاً للجريمة الالكترونية، ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأساسي الذي لا بد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال للبحث عن أركانها.

حيث أنه مستوى الدول العربية، تم إصدار قرار عن مجلس وزراء العدل العرب بجامعة الدول العربية بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، يتكون من 27 مادة وضع من خلالها القواعد الأساسية التي يتعين على

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

التشريعات العربية الاستعانة به عند وضع قانون لمكافحة الجرائم الالكترونية، كما تسعى الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الالكترونية والتشجيع على قيام اتحادات عربية تهتم بالتصدي لتلك الجرائم وتفعيل دور المنظمات والادارات والحكومات العربية في مواجهتها عن طريق نظام الأمن الوقائي.

ولم يتخلق المشرع الجزائري بدوره عن ركب الدول العربية التي وضعت الكثير من التشريعات في مجال نظام المعلومات حيث أنه عرفه من خلال المادة 2 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مسمىاً إياه "المنظومة المعلوماتية" وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين.

ولقد جرم المشرع الجزائري الأفعال التي تمس بأنظمة الكمبيوتر وذلك بسبب تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة لنوعية الجرائم التي لم تكون موجودة في المجتمع الجزائري من قبل، ما دفع لتعديل قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم للأمر رقم 156/66 المتضمن قانون العقوبات والذي جاء في القسم السابع مقرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 8 مواد من المادة 394 مكرر وحتى المادة 17¹.

¹- شاين نوال، الجريمة الالكترونية في التشريع الجزائري-ماهيتها، موضوعها، خصائصها، مظاهر تحدياتها، جامعة الحاج لخضر باتنة1، الجزائر تاريخ، مجلة سوسيولوجيا، المجلد06، العدد 02، 2022، ص73.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

وهكذا يمكن أن نستنتج مما سبق عن الجريمة الالكترونية في التشريع الجزائري موقف المشرع من هذه الجريمة، وهو أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام، مما دفع الكثير من الدول إلى النص على معاقبة هذا النوع من الجرائم، بسعيها من خلال ذلك لتوفير حماية الجزائرية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال، حيث أثار المشرع الجزائري استخدامه لمصطلح لدلالة على كلمة المعلومات وسيلة ارتكابها، وتم تبينها فقط في الأفعال والتصرفات التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها.

وقد قدر المشرع في تدخله أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها، بقيامه بحماية هذه المعطيات ومن أوجه عدة للاختراق والهكر والسرقة والتجسس...إلخ.

لاحقا بعد هذه المرحلة تم اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية بأنها التي ترتبط مباشرة بأنظمة المعالجة الآلية للمعطيات¹.

هذا بالإضافة إلى أنه المشرع الجزائري لم يجد بدأ من تعديل قانون العقوبات لما احتواه من فراغ قانوني في هذا المجال، وهذا بموجب القانون رقم 16/04 المؤرخ في 2004/11/10 المتمم والمعدل لأمر 156/66 المتضمن قانون العقوبات الذي أقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، والذي احتواه عرض أسباب

¹ - شاين نوال، المرجع نفسه، ص74.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

التعديل الذي قد تم بأن ما حدث من تطورات تكنولوجية وانتشار وسائل اتصال حديثة وجديدة أدى بظهور أشكال جديدة الإجرام.

وأهم موقف قد صدر من المشرع الجزائري حين عرفها بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى¹ ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ومن هنا نستنتج بأنه قد وقف في تعريفها إذ أنه لم يكمل الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية²، ولولا شبكات الاتصال والأنظمة المعلوماتية لم يكن لنا الإمكانية من إعطاء صفة المعلوماتية لهاته الجرائم.

وللتوضيح أكثر فيما يخص بنظام المعالجة الآلية للمعطيات الذي جاء به المشرع الجزائري قد قسمنا هذا المطلب لفرعين تكلمنا في الفرع الأول حول المقصود بنظام المعالجة الآلية للمعطيات، بينما الفرع الثاني فقد تم فيه معالجة مدى اشتراط الحماية التقنية للنظام المعلوماتي وهذا على النحو الآتي:

¹- د. بوضياف اسمهان، الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، ص09.

²- د. بوضياف اسمهان، نفس المرجع، ص352.

الفرع الأول: المقصود بنظام المعالجة الآلية للمعطيات¹:

مما لا شك فيه أنّ كل عملية معالجة معطيات تحتاج إلى آلية منظمة لكي تتولى عملية الجمع والإمام مع توفير المعلومات المستوجبة ومعالجتها الأمر نفسه خلق الحاجة لوسائل وتقنيات لتسهيل عملية القيام بذلك ما خلف نتيجة عرفت بـ "نظم المعلومات المبنية على الحاسبات الآلية"، والذي عرف هو نفسه بمصطلح آخر "المعلومات المحسوبة"، إذ يعتبر نظام يقوم على الأجهزة والمكونات البرمجية للحواسيب وذلك لإسترجاع المعلومات ومعالجة المعطيات.

إضافة إلى ذلك تم تعريفه بأنه إجراءات وآلية محكمة التنظيم تعمل على تنظيف وفرز وجمع البيانات مع معالجتها وهذا النحو يليها إلى معلومات يقوم الإنسان (المستخدم) بإسترجاعها عند حاجته لها لتمكنه من اتخاذ قرارات أو إنجاز أعمال أو القيام بأي وظيفة من خلال المعلومات المعرفية التي يتحصل عليها من المعلومات التي إستعادها من النظام.

والظاهر أن المشرع الجزائري عند ما قام بعملية تعديل لقانون العقوبات وإضافته للقسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات عارضاً من خلاله صور هذه الاعتداءات لم يعرف نظام المعالجة الآلية للمعطيات وأوكل بذلك مهمة تعريفه للفقهاء²، ونرى

¹- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، 2013/2012، ص42-45.

²- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، جامعة قاصدي مرباح، ورقلة، 2018-2019، ص19.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

من خلاله أن ماقام به المشرع كان في محله حين تجنبه للتعريف المقيد بمعنى لم يعطي تعريف محدد لنظام المعالجة الآلية للمعطيات وهذا لأن النظام المذكور دائما في حالة تطور تكنولوجي، يخضع لتغيرات وفقرات سريعة ومتلاحقة، التي تتسع لإمكانية شمول وسائل تقنية حديثة، خاصة وأن عالم المعلوماتية والعالم الافتراضي صعب إحتواءه وبالأخ لأنه في بدايته.

ومن خلال المفهوم السابق وما ذكرناه من عناصر حول المقصود بنظام المعالجة الآلية للمعطيات فإننا نستنتج بأنه مصطلح ينطبق على أي نظام من الأنظمة مهما كان مسماه أيضا يتوفر على عدة عناصر مترابطة ببعضها البعض بعدد معين من الموصلات ذلك بهدف تحقيق المعالجة الآلية للمعلومات من خلال التجميع، والتخزين و المعالجة ، والنقل، والتبادل عبر برنامج معلوماتي. وعليه فإن فكرة نظام المعالجة الآلية للمعطيات ذات حدود مرسومة قائمة على أساس الروابط بين مختلف أجزاء هذا النظام.

الفرع الثاني: مدى اشتراط الحماية التقنية للنظام المعلوماتي¹:

لقد اختلف الفقه القانوني في مدى اعتبار الحماية الأمنية لنظام المعالجة الآلية للمعطيات كشرط ضروري كي يحظى هذا النظام بالحماية الجزائية من عدمها، فقد اعتبر جزء من الفقه الفرنسي إلى عدم اشتراط توفر الحماية الفنية للنظام المعلوماتي لقيام الجريمة المعلوماتية²,

¹ - سعيداني نعيم، المرجع السابق، ص45.

² - د. بن دراج علي إبراهيم، الجرائم المعلوماتية- محاضرات-، معهد الحقوق والعلوم السياسية المركز الجامعي آفلو،

أغواط، 2020-2021، ص11.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

وذلك راجح بأن نظام الحماية الفنية والتقنية والأمن ليس له سوى إيجابي، وأن ثبوت سوء نية المنتهك لهذا النظام ودخوله إليه بطريقة غير شرعية هي متوفرة أساساً¹.

وفي الناحية الأخرى قام اتجاه آخر من الفقه المتمسك بضرورة وجود نطاق كاف من الحماية الأمنية للمختلف الأنظمة المعلوماتية التي تم معالجتها آلياً بتقسيم هذه الأخيرة إلى ثلاثة أصناف.

1- أنظمة مفتوحة للجمهور.

2- أنظمة قاصرة على أصحاب الحق فيها مع توفرها على حماية فنية لها.

3- أنظمة قاصرة على أصحاب الحق فيها، ولكن دون حماية فنية.

حيث اعتبرها هذا الفقه أن النوع الأخير من الأنظمة المعلوماتية هو الذي يتمتع بالحماية الجنائية، وحجبتهم في ذلك أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنياً لأنه من الطبيعي أن يقوم بإستغلالها أي شخص، لذا فإن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم ويتوفر الحماية الأمنية، ولو بقدر أدنى².

لذا فإن توفر الحماية التقنية له دور مهم وكبير خاصة في تحديد القصد الجنائي لدى القائم بجريمة المعلوماتية المعروف بـ (المجرم المعلوماتي)، ما جعل النقاش حول هذا الموضوع غير متوفر في الآونة الأخيرة.

¹ - أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي-دراسة مقارنة-، دار النهضة العربية للنشر والتوزيع، ط1، مصر، 2000، ص264.

² - د. بن دراح علي إبراهيم، المرجع السابق، ص11-12.

المطلب الثاني: مظاهر وتحديات الجريمة الالكترونية

مما لا شك فيه أن الجريمة الالكترونية لا تختلف عن باقي الجرائم التقليدية سوى في أنها حديثة الظهور فقط، لها مظاهر مختلفة وتحديات عديدة عبر نطاق واسع في العالم نظراً للانتشار السريع والمتداول بكثرة لشبكة الإنترنت هي قبل مختلف الأطوار والأعمار كما ذكرنا سابقاً، وما خلفته من آثار جانبية حادة على مستخدميها هي انتهاكات لحقوق شخصية وملكيات مالية وغيره ما دفع بأغلب دول العالم بتجريم الجريمة الالكترونية وسعت جاهدة من أجل تعديل القوانين والنصوص حتى تضع مواد تنص على معاقبة مرتكبي هذه الجرائم كقانون العقوبات السعودي الذي جعل تجريم الجرائم الالكترونية بالسجن لمدة لا تزيد على سنة وبغرامة مالية لا تزيد عن خمسمائة ألف ريال سعودي¹. والأمر نفسه جرمه المشرع الجزائري واعتبره ظاهرة خطيرة تهدد المجتمع والمواطن ونص عليها في القانون العقوبات - التعديل - كما قام بتقسيم الجريمة الالكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها²، وتشمل هي الأخرى جل الجرائم التي ارتكبت عن طريق تكنولوجيا الاعلام والاتصال، أما الثاني فيبرز في الجريمة التي تقع على النظام المعلوماتي والتي قام المشرع بدوره بتحديددها في قانون العقوبات الجزائري، وعليه فإن ظاهرة الجريمة الالكترونية يترتب عليها العديد من التحديات المختلفة مثل:

¹ - شاين نوال، المرجع نفسه، ص 74.

² - نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الاداري، جامعة أحمد درارية، أدرار، 2016-2017، ص24.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

- ظهور وتنامي الأنشطة الإجرامية الالكترونية وتوسل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها، الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية هذا النوع من الجرائم ودعوته الدول إلى التصدي لها ومكافحتها¹، وهذا نظرا لصعوبتها وصعوبة إدراج بعض الأنشطة ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ومن حيث ما يربط بهشاشة نظام الملاحقة الإجرائية² التي تتميز بالقصور والعجز على تقبل هذه الظاهرة الإجرامية الحديثة على كلا الصعيدين (الملاحقة الجنائية في إطار القوانين الوطنية) (الملاحقة الجنائية الدولية).

- وعلى خلاف ما ذهب إليه البعض الذي قال بأن القوانين القائمة وحدها تكفي للحد من الجرائم الالكترونية، ظهر رأي آخر يقر ببعض الصعوبات التي تواجهه في تطبيق بعض النصوص القانونية، منها ما يتعلق بطبيعة الجريمة الالكترونية غير المادية، ومما ما يتعلق بهاجس التعارض مع مبادئ هامة ومستقرة في القانون الجنائي³ كمبدأ شرعية العقوبات والجرائم التفسير الضيقا، ما جعل ببعض المشرعين مختلف الدول إلى التدخل من خلال تعديل بعض النصوص التشريعية القائمة ووضع نصوص

¹-شاين نوال، المرجع السابق، ص 74.

²- شاين نوال، المرجع نفسه، ص 74.

³- شاين نوال، المرجع السابق، ص 75.

جديدة تتناسب مع تلك الجرائم والعمل بالدعوة إلى التوسع والتفصيل في النصوص القانونية الجنائية السارية.

- وما تم ذكره من خطورة هذه الظاهرة الإجرامية التي باتت تلعب دوراً تهديدياً خطيراً واتخذت نمطاً أو بالأحرى أنماطاً جديدة وصنفت كإحدى أنواع الذكاء الإجرامي في حد ذاته يمثل تحدياً جديداً وجدياً في الزمن الحاضر، و الحد منه وتجاوزه يتطلب دراسات مكثفة وعميقة بداية من التعرف على هذه التحديات بإبراز جوانبها والتفصيل فيها وتشخيصها ثم العمل على مكافحتها على كلا الصعيدين المذكورين سابقاً (التجريم والعقاب) و(الملاحقة الإجرائية).

والقيام بذلك يستلزم:

أولاً: الاقتناع بخطورة الجرائم الالكترونية كنقطة انطلاق ليلبها محاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة الذي بقدر نجاحه تتحقق فعالية كل الجهود والإمكانيات¹ من أجل وضع حد لهذه الظاهرة والتصدي لها ومكافحتها بقوة القانون.

ثانياً: العمل على تطوير التشريع الجنائي وتثخين بنيته وذلك بقوة القانون والتشريعات المتواصلة ونهج طرق تعمل على سد الثغرات والنقائص التي تسود الأنظمة الجنائية، وفق نحو يمنحها القدرة على إخضاع هذه الأعمال الإجرامية للقانون والنصوص التشريعية، لكن شرط أن تتم هاته العملية و هذا التطور في إطار قانوني مع احترام مبدأ شرعية الجرائم والعقوبات ومبدأ الشرعية الجزائية، بهدف متكامل ومتناسق مع المعاهدات الدولية.

¹ - شاين نوال، نفس المرجع، ص75.

المبحث الثاني: آليات مكافحة ومعالجة جريمة المساس بالأموال الالكترونية

عرفنا ظاهرة الجريمة الالكترونية ومدى خطورتها في المجتمع وتهديدها بالمساس بحقوق مستخدمي شبكات الإنترنت خاصة في الدفع والسحب، إذ أنها هاته الجريمة تسمى بالملكية المادية والأموال الالكترونية للمستخدمين ما يشكل خطراً كبيراً في ضياعه وضياع الأمان. وقد برز دور المشرع الجزائري خاصة حيال تعديله لقانون العقوبات حيث نص على بعض العقوبات المترتبة عن هذه الجريمة الجديدة، ونلاحظ من تحليلنا السابق أنه بالرغم مما قدمته الأموال الالكترونية من مزايا وتسهيلات لمستخدميها غير أنه واكبها العديد من المشاكل القانونية وذلك جراء الاستخدامات التعسفية وغير المشروعة - الاستخدام غير المشروع للأموال الالكترونية- أو ما يعرف بالجرائم في الصياغات القانونية وبالتالي فإن الأمر لشدة خطورته فإنه يتطلب حماية المساس بالأموال الالكترونية.

أيضا لا بد من مكافحتها والحد والتقليل منها لأنها سريعة الانتشار وهذا راجع للمعلوماتية والعولمة والإنترنت إذ أنه بالرغم من النصوص القانونية والآليات التي شرعها المشرع غير أنه يوجد من هاته الجرائم ما يفلت من نطاق التجريم بالرغم من خطورتها والأمر كله يعود إلى التقدم العلمي والتكنولوجي المتسارعان ما يعجز نصوص القانونية مواكبتها.

وهذا ما سنحاول الوصول إليه وشرحه من خلال دراسة الحماية القانونية لوسائل الدفع الالكتروني في المطلب الأول والهيئات المكلفة بمواجهة المعلوماتية في الجزائري في المطلب الثاني على النحو الآتي:

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

المطلب الأول: الحماية القانونية لوسائل الدفع الالكتروني

لا ننكر ما وصلت إليه وسائل الدفع الالكتروني من تطورات هائلة ورغم ما حققته من نجاحات عالمية بواسطة بطاقة السحب والدفع الالكترونية أو الأموال الالكترونية وغيرها إلا أنها لم تسلم من الثغرات الغنية وذلك بسبب التطور لا محدود للجانب التقني في صياغة هذه الوسائل الأمر الذي فتح مجالاً كبيراً وأفاقاً كثيرة للجرائم كعصابات منظمة ومجرمين محترفين تمثلت أدوارهم في الاعتداء على حقوق المالية المتعلقة بالمستخدمين لها -عملاء وسائل الدفع- حيث يتميزون بقدرة عالية في التحرك والسرعة والبيديهية والذكاء خاصة في استخدام الوسائل التكنولوجية والمعلوماتية، زيادة على ذلك سرعة التحرك بين الحدود الدولية وتعدد جرائمهم ونشاطاتهم الإجرامية، وغيرها من التصرفات اللاقانونية والحادة.

ما استوجب على المشرع وضع حداً لها وعلى الأقل التقليل منها لأن سرعة القانون لا تواكب سرعة المعلوماتية، ومحافظة على سلامة ملكية المستخدمين وما دفع به أيضاً أن يصرح بنصوص قانونية واضحة بأنها جريمة وطنية تعاقب قوانين العقوبات الوطنية الداخلية عليها وذلك لأنها كما ذكرنا جرائم قانونية تخلف مسؤوليات جنائية¹. وهذا ما سنتطرق إليه في مطلبنا من خلال تقسيم إلى نوعين يتناول الفرع الأول والمسؤولية الجنائية المباشرة، والمسؤولية الجنائية الغير المباشرة في الفرع الثاني على النحو الآتي:

¹- بلعربي إكرام، بطاقة الائتمان المصرفية ومسؤوليتها الجزائية، مذكرة لنيل شهادة الماستر، جامعة أبو بكر بلقايد، تلمسان،

2022-2023، ص43.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

الفرع الأول: الحماية الجنائية المباشرة

اعتبرت جريمة الاحتيال احدى أخطر الجرائم التي تهدد وسائل الدفع الالكتروني، حيث تتمثل جريمة الاحتيال في الاستيلاء على الحيازة الكاملة للأموال الغير بطريقة يتوغلها الخداع، كما عرفها بعض الفقهاء بأنها استعمال إحدى وسائل التدليس التي نص عليها القانون وذلك على سبيل الحصر لحمل المجني عليه على تسليم الجاني أموالاً مملوكة للغير نتيجة الوقوع في الغلط.

ولقد برز اختلاف كبير في تسمية هذه الجريمة في مختلف القوانين، كما هو الحال بالنسبة للمشرع الجزائري هو الآخر تناول جريمة الاحتيال في قانون العقوبات وذلك من خلال نص المادة 372 حيث قال بأنها: " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو ملخصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو آية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 ديناراً¹.

¹- دحلوز محمد، النصب والاحتيال على المواقع الالكترونية وسبيل مواجهتها، مذكرة لنيل شهادة الماستر، جامعة عبد

الحميد ابن باديس، مستغانم، 2022-2023، ص20.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

أما عن جريمة الاحتيال الالكتروني فإنها تحمل نفس المفهوم الذي تناولناه، فقط الفرق بينهما وبين جريمة الاحتيال سابقة الذكر أن الاحتيال الالكتروني يتم بوسيلة أخرى وسيلة حديثة يتم بموجبها تنفيذ الجريمة و المتمثلة في الحاسب الآلي بالإضافة إلى توافر شبكة الإنترنت التي تعتبر جوهر وأساس هاته الجريمة، إذ بدون الشبكة العنكبوتية لا يكون هناك وجود للاحتيال الالكتروني ويندرج تعريفها تحت تعريف الاحتيال وهذا ما سنشرع في دراسته من خلال ذكر مفهومها وذكر بعض خصائصها.

- نظرا لخطورتها سنتطرق في هذا الفرع إلى تجريم الاحتيال الالكتروني على النحو الآتي بالإضافة إلى تجريم استخدام الحصول على أرقام وبيانات وسائل الدفع الالكتروني.

أولاً: مفهوم جريمة الاحتيال الالكتروني

جرائم الاحتيال الالكتروني إحدى نتائج وحوصلات الاستخدام غير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي وهذا ما أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم¹، وقد عرفت أيضا بأنها كل نشاط إجرامي يتم فيه استخدام التقنية الالكترونية المعروفة بالحاسوب الآلي، والإنترنت أي أنها تعتمد على الرقمنة.

والاحتيال المعلوماتي هو كل السلوكات الاحتيالية التي تنتهج منهج الحوسبة بنية الحصول على مال، ويعتبر هذا الفعل تلاعب عمدي ببيانات ومعلومات تمثل قيمة مادية يتم

¹ - محمد العبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص32.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

تخزينها في نظام الآلي، أو إضافة وإدخال بيانات ومعطيات صحيحة بدون تصريح أو التأثير على الحاسوب الآلي بالتلاعب في الأمر والتعليمات التي تحكمه أو كما تحكم عملية البرمجة بهدف الحصول على ربح غير مشروع وإلحاق الضرر بالغير.

وبالتالي فإن الاحتيال الالكتروني يعتبر وسيلة حديثة ومتطورة يتم اللجوء إليها للاختراق، الوصول لأهداف معينة بطرق غير مشروعة، وذلك استثناءً على الشبكة العنكبوتية التي تعتبر أساساً لهذه الجريمة، دون النظر إلى المخلفات والنتائج المضرة بالغير (معنوية ومادية)، أما عن الفاعل (مرتكب الجريمة) فإنه ذوي كفاءات ومهارات عضلية تقنية عالية، وذو ملكة معلوماتية تعطيه الفرصة مع القدرة للتمكن من التحايل في اختراق البيانات السرية بطريقة سلسلة نوعاً ما بغية الحصول على معلومات مجانية.

أو مخلصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشبية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار¹.

¹ - دحلوز محمد، النصب والاحتيال على المواقع الالكترونية وسبل مواجهتها، مذكرة لنيل شهادة الماستر، جامعة عبد

الحميد بن باديس، مستغانم، 2022-2023، ص20.

أما عن جريمة الاحتيال الالكتروني فإنها تحمل نفس المفهوم الذي تناولناه فقط الفرق بينهما وبين جريمة الاحتيال سابقة الذكر أن الاحتيال الالكتروني يتم بوسيلة أخرى وسيلة حديثة يتم بموجبها تنفيذ الجريمة والمتمثلة في الحاسب الآلي بالإضافة إلى توافر شبكة الإنترنت التي تعتبر جوهر وأساس هاته الجريمة، إذ بدون الشبكة العنكبوتية لا يكون هناك وجود الاحتيال الالكتروني ويندرج تعريفها تحت تعريف الاحتيال الالكتروني.

❖ تجريم الاحتيال الالكتروني:

عادة في سرقة بيانات وأرقام وسائل الدفع الالكتروني خاصة بطاقة الدفع من طرف المجرمين وقرصنة المعلوماتية ولخطورة هذه العملية من شأنها أن تقع على المستهلك عند قيامه بالمواقع على طلب شراء سلعة أو خدمات عبر شبكة الإنترنت¹.

كما حذرت بعض التشريعات المقارنة على هذا الاعتداء وجرمته واعتبرته جريمة احتيال وقد تناول الموضوع التشريع الفيدرالي المعروف ب CFAR في المادة (2/a/1030) والتي تعاقب كل من يصل عمداً وبدون ترخيص أو يتجاوز الترخيص الممنوح له من أجل الحصول على بيانات أو معلومات واردة في سجل مالي لمؤسسة المالية أو المصدر البطاقة، كما هو منصوص عليه في المادة (1/1607) من الفصل 15 من هذا القانون². وغيره من التشريعات التي جرمته ونصت عليه في قوانينها وحذرت لشدة خطورتها خاصة سرقة واستعمال أرقام هذه البطاقات الالكترونية لسد قيمة السلع

¹ - لجلط فواز، المرجع السابق، ص196.

² - لجلط فواز، المرجع نفسه، ص196.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

والاستفادة من الخدمات عبر الإنترنت التي تم تجريمها من قبل المشرع الجنائي الفرنسي من خلال نص المادة 1/313.

- تجريم استخدام أو الحصول على أرقام وبيانات وسائل الدفع الالكتروني:

لجأت بعض التشريعات لتجريم استخدام أو الحصول على أرقام وبيانات وسائل الدفع الالكتروني عن طريق شبكة الإنترنت أو أي وسيلة من وسائل تقنية المعلومات بدون وجه حق، وما ذلك إلا حماية لوسائل الدفع حيث أن الحماية لا تحقق إلا بتوفر الأمان والثقة في استخدامها ومن بين التشريعات التي جرمت هذه العملية نذكر منها:

التشريع الإماراتي الذي نص عليها في نص المادة 12 المتعلقة بمكافحة جرائم تقنية المعلومات من المرسوم الاتحادي رقم 05 لسنة 2021، كما جرم المشرع القطري فعل الاستعمال العتيق باستخدام أو الحصول على أرقام وبيانات بطاقات الدفع كبطاقة الائتمان عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في نص المادة 12 من القانون 14 لسنة 2014، والمتعلق بمكافحة الجرائم الالكترونية¹.

ويعتبر تجريم استخدام أو الحصول على البيانات والأرقام الخاصة بأي وسيلة من وسائل الدفع الالكتروني بدون وجه حق ما هو إلا نتيجة تطبيق هذه الدول -سابقة الذكر- للقانون العربي الاسترشادية للمعاملات والتجارة الالكترونية، والذي نص على تجريم ذلك في نص المادة 44 منه، وترك تحديد العقوبة لمشرعي الدول العربية المنظمة إلى هذه الاتفاقية². وبما

¹ - لجلط فواز، المرجع السابق، ص197.

² - لجلط فواز، المرجع نفسه، ص197.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

أن الجزائر ضمن الدول التي صادقت على الاتفاقية العربية المختصة لمكافحة جرائم تقنية المعلومات، فقد قامت هي أخرى بدورها بتجريم الاستيلاء على بيانات أي أداة من أدوات الدفع أو استخدامها بعنف والاستفادة منها بطرق غير شرعية كتقديمها لغير حاملها أو تسهيل للغير التصرف بها أو الحصول على بياناتها ومعلوماتها وهذا ما تناوله المشرع الجزائري في الفقرة الثانية من المادة 18 ليس هذا فقط بل جرمت استخدام الشبكة المعلوماتية ووسائل تقنية المعلومات بهدف الوصول لأي من المعلومات أو البيانات والمعطيات المتعلقة بأي أداة من أدوات الدفع الالكتروني وهذا ما ورد في الفقرة الثالثة من المادة 18.

لكن ما لا يمكن تجاوزه أن المشرع الجنائي الجزائري لحد الساعة لم يفرع هذه الاتفاقية في القانون الداخلي يحدد عقوبة هذه الجرائم، مما يجعل القاضي أثناء تطبيقه يصطدم بمبدأ الشرعية الجنائية للعقوبة¹.

الفرع الثاني: الحماية الجنائية غير المباشرة

تتمثل الحماية غير المباشرة لوسائل الدفع الالكتروني في تدخل مختلف التشريعات لفرض حماية جديدة للمستخدم في إطار اقتناء للسلع أو استفادته من خدمات غير شبكة الانترنت حيث تتعلق هذه الحماية بتجريم الاعتداء على بيانات المواقع والوسائل الدفع وتجريم الاعتداء على المواقع الالكترونية وهذا ما سنفصل فيه في هذا الفرع على النحو الآتي:

¹ - لجلط فواز، نفس المرجع، ص 197.

أولاً: تجريم الاعتداء على نظام المواقع الالكترونية:

إن الاعتداء على نظام المواقع الالكترونية و الدفع الالكتروني قد كان اهتمام العديد من التشريعات التي تدخلت بهدف فرض حماية مستحدثة للمستهلكين، حيث نصت بعض التشريعات المقارنة على تجريم سلوك الاعتداء المذكور كما تجريم الدخول المتعمد والبقاء بطريقة غير شرعية في نظام المواقع الالكترونية وبما أننا بصدد الحديث على مكافحة هذا النوع من الجرائم في التشريع الجزائري فإن المشرع الجزائري قد نص على تجريم الاعتداء على نظام الدفع الالكتروني في نص المادة 394 مكرر، والتي تعاقب كل من يدخل عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يعادل ذلك¹.

نلاحظ من خلال نص المادة أن المشرع اعتبر كل دخول إلى نظام معلوماتي لموقع الكتروني أو جزء منه يعتبر جريمة ويعاقب عليها القانون ومن هنا نستنتج بأن الدخول إلى أي نظام معلوماتي بدون رخصة أو تصريح بغض النظر عن الطريقة التي تتم الدخول بها سواء تم الدخول إلى النظام أو جزء منه ولا يشترط تحقق النتيجة فيها حيث تعتبر من جرائم السلوك المحض، وهذه الحلة تمثل جريمة الدخول غير المرخص في صورتها البسيطة، أما إذا أدى فعل الدخول أو البقاء إلى حذف أو تغيير في المعطيات أو تخريب النظام في المعلوماتي للموقع الالكتروني فإن المشرع الجزائري قد وفر الحماية الجنائية للمواقع

¹ - لجلط فواز، المرجع السابق، ص 198.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

الالكترونية من خلال تجريم أفعال التغيير أو التخريب للمعطيات وبيانات هذه المواقع الالكترونية¹.

ثانيا: تجريم الاعتداء على بيانات المواقع الالكترونية

إن الاستخدام غير المشروع لبيانات المواقع الالكترونية يعتبر اعتداء عليها والاعتداء بصفته تصرف عنيف فقد اعتبر جريمة محض، تترتب عليها عقوبات قانونية، حيث أن المشرع الجزائري نص على تجريم الاعتداء على بيانات المواقع الالكترونية

المطلب الثاني: الهيئات المكلفة بمواجهة الجريمة المعلوماتية في الجزائر

تختلف جرائم الحاسوب الآلي عن باقي الجرائم التقليدية خاصة فيما يتعلق بالتحقيق وجمع الأدلة فمنها جريمة النصب المعلوماتي التي تختلف في صورتها في جرائم النصب المعتادة، بأنها أكثر خطورة منها مما استوجب على السلطات العليا الهيئات المختصة بالتحقيق الدقيقة والواسع الملم بمعطيات الحاسوب وطبيعته وتشغيله حيث يتعين على المحقق معرفة بيئة الحاسوب والإنترنت وجمع المعرفة الكافية المتعلقة بمسائل التفتيش والضبط وكشف الأدلة والتحفظ عليها.

كما أن من سمات جرائم الحاسوب التي تميزها عن غيرها بأنها تنشأ في الخفاء ويعتمد الاعتداء فيها على معطيات الحاسوب المخزنة والمعلومات التي تنتقل عبر نظم شبة

¹ - لجلط فواز ، المرجع نفسه، ص198.

الفصل الثاني: الجريمة الإلكترونية في التشريع الجزائري

الإنترنت ونظراً لكثرة استخداماتها والأساليب الحديثة والمنظورة الناتجة عن الغزو المعلومات والتطور التكنولوجي فيكون الإجرام ضد الأشخاص أيضاً¹:

وعليه أدرك المشرع الجزائري جيداً بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية والتي من شأنها أن تجنبنا وقوع الجريمة الإلكترونية. أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها²، هذا إضافة إلى الهياكل والهيئات المكلفة بمواجهة جريمة المعلوماتية في الجزائر التي لعبت هي الأخرى دوراً مهماً في الحد من هاته الجرائم ومكافحتها وهذا ما سيكون محلاً لدراستنا من خلال تقسيم مطلبنا إلى فرعين حيث تحدثنا في الفرع الأول عن الهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بينما الفرع الثاني فقد تناولنا فيه التدابير الوقائية المستحدثة وهذا على النحو الآتي:

¹ - خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2011، ص184.

² - عقباش فريزة ومبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2021-2022، ص38.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

الفرع الأول: الهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نظرا للانتشار السريع لظاهرة المعلوماتية من يوم لآخر وبالاضطلاع على الطبيعة الخاصة التي تميز هذه الجرائم فإن معظم الدول سعت لاستحداث وحدات خاصة لمواجهة الجريمة الالكترونية.

الأمر نفسه سعت له الجزائر، حيث تم تسخير هيئات ووحدات مختصة أهمها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، تم إنشاء هذه الهيئة في الجزائر بموجب المادة 13 من القانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹.

حيث نصت المادة المذكورة على: "تتشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"².

ومن خلال هذه الجزئية من دراستنا سوف نحاول التطرق للتعرف على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهذا على النحو الآتي:

¹ - عقباش بريزة ومبارك حنان، المرجع نفسه، ص44.

² - مهداوي حنان، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة محمد الأمين دباغين، سطيف2، المجلد6، العدد2، 2022، ص1072.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

أولاً: تنظيم الهيئة وتشكيلها وكيفية سيرها:

قام المشرع الجزائري من خلال نص المادة 3 السالف الذكر إحالة بخصوص تشكيلة الهيئة وتنظيمها والمنهج الذي تسير عليه نحو التنظيم، وهو فعلاً ما قام به المشرع في وقت لاحق من خلال المرسوم الرئاسي 172/19 بعد أن كانت تخضع لأحكام المرسوم الرئاسي رقم 261/15 والملغى بموجب المرسوم 172/19 اعتبر من خلاله المشرع الجزائري الهيئة مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلال المالي، نوضع تحت سلطة وزارة الدفاع الوطني¹.

أم في تنظيم الهيئة وتشكيلها فقد أشارت المادة 4 من المرسوم الرئاسي 172/19 بأن الهيئة تتشكل من مجلسين:

- مجلس توجيه ومديرية عامة (مجلس إداري).
- مجلس التوجيه (مجلس بشري).

كما تشير المادة سابقة الذكر إلى أن الهيئة تتشكل من الوزارات التالية: الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية².

¹مهداوي حنان، المرجع فسه، ص1072/1073.

² - مهداوي حنان، المرجع نفسه، ص1073.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

أ- **الجهاز الإداري:** تتكون الهيئة من مجلس التوجيه والمديرية العامة، يوضعان تحت السلطة مباشرة لرئيس الجمهورية ويقدمان له عرضه عن نشاطاتهما وفق ما نصت عليه المادة 5 من هذا القانون.

- أ. **1 مجلس التوجيه:** لقد نصت المادة 6 حيث أشارت بأنه يتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه الذي يتشكل هو الآخر من الأعضاء الآتية ذكرهم:
- الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج.
 - الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية.
 - الأمين العام لوزارة العدل.
 - الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية.
 - قائد الدرك الوطني.
 - المدير العام للأمن الداخلي.
 - المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي.
 - المدير العام للأمن الوطني.
 - رئيس مصلحة الدفاع السبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي.
 - مراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي .
 - ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية.
 - المدير العام للهيئة أمانة مجلس التوجيه.

أ- 2 المديرية العامة:

بموجب نص المادة 9 فإن المديرية العامة يديرها مدير عام يتم تعيينه بموجب مرسوم رئاسي، وتنتهي مهامه حسب نفس الأشكال، كما تعد وظيفته وظيفة عليا في الدولة وتنظم المديرية العامة كل من:

- مديريات ومصالح وملاحق حسب نص المادة 11 وفقاً لما يلي: "مديرية المراقبة الوقائية واليقظة الالكترونية، مديرية الإدارة والوسائل، مصلحة الدراسات والتلخيص، مصلحة التعاون واليقظة التكنولوجية، ملحقات جهوية¹.

وبموجب قرار الأمين العام لرئاسة الجمهورية بناء على اقتراح من المدير العام للهيئة فقد تم تحديد النظام الداخلي لهياكل الهيئة، كما جاء في نص المادة 13.

ب) الجهاز البشري:

هناك مستخدمين وأفراد آخرين إضافة على موظفي الدولة، للذين يشغلون وظائف عليا في الهيئة والموظفين، نصت عليهم المواد 20، 21، 20 يساهمون في سير الهيئة. حيث جاء في نص المادة 20 لسير الهيئة يلحق بها:

- قضاة وذلك وفقاً للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول.

¹-عقباش بريزة ومبارك حنان، المرجع السابق، ص 47.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

- ضباط وأعوان الشرطة القضائية مؤهلون من المصالح العسكرية الأمن والدرك الوطني والأمن الوطني، الذين يحدد عددهم بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمن العام للرئاسة¹.
 - كذلك مستخدمو الدعم التقني والإداري للمصالح والعسكرية للأمن المختصة والدرك الوطني والأمن الوطني، كما أن المادة 21 من نفس المرسوم رخصت الهيئة بتوظيف فئات أخرى من المستخدمين حسب حاجاتها إلى ذلك كما نصت المادة 32 على إمكانية الاستعانة بموظفين مختصين من الوزارات المعنية بمجال تكنولوجيات الإعلام والاتصال أو أي شخص آخر سواء خبير أو شخص عادي قادر على المساعدة في العمل².
- أما بخصوص كيفية سير عمل الهيئة، فتتص المادة 7 من المرسوم 172/19 على أن مجلس التوجيه يجتمع في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضرورياً بناءً على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة³.

¹-عقباش بريزة ومبارك حنان، المرجع السابق، ص46.

²-عقباش بريزة ومبارك حنان، المرجع السابق، ص46.

³-مهداوي حنان، المرجع السابق، ص1073.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

ثانيا: مهام الهيئة

تنص المادة 14 من القانون 04/09 تحت رقابة السلطة القضائية طبقاً لأحكام قانون الإجراءات الجزائية وكذا القانون 4/09، وجدت المادة 14 مهام الهيئة وصلاحياتها¹ وهي على النحو الآتي:

. I. المهام الحصرية للهيئة:

تتنوع مهام الهيئة الوطنية بين ما هو استشاري وبين أنها هيئة تحري ومرصد لاستجماع وتسجيل وحفظ المعطيات الرقمية وهي مساعدة الجهاز القضاء والضبط الإداري إضافة إلى ذلك تعتبر هيئة تكوينية للمحققين المتخصصين في مجال التحريات التقنية المرتبطة بتكنولوجيا الإعلام والاتصال.

. II. مهام عامة وأصلية للهيئة:

تتمثل مهام الهيئة الوطنية في تنشيط وتنمية الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مساواة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية² الأمر الذي نصت عليه المادة 14 فقرة ب من القانون 04/09.

¹ - مهداوي حنان، المرجع السابق، ص 1073.

² - عقباش بريزة ومبارك حنان، المرجع السابق، ص 47.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

زيادة على ذلك تقوم الهيئة بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية وذلك بإذن من السلطات القضائية ويهدف الكشف عن أي جريمة متصلة بتكنولوجيا الإعلام والاتصال وكذا جمع ومركزة واستقلال كل المعطيات والمعلومات التي تسمح بالكشف عن الجرائم الالكترونية مع مكافحتها وحفظها.

هذا بالإضافة إلى تزويد مصالح الشرطة والسلطات القضائية تلقائيا أو يطلب منها بالمعطيات والمعلومات التي تتعلق بالجرائم الالكترونية.

القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية باستثناء ذلك التابعة لوزارة الدفاع الوطني وهذا من خلال عمل مديرية الرقابة الوقائية واليقظة الالكترونية¹.

ج) المهام العامة للهيئة:

تتمثل في:

- تطوير التعاون مع المؤسسات والهيئات الوطنية التي تختص في نفس المجال.
- العمل على جمع وتسجيل وحفظ البيانات والمعطيات الرقمية مع تحديدها وتحديد مصادرها ومساراتها بهدف استعمالها في الإجراءات القضائية وهذا لمساعدة السلطات القضائية ومصالح الشرطة القضائية.

¹-عقباش بريزة ومبارك حنان، المرجع السابق، ص47.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

- اقتراح عناصر الإستراتيجية الوطنية وتنشيط وتنسيق عمليات ومكافحة للوقاية من الجرائم الالكترونية.

.III على المستوى الدولي:

تتمثل مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في:

- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والتعرف عليهم¹.
- اتخاذ كل الإجراءات التحفظية وتبادل المعلومات والمعطيات وفقا للاتفاقيات الدولية التي لها علاقة وصلة بالاتفاقيات الدولية الثنائية ومبدأ المعاملات بالمثل².

وفي الأخير ما يمكن استنتاجه من خلال دراستنا لمهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال نلاحظ أن مضمون المادة 14 جاء بصيغة العموم. غير مفصل لمهام الهيئة، الأمر الذي دفع المشرع إلى تفصيل مهامها في المرسوم 172/19 وتقسيمها بين مجلس التوجيه والمديرية العامة للهيئة، حيث تولى المشرع تفصيل هذه المهام في المواد 6، 9، 11، 13، 14 من المرسوم 172/19³.

¹- عقباش بريزة ومبارك حنان، المرجع السابق، ص48.

²- بدرة إبراهيم لعور الأمن الالكتروني وفقا للتشريع الجزائري، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال نموذجا، ص264.

³- مهداوي حنان، المرجع السابق، ص1073.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

الفرع الثاني: إجراءات التحري المستحدثة للكشف عن جرائم المعلوماتية

جاء قانون الإجراءات الجزائية الجزائري في إطار تعديله بقانون 22/06 المؤرخ في 2006/12/20 بجملة من الإجراءات المستحدثة بهدف الكشف عن الجرائم التي تمس أنظمة المعالجة للمعطيات و الحد منها وتتمثل هذه الإجراءات فيما يلي:

أولاً. الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أعطى المشرع الجزائري الإمكانية لضباط الشرطة القضائية الصلاحية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة¹.

أما في إتقاط الصور فعادة يكون عن طريق إتقاط صورة لشخص أو مجموعة من الأشخاص ويتم انتهاج هذه الوسيلة في الأماكن العامة والخاصة والمحلات السكنية أما فيما يخص تسجيل الأصوات فيتم من خلال وضع رقابة على الهواتف وتسجيل المحادثات التي تتم من خلالها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو

¹ - يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار المادة 2 من القانون رقم 04/09 المؤرخ في 05 أوت يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتجددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

إذاعية¹، والمهم في الأمر أن هذه الإجراءات يمكن لها المساس بالحرية الشخصية، خاصة إذا علمنا أن سرية المراسلات هي إحدى الحقوق المنصوص عليها في الدستور، فقد جاء في نص المادة 03 من القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها².

حيث تنص بأنه: "كل مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية³، وما هو معروف أيضا ن كل متهم بريء حتى تثبت إدانته لذلك فإنه من غير المعقول إثبات اتهام من مشتبه فيه استنادا على وسيلة التسجيل الصوتي أو التقاط الصور أو افتراض مراسلات سواء كان ذلك في الأماكن العامة أو الخاصة، خاصة وأن مثل هذه الطرق والوسائل المتخذة كإجراءات لا تولي مساساً بالمتهم فحسب، بل كذلك بالمحيطين به أقارب كانوا أو معارف هذا ما تم الإختلاف حول مدى

¹- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012، ص126.

²- حسن صادق المصفاوي، المصفاوي في التحقيق الجنائي، ط2، منشأة المعارف، الإسكندرية، مصر، 1990، ص78.

³- يقصد بالمعطيات المعلوماتية في إطار المادة 2/ج من القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أي عملية عرض الوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

صحته حيث أن الفقه يفرق بين مصطلحين وضع الخط الهاتفي تحت المراقبة وبين اعتراض المكالمات الهاتفية فبينما يكون الأول برضا أو بطلب من صاحب الشأن وبخضوع لتقدير الهيئة القضائية بعد تسخير مصالح المواصلات والبريد لذلك، فإن الثاني يكون دون رضا المعني.

ويعد هذا النوع من الإجراءات الحديثة من أهم الإجراءات التحقيق، حيث أعطى المشرع لضابط الشرطة القضائية إمكانية ممارسته للكشف عن الجرائم المحددة على سبيل الحصاد وذلك في المادة 65 مكرر 6 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضائع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية¹.

غير أنه نجد أن المشرع حاول التوفيق بين هذه الاختلافات المتعارضة حيث قام بإجازة هذه الأساليب لكن بشرط الالتزام بضوابط وشروط والمتمثلة في:

- مباشرة التحري بإذن من وكيل الجمهورية المختص والتزام أعوان وضباط الشرطة القضائية القائمين بإجراء السر المهني².

¹- عمار حشمان، المرجع السابق، ص55.

²- عمار حشمان، المرجع نفسه، ص55.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

ورغم إقرار المشرع لأساليب التحري الخاصة وإجازتها غير أنه يعاقب كل من يحاول استغلالها أو استعمالها بعنف وبطرق غير مشروعة وفيما يلي سوف نتطرق لشرح كلا الضابطين على النحو الآتي:

أ) مباشرة التحري بإذن من وكيل الجمهورية:

لقد حصر المشرع الجزائري التصريح بإجراء اعتراض لمراسلات وتسجيل والتقاط الصور سواء في أماكن عامة أو خاصة بهدف التحري والتحقيق حول ما يخص جرائم المساس بأنظمة المعالجة الآلية للمعطيات فقط بإذن وكيل الجمهورية المختص، هذا الأخير هو الوحيد الذي يملك الصلاحية في تصريح بإتمام إجراءات التحقيق، بحيث تباشر هذه العمليات تحت المراقبة وهذا ما ذكرته المادة 04 من القانون 04/09 الذي جاء فيه أنه: " لا يجوز إجراء عمليات لمراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة¹."

والإذن في حد ذاته يجب أن يتوفر على جملة من العناصر التي تسمح بالتعرف على مكالمات والاتصالات المطلوب النقاطها والتحري عنها وحتى الأماكن المقصودة سواء كانت سكنية أو غير سكنية.

¹ - المادة 303 مكرر من الأمر رقم 156/66 معدلة ومتممة بموجب المادة 33 من القانون 23/06 المؤرخ في 20

ديسمبر 2006.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

إضافة إلى ذلك يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير¹ لهذا فإن التصريح الصادر من وكيل عن وكيل الجمهورية والإذن المسلم من قبله من أجل التحقيق في الجريمة ما لا يصلح للتحقيق في الأخرى إلا بتسليم إذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوه به بصفة خاصة من شخص أو عدة أشخاص²، وعند الشروع في التحريات، يقوم ضابط الشرطة القضائية الذي تم له الإذن من قبل القاضي المختص بتحرير محضر عن كل عملية تسجيل الأصوات والتقاط صور و اعتراض للمراسلات، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها³.

ومن ميزات المحضر أنه شامل لكل البيانات المذكورة سابقاً وبطريقة محددة بحيث يكون التحديد نافياً للجهالة، بشرط أن يشتمل المحضر على توقيع من الشخص الذي حرره في نهايته.

وبعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في

¹ - المادة 65 مكرر 7 الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

² - عمار حشمان، المرجع السابق، ص56.

³ - المادة 65 مكرر 9 الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

محضر يودع بملف المتهم، وتنتسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الإقتضاء، بمساعدة مترجم يسخر لهذا الغرض¹.

(ب) إلتزام السر المهني: تتميز إجراءات التحري والتحقيق بالسرية، السرية هنا معناها القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كانت عليه من قبل هو تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية².

لقد نص المشرع الجزائري بنص صريح بأن هذه العمليات تتم بمراعات السر المهني ودون المساس به³، فالضباط المأذون لهم باعتراض المراسلات وتسجيل الأصوات والنقاط الصور ملزم قانوناً بكتمان السر المهني ويجب أن يتخذ مقدماً التدابير اللازمة لضمان احترام ذلك السر الأمر نفسه أقر به قانون الإجراءات الجزائية بأن تتم عملية التحريات بسرية⁴. وبالتالي فإن كل شخص يقوم بعملية التحري يستوجب عليه الإلتزام بكتمان السر المهني لذلك فإن عملية التحري عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات تتم بسرية مطلقة⁵، حيث يمنع قطعاً أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على

¹ - عمار حشمان، المرجع السابق، ص 57.

² - عمار حشمان، المرجع نفسه، ص 57.

³ - المادة 65 مكرر 7 الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

⁴ - المادة 3/45 من الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

⁵ - عمار حشمان، المرجع السابق، ص 57.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومروسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهدد ببيانات غير مؤكدة¹.

ثانيا: أسلوب التسرب والاختراق

يعتبر الاختراق والتسرب إحدى التقنيات الجديدة التي أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة² ويشترط بالتسريب الحصول على الإذن من وكيل الجمهورية المختص، والعملية يجب أن تتم تحت مراقبته و إشرافه، فإن قرر ضابط الشرطة القضائية مباشرة هذا الإجراء وجب عليه أولاً إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه³، وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوباً يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

¹ - عمار حشمان، المرجع نفسه، ص57.

² - المادة (65 مكر 11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (19) من القانون رقم 22/06.

³ - محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، ط2، الجزائر، 2009، ص115.

الفصل الثاني: الجريمة الالكترونية في التشريع الجزائري

أما عن التسرب فهو معروف بعملية يقوم بها ضباط وأعوان الشرطة حيث يقوم العناصر المذكورة تحت لا مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم¹، وبالتالي فهو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم الجريمة أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم².

¹ - المادة (66مكرر7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

² - عمار حشمان، المرجع السابق، ص58.

الخاتمة

الخاتمة:

توصلنا من خلال دراستنا بأنه نتيجة لظهور التطور التقني إنتشاره السريع الذي غزى العالم بأكمله وأحاط به من جميع جوانبه، ونتيجة لظهور ما يعرف بالكمبيوتر والحواسيب الآلية وانتشار المعلوماتية وعولمتها فقد أصبحت جزء لا يتجزء من الاحتياجات والضروريات اليومية في شتى المجالات حيث أصبحت تعتبر المحرك الرئيسي في التطورات الحديثة، وما هو معلوم لكل شيء جانبيين من الإيجابية والسلبية فبالرغم مما تحمله تكنولوجيا الإعلام والاتصال من الايجابيات وتسهيلات في المعاملات والتبادلات التجارية والمالية وغيرها إلا أنها تحمل في طياتها ثغرات بالغة العمق وسلبيات جد خطيرة مهددة لسلامة وأمن المستخدم خاصة أنها تستعمل من قبل شتى الفئات العمرية والمراقبة عليها ليست بالأمر الهين نتيجة سرعة حركتها وإنتشارها الواسع عبر العالم. حيث أنه في هذا الوسط من الحداثة والتطور تم ظهور العديد من الجرائم والتصرفات غير الشرعية خاصة فيما يخص المعاملات والمبادلات النقدية الالكترونية والدفع الالكتروني اللذان ظهرتا نتيجة التطور العلمي والتكنولوجي.

ومن أهم هذه الجرائم الحديثة والمتنامية نذكر الجرائم الالكترونية والأجرام المالي والاحتيال الالكتروني الذي أصبح يهدد أمن وسلامة الملكية المالية والشخصية للمستخدمين وبل إنه يمس بالاقتصاد العالمي والوطني على حد سواء، بل أدى بظهور جرائم مالية الكترونية لم يسبق لها مثيل في العالم والجرائم الالكترونية يرتبط وجودها بالتكنولوجيا والمعلومات والحواسيب الآلية وتعتبر من أخطر المعاملات والتهديدات التي تمس بالملكية المالية والأموال النقدية وذلك كما ترتبه من آثار حادة.

بما أنها ظاهرة عالمية فإنها حتماً مست بالعالَم العربي بصفة عامة والمجتمع الجزائري بصفة خاصة، فموضوع الأموال الإلكترونية يعد من أهم المواضيع العصرية لما أثاره من اشكالات وصعوبات قانونية خاصة في حوَل العالم الثالث، كونه كما ذكرنا ينصب على نوع من الجرائم المستحدثة، الأمر الذي أظهر قصوراً في النصوص الجنائية التي عانت بدورها من عجز حاد عن ضمان الحماية اللازمة والفعالة لما أفرزته ثورة الاتصالات.

وبالرغم من أن المشرع الجزائري كما ظهر من خلال دراستنا للموضوع أنه أسس منظومة تشريعية ومؤسسية للتصدي ومواجهة الجريمة الإلكترونية غير أن الظاهرة هذه لازالت في انتشار رهيب ومخيف لا يوجد للقانون قدرة على مواكبته وهذا سبب الرقمنة والتطورات الحديثة للآليات الإلكترونية والتقنية.

كما أن المشرع قد سعى لتدارك الفراغ التشريعي الذي وقع فيه بخصوص مكافحة الجرائم المعلوماتية، حيث قام بإدراج تعديلات خاصة على قانون العقوبات الجزائري ونص بقوانين خاصة متعلقة بالوقاية من الجرائم المستحدثة المتصلة بتكنولوجيات الإعلام والاتصال وكافحتها وهذا ما جاء في قانون رقم 04/09، وذلك محاولة منه للتقليص من هذه الجرائم المستحدثة والعبارة للحدود.

من خلال دراستنا السابقة للموضوع فإننا نستنتج في الأخير بعض النتائج وهي كالآتي:

- تعتبر الأموال الإلكترونية وسيلة من وسائل الدفع الجديدة وتمثل إحدى المراحل المتقدمة من مراحل التطورات في المالية، وذلك لأنها أصبحت تحل محل النقود التقليدية وهذا ما يميزها عن غيرها إذ أنها توفر لحاملها فرض للتخلص من الجهد والاختصار في الوقت

- غير أنه ما تحمله هذه النقود من مزايا وإيجابيات لا يمنحها الكمالية والمثالية إذ أنها تعاني من ثغرات عديدة أثارت العديد من الإشكالات القانونية.
- نظرا لسرقة انتشار المعلوماتية والأموال الالكترونية نجد بأن هذه الأخيرة لازالت تحمل غموضا كبيرا وبقيت مبهمة خاصة وأن سر حداثتها لا تتوافق مع سرعة القوانين لأمر الذي جعلها خطيرة نوعا ما ويصعب على قانون العقوبات مسايرتها.
 - نلاحظ بأنه رغم سعي المشرع في محاربة ومكافحة هذا النوع من التهديدات والجرائم الالكترونية والمالية إلا أنه يوجد قصور كبير في نصوص التشريع الجزائي التقليدية خاصة عن الإحاطة بجوانب الجرائم الواقعة على الأموال الالكترونية خاصة وأن هذه الأخيرة تختلط كليا على الجرائم التقليدية الأخرى.
 - لقد أخذت جرائم الاحتيال الالكتروني التي أكتشفت حديثا العديد من الأشكال و سيناريوهات مختلفة إلا أنها تشترك في طريقة التنفيذ والآلية المعتمدة في ارتكابها جريمة الاحتيال الالكتروني حيث يتم الاتصال بالمجني عليه -الضحية- بواسطة البريد الالكتروني بدون سابق إنذار وبدون وجود أي اتصالات سابقة.
 - خطورة الجرائم الالكترونية جعلت الدول تتسارع لإيجاد حلول قانونية ردعية للحد من انتشار هذه الجريمة مع توفير تنمية بشرية للوقاية من مظاهر وتأثيرات هذه الجرائم على الأمن العام وكذلك حماية المستخدمين والعملاء من خطورتها.
 - عدم إقرار المشرع الجزائري نصوص قانونية خاصة بالجرائم الالكترونية هذا بالإضافة إلى افتقار الاجتهادات القضائية المعنية بالأمر.
 - إحداث المشرع الجزائري تعديلات في قانون العقوبات وقانون الإجراءات الجزائية 15/04 واستحداث قانون 04/09 لمكافحة هذه الجريمة غير أن هذا ليس بالكافي نظرا لسرعتها وحداثتها التي لا يمكن للقانون مواجهتها ما جعلها في تزايد مستمر.

أما بالنسبة للاقتراحات التي يمكن تقديمها فهي كالآتي:

- إن جريمة الاحتيال الإلكتروني جريمة دولية فإنه يجب وبشكل مستمر توعية المستخدمين والناس عامة ورجال الأعمال وغيرهم بمدى خطورة الاستجابة لهذه الأمور من رسائل إلكترونية مع البعد عن الطمع في مكاسب لا يمكن تحقيقها أبدا جراء الانسياق في مثل هذا النوع من جرائم الاحتيال الإلكتروني.
- ضرورة توفير ركيزة متينة من قوانين وهيئات لحماية الأموال الإلكترونية من مثل هذه الجرائم وذلك صيانة لها من التعدي عليها، خاصة توفير الحماية الجنائية.
- ضرورة اهتمام المؤسسات المالية والبنوك المصدرة لبطاقات الأموال الإلكترونية والشركات التجارية والتي تتعامل بها بالوقوف على كل صور الاستخدامات غير المشروعة والتعاملات التعسفية لها وتدريب العاملين فيها وتمكينهم على مستجدات هذا المجال.
- ضرورة نص القوانين وإفراد نصوص خاصة تنظم عمليات التعامل بالأموال الإلكترونية، وتسلب الضوء على كل جريمة أو سلوك غير قانوني يمس بها وتصنف كل جريمة على حدى وهذا استنادا لمبدأ شرعية الجرائم والعقوبات بحيث تجاري التطور العلمي والتقني وتتوافق مع التحديات والمستجدات المستمرة.
- قيام الهياكل والهيئات بالوقاية من هذه الجرائم بدورها على أتم وجه والحرص على إبلاغها القطب الجزائري الوطني بالأفعال المشتبه فيها.
- ضرورة تكوين قضاة مختصين في جرائم تكنولوجيات الإعلام والاتصال مع إنشاء مراكز متخصصة لدراسة هذا النوع من الجرائم.

وفي الأخير نرجو أن ينال بحثنا هذا رضاكم ونكون قد تعرضنا للموضوع عرضاً شاملاً وافياً بالغرض فإن أصبنا فله المنة وإن أخطئنا فالعصمة من شأن الرسل.



قائمة
المصادر
والمراجع

النصوص القانونية:

القوانين والأوامر:

المادة (65 مكرر 11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (19) من القانون رقم 22/06.

المادة (66 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

المادة 303 مكرر من الأمر رقم 156/66 معدلة ومتممة بموجب المادة 33 من القانون 23/06 المؤرخ في 20 ديسمبر 2006.

المادة 3/45 من الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

المادة 65 مكرر 7 الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

القانون 04/09 وقانون العقوبات في المواد 394 و 394 مكرر 7.

قانون رقم 04/09 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، العدد 74.

المادة 65 مكرر 9 الأمر رقم 155/66 المعدل والمتمم بموجب المادة 14 من القانون رقم 22/06.

الكتب:

الكتب العامة:

1- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، ط2، الجزائر، 2009.

2- أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، حق الملكية، الجزء الثاني، دار إحياء التراث العربي، بيروت، 1952.

- 3- حسن صادق المصفاوي، المصفاوي في التحقيق الجنائي، ط2، منشأة المعارف، الإسكندرية، مصر، 1990.
- 4- عبد الكريم الردايدة، جرائم بطاقات الائتمان لدراسة تطبيقية ميدانية، الطبعة الأولى، الأردن، دار حامد، 2013.
- 5- مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الإرهاب الإلكتروني المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ط1، 2014.
- 6- خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2011.

الكتب الخاصة:

- 1- أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، 2007.
- 2- عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، الأردن، ط2، 2014.
- 3- نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الانترنت، دار نور للنشر، د.ط، الاسكندرية، 2017.
- 4- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجيستر في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012.
- 5- محمد العبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، مصر، 2009.
- 6- أسامة أحمد المناعة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان، 2014.
- 7- أمال قارة، الحماية الجزائرية المعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر، (د.ط)، الجزائر، 2006.

- 8- بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر.
- 9- جلال محمد الزعبي وأسامة أحمد المناعة، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، 2010.
- 10- حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
- 11- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر والتوزيع، الجزائر، ط1، 2008.
- 12- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار النشر والتوزيع، ط1، عمان، 2011.
- 13- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، (د ط)، الاسكندرية، 2019.
- 14- شفيق حسنين، الإعلام الجديدة والجرائم الإلكترونية، دار الفكر وفن للطباعة والنشر والتوزيع، (د.ط)، (د،ب،ن)، 2015.
- 15- شمس الدين إبراهيم أحمد، وسائل الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دار النهضة العربية، ط1، القاهرة، 2005.
- 16- طارق عفيفي صادق أحمد، الجرائم الالكترونية جرائم الهاتف المحمول، د د ن، مصر ط1، 2015.
- 17- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت دراسة متعمقة في جرائم الحاسب الآلي و الإنترنت، بهجات للطباعة والتجليد، (د.ط)، مصر، 2009.

- 18- عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، 2009.
- 19- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، (د.ط)، بيروت، 1999.
- 20- علي عدنان الفيل، المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الالكتروني، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان 2011.
- 21- غنية باطلي، الجريمة الالكترونية، دار الجزائرية للنشر والتوزيع، (د.ط)، بيروت، 2015.
- 22- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة والتزيع، ط1، عمان، 2009.
- 23- محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، (د.ط)، القاهرة، 1984.
- 24- محمد حماد مرهج الهيتي، الحماية الجنائية لبطاقة الائتمان الممغنطة، دون طبعة، دار الكتب القانونية، 2014.
- 25- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، الجزء الثاني، وزارة الداخلية "الأكاديمية الملكية للشرطة"، البحرين، مارس 2010.
- 26- يوسف عبد النبي شكري، المعلوماتية وأزمة الشرعية، (د.ذ.د.ن)، الكوفة، (د.ذ.ط)، 2008.
- 27- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط2، عمان، 2010.
- 28- عبد الإله النوايسه، جرائم تكنولوجيا المعلومات، دار وائل للنشر و التوزيع، ط1، الأردن، 2017.

29- عادل عزام سقف الحيط، جرائم الذم والقذح والتحقيق المرتكبة عبر الوسائط الإلكترونية، شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات، دار الثقافة للنشر والتوزيع، 2019.

المجلات:

1. أحمد حسين، حجية الأدلة المستمدة من الهواتف النقالة في الإثبات الجنائي، مجلة الفكر، د.م.ج، العدد 15، جوان 2017.
2. بن عميروش ريمة، (عن خصوصية الجريمة المعلوماتية)، مجلة الفقه القانوني والسياسي، المجلد 02، العدد 02، ديسمبر 2020.
3. جمال الدين بوقرة، جمال الدين عنان، (القطب الجزائري لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)، مجلة الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01 جوان 2022.
4. د. بخدة صفيان- د. وقاص ناصر، الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الإنترنت كنموذج، جامعة دكتور مولاي الطاهر سعيدة، مجلد 03، العدد 16، 18-14-2021.
5. د. بخدة صفيان ود. وقاص ناصر، الطبيعة القانونية لجرائم المستحدثة ووسائل ارتكابها جريمة الإنترنت كنموذج، جامعة دكتور مولاي الطاهر، سعيدة، مجلة البحوث القانونية والسياسية، المجلد 03، العدد 16، 2021.
6. د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهةها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، 2018.
7. ذياب سليمة، بوترة بلال، الجريمة الإلكترونية الأسس والمفاهيم، مجلة تطور العلوم، المجلد 13، العدد 01، الجزائر، جامعة زيان عاشور، الجلفة، 2020.

8. شاين نوال، الجريمة الالكترونية في التشريع الجزائري-ماهيتها، موضوعها، خصائصها، مظاهر تحدياتها، جامعة الحاج لخضر باتنة1، الجزائر تاريخ، مجلة سوسيوولوجيا، المجلد06، العدد 02، 2022.
9. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائرية، مجلة مركز دراسات الكوفة، جامعة الكوفة، كلية القانون، العدد السابع، 2008.
10. مهداوي حنان، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، جامعة محمد الأمين دباغين، سطيف2، المجلد6، العدد2، 2022.
11. ياسمين بونعارة، الجريمة الالكترونية، مجلة المعيار لكلية أصول الدين، جامعة الأمير عبد القادر، 2015/06/19، العدد39.

المدخلات العلمية:

1. بدرة إبراهيم لعور، الأمن الالكتروني وفقا للتشريع الجزائري، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال نموذجاً.
2. بن غدفة شريفة والقص صليحة، الجريمة الالكترونية الممارسة ضد المرأة على صفحات الإنترنت وطرق محاربتها، أعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017.
3. فضيلة عاقل، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الالكترونية"، طرابلس، بتاريخ 24-24 مارس 2017.
4. نمدي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017.

المذكرات وأطروحات دكتوراه

المذكرات الماستر:

1. أسماء بن لعربي، خصوصية الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2021/2020.
2. دحلوز محمد، النصب والاحتيال على المواقع الالكترونية وسبل مواجهتها، مذكرة لنيل شهادة الماستر، جامعة عبد الحميد بن باديس، مستغانم، 2023-2022.
3. بسمة خوني، جرائم الاعتداء على الأموال عبر الوسائط الالكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي، أم البواقي، 2018/2017.
4. بلعربي إكرام، بطاقة الائتمان المصرفية ومسئوليتها الجزائية، مذكرة لنيل شهادة الماستر، جامعة أبو بكر بلقايد، تلمسان، 2022-2023.
5. دحلوز محمد، النصب والاحتيال على المواقع الالكترونية وسبل مواجهتها، مذكرة لنيل شهادة الماستر، جامعة عبد الحميد ابن باديس، مستغانم، 2023-2022.
6. نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الاداري، جامعة أحمد درارية، أدرار، 2017-2016.
7. يوسف جفال، التحقيق في الجريمة الالكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016-2017.
8. عقباش فريزة ومبارك حنان، آليات مواجهة الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد البشير الإبراهيمي، برج بوعرييج، 2021-2022.

رسائل الماجستير:

1. حدي نسيمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2014/2013..

2. حمزة بن عقون ، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الاجرام وعلم العقاب،جامعة الحاج لخضر-باتنة-، كلية الحقوق والعلوم السياسية، 2012/2011.
3. سفيان سوبر، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011/2010.
4. صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون "تخصص القانون الدولي للأعمال"، جامعة مولود معمري، تيزي وزو- كلية الحقوق والعلوم السياسي، 2013.

أطروحة الدكتوراه:

1. جمال خفيف، جرائم المعلوماتية الواقعة على الأموال، أطروحة لنيل شهادة الدكتوراه، تخصص القانون، كلية الحقوق، جامعة الجزائر 01، 2016-2017.
2. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، 2018.
3. رضا بوغرزة، شبكة الإنترنت وعلاقتها باكتساب السلوك الانحرافي لدى الشباب المراهق، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة محمد لمين دباغين، سطيف، 2016/2017.
4. محمد التوجي، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2018/2019.
5. مراد يرمش، خصوصية الجريمة الالكترونية، أطروحة الدكتوراه علوم في القانون الخاص، تخصص الملكية الفكرية، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2020-2021.

مواقع الإنترنت:

- عبد العال الديبي، الجريمة المعلوماتية (تعريفها - أسبابها - خصائصها)، صادر عن المركز العربي لأبحاث القضاء الالكتروني، 2013،
[.http://accronline.com/article_detail.aspx?id=7509](http://accronline.com/article_detail.aspx?id=7509)



فهرس
المحتوى

الفهرس

	الشكر
	الإهداء
(1)-(5)	المقدمة
07	الفصل الأول: الإطار المفاهيمي لجريمة المساس بالأموال الإلكترونية
08	المبحث الأول: ماهية الجريمة المساس الإلكترونية
08	المطلب الأول: مفهوم جريمة المساس بالأموال الإلكترونية
08	الفرع الأول: تعريف الجريمة الإلكترونية
08	أولاً: المفهوم الضيق للجريمة الإلكترونية
12	ثانياً: المفهوم الواسع للجريمة الإلكترونية
14	ثالثاً: التعريف القانوني للجريمة الإلكترونية
15	الفرع الثاني: تعريف المال المعلوماتي وصوره
15	أولاً: تعريف المال المعلوماتي
19	ثانياً: صور المال المعلوماتي
21	المطلب الثاني: خصائص الجريمة الإلكترونية و أركانها
21	الفرع الأول: خصائص الجريمة الإلكترونية
32	الفرع الثاني: أركان الجريمة الإلكترونية
35	المبحث الثاني: الطبيعة القانونية للجرائم الماسة بالأموال الإلكترونية و أنواعها
36	المطلب الأول: الطبيعة القانونية للجرائم الماسة بالأموال الإلكترونية
36	المطلب الثاني: أنواع الجرائم الماسة بالأموال الإلكترونية الإلكترونية.
37	الفرع الأول: كيفية ارتكاب الجريمة الإلكترونية
41	الفرع الثاني: الأساليب التقنية المستخدمة في إتلاف المعلومات
41	الفرع الثالث: أنواع الجرائم الماسة بالأموال الإلكترونية

45	الفصل الثاني: الجريمة الإلكترونية في التشريع الجزائري
46	المبحث الأول: نظرة المشرع الجزائري للجريمة الإلكترونية.
46	المطلب الأول: موقف المشرع الجزائري للجريمة الإلكترونية
50	الفرع الأول: المقصود بنظام المعالجة الآلية للمعطيات
51	الفرع الثاني: مدى اشتراط الحماية التقنية للنظام المعلوماتي
53	المطلب الثاني: مظاهر وتحديات الجريمة الإلكترونية.
56	المبحث الثاني: آليات مكافحة ومعالجة جريمة المساس بالأموال الإلكترونية
57	المطلب الأول: الحماية القانونية لوسائل الدفع الإلكتروني.
58	الفرع الأول: الحماية الجنائية المباشرة
58	أولا: تجريم الاحتيال الإلكتروني
57	ثانيا: تجريم استخدام أو الحصول على أرقام بيانات ووسائل الدفع الإلكتروني
63	الفرع الثاني: الحماية الجنائية غير المباشرة
64	أولا: تجريم الاعتداء على نظام الدفع الإلكتروني
65	ثانيا: تجريم الاعتداء على بيانات المواقع الإلكترونية
65	المطلب الثاني: الهيئات المكلفة بمواجهة الجريمة المعلوماتية في الجزائر.
67	الفرع الأول: الهيئات الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال.
75	الفرع الثاني: إجراءات التحري المستحدثة للكشف عن جرائم المعلوماتية
84	الخاتمة
	قائمة المراجع

ملخص مذكرة الماستر

تعتبر جرائم المساس بالأموال الالكترونية من الجرائم المستحدثة والمتميزة عن مختلف أشكال الجرائم الكلاسيكية وهذا من خلال طبيعتها وموضوعها وخصائصها. إذ أن المشرع الجزائري لم يتحدث عن جريمة المساس بالأموال الالكترونية بصفة خاصة بل بالجرائم الالكترونية بصفة عامة.

وتشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري جرمي الدخول والبقاء غير المشروع للنظام المعلوماتي، وجرمي الغش المعلوماتي وكذا جريمة اتلاف النظام الآلي ولقد حاول المشرع الجزائري مواجهة هذه الجرائم في ذلك مختلف التشريعات الحديثة من خلال تعديل قانون العقوبات وفق 15/04 الذي إستحدث بعض الجرائم ضمن القسم السابع منه المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات".

الكلمات المفتاحية:

- | | | |
|------------------------|------------|-------------------|
| 1/ الأموال الالكترونية | 2/ الجرائم | 3/ قانون العقوبات |
| 4/ الجريمة الالكترونية | 5/ الآلي | 6/ الأنظمة |

Abstract of Master's Thesis

The offences of infringement of electronic funds are the crimes developed and distinct from the various forms of classical crimes through their nature, object and characteristics. The Algerian legislature had not spoken of the crime of infringing electronic funds in particular, but of cybercrime in general.

The offences of infringement of automated data-processing regulations in Algerian legislation include the offences of entry and unlawful survival of the information system, the offences of information fraud, as well as the offence of damaging the automated system. Algerian legislation has attempted to counter these offences in various modern legislation by amending the Penal Code in accordance with the 04/15 introduced by section VII of the Code, entitled "Inf.

Keywords:

- | | | |
|---------------------|--------------|---------------|
| 1/ electronic money | 2/ crimes | 3/ penal code |
| 4/ cybercrime | 5/ automated | 6/ systems |